

ИНИЦИЈАТИВИ НА ГРАЃАНСКОТО ОПШТЕСТВО ЗАЈАКНАТИ СО БЕЗБЕДНОСТ НА ИНФОРМАЦИИТЕ И ПОДАТОЦИТЕ

ПРАКТИЧЕН ВОДИЧ ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА И НАСТАВНА ПРОГРАМА ЗА ЗАЈАКНУВАЊЕ НА ДИГИТАЛНАТА БЕЗБЕДНОСТ ВО ГРАЃАНСКОТО ОПШТЕСТВО

ПРАКТИЧЕН ВОДИЧ ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА И НАСТАВНА ПРОГРАМА ЗА ЗАЈАКНУВАЊЕ НА ДИГИТАЛНАТА БЕЗБЕДНОСТ ВО ГРАЃАНСКОТО ОПШТЕСТВО

Анкара, 2026 година

Оваа студија е спроведена во рамките на проектот насловен како „ИНИЦИЈАТИВИ НА ГРАЃАНСКОТО ОПШТЕСТВО ЗАЈАКНАТИ СО БЕЗБЕДНОСТ НА ИНФОРМАЦИИТЕ И ПОДАТОЦИТЕ“ (2023-1-TR01-KA220-YOU-000161230), поддржан од Турската национална агенција и Европската комисија во рамките на програмата Еразмус+. Содржината презентирана овде ги одразува ставовите на авторот и ниту Европската комисија ниту Турската национална агенција не можат да бидат одговорни за овие ставови.



2026 година

Академски советник: Erman Akıllı

Дизајн и распоред на корицата:

Уредници: Sibel Koru

Zeyneb Güşta Arık

Ревизии на текстот: Cenay Babaoğlu

Датум: Анкара, 2026 година

Во денешниот хиперповрзан свет, организациите на граѓанското општество (ГО), почнувајќи од невладините организации и групите за застапување, до независните медиуми и мрежите на заедницата, работат на сè посложена дигитална фронтовска линија. Иако дигиталните алатки го проширија досегот, ефикасноста и влијанието на граѓанското општество, тие истовремено ги изложија организациите на зголемени ризици од сајбер безбедноста. Како што граѓанското општество станува сè подигитално зависно, тоа станува и сè подигитално ранливо.

Низ цела Европа и пошироко, граѓанските организации сè повеќе се препознаваат како актери со висок ризик во дигиталниот екосистем. Сајбер заканите насочени кон граѓанското општество сега се движат од фишинг, рансомвер, шпионски софтвер и напади со одбивање на услуга, до софистициран надзор спонзориран од државата, насочен кон замолчување на несогласувањата и поткопување на демократските вредности. За организациите кои често работат со ограничен технички капацитет, а сепак управуваат со чувствителни лични и организациски податоци, дигиталната несигурност претставува не само оперативен ризик, туку и егзистенцијален.

Во овој контекст, дигиталната безбедност повеќе не е чисто техничка грижа. Таа е од клучно значење за мисијата. Способноста на организациите на граѓанското општество безбедно да работат онлајн е неразделна од нивната способност да ја заштитат слободата на изразување, транспарентноста, отчетноста и заедниците на кои им служат. Затоа, зајакнувањето на дигиталната безбедност во рамките на граѓанското општество бара повеќе од ad hoc технички поправки. Потребно е структурирано учење, стратешко планирање и практични насоки што можат да се имплементираат во реални организациски услови.

Како одговор на оваа потреба, проектот KA220 Erasmus+ „Иницијативи на граѓанското општество зајакнати со безбедност на информациите и податоците“ беше иницира како колаборативен, мултинационален напор за подобрување на капацитетот за дигитална безбедност на организациите на граѓанското општество. Еден од централните резултати на овој проект е оваа публикација, која намерно ги спојува двете комплементарни функции во еден том.

Оваа книга е дизајнирана и како наставна програма и како практичен водич.
Од една страна, функционира како структурирана наставна програма за дигитална безбедност за граѓанското општество, нудејќи кохерентен пат на учење што постепено гради знаење – од разбирање на дигиталниот пејзаж на закани до развивање организациски политики и механизми за одговор на инциденти. Структурата ориентирана кон наставната програма го прави погоден за употреба во обуки, работилници, програми за градење капацитети и активности за обука на обучувачи во различни национални контексти.

Од друга страна, книгата служи како практичен водич, обезбедувајќи конкретни, практични упатства што организациите можат директно да ги применат во нивното секојдневно работење. Наместо да остане на ниво на теорија, таа ги преведува принципите на сајбер безбедноста во практични чекори, контролни листи, примери и рамки за донесување одлуки прилагодени на реалноста на граѓанските организации и на иницијативите на локално ниво што работат со ограничени ресурси.

Со комбинирање на овие две димензии, книгата премостува критичен јаз помеѓу учењето и имплементацијата. Им овозможува на читателите не само да разберат зошто дигиталната безбедност е важна, туку и како да ја операционализираат во рамките на сопствените организации. Читателите можат да пристапат кон книгата секвенцијално како наставна програма или селективно како референтен водич што се справува со специфични предизвици како што се обезбедување на комуникациите, заштита на податоците, проценка на ризиците или градење внатрешна култура на дигитална безбедност.

Напишана на достапен, но академски заснован стил, публикацијата се потпира на искуство базирано на проекти, теренски сознанија и воспоставени најдобри практики во сајбер безбедноста и градењето капацитети на граѓанското општество. Нејзината модуларна структура овозможува прилагодување кон различни организациски потреби, технички нивоа и национални регулаторни средини.

На крајот на краиштата, овој комбиниран наставен план и водич има за цел да ги оспособи организациите на граѓанското општество да ја преземат одговорноста за нивната дигитална безбедност. Со поттикнување и на знаењето и на практичните способности, ги поддржува граѓанските организации во зајакнувањето на нивната отпорност, заштитата на нивната дигитална инфраструктура и продолжувањето на нивната суштинска работа со поголема самодоверба и одржливост во сè поконкурентниот дигитален простор.

СЕТА, Анкара/Турција

СОДРЖИНА:

1.1 ЦЕЛ НА ПРОЕКТОТ:

„Иницијативи на граѓанското општество зајакнати со безбедност на информациите и податоците“ е проект КА220 Еразмус+ координиран од SETA (Турција) и имплементиран во соработка со партнерски организации од Северна Македонија, Норвешка, Босна и Херцеговина, Белгија и Турција. Проектот беше финансиран од Европската комисија преку Турската национална агенција и беше дизајниран да се справи со растечките предизвици со кои се соочуваат организациите на граѓанското општество во сè повеќе дигитализирана средина.

Примарната цел на проектот беше да се подобри дигиталната писменост, свеста за сајбер безбедноста и капацитетите за заштита на податоците во рамките на граѓанското општество, а истовремено да се промовира инклузијата, различноста и еднаквиот пристап до дигитални вештини. Во текот на неговото спроведување, проектот ги поддржа и поединците и институциите во справувањето со процесите на дигитална трансформација и во зајакнувањето на нивната отпорност кон сајбер заканите, и дезинформациите. Во оваа рамка, проектот произведе низа значајни интелектуални и практични резултати. Тие вклучуваа сеопфатна **наставна програма за дигитална безбедност за граѓанското општество,** модули за обука за дигитална писменост и сајбер безбедност, со што се обезбеди пристапност и инклузивноста на процесите на дигитална трансформација. Покрај тоа, беше развиен и **Практичен водич за дигитална трансформација** за да им помогне на организациите на граѓанското општество во планирањето, спроведувањето и одржувањето на ефективни стратегии за дигитална трансформација.

Понатаму, проектот разви софтверски базиран **онлајн центар за тестирање на дигитална безбедност за граѓански организации за** да се процени подготвеноста за сајбер безбедноста на организациите од граѓанското општество. Платформата им овозможува на граѓанските организации да ги проценат своите нивоа на дигитална безбедност, вклучувајќи аспекти како што се практиките за заштита на податоците, конфигурациите за безбедност на системот и безбедната употреба на онлајн алатките (на пр.: структури на домени, користење на HTTPS и основни заштитни мерки за дигитална инфраструктура). Преку оваа алатка, организациите се во можност да идентификуваат ранливости, да ја подигнат свеста за постојните ризици и да поддржат процеси на градење капацитети и подобрување на дигиталната безбедност засновани на докази.

Покрај образовните резултати, проектот генерираше и материјали и кампањи за подигање на свеста фокусирани на безбедни и одговорни дигитални практики. Покрај тоа, успеа да воспостави робусна меѓународна мрежа за соработка меѓу земјите-партнери, поставувајќи ја основата за долгорочно градење капацитети, размена на знаење и одржлива соработка во областа на дигиталната безбедност за граѓанското општество.

1.2 ПАРТНЕРИ НА ПРОЕКТОТ:

ФОНДАЦИЈА ЗА ПОЛИТИЧКИ, ЕКОНОМСКИ И СОЦИЈАЛНИ ИСТРАЖУВАЊА – SETA (КООРДИНАТОР)

Фондацијата за политички, економски и социјални истражувања (SETA) е непрофитна тинк-тенк организација фокусирана на производство на точни и ажурирани

анализи за национални, регионални и меѓународни прашања. Нејзината цел е да ги информира креаторите на политики и јавноста за политичките, економските, социјалните и културните случувања во рамките на историскиот и културниот контекст. Како институција за истражување и препораки за политики, СЕТА поттикнува меѓународен дијалог, зближувајќи ги различните перспективи преку научни стандарди. Придонесува за информирано донесување одлуки од страна на владата, граѓанското општество и бизнис лидерите преку истражувачки извештаи, публикации, конференции и препораки за политики. СЕТА усвојува интердисциплинарен пристап, препознавајќи ја меѓузависноста на политичките, економските и социо-културните прашања и се стреми да промовира визија вкоренета во мирот, правдата, еднаквоста и владеењето на правото. Нејзината мисија е да ги збогати стратешките дебати и да обезбеди независни, авторитативни увиди за донесувачите на одлуки и во јавниот и во приватниот сектор.

ФОНДАЦИЈА ЗА ПОЛИТИЧКИ, ЕКОНОМСКИ И СОЦИЈАЛНИ ИСТРАЖУВАЊА – СЕТА БРИСЕЛ

Фондацијата СЕТА за политички, економски и социјални истражувања е непрофитен истражувачки институт фокусиран на иновативни студии поврзани со национални, регионални и меѓународни прашања со седиште во Брисел. Нејзината цел е да произведува точни знаења и анализи во политиката, економијата и општеството, а воедно да ги информира креаторите на политиките и јавноста за еволуирачките политички, економски, социјални и културни услови. Таа го поттикнува меѓународниот дијалог преку спојување на различни перспективи преку истражувачки извештаи, публикации, конференции и препораки за политики. Фондацијата има за цел да го поддржи информираното донесување одлуки во Турција преку обезбедување авторитетни информации и анализи за лидерите во јавниот и во приватниот сектор. Интердисциплинарниот истражувачки пристап на СЕТА се занимава со меѓузависноста на политичките, економските и социо-културните прашања, стремејќи се кон визија заснована на мир, правда, еднаквост и владеење на правото.

ЗДРУЖЕНИЕ ЗА ИДНИНА И ИНОВАЦИИ АНКА

АНКА е иновативна и динамична невладина организација (НВО) со седиште во Истанбул. Основана во мај 2019 година, таа се фокусира на подобрување на менталната, физичката и економската благосостојба на поединците преку нудење алтернативни спортски активности, обуки, иницијативи и можности. АНКА има за цел да ја интегрира технологијата и образованието, обезбедувајќи решенија што додаваат вредност на поединците и општеството. Организацијата има експертиза во развој на мобилни апликации, вештачка интелигенција, веб-технологии, управување со проекти и 3Д моделирање. Нејзините членови доаѓаат од различни професионални средини, вклучувајќи претприемништво, софтвер, технологија, здравство и образование. Дополнително, АНКА организира образовни, културни и социјални активности за да ги вклучи младите и да поттикне активен, здрав живот. Организацијата се стреми континуирано да ги развива своите вештини во софтверскиот сектор и да придонесува кон процесите на доживотно учење преку иновативни технолошки решенија.

БОСАНСКО РЕПРЕЗЕНТАТИВНО ЗДРУЖЕНИЕ ЗА ВРЕДНИ МОЖНОСТИ (БРАВО)

Босанското репрезентативно здружение за вредни можности (БРАВО) е динамична невладина организација со седиште во Босна и Херцеговина, фокусирана на јакнење на поединците и заедниците преку образование, развој на вештини и градење капацитети. Нејзината мисија нагласува социјална инклузија, културна размена и одржлив развој. БРАВО работи во различни сектори, вклучувајќи го јакнењето на младите, свеста за животната средина, претприемништвото и технологијата. Има посветен тим од платен персонал и волонтери кои соработуваат на бројни проекти. БРАВО организира програми за размена на млади за промовирање на меѓукултурното разбирање и личниот раст, а воедно ја поддржува и еколошката одржливост преку иновативни проекти. Им помага на амбициозните претприемачи со менторство и ресурси, фокусирајќи се на социјалното влијание. Дополнително, БРАВО нуди работилници за дигитални вештини, како што се програмирање и веб развој, помагајќи им на поединците да го подобрат својот личен и професионален раст во технологијата.

ТЕХНОЛОГИЈА ЗА ПОДОБРУВАЊЕ НА УТРЕШНИНАТА (ТТВ)

Технологија за подобрување на утрешнината (ТТВ) е невладина организација со седиште во Норвешка, посветена на обезбедување образование и обука за технологија и дигитални вештини за промовирање одржлива иднина. Основана на 6 октомври 2019 година од студенти во Тронdхајм, ТТВ има за цел да го зголеми учеството на младите во заедницата преку нудење можности за стекнување знаење и корисни вештини. Со тим од 15 платени вработени и бројни волонтери, ТТВ спроведува проекти во образованието, животната средина и претприемништвото. Организацијата се фокусира на дигитални иновации, младинска работа и интеграција на дигитални алатки. Клучните активности вклучуваат образование за дигитални вештини, еколошки иницијативи и поддршка на претприемачи, особено во технологијата и во одржливоста. ТТВ ја цени отвореноста, соработката, храброста и грижата, поттикнувајќи одржлива, етичка и општествено одговорна средина. Се вклучува во регионална и меѓународна соработка.

МЛАДИНСКА ФОНДАЦИЈА НА ТУРЦИЈА (ТУГВА)

Основана во 2014 година, Фондацијата за млади на Турција (ТУГВА) е една од најголемите граѓански организации во Турција, со тим од над 100 професионалци и 300.000 волонтери. Нуди работилници за роботско кодирање во 39 градови и управува со 42 студентски домови. Фондацијата работи со 10 координатори во различни области, вклучувајќи спорт, женски права, претприемништво, медиуми, образование, култура и кариерен развој. Нејзината примарна мисија е да го поддржи сеопфатниот развој на младите, фокусирајќи се на физичката и на менталната благосостојба, особено во Турција. Фондацијата има за цел да ги оспособи младите луѓе да станат иновативни, продуктивни и вредни членови на општеството. Со повеќе од 200 завршени национални и меѓународни проекти, нејзината визија е да негува генерации способни за обнова и унапредување на цивилизацијата преку континуирано самоподобрување и културно збогатување.

ЗДРУЖЕНИЕ НА ГРАЃАНИ – МАКЕДОНСКА АСОЦИЈАЦИЈА ЗА ЧОВЕЧКИ РЕСУРСИ, СКОПЈЕ (МАЧР)

Македонската асоцијација за човечки ресурси (МАЧР) е непрофитна, невладина национална организација фокусирана на развој на вештини на работната сила, промоција на човечкиот капитал и стандардизација на неформалното образование. Членството на МАЧР вклучува над 120 активни индивидуални членови, првенствено жени, и повеќе од 600 пасивни членови од областа на човечки ресурси, заедно со над 60 компании од јавниот и приватниот сектор. Здружението делува како отворена платформа која ги интегрира поединците во сите фази од кариерата, вклучувајќи менаџери за човечки ресурси, консултанти, вработени и студенти. Вклучено е во обликувањето на политиките поврзани со бизнисот, образованието и социо-економските прашања на национално и на локално ниво. Официјален член на Европската асоцијација за управување со луѓе (EAPM) од 2012 година, МАЧР, исто така, го прифаќа волонтирањето како основна вредност во своите локални и меѓународни иницијативи.

2. ПРАКТИЧЕН ВОДИЧ ЗА ДИГИТАЛНА ТРАНСФОРМАЦИЈА

2.1 ПОГЛАВЈЕ 1: ДИГИТАЛНА БЕЗБЕДНОСТ ЗА ГО

Што е дигитална безбедност?

Дигиталната безбедност, позната и како сајбер безбедност, е практика на заштита на дигитални информации, уреди и други средства од неовластен пристап или штета. Опфаќа мерки за заштита на лични податоци, сметки, датотеки, па дури и финансиски ресурси складирани или пренесени онлајн. Во суштина, дигиталната безбедност има за цел да обезбеди доверливост, интегритет и достапност на информациите (честопати сумирани како „тријада на ЦИА“ - Доверливост, Интегритет, Достапност).

Зошто е важна дигиталната безбедност?

Во денешниот хиперповрзан свет, речиси секоја организација и поединец се потпира на дигитални системи. За граѓанските организации и за невладините организации, ова потпирање вклучува комуникација со засегнатите страни, управување со информациите за донаторите и испорака на услуги. Заштитата на овие дигитални активности е клучна. Сајбер нападите можат да ги нарушат операциите, да ги прекршат чувствителните податоци и да ја нарушат довербата што донаторите и заедниците ја имаат во организацијата. На пример, прекршување на податоците во Австралискиот црвен крст во 2016 година ги откри личните податоци на над 550.000 дарители на крв поради човечка грешка (необезбедена резервна датотека). Инцидентот не само што покрена прашања за практиките на организацијата во врска со податоците, туку доведе и до губење на довербата на донаторите, илустрирајќи како сајбер инцидентите можат да им наштетат на вистински луѓе и да ја еродираат јавната доверба во мисијата на граѓанските организации.

Важно е да се напомене дека непрофитните организации се сè повеќе цел на сајбер криминалци, па дури и на хакери поддржани од државата. Извештај на „Мајкрософт“ покажа дека хуманитарните организации и организациите за човекови права се вториот сектор подложен на сајбер нападите од националните држави, сочинувајќи 31% од

известувањата за вакви напади во 2025 година. Студија од 2023 година за непрофитните организации со седиште во Женева откри дека 41% доживеале сајбер напад во последните години. Сепак, над половина од тие организации немале наменет буџет за сајбер безбедност, а 70% сметале дека им недостасуваат вештини и отпорност за да одговорат на напади. Овие бројки нагласуваат дека дигиталната безбедност повеќе не е опционална, туку императив за организациите. Без соодветни заштитни мерки, сајбер инцидентите можат да ги запрат критичните услуги, да ги компромитираат податоците на корисниците и да го загрозат финансирањето со оштетување на угледот на организацијата.

Покрај тоа, дигиталната безбедност е тесно поврзана со физичката безбедност и човековите права во работата на граѓанското општество. Активистите, новинарите и граѓанските организации често се соочуваат со дигитални закани насочени кон надзор или кон заплашување. Нарушувањето на безбедноста или хакирањето може да ги открие чувствителните комуникации или идентитетите на партнерите и на корисниците, потенцијално доведувајќи ги во опасност животите или средствата за живот. Затоа, инвестирањето во дигитална безбедност е инвестирање во целокупната отпорност и доверливост на работата на една организација.

Што значи дигиталната безбедност за граѓанските организации?

За организациите на граѓанското општество, дигиталната безбедност значи заштита на информациите и технологијата што им овозможуваат за нивните општествени мисии. ГО рутински собираат и складираат чувствителни податоци – од лични податоци на поддржувачите и персоналот до стратешки планови и истражувања. Обезбедувањето на доверливоста и интегритетот на овие податоци е од најголема важност за да не паднат во погрешни раце или да бидат манипулирани. На пример, група за застапување можеби ќе треба да обезбеди контакт листи на активисти или докази за злоупотреба на човековите права. Доколку таквите информации протекуваат или се менуваат од злонамерни актери, тоа би можело да ги загрози поединците или да ја поткопа каузата.

Дигиталната безбедност за граѓанските организации (ГО) вклучува и заштита на секојдневните операции. Многу организации се потпираат на е-пошта, апликации за пораки и облак платформи за координирање на активностите. Доколку тие сметки се компромитирани, напаѓачите би можеле да ги прекинат комуникациите или да се претстават како ГО. Во еден реален случај, е-пошта системот на добротворна организација бил хакиран преку фишинг е-пошта со прилог од малициозен софтвер, што довело до напад со рансомвер кој го криптирал серверот на организацијата. Напаѓачите побарале откуп во замена за клучот за дешифрирање. Бидејќи ГО имала неодамнешни резервни копии на податоци и одлучила да не плати, успеала да ги врати повеќето од своите податоци, но околу две недели информации биле трајно изгубени. Овој инцидент ја илустрира и заканата и важноста на подготвеноста: без силни резервни копии и план за одговор, исходот можел да биде многу полош.

За групите на граѓанското општество кои работат во чувствителни политички средини, дигиталната безбедност добива дополнително значење на заштита на безбедноста на нивните членови и заедниците на кои им служат. Репресивните субјекти можат да користат сајбер средства за да ги шпионираат граѓанските организации или да ги таргетираат со дезинформации. Така, дигиталната безбедност за граѓанските организации

честопати нагласува алатки за подобрување на приватноста (како што е енкрипција за е-пошта и пораки) и безбедни комуникациски канали за да се спречи надзор. Како што забележува Liberties, европска организација за граѓански слободи: граѓанските организации кои користат дигитални алатки за активизам се соочуваат со уникатни закани и мора да негуваат култура на „дигитална самоодбрана“ што ги опфаќа луѓето, процесите и технологијата. Во практична смисла, ова значи обука на персоналот и волонтерите за безбедносна свест, воспоставување јасни политики (на пример, за ракување со лични податоци или користење безбедни апликации) и континуирано ажурирање на техничката заштита.

Конечно, дигиталната безбедност за граѓанските организации е поврзана со одржување на довербата. Донаторите и корисниците очекуваат организациите да бидат добри чувари на информациите. Добро објавен сајберинцидент може да ја разниша довербата на јавноста и да ги одврати луѓето од ангажирање или придонес. На пример, по претходно споменатото протекување на податоци од Црвениот крст, организацијата забележа пад на донациите на крв и мораше да работи на повторно градење на довербата. Со давање приоритет на дигиталната безбедност, граѓанските организации ја покажуваат својата посветеност на отчетноста и приватноста, кои се основни вредности во секторот на граѓанското општество.

Чести дигитални закани и ризици за граѓанските организации

Граѓанските организации се соочуваат со многу од истите сајбер ризици како и бизнисите и поединците, но честопати со помалку ресурси за справување со нив. Некои вообичаени закани вклучуваат:

- **Хакери и малициозен софтвер:** Напаѓачите може да се обидат да се инфилтрираат во мрежата или уредите на организацијата за заштита на лични податоци (CSO) за да украдат податоци или да ги нарушат услугите. Ова може да се случи преку малициозен софтвер (малициозен софтвер како вируси, шпионски софтвер или ransomware) доставен преку прилози во е-пошта, штетни линкови или заразени USB-уреди. Ransomware е особено штетен малициозен софтвер кој ги криптира датотеките и бара плаќање. Тој нападнал организации од сите големини, од мали непрофитни организации до цели градски самоуправи. Ако организацијата за заштита на лични податоци нема силна одбрана од малициозен софтвер и резервни копии на податоци, нападот со ransomware би можел ефикасно да ги парализира нејзините операции.
- **Фишинг и социјален инженеринг:** Фишингот е тактика каде што напаѓачите испраќаат лажни е-пораки или пораки што изгледаат легитимно (на пример, претставувајќи се како колега или давател на услуги) за да ги измамат примателите да откријат лозинки или да преземат малициозен софтвер. Фишингот е една од најраспространетите закани и честопати е влезна точка за поголеми напади. Граѓанските организации биле мета на фишинг измами; на пример, една образовна непрофитна организација речиси изгубила финансирање кога напаѓачите лажирале е-пораки за да измамат партнер да испрати плаќање на погрешна банкарска сметка (форма на „компромитирање на деловна е-пошта“). Вообичаените знаци на фишинг вклучуваат итен или алармантен јазик, барања за чувствителни информации или малку погрешно

напишани е-адреси. Социјалниот инженеринг може да се случи и преку телефонски повици (вишинг) или текстуални пораки (смишинг) кои се претставуваат како доверливи субјекти.

- **Пробивање податоци:** Пробивањето на податоци се случува кога се пристапува до доверливи информации или се откриваат без овластување. Ова може да биде резултат на хакирање, злоупотреба од страна на инсајдери или дури и случајно изложување. Граѓанските организации често чуваат лични податоци (на пр., детали за корисниците, финансиски евиденции на донаторот, информации за здравјето или правниот случај) кои се привлечни за напаѓачите или би можеле да бидат протечени. Како што споменавме, погрешно конфигурираните сервери или складирањето во облакот можат ненамерно да протекуваат податоци – инцидентот со Црвениот крст е еден пример. Влијанието на прекршувањето за граѓанските организации е сериозно: може да доведе до кражба на идентитет за поединци во податоците, да ги прекрши законите за приватност и да го оштети угледот и правната положба на организацијата. За жал, многу прекршувања се должат на човечка грешка. Всушност, извештај од индустријата откри дека 74% од прекршувањата вклучуваат „човечки елемент“, како што се грешки или станување жртва на фишинг. Ова ја истакнува потребата од обука и внимателно ракување со податоците.
- **Неовластен пристап до сметка:** Напаѓачите можат да ги таргетираат сметките што ги користат вработените во Здружението на граѓански организации (ЗЗО), како што се е-пошта, социјални медиуми или платформи за собирање средства. Со крадење или погодување лозинки (или користење протечени податоци од претходни пробиви), тие можат да ги „ограбат“ овие сметки. Знаците на компромитирање вклучуваат известувања за најавување од непознати локации, нови е-пораки или објави испратени од корисникот или неможност за најавување (лозинката е променета од напаѓач). На пример, ако официјалната сметка на ЗЗО на социјалните медиуми е хакирана, таа може да се користи за ширење лажни информации или измама на следбениците на ЗЗО. Користењето силни, уникатни лозинки и двофакторска автентикација (дискутирано во Поглавје 2) се клучни одбрани од преземањето сметки.
- **Дефејсинг на веб-страница или DDoS:** Граѓанските организации со веб-страници наменети за јавноста би можеле да доживеат обезличување (напаѓачи кои ја менуваат содржината на страницата за да шират пораки или пропаганда) или напади со дистрибуирано одбивање на услуга (DDoS) кои ја преплавуваат страницата со сообраќај за да ја исклучат. Овие напади понекогаш ги извршуваат хактивисти или противници кои се обидуваат да го замолчат гласот на граѓанската организација. Една граѓанска организација открила дека нивната веб-страница била пренасочена кон страница од трета страна откако напаѓачите ги искористиле ранливостите, и бидејќи немале неодамнешна резервна копија, им биле потребни девет месеци за да ја обноват нивната страница. Обезбедувањето ажуриран и резервен софтвер на веб-страницата може да ги ублажи ваквите ризици.
- **Внатрешни закани и човечки грешки:** Не сите ризици доаѓаат од анонимни хакери. Понекогаш, внатрешните лица (вработени или волонтери) можат случајно или намерно да предизвикаат безбедносни инциденти. Ова може да се движи од губење на необезбеден лаптоп што содржи чувствителни датотеки до погрешно конфигурирање на базата на податоци до незадоволен член на персоналот што презема податоци пред заминување. ГО треба да бидат внимателни на внатрешните контроли за пристап и

принципот на најмали привилегии (давање пристап на персоналот само до информациите и системите потребни за нивната улога). Покрај тоа, негувањето на организациска култура на безбедност може да ги намали грешките – кога луѓето разбираат зошто, на пример, не треба да користат лични USB-уреди или мора да ги следат процедурите за ракување со податоци, помала е веројатноста ненамерно да создадат ранливости.

Накратко, граѓанските организации се соочуваат со широк спектар на дигитални закани – од секојдневни измами како што е фишингот до поцелни напади од страна на софистицирани актери. Поглавје 2 ќе истражи како да се започне со заштита од овие ризици со основни најдобри практики. Но, дури и во оваа воведна фаза, една клучна точка треба да биде јасна: препознавањето на вообичаените ризици е првиот чекор кон нивно управување. Со тоа што знаат што може да тргне наопаку (без разлика дали станува збор за украдена лозинка, вирусна инфекција или протечен документ), организациите и поединците стануваат поподготвени да преземат мерки за да спречат и да одговорат на тие сценарија.

Што ќе понуди оваа книга?

Овој водич е дизајниран да ги опреми организациите на граѓанското општество со практично знаење и вештини за подобрување на нивната дигитална безбедност. Потребно е едноставен, практичен пристап – сличен на курс во стилот на отворен универзитет – со реални примери, контролни листи и едноставни вежби за зајакнување на учењето. Со читање низ поглавјата, вие, читателите ќе ги:

- **Разберете основите:** Ќе ја научите терминологијата и основните концепти на дигиталната безбедност (не грижете се, во Додатокот е вклучен Речник на термини за брза референца). Од основни дефиниции како што е малициозен софтвер до концепти како двофакторска автентикација, ќе го демистифицираме жаргонот за да можете со сигурност да комуницирате за безбедносните прашања.
- **Идентификувате вашите ризици:** Книгата ќе ве води низ проценката на специфичните закани со кои може да се соочи вашата ГО и на кои средства им е потребна заштита. Преку кратки прашања и сценарија за самооценување, ќе започнете со мапирање на профилот на ризик на вашата организација (Глава 3).
- **Имплементирате најдобрите практики:** Нудиме јасни, чекор-по-чекор совети за итни дејствија – на пример, како да креирате силни лозинки, да ги обезбедите вашите уреди и безбедно да го користите интернетот и е-поштата (Поглавје 2). Ова се „брзите победи“ на сајбер-безбедноста кои драстично ја намалуваат вашата ранливост кога се прави доследно.
- **Развиете план за безбедност:** Освен индивидуалните совети, ќе ви покажеме како да го споите сето тоа во едноставен, но ефикасен план за дигитална безбедност за вашиот орган за социјална работа (Глава 3). Ова вклучува предлози за политики, планови за обука за вашиот тим и методи за резервна копија и криптирање на податоци. Дадени се шаблони и примери за да ви помогнат да го изготвите или подобрите сопствениот план.
- **Научите да користите безбедносни алатки:** Поглавје 4 воведува алатки и софтвер за безбедност кои се лесни за користење (од менаџери за лозинки и антивирусни програми до апликации за безбедни пораки). Ги нагласуваме алатките кои се лесни за

користење и често достапни, дури и со мал буџет. Секоја алатка или метод што се дискутира доаѓа со објаснување зошто е корисна и како да се започне со неа.

- **Се подготвите за инциденти:** И покрај најдобрите напори, може да се случат инциденти. Во Поглавје 5, ќе разгледаме како да препознаеме знаци на сајбер инцидент (како знаци дека вашиот компјутер можеби е хакиран) и непосредните чекори што треба да се преземат како одговор. Сфатете го тоа како вежба за итни случаи – знаењето што да се прави може значително да ја ограничи штетата. Исто така, наведуваме ресурси и контакти за добивање помош, бидејќи навремената поддршка може да биде клучна во криза.
- **Ја нагласите соработката:** Клучна тема во ова упатство е дека не сте сами во справувањето со дигиталната безбедност. Поглавје 6 ја дискутира моќта на врсничка поддршка – како граѓанските организации можат да си помагаат едни на други преку споделување предупредувања, совети, па дури и здружување на ресурси за обука. Исто така, се посочуваат мрежи и институции (локални или меѓународни) кои нудат поддршка, од технолошки волонтери до телефонски линии за помош.
- **Обезбедите контекст од реалниот живот:** Во Поглавје 7, презентираме студии на случаи и вообичаени стапици. Ќе прочитате кратки приказни за граѓански организации кои се соочиле со сајбер предизвици и како ги надминале, како и чести грешки што ги прават организациите (за да можете да ги избегнете). Вклучуваме и неколку едноставни вежби за да ја „тестирате“ вашата безбедност - на пример, листа за проверка за ревизија на вашата канцеларија или квиз за фишинг е-пошта за вашиот тим.

До крајот на оваа е-книга, треба да се чувствувате посигурни и поовластени во справувањето со дигиталната безбедност. Содржината е структурирана да биде достапна дури и ако немате ИТ-подготвеност. Секое поглавје се надоградува на претходните, а можете да се вратите и на одредени делови по потреба. Целта не е да ве претвориме во експерт за сајбер безбедност преку ноќ, туку да ви ги дадеме знаењата и навиките што значително ќе ја подобрат вашата заштита од вообичаени закани. Замислете го како прирачник за возачи за дигиталниот пат – не мора да бидете механичар за безбедно возење, но треба да ги научите правилата, да ги користите вистинските алатки (како безбедносни појаси) и да бидете внимателни на опасностите.

Дополнително, низ поглавјата, ќе најдете дополнителни белешки „Дали знаевте?“ и кратки практични совети за да го примените она што сте го научиле. Одвојте малку време да се вклучите во нив; тие се таму за да го зацврстат вашето разбирање и да го направат искуството на учење поинтерактивно. На пример, по делот за лозинки, еден совет може да ве замоли да ја процените јачината на примерокот на лозинката или по делот за резервна копија, да размислите кои податоци во вашата организација се најважни за резервна копија.

На крајот на краиштата, она што оваа публикација ви го нуди е основа во дигиталната безбедност прилагодена за контекстот на граѓанското општество. Со инвестирање време во овие поглавја, правите важен чекор кон заштита на работата на вашата организација и луѓето поврзани со неа. Затоа, да го започнеме патувањето кон побезбедна дигитална иднина за вашата граѓанска организација!

Резиме на поглавјето

Ова поглавје ја воведува критичната важност на дигиталната безбедност за граѓанските организации, истакнувајќи ја нивната ранливост како главни цели за сајбер напади поради нивните улоги на застапување. Ги опишува вообичаените закани како што се малициозен софтвер, фишинг, пробивање податоци, неовластен пристап до сметки, деформирање веб-страница и DDoS напади, нагласувајќи го нивното влијание врз работењето, довербата и безбедноста. Примери од реалниот свет, како што е пробивањето на податоците на Австралискиот црвен крст во 2016 година, со кое беа откриени информации за 550.000 донатори и нападот со ransomware врз добротворна организација, ги илустрираат последиците од несоодветната одбрана. Поглавјето забележува дека 31% од нападите на националните држави во 2025 година биле насочени кон граѓанските организации, при што 41% од непрофитните организации со седиште во Женева се соочиле со напади, но сепак, над половина од нив немаат буџети за сајбер безбедност. Се нагласува дека дигиталната безбедност е критична за мисијата, заштитувајќи чувствителни податоци (на пр. детали за корисниците) и обезбедувајќи континуитет на работењето. За граѓанските организации во чувствителни политички средини, сајбер безбедноста е поврзана со физичката безбедност, спречувајќи надзор или дезинформации. Поглавјето се залага за култура на „дигитална самоодбрана“, комбинирајќи луѓе, процеси и технологија. Ја поставува основата за е-книгата со тоа што ја претставува сајбер-безбедноста како неопходност за преживување, а не само како ИТ прашање, и ги подготвува читателите за практични решенија во следните поглавја. Клучните заклучоци вклучуваат потреба од свест, подготвеност и градење доверба за да се заштитат мисиите на граѓанските организации.

Контролна листа за сајбер безбедност за брз почеток за граѓански организации

Оваа листа за проверка нуди едноставни, непосредни чекори за подобрување на дигиталната безбедност на вашата организација. Завршете ги овие активности во текот на следната недела за да ги намалите ранливостите и за да изградите основа за безбедна дигитална средина. Секој чекор е дизајниран да биде евтин, лесен за користење и ефикасен за граѓанските организации со ограничени ресурси.

1. Заштитете ги вашите сметки

- Овозможете двофакторска автентикација (2FA): Вклучете 2FA за сите критични сметки (на пр., е-пошта, социјални медиуми, складирање во облак) денес. Користете апликација за автентикација (како Google Authenticator или Authy) или SMS кодови за да додадете дополнителен слој на заштита..
    - ⇒ Проверете ги поставките на сметката (на пр. Gmail: Поставки > Безбедност > Верификација во 2 чекори).
- Креирајте силни, уникатни лозинки: Ажурирајте ги лозинките за клучните сметки да бидат долги најмалку 14 знаци, мешајќи букви, броеви и симболи (на пр. „sunbird&glass7rain“). Користете различна лозинка за секоја сметка.
    - ⇒ Размислете за бесплатен менаџер за лозинки како Bitwarden за безбедно генерирање и складирање на лозинки.
- Проверете за пробиени сметки: Посетете ја страницата „Have I Been Pwned“ (haveibeenpwned.com) за да видите дали вашата е-пошта или сметки биле изложени на пробивање на податоци. Веднаш променете ги засегнатите лозинки.

⇒ Протечените акредитиви може да се користат за напад на вашите сметки.

2. Заштитете ги вашите уреди

- Ажурирајте го софтверот денес: Осигурете се дека сите уреди (компјутери, телефони, таблети) и софтвер (на пр. оперативни системи, прелистувачи, апликации) се ажурирани со најновите безбедносни закрпи.
  ⇒ Проверете ги поставките за Windows Update, macOS Software Update или App Store за ажурирања што чекаат.
- Инсталирајте антивирусен софтвер: Инсталирајте бесплатна антивирусна програма (на пр., Windows Defender, Avast Free Antivirus) на сите уреди и осигурете се дека е активна и ажурирана.
  ⇒ Преземајте од доверливи извори и закажете неделно скенирање.
- Овозможете заклучување на уредот: Поставете ги уредите автоматски да се заклучуваат по пет минути неактивност со силна лозинка или ПИН. Осигурете се дека шифрирањето е овозможено (повеќето модерни уреди го имаат ова по дифолт).
  ⇒ Бравите и енкрипцијата спречуваат кражба на податоци ако уредите се изгубени или украдени.

3. Безбедни комуникации

- Користете апликации за безбедни пораки: Префрлете се на апликации за енкриптирање од крај до крај како Signal или WhatsApp за чувствителни комуникации. Проверете ги контактите пред да споделите чувствителни информации.
  ⇒ Преземете и овозможете исчезнување на пораките за чувствителни разговори.
- Е-пораки за откривање на фишинг: Обучете го персоналот да избегнува кликнување на линкови или споделување информации во е-пораки со итен јазик, правописни грешки или непознати испраќачи. Внимателно проверувајте ги е-адресите.
  ⇒ Задржете го курсорот над линковите за да ги потврдите URL-адресите пред да кликнете и пријавете сомнителни е-пораки на ИТ-страницата.

4. Заштита на податоци

- Направете резервна копија на критични податоци: Направете резервна копија на важните датотеки (на пр., листи на донатори, документи за проекти) на безбеден надворешен диск или услуга во облак (на пр. Google Drive со 2FA) оваа недела.
  ⇒ Закажете автоматски резервни копии или рачно копирајте датотеки на безбедна локација.
- Ограничување на пристапот до податоци: Прегледајте кој има пристап до чувствителни податоци (на пр. споделени дискови, бази на податоци). Отстранете го пристапот за поранешни вработени или волонтери.
  ⇒ Ограничувањето на пристапот го намалува ризикот од внатрешни закани или протекување на информации.

5. Обезбедете го вашето онлајн присуство

- Проверете ја безбедноста на веб-страницата: Потврдете дека вашата веб-страница користи HTTPS (побарајте го катанецот во прелистувачот). Контактирајте го вашиот

веб-домаќин за да обезбедите редовни резервни копии и ажуриран софтвер (на пр. CMS, додатоци).

⇒ Проверете кај вашиот давател на услуги за хостирање или користете бесплатни алатки како Let's Encrypt for HTTPS.

- Безбедни сметки на социјалните медиуми: Овозможете 2FA и силни лозинки на сите сметки на социјалните медиуми на CSO. Отстранете го пристапот за неактивни администратори.

⇒ Заштитете сеод киднапирање на сметка и дезинформации.

2.2 ПОГЛАВЈЕ 2: ПРВИ ЧЕКОРИ ВО ДИГИТАЛНАТА БЕЗБЕДНОСТ

Први чекори во дигиталната безбедност

Ова поглавје ги опфаќа основните практики што секој поединец во организацијата треба да ги следи за основна дигитална безбедност. Овие „први чекори“ често се едноставни навики и мерки што обезбедуваат значајни безбедносни придобивки. Како што вели поговорката, сајбер безбедноста започнува со сајбер хигиена – секојдневните рутини и мерки на претпазливост што ве одржуваат безбедни онлајн. Ќе истражиме како да креирате силни лозинки, внимателно да го користите интернетот, да ги обезбедите вашите комуникации и да ги заштитите вашите компјутери и паметни телефони. Дури и ако првично ги имплементирате само овие основи, веќе ќе ублажите голем дел од вообичаените закани.

Креирање и заштита на силни лозинки

Еден од најнепосредните начини да ја зголемите вашата дигитална безбедност е да ги зајакнете вашите лозинки. Лозинките се клучеви за вашите сметки и уреди – ако се слаби или компромитирани, напаѓачите можат да отклучат сè, од вашата е-пошта до вашите банкарски информации. За жал, луѓето често ги користат повторно лесните за паметење лозинки или избираат такви што напаѓачите лесно ги погодуваат (како „123456“ или „password“). Всушност, слабите или украдените лозинки остануваат водечка причина за нарушувања на безбедноста.

Што е силна лозинка?

Според упатствата за сајбер безбедност, силната лозинка е долга, единствена и сложена. Безбедносните упатства на Microsoft сугерираат најмалку 14 знаци, вклучувајќи мешавина од големи и мали букви, броеви и симболи. Не треба да содржи лесни лични информации (како вашето име или датум на раѓање) или вообичаени зборови. Добра практика е да користите лозинка – низа од случајни зборови или реченица што е лесна за паметење за вас, но тешка за другите да ја погодат. На пример, „sunbird&glass7rain“ е многу посилна од кратка лозинка како „blue123“, но можеби е полесна за паметење бидејќи е фраза.

Уникатноста е клучна: секоја сметка или услуга треба да има своја лозинка. Ако повторно користите лозинки и една сметка е пробиена, напаѓачите ќе ја пробаат истата лозинка на вашите други сметки (тактика наречена полнење на акредитиви). Користењето уникатни лозинки ја содржи штетата од едно пробивање. Како што советува ENISA

(агенцијата за сајбер безбедност на ЕУ), избегнувајте да ја користите истата лозинка на повеќе сметки. Исто така, размислете за проверка дали вашите сметки се појавиле во познати пробиви на податоци (веб-страници како „Дали сум бил Pwned“ ви овозможуваат да ја пребарувате вашата е-пошта во бази на податоци за пробиви). Ако е така, веднаш променете ги тие лозинки.

Менаџери за лозинки: Нереално е да се запомнат десетици долги, сложени лозинки. Тука влегуваат во игра алатките за управување со лозинки. Менаџерот за лозинки е апликација (или безбедна услуга во облак) што може да генерира силни случајни лозинки за вас и да ги чува во шифриран трезор, така што треба да запомните само една главна лозинка. Многу експерти за безбедност и агенции препорачуваат користење менаџери за лозинки за подобра безбедност. На пример, Bitwarden (компанија за управување со лозинки) го пофали советот на ENISA, кој експлицитно вклучува користење менаџер за лозинки за да се одржат лозинките уникатни и безбедни. Популарните менаџери за лозинки вклучуваат Bitwarden, LastPass, 1Password и KeePass (меѓу другите). Пронајдете еден што ѝ одговара на вашата организација (некои имаат бесплатни верзии) и почнете да го користите за да ги надградите сите тие слаби или повторувачки лозинки.

Заштита на вашите лозинки: Дури и силната лозинка мора да биде заштитена. Никогаш не ги споделувајте вашите лозинки преку е-пошта или пораки и бидете претпазливи кон секој што непосакувано ќе ве праша за вашата лозинка – легитимниот персонал за поддршка (дури и во ИТ компаниите) нема да има потреба од вашата вистинска лозинка. Исто така, овозможете двофакторска автентикација (2FA) на вашите сметки секогаш кога е можно. 2FA (исто така, наречена повеќефакторска автентикација, MFA) значи дека обезбедувате втор доказ за идентитет при најавување – на пример, еднократен код испратен на вашиот телефон или генериран од апликација за автентикација или скенирање на отпечаток од прст. На овој начин, дури и ако некој ја дознае вашата лозинка, веројатно нема да може да пристапи до сметката без тој втор фактор. Главниот совет на ENISA вклучува користење на „дополнителен чекор“ како телефонски код или биометриски податоци за најавување. Многу услуги (Google, Facebook, Microsoft, итн.) дозволуваат 2FA преку апликација или СМС. Препорачливо е да го вклучите ова за сметки за е-пошта, социјални медиуми, банкарство, складирање во облак – во суштина секоја сметка што би била чувствителна ако биде хакирана.

Друга важна навика е да се менуваат стандардните лозинки на уредите или апликациите. Многу хардверски уреди (како Wi-Fi рутери) или софтверски алатки доаѓаат со претходно поставени администраторски лозинки (честопати нешто генеричко како „admin/admin“). Овие стандардни поставки им се широко познати на напаѓачите, затоа секогаш поставувајте нова, силна лозинка за време на поставувањето. На пример, ако вашиот CSO постави нов канцелариски рутер или онлајн база на податоци, една од првите задачи треба да биде прилагодување на акредитивите за пристап.

Конечно, размислете за распоред за периодично ажурирање на лозинките. Мислењата се разликуваат за тоа колку често да се менуваат лозинките – некои експерти велат дека честите присилни промени можат да имаат спротивен ефект (корисниците може да изберат поедноставни лозинки или само да го зголемат бројот). Современите упатства

сугерираат дека ако лозинките се силни и уникатни, треба да ги менувате само кога има индикации за компромитирање или периодично (да речеме, еднаш годишно) како освежување. Старото правило за менување на секои три месеци повеќе не е строг услов ако се воспоставени други контроли (како 2FA). Меѓутоа, ако се сомневате дека некоја сметка може да биде компромитирана, веднаш променете ја таа лозинка и на кое било друго место каде што сте користеле слична.

Накратко, силни лозинки + 2FA = моќна одбрана. Со користење робусни, различни лозинки и додавање на втор чекор за најавување, ја затворате вратата на многу обиди за упад. Замислете го тоа како заклучување на вашата куќа со висококвалитетна брава (лозинка) и отварач (2FA) – натрапникот би морал да ги победи обете за да влезе. Како тим, охрабрете ги сите во вашата организација да ги усвојат овие практики. Поглавје 3 ќе се осврне на тоа како да се спроведат добри политики за лозинки низ целата организација, но промената може да започне со тоа што вие ќе водите со пример во користењето на менаџер за лозинки и 2FA за вашите сметки.

Безбедно користење интернет: На што треба да внимавате

Интернетот е главна артерија на информации и комуникација за повеќето организации, но може да биде и извор на закани доколку се користи невнимателно. „Безбедното користење интернет“ се однесува на практикувањето претпазливост и паметно однесување при прелистување веб-страници, користење онлајн услуги и преземање содржина. Еве ги клучните принципи и совети што треба да ги следат вработените во граѓанските организации:

***Потврдете ја легитимноста на веб-страницата*:** Пред да внесете какви било чувствителни информации на веб-страница (како што се акредитиви за најавување или лични податоци), проверете дали страницата е автентична и безбедна. Проверете дали URL-то е точно (внимавајте на печатни грешки или чудни домени што имитираат вистински) и дали врската е шифрирана – означено со https:// и икона на катанец во лентата за адреси на прелистувачот. На пример, https://secure.CSOportal.org е поверодостојно од http://CSO-лажни веб-страници што изгледаат легитимно (на пример, страница што се претставува како страница за најавување на е-пошта) за да ги пронајдат лозинките. Секогаш проверувајте ја лентата за адреси кога се најавувате. Современите прелистувачи, исто така, често го истакнуваат името на компанијата во деталите за сертификатот за главните страници – користете ги тие знаци. Кога се сомневате во врска со примена врска (да речеме, преку е-пошта или социјални медиуми), не кликнувајте директно на неа. Наместо тоа, одете до официјалната веб-страница преку Google или обележувачи или задржете го курсорот над врската за да ја прегледате URL-то (без да кликнете). Ако врската изгледа сомнително или не се совпаѓа со наводниот испраќач (на пр. е-пошта тврди дека е од вашата банка, но URL-то е некој неповрзан домен), веројатно е злонамерна.

Размислете пред да кликнете или преземете: Злонамерните линкови и преземања се примарен начин за ширење на малициозен софтвер. Бидете внимателни кога пребарувате непознати страници или кога ќе бидете замолени да преземате датотеки. Скокачките прозорци што ве поттикнуваат да преземете „кодек“ или „ажурирање“ за да ја видите содржината често се стапици. Ако ви е потребен одреден софтвер или документ,

преземете го од реномиран извор (на пример, софтвер од официјалната страница на продавачот или добро позната продавница за апликации). Избегнувајте преземање пиратски софтвер или медиуми – покрај правните проблеми, ваквите датотеки често кријат малициозен софтвер. Исто така, оневозможете ги автоматските преземања во поставките на вашиот прелистувач; контролата значи дека можете да откажете сè ненамерно. Ако вашиот прелистувач или безбедносна алатка ве предупреди дека некоја страница може да биде небезбедна, послушајте го предупредувањето и напуштете ја страницата. Слично на тоа, бидете скептични кон екстензиите или приклучоците на прелистувачот од непознати издавачи. Инсталирајте само додатоци што навистина ви се потребни и од официјални веб-продавници, бидејќи малициозната екстензија може да ја следи вашата активност или да инјектира реклами/вируси.

Користете безбедни врски (Wi-Fi и VPN): Кога се поврзувате на интернет, особено надвор од канцеларијата, бидете свесни за безбедноста на мрежата. Јавните Wi-Fi мрежи (како оние во кафулиња, аеродроми итн.) можат да бидат ризични бидејќи напаѓачите на истата мрежа може да го пресретнат вашиот сообраќај. Ако мора да користите јавен Wi-Fi, избегнувајте пристап до чувствителни сметки освен ако врската не е шифрирана (побарајте HTTPS). Дури и тогаш, искусен напаѓач би можел да постави нечесна Wi-Fi жешка точка со привлечно име („Бесплатен WiFi на аеродромот“) за да ги привлече корисниците. Добра практика е да користите VPN (Виртуелна приватна мрежа) кога сте на недоверливи мрежи. VPN создава шифриран тунел за целиот ваш интернет сообраќај, што значително ги намалува шансите за прислушкување. Многу организации обезбедуваат VPN пристап за далечинска работа; ако вашата нуди, осигурете се дека знаете како да ја користите. Ако не, размислете за користење реномирана комерцијална VPN услуга кога патувате или кога работите од јавни места. Дополнително, осигурете се дека вашиот домашен или канцелариски Wi-Fi е заштитен со силна лозинка и користи WPA2 или WPA3 шифрирање. Променете ја стандардната администраторска лозинка на вашиот рутер како што е споменато и оневозможете го далечинското управување освен ако не е апсолутно потребно.

Бидете внимателни со прилозите и линковите во е-пошта: Иако е-поштата ќе биде подетално разгледана во следниот дел, вреди да се напомене дека како дел од безбедните интернет навики, кликнувањето на линкови во е-пошта или на веб-страници бара претпазливост. Честа онлајн измама се лажните известувања како „Вашиот компјутер е заразен! Кликнете тука за скенирање“ – овие често водат до малициозен софтвер. Слично на тоа, избегнувајте кликнување на банер реклами или скокачки прозорци кои тврдат дека сте добиле нешто или дека ви треба итно ажурирање. Ова се обиди за социјален инженеринг за да се искористи љубопитноста или стравот. Имајте ја предвид поговорката: ако нешто онлајн звучи премногу добро (или премногу страшно) за да биде вистина, веројатно е измама. На пример, онлајн реклама што вели: „Добијте грант од 5.000 долари сега – ограничено време!“ треба да предизвика сомнежи. Обучете се да ги препознавате овие тактики и да не реагирате импулсивно.

Заштитете ги личните и организациските информации: Бидете внимателни со информациите што ги споделувате јавно на веб-страниците и социјалните медиуми, бидејќи тие можат да се користат против вас во сајбер напади. Напаѓачите често собираат детали од профилите на социјалните медиуми или веб-страниците за да создадат

поубедливи фишинг е-пораки (пракса наречена spear phishing кога е високо насочена). На пример, ако страницата на вашата организација за граѓански организации ги наведува е-поштите и интересите на персоналот, некој може да ви испрати е-пошта со наведување на тие информации за да ја придобие вашата доверба. Затоа, ограничете го она што го откривате за внатрешни прашања на јавните форуми. Кога пополнувате веб-формулари, размислете дали сите барани податоци се неопходни. Ако некоја страница бара моминско презиме на вашата мајка или други лични податоци без јасна потреба, размислете двапати. Од перспектива на приватноста, користете ги поставките за приватност на социјалните медиуми за да ограничите кој може да ги види вашите објави. А за организацијата, осигурете се дека директориумите или чувствителните документи не се ненамерно изложени на вашата веб-страница. Периодично пребарувајте го името на вашата организација за граѓански организации на интернет за да видите какви информации има таму – на овој начин може да откриете изложен документ или лажна страница.

Користете ажурирани прелистувачи и безбедносни алатки: Безбедното користење интернет не е само прашање на однесување; туку е и користење ажурирана технологија. Секогаш користете ја најновата верзија на вашиот веб-прелистувач (Chrome, Firefox, Edge, итн.), бидејќи ажурирањата често ги поправаат безбедносните ранливости. Овозможете ги вградените безбедносни функции на прелистувачот: повеќето прелистувачи имаат заштита од фишинг и малициозен софтвер што може да блокира познати лоши веб-страници. Исто така, треба да имате активна реномирана антивирусна/програма против малициозен софтвер на вашиот уред, која понекогаш може да открие дали преземањето или страницата е злонамерна. Современите антивирусни решенија често вклучуваат веб-заштита што предупредува или блокира ако се обидете да посетите страница позната по фишинг или хостирање малициозен софтвер. На пример, Microsoft Defender или Avast може да прикажат страница за предупредување ако се обидете да пристапите до опасна страница. Обрнете внимание на овие предупредувања; тие се тука за да ве заштитат.

Накратко, безбедното користење интернет во голема мера се однесува на тоа да се биде буден и скептичен кога сте онлајн. Слично како уличните шеги во голем град – останувате свесни за вашата околина и размислувате двапати пред да влезете во сомнителна улица – онлајн, треба да внимавате каде „патувате“ и со кого комуницирате. Охрабрете ги сите во вашиот тим да усвојат претпазлив начин на размислување: задржете го курсорот над линковите пред да кликнете, преземајте само од доверливи извори и третирајте ги несаканите скокачки прозорци или пораки со сомнеж. Во следниот дел, ќе навлеземе подлабоко во еден од најчестите начини на напад, е-поштата и пораките, и како да ги обезбедиме тие комуникации.

Безбедност на е-пошта и пораки

Е-поштата е неопходна алатка за граѓанските организации, а апликациите за пораки (како WhatsApp, Signal или Telegram) се користат широко за брза комуникација. Сепак, овие канали се чести цели на сајбер напади како што се фишинг, прислушување и киднапирање на сметки. Овој дел дава упатства за тоа како да комуницирате побезбедно и да избегнете вообичаени стапици.

Свесност за фишинг: Фишингот преку е-пошта беше спомнат претходно бидејќи е толку распространет. Да повториме и да проширими: Секогаш внимателно проверувајте ги

неочекуваните е-пораки, особено оние што бараат итна акција или бараат чувствителни информации. Типична фишинг е-пошта може да изгледа како да доаѓа од колега, банка или онлајн услуга и да содржи линк за „најавување“ или прилог за отворање. Пред да кликнете на кој било линк во е-пошта, проверете го испраќачот и целта на линкот. Внимателно проверете ја адресата на испраќачот – напаѓачите често користат адреса што е погрешна за буква (на пр. john.doe@micros0ft.com наместо легитимна е-пошта на Microsoft) или јавна е-пошта што не се совпаѓа со наведената организација. Ако е-поштата тврди дека треба да ја ресетирате лозинката или да дадете информации, побезбедно е да не кликнете на линкот од е-поштата. Наместо тоа, одете сами на официјалната веб-страница. За прилози, не отворајте датотеки од непознати или недоверливи е-пораки. Дури и ако е од познат контакт, ако е неочекувано и чудно (на пр. случаен документ со наслов „Фактура“ што не сте го очекувале), потврдете со испраќачот преку друг канал. Како по правило, избегнувајте овозможување макроа или овозможување содржина во Office документи, освен ако не сте апсолутно сигурни за нивниот извор – многу инфекции со малициозен софтвер доаѓаат преку макроа во Word/Excel во фишинг прилози.
Граѓанските организации треба да ги едуцираат своите вработени дека е во ред (дури и охрабрено) да бидат малку параноични со е-поштата – кога се сомневате, проверете. Брз телефонски повик или порака до наводниот испраќач би можеле да потврдат дали навистина го испратиле тоа барање. Подобро е да проверите двапати отколку да кликнете и да се покаете. Запомнете, фишингот не е ограничен само на е-пошта; може да се случи и преку СМС (текстуални пораки со лоши врски) или апликации за пораки. На пример, член на персоналот може да добие WhatsApp порака што изгледа како известување од онлајн услуга за плаќање со линк – третирајте ги на ист начин, со претпазливост.

Безбедност на е-пошта сметка: Бидејќи сметките за е-пошта можат да бидат портал за ресетирање на други лозинки и да содржат чувствителна кореспонденција, обезбедувањето на вашето најавување преку е-пошта е клучно. Користете силна лозинка и 2FA за вашата сметка за е-пошта (како што е дискутирано во 2.1) – многу даватели на е-пошта како Gmail, Outlook или ProtonMail поддржуваат двофакторска автентикација преку апликација или SMS. Ова драстично го намалува ризикот некој да ја хакира вашата е-пошта. Исто така, бидете внимателни кога пристапувате до е-пошта на споделени или јавни компјутери; секогаш одјавете се потоа и осигурете се дека прелистувачот не ги зачувува вашите акредитиви. Доколку е можно, користете безбедни протоколи за е-пошта (повеќето модерни услуги се стандардни со ова): осигурете се дека веб-поштата користи HTTPS, а ако користите апликација за е-пошта (како Outlook, Thunderbird или на вашиот телефон), осигурете се дека е поставена да користи шифрирани врски (SSL/TLS) и за примање (IMAP/POP) и за испраќање (SMTP). Документацијата на вашата ИТ поддршка или давателот на услуги можат да ги потврдат овие поставки.

Размислете за енкрипција на е-пошта за високо чувствителни комуникации. Стандардните е-пораки не се енкриптирани од крај до крај, што значи дека во теорија, содржината на е-поштата може да биде прочитана од ненамерни страни (како што се даватели на е-пошта или секој што ќе добие пристап до сметката). За чувствителни податоци, можете да користите алатки како што е енкрипција на е-пошта PGP/GPG или да преминете на безбедни платформи за пораки за тој разговор. Сепак, PGP може да биде

комплексен за секојдневна употреба, па затоа друга стратегија е да се користи безбедно споделување датотеки за чувствителни прилози, наместо да се става доверлив текст во телото на е-поштата. Некои услуги за е-пошта фокусирани на граѓански организации или пакети за претпријатија нудат вградена енкрипција или барем можност за заштита на е-пораките или прилозите со лозинка. Ако вашата организација се занимава со исклучително чувствителни информации (на пример, случаи на човекови права), треба да се консултирате со експерт за дигитална безбедност за поставување работен тек на енкрипција.

Апликации за безбедни пораки: Многу граѓански организации користат инстант пораки за брзи разговори и координација. Важно е да се изберат апликации за пораки кои нудат енкрипција од крај до крај (E2EE), што гарантира дека само корисниците што комуницираат (и никој помеѓу нив, дури ни давателот на услуги) не може да ги чита пораките. WhatsApp, на пример, има E2EE по дифолт за разговори, како и „тајните разговори“ на Signal и Telegram (забелешка: Разговорите во облак на Telegram не се E2EE по дифолт). Signal е широко препорачан во заедницата на граѓанското општество за чувствителни комуникации бидејќи е со отворен код, E2EE, и има силни практики за приватност. Друг е Wire, кој е, исто така, безбеден и е во согласност со европскиот GDPR. Threema и Element (Matrix) се други опции за безбедни пораки што ги користат некои групи за човекови права. Специфичниот избор на апликација може да зависи од вашиот контекст и она што вашите колеги го користат, но општо правило е: избегнувајте канали со обичен текст (SMS текстови или неенкриптирани е-пораки) за чувствителни прашања и мигрирајте на енкриптирана апликација каде што е можно.

Дури и со шифрирани апликации, бидете внимателни на метаподатоците (кој со кого разговара, кога). Повеќето E2EE апликации сè уште откриваат некои метаподатоци за услугата (иако Signal се обидува да го минимизира ова). За исклучително чувствителни операции, може да се користат алатки фокусирани на анонимност како Session или да се користи размена на пораки преку Tor, но тоа се напредни сценарија. За општа употреба од страна на CSO, мејнстрим E2EE апликацијата значително ќе ја подобри безбедноста во споредба со нешифрираните канали.

Исто така, заклучете ги вашите апликации за пораки: Користете функции за заклучување апликации или PIN-ови на уредот, така што ако вашиот телефон е изгубен или украден, некој не може едноставно да ги отвори вашите разговори. Овозможете исчезнување на пораките за многу чувствителни разговори – многу апликации ви дозволуваат да поставите пораките автоматски да се бришат по одредено време (Signal, WhatsApp, итн.). На тој начин, ако некој подоцна ја компромитира вашата сметка, минатите пораки можеби веќе ги нема.

Внимавајте на измамите со пораки: Фишинг измамите не ја злоупотребуваат само е-поштата. Може да добиете лажни пораки преку СМС-порака или апликации во кои ќе ве замолат да кликнете на линк (честопати скратени URL-адреси) или да пренасочите нешто. Пример е измамата со „WhatsApp код“: добивате СМС-порака со код за најавување што не сте го побарале, а потоа веднаш добивате WhatsApp порака од пријател во која се вели: „Имам проблем, ве молам испратете ми го кодот што штотуку го добивте“. Сметката на тој пријател веројатно е хакирана, а напаѓачот се обидува да го искористи вашиот код за да го преземе вашиот WhatsApp. Лекцијата: никогаш не давајте кодови за верификација на други и бидете сомничави кон итни, чудни барања во разговор, дури и ако се од пријатели.

Прилози и врски во облак: Наместо да прикачуваат документи во е-пошта, многумина се префрлија на линкови во облак (на пр. линкови од Google Drive, Dropbox, OneDrive). Овие се практични, но имаат свои безбедносни причини. Ако испратите линк за споделување во облак, осигурајте се дека е достапен само за наменетите лица (користете приватни линкови или додајте ги нивните е-пошти експлицитно) и размислете за поставување датуми на истекување за линкот. Ако добиете линк во облак, бидете внимателни како и со секоја врска – осигурете се дека е од легитимен домен на услуга во облак и дека сте го очекувале. Тактиката за фишинг може да испрати линк што изгледа како датотека од Google Drive, но води до лажна страница за најавување. Секогаш потврдувајте доколку е потребно и, идеално, пристапувајте до споделените дискови преку познатиот интерфејс (на пр. најавете се директно на вашиот Google Drive за да видите дали датотеката е споделена со вас).

Хигиена на е-пошта и најдобри практики: Уште неколку брзи совети: Користете филтри за спам – модерните услуги за е-пошта добро го фаќаат поголемиот дел од несаканите пораки/фишинг. Сепак, повремено проверувајте ја вашата папка со спам за лажни позитиви, но не комуницирајте со е-пораки во спам освен ако не сте сигурни дека се безбедни. Не се отпишувајте од спам е-пораки освен ако не се од реномирани извори; кликнувањето на „отпишување“ на навистина спам е-пораки може да им потврди на спамерите дека вашата адреса е активна. Подобро е само да ги избришете. Кога испраќате е-пораки до големи групи, користете BCC за да ги заштитите адресите на примателите од тоа да бидат видени од сите (спречување на случајни протекувања на листи со контакти). И размислете да овозможите известувања за пренасочување на е-пошта или известувања за најавување ако вашиот провајдер ги нуди, за да знаете дали ќе се случи некоја необична активност (на пример, Gmail може да ве извести ако се случи ново најавување од нов уред). Со следење на овие практики, вашата организација може значително да го намали ризикот од станување жртва на напади базирани на е-пошта или пораки. Бидејќи е-поштата е често првата точка на контакт за напаѓачите, совладувањето на безбедноста на е-поштата носи голема безбедносна корист. Замислете го тоа како безбедно возење: поголемиот дел од времето, „патиштата“ (интернетот) се во ред, но мора да го носите безбедносниот појас (2FA), да ги почитувате сигналите (предупредувања за сомнителни врски) и да бидете внимателни за да избегнете несреќи.

Основни совети за безбедност на компјутери и телефони

Лаптопите, десктоп компјутерите и паметните телефони се работните коњи на секоја модерна организација. Тие, исто така, складираат многу чувствителни податоци и можат да бидат влезни точки за напаѓачите доколку не се заштитени. Овој дел дава основни совети за да ги заштитите овие уреди од вообичаени закани. Многу од овие совети спаѓаат во рутинско одржување и разумно користење – дигиталниот еквивалент на заклучување на вратите и редовна промена на маслото.

Одржувајте го софтверот ажуриран: Осигурете се дека сите оперативни системи и апликации на вашите уреди се ажурирани со најновите безбедносни закрпи. Ажурирањата на софтверот често ги поправаат ранливостите што напаѓачите би можеле да ги искористат. Вклучете ги автоматските ажурирања секогаш кога е можно – на пример,

овозможете ги автоматските ажурирања на Windows Update или macOS и направете го истото на вашиот iPhone/Android телефон за системот и апликациите. Исто така, редовно ажурирајте ги вашите апликации (прелистувачи, канцелариски програми, итн.); многу од нив ќе ве прашаат кога е достапно ажурирањето – не ги игнорирајте тие инструкции. За секој софтвер што не се ажурира автоматски, поставете периодичен потсетник за проверка за ажурирања или користете централизирана алатка за управување доколку е достапна. Запомнете дека ова ги вклучува додатоците и рамките на прелистувачите како Java или Adobe Reader, кои историски гледано биле патишта за малициозен софтвер ако се застарени. Ажурираниот уред е зајакнат уред.

Инсталирајте антивирусна/заштита од малициозен софтвер: Користете реномирано антивирусно решение на вашите компјутери (и разгледајте една од реномираните апликации за мобилна безбедност за Android уреди). Современиот антивирусен софтвер обезбедува заштита во реално време, што значи дека активно ќе скенира датотеки и ќе го следи однесувањето на системот за да блокира малициозен софтвер. Windows 10/11 доаѓа со вграден Microsoft Defender, што е доста добро за основна употреба ако се ажурира. Може да се земат предвид и опции од трети страни (платени или бесплатни) како Avast, Bitdefender и ESET, итн. Клучот е да имате нешто и да ги ажурирате неговите дефиниции за вируси дневно. Избегнувајте користење на повеќе антивирусни програми одеднаш (тие можат да се судрат). На телефоните, iPhone-ите генерално не бараат посебни AV апликации поради тоа како е дизајниран iOS, но Android телефоните може да имаат корист од апликација против малициозен софтвер, особено ако понекогаш инсталирате апликации надвор од официјалната Play Store. Сепак, најдобрата одбрана за телефоните е да инсталирате апликации само од доверливи продавници за апликации и да ги проверувате дозволите за апликациите – на пример, апликацијата со фенерче не треба да ги гледа вашите контакти или пораки.

Уште една работа: никогаш не го оневозможувајте вашиот безбедносен софтвер од ваша погодност. Ако блокира некоја акција, истражете зошто, наместо едноставно да го исклучите. Исто така, не инсталирајте пиратски софтвер, како што споменавме – покрај легалноста, хакираниот софтвер често доаѓа во комплет со тројанци што антивирусниот софтвер може, а може и не мора да ги фати.

Користете заклучувања на уредот и шифрирање: Секогаш заклучувајте ги вашите уреди со ПИН, лозинка или биометриско заклучување (отпечаток од прст, препознавање лице) кога не се во употреба. Поставете краток временски период за автоматско заклучување (на пр. екранот се заклучува по пет минути неактивност или помалку). Ова спречува неовластен пристап ако некој физички го фати вашиот уред. Ако лаптоп од CSO е украден од автомобил или телефонот е изгубен на конференција, силното заклучување на екранот може да ги заштити податоците од љубопитните очи – но само ако е поставено. За лаптопите, размислете за енкрипција на целиот диск. Современите оперативни системи често го имаат ова по дифолт: Windows има BitLocker (Pro изданија) или Device Encryption, а macOS има FileVault. Кога е овозможено, дури и ако хард дискот е отстранет, податоците остануваат измешани без клучот за дешифрирање (обично поврзан со вашата лозинка за најавување). На паметните телефони, и iOS и Android поддржуваат енкрипција на уредот (поновите верзии енкриптираат по дифолт кога користите ПИН/лозинка). Проверете дали енкрипцијата е овозможена, особено на постарите верзии на Android каде што можеби

била опционална. Енкрипцијата е клучна за чувствителни податоци; На пример, ако е изгубен лаптоп што содржи податоци за учесниците за студијата, но е криптиран, податоците остануваат безбедни, а инцидентот е проблем со изгубен уред, а не повреда на податоци.

Редовни резервни копии: Иако резервните копии се првенствено мерка за обновување на податоци, тие се, исто така, и безбедносна мерка – тие ви овозможуваат да закрепнете од ransomware или од губење уред без да подлегнете на изнудување или да претрпите целосна загуба. Поглавје 3 ќе ги детализира стратегиите за резервна копија, но како основен совет: редовно правете резервни копии на важни датотеки и чувајте ги резервните копии на безбедна локација одвоена од вашиот компјутер (надворешен диск безбедно складиран или услуга за резервна копија во облак). Повремено тестирајте ги тие резервни копии за да бидете сигурни дека можете да ги вратите податоците. За мобилни уреди, размислете за правење резервна копија на важни фотографии/документи (телефоните може да се постават да прават резервна копија во облак или компјутер). Во случај на кражба на телефон, барем вашите податоци не се изгубени засекогаш.

Безбедна инсталација на апликации/програми: Инсталирајте софтвер само од доверливи извори. На компјутерите, тоа обично значи официјалната веб-страница на софтверот или позната продавница за апликации (како Microsoft Store или Mac App Store). На телефоните, користете Google Play Store, Apple App Store или F-Droid (за апликации со отворен код за Android). Бидете претпазливи со бесплатните алатки од непознати веб-страници – ако ви треба PDF конвертор или видео плеер, на пример, истражете некој реномиран, наместо да го преземете првото нешто што ќе го најдете. Некои малициозни програми се маскираат како корисни алатки. Исто така, за време на инсталацијата, обрнете внимание на упатствата и одбијте ги сите понуди за инсталирање дополнителни ленти со алатки или промена на пребарувачот (често кај инсталатерите на бесплатни програми). Ова не се баш безбедносни закани, но тие го преоптоваруваат вашиот систем и можат да доведат до ранливости или проблеми со приватноста.

Безбедна конфигурација и поставки: Одвојте малку време за да ги конфигурирате основните безбедносни поставки на вашите уреди. На пример, на Windows, осигурете се дека заштитниот sид е вклучен (обично е по дифолт). Заштитниот sид помага да се блокираат несаканите влезни врски. Повеќето корисници нема да треба да го прилагодуваат надвор од стандардните вредности, но треба да остане овозможен. На вашиот рутер, осигурете се дека заштитниот sид/NAT е вклучен, а далечинското администрирање е исклучено (како што е споменато во Безбеден интернет). На паметни телефони, проверете ги поставките за приватност за секоја апликација – оневозможете ги непотребните дозволи (Дали играта има потреба од пристап до вашиот микрофон? Веројатно не). И Android и iOS ви дозволуваат да видите какви дозволи има секоја апликација и да ги поништите оние што изгледаат прекумерни.

Физичка безбедност на уредите: Дигиталната безбедност не е само дигитална – физичкото обезбедување на уредите е, исто така, важно. Не оставајте лаптопи или телефони без надзор на јавни места. Во канцеларијата, имајте политика за заклучување на екраните кога се оддалечувате од вашата работна маса (и Windows и Mac имаат кратенки за ова). Ако патувате, бидете внимателни со лаптопите на обезбедувањето на аеродромите или во такси – многу пробиви се едноставно изгубени уреди со чувствителни информации.

Исто така, размислете за екрани за приватност за лаптопите ако често работите јавно (за да спречите пребарување на екранот преку рамо). За десктоп компјутерите, особено ако вашиот орган за заштита на животната средина има канцеларија достапна за посетители или заеднички простори, заклучувањето на серверските соби или користењето на брави со кабел за опрема може да спречи кражба.

Употреба на управување со мобилни уреди (MDM) за организации: Доколку вашиот CSO има капацитет (или како што расте), можете да имплементирате MDM решение. MDM софтверот ѝ овозможува на организацијата централно да спроведува безбедносни политики на телефони и лаптопи – на пример, барање PIN, објавување автоматски ажурирања или далечинско бришење на уред ако е изгубен. Дури и без формален MDM, барем осигурете се дека можете далечински да ги избришете уредите: за телефони, услуги како Find My iPhone или Find My Device на Android можат далечински да лоцираат и да избришат изгубен телефон. За лаптопи, ако користите Windows поврзан со сметка на Microsoft или корпоративни алатки, понекогаш постојат слични опции. Како минимум, знајте како да менувате лозинки и да ги поништувате сесиите за сметки на изгубен уред (на пример, ако вашиот волонтер изгуби телефон што имал пристап до е-поштата на CSO, веднаш променете ја таа лозинка за е-пошта и одјавете се од сите сесии).

План за неуспеси: Понекогаш, хардверот откажува или се оштетува. Иако не се работи за „сајбер напад“, овие настани можат да предизвикаат губење на податоци или застој. Основен совет: користете сигурен антивирус, но, исто така, држете при рака некои алатки за обновување (како „бутабилен“ чист USB-стик со антивирус или алатки за поправка на системот). И осигурете се дека важните датотеки не се складираат само на еден лаптоп; ако хардверот откаже, имате резервни копии или синхронизација на место.

Со примена на овие основни совети, создавате основно ниво на заштита за вашите лични и работни уреди. Замислете го тоа како обезбедување на „крајните точки“ – секој телефон или компјутер е крајна точка што може да се искористи ако е слаб, но заедно тие ја формираат дигиталната средина на вашиот CSO. Напаѓачот честопати ќе се одлучи за најлесната цел. Овие мерки (ажурирања, антивирус, силни конфигурации) ги отстрануваат ниско висечките плодови, принудувајќи ги противниците да работат многу понапорно или идеално, целосно да ги одвратат. Тоа е аналогно на безбедноста на домот: заклучувате врати, инсталирате детектори за чад и можеби имате куче – ништо од ова не гарантира безбедност, но тие значително ги намалуваат ризиците и обезбедуваат предупредувања. Во сајбер безбедноста, вашиот ажуриран, добро конфигуриран уред со безбедносен софтвер е како дом со брави и аларми – многу помалку привлечен за натрапниците отколку незаштитен систем.

Со воспоставени навики за лична безбедност и безбедност на уредите, сега преминуваме на организациско ниво: развивање план и култура во вашата организација за заштита на лични податоци (OCSO) што ја поддржува дигиталната безбедност. Следното поглавје ќе се осврне на тоа како да се проценат ризиците и да се создаде едноставен, но ефикасен план за дигитална безбедност прилагоден на потребите на вашата организација за заштита на лични податоци.

Резиме на поглавјето

Глава 2 дава достапен вовед во фундаменталните концепти за сајбер безбедност прилагодени за граѓанските организации, фокусирајќи се на тријадата на ЦИА: доверливост, интегритет и достапност. Доверливоста гарантира дека податоците (на пр. евиденцијата на донаторите) остануваат приватни, интегритетот спречува неовластени промени, а достапноста ги одржува системите достапни. Главата користи едноставен јазик и примери релевантни за граѓанските организации, како што е обезбедувањето на контакт листи на активисти, за да ги објасни овие принципи. Воведува моделирање на закани, процес за идентификување на ризици и приоритетизација на заштитата, што го прави релевантен за организациите со ограничени ресурси. Практичните најдобри практики вклучуваат силни лозинки, двофакторска автентикација (2FA) и претпазлива употреба на интернет. Главата нагласува решенија со ниска цена, како што се бесплатни менаџери за лозинки (на пр., Bitwarden), за да се справат со буџетските ограничувања на граѓанските организации. Исто така, го истакнува човечкиот елемент, забележувајќи дека 74% од прекршувањата вклучуваат грешки, како што е паѓање на жртвите на фишинг измами. Со поттикнување на свеста, граѓанските организации можат да ги ублажат ризиците без техничка експертиза. Главата охрабрува да се започне со едноставни чекори (на пр. ажурирање на софтвер) за да се изгради безбедносна основа. Ја поврзува дигиталната безбедност со мисиите на граѓанските организации, објаснувајќи како заштитата на податоците ја одржува довербата и одговорноста. На пример, компромитирана база на податоци за донатори би можела да ја поткопа довербата на јавноста, како што беше видено во минатите инциденти. Поглавјето поставува практичен тон за е-книгата, опремувајќи ги читателите со основно знаење за ефикасно спроведување на безбедносните мерки.

Водич во чекори за спроведување на основна проценка на ризик

Ова упатство обезбедува структуриран процес за граѓанските организации да го пополнат образецот за проценка на ризик, со примери прилагодени на вообичаените средства на граѓанските организации, како што се базите на податоци на донаторите и евиденцијата на волонтерите. Чекорите се дизајнирани да бидат достапни за организации со ограничена техничка експертиза, усогласувајќи се со акцентот на наставната програма на практичните рамки (Модул 2) и упатството за проценка на ризик во е-книгата (Поглавје 5).

Чекор 1: Идентификувајте ги критичните дигитални средства

- Што да направите: Наведете ги дигиталните средства (податоци, системи, сметки) кои се неопходни за работењето на вашата граѓанска организација. Фокусирајте се на она што би ја нарушило вашата мисија или би им наштетило на засегнатите страни доколку биде компромитирано.
- Како да го направите тоа: Соберете мал тим (на пр. раководство, програмски персонал, контакт лице за ИТ) за размена на идеи. Разгледајте ги податоците (на пр. листи на донатори, информации за корисници), системите (на пр. е-пошта, веб-страница) и сметките (на пр. социјални медиуми, складирање во облак).
  Пример:
  - База на податоци за донатори: Табеларна пресметка или CRM систем што содржи имиња на донатори, контакт информации и износи на донации.
  - Записи за волонтери: Датотеки со имиња на волонтери, информации за контакт и распореди складирани на споделен диск или платформа во облак.
  - Е-пошта сметки: Gmail или Outlook сметки на персоналот што се користат за комуникација со засегнатите страни.

Чекор 2: Идентификувајте ги заканите за секој имот

- Што да се прави: За секој ресурс, наведете ги потенцијалните закани (на пр. хакирање, фишинг, малициозен софтвер, човечка грешка) што би можеле да го компромитираат.
- Како да го направите тоа: Дискутирајте како напаѓачите би можеле да го нападнат средството или што би можело да тргне наопаку (на пр. случајни протекувања, кражба на уред). Погледнете ги вообичаените закани од е-книгата (Поглавје 1.3), како што се фишинг, кршење на податоци или рансомвер.
  Пример:
  - База на податоци за донатори:
    - Закана: Напад на податоци преку фишинг (напаѓачот ги измамува вработените да ги откријат акредитивите за најавување).
    - Закана: Ransomware ја енкриптира базата на податоци.
  - Волонтерски записи:
    - Закана: Неовластен пристап поради слаби лозинки или споделени акредитиви.
    - Закана: Губење на податоци ако лаптопот е украден.

Чекор 3: Проценете ја веројатноста за секоја закана

- Што да направите: Оценете ја веројатноста за појава на секоја закана на скала од 1 (ретка) до 5 (речиси сигурна).
- Како да го направите тоа: Размислете за фактори како што се видливоста на вашата организација за граѓански организации, минатите инциденти или вообичаените трендови на напади (на пр. фишингот е широко распространет). Користете локален контекст доколку е достапен (на пр. чест фишинг во вашиот регион).

Пример:

- База на податоци за донатори:
  - Фишинг: Веројатност = 3 (Можно, бидејќи фишингот е чест, но вашиот персонал има одредена обука).
  - Ransomware: Веројатност = 2 (Малку веројатно, ако е инсталиран антивирус, но не и невозможно).
- Волонтерски записи:
  - Неовластен пристап: Веројатност = 4 (Веројатно, ако лозинките се слаби или пристапот не е ограничен).
  - Кражба на лаптоп: Веројатност = 2 (Малку веројатна, но можна при теренски операции).

Чекор 4: Проценка на влијанието на секоја закана

- Што да се прави: Оценете ја сериозноста на последиците од заканата на скала од 1 (Ниска) до 5 (Тешка), земајќи ги предвид нарушувањето на мисијата, губењето на податоци или нарушувањето на репутацијата.
- Како да го направите тоа: Размислете за најлошото сценарио (на пр. правни проблеми, губење на доверба, штета на корисниците). Повикајте ги примерите од е-книгата, како што е прекршувањето на правилата од страна на Австралискиот Црвен крст (Поглавје 1.1).

  Пример:
  - База на податоци за донатори:
    - Фишинг/Прекршување: Влијание = 5 (Сериозно, поради изложеност на податоци на донатори, казни според GDPR, губење на доверба).
    - Ransomware: Влијание = 4 (Високо, бидејќи операциите може да запрат без резервни копии).
  - Волонтерски записи:
    - Неовластен пристап: Влијание = 4 (Високо, бидејќи прекршувањата на приватноста од страна на волонтерите би можеле да му наштетат на угледот).
    - Кражба на лаптоп: Влијание = 3 (Умерено, ако податоците се шифрирани, но обновувањето е скапо).

Чекор 5: Пресметајте ги резултатите од ризикот и дајте приоритет

- Што да направите: Помножете ја веројатноста со влијанието за да добиете резултат за ризик (1-25). Повисоките резултати укажуваат на ризици на кои им е потребно итно внимание.
- Како да го направите тоа: Користете го шаблонот за да пресметате резултати и да ги сортирате ризиците од највисок до најнизок. Прво фокусирајте се на справување со ризиците со највисок резултат.

  Пример:
  - База на податоци за донатори:
    - Фишинг: 3 x 5 = 15 (Висок приоритет).
    - Ransomware: 2 x 4 = 8 (Среден приоритет).
  - Волонтерски записи:

- Неовластен пристап: 4 x 4 = 16 (Висок приоритет).
- Кражба на лаптоп: 2 x 3 = 6 (низок приоритет).

Чекор 6: Развијте чекори за ублажување

- Што да се прави: Наведете специфични, акциони чекори за спречување или намалување на секоја закана, фокусирајќи се на практични мерки со ниска цена.
- Како да го направите тоа: Црпете од наставната програма (Модул 1-5) и е-книгата (Поглавја 2-4) за решенија како што се 2FA, енкрипција или обука. Осигурете се дека чекорите се изводливи за ресурсите на вашата ГО.

  Пример:
  - База на податоци за донатори:
    - Фишинг: Овозможете 2FA при пристап до базата на податоци, шифрирајте датотеки и обучете го персоналот за откривање фишинг.
    - Ransomware: Закажете неделни резервни копии во безбеден облак, инсталирајте ажуриран антивирусен софтвер.
  - Волонтерски записи:
    - Неовластен пристап: Користете силни лозинки, ограничете го пристапот само за овластен персонал и проверувајте ги дозволите месечно.
    - Кражба на лаптоп: Овозможете енкрипција на уредот, користете алатки за далечинско бришење на изгубени уреди.

Чекор 7: Преглед и ажурирање

- Што да се прави: Назначете член на тимот да ја прегледува проценката на ризикот годишно или по поголеми промени (на пр. нов софтвер, промени во персоналот). Ажурирајте го шаблонот по потреба.
- Како да го направите тоа: Закажете состанок за преглед за да проверите дали средствата, заканите или чекорите за ублажување се променети. Документирајте ги ажурирањата за да се осигурите дека планот останува релевантен.

  Пример: По имплементацијата на 2FA, веројатноста за неовластен пристап до евиденцијата на волонтерите се намалува на 2, со што се намалува оценката за ризик на 8. Ажурирајте го шаблонот соодветно.

2.3 ПОГЛАВЈЕ – 3: ДИГИТАЛНИ ПЛАНОВИ ЗА БЕЗБЕДНОСТ ЗА ГО

План за дигитална безбедност за граѓанските организации

Откако ги опфативме поединечните практики, се свртуваме кон поширокиот организациски пристап. Планот за дигитална безбедност е стратешка и оперативна мапа на патот за тоа како вашата организација за дигитална безбедност ќе ги заштити своите дигитални средства и ќе одговори на заканите. Не мора да биде комплициран или долг документ. Всушност, концизен план што сите го разбираат е често подобар од гломазна политика што стои на полица. Ова поглавје ве води низ креирање основен план за безбедност, фокусирајќи се на **четири клучни елементи:**

– Препознавајќи ги вашите ризици,

– Формулирање на планот со соодветни мерки,

– Градење на свеста преку обука,
– Заштита на вашите податоци преку резервни копии и безбедно складирање.

Препознавање на ризиците: Со какви закани се соочува вашата организација?

Секоја организација има уникатен профил на ризици во зависност од нејзините активности, податоци и противници. Првиот чекор во развојот на безбедносен план е да се идентификуваат и проценат овие ризици – во суштина, да се изврши едноставна дигитална проценка на ризикот. Ова не бара напредна диплома; тоа значи систематско размислување за тоа што би можело да тргне наопаку и колку лошо би можело да им наштети на вашите операции ако се случи.

Идентификувајте ги вашите средства и податоци: Започнете со наведување на важните дигитални средства и информации што ги поседува вашата граѓанска организација. Тие вклучуваат: хардвер (компјутери, телефони, сервери), софтвер и услуги (е-пошта сметки, веб-страници, облак дискови, бази на податоци) и податоци (списоци на членови, финансиски записи, податоци за истражувања, комуникации итн.). Поставувајте прашања како: Кои податоци би предизвикале најголема штета доколку бидат јавно објавени? Кои системи се критични за нашата секојдневна работа? На пример, граѓанска организација што обезбедува правна помош може да им даде приоритет на досиејата на клиентите и на комуникациите со адвокатите како критични средства што треба да се заштитат (поради доверливоста). Развојната граѓанска организација може да ја идентификува својата база на податоци за донатори и податоците од теренските истражувања како витални. Познавањето на вашите „крунски скапоцености“ ќе ви помогне да ги фокусирате вашите безбедносни напори.

Идентификувајте ги потенцијалните закани и актерите на закани: Потоа, размислете кој или што би можело да сака да ја оштети дигиталната инфраструктура на вашата организација. Некои вообичаени закани се неселективни – на пр. случајни сајбер криминалци кои шират рансомвер за профит, што би можело да го погоди секого. Други може да бидат поцелни: можеби компании или поединци кои се спротивставуваат на вашето застапување, па дури и на владиниот надзор ако работите на чувствителни прашања. Наведете ги категориите на закани: хакери кои бараат финансиска добивка, инсајдери (персонал или волонтери) кои би можеле случајно или намерно да ја компромитираат безбедноста и закани специфични за вашиот контекст (на пример, граѓанска организација која води кампања против корупцијата може да привлече целни обиди за фишинг или хакирање телефони од засегнатите страни). Исто така, разгледајте ги физичките закани за дигиталните средства, како што се кражба на опрема или уништување поради катастрофи (поплава, пожар – овие, исто така, можат да предизвикаат прекини во ИТ-информациите, поради што се потребни резервни копии надвор од локацијата).

За секоја закана, размислете за можните сценарија: Како би можела да се манифестира оваа закана? На пример:

- Киберкриминалец може да се обиде да ја хакира вашата веб-страница за да ја оштети или да ја користи за дистрибуција на малициозен софтвер.
- Непријателски настроен актер може да испраќа фишинг е-пораки до вашиот персонал, обидувајќи се да украде лозинки и да ги прочита вашите е-пораки.

- Малициозен софтвер како што е ransomware може да зарази компјутер на персоналот, шифрирајќи датотеки и барајќи откуп, како што беше дискутирано во претходните поглавја.
- Волонтер може да изгуби лаптоп со нешифрирани чувствителни податоци.
- Незадоволен поранешен вработен може сè уште да има пристап до сметка ако исклучување од работа не е извршено правилно, што претставува ризик од кражба на податоци или саботажа.

Проценка на веројатноста и влијанието: Не сите ризици се еднакви. Додека некои настани може да бидат многу неверојатни, но катастрофални доколку се случат, други може да бидат веројатни, но со мало влијание. За секое идентификувано сценарио на ризик, оценете колку е веројатно да се случи (ниско, средно, високо) и какво би било влијанието доколку се случи (ниско, средно, високо влијание). На пример, фишинг нападите се многу веројатни (голема веројатност) и би можеле да имаат големо влијание (доколку се украдат акредитивите на сметката) – така што, тоа е висок ризик кој бара силно ублажување. Од друга страна, хардверскиот дефект е доста веројатен со текот на времето (на крајот дискот откажува), но ако имате резервни копии, влијанието е ниско, па затоа е умерен ризик што го управувате со резервни копии. Или целното хакирање спонзорирано од државата може да има големо влијание (тие би можеле длабоко да компромитираат), но ако сте мала локална граѓанска организација без кампањи со висок профил, веројатноста може да биде мала – сепак вреди да се заштитите, но не е ваш фокус број 1.

Овој вид квалитативна проценка ви помага да ги поставите приоритетите. Како што сугерира еден водич фокусиран на граѓански организации, разбирањето на сајбер ризиците и знаењето што треба да се заштити се првите чекори кон ефикасна безбедност. Можете дури и да ги формулирате како прашања како што прави водичот на Liberties: „Кои се нашите најважни дигитални средства? Кој би можел да се обиде да ги нападне и зошто? Што би се случило ако X средство е пробиено или недостапно?“ Вклучете го вашиот тим во ова размислување – различни вработени може да истакнат различни загрижености (на пр. финансискиот службеник се грижи за акредитивите на банкарската сметка, службеникот за комуникации се грижи за хакирање на социјалните медиуми итн.).

Размислете за правните ризици и ризиците поврзани со усогласеност: ГО, исто така, мора да размислат за регулативи како што се законите за заштита на податоци. На пример, во ЕУ, GDPR бара од организациите да ги заштитат личните податоци и да пријавуваат прекршувања. Значи, еден ризик од слаба безбедност е непочитување на законските прописи и казните. Ако вашата ГО обработува лични информации на донаторите или корисниците, прекршувањето може да значи кршење на законите за приватност. Затоа, вклучете ја усогласеноста во размислувањето за ризик – на пр. „Ризик од протекување на лични податоци – влијанието вклучува штета на поединци + законски казни“. Тој ризик очигледно би бил со големо влијание, а ако имате многу лични податоци, можеби со средна веројатност, што бара силни контроли.

***Ризици за документирање и рангирање*:** Напишете краток регистар на ризици – дури и едноставна табела на сценарија за ризик, веројатност, влијание и моментално воспоставени мерки. Рангирајте ги според нивото на ризик (некоја комбинација од веројатност и влијание). Ова ќе ве води каде да распределите ресурси. На пример, може да го рангирате „Фишинг нападот што доведува до компромитирање на сметката“ како

врвен ризик, додека „DDoS нападот на веб-страницата“ може да биде помал ако вашата страница не е контроверзна и има заштита во облакот. Или „Инсајдер случајно протекува податоци преку врската на Google Drive“ може да биде среден ризик за справување преку обука и контроли на пристап.

Апетит за ризик: Исто така, добро е да се препознае дека ниедна организација не може да ги елиминира сите ризици. Дел од управувањето со ризици е одлучувањето за тоа кое ниво на ризик е прифатливо со оглед на вашите ресурси. Ова често се нарекува ваш „апетит за ризик“. Мало граѓанско здружение може да го прифати ризикот од тоа што нема тим за ИТ безбедност достапен 24/7 и наместо тоа да се фокусира на основната одбрана и надворешната поддршка кога е потребно. Целта е да се намалат ризиците на ниво на кое се чувствувате удобно. За високи ризици, спроведувате силни ублажувања; за пониски, можеби поосновни или ги следите со текот на времето.

До крајот на оваа фаза на препознавање на ризикот, треба да имате појасна слика за тоа каде се наоѓате. На пример, може да заклучите: Нашите најголеми ранливости се фишингот и слабите лозинки (висок ризик), плус застарениот софтвер на нашата веб-страница (среден ризик) и ниската свест кај волонтерите (што придонесува за ризиците). Имаме умерен ризик од изгубени уреди (понекогаш споделуваме лаптопи), но ако овозможиме енкрипција, тоа може да се намали. Веројатно не сме конкретно цел на националните држави, но ракуваме со чувствителни информации од заедницата што мора да се чуваат во тајност. Овие сознанија ја поставуваат основата за изработка на вашиот план за безбедност – во суштина, планот ќе се справи со овие идентификувани ризици со соодветни мерки.

Со познавање на дигиталните слаби точки на вашата организација и заканите што највероватно ќе ги искористат, можете ефикасно да планирате одбрана. Овој пристап е во согласност со концептот на донесување одлуки врз основа на ризик – основен принцип препорачан во рамките на сајбер безбедноста. Тој ви гарантира дека ќе се фокусирате на она што е најважно, наместо да се обидувате да правите сè насекаде. Сега, имајќи ја предвид оваа слика за ризик, да продолжиме со градење план што опфаќа политики и практики за ублажување на овие ризици.

Создавање едноставен план за дигитална безбедност

Откако ќе ги идентификувате ризиците, следниот чекор е да формулирате план за управување и ублажување на тие ризици. Планот за дигитална безбедност за ГО обично вклучува политики, процедури и контроли кои се однесуваат на главните области на ризик, како и описи на улогите и одговорностите. Не плашете се од терминот „план“ – може да биде едноставен како листа за проверка или краток документ. Клучот е во тоа што треба да биде практичен и прилагоден на големината и потребите на вашата организација.

Безбедносна политика и управување: Започнете со воспоставување на некои водечки политики. Ова може да биде краток дел во кој се наведува посветеноста на организацијата кон дигиталната безбедност и основните правила што секој треба да ги следи. На пример, имајте Политика за лозинки (на пр. барајте силни лозинки со одредена должина и 2FA за сите критични сметки – можете да се повикате на Дел 2.1 за детали), политика за прифатлива употреба (на пр. упатства за користење на работни уреди и

интернет за соодветни цели, неинсталирање неовластен софтвер итн.) и Политика за заштита на податоци (на пр., правила за ракување со лични податоци, следење на законските барања како што е GDPR и класифицирање на чувствителноста на податоците). ENISA советува дека треба да се напишат јасни политики за сајбер безбедност и да им се соопштат на вработените, во кои ќе биде наведено како се очекува да се однесуваат со ИКТ ресурсите и какви последици постојат за непочитување. На пример, вашата политика може да наведува дека персоналот не смее да споделува лозинки за сметки и мора веднаш да го пријави секој сомнителен обид за фишинг до ИТ контактната точка.

Ако вашата граѓанска организација е мала, можете да споите многу работи во еден документ за општа политика – тоа е во ред. Важниот дел е доделувањето одговорност. Одлучете кој во вашиот тим е задолжен за надзор на безбедноста (може да биде извршен директор или вработен со технолошки вештини кој станува „лице задолжено за безбедноста“). Водичот на ENISA за мали и средни претпријатија забележува дека доделувањето на менаџерска одговорност за сајбер безбедноста е клучен елемент за успех. Затоа, експлицитно наведете улога: на пр. „Менаџерот за операции ќе служи како службеник за безбедност на информациите, одговорен за координирање на безбедносните напори и обезбедување спроведување на политиките“. Ако имате одбор или раководство, осигурете се дека го поддржуваат овој план – поддршката од раководството е клучна за добивање согласност од сите.

Активности за управување со ризик: За секој идентификуван главен ризик (од 3.1), наведете што ќе преземете во врска со него. Ова ефикасно станува јадро на вашиот план:

- На пример, ако „фишингот“ е најголем ризик, вашиот план може да вклучува активности како што се имплементирање на 2FA на е-пошта (веќе дискутирано), спроведување обука за подигање на свеста за фишинг (видете 3.3) и поставување процедури за проверка на необични барања (како процес на потврда на финансиска трансакција).
- Доколку „застарениот софтвер“ претставува ризик, вашиот план би вклучувал одржување на инвентар на клучниот софтвер и распоред или одговорност за ажурирања (можеби лицето за безбедност или надворешната ИТ поддршка обезбедуваат месечни ажурирања).
- Доколку се идентификува ризик од „пробив на лични податоци“: испланирајте мерки како што се ограничување на пристапот до тие податоци (само одредени луѓе можат да пристапат до чувствителни папки), користење енкрипција за особено чувствителни датотеки и воведување постапка за одговор на инциденти (во случај да се случи пробив, како да се спречи и извести – повеќе за тоа во Поглавје 5).
- Доколку постои ризик од „губење на уредот“: испланирајте енкрипција на целиот диск и далечинско бришење како што е споменато, плус можеби и евиденција за пријавување/одјавување на уреди за споделени уреди.

План за одговор на инциденти: Добриот план, дури и едноставен, предвидува дека работите можат да тргнат наопаку. Затоа, вклучете основна постапка за одговор на инциденти: ако се случи инцидент со сајбер безбедност (како инфекција со малициозен софтвер, сомневање за хакирање итн.), кому треба да се јави персоналот и какви чекори ќе преземете? Поглавје 5 го опфаќа ова детално, но во вашиот план, само наведете ги улогите:

на пр. „Целиот персонал мора веднаш да го пријави секој сомнителен безбедносен инцидент на [Име/Улога]. Ќе ги изолираме погодените компјутери од мрежата, ќе го процениме обемот и ќе контактираме со [ИТ поддршка или надворешен експерт], доколку е потребно. Исто така, ќе го информираме раководството и, доколку се вклучени лични податоци, ќе се подготвиме да ги известиме засегнатите страни и властите како што е пропишано со закон.“ Имањето на ова во писмена форма значи дека во жештината на кризата, имате референца што треба да ја следите, што може да заштеди драгоцено време и да ја намали паниката.

Контроли на пристап и управување со сметки: Планот треба да дефинира како управувате со корисничките сметки и пристапот. Ова може да вклучува одржување на список за тоа кој има пристап до кои системи, користејќи го принципот на најмали привилегии (дајте им пристап на луѓето само до она што им е потребно) и, што е важно, процедури за вклучување и исклучување на персоналот/волонтерите. На пример, кога некој ќе ја напушти организацијата, вашиот план мора да обезбеди неговите сметки да бидат веднаш оневозможени или лозинките да бидат променети. Многу безбедносни инциденти се случуваат затоа што поранешните вработени или партнери сè уште имаат активни акредитиви. Вклучете чекори како „По заминувањето на персоналот, ИТ одделот ќе го поништи пристапот до е-пошта, облак дискови и сите споделени лозинки во рок од 24 часа“. Ако користите споделени сметки или генерички најавувања (обидете се да ги минимизирате), имајте план рутински да ги менувате тие лозинки или кога некој со знаење ќе си замине.

Управување од трети страни: Сфатете дека вашата безбедност зависи и од сите услуги или изведувачи од трети страни што ги користите. Доколку сте идентификувале „добавувачи“ како ризик (на пр. аутсорсинг на ИТ поддршка или облак-провајдер кој ја хостира вашата база на податоци), вклучете мерки за управување со тоа. Упатството на ENISA предлага да се осигурите дека сите добавувачи со пристап до чувствителни податоци ги исполнуваат безбедносните барања и имаат договорни договори за безбедност. На едноставен начин, ова би можело да значи проверка дека секоја облак-услуга што ја користите е реномирана и е во согласност со стандардите за заштита на податоците и дека имате резервни копии независни од нив доколку е потребно. Исто така, ако ангажирате веб-развивач или ИТ консултант, осигурете се дека тие ќе потпишат договор за следење на вашите безбедносни политики (како на пример, да не ги користат повторно вашите акредитиви на друго место или да ги чуваат податоците доверливи).

Имплементирајте основни контроли: Резимирајте ги конкретните контроли што ќе ги имплементирате (некои се преклопуваат со советите од Поглавје 2, но тука ги формализирате):

- **Безбедност на уредот:** „Сите организациски лаптопи ќе имаат овозможен антивирус и заштитен sид, како и вклучено енкрипција на целиот диск (BitLocker/FileVault). Автоматското заклучување на екранот ќе биде поставено на 10 минути неактивност“.
- **Безбедност на лозинка**: „Спроведување на политика за лозинки: најмалку 12 знаци, без вообичаени зборови, единствена по сметка. Се охрабрува користењето на менаџер за лозинки и тој ќе биде поставен за персоналот.

2FA ќе биде овозможен на критични сметки (е-пошта, финансиски системи итн.)“.

- **Резервна копија на податоци:** „Критичните податоци (на пр., база на податоци на донатори, програмски датотеки) ќе се резервираат неделно на [безбеден облак/шифриран надворешен диск]. Тест-обновувањата ќе се спроведуваат квартално“.
- **Безбедна конфигурација**: „Осигурете се дека стандардните лозинки на целата опрема се променети. Оневозможете ги непотребните услуги на нашата веб-страница и ажурирајте ја. Периодично проверувајте ги корисничките привилегии за да го отстраните вишокот администраторски права“.
- **Шифрирање за податоци во транзит:** „Користете шифрирани канали за чувствителни комуникации (на пр. Сигнал за доверливи пораки или PGP е-пошта за одредени контакти, доколку е можно). Нашата веб-страница има SSL сертификат (HTTPS) и ние ќе ја спроведеме неговата употреба така што поднесоците од корисниците ќе бидат шифрирани“.

Додека ги наведувате контролите, избегнувајте јазик што е премногу општ или невозможно да се измери („Ќе ги спречиме сите напади“ – нереално). Наместо тоа, фокусирајте се на контролни мерки што можат да се применат. Можеби ќе помогне да се користи рамка како листа за проверка – на пример, CIS контролите (популарна листа на основни сајбер практики) или домените ISO 27001 за инспирација. Но, прилагодете го на она што можете да го имплементирате.

Временска рамка и одржување: Наведете колку често ќе се разгледува самиот план и кој ќе го одржува. Технологијата и заканите еволуираат, па можеби „Овој безбедносен план ќе се разгледува и ажурира годишно (или секогаш кога ќе се случи голема промена во нашиот ИТ) од страна на [Улога]“. Исто така, додека го имплементирате, можеби нема да правите сè одеднаш. Во ред е да ги приоритетизирате активностите во фази. Вашиот план може да има дел „Акционен план“ каде што ќе ги наведете непосредните чекори (на пр. овозможете 2FA на е-пошта во рок од 1 месец, закажете обука следниот месец, имплементирајте резервни копии до третиот квартал итн.). Ова го претвора од само политика во проект со рокови.

Комуникација и спроведување: Планот функционира само ако луѓето знаат за него и ако се спроведува. Откако ќе биде изготвен, споделете го со сите вработени и волонтери. Можеби да одржите краток состанок за да ги објасните клучните точки („сега имаме политика, еве што значи тоа за вашата секојдневна работа“). Добијте повратни информации – можеби некој гледа празнина или има предлог. Вклучете ги во планот или придружните материјали последиците од непочитување на пријателски начин – на пр. „Ако политиките не се следат, тоа може да резултира со дисциплинска мерка, но ние се стремиме да ги поддржиме сите во постигнувањето на овие најдобри практики преку обука и ресурси“. Ова поставува тон дека безбедноста е дел од работата на секого, а не само ИТ работа. Добра аналогија од Институтот CyberPeace: третирајте ја сајбер безбедноста не како изолиран ИТ трошок, туку како овозможувач на вашата мисија. Со вградување на безбедноста во секојдневните процеси, вие обезбедувате континуитет и доверба во вашите операции.

За илустрација, замислете извадок од планот за безбедност на мала еколошка невладина организација:

- **Ризик:** Фишинг на е-пошта на персоналот – **Ублажување**: задолжителен 2FA за е-пошта, обука за препознавање фишинг (водена од ИТ волонтер) и креирање протокол за пријавување на сомнителни е-пораки.
- **Ризик:** Губење на теренски лаптопи – **Ублажување** овозможено е енкрипција на целиот диск, дневна синхронизација на податоците со облакот кога е достапен интернет, поставени се кодови за заклучување на уредот.
- **Ризик**: Деформирање на веб-страницата – **Ублажување**: редовни ажурирања од страна на веб-домаќинот, користење на безбедносен додаток или услуга, резервни копии на содржината на страницата, план за брзо враќање во случај на хакирање.
- **Политика**: Сите нови волонтери мора да добијат основна безбедносна ориентација и да го потпишат договорот за користење на ИКТ (кој опфаќа и несподелување на сметки итн.).
- **Одговорност:** Ја назначив Џејн Доу (менаџер на програмата) за координатор за безбедност за следење и водење на овие активности.

Со мапирање на дејствијата според ризиците и доделување кој, што прави, вашиот план станува спроведлив. Можеби е долг само неколку страници, но тоа е во ред. Краткоста може да биде моќна ако е јасна. Всушност, водичот за мали и средни претпријатија на ENISA ги дестилира советите во 12 чекори на високо ниво кои служат како мини-план за бизнисите (работи како „Развијте добра култура на сајбер безбедност – доделувајте одговорност“, „Планирајте инциденти“ и „Обезбедете резервни копии“). Многу од нив се отсликани овде. Последниот дел од планирањето е спроведување на тие мерки и поттикнување на свеста, што нè води до следниот дел. Држете го вашиот нацрт-план при рака додека разговараме за обуката и културата, бидејќи тоа често е една од компонентите на планот.

Обука за подигање на свеста за персоналот и волонтерите

Дури и најдобриот план за безбедност на хартија може да пропадне ако луѓето во организацијата не се вклучени или не се добро информирани. Човечкото однесување е клучен фактор во дигиталната безбедност – како што беше забележано претходно, значително мнозинство од прекршувањата вклучуваат човечки елемент (грешки или социјален инженеринг). Затоа, едукацијата на вашиот тим и градењето култура на безбедносна свест е едно од највлијателните нешта што можете да ги направите. Сметајте ги вашите вработени и волонтери како прва линија на одбрана (или обратно, најслабата алка ако не се обучени). Овој дел опишува како да се создаде и да се одржи ефикасна обука за безбедносна свест во контекст на ГО.

Започнете со основите: Обуката не мора да биде премногу техничка. Всушност, честопати е подобро да се фокусирате на основните работи што треба и што не треба да се прави, реални примери и интерактивна дискусија. Покријте ги вообичаените закани на начини со кои луѓето можат да се поврзат. На пример, покажете како изгледа фишинг е-пошта (можеби покажете вистинска фишинг е-пошта што ќе ја дезинфицирате за обуката) и нека луѓето ги посочат црвените знамиња (лоша граматика, чудна адреса на испраќачот,

неочекуван прилог итн.). Дискутирајте сценарио: „Ако добиете е-пошта од директорот со која се бара итен трансфер на пари, што треба да направите?“ (Одговор: секогаш проверете со телефонски повик или лице в лице пред да дејствувате, бидејќи може да биде измама од извршен директор). Овие практични вежби им помагаат на вработените да сфатат како би можел да се одвива нападот и како да реагираат мирно. ENISA препорачува обуката да се фокусира на ситуации од реалниот живот со кои се соочуваат малите и средни претпријатија, што важи и за граѓанските организации. Возрасните ученици честопати подобро ги разбираат концептите преку сценарија и приказни отколку преку апстрактни правила.

Клучни теми што треба да се вклучат: Како минимум, опфатете ги темите од Поглавје 2 во форма на обука:

- Безбедни практики за лозинки и употреба на менаџери за лозинки.
- Како да се овозможи и користи 2FA (можеби демонстрација во живо за поставување апликација за автентикација).
- Препознавање на фишинг е-пораки, сомнителни линкови и што да се прави (не кликнувајте, пријавете го).
- Правилно ракување со чувствителни информации (на пр. користење шифрирани алатки за доверливи податоци, некористење лична е-пошта за работна содржина итн.).
- Безбедност на уредот: важноста на ажурирањата, неинсталирањето неовластени апликации, заклучувањето на екраните и внимателноста со

- Предупредување за социјалните медиуми: не споделувајте премногу информации чувствителни на работата на Фејсбук/Твитер, внимавајте на социјалниот инженеринг (како некој што се јавува преправајќи се дека е ИТ поддршка).
- Пријавување инциденти: нагласете култура на необвинување. Луѓето треба да се чувствуваат удобно да пријават ако кликнале на нешто лошо или изгубиле уред, наместо да го кријат тоа. Јасно дајте им до знаење дека брзото пријавување е клучно и дека нема да бидат казнети за искрена грешка - приоритет е да се реши проблемот.

Интерактивна и OCSO-ing обука: Подигнувањето на свеста не е еднократен настан. Планирајте да имате сесии за освежување на знаењето или барем периодични потсетници. Многу организации спроведуваат годишна обука за безбедност. Но, помеѓу нив, можете да споделувате совети на состаноците на персоналот или да испраќате е-пошта со „совет за безбедност на месецот“. На пример, во октомври (Месец на свеста за сајбер безбедноста, кој често се промовира во ЕУ од страна на ENISA), можете да одржите забавен квиз или да споделите кратко видео за безбедноста. Обуката не мора да биде сува. Некои граѓански организации поканууваат експерт за безбедност или користат бесплатни онлајн модули (постојат многу бесплатни курсеви и видеа за сајбер безбедноста насочени кон непрофитни организации и мали бизниси).

Размислете и за искористување на надворешни ресурси: Ако имате ИТ партнер или ако има локален технолошки универзитет, понекогаш тие можат да помогнат со одржување

работилница. Исто така, постојат непрофитни иницијативи кои нудат бесплатни работилници за сајбер-свест за граѓанското општество (на пример, организации како што се TechSoup или CyberPeace Builders може да помогнат во спроведувањето обуки).

Посебен фокус за клучни улоги: Прилагодете ги деловите од обуката на улогите. На вашиот финансиски службеник можеби ќе му треба подлабока обука за откривање измами со фактури или обезбедување на банкарски најавувања (бидејќи граѓански организации биле измамени преку лажни фактури или е-пораки со „имитација на извршен директор“ за да испраќаат пари до измамници). На вашиот персонал за комуникации кој работи со социјалните медиуми можеби ќе му требаат совети за избегнување преземање сметки (како користење на 2FA и претпазливост кон фишинг директни пораки). Раководството треба да ја разбере и својата улога – раководителите често се мета на spear phishing (трикот за е-пошта на „шефот“), па затоа треба да бидат пример за добро однесување (како никогаш да не бараат чувствителни информации или трансфери само преку е-пошта без верификација). Исто така, осигурете се дека волонтерите или краткорочните вработени ќе добијат барем минимално образование во безбедноста, бидејќи можеби нема да присуствуваат на формална обука за персоналот. Едностраничен лист за шеги или краток брифинг за „што треба и што не треба“ кога ќе се приклучат може да помогне.

Создадете култура на поставување прашања: Охрабрете ги сите дека е во ред да се прашуваат работи што изгледаат несоодветни. На пример, ако волонтерот добие необична ИТ инструкција за која не е сигурен, треба да праша. Бидете сигурни дека знаат кого да прашаат – на пр. „Ако добиете каква било сомнителна комуникација или сте несигурни за датотека или врска, контактирајте ја нашата ИТ контакт-точка (или координатор за безбедност) на [контакт]“. Ова се навраќа на советот на Мајкрософт: сајбер-безбедноста е тимска игра и ако видите нешто, кажете му нешто на доверлив советник. Ако некој мисли дека можеби направил безбедносна грешка, како што е кликнување на погрешна врска, треба да се чувствува безбедно веднаш да го пријави тоа, наместо да се плаши од обвинување. Брзата реакција честопати може да ја спречи или минимизира штетата (како исклучување на компјутерот ако се сомнева на малициозен софтвер).

Мерење и засилување: Помага да се процени колку добро функционира вашата обука. Еден начин е да се спроведат внатрешни тестови за фишинг (доколку ресурсите дозволуваат): испратете безопасна е-пошта за „лажен фишинг“ до персоналот по обуката за да видите кој кликнува. Оние што кликнуваат можат да добијат нежна дополнителна обука. Но, ако сте многу мала организација, неформалните прашања и одговори и дискусии може да бидат доволни за да почувствувате разбирање. Дури и прашањето на состанок на персоналот: „Што би направиле ако добиете прилог во е-пошта од некој што не го познавате?“ и слушањето одговори може да открие разбирање. Зајакнете ги пораките со објавување краток список на совети за безбедност на огласната табла во канцеларијата или на каналот Slack. Некои организации дури ја вклучуваат безбедноста во прегледите или рутините за перформансите на персоналот („Дали го завршивте годишниот квиз за безбедност?“), Но, во граѓанските организации, полесен пристап често е доволен освен ако не ракувате со исклучително чувствителни податоци.

Останете информирани и споделувајте новости: Прегледот на заканите се менува. Доколку станете свесни за нова релевантна закана, известете го вашиот тим. На пример, доколку колега од граѓанската организација пријави фишинг кампања насочена кон

организации во вашиот сектор, известете ги вашите вработени: „Внимание, се шири фишинг е-пошта во која се тврди дека е од финансиер - не кликнувајте на такви е-пораки и известете нè ако добиете“. Членството во мрежи на граѓанската организација или групи за споделување безбедносни информации (како што ќе видиме во Поглавје 6) може да обезбеди такви информации што можете да ги пренесете. Ова ја одржува безбедносната свест актуелна и им покажува на вработените дека заканите се реални и се случуваат во нивната околина, а не само теоретски.

Накратко, обуката за подигање на свеста ги претвора вашите луѓе од потенцијални обврски во средства во вашата безбедносна позиција. Како што вели еден слоган за сајбер безбедност: „Вашите вработени се вашиот најдобар заштитен sид“. Со негување на знаењето и будниот начин на размислување, значително ги намалувате шансите за скапа грешка. Запомнете, самата технологија не е доволна – дури и најсилниот заштитен sид може да се заобиколи ако корисникот несвесно го пушти напаѓачот да влезе. Но, добро обучен тим, поддржан од позитивна безбедносна култура, може да спречи многу инциденти пред да започнат или да ги открие рано. Ова зајакнување на човечкиот фактор е во срцето на отпорната дигитална безбедност за граѓанското општество.

Заштита на вашите податоци: Резервна копија и безбедно складирање

Податоците често се опишуваат како „крв на животот“ на организациите. За граѓанските организации, податоците може да вклучуваат информации за корисниците, наоди од истражувања, детали за донаторите, финансиски записи, извештаи за проекти, фотографии и друго. Заштитата на овие податоци не е само спречување на неовластен пристап (доверливост), туку и осигурување дека тие нема да бидат изгубени (достапност) и неправилно изменети (интегритет). Во овој дел, се фокусираме на два фундаментални аспекти на заштитата на податоците: редовни резервни копии и безбедно складирање (и физичко и во облакот).

Важноста на резервните копии: Замислете ги најлошите сценарија – напад со ransomware ги криптира сите ваши датотеки, или пожар/поплава ги уништува вашите канцелариски компјутери, или практикант случајно брише клучна папка. Во секој од овие случаи, неодамнешната резервна копија буквално може да ја спаси вашата организација. Резервната копија е посебна копија од вашите податоци што се чуваат на друг медиум (и по можност на друга локација) од која можете да ги вратите доколку е потребно. Без резервни копии, кое било од горенаведените сценарија би можело да значи неповратна загуба. Со резервни копии, имате безбедносна мрежа.

Еве ги најдобрите практики за резервна копија, од кои многу се усогласуваат со стандардните совети:

Редовна фреквенција: Редовно правете резервни копии на вашите важни податоци. „Редовно“ зависи од тоа колку често се менуваат податоците и колку се критични. За прилично статични податоци, може да биде доволно неделно; за брзо менување на податоци (како дневни логови на програми или активни бази на податоци), може да биде подобро дневно или дури и повеќе пати на ден. Определете ја вашата цел за точка на обновување (RPO): „Колку податоци можеме да си дозволиме да изгубиме?“. Ако тоа е вредност за еден ден, тогаш дневните резервни копии се во ред. Ако губењето дури и на еден час податоци би било катастрофално, стремете се кон почести снимки на податоци.

Автоматизирајте: Процесите за бекап кои зависат од луѓе честопати не успеваат поради заборавеност или зафатен распоред. Користете автоматизирани решенија за бекап кога е можно. На пример, поставете го вашиот датотечен сервер или NAS да прави бекап на надворешен диск секоја вечер во 2 часот наутро или користете услуги за бекап во облак (како Backblaze, Acronis, итн.) кои работат континуирано или според распоредот. Многу услуги за складирање во облак, како Google Drive или OneDrive, исто така чуваат претходни верзии на датотеки, што може да послужи како форма на бекап за уредување или бришење на датотеки.

Повеќе копии и надвор од локацијата: Следете нешто како правилото 3-2-1: 3 копии од податоци (примарни + две резервни копии), на 2 различни медиуми, од кои 1 е надвор од локацијата. Ова може да биде претерано за многу мала организација за граѓански организации, но идејата е добра. На пример, би можеле да имате една резервна копија на надворешен хард диск во канцеларијата и друга шифрирана резервна копија во услуга во облак. Надвор од локацијата значи дека ако канцеларијата изгори, резервната копија надвор од локацијата (или облакот) е безбедна. Резервните копии во облакот по својата природа се надвор од локацијата. Ако користите физички медиуми, размислете за складирање на диск во куќата на член на одборот или во сеф, ажурирајќи го периодично.

Обезбедете ги вашите резервни копии: Резервната копија е копија од вашите чувствителни податоци, затоа заштитете ја. Ако користите надворешен диск, шифрирајте го тој диск (многу алатки за резервна копија или оперативни системи како Windows BitLocker можат да шифрираат надворешни дискови). Ако користите резервна копија во облак, осигурете се дека услугата ги шифрира податоците (повеќето го прават тоа, но можеби ќе изберете да ги шифрирате датотеките пред да ги прикачите за дополнителна безбедност). Ограничете кој може да пристапи до резервните копии. На пример, не оставајте го резервниот диск постојано вклучен во систем што е онлајн – ако се појави ransomware, тој би можел да го шифрира и тоа. Идеално, резервните копии што не се постојано поврзани (офлајн резервни копии) се имуни на малициозен софтвер во вашата мрежа. Ако користите мрежен диск за резервни копии, осигурете се дека има верзија или некоја заштита дека малициозниот софтвер не може веднаш да ги оштети старите резервни копии.

Тест враќања: Резервните копии малку значат ако не работат кога се потребни. Барем неколку пати годишно, тестирајте го процесот на враќање. Обидете се да вратите датотека од резервна копија и видете дали се отвора правилно. Направете вежба за пожар: „Што ако нашиот главен споделен диск умре – можеме ли лесно да ја вратиме резервната копија од синоќа на нов уред?“. Тестирањето ќе открие какви било проблеми како што се оштетена резервна копија, клучеви за криптирање што недостасуваат или процедури што треба да се рафинираат. Многу организации откриле во криза дека нивните резервни копии биле нецелосни или одамна тивко откажале – не дозволувајте тоа да ви се случи вам.

Процедури за резервна копија на документи: Запишете што е резервно копирано, како и каде. Исто така, забележете кој е одговорен за надгледување на резервните копии и како да се изврши обновување. На пример: „Нашата база на податоци за донатори на Salesforce е резервна копија преку сопствен дневен извоз на Salesforce и дополнително преку рачен извоз од страна на Џон на 1-ви од секој месец на шифриран USB-уред“. Ако Џон си замине, некој друг може да го прочита тоа и да продолжи со практиката. Исто така,

документирајте ги потребните акредитиви за резервни копии (безбедно, се разбира), за да не се мачите да пронајдете лозинка за време на итно обновување.

Безбедно складирање и контрола на пристап: Освен резервните копии, заштитата на податоците значи и нивно безбедно складирање за секојдневна употреба. Ова вклучува и физичко складирање (како печатени датотеки, USB-уреди и сервери) и решенија за складирање во облак.

Физички датотеки и уреди: Доколку имате чувствителни информации во физичка форма (хартиени документи, USB-стикови, надворешни хард дискови), чувајте ги во заклучени ормани или во сеф. Не оставајте документи со лични податоци расфрлани на бироата. На пример, листовите за пријавување волонтери или формуларите за корисници треба да се чуваат настрана кога не се користат активно. Искинете ги чувствителните документи пред да ги фрлите. За уредите, како што е дискутирано, користете енкрипција на целиот диск, така што доколку се изгуби компјутер или диск, до податоците нема лесно да се пристапи. Водете инвентар на уредите – знајте кој го има кој лаптоп или телефон. Доколку уредот содржи чувствителни податоци, размислете за политиките да не се остава на небезбедни места (на пр. заклучен во фиока во канцеларија или земен дома од страна на персоналот и безбедно чуван). За време на патувањето, можеби да користите филтри за приватност и чувајте ги уредите со вас (не проверувајте ги лаптопите во багажот доколку е можно).

Облак-складирање (Google Drive, Dropbox, итн.): Услугите во облак се многу практични и имаат вградена редундантност, но мора правилно да ги конфигурирате за безбедност. Прво, овозможете 2FA на сметките во облак за да спречите неовластени најавувања. Второ, внимателно управувајте со дозволите за споделување. Наместо отворено да споделувате цел диск, споделувајте папки/датотеки само со одредени луѓе на кои им е потребен пристап. Периодично проверувајте кој има пристап до што во вашиот Google Drive или Dropbox – отстранете го секој на кого повеќе не му е потребен (вклучувајќи ги и надворешните соработници чии проекти завршиле). Бидете претпазливи со функциите „споделување преку линк“; ако креирате јавна врска до датотека, теоретски, секој што ќе ја пронајде таа врска може да пристапи до неа (некои системи сега нудат врски заштитени со лозинка или врски што истекуваат; користете ги доколку е потребно). За високо чувствителни датотеки, размислете за користење на енкрипција од страна на клиентот пред да ги прикачите (некои алатки се интегрираат со Dropbox/Google Drive за локално енкриптирање на датотеките, така што дури и ако некој ја хакира вашата сметка во облак, ќе види глупости без вашиот клуч).

Упатствата на ENISA за облакот за мали и средни претпријатија ги повторуваат следниве точки: разберете ги уникатните ризици од облакот и осигурете се дека избирате реномирани добавувачи. Тие посебно наведуваат дека треба да се осигурите дека користите добавувачи кои не ги прекршуваат законите во врска со податоците (како што се ограничувањата на GDPR за складирање на лични податоци надвор од ЕУ без заштитни мерки). На пример, ако вашата организација за заштита на податоци работи во ЕУ и складира лични податоци, треба да проверите каде вашиот добавувач на облак складира податоци и евентуално да потпишете договори за обработка на податоци. Ако користите услуги како Dropbox или Google, проверете ја нивната усогласеност и можеби одлучете се

за оние со сервери во региони на кои им верувате, или користете европска алтернатива доколку е потребно.

Шифрирање во транзит и во мирување: Осигурете се дека податоците се шифрирани не само на дисковите, туку и при преносот. Повеќето даватели на услуги во облак ги шифрираат податоците што се во мирување на своите сервери и користат HTTPS за пренос, што е добро. Ако сами ги хостирате податоците (како NAS на лице место достапен преку интернет), поставете VPN или барем осигурете се дека веб-врските се преку HTTPS. Исто така, за исклучително чувствителни информации, можете да поставите слоеви на шифрирање – на пример, шифрирајте документ со лозинка пред да го прикачите дури и во шифрирана папка во облак (двојно шифрирање). Ова може да биде релевантно, да речеме, за списоци на активисти во непријателски регион.

Сегментација на податоци: Не секој во CSO треба автоматски да има пристап до сите податоци. Користете контроли за пристап за сегментирање на податоците. На пример, датотеките со човечки ресурси или медицинските информации за персоналот можат да бидат ограничени само на персоналот за човечки ресурси. Финансиските записи се само за финансискиот тим. Датотеките на проектот се само за оние во тој проект, итн. Многу cloud платформи дозволуваат нивоа на дозволи и пристап базиран на група. На овој начин, ако сметката на еден корисник е компромитирана, напаѓачот не мора да добие сè, туку само она до што тој корисник можел да пристапи. Исто така, се намалува ризикот од внатрешна злоупотреба – луѓето не можат да шпионираат податоци што не се поврзани со нивната улога.

План за задржување и уништување на податоци: Дел од безбедното складирање не е чувањето на податоците подолго од потребното. Старите хард дискови од заменетите компјутери треба безбедно да се избришат или да се уништат (едноставното бришење на датотеки не е доволно; користете софтвер за пребришување или физичко уништување на дискот). Истото важи и за USB-уредите што повеќе не се користат. Ако вашиот CSO акумулира децении лични податоци без потреба, размислете за политика за архивирање или бришење на старите записи. Ова ја намалува количината на чувствителни информации што би можеле да бидат откриени при прекршување на законот и е во согласност со принципите на законите за заштита на податоците (минимизирање на задржувањето на податоците). На пример, ако сте спровеле обука пред пет години и сè уште имате копии од личните карти на учесниците, одлучете дали навистина ви се потребни сега.

Редундантност и континуитет на работењето: Резервните копии обезбедуваат континуитет на податоците, но размислете и за оперативниот континуитет. Ако вашиот канцелариски сервер се сруши, правењето резервна копија на податоците е првиот чекор, но вториот чекор е враќање на функционалноста. Вашиот план може да вклучува резервен уред или префрлување на услугата во облак. За многу мали организации за граѓански организации, работењето од услуги во облак за критични функции (е-пошта, документи итн.) по природа обезбедува континуитет – можете да продолжите со работа од каде било на друг уред ако еден откаже. Но, идентификувајте ги сите поединечни точки на дефект. Ако само едно лице знае како да пристапи до резервни копии, тоа е ризик – вкрстено обучете некого друг или документирајте го тоа, како што е споменато.

Пример за имплементација: Да претпоставиме дека вашиот CSO има споделен диск на NAS уред во канцеларијата за сите датотеки на проектот. Вие имплементирате

ноќна резервна копија од тој NAS на шифриран надворешен HDD што вашиот директор го носи дома за време на викендите (надвор од локацијата). Дополнително, критичните подфолдери се синхронизираат со безбеден облак (како Google Drive или Nextcloud) во реално време за соработка и безбедност надвор од локацијата. Вие закажувате резервни копии на вашата база на податоци за донатори од вашиот CRM и преземате копија месечно, која ја шифрирате и складирате во облакот. За физички датотеки како потпишани формулари за согласност од корисници, ги скенирате и прикачувате (за да се направи резервна копија) и ги чувате оригиналите во заклучен кабинет. За сите лаптопи, вие осигурувате дека BitLocker е вклучен и дека секој има лозинка за BIOS/фирмвер за крадците да не можат да стартуваат од USB за лесно да го заобиколат шифрирањето. Еднаш на квартал, симулирате сценарио за губење на податоци за да се осигурите дека можете да ги вратите од вашите резервни копии.

Со сето ова, постигнувате отпорност: дури и ако се случи сајбер катастрофа или хардверски дефект, вашите податоци се безбедни и можете да продолжите со работа со минимални прекини. Институтот „Сајбер мир“ истакна дека непрофитните организации треба да ја гледаат сајбер безбедноста (а со тоа и мерките за заштита на податоците) како начин што им овозможува безбедно да ја користат технологијата за општествено влијание. Безбедните податоци и резервните копии значат дека можете да ги прифатите дигиталните алатки без постојан страв од губење на критични информации.

Како заклучок, резервните копии и безбедното складирање се како безбедносниот појас и воздушните перничиња на вашето дигитално работење – се надевате дека никогаш нема да ви бидат потребни во итна ситуација, но ако ви бидат потребни, тие можат да ја спасат вашата организација од катастрофални загуби. Комбинирајте го тоа со проактивните мерки од претходните делови (како што се хигиена на лозинки и контрола на пристап) и ќе создадете силен штит за информациските средства на вашата организација за граѓански организации. Потоа, ќе истражиме некои од алатките што се лесни за употреба, кои можат дополнително да ја зајакнат вашата безбедност во пракса, надополнувајќи го планот и политиките што ги воспоставивме.

Резиме на поглавјето

Ова поглавје нуди практични упатства за граѓанските организации за обезбедување комуникации и чувствителни податоци, кои се критични за секојдневното работење и довербата. Опфаќа енкрипција за е-пошта, пораки и складирање на податоци, препорачува алатки како Signal за безбедни разговори и HTTPS за веб сообраќај. Нагласени се силни контроли за пристап, како што се робусни лозинки и 2FA, за да се спречи неовластен пристап до сметки како што се е-пошта или cloud платформи (на пр. Google Drive). Поглавјето се залага за редовни резервни копии на безбедни локации (на пр. енкриптирани дискови) за закрепнување од ransomware или губење на податоци, наведувајќи случај каде што резервните копии спасиле граѓански организации од напад со ransomware. Нагласени се безбедни методи за споделување датотеки, како што се енкриптирани cloud услуги, за да се заштитат податоците на корисниците. Поглавјето се осврнува на усогласеноста со GDPR, нагласувајќи го законското ракување со податоци и согласноста. Вклучува акциони чекори, како што се овозможување 2FA на Gmail или користење бесплатни алатки за енкрипција, што го прави достапен за нетехнички персонал. Примерите како хакирањето на е-пошта на добротворна организација преку фишинг ја нагласуваат потребата од будност. Поглавјето, исто така, опфаќа безбедни видео конференции и практики на социјалните медиуми, осигурувајќи дека граѓанските организации можат безбедно да комуницираат во далечински или во високоризични услови. Со спроведување на овие мерки, граѓанските организации ги заштитуваат чувствителните информации, одржуваат континуитет на работењето и градат доверба кај донаторите.

Контролна листа за годишен преглед и ажурирање на планот за сајбербезбедост за граѓанските организации

Оваа листа за проверка гарантира дека планот за сајбер безбедност на вашата организација за граѓански организации останува актуелен и ефикасен преку преглед на средствата, заканите, политиките и стратегиите за одговор на инциденти годишно или по значајни промени (на пр. нови системи, флуктуација на персонал). Завршувањето на овие чекори одржува робусна дигитална безбедносна позиција за да ја заштити вашата мисија и засегнатите страни:

1. Преглед и ажурирање на дигитални средства

- ⇒ Идентификувајте нови или изменети дигитални средства (на пр. нова база на податоци за донатори, складирање во облак, сметки на социјалните медиуми) додадени од последниот преглед.
- ⇒ Отстранете ги застарените средства (на пр. прекинат софтвер, стари е-пошта сметки) од планот.
- ⇒ Пример: Додаден е нов CRM систем за управување со донатори? Вклучете го во проценката на ризикот. Отстранет е старата база на податоци за волонтери? Отстранете ја од планот.

2. Проценка на нови или еволуирачки закани

- ⇒ Прегледајте ги неодамнешните трендови или закани за сајбер безбедноста што се однесуваат на организациите на граѓанското општество (на пр. зголемен фишинг, рансомвер или локални ризици од надзор).
- ⇒ Консултирајте се со локалните ресурси (на пр. националниот CERT, мрежите на CSO) или глобалните извештаи (на пр. статистиката за напади на CSO на Microsoft) за ажурирања.
- ⇒ Ажурирајте го шаблонот за проценка на ризик за да ги одрази новите закани или промените во веројатноста/влијанието.
- ⇒ Пример: Забележавте пораст на фишинг е-пораки насочени кон граѓанските организации во вашиот регион? Зголемете го резултатот на веројатност за фишинг во вашата проценка на ризик.

3. Преглед на неодамнешни инциденти или несреќи кои за малку ќе се случеле

- ⇒ Документирајте ги сите инциденти со сајбер безбедност или несреќи кои за малку ќе се случеле (на пр. обиди за фишинг, предупредувања за малициозен софтвер) од последниот преглед.
- ⇒ Анализирајте што помина добро, а што не успеа во вашиот одговор (на пр. дали резервните копии функционираа? Дали инцидентот беше навремено пријавен?).
- ⇒ Ажурирајте го планот со научените лекции за да ги подобрите идните одговори.
- ⇒ Пример: Член на персоналот кликнал на фишинг линк, но 2FA спречил пристап. Додадете белешка за да ја зајакнете обуката за 2FA и да ги ажурирате филтрите за е-пошта.

4. Ажурирање на процедурите за одговор на инциденти

- ⇒ Потврдете дека планот за одговор на инциденти ги вклучува тековните чекори, улоги и одговорности (на пр. кој открива, содржи, комуницира).
- ⇒ Ажурирајте ги контакт листите за внатрешни лица кои реагираат (на пр. ИТ персонал, раководство) и надворешна поддршка (на пр. локален CERT, правен советник).
- ⇒ Тестирајте го планот со вежба на маса (на пр. симулирајте напад со ransomware) за да идентификувате празнини.
- ⇒ Пример: Нов ИТ менаџер? Ажурирајте ја неговата улога како раководител за одговор на инциденти. Стариот контакт на CERT е застарен? Заменете го со тековни детали.

5. Проверете ги безбедносните политики и усогласеноста

- ⇒ Прегледајте ги и ажурирајте ги безбедносните политики (на пр. прифатлива употреба, заштита на податоци, BYOD) за да ги одразат новите алатки, регулативи или практики.
- ⇒ Потврдете ја усогласеноста со законите за заштита на податоци (на пр. GDPR, локални прописи) и ажурирајте ги процедурите доколку е потребно (на пр. формулари за согласност, пријавување на прекршување).
- ⇒ Пример: GDPR бара известување за прекршување во рок од 72 часа. Осигурете се дека вашата политика го вклучува овој временски рок и назначен контакт за пријавување.

6. Потврдете ја техничката заштита

- ⇒ Ревидирајте ги безбедносните мерки (на пр., 2FA, антивирус, резервни копии, енкрипција) за да се осигурите дека се активни и ажурирани на сите уреди и сметки.
- ⇒ Проверете за нови безбедносни функции во алатките (на пр. облак платформи, даватели на е-пошта) и овозможете ги доколку е применливо.
- ⇒ Пример: Дали Google Workspace додаде нова безбедносна функција за споделени дискови? Овозможете ја и ажурирајте ги контролите за пристап.

7. Планирајте обука и подигнување на свеста за персоналот

⇒ Закажете обука или освежување на часовите за сајбер безбедност (на пр. свест за фишинг, управување со лозинки) за сите вработени и волонтери.

⇒ Вклучете нови теми врз основа на неодамнешни закани или инциденти (на пр. фишинг управуван од вештачка интелигенција, безбедност во облакот).

⇒ Пример: По локален скок на ransomware, додадете 30-минутна сесија за препознавање на предупредувачки знаци за ransomware.

8. Тестирајте резервни копии и обновување

⇒ Потврдете дека резервните копии се извршуваат според распоредот и се чуваат безбедно (на пр. шифриран облак или надворешен диск).

⇒ Спроведете тест за враќање на резервна копија за да се осигурите дека податоците можат брзо и прецизно да се обноват.

⇒ Пример: Вратете примерок од резервната копија од минатиот месец за да потврдите дека е достапна и недопрена.

9. Вклучете ги лидерството и засегнатите страни

⇒ Кратко информирање на раководството за ажурираниот план и за сите потреби за ресурси (на пр. буџет за нови алатки, време за обука).

⇒ Споделете ги клучните ажурирања со засегнатите страни (на пр. донатори, партнери) за да ја зајакнете довербата во вашите безбедносни практики.

⇒ Пример: Информирајте ги донаторите дека сте ја зајакнале заштитата на податоците за да се усогласат со GDPR, зголемувајќи ја транспарентноста.

10. Документирајте и закажете го следниот преглед

⇒ Запишете ги сите ажурирања во планот за сајбер безбедност и складирајте го на безбедна, достапна локација (на пр. шифриран споделен диск).

⇒ Закажете го следниот годишен преглед или активирајте преглед по поголеми промени (на пр. нов софтвер, преселба во канцеларија).

⇒ Пример: Поставете годишен потсетник во календарот за да го повторите овој процес.

2.4 ПОГЛАВЈЕ 4: БЕЗБЕДНОСНИ АЛАТКИ ПРИЛАГОДЛИВИ ЗА КОРИСНИКОТ

Безбедносни алатки лесни за користење

Досега ги опфативме практиките и планирањето. Во ова поглавје, се фокусираме на алатките и технологиите што можат да го олеснат имплементирањето на безбедноста. Добрата вест е дека не треба да бидете технички волшебник или да инвестирате во многу скапи решенија за да добиете солидно ниво на заштита. Постојат многу економични алатки, достапни и лесни за користење, – честопати дизајнирани имајќи ги предвид непрофитните организации или малите бизниси – кои можат значително да ја подобрат вашата дигитална безбедност. Ќе разгледаме категории на алатки: идентификување безбедни апликации, помагала за безбедно прелистување, обезбедување складирање во облак и алатки за заштита на вашите компјутери и телефони. Секој пододдел ги воведува клучните алатки или методи, со акцент на практичност и леснотија на користење.

Препознавање безбедни апликации

Со безброј достапни софтвери и апликации, како знаете кои се „безбедни“? Овде наведуваме неколку критериуми и примери кои ќе ви помогнат да изберете апликации кои даваат приоритет на безбедноста и приватноста.

Што ја прави апликацијата безбедна? Безбедната апликација обично ги има следниве атрибути:

- Доаѓа од реномиран развивач или извор и активно се одржува (редовно се ажурира за да се поправат грешки).
- Користи енкрипција за заштита на податоците во пренос и во мирување (особено важно за апликации за комуникација и складирање).
- Има добра контрола на пристап (на пр. овозможува силна автентикација, можеби 2FA за сметки).
- Има евиденција за реагирање на ранливости (програмерите издаваат закрпи) и идеално е да има поминато низ безбедносни ревизии.
- Апликацијата ја почитува приватноста (не собира прекумерни податоци ниту прикажува сомнителни реклами што би можеле да инјектираат малициозен софтвер).

На пример, апликациите за пораки како Signal се сметаат за безбедни бидејќи се софтвер со отворен код (секој може да го провери кодот за задни врати), стандардно користат енкрипција од крај до крај и не собираат метаподатоци непотребно. Од друга страна, некои бесплатни апликации може да изгледаат практични, но може да бидат небезбедни – на пример, апликација за случајно споделување датотеки што не е енкриптирана или менаџер за лозинки без опција за 2FA би биле помалку безбедни од алтернативите.

Избор на софтвер за клучни задачи: Еве неколку вообичаени категории на апликации со безбедни препораки:

***Управување со лозинки*:** Користете наменска апликација за управување со лозинки како што е споменато. Добрите опции вклучуваат Bitwarden (отворен код, базиран на облак, бесплатен за основна употреба), LastPass (популарен, има бесплатен пакет, иако имаше пробив во 2022 година, што ја нагласува потребата од користење силни главни лозинки), 1Password (платено, лесно за користење) или KeePass (отворен код, офлајн). Овие имаат силно енкрипција за безбедно складирање на вашите податоци за најавување, а многу поддржуваат 2FA за отклучување на трезорот. Тие, исто така, можат да генерираат случајни лозинки за вас. Користењето на која било од овие е далеку подобро од чување лозинки во табела или нивно повторна употреба.

Безбедни пораки и е-пошта: За пораките, како што е дискутирано: Сигнал за повеќето безбедни разговори; WhatsApp е исто така енкриптиран од крај до крај (и широко користен, иако е во сопственост на Meta, има силни основи на енкрипција). Wire или Threema можат да бидат добри за организациска употреба ако сакате решение хостирано во Европа. За е-пошта, ако ви е потребна поголема безбедност, разгледајте ги провајдерите како ProtonMail или Tutanota, кои нудат енкрипција од крај до крај (особено за внатрешни е-пораки или е-пораки помеѓу корисници на истата услуга). Ако се држите до Gmail или Outlook.com, тие се релативно безбедни ако се користат со 2FA, но чувствителните е-пораки

можеби подобро ќе се испраќаат преку енкриптиран канал или со користење на алатки како GnuPG/PGP за енкрипција (иако PGP е комплексен во пракса).

Антивирус/Анти-малициозен софтвер: Користете добро познати, добро оценети антивирусни решенија како што е споменато. Windows Defender (вграден во Windows 10/11) е солидна основа и без проблеми. Ако сакате трета страна: Avast, AVG, Bitdefender, Kaspersky (имаме предвид дека некои имаат загрижености со Kaspersky поради потеклото, но технички се силни), ESET, итн. Многу од нив имаат бесплатни верзии за основна заштита. Изберете една што не го забавува премногу вашиот систем и има добра стапка на откривање (независни лаборатории за тестирање на антивирусни програми можат да го водат ова). Одржувајте го ажуриран.

Заштитен ѕид и мрежна безбедност: За повеќето, вградениот заштитен ѕид на оперативниот систем е во ред. Ако ви треба повеќе контрола и визуелни знаци (за напредни корисници), алатките како ZoneAlarm или TinyWall на Windows можат да понудат управување со заштитен ѕид на ниво на апликација во попријателски интерфејс. На вашиот рутер, осигурете се дека неговиот заштитен ѕид е вклучен. Некои CSO се одлучуваат за хардверски заштитен ѕид или UTM уреди ако имаат канцелариска мрежа, но тие можат да бидат сложени; честопати, добар рутер (со ажуриран фирмвер) делува како основен заштитен ѕид. Ако управувате со веб-страница, користењето услуга како Cloudflare или безбедносните додатоци на вашиот домаќин може да обезбеди заштитен ѕид против веб-напади.

Безбедни прелистувачи и екстензии: Користете современ безбеден прелистувач (Chrome, Firefox, Edge, Brave). Сите се прилично безбедни; Brave е познат по стандардните поставки за приватност (блокирање на тракери). Firefox е со отворен код и лесно се конфигурира за приватност. Chrome е многу робустен во безбедноста (Google Project Zero агресивно ги открива експлоатите и ги поправа), но испраќа податоци до Google (иако претежно бенигни статистики за употреба). Edge е исто така добар (изграден на моторот на со екстензии: на пр. HTTPS Everywhere (сега во голема мера излишно бидејќи повеќето страници автоматски се HTTPS, но обезбедува енкрипција кога е можно), uBlock Origin или ризикот од злонамерна реклама), а сопствениот блокатор на скокачки прозорци и филтерот против фишинг на прелистувачот треба да бидат вклучени. Некои користат NoScript (стандардно ги блокира сите скрипти), но тоа е напредно и може да ги расипе страниците; тоа е опционално за искусни корисници кои се загрижени за напади базирани на скрипти. Обезбедете клик-за-репродуцирање за Flash/Java (повеќето прелистувачи сега целосно го оневозможуваат Flash, што е добро).

VPN услуги: Ако вашиот тим често користи јавен Wi-Fi или работи од далечина, користењето VPN може да ја зголеми безбедноста. Добрата VPN услуга го шифрира вашиот интернет сообраќај и може да спречи шпионирање на локалната мрежа. Исто така, ја крие вашата IP адреса, што може да додаде приватност. Сепак, користете само реномирани платени/бесплатни (некои бесплатни VPN се фатени како го прават спротивното од приватноста – евидентирање или вбризгување реклами). Алтернативно, ако имате ИТ способности, можете да поставите своја VPN на cloud сервер за вашиот тим. Поедноставно:

многу рутери сега поддржуваат креирање VPN за домашна канцеларија, така што персоналот може безбедно да се врати на мрежата на канцеларијата кога е во странство.

Алатки за енкрипција на диск:

Покрај вградената енкрипција во оперативниот систем, постојат алатки како VeraCrypt (бесплатен, наследник со отворен код на TrueCrypt) кои можат да креираат енкриптирани контејнери или да енкриптираат цели дискови. Корисно ако сакате да енкриптирате USB-стикови или да креирате енкриптирана папка (датотека со контејнер) што можете да ја складирате насекаде (дури и во облакот) и да знаете дека е безбедна. VeraCrypt е малку технолошки комплициран, но добро документиран. Исто така, постојат поедноставни апликации за трезор за телефони и компјутери кои штитат со лозинка и енкриптираат одредени датотеки (на пр. 7-Zip може да креира енкриптирани архиви за датотеки).

Безбедни алтернативи и ажурирања: Како дел од препознавањето безбедни апликации, понекогаш тоа значи замена на ризична апликација со побезбедна алтернатива. На пример, ако некој користи застарена верзија на апликација за која е познато дека има ранливости (да речеме, стар CMS за веб-страница или стар Adobe Acrobat), ажурирајте ја или преминете на алтернативи (како што е користењето на прегледувачот на PDF на Chrome или SumatraPDF наместо стар Adobe Reader, кој беше честа цел на малициозен софтвер). Заменете го софтверот што е на крајот од својот животен век (како Windows 7, кој повеќе не добива ажурирања – надградете на Windows 10/11 или користете лесен Linux ако буџетите се ограничување).

Мобилни апликации: На телефоните, инсталирајте апликации само од официјални продавници за апликации, како што е нагласено. За безбедна комуникација, повторно Signal, WhatsApp (со претпазливост во врска со резервните копии, бидејќи резервните копии на WhatsApp во облакот може да бидат нешифрирани освен ако не се согласите на нивната нова функција за шифрирано резервно копирање). За безбедно складирање на телефоните, користете ги вградените функции за безбедни папки (Samsung Secure Folder) или апликации како KeePassDX за Android за управување со лозинки офлајн.

Обука за алатки: Воведувањето нови апликации е добро само ако луѓето ги користат правилно. Значи, дел од воведувањето на која било алатка (како што е менаџер за лозинки или VPN) е да се даде краток туторијал или водич за мамење. Многу алатки се интуитивни, но почетните упатства обезбедуваат правилна употреба (на пр. покажување како безбедно да се споделуваат лозинки преку менаџерот, а не преку е-пошта).

Со внимателно избирање и користење на безбедни апликации, ги намалувате ранливостите. Сепак, одржувајте рамнотежа: „најбезбедно“ понекогаш значи помалку лесно за користење, што може да доведе до заобиколни решенија што воведуваат ризик (како на пример, ако апликацијата за безбедни пораки е премногу гломазна, персоналот може да се врати на користење на отворена е-пошта за погодност). Изберете алатки што вашиот тим може удобно да ги усвои – честопати, добро конфигурираните алатки обезбедуваат и безбедност и употребливост. На пример, Google Workspace или Microsoft 365, ако се поставени со 2FA и соодветни административни контроли, нудат силна безбедност за е-пошта/документи и се лесни за користење. Тие можеби не се толку затворени како некои нишни решенија, но ако луѓето навистина ги следат безбедносните практики на нив, тие можат да бидат доволни и полесни за интегрирање.

Всушност, препознавањето на безбедните апликации значи малку „домашна работа“ пред да инсталирате нешто ново и да ги фаворизирате оние познати по безбедноста. Многу организации од граѓанското општество споделуваат листи на препорачани алатки (како што е Security-in-a-Box на Front Line Defenders, кој нуди водичи за алатки). Во следните делови, ќе истакнеме специфични области (прелистување на веб, облак, уреди) со конкретни совети и алатки за секоја од нив.

Побезбедно прелистување на интернет

Пребарувањето на интернет е толку вообичаена активност што лесно се заборавааат потенцијалните опасности. Овој дел се темели на практиките за безбедно користење на интернет од Поглавје 2, а сега се фокусира на алатките и поставките на прелистувачот што можат да го направат пребарувањето на интернет побезбедно и поприватно.

Поставки за безбедност на прелистувачот: Прво, проверете дали сте ги конфигурирале вградените безбедносни функции на вашиот веб-прелистувач:

- Одржувајте го прелистувачот ажуриран (повеќето автоматски ажурирања се стандардни; не го исклучувајте тоа).
- Овозможете заштита од фишинг и малициозен софтвер (прелистувачите како Chrome, Firefox и Edge го имаат вклучено ова по дифолт, кое ги проверува посетените URL-адреси во однос на познати лоши листи и прикажува големо црвено предупредување ако страницата е осомничена за фишинг или содржи малициозен софтвер).
- Вклучете ја опцијата „Не следи“ (иако во голема мера е советодавна, некои страници ја почитуваат).
- Размислете за користење на функциите за изолација на сајтови или „песочник“ на прелистувачот, доколку се достапни (Chrome има изолација на сајтови за ублажување на одредени напади – обично е вклучена по дифолт за домени со висок ризик).
- Во Chrome, можете да го користите и режимот „Подобрено безбедно прелистување“, кој споделува повеќе податоци со Google за подобрена проценка на заканите (опционално ако му верувате на Google со тие податоци).

Блокатори на реклами и блокатори на скрипти: Како што е наведено, многу инфекции со малициозен софтвер се јавуваат преку злонамерни реклами или злонамерни скрипти на компромитирани страници. Користењето реномирана екстензија за блокирање реклами како uBlock Origin или Adblock Plus помага не само во приватноста и естетиката, туку и во безбедноста со прекинување на вообичаените вектори на испорака на малициозен софтвер. Овие екстензии блокираат познати домени за реклами и можат да спречат вчитување на сомнителни скрипти. Екстензиите ориентирани кон приватноста како Privacy Badger (од EFF) учат да блокираат тракери и често убиваат злонамерна содржина од трети страни во процесот. Ако сте многу загрижени или посетувате ризични страници, NoScript (Firefox) или ScriptSafe (Chrome) можат да ги блокираат сите скрипти по дифолт - многу безбедно, но бара рачно ставање во бела листа за легитимна функционалност на страницата, што може да биде мачно освен ако не сте технолошки упатени. Може да користите полесен пристап: Firefox во строг режим на подобрена заштита од следење или прелистувачот Brave, кој по дифолт блокира многу скрипти и реклами.

Безбедни врски и екстензии: Секогаш обидувајте се да користите HTTPS верзии на веб-страниците. Екстензијата HTTPS Everywhere (од EFF) автоматски пренасочува кон HTTPS кога е можно, иако денес повеќето големи страници секако се стандардни на HTTPS. Иконата за катанец на прелистувачот е ваш пријател – кликнете на неа за да ги проверите деталите за сертификатот или барем за да се осигурите дека е присутна за која било страница каде што внесувате лозинки или чувствителни податоци. Ако често користите јавен Wi-Fi, размислете за екстензија како HTTPS Everywhere (ако не користите VPN) за да обезбедите енкрипција или само бидете внимателни рачно. Некои современи прелистувачи (Chrome, Firefox) сега ги означуваат страниците што не се HTTPS и имаат формулари како „Небезбедни“ во лентата за адреси – послушајте го тоа предупредување.

Пребарувачи и следење: Пребарувањето на Google е моќно, но ги следи пребарувањата. Ако сакате да избегнете целни реклами или профилирање, сметајте го DuckDuckGo како ваш стандарден пребарувач. Не ги следи пребарувањата и има пристојни резултати за општи пребарувања. Исто така, нуди додаток кој ги оценува практиките за приватност на страниците и спроведува енкрипција. Алтернативно, Startpage дава резултати од Google, но ги отстранува информациите за идентификација. Ова може малку да ја подобри приватноста без многу жртвување на квалитетот на пребарувањето.

Избегнување на отровни резултати од пребарувањето: Понекогаш во резултатите од пребарувањето се појавуваат сајтови со малициозен софтвер или фишинг страници (на пр. лажни сајтови за техничка поддршка). Обучете го персоналот да биде претпазлив кога кликнува на нејасни резултати од пребарувањето и можеби да се држи до познати веб-страници за преземања (на пр. земете софтвер од официјален извор, а не од случајна агрегациска страница). Користењето на екстензија како Web of Trust (WOT) или Bitdefender TrafficLight може да даде икони за репутација до резултатите од пребарувањето, што укажува дали некоја страница се смета за безбедна од заедницата/алгоритмот – иако самите такви алатки имале контроверзии (беше откриено дека WOT собира кориснички податоци, затоа користете ги со претпазливост).

Режим на приватно прелистување: Користете „Инкогнито“ или приватен режим во прелистувачите кога е соодветно – тоа не ве прави анонимни на интернет, но не зачувува колачиња, историја или кеш откако ќе го затворите. Ова е корисно ако се најавувате на услуга на споделен компјутер или ако само сакате да бидете сигурни дека нема остатоци од одредена сесија (како тестирање како вашата веб-страница изгледа на нов корисник). Забелешка: Ова не е алатка за безбедност сама по себе против надворешни закани, но може да спречи други корисници на истиот компјутер да ги шпионираат вашите сесии.

Tor прелистувач за анонимно пребарување: За ситуации каде што ви е потребна анонимност на високо ниво или за да ја заобиколите локалната интернет цензура, прелистувачот Tor е алатка што треба да ја земете предвид. Тој го насочува вашиот сообраќај низ мрежата Tor, криејќи ја вашата IP адреса и шифрирајќи го сообраќајот во мрежата (иако сообраќајот излегува до дестинацијата нешифрирано освен ако не се користи HTTPS). ГО, новинарите и активистите понекогаш го користат Tor за да стигнат до блокирани страници или да избегнат надзор. Недостатокот е што е побавен, а некои страници ги блокираат излезните јазли на Tor. Но, може да биде дел од вашиот комплет алатки во репресивни средини или за чувствително истражување. Користете го само официјалниот прелистувач Tor од torproject.org и разберете ги неговите упатства за

употреба (на пр., не инсталирајте дополнителни додатоци за прелистувач во прелистувачот Tor, не отворајте документи додека сте онлајн бидејќи тие може да го заобиколат Tor, итн.). Ако не е потребен за вашиот контекст, добро конфигуриран нормален прелистувач со VPN може да биде доволен.

Размислувања за избор на прелистувач: Користењето различни прелистувачи понекогаш може да ги „затвори“ активностите. На пример, може да користите еден прелистувач исклучиво за најавување на чувствителни сметки (и со минимални екстензии, само безбедносни), а друг за повремено прелистување. На тој начин, повремениот прелистувач може да ги има сите експериментални екстензии или повремено да посетува помалку безбедни страници, додека „безбедниот прелистувач“ (да речеме, Firefox) го третирате внимателно (без непотребни екстензии, строги поставки, одење само на познати страници како вашата банка, е-пошта итн.). Ова ја ограничува изложеноста на критични колачиња или податоци за сесијата.

Интеграција со е-пошта/веб: Многу современи услуги за е-пошта отвораат линкови или прилози во некаков вид песочник или безбеден прегледувач (Google го има својот „Заштитен приказ“ за прилози, Outlook Web има безбедни линкови ако се овозможени од администраторите). Ако ги имате овие функции, продолжете да ги вклучувате; тие додаваат дополнителен слој, отворајќи содржина во контролирана средина.

Ажурирајте ги додатоците и приклучоците или отстранете ги: Додатоците за прелистувачи како Flash или Java, како што е споменато, треба да се деинсталираат доколку е можно. На повеќето веб-страници повеќе не им се потребни. Ако апсолутно ви треба Flash или други од некоја причина, поставете ги на „Прашај за активирање“ за да не се стартуваат автоматски. Отстранете ги сите неискористени екстензии за прелистувачи; чувајте ги само оние на кои им верувате и на кои им се потребни, бидејќи злонамерните или компромитирани екстензии можат да го „киднапираат“ прелистувањето.

Обележување доверливи страници: Поттикнете го користењето обележувачи/омилени за важни страници (како што се најавувањето на вашата платформа за донации или владини портали што ги користи вашата граѓанска организација). Ова помага да се избегнат печатни грешки (случајно одење на yourbank-secure.com наместо yourbank.com). Исто така, го забрзува препознавањето – корисниците кликнуваат на познатиот обележувач, наместо секој пат повторно да го пишуваат или да го пребаруваат сајтот на Google (што би можело да ги наведе на погрешен пат).

Образование за скокачки прозорци и измами: Ниту една алатка не ги спречува целосно измамите како што се скокачките прозорци „техничка поддршка“ што велат: „Имате вирус, јавете се на овој број“. Затоа, бидете внимателни: ако се појави таков скокачки прозорец или одеднаш започне преземање, затворете го прелистувачот или табот. Современите прелистувачи ги блокираат повеќето скокачки прозорци, но некои реклами ги симулираат. Користењето блокатор на реклами најчесто ги елиминира овие. Исто така, современите оперативни системи имаат паметни функции: SmartScreen на Windows 10 често ќе блокира познати злонамерни преземања или ќе ве предупреди ако некоја апликација не се презема често.

Со комбинирање на овие алатки и поставки, секојдневното прелистување станува значително побезбедно. Целта е повеќеслојна одбрана – една екстензија може да блокира

лоша реклама, прелистувачот може да предупреди за измамничка страница, а вашата претпазливост ќе го направи останатото. Ако нешто се протне, вашиот антивирус може да го открие при преземање. Ниеден поединечен слој не е безгрешен, но заедно тие значително го намалуваат ризикот.

Складирање во облак: Google Drive, Dropbox и нивната безбедност

Услугите за складирање во облак како Google Drive, Dropbox, Microsoft OneDrive и други го револуционизираа начинот на кој организациите за граѓански права соработуваат и складираат податоци. Тие нудат погодност и резервна копија по дифолт, но исто така воведуваат и безбедносни аспекти. Овој дел објаснува како безбедно да ги користите овие услуги.

Поставки за контрола на пристап и споделување: Еден од најголемите ризици со складирањето во облак е случајното прекумерно споделување. Секогаш проверувајте двапати како споделувате датотеки или папки. Стандардно, чувајте ги документите приватни за вашата организација или одредени корисници. На пример, Google Drive дозволува споделување со „Секој што ја има врската“ – користете го тоа само кога е потребно и размислете за додавање лозинка или рок на траење (Google не нуди лозинка за врски, но OneDrive for Business и Dropbox го прават тоа за платени сметки). Наместо тоа, претпочитајте споделување со е-пошта на одредени луѓе (тие ќе треба да се најават, што е побезбедно). Dropbox и Google покажуваат икони што означуваат дали папката е споделена - запознајте се со тие индикатори и периодично ревидирајте ги. Делот „Споделено со мене“ на Google и списокот со споделени папки на Dropbox можат да помогнат во прегледот на она што е отворено.

Ако вашиот CSO користи G Suite/Google Workspace или Microsoft 365, искористете ги административните поставки: можете да го ограничите надворешното споделување или барем да го следите. Можеби ограничете кој може да споделува надворешно или поставете стандардно дека споделувањето линкови надвор од организацијата е исклучено. На тој начин, вработениот мора намерно да го замени за да споделува јавно. Ако користите лична/бесплатна сметка на Google, бидете дополнително внимателни, бидејќи на нив им недостасува административен надзор и може ненамерно да се открие датотека на светот.

Овозможете двофакторска автентикација на сметки во облак: Постојано го нагласуваме 2FA, а тоа е клучно за складирање во облакот, бидејќи пробивот на вашата сметка може да открие многу податоци. Google, Dropbox, Microsoft, Box итн., сите поддржуваат 2FA (обично преку апликации за автентикација или SMS). Осигурете се дека секој корисник во вашиот тим со пристап го прави ова. Многу пробиви се случуваат затоа што се крадат акредитивите за најавување, но 2FA би го спречил напаѓачот.

Управување со уреди и далечинско бришење: Користете ги опциите за управување со уреди. На пример, Dropbox и OneDrive ги прикажуваат сите поврзани уреди (компјутери, телефони). Ако уредот е изгубен или некој си замине, можете далечински да ја прекинете врската, а во случајот на Dropbox, дури и далечински да ги избришете датотеките што биле поставени на локално ниво. Google Drive (Backup and Sync или новиот Drive за десктоп) не ги брише сосема локалните датотеки бидејќи тие обично се само во кешот, но отповикувањето на пристапот е сè уште важно. Административниот панел на Google (за поставите управување со уреди. Дури и ако не можете автоматски да ги избришете,

менувањето на лозинката и одјавувањето од сите сесии (обично поставка за безбедност на сметката) помага да се осигури дека изгубениот лаптоп не може да синхронизира нови податоци или дека не може да се пристапи до сметката.

Шифрирање чувствителни податоци: Како што споменавме претходно, иако овие услуги шифрираат податоци на нивните сервери, тие ги држат клучевите (освен за одредени производи како MEGA или SpiderOak, кои се шифрирани од крај до крај, но се користат поретко). Ако имате особено чувствителни податоци што ги внесувате во Google Drive или Dropbox, можете да додадете свој слој на шифрирање. Опции:

- Користете алатки како VeraCrypt за да креирате шифриран контејнер и да ја зачувате таа датотека на Drive/Dropbox. Потоа ви е потребен VeraCrypt за да го отворите со лозинката. Недостатоци: целиот контејнер мора повторно да се синхронизира кога ќе се промени, а истовремената соработка во него не е едноставна.
- Користете 7-Zip или WinZip за шифрирање на одредени датотеки пред да ги прикачите ако планирате да ги споделите надворешно. Користете силна лозинка и споделете ја таа лозинка преку друг канал.
- Некои cloud услуги нудат шифриран „трезор“ или „шкафче“ како функција (на пр., Dropbox Professional има трезор). Запознајте ги карактеристиките на вашата алатка.
- Ако користите Office 365, можете да примените етикети за чувствителност што ги шифрираат датотеките, така што само одредени сметки можат да ги отворат (сепак, ова е понапредна функција за претпријатија).
- Доколку користите Google, избегнувајте да ставате екстремно чувствителна содржина во текстот на Google Docs освен ако е потребно, бидејќи Google технички може да пристапи до неа. Можеби користете офлајн шифрирани формати и едноставно складирајте ги таму, или користете нешто како клиентот пред да се синхронизираат со облакот (таа создава виртуелен диск; датотеките што се внесуваат се шифрираат, а потоа се синхронизираат). Cryptomator работи добро со Dropbox, Google Drive итн. и не бара посебен серверски софтвер (облакот гледа само бесмислени датотеки). За CSO што ракува со високо доверливи информации, тоа може да вреди да се имплементира за подмножество на податоци.

Мониторинг и предупредувања: Некои услуги овозможуваат следење на активностите. На пример, Dropbox прикажува дневник на настани за споделување и најавувања на страницата на сметката. Администраторот на Google Workspace може да постави известувања за работи како „датотека споделена однадвор“ или „сомнителен обид за најавување“. Доколку се достапни, конфигурирајте ги овие. Дури и на лични сметки, Google Account Security ќе ве предупреди за нови најавувања на уреди – обрнете внимание на тие е-пораки или потсетници („Дали штотуку се најавивте од X уред?“).

Едуцирајте за социјално инженерство: Напаѓачите можеби нема директно да го хакираат Google, но би можеле да ве измамат. Пример: добивате е-пошта што изгледа како споделување на Google Drive од колега, но всушност е вешто прикриена фишинг врска што води до лажно најавување на Google. Фишингот на Google Drive е позната тактика – бидејќи

луѓето им веруваат на е-пораките за споделување на Drive/Docs. Затоа, проверете ги неочекуваните споделувања пред да се најавите преку нив. Google се подобри со додавање безбедносни скенирања на Docs, но потребна е претпазливост. Слично на тоа, не ја внесувајте вашата лозинка за облак во ниту еден скокачки прозорец неочекувано – подобро е рачно да одите на drive.google.com ако бидете замолени.

Историја на верзии и заштита од Ransomware: Една предност на складирањето во облак е историјата на верзии. Ако ransomware ги криптира вашите локални датотеки и тие се синхронизираат со облакот како бесмислица, услугите како Dropbox и OneDrive ги чуваат постарите верзии неколку дена. Можете да ги вратите претходните верзии на многу датотеки (Dropbox Pro дури има и опција за проширена историја на верзии). Запознајте се со тој процес. OneDrive (бизнис) исто така има функција „Врати ги сите датотеки на претходно време“ за масовно обновување по настан на ransomware. Знајте дека е таму, но превенцијата е клучна за да не ви е потребна.

Користење организациски сметки наспроти лични: Доколку е можно, користете сметка управувана од организацијата за складирање во облак, наместо еден куп лични сметки. На пример, со Google Workspace за непрофитни организации (кој често е бесплатен/со попуст за граѓански организации), добивате управувани сметки (како [name]@CSO.org) со Drive. На тој начин, податоците можат да бидат во сопственост на организацијата и можете да ги контролирате ако некој си замине. Личните сметки ги поврзуваат податоците со поединци, што може да биде незгодно ако лицето си замине. Исто така, Google Workspace и Microsoft 365 за организации имаат подобри безбедносни контроли по дизајн отколку бесплатните сметки. Разгледајте ги понудите за непрофитни организации (Google за непрофитни организации, Microsoft за непрофитни организации), бидејќи тие можат значително да ја зголемат безбедноста (и соработката) по ниска или без трошоци.

Редовни ревизии: Одвојте време, можеби квартално или полугодишно, за ревизија на вашите облак-дискови. Отстранете ги старите податоци што повеќе не ви се потребни (ја намалува изложеноста). Проверете ги поставките за споделување на критичните папки. Отстранете го пристапот за корисниците на кои повеќе не им е потребен. Ова одржување осигурува дека вашата облак-околина останува уредна и безбедна.

Накратко, услугите како Google Drive и Dropbox можат да бидат безбедни за организациите на граѓански организации (CSO) ако се користат мудро: заштитете ги сметките со силна автентикација, внимателно конфигурирајте го споделувањето и можеби додадете дополнително енкрипција за високо чувствителни датотеки. Придобивките од практичноста и соработката се огромни, па затоа главно станува збор за целосно користење на безбедносните функции на алатките. Повеќето инциденти на овие платформи се случуваат поради човечка грешка (како споделување линк јавно по грешка или користење слаба лозинка), а не поради прекршување на безбедноста на добавувачите. Со справување со тие човечки фактори и технички поставки, можете со сигурност да го искористите облакот.

Заштита на вашиот телефон и компјутер

Во претходните делови, дискутиравме за општите практики за безбедност на уредите. Овде ќе разгледаме некои специфични алатки и поставки за дополнително да ги заштитите

вашите компјутери и мобилни уреди, бидејќи тие се крајните точки каде што пристапувате до сите ваши дигитални ресурси.

Осигурете се дека FDE е овозможен на сите лаптопи и мобилни уреди. На современите компјутери, ова често бара само вклучување:

- Windows 10/11: Користете **BitLocker** (на Pro изданија) или Device Encryption во Home (доколку е достапно). Откако ќе се вклучи, го шифрира целиот диск и ја поврзува дешифрирањето со вашата лозинка/PIN (и TPM чип). BitLocker може да шифрира и USB дискови (за тоа можете да користите BitLocker To
- macOS: Вклучете го **FileVault** во поставките за безбедност; со еден клик можете да го шифрирате дискот на Mac.
- Linux: Ако користите Linux, инсталирајте со овозможено LUKS енкрипција или користете алатка како cryptsetup. Многу дистрибуции лесни за користење дозволуваат овозможување на енкрипција за време на инсталацијата.
- Android: Повеќето современи Android уреди го шифрираат складиштето по дифолт (особено од Android 7.0+). Само осигурејте се дека сте поставиле силен PIN/лозинка/шаблон, бидејќи шифрирањето е толку силно колку што е силно заклучениот екран.
- iPhone/iPad: Тие се автоматски хардверски шифрирани сè додека поставите лозинка. Затоа, секогаш користете лозинка (и Touch/Face ID за погодност, но таа е заклучена со лозинката како резервна копија).

Апликации за безбедност на мобилни уреди: За Android, размислете за инсталирање на реномирана апликација за безбедност. Опции: Google Play Protect е вграден и ги скенира апликациите (проверете дали е тоа овозможено во поставките на Play Store). Антивирусните програми од трети страни како Avast Mobile, Bitdefender Mobile или Lookout можат да додадат заштита од фишинг и функции „најди го мојот телефон“. Тие исто така можат да скенираат за малициозни апликации надвор од она што Play Protect го наоѓа (иако онаа на Google е пристојна). За iOS, посебните апликации за безбедност се помалку потребни поради sandboxing (иако апликации како Lookout можат да помогнат при лоцирање на телефонот или проверка дали вашиот iOS е џејлбрејк).

Пронајди го мојот уред**:** Секогаш овозможете ги услугите за пронаоѓање и бришење од далечина:

- Android: Користете **Find My Mobile** (услуга на Google) – обично е вклучена ако имате сметка на Google на телефонот. Тестирајте ја (пребарајте „најди го мојот уред“ на Google и видете дали вашиот телефон е пронајден).
- Уредите на Samsung исто така имаат и **Find My Mobile**, што може да биде алтернатива со повеќе функции.
- iPhone: Проверете дали функцијата **Find My iPhone** е вклучена (во поставките на iCloud). Ова ви овозможува да го лоцирате или избришете изгубениот телефон.
- Лаптопи: Размислете за софтвер за следење на лаптопи ако станува збор за кражба. PreyProject (Prey) има бесплатен план за до три уреди и може да помогне во лоцирањето на изгубен/украден лаптоп, па дури и да

фотографира или да испраќа пораки. Некои деловни лаптопи имаат вградена заштита од кражба (како Computrace/LoJack). Но, дури и без специјализиран софтвер, ако лаптопот е изгубен, веднаш променете ги лозинките за сметките до кои имал пристап, и ако бил шифриран, барем знаете дека податоците се безбедни.

Заштитен sид на компјутери: Заштитниот sид на Windows е вклучен по дифолт – држете го вклучен. Тој тивко си ја врши својата работа, блокирајќи го непобараниот влезен сообраќај. Можете исто така да го користите за да блокирате одредени апликации од излез доколку е потребно (помалку вообичаено за CSO сценарио). На Mac, вклучете го заштитниот sид во поставките за безбедност. Веројатно не ви е потребен софтвер за заштитен sид од трети страни; вградените се во ред и избегнуваат збунувачки инструкции што помалку технолошки упатените би можеле да ги дозволат.

Безбедност на фирмверот и BIOS-от: За потреби со висока безбедност, размислете за поставување лозинка за BIOS/UEFI на лаптопите (така што стартувањето од надворешен медиум или менувањето на поставките за стартување бара лозинка). Исто така, овозможете Безбедно стартување (за да спречите rootkit-ови). Овие чекори спречуваат напаѓач со физички пристап, да речеме, да стартува активен оперативен систем за да ја заобиколи безбедноста на вашиот систем. Сепак, ако имате FDE и силна лозинка, тие не треба да влезат во системот. Но, лозинката за BIOS додава слој против неовластено ракување или користење на машината.

Автоматизација на ажурирања на уреди: Разговаравме за ажурирањата на оперативниот систем; дополнително:

- Ажурирајте ги апликациите, на пр. осигурете се дека Microsoft Office или LibreOffice се ажурирани (Office обично се ажурира автоматски преку Office 365 ако го имате, во спротивно проверете го Windows Update или ажурирањето на Office).

  DF читач: Ако користите Acrobat Reader, ажурирајте го. Или користете побезбеден читач како SumatraPDF или PDF прегледувачот на вашиот прелистувач, кои се поедноставни и помалку искористени.
- Јава: Ако мора да ја имате, поставете ја да се ажурира автоматски. Ако не ви е потребна, целосно деинсталирајте ја.
- На телефони, ажурирајте ги апликациите преку Play Store/App Store секогаш кога има достапни ажурирања (овозможете автоматско ажурирање преку Wi-Fi за да го направите тоа лесно).

Оневозможете ги непотребните функции: Неискористените отворени врати можат да се затворат:

- На Windows, ако не ви се потребни функции како RDP (Remote Desktop) или споделување датотеки, исклучете ги за да ја намалите површината на напад.
- На телефоните, внимавајте на Bluetooth и NFC – држете ги исклучени кога не се во употреба (нападите преку Bluetooth се поретки сега со закрпите, но сепак е добра хигиена, особено на јавни места).
- Отстранете ги апликациите со „bloatware“ на телефоните што не ги користите, особено оние што може да работат во позадина или имаат

дозволи (некои Android телефони доаѓаат со претходно инсталирани апликации што би можеле да „рударат“ податоци).

- На кој било систем, не се најавувајте како администратор за секојдневна употреба. Имајте стандардна корисничка сметка за рутинска работа и администраторска сметка за инсталирање на софтвер. На овој начин, ако се активира малициозен софтвер, можеби нема администраторски права за да прави длабоки промени. Секако, многу луѓе го игнорираат ова, но тоа е препорачана практика на Windows и Linux. На Mac, почетниот корисник е администратор, но Mac ќе побара ескалација на лозинката, што делува слично на одвојување на привилегиите.

Користете добар пакет софтвер за безбедност: Доколку буџетот дозволува или бесплатните опции се доволни, користете добро заокружен безбедносен пакет. На пример, Microsoft Defender всушност вклучува не само анти-малициозен софтвер, туку и контролиран пристап до папки (заштита од ransomware што ги спречува непознатите апликации да ги уредуваат вашите документи) и заштита базирана на облак доколку е вклучена. Пакетите од трети страни може да вклучуваат менаџер за лозинки, пробна VPN верзија итн. Инвестирајте само ако ви се потребни тие додатоци; во спротивно, повеќеслојните индивидуални алатки работат.

Безбедност на е-пошта на уредот: Доколку користите е-пошта клиент како Outlook или Thunderbird, осигурете се дека е ажуриран. Бидете внимателни со прилозите што ги отворате. Современите е-пошта клиенти имаат одредено „sandboxing“ (Outlook, на пример, по дифолт не вчитува слики или не извршува макроа и предупредува ако некоја апликација се обиде да пристапи до податоците од е-поштата). Не овозможувајте „дозволи програмски пристап“ освен ако не е потребно за некоја интеграција.

Физичка заштита: Лаптопи – размислете за користење кабел за брава Kensington ако го оставате во заеднички простор (за да спречите кражба од опортунистички причини). За телефони, користете заштитни футроли и можеби заштитници за екрани за приватност ако ракувате со чувствителни информации на нив во јавност (спречува превртување на рамената).

Резервни копии на податоци за уреди: Зборувавме за резервни копии, но еден аспект: за мобилни уреди, направете резервна копија и на вашите податоци (резервна копија во облак или рачно). За iPhone, користете iCloud или локални резервни копии на iTunes; за Android, користете ги услугите или апликациите за резервна копија на Google за критични податоци. На тој начин, изгубениот уред не значи изгубени податоци и можете далечински да ги избришете без двоумење, знаејќи дека се зачувани.

Означување против кражба: Понекогаш наједноставните решенија се најдобри: Означете ги вашите уреди со контакт информации. Лице кое ќе пронајде изгубен уред може да го врати ако е лесно (како налепница на која пишува „Ако се најде, јавете се на [број на CSO]“). Ова е повеќе совет за враќање отколку за безбедност, но може да го спаси денот.

План за замена на уредот: Имајте едноставен план ако уредот е компромитиран или застарен. На пример, ако компјутерот повеќе не добива ажурирања (Windows 7, стар Android), постепено исклучете го или изолирајте го од чувствителни задачи. Можеби

користете го офлајн доколку е потребно за нешто застарено. Но, инвестирајте во одржување на хардверот во рамките на поддржаниот век на траење за безбедност.
Со користење на горенаведените методи и алатки на вашите телефони и компјутери, создавате силен одбранбен периметар околу вашите лични и работни податоци. Замислете го вашиот уред како безбеден трезор: сте го заклучиле (силно најавување), го алармирале (антивирус и заштитен sиd), го зајакнале (ажурирања и енкрипција) и сте поставиле начин за лоцирање или уништување на содржината ако е зафатена (најди го мојот уред, далечинско бришење). Со вакви мерки, дури и ако се појават закани, или ги блокирате или сте подготвени да одговорите без катастрофални загуби.
Со ова се заклучува поглавјето за алатките. Со усвојување на безбедни апликации (4.1), практикување на безбедно прелистување (4.2), правилно користење на складирање во облак (4.3) и зајакнување на уредите (4.4), вашиот CSO ќе има многу посилна дигитална безбедносна позиција. Потоа, ќе разговараме што да правите ако, и покрај сето ова, се појави сајбер проблем – бидејќи ниедна одбрана не е 100% совршена, од витално значење е да имате план за одговор.

Резиме на поглавјето

Поглавје 4 се фокусира на обезбедување на технологијата на која се потпираат граѓанските организации, вклучувајќи компјутери, мрежи и веб-страници. Препорачува ажурирање на софтверот за да се поправат ранливостите, користење антивирусни алатки (на пр. Avast Free) за борба против малициозен софтвер и обезбедување на Wi-Fi со WPA2/WPA3 енкрипција. За веб-страниците, се советува овозможување на HTTPS, редовни резервни копии и ажурирање на Системите за управување со содржини (на пр. WordPress) за да се спречи оштетување или DDoS напади. Студија на случај на веб-страница на граѓански организации што пренасочува кон веб-страница од трета страна поради застарен софтвер ги илустрира ризиците. Поглавјето промовира VPN мрежи (на пр. ProtonVPN) за безбедни врски на јавен Wi-Fi, што е од витално значење за теренскиот персонал. Се нагласуваат евтини решенија, како што е бесплатниот HTTPS преку Let's Encrypt, за да одговараат на буџетите на граѓанските организации. Нетехничкиот персонал е воден да ги потврди поставките (на пр. проверка за HTTPS катанци) без потреба од ИТ експертиза. Поглавјето, исто така, опфаќа енкрипција на уредот и силни лозинки за заштита од кражба или губење. Со обезбедување на инфраструктурата, граѓанските организации спречуваат прекини и прекршувања на податоците, обезбедувајќи континуитет на мисијата. Практичните чекори во поглавјето, како што е закажувањето автоматски ажурирања, ја олеснуваат имплементацијата, усогласувајќи се со целта на е-книгата за достапна сајбер безбедност.

Контролна листа за безбедност на сметките на социјалните медиуми за граѓански организации

Оваа листа за проверка им помага на граѓанските организации да ги обезбедат своите сметки на социјалните медиуми (на пр., Twitter/X, Facebook, Instagram) за да го заштитат своето онлајн присуство и репутација од киднапирање, дезинформации или неовластен пристап. Овие чекори се дизајнирани за персоналот на програмата и волонтерите со минимална техничка експертиза да ги завршат за еден или два часа. Работете на секоја ставка, означете ги завршените задачи. Доколку не сте сигурни, побарајте помош од вашиот менаџер за социјални медиуми, ИТ контакт или поддршка на платформата. Споделете ги наодите со вашиот тим за да одржите безбедно онлајн присуство.

1. Овозможете двофакторска автентикација (2FA)

⇒ Вклучете го 2FA за сите сметки на социјалните медиуми за да биде потребен втор чекор за верификација (на пр. код испратен на вашиот телефон или апликација).

⇒ Совети за платформата:

- Twitter/X: Одете во Поставки > Приватност и безбедност > Двофакторска автентикација. Изберете апликација за автентикација (на пр. Google Authenticator) или SMS.
- Фејсбук: Одете во Поставки > Безбедност и најавување > Двофакторска автентикација. Изберете апликација за автентикација или текстуална порака.
- Инстаграм: Одете во Поставки > Безбедност > Двофакторска автентикација. Овозможете автентикација преку апликација или SMS.

⇒ Пример: Хакиран Твитер профил на граѓанска организација објавил лажни пораки. 2FA спречил понатамошен неовластен пристап.

⇒ Најавете се на секоја сметка, овозможете 2FA и тестирајте го со уредите на вашиот тим.

. Користете силни, уникатни лозинки

⇒ Ажурирајте ги лозинките на најмалку 14 знаци, мешајќи букви, броеви и симболи (на пр., „sunbird&glass7rain“). Користете различна лозинка за секоја сметка.

⇒ Размислете за бесплатен менаџер за лозинки (на пр. Bitwarden) за безбедно складирање на лозинките.

⇒ Совети за платформата:

- Twitter/X: Ажурирајте во Поставки > Промени лозинка. Избегнувајте повторна употреба на лозинки од други платформи.
- Фејсбук: Одете во Поставки > Безбедност и најавување > Промена на лозинка. Уверете се дека е единствена од е-поштата или другите сметки.
- Инстаграм: Одете во Поставки > Безбедност > Лозинка. Користете лозинка за полесно запомнување.

⇒ Пример: Инстаграм-адресата на една граѓанска организација беше компромитирана поради повторно употребена лозинка за е-пошта. Уникатна лозинка го реши проблемот.

⇒ Променете ги лозинките за сите сметки и зачувајте ги во менаџер за лозинки.

3. Отстранете ги неискористените администраторски сметки

⇒ Проверете кој има администраторски или уреднички пристап до вашите сметки на социјалните медиуми и отстранете ги поранешните вработени, волонтерите или неактивните корисници.

⇒ Совети за платформата:

- Twitter/X: Одете во Поставки > Претплати за создавачи > Управувај со тимот за да ги прегледате и отстраните администраторите.
- Фејсбук: Одете во Поставки на страница > Улоги на страница за да ги видите и избришете непотребните администратори или уредници.
- Инстаграм: Проверете Поставки > Овластени апликации или Деловни поставки > Корисници за да го отповикате пристапот за неискористени сметки.

⇒ Пример: Администраторски пристап на поранешен волонтер бил искористен за објавување неовластена содржина. Отстранувањето на старите администратори спречило повторување.

⇒ Прашајте го вашиот менаџер за социјални медиуми: „Можеме ли да ги прегледаме и отстраниме застарените администраторски сметки?“.

4. Поставете и потврдете е-пошта/телефон за обновување

⇒ Осигурете се дека секоја сметка има важечка е-пошта или телефонски број за обновување контролиран од доверлив персонал за обновување на сметката доколку е заклучена или хакирана.

- Совети за платформата:
    - Twitter/X: Ажурирајте во Поставки > Вашата сметка > Информации за сметката. Потврдете дека е-поштата за обновување е активна.
    - Фејсбук: Одете во Поставки > Безбедност и најавување > Контакт за да додадете или ажурирате е-пошта/телефон за обновување.
    - Инстаграм: Одете во Поставки > Безбедност > Обнова на сметка за да потврдите важечка е-пошта или телефонски број.

⇒ Пример: една граѓанска организација (ГО) си ја врати хакираната Фејсбук сметка користејќи е-пошта за обновување. Без неа, обновувањето траеше со недели.

⇒ Додајте или ажурирајте ги деталите за обновување и тестирајте со барање код за обновување.

5. Следење на активноста на сметката

⇒ Редовно проверувајте за необични активности (на пр. објави што не сте ги креирале вие, најавувања од непознати локации).

⇒ Овозможете известувања за најавување каде што е достапно за да добивате известувања за сомнителна активност.

⇒ Совети за платформата:

- Twitter/X: Проверете Поставки > Приватност и безбедност > Поврзани сметки за непознати уреди или апликации.
- Фејсбук: Одете во Поставки > Безбедност и најавување > Каде сте најавени за да ги прегледате активните сесии. Овозможете известувања за најавување.
- Инстаграм: Одете во Поставки > Безбедност > Активност за најавување за да ги видите локациите за најавување и да овозможите известувања.

⇒ Пример: граѓанска организација забележала најавување од друга земја и ја заклучила сметката пред да биде нанесена штета.

⇒ Прегледувајте ги дневниците на активности неделно и пријавувајте чудно однесување до поддршката на платформата.

6. Ограничете го пристапот до апликации од трети страни

⇒ Отстранете го пристапот за апликации или алатки од трети страни (на пр. алатки за закажување, апликации за аналитика) кои повеќе не се користат или не се доверливи.

⇒ Совети за платформата:

- Twitter/X: Одете во Поставки > Приватност и безбедност > Поврзани сметки за да ги повлечете дозволите за апликацијата.
- Фејсбук: Одете во Поставки > Апликации и веб-страници за да ги отстраните неискористените или сомнителните апликации.
- Инстаграм: Проверете Поставки > Безбедност > Апликации и веб-страници за да го отповикате пристапот за непотребни апликации.

⇒ Пример: Апликација за закажување со застарен пристап беше користена за објавување спам на Твитер на граѓанска организација. Со одземање на пристапот проблемот беше решен.

⇒ Прегледајте ги и отстранете ги непотребните врски со апликации во поставките на сметката.

7. Обучете го персоналот за безбедно користење на социјалните медиуми

⇒ Потсетете ги персоналот и волонтерите да не споделуваат информации за сметката, да не кликнуваат на сомнителни линкови или да објавуваат чувствителни податоци (на пр. информации за донаторот) на социјалните медиуми.

⇒ Споделете совет: „Одјавете се од сметки на споделени или јавни уреди".

⇒ Пример: Волонтер објави чувствителни детали за кампањата на јавна објава на Инстаграм. Обуката спречи идни грешки.

⇒ Испратете е-пошта до тимот: „Никогаш не споделувајте најавувања на социјалните мрежи. Одјавете се по употреба на споделени уреди".

8. План за дезинформации или киднапирање

⇒ Развијте едноставен план за одговор во случај на хакирани сметки или дезинформации (на пр., извештај за платформата, објавете појаснување до следбениците).

⇒ Чувајте подготвена нацрт-изјава: „Нашата сметка е компромитирана. Ве молиме игнорирајте ги неодамнешните објави. Го решаваме ова".

⇒ Совети за платформата:

Пријавете хакерски напади преку help.twitter.com/forms/security.

- Фејсбук: Користете го facebook.com/hacked за да пријавите компромитирани сметки.
- Инстаграм: Пријавете проблеми преку Поставки > Помош > Пријави хакиран профил.

⇒ Пример: една граѓанска организација брзо разјасни хакирана објава на Фејсбук, намалувајќи го ширењето на дезинформации.

⇒ Напишете изјава за одговор и зачувајте ги линковите за поддршка на платформата за брз пристап.

ПОГЛАВЈЕ 5: ПРИМЕРИ НА СЦЕНАРИИ НА ИНЦИДЕНТИ СО САЈБЕР БЕЗБЕДНОСТА

Што да направите ако доживеете сајбер инцидент

И покрај најдобрите напори за превенција, инцидентите сè уште можат да се случат. Брз, смирен и методичен одговор може значително да ја намали штетата предизвикана од сајбер инцидент. Ова поглавје ве води низ препознавањето на знаците на инцидент, итните чекори што треба да се преземат, кого да контактирате за помош и како да ја вратите безбедноста потоа. Во суштина, тоа е вашиот план за итни дејствија за дигиталното царство.

Препознавање на знаците на сајбер напад

Колку побрзо сфатите дека нешто не е во ред, толку побрзо можете да реагирате. Сајбер нападите можат да се манифестираат на различни начини; некои очигледни, некои суптилни. Еве ги вообичаените црвени знамиња што можат да укажуваат на проблем:

Порака за Ransomware или заклучен екран: Многу јасен знак – вашиот компјутер одеднаш прикажува порака дека вашите датотеки се криптирани или бара откуп за да го отклучи вашиот систем. Можеби не можете да отворате датотеки, а тие може да имаат чудни екстензии. Честопати, позадината може да се промени во упатства или се појавува прозорец со листа на датотеки и упатства за плаќање. Ако го видите ова, речиси сигурно е напад со ransomware.

Антивирусни предупредувања или лажни AV скокачки прозорци: Ако вашиот антивирус открие нешто, сфатете го сериозно. Обратно, ако видите нечесен скокачки прозорец со натпис „Вашиот компјутер е заразен! Кликнете тука за скенирање“, а не е од вашиот антивирусен софтвер, туку од веб-страница, тоа е тактика за да ве намамат да инсталирате малициозен софтвер. Препознајте ја разликата: вашиот вистински антивирусен софтвер ќе има познат интерфејс и веројатно нема да ве прашува преку случајна реклама во прелистувачот.

Неочекувано однесување на лентите со алатки или прелистувачот: Одеднаш, вашиот прелистувач има нови ленти со алатки, или вашата почетна страница/пребарувач се промени без ваш влез, или пребарувањата пренасочуваат кон чудни страници. Ова сугерира дека е инсталиран рекламен или малициозен софтвер. Слично на тоа, честите скокачки реклами кога сте офлајн или на страници што нормално не ги прикажуваат може да укажуваат на инфекција.

Непознати програми или процеси: Забележувате апликација што никогаш не сте ја инсталирале. Или вентилаторот на вашиот компјутер работи преполно и е бавен, а менаџерот на задачи/мониторот за активности прикажува непознати процеси што го оптоваруваат процесорот. Некој малициозен софтвер може да работи невидливо, но многумина ќе трошат ресурси (како крипто-рудари, што го прави вашиот систем бавен). Ако видите програма што се отвора накратко, а потоа исчезнува, или нови икони на работната површина, истражете.

Вашите пријатели добиваат чудни пораки од вас: Ако колегите или пријателите кажат дека добиле чудна е-пошта или порака на социјалните мрежи од вас што не сте ја испратиле вие, вашата сметка може да биде компромитирана. Примери: спам е-пораки од вашата адреса или вашиот WhatsApp испраќа сомнителен линк во групни разговори. Ова е знак дека или вашиот уред или таа сметка биле преземени.

Лозинката не работи: Многу алармантен знак е ако одеднаш не можете да се најавите на сметката затоа што лозинката е променета (а вие не сте ја промениле). Ако вашата позната точна лозинка е одбиена и враќањето на сметката укажува на промена, претпоставете дека имало пробив во таа сметка.

Невообичаена мрежна или системска активност: Ова може да биде потешко за забележување за просечен корисник, но не и ако имате алатка за мрежен мониторинг или ИТ администратор. Примери за тоа се: пораст на излезниот сообраќај, непознати уреди на мрежата или светлото на тврдиот диск постојано трепка кога не правите ништо (може да значи дека податоците се ексфилтрираат или вирус ги скенира вашите датотеки). Проверете ги и известувањата на заштитен sид (доколку ги има) или логовите на Windows Defender за повторени блокирани дејства.

Датотеки што недостасуваат или се изменети: Ако откриете дека датотеките се избришани или содржината е променета без објаснување, тоа е загрижувачко. Податоците може да бидат бришени или менувани од страна на напаѓач. Исто така, ако видите датотеки што имаат измешани имиња или екстензии како да се заклучени или шифрирани, тоа укажува на ransomware.

Чуден курсор или контрола: Во екстремни случаи, ако глувчето се движи самостојно или прозорците се отворени, а вие не го правите тоа, некој може да има далечинско управување (како да работи малициозен софтвер од далечина или RAT). Веднаш исклучете се од интернет ако се случи тоа.

Системски предупредувања или екрани за пад: Повторените падови или сините екрани може да бидат само проблеми со хардверот/софтверот, но понекогаш руткитите или длабокиот малициозен софтвер предизвикуваат нестабилност. Ако почнало да се случува заедно со други знаци, земете го предвид малициозниот софтвер како можност.

Пренасочувања на прелистувачот: Кога се обидувате да посетите вообичаени страници (како банка или Gmail), ако постојано се пренасочувате кон малку поинаква URL адреса или неочекувано гледате предупредувања за сертификат, можеби имате малициозен софтвер или DNS киднапирање. На пример, обидот да отидете на facebook.com, но секогаш да слезете на страница што не изгледа правилно, значи проблеми.

Во пракса, многу од овие знаци се преклопуваат. На пример, напад со ransomware ќе произведе криптирани датотеки (кои не можете да ги отворите), евентуално текстуална датотека со белешка за откуп во секоја папка и можеби променета позадина на работната површина што го најавува тоа. Компромитирањето на фишинг сметки често се открива кога другите ве информираат за чудни пораки или кога добивате известувања за најавување од необични места.

Ако се сомневате во проблем, но не сте сигурни, бидете претпазливи:

- Ако е потенцијален вирус, извршете целосно антивирусно скенирање.
- Доколку сметката е можеби компромитирана, обидете се да се најавите од друг безбеден уред и променете ја лозинката ако сè уште можете или погледнете ги дневниците за активности на сметката.
- Внимавајте на користењето на мрежата (на Windows 10, можете да ја видите употребата на мрежата по апликација и во Task Manager).

- Ако вашиот уред има алатка за дијагностика или безбедносно скенирање (како што е Windows Security или трета страна), користете ја.

Клучот е да се остане буден. Една практика на граѓанските организации е да ги охрабри вработените да проговорат ако „нивниот компјутер се однесува чудно“. Подобро е да се истражат лажните аларми отколку да се пропушти вистинско нарушување на безбедноста. Не дозволувајте потенцијалната стигма да го спречи пријавувањето; во обуката за безбедност, нагласете дека навременото пријавување е клучно и дека тие нема да бидат обвинети за покренување на загриженост.

Сега кога знаете каде да барате, следниот чекор е да дејствувате брзо кога нешто ви изгледа погрешно. Следните делови ќе опфатат чекори за итен одговор, кого да повикате за помош и како да се закрепнете.

Чекор-по-чекор одговор: Што да направите кога нешто тргне наопаку

Во моментот кога ќе сфатите дека можеби се случува сајбер инцидент, клучно е да преземете намерни чекори за да го контролирате и истражите проблемот. Паниката или погрешната работа (како што е веднаш плаќање откуп или бришење докази) може да ја влоши ситуацијата. Еве еден водич чекор-по-чекор што се усогласува со стандардните фази на одговор на инциденти (идентификување, ограничување, искоренување, закрепнување) на поедноставен начин за CSO средина:

е паничете, проценете ја ситуацијата: Вдишете длабоко и обидете се да разберете што се случува. Кои се знаците и обемот? На пример, дали еден компјутер се однесува чудно или повеќекратно? Дали е проблем со сметката или со уредот? Идентификувањето на природата на инцидентот е водич за следните чекори. Запишете што сте забележале (време, симптоми). Доколку е потребно, брзо направете фотографии или снимки од екранот на сомнителни пораки или екрани за грешки со вашиот телефон (корисно за докази и подоцна прашување експерти).

склучете ги засегнатите системи: Доколку се сомневате дека има активен малициозен софтвер, особено ако се крадат податоци или ако се заразени повеќе системи, веднаш изолирајте го уредот од мрежата. Исклучете го Ethernet кабелот или исклучете го Wi-Fi. Ова го спречува ширењето (на пр. некои црви или рансомвер се обидуваат да скокнат на мрежни дискови) и го спречува далечинскиот управувач на напаѓачот или ексфилтрацијата на податоци. Сепак, не го исклучувајте системот освен ако не морате – едноставно исклучете ја мрежата. Постои нијанса: исклучувањето го спречува малициозниот софтвер, но, исто така, може да избрише непостојани докази. За повеќето сценарија на CSO, во ред е да го оставите вклучен и исклучен, а потоа да извршите скенирања. Но, ако рансомверот активно шифрира датотеки пред вашите очи, можеби брзо ќе го исклучите за да го запрете. Користете проценка; кога се сомневате, исклучувањето на мрежата е добар прв потег.

безбедете ги вашите сметки: Доколку сметката е компромитирана (како е-пошта или социјални медиуми), обидете се да ја вратите контролата. Користете ги процесите за враќање на сметката: веднаш ресетирајте ги лозинките. Одјавете се од сите активни сесии (многу услуги имаат функција „одјавување од сите уреди“). Овозможете 2FA (директна сесија) ако веќе не сте (дури и ако хакерот сè уште има сесија, откако ќе го исклучите, 2FA ќе помогне да се спречи повторното најавување). Известете ги колегите дека сметката е

компромитирана, за да можат сите неодамнешни пораци да ги третираат како потенцијално лажни. Доколку не можете да го вратите пристапот (хакерот ја сменил лозинката и ве заклучил), веднаш контактирајте ја поддршката на давателот на услуги за да пријавите преземање на сметката.

нформирајте го одговорното лице (и можеби сите): Според вашиот безбедносен план (од Поглавје 3), треба да имате лице или тим одговорно за инциденти. Веднаш известете ги. Ако сте вие тоа лице, соберете ги релевантните луѓе. На пример, ако е погоден споделен сервер, известете ги сите корисници да не го користат до понатамошно известување. Ако компјутерот на еден вработен е заразен, може да ги предупредите другите да не отвораат е-пошта од тој компјутер итн. Не го чувајте инцидентот во тајност – неговото криење може да ја влоши штетата. Брзата комуникација им овозможува на другите да бидат внимателни или да преземат заштитни чекори (како што е промена на лозинките доколку е потребно). Исто така, ако имате ИТ поддршка (внатрешна или по договор), веднаш јавете им се. Тие можат да почнат да помагаат со технички мерки или подлабока анализа.

онтролирајте ја штетата: Освен исклучувањето на мрежата, еве чекори за ограничување:

- Доколку станува збор за малициозен софтвер на компјутер, извршете антивирусно скенирање во безбеден режим, доколку е можно, или користејќи „бутабилен“ диск за спасување. Ова може да го стави малициозниот софтвер во карантин, спречувајќи понатамошна штета. Сепак, прво контролирајте го (мрежата е исклучена), а потоа скенирајте – не извршувајте скенирања додека сте сè уште онлајн ако активен напаѓач можеби ве гледа или може да се преземат дополнителни носивост.
- Ако станува збор за ransomware и датотеките се криптирани, утврдете дали запрел или сè уште работи. Исклучете ги сомнителните процеси преку Task Manager ако ги видите (некои користат очигледни имиња, други се случајни). Но, во оваа фаза, веројатно енкрипцијата се прави брзо. Контролирањето тогаш значи ставање на тој компјутер во карантин и недопирање на датотеките (па форензичките експерти или алатките за декрипција би можеле да се обидат да ги обноват).
- Доколку веб-страницата е нападната (оштетена или хакирана), исклучете ја од мрежата доколку можете (на пр. поставете страница за одржување или побарајте од домаќинот привремено да ја суспендира) за да спречите понатамошна штета на посетителите и да ви дадете време да ја поправите.
- За прекршувања на е-пошта, покрај промената на лозинката, размислете за испраќање е-пошта на контактите за да ги предупредите за потенцијален фишинг што доаѓа од вашата сметка.
- Ако податоците се протечени (како на пример, ако ја најдете вашата база на податоци на веб-страница за лепење), ограничете го пристапот до тие системи додека не ја разберете патеката на експлоатација и поправете ја.

окументирајте сè: Додека го правите горенаведеното, водете белешки. Запишувајте ги времињата, дејствијата што сте ги презеле и кој е известен. Ако најдете сомнително име на датотека или процес, запишете го. Оваа документација подоцна помага за обновување, известување и подобрување на вашиот безбедносен план. Исто така е корисна ако

вклучите органи за спроведување на законот или професионалец за одговор на инциденти; тие ќе сакаат да го знаат редоследот на настаните.

обарајте помош доколку е потребно: Не двоумете се да побарате надворешна помош. Доколку имате контакт за сајбер безбедност (можеби ИТ од друга граѓанска организација, експерт волонтер или телефонска линија за помош за сајбер безбедност), јавете им се. Многу земји имаат и CERT (тимови за одговор во итни случаи во компјутери) кои можат да им помогнат или советуваат дури и мали организации. Исто така, постојат бесплатни ресурси во заедницата; на пример, во случај на ransomware, можете да ја проверите веб-страницата „Нема повеќе откуп“ за да видите дали постои алатка за дешифрирање за вашиот тип. Но, користете само реномирани алатки – за каков било совет преку интернет, осигурете се дека е легитимен. Доколку не сте сигурни, прашајте ги вашите доверливи ИТ советници.

ачувајте докази (особено за сериозни инциденти): Доколку инцидентот може да вклучува криминал (на пр. намерно хакирање, голема кражба), подоцна можете да ги вклучите органите за спроведување на законот. Во такви случаи, зачувувањето на логовите и доказите е од клучно значење. Избегнувајте бришење на системските логови или бришење на системот сè додека проблемот не се разбере и реши. Доколку треба да го обновите системот, прво размислете за правење слика од дискот. Во помалку критични случаи, доказите се сè уште корисни за учење – на пр. задржете ја фишинг-пораката што го измамила некого, за да ја проучите и да ги едуцирате другите.

лиминирајте ја заканата: Откако ќе се локализира, работете на отстранување. За малициозен софтвер: користете антивирусна заштита за целосно да го отстраните, или во тврдоглави случаи, реформатирајте/повторно инсталирајте го оперативниот систем (стартувањето одново е најсигурниот начин ако имате резервни копии и не е премногу оптоварувачко). За компромитирани сметки: проверете уште еднаш дали нема задни врати (како на пример, осигурете се дека во е-поштата не се поставени нови правила за препраќање од страна на напаѓачот за тајно препраќање на е-пошта, што често се занемарува). Проверете ги другите сметки бидејќи понекогаш еден кредит добива многу – на пример, ако прелистувачот ги зачувал лозинките, напаѓачот може да ги зграпчи, па можеби ќе треба да ги промените и лозинките на другите сметки.

Ако инцидентот бил ранливост (како на пример, вашата веб-страница имала застарен приклучок што бил експлоатиран), поправете го или отстранете го. Ако проблемот бил нечесен инсајдер, секако, отстранете го неговиот пристап.

бновување: Откако ќе се отстрани непосредната закана, почнете да се враќате во нормала:

- Вратете ги изгубените или оштетените податоци од резервни копии. Проверете дали резервните копии се чисти (скенирајте ги со AV пред да ги вратите, доколку е можно).
- Внимателно повторно поврзете ги системите. На пример, откако ќе го исчистите компјутерот, вратете го на мрежата и следете дали ќе продолжи сомнителниот излезен сообраќај (ако се случи тоа, можеби малициозниот софтвер не е целосно исчезнат).
- Ако повторно сте ги овозможиле сметките или сте ги промениле акредитивите, осигурете се дека секој може повторно да пристапи до она што му е потребно, со нови безбедни лозинки.

- Доколку операциите се запрени (како на пример, сте го исклучиле серверот од работа), координирајте се за да го вклучите вон од шпиц за тестирање, осигурувајќи се дека нема преостанати проблеми.

омуницирајте со ажурирања: Информирајте го персоналот за тоа што се случило и што се презема. Транспарентноста гради доверба и соработка. Исто така, доколку е релевантно, информирајте ги надворешните засегнати страни по потреба (видете го следниот дел за тоа кого да контактирате, на пр., донаторите ако нивните податоци се пробиени итн.). Сепак, генерално, внатрешните проблеми можат да се чуваат интерно, освен ако нема потреба или обврска за известување однадвор.

Низ целиот овој процес, одржувајте став на учење, а не на обвинување. Нападите им се случуваат и на најдобрите од нас. Фокусирајте се на решавање на проблемот и спречување на повторување, наместо да се задржувате на тоа кој кликнал на што (освен користењето на тие информации за подобрување на обуката).

Овој структуриран одговор – идентификувај, содржи, искорени, обнови – ги отсликува упатствата од експертите. За малите граѓански организации, чекорите може да ги преземе едно лице со повеќе функции, но принципот останува.

Следно, да разгледаме подетално кого можеби ќе треба да повикате или пријавите, бидејќи справувањето со инцидент може да вклучува повеќе страни освен вашата организација.

На кого да се обратите за помош: Ресурси за поддршка и добивање помош

Кога се справувате со сајбер инцидент, не мора сами да се справувате со сè. Постојат неколку места и луѓе до кои можете да се обратите за помош, совет и пријавување. Еве преглед на ресурсите за поддршка:

Внатрешен тим и ИТ поддршка: Прво, во рамките на вашата организација, вклучете го секој што е одговорен за ИТ или безбедност (вашиот „технички“ персонал/волонтер или лицето кое ги поставило вашите системи). Доколку имате давател на услуги за управување со ИТ или волонтерски ИТ советник, веднаш контактирајте ги и опишете ја ситуацијата. Тие веројатно виделе слични проблеми и можат да ве упатат кон технички чекори. Дури и член на одборот кој е технолошки искусен или ИТ лице на партнерска организација може да биде вреден сојузник во итна ситуација.

Врснички мрежи и други граѓански организации: Размислете за дискретно контактирање со збратимени организации или мрежи. Честопати, мрежите на граѓански организации (на пример, мрежа за човекови права или чадор организација на граѓански организации) може да имаат споделени ресурси или барем колективно знаење. Тие може да знаат за вообичаени закани во вашиот сектор или регион и да имаат препораки (како „Да, две други граѓански организации ја добија истата фишинг е-пошта; еве што направивме ние“). Соработката може да биде моќна овде. Сепак, проценете колку детали да споделите надворешно – чувајте ги чувствителните специфики за доверливи контакти за да избегнете каков било ризик за репутацијата додека не биде официјално.

Телефонски линии за помош за сајбер безбедност за граѓанското општество: Постојат иницијативи конкретно за помош на граѓанското општество во итни случаи поврзани со дигиталната безбедност. Значајна е телефонската линија за помош за дигитална безбедност на Access Now, која обезбедува бесплатна помош 24/7 за граѓански организации, активисти и новинари во светот. Тие можат да помогнат во случаи како што

се напади на веб-страници, компромитирање на сметки итн., честопати поврзувајќи се со стручни волонтери или давајќи прилагодени упатства. Доколку се најдете во сериозна ситуација надвор од вашите можности, не двоумете се да испратите е-пошта или да се јавите на таква телефонска линија за помош (Access Now е ). Тие одржуваат доверливост и се навикнати на справување со итни случаи.
Друг пример: Програмата „CyberPeace Builders“ на CyberPeace Institute нуди бесплатна помош за сајбер безбедност од страна на корпоративни волонтери за граѓански организации. Доколку веќе сте запишани или поврзани со нив, користете го тој канал. Ако не, можеби е нешто што треба да се земе предвид за во иднина.

Спроведување на законот: Ова зависи од природата на настанот:

- Доколку станува збор за значителен прекршок на податоци што вклучува кражба на лични податоци или намерно хакирање, можеби ќе размислите да ги информирате локалните органи за спроведување на законот или единицата за сајбер криминал. Тие можат да истражат, особено ако се украдени пари или чувствителни информации од донатори или ако има изнуда (како што се барања за ransomware). Сепак, искуствата се разликуваат – на некои места, полицијата е од помош; на други, тие можеби немаат приоритет или немаат експертиза.
- Во земјите со задолжителни закони за известување за прекршувања (како според GDPR во ЕУ, сериозните прекршувања на личните податоци мора да се пријават кај органите за заштита на податоци во рок од 72 часа), треба да ги следите тие прописи. Тоа значи информирање на надлежниот орган за заштита на податоци, доколку е применливо, и евентуално на засегнатите лица (повеќе за тоа во следниот дел).
- Доколку се сомневате дека напаѓачот е од одреден регион или дека постои шема што влијае на повеќе организации, органите за спроведување на законот може да ги спојат овие работи.
- Забелешка: Доколку вашата граѓанска организација работи на чувствителни прашања во земја каде што властите можеби не се пријателски настроени или може да ги злоупотребат тие информации (на пример, ако нападот може да биде спонзориран од државата), ќе треба внимателно да размислите за ангажирање на органите за спроведување на законот. Во такви случаи, првично може да се претпочита консултација со меѓународни тела (како можеби CERT во неутрална земја или само користење на телефонски линии за помош на граѓанска организација).

Национален CERT/CSIRT: Многу земји имаат тим за одговор во итни случаи во компјутери (CERT) или CSIRT, честопати под владин или академски кадар. Тие понекогаш им помагаат на организациите (не само на критичната инфраструктура). Некои имаат посебни гранки за мали бизниси или непрофитни организации. На пример, CERT во ЕУ често реагираат на инциденти и можат да дадат совети или да се координираат со органите за спроведување на законот. Ако имате контакт или лесно можете да пријавите преку нивната веб-страница, тоа може да биде корисно. Тие, исто така, можат да ги предупредат другите или да го следат ширењето на кампањата за малициозен софтвер.

Донатори или партнери: Доколку е вклучен проект или податоци од донатори, или доколку е засегната испораката на услуги, можеби ќе треба да ги информирате партнерите. На пример, ако спроведувате заеднички проект и хакерите ја оштетат веб-страницата на

проектот, информирањето на партнерот од другата граѓанска организација гарантира дека е свесен и може да помогне, или барем дека нема да биде изненаден. Донаторите може да имаат барања за известување доколку средствата се засегнати (на пример, финансиска измама). Од страна на поддршката, некои донатори (особено поголемите или оние кои финансираат капацитети за сајбер безбедност) може да имаат ресурси да ви помогнат. Но, внимателно управувајте со комуникацијата – фокусирајте се на она што се прави за да се реши проблемот, а не само на проблемот, за да ја одржите довербата.

Осигурување: Доколку имате сајбер осигурување или осигурување од општа одговорност кое покрива сајбер инциденти, што е можно поскоро известете ја телефонската линија за инциденти на осигурителот (честопати е потребно за покривање). Тие можат да испратат професионални лица кои реагираат на инциденти или да ве водат кон следните чекори. Многу полиси за осигурување бараат координација од осигурителот за работи како што се одлуки за плаќање откуп. Ако немате осигурување, ова не важи, очигледно.

Заеднички и онлајн ресурси: Постојат онлајн форуми како Reddit r/cybersecurity или r/techsupport или StackExchange Security каде што професионалци понекогаш помагаат. Но, бидете внимателни да не откривате чувствителни детали на јавни форуми. Наместо тоа, може да се пребаруваат тие форуми за да се види дали други се справиле со специфичниот малициозен софтвер или грешка (честопати некој објавил за таа специфична белешка за откуп или однесување на вирусот, што може да даде индиции за поправки). Веб-страници како BleepingComputer имаат посебни делови за помош при отстранување на малициозен софтвер и специфични теми за поддршка на рансомвер, честопати модерирани од експерти кои им помагаат на жртвите бесплатно. Тие често соработуваат и со проектот објавување на лог датотеки итн. – но не правете ништо што не ви е удобно; можеби користете псевдоним ако јавно го дискутирате вашиот случај).

Кога и како да се информираат засегнатите лица/јавноста: Ова е повеќе како „кого да се извести“: ако личните податоци на корисниците или засегнатите страни протекуваат, етичката и можеби законската обврска може да ве принуди да ги информирате тие лица за да можат да се заштитат себеси (на пр. да ги смените лозинките ако нивната е-пошта е протечена, да внимавате на кражба на идентитет). Создавањето вакви комуникации може да биде тешко; треба да биде искрено, извинувачко и да дава насоки (како „Доживеавме безбедносен инцидент каде што вашата е-адреса можеби е откриена. Бидете внимателни за сомнителни е-пораки и размислете за промена на вашата лозинка ако сте ја користеле повторно...“). Ако не сте сигурни, консултирајте се со советник за комуникации или правен советник – сакате да го употребите вистинскиот тон и да не ја признаете неправилно одговорноста, итн.

Психолошка поддршка: Ова можеби звучи надвор од темата, но сериозен инцидент може да биде стресен. Луѓето може да се чувствуваат повредено или виновно (лицето кое кликнало на фишинг може да се чувствува ужасно). Вреди да се обрне внимание на моралот. Осигурете се дека сите знаат дека се случуваат грешки и фокусирајте се на движење напред. Ако сте исклучително стресни, можеби направете кратка пауза или побарајте некого со кого да разговарате (дури и исплашете се пред колега во друга граѓанска организација кој поминал низ слично искуство – може да биде смирувачко).

Откако работите ќе се смират, размислете за сесија за дискусија што е поддржувачка: разговарајте што се случило и како да си помогнете едни на други да се справите и да се зајакнете.
Во сите комуникации со надворешни субјекти, водете евиденција за тоа со кого сте контактирале и кога, како и за сите броеви на случаи/референци или дадени совети. Ова е дел од документацијата и помага при следење на состојбата.
Конечно, користете ги овие канали за поддршка не само за време на инцидентот, туку и потоа за да се подобрите. На пример, телефонската линија за помош Access Now може да ве советува какви чекори да преземете во иднина за да избегнете повторување, или CERT може да ви го испрати својот извештај и препораки.

Враќање на безбедноста: Чекори за обновување
По локализирањето на инцидентот и добивањето помош, последната фаза е враќање на системите во нормална работа и спроведување мерки за спречување на повторување. Обновувањето не е само враќање на податоците, туку и враќање на довербата дека вашата околина е повторно чиста и безбедна.
Чистење и реконструкција на системи: Доколку некои машини биле заразени, по отстранувањето на малициозниот софтвер, оценете дали е потребно целосно повторно инсталирање на оперативниот систем. Честопати, експертите за безбедност сугерираат дека за сериозни компромиси (како руткити или непознат малициозен софтвер), бришењето и повторното инсталирање е најбезбедниот начин да се осигурите дека системот е чист. Да, одзема многу време повторно инсталирањето на апликациите и враќањето на датотеките, но ви дава спокојство што не останува скриена задна врата. Ако одлучите да не го направите тоа, барем стартувајте повеќе алатки за скенирање (еден антивирусен софтвер може да пропушти нешто што друг ќе го фати). Алатки како Malwarebytes, HitmanPro итн., може да се стартуваат покрај вашиот главен антивирусен софтвер за второ мислење. Осигурете се дека оперативниот систем е целосно закрпен по чистењето.
За сметки, по повторното добивање пристап, проверете ги поставките на сметката: Дали напаѓачот поставил правила за пренасочување, додал е-пошта за обновување или уреди со 2FA? (Ова е вообичаено: на пр. хакер на Gmail може да ја додаде својата е-пошта како е-пошта за обновување, па дури и по промена на лозинката, тие се обидуваат да ја вратат сметката.) Отстранете ги сите такви неовластени промени. Проверете ги филтрите за пошта, лозинките за апликации, поврзаните апликации – во основа сè во поставките на сметката што би можело да дозволи континуиран пристап.
Доколку веб-страницата е хакирана, откако ќе ја поправите ранливоста и ќе ја вратите содржината, размислете за преместување на побезбеден хост или додавање заштитен sид за веб-апликации (WAF). Можно е да направите безбедносна ревизија на кодот ако станува збор за прилагодена страница. Исто така, променете ги сите лозинки за базата на податоци и FTP во случај да биле компромитирани.
Вратете ги податоците од резервни копии: Вратете ги сите изгубени податоци. На пример, ако моравте да избришете компјутер, преземете ги неговите кориснички датотеки од резервната копија (но прво скенирајте ги, за секој случај, во случај заразена датотека да се крие во документите). Ако базата на податоци е избришана или криптирана,

вратете ја најновата резервна копија. Проверете дали обновените податоци се недопрени и дали системите што ја користат работат правилно. Понекогаш резервните копии не се толку свежи колку што би сакале, па може да изгубите малку работа. По обновувањето, замолете го персоналот брзо да провери дали нешто недостасува од празнината и, ако е така, проверете дали може повторно да се внесе или повторно да се собере.

Доколку е вклучен ransomware и немате резервни копии, обновувањето е потешко. Консултирајте се со експерти или NoMoreRansom за алатки за дешифрирање – понекогаш постојат бесплатни решенија за одредени видови ransomware. Плаќањето откуп генерално не се препорачува (финансира криминалци и нема гаранција), но некои организации го прават тој тежок избор. Ангажирајте ги органите за спроведување на законот пред да платите, бидејќи тие понекогаш имаат клучеви или можат да советуваат. Ако на крајот има загуба на податоци, испланирајте како да ги обновите тие податоци (можеби контактирајќи ги партнерите за да ви испратат копии од датотеките што ги имаат, итн.).

Подобрете ги и ажурирајте ги безбедносните мерки: По пробивот, одбраната мора да се зацврсти. Ова е фазата на „научени лекции“, каде што ги поправате дупките што биле искористени:

- Доколку станува збор за фишинг, очигледно е потребна поголема обука и можеби технички контроли (како подобар филтер за спам или спроведување на MFA). На пример, наметнете дека сите сметки за е-пошта имаат овозможено 2FA и можеби имплементирајте предупредување за е-пошта за надворешни испраќачи (некои системи стават „[Надворешно]“ во предметот ако поштата доаѓа однадвор, за да се помогне во откривањето на лажирање).
- Доколку станува збор за слаба лозинка или повторно употребени акредитиви, засилете ги политиките за лозинки (подолги, уникатни) и размислете за користење на менаџер за лозинки низ целата организација за да помогнете во тоа. И дефинитивно 2FA за сè што е критично.
- Доколку малициозниот софтвер дошол преку незакрпен софтвер, осигурете се дека ажурирањата се применуваат побрзо. Можеби користете алатка за следење на исчезнатите закрпи или претплатете се на безбедносни билтени релевантни за вашиот софтвер.
- Ако одредена услуга е изложена (како отворен RDP порт кој е активиран со брутален пристап), затворете ја или ставете ја зад VPN.
- Проверете дали правилата на вашиот заштитен ѕид се затегнати, непотребните услуги се оневозможени (како што опфативме во 4.4).
- Размислете за сегментирање на вашата мрежа или податоци: на пр. во иднина чувајте резервни копии на уред кој не е секогаш поврзан за да не може рансомвер да ги погоди или одделете ги чувствителните податоци на диск до кој не секој има пристап.
- Имплементирајте подобро следење: можеби овозможете системско евидентирање и поставете известувања (постојат бесплатни алатки за следење на евиденцијата или дури и само Windows Event Forwarding за да се следат одредени настани како што се повеќекратни неуспешни најавувања).
- Планирајте формална постапка за одговор на инциденти доколку немате таква – во основа запишете што сте направиле овој пат и подобрете го за следниот пат (дел од ажурирањата на безбедносниот план).

Комуницирајте со засегнатите страни: Доколку моравте да ги известите луѓето за инцидентот, следете ги мерките откако ќе се реши. На пример, известете го вашиот одбор или донаторите: „Доживеавме X, презедовме чекори Y и сега операциите се обновени. Го имплементираме Z за да се осигуриме дека ова нема да се случи повторно". Ова уверување и одговорност можат да ја зајакнат довербата ако се направи транспарентно и компетентно. Слично на тоа, ако волонтерите или корисниците биле информирани претходно да бидат претпазливи, подоцна известете ги дека проблемот е решен: на пр.: „Нашата веб-страница сега е безбедна и повторно е достапна онлајн. Ви благодариме за вашето трпение".

Психолошко закрепнување: По пробивот, моралот на тимот може да биде нарушен. Луѓето може да се чувствуваат непријатно („Дали сме сигурни дека хакерите не се сè уште тука?") или виновни. Организирајте состанок за дебрифинг за отворено да разговарате што се случило и третирајте го како можност за учење, а не како лов на вештерки. Пофалете го брзото известување или активностите што ја ограничија штетата. Можеби организирајте мала работилница за „научени лекции" каде што ќе ги информирате сите за тоа кои нови мерки се во сила, што, исто така, ќе ги увери дека работите сега се побезбедни. Тонот треба да биде: се соочивме со предизвик и го надминавме, сега сме посилни.

Документација и известување: Напишете внатрешен извештај за инцидентот – дури и ако е само една страница. Документирајте ја временската рамка, основната причина (доколку е позната), преземените мерки и препораките. Ова е корисно за меморија (шест месеци подоцна, може да заборавите детали што се важни ако се случи нешто слично) и за какви било обврски за надворешно известување. Доколку е потребно со регулатива (на пр. GDPR), поднесете го тој формален извештај до надлежниот орган, вклучувајќи ги и тие детали. Ако се координирате со чадор организација или имате обврска кон донаторите (некои грантови бараат известување за сериозни настани како дел од управувањето со ризик), користете го внатрешниот извештај за соодветна комуникација.

Планови за тестирање и ажурирање: Откако сè ќе биде нормално, совршено време е да го усовршите вашиот план за безбедност и одговор на инциденти. Ажурирајте ги вашите контакт листи (можеби сте сфатиле дека го немате при рака бројот на CERT – сега зачувајте го). Кога одредена алатка би помогнала да се открие или запре порано, размислете за нејзино имплементирање. Дури и размислете за спроведување мала „вежба за противпожарна заштита" во иднина – на пример, тестирајте го враќањето на резервни копии или направете симулиран тест за фишинг за да видите дали новата обука е валидна. Запомнете дека целосното закрепнување вклучува враќање на довербата. Довербата на вашиот персонал во системите, довербата на надворешните партнери во вашето работење. Транспарентноста, дејствувањето и следењето помагаат да се обнови таа доверба. Тоа покажува дека сте го сфатиле сериозно и сте се подобриле.

Конечно, вреди да се сподели знаење (без чувствителни детали) со заедницата доколку е соодветно. На пример, ако откривте нова измама насочена кон граѓанските организации, предупредувањето на другите преку мејлинг листа или мрежа може да ги спречи да станат жртви – позитивен исход од вашата тешка ситуација.

Со внимателно поминување низ овие чекори за закрепнување, не само што ја враќате нормалноста, туку идеално излегувате со посилна безбедносна позиција. Многу организации сметаат дека прекршувањето на безбедноста било повик за будење што на

крајот ги направило подобро подготвени за иднината (иако секогаш е подобро да се подобрите без болката од инцидент!).
Во овој момент, разгледавме како да се справиме со самите инциденти. Потоа, ќе преминеме на моќта на соработката и заедницата во одржувањето на безбедноста, што е честопати недоволно искористен аспект на сајбер безбедноста за граѓанското општество.

Резиме на поглавјето

Ова поглавје ја нагласува човечката страна на сајбер безбедноста, застапувајќи култура свесна за безбедноста преку обука и политики. Истакнува дека 74% од прекршувањата вклучуваат човечка грешка, како што е фишинг, што ја прави едукацијата на персоналот критична. ГО се водени да спроведат основна обука за сајбер безбедност, која опфаќа управување со лозинки и откривање на фишинг е-пораки, користејќи вежби како фишинг квизови. Поглавјето дава совети за изготвување политики за прифатлива употреба на уреди и податоци, обезбедувајќи јасни правила за персоналот и волонтерите. Исто така, ги наведува протоколите за пријавување инциденти, охрабрувајќи брза комуникација за да се спречат прекршувања. Примерите вклучуваат обука на персоналот на ГО за пријавување сомнителни е-пораки, спречување на напад со малициозен софтвер. Поглавјето ја нагласува улогата на раководството во моделирањето безбедни практики (на пр. користење 2FA) за легитимирање на напорите. Препорачува наградување на будноста, како што е пофалба на персоналот за пријавување фишинг, за да се зајакнат навиките. Со вградување на безбедноста во секојдневните работни процеси, ГО создаваат отпорна култура. Фокусот на поглавјето на едноставни, инклузивни практики обезбедува пристапност за сите вработени, усогласувајќи се со моделот „обучи го обучувачот“ од наставната програма и целта на е-книгата за поттикнување долгорочни безбедносни навики.

Не-Техничка контролна листа за безбедност на веб-страницата за граѓански организации

Оваа листа за проверка им овозможува на персоналот на програмата и волонтерите да ја потврдат и подобрат безбедноста на веб-страницата на вашата ГО без потреба од техничка експертиза. Овие чекори помагаат да се заштити вашата веб-страница од напади (на пр. деформирање, DDoS) и да се осигури дека таа останува доверлива платформа за вашата мисија:

1. **Проверете дали вашата веб-страница користи HTTPS**
   - ⇒ Посетете ја вашата веб-страница и побарајте икона за катанец во лентата за адреси на прелистувачот (пред URL-то) или „https://“ на почетокот на адресата.

⇒ Ако видите предупредување „http://“ или „Не е безбедно“, контактирајте го вашиот веб-домаќин за да овозможите HTTPS (на пр. побарајте бесплатен сертификат Let's Encrypt).

⇒ Пример: Вашата страница е „www.CSOexample.org”. Осигурете се дека лентата за адреси прикажува „https://www.CSOexample.org”со катанец.

⇒ Доколку HTTPS недостасува, испратете е-пошта до вашиот веб-домаќин: „Ве молиме овозможете HTTPS за нашата веб-страница“.

2. Потврдете редовни резервни копии

⇒ Прашајте го вашиот веб-домаќин или менаџер на веб-страница дали вашата веб-страница редовно се резервира (на пр. дневно или неделно) и каде се чуваат резервните копии (на пр. во облак или надворешен сервер).

⇒ Побарајте тест-враќање за да се осигурите дека резервните копии работат (на пр. прашајте: „Можете ли да ја вратите нашата страница на верзијата од минатата недела?“).

⇒ Пример: Вашата веб-страница е исклучена по напад. Неодамнешната резервна копија ви овозможува брзо да ја вратите.

⇒ Контактирајте го вашиот домаќин: „Дали имаме автоматски резервни копии на веб-страниците? Колку често се прават?“

3. Потврдете ги ажурирањата на софтверот на веб-страницата

⇒ Проверете кај вашиот веб-домаќин или менаџер на веб-страница дали системот за управување со содржини (CMS, на пр. WordPress, Joomla) и додатоците/темите се ажурираат редовно.

⇒ Прашајте дали ажурирањата се автоматски или дали некој ги проверува месечно.

⇒ Пример: Застарен WordPress додаток предизвика хакирање на страницата на една организација за граѓански организации. Редовните ажурирања го спречуваат ова.

⇒ Испратете е-пошта до вашиот домаќин: „Дали нашиот CMS и додатоци се ажурирани? Ако не, ве молиме овозможете автоматски ажурирања”.

4. Безбеден администраторски пристап

⇒ Осигурете се дека само доверлив персонал има администраторски пристап до веб-страницата. Проверете кај менаџерот на вашата веб-страница за да го отстраните пристапот за поранешни вработени или волонтери.

⇒ Потврдете дека администраторските сметки користат силни лозинки (на пр. 14+ знаци, како „sunbird&glass7rain“) и двофакторска автентикација (2FA).

⇒ Пример: Старото најавување на поранешен волонтер било искористено за деформирање на страницата. Отстранувањето на неискористените сметки го спречува ова.

⇒ Прашајте го менаџерот на вашата веб-страница: „Кој има администраторски пристап? Можеме ли да ги отстраниме старите сметки и да овозможиме 2FA?“

5. Проверете за сомнителни промени на веб-страницата

⇒ Посетете ја вашата веб-страница и побарајте необична содржина (на пр. чуден текст, непознати слики или пренасочувања кон други страници).

⇒ Веднаш пријавете какво било чудно однесување кај вашиот веб-домаќин или ИТ-контакт.

⇒ Пример: почетната страница на граѓанска организација е пренасочена кон измамничка страница поради хакерски напад. Раното известување брзо го реши проблемот.

⇒ Пребарувајте ја вашата страница и забележете сè што е необично. Контактирајте го вашиот домаќин: „Нашата страница има [проблем]; ве молиме истражете”.

6. Заштитете се од DDoS напади

⇒ Прашајте го вашиот веб-домаќин дали обезбедуваат DDoS (Distributed Denial of Service) заштита за да ја одржат вашата страница онлајн за време на пренатрупани сообраќајни пренапони.

⇒ Потврдете дали се овозможени основните заштити (на пр. бесплатниот план на Cloudflare).

⇒ Пример: Веб-страницата на граѓанска организација за човекови права е исклучена за време на DDoS напад. Бесплатната DDoS заштита ја одржуваше во функција.

⇒ Испратете е-пошта до вашиот домаќин: „Дали имаме DDoS заштита? Можеме ли да овозможиме бесплатна услуга како Cloudflare?“.

7. Ограничете го јавниот пристап до чувствителни страници

⇒ Проверете дали чувствителните страници на веб-страницата (на пр. најавување за администратор, внатрешни документи) се заштитени со лозинка или скриени од јавноста.

⇒ Побарајте од менаџерот на вашата веб-страница да го ограничи пристапот само на овластени корисници.

⇒ Пример: списокот на донатори на една граѓанска организација беше случајно објавен. Проблемот беше решен со заштита на страницата со лозинка.

⇒ Прашајте: „Дали чувствителните страници како што се најавувањата на администраторите се заштитени? Можеме ли да додадеме лозинки доколку е потребно?“.

8. Обучете го персоналот за безбедно користење на веб-страницата

⇒ Потсетете ги персоналот и волонтерите да не споделуваат администраторски акредитиви или да објавуваат чувствителни информации (на пр. податоци за донатори) на веб-страницата.

⇒ Споделете брз совет: „Секогаш одјавувајте се од административниот панел на веб-страницата по употреба“.

⇒ Пример: Член на персоналот споделил администраторска лозинка во е-пошта, што довело до хакерски напад. Обуката го спречува ова.

⇒ Испратете е-пошта до тимот: „Никогаш не споделувајте детали за најавување на веб-страницата. Одјавете се откако ќе ја уредите страницата“.

ПОГЛАВЈЕ 6: СОРАБОТКА И ПОДДРШКА ЗА ДИГИТАЛНА БЕЗБЕДНОСТ

Заедно посилни: Соработка и поддршка

Дигиталната безбедност не е само индивидуален или организациски напор; тоа е колективен потфат. Организациите на граѓанското општество можат да имаат голема корист од заедничката работа, споделувањето знаење и меѓусебната поддршка во услови на сајбер закани. Во ова поглавје, дискутираме како соработката може да ја подобри безбедноста – од споделување информации со други граѓански организации и градење култура на безбедност во заедницата, до едукација на јавноста и користење на локални и меѓународни мрежи за поддршка.

Споделување информации со други граѓански организации

Ниедна граѓанска организација не е остров, особено во дигиталната сфера. Честопати, нападите или ризиците што се насочени кон една организација можат да влијаат и врз други во истиот сектор или регион. Со споделување информации за заканите и најдобрите практики, граѓанската организација може колективно да ја подобри својата одбрана.

Зошто да споделите? Може да има двоумење да се споделат безбедносни инциденти од срам или страв дека тоа открива ранливост. Сепак, придобивките обично ги надминуваат ризиците кога се прават во вистинската средина. Ако вашата организација за граѓански организации станала жртва на фишинг кампања, информирањето на другите може да им помогне да ја избегнат таа стапица. Слично е на набљудувањето на соседството: ако една куќа е цел на измама, тие ги предупредуваат соседите. Во сајбер безбедноста, овој концепт на споделување информации е формализиран во некои сектори преку ISAC (центри за споделување и анализа на информации). Додека постојат формални ISAC за индустрии како финансии или здравство, организациите за граѓански организации можат да создадат свои неформални кругови или групи за споделување.

Што и како да споделите:

- **Предупредувања за закани:** Доколку наидете на специфична фишинг е-пошта, датотека со малициозен софтвер или сомнителен пристап (како некој што се претставува како донатор), можете да споделите индикатори: на пр. „Добивме е-пошта од адресата X со наслов Y која беше злонамерна. Бидете внимателни“. Обезбедете доволно детали за другите да ја препознаат. Некои мрежи на граѓански организации поставуваат листи со е-пошта или безбедни групи за разговор за такви известувања.
- **Тактики и лекции:** Откако ќе доживеете инцидент или дури и вежба, споделете го она што сте го научиле, можеби анонимизирајќи ги чувствителните делови. На пример, би можеле да споделите: „Имплементиравме двофакторска авторизација на сите наши сметки и тоа блокираше повеќе неовластени обиди за најавување. Вреди трудот“. Ова ги мотивира другите да усвојат слични мерки.
- **Политики и материјали за обука:** Размената на ресурси како што се примероци на безбедносни политики или слајдови за обука може да биде заемно корисна.

Една ГО може да има одлична основна презентација „Сајбер безбедност 101 за вработените“ што би можела да ја дистрибуира за другите да ја прилагодат, наместо сите да го измислуваат тркалото одново.

- **Контакти за помош:** Доколку имате добро искуство со консултант за безбедност или ИТ волонтер, можете да го споделите тој контакт со колега од граѓанската организација на која ѝ е потребна помош (секако, со дозвола). Слично на тоа, доколку член на граѓанската организација присуствува на работилница или вебинар за сајбер безбедност, може да им ги пренесе клучните заклучоци на колегите кои не можеле да присуствуваат.
- **Вежби за зглобови:** Можно е да се организираат заеднички настани како што е обука за безбедност за повеќе организации или дури и симулирана вежба за фишинг меѓу неколку граѓански организации. Ова не само што ги подобрува вештините, туку и ја поттикнува довербата меѓу учесниците.

Градење доверба за споделување: Безбедносните информации се чувствителни. За да споделувате отворено („бевме хакирани со методот X, ги изгубивме податоците Y“), потребна ви е доверба дека колегите нема да ги злоупотребат тие информации или да судат строго. Воспоставете норма на доверливост. Можеби прво формирајте мала, доверлива група (како во рамките на коалиција или работна група на граѓански организации кои се познаваат) пред да се проширите. Некои заедници го воспоставуваат Правилото на Чатам Хаус (можете да ги користите информациите, но да не откриете кој ги кажал). Некои дури може да потпишат и едноставен меморандум за внимателно ракување со споделените информации. Со текот на времето, како што се случуваат корисни размени, довербата расте.

Употреба на платформи: Некои платформи и алатки можат да го олеснат безбедното споделување:

- Шифрирани листи за е-пошта (користејќи услуги или PGP ако сите учесници можат да управуваат со нив, иако PGP е комплицирано).
- Групи за пораки на Signal или слични апликации за брзо информирање за итни проблеми.
- Можно е да се користи платформа како Rocket.Chat или Matrix/Element за да се создаде затворен форум за граѓански организации (самостојно хостирани или на сигурен сервер) каде што можат да дискутираат за безбедносни теми подалеку од очите на јавноста.
- Некои мрежи може да соработуваат со CERT за да им доставуваат анонимизирани информации и да добиваат совети за возврат.

Успешни примери: Имаше иницијативи како „CyberPeace Cafe“ или средби на граѓански организации за безбедност. Исто така, NetHope (конзорциум од хуманитарни граѓански организации) работи на споделени упатства за сајбер безбедност и информации за инциденти, третирајќи ја инфраструктурата на граѓанското општество како критична. Друг е концептот „Организација за споделување и анализа на информации (ISAO) за граѓански организации“ што некои го предложија. Во Европа, во рамките на проектите на ЕУ (како можеби контекстот на оваа наставна програма), партнерските граѓански организации би можеле да постават заеднички дневник за инциденти или Slack канал специјално за оваа намена.

Со споделување навремени информации, граѓанските организации можат да го трансформираат нападот врз еден човек во рано предупредување за сите. Исто така, ефикасно ја користат оскудната експертиза – едно ИТ лице во водечка граѓански организација може ефикасно да служи како советник на неколку партнери преку размена на знаење.

Градење заедница за безбедност

Освен реактивното споделување информации, граѓанските организации можат проактивно да создадат култура на заедницата што дава приоритет на дигиталната безбедност. Поддржувачката заедница може да здружи ресурси, да поттикне учење и да го засили застапувањето за подобри безбедносни алатки и политики.

Мрежа на шампиони за безбедност: Идентификувајте луѓе во локалното граѓанско општество кои имаат интерес или вештини за сајбер безбедност. Тие би можеле да бидат технолошки вешти вработени, волонтери со ИТ-искуство или симпатизерски академици. Формирајте локална група „шампиони за безбедност“ која периодично (дури и виртуелно) се состанува за да дискутира за проблеми и решенија. Овие шампиони потоа можат да дејствуваат како клучни лица во нивните соодветни организации. На пример, можеби еден ИТ службеник од граѓанска организација ги учи другите како да ги зајакнат своите Wi-Fi мрежи, додека друг кој научил за GDPR споделува совети за усогласеност.

Работилници и обуки: Организирајте обуки во заедницата, поканувајќи повеќе граѓански организации. Можеби квартална работилница на теми како „Користење менаџери за лозинки“, „Обезбедување мобилни комуникации“ или „Како да се одговори на сајбер инцидент“ – од кои голем дел произлегува од содржината на оваа книга. Со заедничка обука, персоналот на граѓанските организации не само што стекнува знаење, туку и се запознава со колеги, што може да формира основа за доверба за споделувањето информации што ги дискутиравме. Честопати можете да добиете експерти (од универзитети, компании или владини CERT-ови) да дојдат и да ги одржат овие работилници по ниска или бесплатна цена за непрофитни организации како дел од општествената одговорност на граѓаните или службата за заедницата. Моќта е во бројките – корпоративниот тренер можеби нема да одржи бесплатна сесија за една граѓанска организација од пет лица, но можеби ќе одржи за колективна публика од 50 лица од различни граѓански организации..

Врсничка поддршка и менторство: Поттикнете систем на другарство: можеби спојте помала граѓанска организација без ИТ поддршка со поголема граѓанска организација која има ИТ оддел за менторство. На пример, граѓанска организација која успешно имплементирала безбедност во облак може да биде ментор на друга која штотуку започнува. Ова може да биде неформално, но обезбедува брза помош кога е потребно („Еј, како имплементиравте 2FA за сите вработени? Можете ли да ни покажете?“).

Здружување на ресурси: Размислете за заедничка набавка или споделување алатки. Група граѓански организации може да добие попуст на големо за безбедносен софтвер или да сподели претплата (во рамките на условите на лиценцата). Алтернативно, ако граѓанските организации имаат резервен сервер или безбедносен уред, можеби други можат да го користат неговиот капацитет. Во некои контексти, граѓанските организации поставиле заеднички ИТ услуги (како заеднички безбеден сервер за е-пошта или заедничка

ИТ служба за помош во три или четири организации) за колективно да си обезбедат поквалитетна безбедност отколку што секоја од нив би можела поединечно.

Застапување на заедницата: Исто така, постои улога за граѓанските организации колективно да се залагаат за подобри услови за сајбер безбедност. На пример, лобирање кај донаторска заедница за финансирање на градење капацитети за сајбер безбедност или притисок врз добавувачите на софтвер да понудат подобри цени или функции за непрофитни организации (некои непрофитни коалиции ги натераа Microsoft или Google да вклучат бесплатни безбедносни додатоци за граѓанските организации). Дополнително, подигањето на свеста кај добавувачите на интернет услуги или властите за заканите за граѓанското општество (како софистициран фишинг што ги таргетира активистите) може да доведе до пошироки заштитни мерки. Замислете го концептот „граѓанското општество како критична инфраструктура“ што го опиша NetHope – со здружување, граѓанските организации можат да изнесат аргумент дека им е потребна заштита слична на владата или индустријата и на тој начин да привлечат поддршка.

Солидарност во одговорот на инциденти: Кога ќе се случи голем инцидент (како на пример, граѓанска организација е погодена од сериозен напад или се соочува со онлајн вознемирување итн.), заедницата стои посилно спротивставувајќи се на тоа. Друга граѓанска организација може да помогне со работна сила, да го сподели товарот на јавните пораки или да обезбеди привремени услуги. Има случаи, на пример, кога една група за човекови права била нападната со DDoS, друга ја пресликала содржината на нивната веб-страница за да ја одржи достапна (како дигитална солидарност). Таквата кооперативна одбрана им покажува на противниците дека нападот врз една ќе ги обедини многу други, што може да биде одвраќање.

Споделување приказни за успех: При градењето позитивна заедница, споделете и приказни за успех (како што ќе биде истакнато во Поглавје 7). Ако една граѓанска организација успешно спречила обид за фишинг благодарение на обуката, прославете го тоа во билтенот на заедницата. Тоа ги мотивира сите дека инвестирањето во безбедноста се исплати. Препознајте ги и заблагодарете им се на оние кои им помагаат на другите со безбедноста (можеби на годишна конференција на граѓанска организација, пофалете го тој еден ИТ волонтер кој патува наоколу инсталирајќи антивирус бесплатно во различни граѓански организациии – тој вид поттик на моралот поттикнува континуирана поддршка).
Со развивање на тесно поврзана заедница околу безбедноста, граѓанските организации се префрлаат од изолирани, ранливи цели во отпорна мрежа. Напаѓачите (без разлика дали се криминалци или угнетувачки режими) честопати се потпираат на напад врз изолирани организации; обединет фронт значи дека информациите за нивните тактики се шират брзо, а одговорите можат да бидат координирани. Како што вели една максима, „Безбедноста е во солидарноста“.

Информирање на јавноста: Подигање на свеста за дигитална безбедност

Граѓанските организации често служат како едукатори и застапници на заедницата. Дигиталната безбедност не е само внатрешно прашање; многу од луѓето со кои работите (корисници, членови на заедницата, активисти итн.) исто така, би можеле да имаат корист од подобра свест за безбедноста. Со проширување на знаењето за дигитална безбедност на вашата поширока заедница, го мултиплицирате влијанието и помагате во создавање побезбедна средина на граѓанското општество.

Работилници и обуки во заедницата: Размислете за организирање јавни работилници или вебинари за основна дигитална безбедност за вашата публика. На пример, ако сте младинска организација, организирајте сесија на тема „Безбедност на социјалните медиуми“ за тинејџери и нивните родители, која ќе ги опфаќа поставките за приватност, сајбер малтретирањето, фишингот итн. Ако работите со бранители на човекови права, можеби обука за безбедна комуникација (користење на Signal, избегнување на надзор). Овие сесии можат да се интегрираат во вашата редовна програма. Многу граѓански организации веќе спроведуваат обуки за поврзани теми (на пр. медиумска писменост, онлајн приватност) – можете да вклучите модули од оваа наставна програма. Обезбедувањето такво образование не само што ѝ помага на заедницата, туку и ја позиционира вашата граѓански организација како лидер во решавањето на современите проблеми, што може да го зајакне вашиот углед и доверба.

Развијте едноставни образовни материјали: Можете да креирате или да адаптирате летоци, инфографици или блог постови за совети за безбедност и да ги споделите јавно. На пример, едностраничен текст насловен како „5 начини да се заштитите онлајн“ со лесни чекори (користете силни лозинки, не кликнувајте на сомнителни линкови, ажурирајте софтвер итн.), кој го дистрибуирате на настани или на социјалните медиуми. Визуелниот, нетехнички јазик најдобро функционира за јавната публика. Можете да адаптирате содржина од национални кампањи за подигање на свеста за сајбер безбедноста (материјалите за месецот на сајбер безбедноста во октомври често се слободно достапни на повеќе јазици преку ENISA или други). Осигурете се дека материјалите се на локалниот јазик и контекстуално релевантни (споменете локални измами што ги гледаат луѓето, локални контакти за поддршка). Ова, исто така, може да се поврзе со мисијата на вашата организација – на пр. граѓанска организација за права на потрошувачите што предава за избегнување на онлајн измами.

***Кампањи за подигање на јавната свест*:** Доколку ресурсите дозволуваат, спроведете кампања за дигитална безбедност. Ова може да се поврзе со нешто како Денот на побезбеден интернет или некој релевантен локален развој (на пример, пораст на измамите преку СМС во вашата област). Користете ги вашите комуникациски канали за редовно да ги потсетувате следбениците за безбедноста (твитувајте совети за безбедност, споделувајте вести за тековни измами на кои треба да внимавате, итн.). Некои граѓански организации соработуваат со телекомуникациски компании или медиуми за емитување безбедносни PSA пораки. Дури и кампања од мал обем, како што е објавувањето неделно „Вторник за безбедносни совети“ на вашата Фејсбук страница, може полека да ја подигне свеста.

Искористете ги медиумите и раскажувањето приказни: Луѓето разбираат преку приказни. Доколку е соодветно, споделете анонимизирани приказни за дигитални инциденти и како тие биле надминати (можеби како дел од блог или разговор). На пример, приказна за тоа како е-поштата на лидер на заедница била хакирана и искористена за испраќање лажни пораки и што е научено од тоа. Тоа може да го хуманизира проблемот и да ги предупреди другите да бидат претпазливи. Медиумите, исто така, може да бидат заинтересирани ако постои тренд (како што е зголемено таргетирање граѓански организации или активисти на интернет); интервју со вашата граѓански организација на темата може да ја истакне важноста на дигиталната безбедност за поширокаата публика.

Лобирање за подобри политики и поддршка: На повисоко ниво, информирајте ја јавноста и креаторите на политики за потребите на граѓанското општество во сајбер безбедноста. ГО можат колективно да се залагаат за владини програми што им помагаат на ГО со сајбер безбедноста (некои земји имаат програми за грантови или специјален теренски пристап на CERT). Исто така, застапувајте се за лесна за користење безбедност во технолошките производи – на пр. притискање на софтверските компании да ги направат безбедните поставки стандардни, така што корисниците се побезбедни без потреба од обемна експертиза. Во ЕУ, на пример, постојат дијалози за заштита на граѓанското општество од сајбер закани; гласовите на ГО на тие форуми осигуруваат дека мерките на политиката ги вклучуваат и нив (како финансирање и обука).

Соработувајте со училишта и библиотеки: Можеби партнерство со локални образовни институции или библиотеки за да се организираат заеднички сесии за дигитална писменост и безбедност. Многу јавни библиотеки одржуваат часови по компјутери; нудењето дел за безбедност би можело да биде добредојдено. Училиштата сè повеќе треба да предаваат за безбедност на интернет; ГО со експертиза би можеле да ја поддржат таа наставна програма. Со тоа што помагате во едукацијата на младите и пошироката јавност, градите општество кое е посвесно за безбедноста, што индиректно ја штити и вашата ГО (помалку компромитирани лични сметки што би можеле да доведат до фишинг на вашата организација, итн.).

Поттикнување на известување и дијалог: Поттикнете ја јавноста со која комуницирате да пријавува сајбер криминал или сомнителни инциденти. Многу поединци страдаат тивко или се премногу засрамени (како некој да паднал на измама). Создадете клима каде што луѓето можат да побараат помош – можеби вашата невладина организација може да послужи како медијатор за да ги упати до полицијата или телефонските линии за помош ако се жртви на онлајн вознемирување или измама. Некои невладини организации преземаат улога на застапници за дигитални права, истакнувајќи прашања како што се приватноста или надзорот во општеството, што е во корелација со безбедносната свест.

Усогласете се со вашата мисија: Прилагодете го образованието за јавна безбедност во согласност со вашата мисија за кохерентност. На пример, ако вашата граѓанска организација се занимава со правата на жените и знаете дека активистките се соочуваат со онлајн вознемирување, фокусирајте ја свеста на тоа и како да се справите со него (блокирање/пријавување функции, одржување на приватноста). Ако сте граѓанска организација за животна средина, можете да истакнете како се шират лажни информации на интернет и основните практики за верификација – тема поврзана со безбедноста (интегритет на информациите).

Со информирање на јавноста, граѓанските организации извршуваат двојна услуга: ги заштитуваат своите избирачи и ја зајакнуваат сопствената безбедност преку подигнување на целокупната безбедносна „хигиена“ на средината во која работат. Создаваат доблесен циклус каде што свесната заедница е помалку веројатно да биде вектор или жртва на сајбер инциденти.

Накратко, знаењето е моќ, а граѓанските организации, како доверливи субјекти во заедницата, се во добра позиција да ја шират таа моќ широко.

Локални и меѓународни ресурси за поддршка

Покрај соработката меѓу врсниците и јавната свест, постојат формални ресурси за поддршка достапни за граѓанските организации на локално, регионално и меѓународно ниво. Познавањето што се тие и како да им пристапите може да обезбеди многу потребна помош, особено кога се соочувате со софистицирани закани или ви се потребни ресурси надвор од вашите можности.

Локални ресурси:

- **Национални агенции за сајбер безбедност/CERT-ови:** Како што споменавме претходно, многу земји имаат национален CERT (тим за одговор во итни случаи во компјутери) или агенција за сајбер безбедност која нуди насоки. Некои имаат програми фокусирани на граѓански организации или мали бизниси. На пример, Националниот центар за сајбер безбедност (NCSC) на Велика Британија обезбедува бесплатни насоки, па дури и некои бесплатни услуги (како веб-проверка, проверка на пошта) за подобрување на безбедноста за организациите. Проверете дали CERT на вашата земја има теренска работа или ресурси на вашиот јазик (тие често објавуваат билтени за предупредување кои можете да ги следите).
- **Оддели за спроведување на законот за сајбер криминал:** Доколку се соочите со проблеми како што се онлајн измама, вознемирување или подложност на напад, локалните полициски сајбер единици би можеле да ви помогнат. Некои земји имаат специјални единици кои работат со граѓанското општество (особено во контекст на заштита на новинари или активисти). Изградете однос доколку е можно – можеби поканете службеник да зборува на форум на граѓански организации за пријавување сајбер инциденти, за да го демистифицирате процесот.
- **Академски институции:** Локалните универзитети, особено оние со оддели за ИТ или сајбер безбедност, можат да бидат сојузници. Професорите или студентите би можеле да се зафатат со безбедноста на граѓанските организации како дел од истражувачки или волонтерски проекти. На пример, универзитетски ИТ клуб би можел да направи безбедносна ревизија за вашиот граѓански организации како проект на час (со ваша согласност и под надзор). Некои универзитети водат клиники за сајбер безбедност или имаат инкубатори за решенија за социјална технологија.
- **Локални канцеларии на технолошки компании:** Големите технолошки компании често имаат програми за локално присуство и корпоративна општествена одговорност (CSR). Тие понекогаш организираат работилници за дигитална писменост или безбедност (обука за безбедност на интернет на Google, кампањата за дигитална писменост на Meta итн.). Обраќајте им се за да ги вклучите вработените или корисниците на вашата граѓанска организација во тие бесплатни обуки. Тие, исто така, можат да донираат или да дадат попуст на безбедносни производи. На пример, Cisco дониреше хардвер за заштитен sид на некои непрофитни организации преку партнерства.
- **Организации за поддршка на граѓанските организации:** Субјекти како што се технолошки федерации или здруженија (на пр. TechSoup – глобална граѓанска организација која нуди софтвер со попуст, вклучувајќи безбедносни пакети; во Европа, можеби постои Европската мрежа за безбедност на граѓанското општество, итн.). TechSoup, поточно, нуди не само софтвер, туку и ресурси за градење капацитети, а

понекогаш и вебинари за безбедност. Националните мрежи на граѓанска организација може да имаат и работни групи за ИКТ, каде што можете да добиете совети.

Меѓународни ресурси:

- **Телефонска линија за помош за дигитална безбедност на Access Now:** Веќе споменавме дека тоа е глобално достапен тим за брза реакција, 24/7 за граѓанското општество. Тие работат на повеќе јазици (24/7 на англиски, шпански, француски и други јазици). Тие можат да помогнат со сè, од упатства за отстранување на малициозен софтвер до ублажување на DDoS напади до враќање на сметки. Бесплатно е и доверливо.
- **Институтот за сајбер мир:** Оваа организација не само што анализира сајбер напади врз граѓанското општество, туку и координира помош. Нивната програма CyberPeace Builders има волонтери од технолошки компании кои нудат про-боно помош на граѓански организации ширум светот. Можете да аплицирате за да бидете корисник на нивната програма, која би можела да ви обезбеди постојана експертиза, како што е помош за поставување безбедна инфраструктура или политики.
- **Меѓународни организации за слобода на изразување/дигитални права:** Групи како Front Line Defenders, The Engine Room, EFF (Electronic Frontier Foundation) и други често објавуваат водичи или можат да ве поврзат со експерти. На пример, Front Line Defenders има програма „Дигитална заштита“ и комплет алатки „Безбедност во кутија“ прилагоден за бранителите на човекови права (со алатки и тактики).
- **Програми финансирани од донатори:** Понекогаш постојат проекти финансирани од донатори, специјално за зголемување на отпорноста на граѓанските организации на сајбер напади. На пример, во ЕУ, имало проекти во рамките на Еразмус+ или ЦЕФ фокусирани на подобрување на дигиталните вештини, вклучително и безбедноста за непрофитните организации (како можеби проектот КА220 во вашиот наслов е еден од нив). Внимавајте на повиците или мрежите во рамките на ваквите проекти; тие често произведуваат комплети алатки, организираат обуки или нудат консултации за граѓанските организации учеснички.
- **Форуми и конференции:** На меѓународно ниво, конференциите како RightsCon, Форумот за управување со интернет (IGF) или регионалните конференции за сајбер безбедност понекогаш имаат траги од граѓанското општество. Учеството може да ве поврзе со глобална заедница и ресурси. RightsCon, особено, е посветен на дигиталните права и безбедноста на активистите. Многу сесии даваат практични совети или водат до финансиери кои би можеле да ги поддржат вашите подобрувања во безбедноста.
- **Можности за финансирање:** Меѓународните фондации ја препознаа сајбер-безбедноста како критичен капацитет за граѓанското општество. На пример, Фондацијата Форд и Фондот за отворена технологија доделија средства за иницијативи за сајбер-безбедност на граѓанските организации. ЕУ има линии за финансирање во рамките на програми како Хоризонт или Дигитална Европа кои би можеле да поддржат градење капацитети ако станете партнери или аплицирате. Доколку ви се потребни сериозни надградби (како што е вработување персонал за ИТ-безбедност или реновирање на ИТ-инфраструктурата), размислете за интегрирање на тоа во предлозите за грантови за основна поддршка. Образложете го како неопходно ублажување на ризикот – многу донатори сега се посвесни и би можеле да го одобрат буџетот за тоа.

Јазична и културна релевантност: Кога барате помош, обидете се да ја најдете на вашиот јазик или контекст, доколку е можно. Глобалните ресурси се одлични, но може да бидат на англиски јазик или премногу општи. Затоа се важни локалните експерти и преведувањето на меѓународни водичи на локалните јазици. Ако, да речеме, вашата граѓанска организација е во Турција (ја гледам временската зона во Истанбул во пораката), користењето локален турски ресурс (како што е турско советување од CERT или обука за дигитална безбедност на турски) може да биде поедноставно за персоналот. Ако не можете да најдете некој ресурс на вашиот јазик, можеби волонтирајте да преведете релевантен водич – тоа само по себе е придонес на заедницата.

Технолошки донации: Во врска со поддршката, забележете и работи како што се Google for Nonprofits што нуди бесплатен G Suite, Microsoft for Nonprofits нуди бесплатни лиценци O365, Okta нуди бесплатни решенија за еднократно најавување, а некои добавувачи на безбедност имаат програми за донации за непрофитни организации (на пр. намали трошковните бариери за користење на врвни алатки за безбедност.

Бидете во тек: Пределот на закани еволуира. Стекнете навика да следите некои вести за безбедноста или да се придружите на мејлинг листи (некои се креирани за граѓански организации). На пример, мејлинг листата за сајбер безбедност на CIVICUS (доколку постои) или едноставно да следите веродостојни извори на социјалните медиуми (на пр. @enisa_eu на Твитер за вести од ЕУ или блогови на локални фирми за сајбер безбедност).

Накратко, не сте сами. Постои мрежа на поддршка од локална до глобална. Проактивното поврзување со овие ресурси во мирни времиња (не само за време на криза) е вредно. Воспоставете односи со клучни контакти (знајте кого би повикале во 22 часот ако нешто тргне наопаку). И подеднакво, кога ќе стекнете знаење или ресурси, придонесете назад кон овие мрежи – тоа е она што ги одржува стабилни и достапни за следната граѓанска организација на која ќе ѝ биде потребна.

Со искористување на соработката (дел 6.1, 6.2), едуцирање на јавноста (6.3) и контактирање со системи за поддршка (6.4), граѓанските организации можат да ја трансформираат дигиталната безбедност од застрашувачка соло битка во напор поддржан од заедницата. Во следното поглавје, ќе разгледаме конкретни примери и вообичаени стапици за дополнително учење од искуството од реалниот свет.

Резиме на поглавјето

Поглавје 6 обезбедува рамки за граѓанските организации (ГО) проактивно да идентификуваат ризици и да се подготват за сајбер инциденти. Ги води организациите да ги проценат критичните средства (на пр. бази на податоци на донатори) и ранливостите, користејќи едноставни шаблони за проценка на ризик за да ги приоритетизираат заканите како што се фишинг или рансомвер. Поглавјето опишува креирање план за одговор на инциденти, детално опишувајќи ги чекорите за откривање, ограничување, комуникација и закрепнување. На пример, ГО со план за одговор може брзо да ги врати податоците по напад со рансомвер, минимизирајќи ја штетата. Нагласува документирање на инцидентите за да се учи од нив и ажурирање на плановите годишно. Поглавјето се осврнува на правилото за известување за прекршување на GDPR во рок од 72 часа, обезбедувајќи

усогласеност. Практичните чекори вклучуваат доделување улоги (на пр. службеник за заштита на податоци) и тестирање на планови преку вежби на маса. Фокусот на поглавјето на подготовката им помага на ГО брзо да закрепнат, намалувајќи ја оперативната штета и штетата врз репутацијата. Со нудење јасни, нискобуџетни рамки, им овозможува на нетехничкиот персонал да придонесе за отпорност, усогласувајќи се со мисијата на е-книгата да ја направи сајбер безбедноста остварлива за организациите со ограничени ресурси.

Шаблон за политика за заштита на податоци за граѓански организации

Име на организација: [Внесете име на ГО] Датум на стапување во сила: [Внесете датум]
Последно ажурирање: [Внесете датум или „Н/А за почетна политика“]

Оваа Политика за заштита на податоци опишува како [Име на ГО] собира, складира, пристапува до и ги заштитува личните податоци за да обезбеди приватност, безбедност и усогласеност со важечките закони (на пр. GDPR, [Вметнете локален закон за заштита на податоци]). Се однесува на сите вработени, волонтери и партнери кои ракуваат со лични податоци, заштитувајќи ја довербата на нашите корисници, донатори и засегнати страни.

Оваа политика ги опфаќа сите лични податоци (на пр. имиња, контакт информации, здравствени или финансиски информации) управувани од [Име на граѓанска организација], вклучувајќи податоци поврзани со корисниците, донаторите, персоналот и волонтерите.

1. Собирање податоци

Ги собираме само личните податоци потребни за нашата мисија и програми, добивајќи информирана согласност каде што е потребно. Податоците се собираат законски, транспарентно и за специфични цели.

Процедури:

- ⇒ Јасно објаснете зошто се собираат податоци и како ќе се користат пред собирањето (на пр. преку формулари за согласност или известувања за приватност).
- ⇒ Соберете минимални податоци за да ја постигнете целта (принцип на минимизирање на податоците).
- ⇒ Документирајте ја целта на собирањето и добијте согласност каде што е применливо (на пр. потпишани формулари, полиња за избор преку интернет).

2. Складирање на податоци

Ги чуваме личните податоци безбедно, користејќи енкрипција и заштитени системи, за да спречиме неовластен пристап, губење или кражба.

Процедури:

- ⇒ Складирајте податоци на безбедни платформи (на пр. шифрирани cloud услуги како Google Drive со 2FA или заклучени физички датотеки).

⇒ Шифрирајте чувствителни податоци во мирување (на пр. на лаптопи, надворешни дискови) и во пренос (на пр. користејќи HTTPS или безбедна е-пошта).

⇒ Одржувајте редовни резервни копии (на пр. неделно на безбеден облак или надворешен диск) за да се обезбеди обновување на податоците.

⇒ Безбедно отстранете ги податоците кога повеќе не ви се потребни (на пр. уништувајте хартиени записи, користете алатки за безбедно бришење на дигитални датотеки).

3. Контрола на пристап

Пристапот до лични податоци е ограничен на овластен персонал на кој му се потребни за својата улога, следејќи го принципот на најмали привилегии.

Процедури:

⇒ Доделете пристап врз основа на работни улоги (на пр. само менаџерите на програми имаат пристап до податоците за корисниците).

⇒ Користете силни лозинки и двофакторска автентикација (2FA) за сите сметки со пристап до лични податоци.

⇒ Редовно проверувајте ги дозволите за пристап (на пр. месечно) за да го отстраните пристапот за поранешни вработени или волонтери.

⇒ Обучете го персоналот и волонтерите за безбедно ракување со податоци (на пр. не споделување лозинки, одјавување по употреба).

4. Пријавување на прекршување

Брзо откриваме, реагираме и пријавуваме прекршувања на податоците за да ја минимизираме штетата и да се усогласиме со законските обврски (на пр. правилото за известување од 72 часа на GDPR).

Процедури:

⇒ Назначете службеник за заштита на податоци или лице за контакт (на пр. [Внесете име/улога]) за справување со прекршувања.

⇒ Пријавете ги сомнителните прекршувања веднаш до назначеното лице (на пр. преку е-пошта до [Вметни е-пошта]).

⇒ Известете го надлежниот орган за заштита на податоци (на пр. [Внесете име на локалната самоуправа]) во рок од 72 часа доколку прекршувањето на безбедноста претставува ризик за штета на поединци.

⇒ Доколку е потребно, информирајте ги засегнатите лица (на пр. корисници, донатори), давајќи јасни упатства за следните чекори.

⇒ Документирајте ги сите прекршувања и одговори за да се подобри идната превенција (на пр. ажурирајте ја проценката на ризикот).

5. Одговорности

Лидерство: Одобрување и финансирање на спроведувањето на политиката (на пр. буџет за обука, алатки).
Персонал и волонтери: Следете ја оваа политика, пријавете ги проблемите навремено и посетувајте обука за заштита на податоци.
Службеник/лице за заштита на податоци: Надгледува усогласеност со политиките, управува со прекршувања и координира годишни прегледи.

6. Усогласеност и преглед

Усогласеност: Оваа политика е усогласена со GDPR и [Вметнете го локалниот закон за заштита на податоци]. Непочитувањето може да резултира со дисциплински мерки или законски казни.
Прегледувајте ја и ажурирајте ја оваа политика годишно или по значајни промени (на пр. нови програми, регулативи). Следен преглед: [Вметнете датум, на пр. ноември 2026 година].
Сите вработени и волонтери добиваат обука за заштита на податоци при вработувањата и годишно.

Контакт

За прашања или за пријавување на прекршок, контактирајте: [Внесете име на службеник за заштита на податоци/лице за контакт, е-пошта, телефон].
Локален орган за заштита на податоци: [Внесете име и контакт информации, на пр. „Турски орган за заштита на лични податоци (KVKK), [контакт информации]“.

Одобрено од: [Внесете име/улога на раководителот, на пр. извршен директор]
Датум: [Вметни датум]
Забелешки за прилагодување: Заменете ги резервираните места (на пр. [Име на ГО], [Локален закон за заштита на податоци]) со деталите на вашата организација. Додадете локални барања за усогласеност или специфични алатки по потреба.

2.7 ПОГЛАВЈЕ 7: УСПЕСИ ВО БЕЗБЕДНОСТА ВО ГО

Вистински приказни: Безбедносни успеси во граѓанските организации

Охрабрувачки е да се научи како организациите од слични групи ги надминаа безбедносните предизвици. Еве неколку анонимизирани, но реални сценарија кои покажуваат позитивни резултати благодарение на добрите безбедносни практики:

Обид за фишинг спречен од обука: Организација за човекови права во Источна Европа добила е-пошта што личела на споделување на Google Docs од колега. Бидејќи персоналот поминал обука за подигање на свеста за фишинг, еден член на тимот забележал дека нешто не е во ред (е-поштата на испраќачот била малку погрешно напишана) и не кликнал на линкот. Наместо тоа, таа го известила лицето за контакт со ИТ. Тие потврдиле дека станува збор за обид за кражба на акредитиви. Како резултат на тоа, ниедна сметка не била компромитирана. Ова ја зајакнало вредноста на обуката – директорката на организацијата на следниот состанок на персоналот истакнала како претпазливоста на тој вработен ги заштитила сите, претворајќи го во момент за учење. Беше успех во тоа што нападот бил спречен без никаква штета, благодарение на внимателен член на персоналот.

Нападот со Ransomware преживеа благодарение на резервните копии: Средна здравствена организација во Африка беше погодена од ransomware едно утро – персоналот ги пронајде своите датотеки шифрирани и порака за откуп на нивните екрани. На почетокот беше хаос. Сепак, организацијата имаше робустен систем за резервни копии: сите критични податоци беа резервни копии на надворешен сервер секоја вечер. За неколку часа, нивниот ИТ консултант ги изолираше заразените машини, ги избриша, повторно го инсталираше софтверот и ги врати податоците од резервната копија од претходната ноќ. Тие изгубија најмногу еден ден работа на неколку документи. Тие не ја платија откупнината и го пријавија инцидентот. Ова искуство се претвори во приказна за успех во безбедноста што ја споделуваат – нивната инвестиција во планирањето за резервни копии и обновување се исплати, докажувајќи колку е важно. Подоцна, тие дури го презентираа овој случај на вебинар, охрабрувајќи ги другите организации да имплементираат резервни копии офлајн.

Безбедна комуникација Заштитени чувствителни планови: Коалиција за застапување организираше кампања во земја со силен надзор. Тие се сомневаа дека нивните комуникации се следат. Под водство на консултант за дигитална безбедност, тие се префрлија на користење енкриптирани пораки од крај до крај (Signal) и е-пошта со PGP за најчувствителните прилози. За време на кампањата, тие забележаа обиди од страна на противниците да ја предвидат нивната стратегија, но критичните детали никогаш не беа протечени. Анализата по кампањата покажа дека откако преминаа на безбедни комуникации, опозицијата ја изгуби својата предност во „внатрешното знаење“. Коалицијата им ја припишува заслугата на безбедните алатки за заштита на нивните планови и придонес кон успехот на кампањата. Тоа ја зацврсти нивната посветеност да користат енкриптирани канали за идните операции и послужи како пример за другите во нивната мрежа.

Кражба на сметка со двофакторска автентикација: Една граѓанска организација за права на жените во Јужна Азија беше цел на е-пошта за фишинг на Gmail сметка на еден од нејзините вработени. Вработената случајно ја внела својата лозинка на

лажна страница за најавување на Google. Таа лозинка му припаднала на напаѓачот. Кратко потоа, напаѓачот од друга земја се обидел да се најави на нејзината Google сметка – но бидејќи граѓанската организација спровела двофакторска автентикација на сите сметки, најавувањето побарало код за верификација од нејзиниот телефон. Напаѓачот го немал, па бил запрен. Google го предупредил корисникот за блокиран обид за најавување. Таа веднаш сфатила што се случило, го пријавила и ја сменила лозинката. На крајот, 2FA го претворила она што можело да биде сериозен упад во обичен страв без никаква штета. Овој вистински инцидент навистина им покажал на целиот тим зошто тие донекаде досадни барања на 2FA вределе. Тоа беше ден на олеснување и победа за нивните безбедносни мерки.

Соработката во заедницата го запре DDoS: Мрежа на граѓански организации за животна средина започна кампања што предизвика гнев кај некои противници, кои потоа започнаа напад со дистрибуирано одбивање на услуга (DDoS) на заедничката веб-страница на мрежата (преплавувајќи ја со сообраќај за да ја исклучат). Поединечно, граѓанските организации имаа ограничени ИТ ресурси за да го ублажат ова. Сепак, преку канал за технолошка солидарност, еден лидер на граѓански организации брзо побара помош. Партнерска организација во технолошка компанија организираше привремено користење на нивната услуга за заштита од DDoS (Cloudflare), а ИТ персоналот на друга граѓански организација помогна во пренасочувањето на страницата низ таа заштита. За неколку часа, веб-страницата повторно беше активна и покрај тоа што се соочи со напад, а кампањата продолжи. Овој колаборативен одговор беше приказна за успех што илустрираше како поддршката од сојузниците може да се спротивстави дури и на големи сајбер закани. Исто така, ги научи да постават секогаш вклучена заштита од Cloudflare потоа. Подоцна го напишаа овој случај во блог за да им се заблагодарат на оние што помогнаа и да ги водат другите во справувањето со DDoS.

Овие приказни покажуваат дека дури и кога граѓанските организации се цел на сајбер закани, подготвеноста и брзата акција можат да доведат до успешна одбрана или брзо закрепнување. Заедничките нишки вклучуваат: претходни инвестиции во безбедносни мерки (обука, резервни копии, 2FA), брзо препознавање и одговор и искористување на мрежите за поддршка. Со споделување и проучување на ваквите успеси, граѓанските организации можат да научат што навистина функционира и да стекнат доверба дека и тие можат да се справат со слични ситуации.

Чести грешки и како да ги спречите

Учењето од грешките на другите (или од нашите сопствени) е клучно за подобрување на безбедноста. Еве некои чести стапици со кои се соочуваат граѓанските организации, заедно со стратегии за нивно избегнување:

Користење слаби или стандардни лозинки: Можеби најраспространетата грешка е држењето до лесни лозинки (како „123456“, „password“) или оставањето на стандардните лозинки непроменети на уредите (на пр. рутерите често доаѓаат со „admin/admin“). Ова е подарок за напаѓачите. Превенција: Воспоставете политика за лозинки што бара силни, уникатни лозинки и користете менаџери за лозинки за да ги ракувате. За време на обуката, покажете примери на лоши наспроти добри лозинки. И секогаш кога поставувате нов хардвер/софтвер, веднаш променете ги стандардните акредитиви (и документирајте ги безбедно). Спроведувајте повремени ревизии – користете алатка или скрипта за да

проверите дали некои сметки имаат слаби лозинки (некои организации користат бази на податоци за пробивање или алатки за ревизија). Нагласете 2FA за да компензирате за секоја слаба лозинка што се провлекува.

Кликнување пред размислување (успех во фишинг): Многу прекршувања на безбедноста започнуваат со кликнување на злонамерен линк или прилог без проверка. Грешката е дејствување врз основа на импулс од е-пошта или порака (особено оние што повикуваат на итност или љубопитност), наместо проверка на автентичноста. Превенција: Обука, обука, обука. Спроведувајте симулирани фишинг тестови за да идентификувате кому му е потребна повеќе пракса. Поттикнете култура каде што е во ред да се забави темпото и да се потврдат барањата – на пр. „Ако е-поштата изгледа итна и бара пари или акредитиви, во ред е (всушност се охрабрува) да се провери уште еднаш со повик или посебна е-пошта“. Обезбедете едноставни контролни листи: внимателно проверете ја адресата на испраќачот, побарајте правописни грешки, не преземајте неочекувани прилози итн. Дополнително, техничките одбрани како добри филтри за спам и скенирање линкови помагаат да се филтрира очигледната измама.

***Неуспешнонавремено ажурирање на софтверот*:** Чест сценарио: веб-страница на CSO работи на WordPress, но не ги ажурирала додатоците една година, а напаѓачот експлоатира позната маана за да ја оштети. Или персоналните компјутери сè уште работат со постари верзии на оперативниот систем со незакрпени ранливости. Грешката е одложување или игнорирање на ажурирањата (понекогаш од страв дека може да се расипе нешто, понекогаш само заборавање). Превенција: Овозможете автоматски ажурирања каде што е можно. За системи што не можат автоматски да се ажурираат, доделете некому задача да проверува месечно. Користете алатки што ги собираат потребите за ажурирање (дури и едноставно вклучување на известувања „Провери за ажурирања“). За веб-страници, размислете за управувано хостирање што ги обработува ажурирањата или претплатете се на мејлинг листи за безбедност на додатоци. Нагласете го „вторник на закрпи“ или некоја рутина. Доколку ресурсите дозволуваат, водете инвентар на критичен софтвер и следете го нивниот статус на закрпи (постојат бесплатни скенери што ги истакнуваат недостасувачките закрпи). Исто така, разбијте ги митовите како „ажурирањата го забавуваат мојот компјутер“ со тоа што ќе ги покажете безбедносните ризици од неажурирање.

Не се прави резервна копија (или не се тестираат резервните копии): Некои организации ја сфаќаат важноста на резервните копии дури по губењето податоци. Грешките вклучуваат воопшто да не се прави резервна копија или да се имаат резервни копии, но да не се тестираат (потоа откривајќи дека се нецелосни или оштетени кога е потребно). Превенција: Имплементирајте стратегија за резервни копии 3-2-1 (повеќе копии, различни медиуми, една надвор од локацијата). Закажете резервни копии и автоматизирајте ги. Уште поважно, редовно извршувајте тест-врати. Едноставна вежба: случајно изберете датотека и обидете се да ја вратите од резервна копија за да се осигурите дека процесот функционира. Исто така, осигурете се дека самите резервни копии се заштитени (шифрирани и недостапни за нормална мрежа, за да не може да ги погоди ransomware). Многумина научиле на тешкиот начин дека резервната копија на мрежен диск достапен за сите не е безбедна од малициозен софтвер за енкрипција. Решенија: офлајн резервните копии или барем версионираните резервни копии во облак се имуни на енкрипција.

Сметки со прекумерни привилегии и споделени сметки: Грешка: давање администраторски права на сите корисници „затоа што е полесно“ или споделување на едно најавување меѓу неколку луѓе за погодност. Ова може да доведе до големи проблеми – едно лице може ненамерно да инсталира малициозен софтвер со администраторски права или, пак, вработен што си заминал сè уште ја знае лозинката за споделената сметка. И одговорноста се губи кога сметките се споделени (не можете да кажете кој што направил). Превенција: Применете го принципот на најмали привилегии. Креирајте индивидуални сметки за сите и дајте им само пристап што им е потребен. Користете дозволи базирани на улоги за датотеки и системи. Да, тоа е малку повеќе почетно поставување, но модерните системи го олеснуваат управувањето со корисниците. Исто така, имајте јасна листа за проверка за вклучување/исклучување, така што пристапот ќе се одобрува и одзема систематски. За администраторски задачи, имајте посебна администраторска сметка – не пребарувајте на интернет или не читајте е-пошта како администраторски корисник. На тој начин, дури и ако корисникот е измамен, штетата може да биде ограничена на неговото корисничко ниво.

Игнорирање на безбедносните предупредувања или најдобрите практики: Луѓето понекогаш ги игнорираат тие предупредувања од прелистувачот („Сертификатот на оваа страница не е доверлив“) или ги оневозможуваат безбедносните функции затоа што изгледаат досадни („дозволете ми да го исклучам заштитниот sid за да работи оваа апликација“). Тоа може да отвори врати за напад. Друг пример: користење застарени, небезбедни протоколи од навика (како FTP наместо SFTP). Превенција: Едуцирајте зошто постојат предупредувања. На пример, објаснете што значи предупредување за сертификат и дека може да укажува на лажна страница или прислушување. Создадете средина каде што ако некоја безбедносна мерка блокира нешто, наместо да ја оневозможите, персоналот бара соодветни решенија (како додавање исклучок ако е позната безбедна внатрешна страница, итн.). Дајте насоки: ако антивирусот означи датотека, не ја ставајте само на белата листа од фрустрација – контактирајте го ИТ одделот за да анализирате дали е навистина безбедна. Напишете едноставни внатрешни ЧПП: „Ако видите безбедносно предупредување, направете X“. Исто така, кога поставувате нови алатки, направете го тоа безбедно од самиот почеток за персоналот да не биде во искушение да користи небезбедни заобиколувања.

Недостаток на план за одговор на инциденти: Многу граѓански организации се фатени со рамни нозе за време на инцидент – не знаат кого да повикаат или какви чекори да преземат, што троши драгоцено време. Грешка: нема однапред дефиниран план за инциденти или вежби. Превенција: Развијте основен план за одговор на инциденти (како што е направено во Поглавје 5) и осигурете се дека сите ги знаат основите. Можеби е само една страница: „Ако се случи нешто чудно: исклучете се од интернет, јавете се на ова лице итн“. Исто така, направете барем една вежба на маса: разговарајте за хипотетичко „Што ако нè погоди ransomware, што би направиле?“ за да ги забележите празнините. Поседувањето план ги намалува грешките за време на реални кризи, како што е исклучување на погрешен систем или паника.

Со тоа што се свесни за овие вообичаени грешки, ГО може да преземе проактивни мерки за да избегне паѓање во тие стапици. Честопати малите промени во однесувањето или политиката прават голема разлика – како навиката за примена на ажурирања или

двојно проверување пред кликнување. Поттикнете филозофија дека „секој е засегнат во безбедноста“, така што грешките можат да се откријат или да се спречат со колективна внимателност (на пр. рецензија од колеги на сомнителни е-пораки - „Еј колега, дали ова ти изгледа легитимно?“ може да спречи грешка).

Накратко: зајакнете ги слабите лозинки, размислете пред да кликнете, ажурирајте сè, внимателно направете резервна копија, ограничете ги привилегиите, обрнете внимание на предупредувањата и подгответе се за најлошото. Избегнувањето на овие вообичаени грешки драматично ќе ја подобри вашата безбедносна позиција со релативно мали трошоци.

Тестирајте ја сопствената безбедност: Едноставни вежби

Едно е да читате за безбедноста, а друго е да ја примените во пракса. Еве неколку едноставни самопроценки и вежби што вие (и вашиот тим) можете да ги направите за да ја процените и подобрите вашата подготвеност за безбедност. Сфатете ги како „безбедносни вежби“ или проверки:

Вежба за фишинг: Напишете безопасна „лажна фишинг е-порака“ за да ја тестирате свеста во вашиот тим. На пример, испратете е-порака од адреса што не е од организацијата, но користете го името на вашата организација во екранот, со наслов како „Потребно е итно ажурирање“ и линк до Google формулар (кој само вели „Честитки, ова беше тест!“). Видете кој кликнува или испраќа информации. Целта е едукативна, а не да се фати некој: потоа, откријте го и дискутирајте за индициите дека станува збор за фишинг (можеби мала разлика во адресата, итен тон, итн.). Ако малкумина наседнале на тоа, одлично – ако некои наседнале, искористете го како нежна можност за обука. Алтернативно, користете бесплатни алатки како што се квизот за фишинг на Google или алатките за симулација на фишинг (некои AV пакети ја имаат оваа функција) на контролиран начин.

Проверка на јачината на лозинката: Погледнете некои лозинки (без да побарате од некого да ги открие своите, можете да симулирате вообичаени шеми). Користете мерач на јачина на лозинки (има многу на интернет, на пр. Passwordmeter.com) за да тестирате примерок од типични лозинки наспроти препорачаните. Ако користите менаџер за лозинки подобро проверете дали пријавува слаби/повторно користени лозинки – многу од нив имаат функција за безбедносна ревизија. Како вежба, секој нека креира силна лозинка од четири случајни зборови (на пр. „јаболко караван тигар танц“) и тестирајте ја нејзината јачина наспроти нешто како „Winter2020!“ – резултатите често покажуваат дека лозинката е посилна и полесна за запомнување. Ова ги зајакнува добрите навики за креирање лозинки.

Вежба за враќање на резервна копија: Тестирајте ја вашата резервна копија. Симулирајте сценарио: „Ја изгубивме датотеката X, што да правиме?“ Всушност, одете до вашата локација за резервна копија, преземете ја датотеката и отворете ја за да се осигурите дека е недопрена. Или изберете датум и преправајте се дека мора да вратите сè како што било тогаш – можете ли да ја преземете резервната копија од тој датум? Пресметајте колку време е потребно за да се врати репрезентативен сет на податоци. Ова не само што ги потврдува резервните копии, туку ве подготвува и за вистински инциденти со тоа што открива дали упатствата/акредитациите за резервни копии се лесно достапни.

Можеби доделете некој друг (не вообичаеното ИТ лице) да го проба враќањето користејќи само документирани чекори за да видите дали процесот е доволно јасен.

Ревизија на безбедноста на уредот: Направете брза ревизија на вашите канцелариски компјутери и телефони (секако, со дозвола). Проверете: Дали сите оперативни системи се ажурирани (отворете Windows Update или еквивалент, видете го датумот на последното ажурирање)? Дали антивирусот работи и е ажуриран? Дали се вклучени firewall-овите? Дали некои уреди сè уште користат стандардни лозинки (на пр. најавете се на канцелариското рутер и проверете дали стандардните кредити работат – ако да, големо знаменце за да ги промените)? Проверете дали екраните се заклучуваат автоматски кога сте во мирување. Можете да направите едноставна листа за проверка и да го оцените секој компјутер. Потоа поправете ги сите пронајдени проблеми и прославете ако повеќето работи биле безбедни по стандард (тоа ги потврдува вашите практики за конфигурација).

Тест за лажна е-пошта: Интересна вежба: покажете колку лесно може да се лажираат е-пораки, за да се покрене скептицизам. Користејќи контролирана средина (како услуга што овозможува испраќање е-пораки од прилагодена адреса што ја поседувате, или дури и само менување на името „Од“ во Gmail), испратете си е-пошта што изгледа како да е од, да речеме, „“ (но доаѓа од друг домен). Покажете им на вработените како, на прв поглед, изгледа убедливо, но заглавијата на е-поштата или вистинската адреса ја покажуваат вистината. Оваа вежба често ги шокира луѓето, а потоа тие повнимателно ги проверуваат е-адресите.

Чистење на дозволи: Земете една споделена папка или Google Drive и проверете кој има пристап. Можеби ќе откриете дека поранешните волонтери сè уште имале пристап или дека некои датотеки ненамерно биле јавно споделени преку линк. Како „мини вежба“, одземете го секој непотребен пристап и документирајте го. Тоа е како пролетно чистење за права за пристап. Ова служи како потсетник периодично да го правите ова.

Играње улоги со инциденти: Изберете сценарио (како „лаптоп украден од кафуле“ или „ransomware на сервер“) и усно објаснете како би реагирале (кого да повикате, какви чекори да преземете). Играње улоги со персоналот: еден го игра корисникот што паничи, друг ИТ одговорникот итн. Оваа воздржана вежба може да укаже на празнини („О, всушност го немаме бројот на банката при рака за да се јавиме и да замрзнеме сметки ако е-поштата е компромитирана“ или „Сфаќаме дека не ја знаеме администраторската лозинка на нашата веб-страница на памет ако LastPass е недостапен“). Подобро е да се открие сега отколку за време на вистинска криза.

Секоја вежба е замислена да биде едноставна и да не одзема многу време, но многу проникliва. Замислете го како вежба за противпожарна заштита од сајбер закани – вежбате во средина со низок ризик, така што во вистинска вонредна состојба знаете што да правите и се чувствувате помалку вознемирено бидејќи сте направиле нешто слично и претходно.

По секоја вежба, отворено дискутирајте за резултатите без обвинување. Ако нешто тргнало наопаку (на пр. половина од тимот не го поминала тестот за фишинг), третирајте го како колективно учење: можеби фишинг е-поштата била навистина подмолна – сега сите знаат дека следниот пат треба да бидат претпазливи со тој трик. Ако вежбата открие

сериозна слабост, заблагодарете му се на процесот што ја открил и посветете се да ја поправите.

Редовното изведување на вакви вежби ја одржува безбедноста во умовите на луѓето и поттикнува култура на континуирано подобрување. Тоа ја демистифицира безбедноста (затоа што активно правите работи, а не само слушате политики). Дури може да биде и забавно на некој начин – некои организации го гејмизираат, нудејќи мали награди за оние што ќе забележат фишинг или ќе имаат најмалку проблеми при ревизиите.

Интегрирање на дигиталната безбедност во секојдневната рутина

Крајната цел е добрите безбедносни практики да станат втора природа – само нормален дел од тоа како вие и вашата организација работите. Еве совети за беспрекорно вплетување на дигиталната безбедност во секојдневниот живот во организацијата:

Започнете го денот имајќи ја предвид безбедноста: Поттикнувајте едноставни утрински навики. На пример, кога ќе го стартувате компјутерот, прво дозволете му да инсталира ажурирања пред да се фрлите на работа (земете кафе додека се ажурира наместо да притиснете „одложи“). Или проверете ги сите безбедносни известувања (како „Windows Defender: не се пронајдени проблеми“ или барање за ажурирање на софтверот) и адресирајте ги рано. Ова ви гарантира дека ќе започнете со работа во безбедна состојба, наместо да ги игнорирате тие мали штитови и извичници на лентата со задачи.

Менаџер за лозинки секој ден: Направете го користењето на менаџерот за лозинки рутински дел од процесите на најавување. Доколку е правилно поставен, може автоматски да ги пополнува акредитивите – така што персоналот брзо ја гледа користа (побрзо најавување, без проблеми со ресетирање на лозинката) и едноставно станува начинот на кој се најавуваат. Дневната рутина се менува од „запомнете или запишете ги лозинките“ во „отклучете го менаџерот еднаш со силна лозинка, а потоа кликнете за да се најавите насекаде“. Со текот на времето, тие нема да го замислат животот без него. Некои менаџери, исто така, бараат да ги ажурираат слабите лозинки – можеби одвојуваат неколку минути секој петок за да ажурираат една означена лозинка. Малку по малку, сите сметки добиваат посилни лозинки.

Тимски потсетници и култура: Вклучете безбедносни информации во редовните тимски состаноци или интерните билтени. На пример, на неделен состанок, една точка на дневен ред може да биде едноминутен совет за безбедност или вести (на пр. „За ваша информација, моментално има измама преку WhatsApp; запомнете да не споделувате кодови за верификација“). Ова го нормализира разговорот. Не мора да доминира, туку само рутинска проверка. Некои граѓански организации поставуваат постер со „Совет за безбедност на месецот“ на ѕидот или на Slack каналот, што пасивно ја одржува свеста на дневен план.

Заклучување на екрани и чистење на бироа: Стекнете навика да го заклучувате компјутерот (Win+L на Windows, Ctrl+Cmd+Q на Mac) секогаш кога ќе се оддалечите – дури и за минута. Ако сите го прават тоа, се чувствува нормално, а не параноично. Истото важи и за чувањето чувствителни документи или USB-уреди настрана (старата „политика за чистење на биро“). Полесно е во рутината ако го поврзете со нешто: на пример, на крајот од денот, последното нешто: направете резервна копија на датотеките, заклучете ги сите кабинети, проверете дали сте одјавени од системите – тогаш знаете дека сте подготвени.

Можеби креирајте печатена листа за проверка за безбедно затворање на канцеларијата (дигитална и физичка) што персоналот ја следи секојдневно додека не стане втора природа.

Интегрирајте ја безбедноста во работните процеси: Без разлика какви алатки користите, користете ги нивните безбедносни функции по дифолт. Пример: ако споделувате датотека преку облак, рутински користете ја опцијата „сподели со одредени луѓе“ наместо линкот. Потребни се можеби 10 секунди повеќе за да се напише нивната е-пошта, но ако тоа стане единствениот начин луѓето да споделуваат, тоа е сосема нормално. Или закажете периодични прегледи на дозволите како дел од затворањето на проектот: на пр. кога проектот ќе заврши, дел од листата за проверка на крајот е „прегледајте и отстранете го секој надворешен пристап од папките на проектот“. На тој начин, одржувањето на безбедноста е вградено во животниот циклус на управување со проектот.

Ажурирање во вторник (или избран ден): Многу организации закажуваат кога извршуваат задачи за одржување. Можеби во вторник наутро, ИТ/овластеното лице осигурува дека оперативниот систем и апликациите се ажурирани на сите уреди, или секој корисник проверува за ажурирања на телефонот неделно. Ако е очекувано и закажано, тоа нема да се смета за прекин, туку за рутина (како наводнување на растенијата секој понеделник, ние ги ажурираме системите). Услугите во облак се ажурираат сами, но можеби месечно проверувајте ја административната конзола за какви било известувања или нови безбедносни функции за да ги овозможите (давателите често додаваат нови безбедносни поставки; добро е да одвојувате време за нивно редовно интегрирање).

Континуирано учење: Поттикнете го персоналот повремено да посетува кратки онлајн курсеви или квизови. Можеби секој посетува по еден модул од онлајн курсот за безбедност секое тримесечје (некои се интерактивни и кратки). Ако одвоите, да речеме, еден час работно време за тоа, тоа покажува организациска посветеност. Ова го одржува знаењето свежо и сигнализира дека безбедноста е дел од професионалниот развој, а не опционална обврска.

Водете со пример: Раководството треба отворено да го моделира безбедносното однесување. Ако директорот секогаш користи токен 2FA и се фали: „Ми се допаѓа колку е безбедно и лесно ова“, другите го следат. Ако раководството навлезе во измами или користи слаби практики, другите потсвесно ќе мислат дека е во ред. Затоа, интегрирајте го тоа на врвот – на пример, ако член на персоналот испраќа чувствителни податоци преку лична е-пошта, менаџерот треба нежно да го исправи: „Ве молиме користете ја нашата официјална сметка или шифрирајте ја таа датотека – така работиме тука“. Со текот на времето, групните норми се менуваат.

Автоматизација на снопот: Еден начин да се обезбеди безбедност без секојдневен човечки напор е автоматизирање. На пример, поставете ги сите компјутери автоматски да се заклучуваат по пет минути неактивност – потоа персоналот се прилагодува на тој шаблон (и можеби ќе смета дека пет минути се прекратки, па затоа проактивно се заклучуваат кога ќе излезат, наместо да бидат заклучени на средина од реченицата). Користете автоматски ажурирања, автоматски скенирања (закажете целосни AV скенирања за време на паузата за ручек неделно). Ова ја намалува зависноста од меморијата или мотивацијата – системот ја поддржува рутината. Слично на тоа, користењето решение за еднократно најавување (SSO), доколку е достапно, може да интегрира безбедност (едно

силно најавување отклучува повеќе апликации, така што корисниците секогаш се најавуваат со тој еден робустен метод, наместо да жонглираат со послабите).

Наградете и зајакнете: Позитивното засилување помага во навиките. Размислете за мали награди или признанија за добро безбедносно однесување. Пример: „Безбедносна ѕвезда на месецот“ за некој што пријавил фишинг е-пошта или смислил идеја за подобрување на безбедноста. Дури и само јавна пофалба, „Благодарение на Алис што ја забележа необичната е-пошта – големо внимание на деталите!“, ги охрабрува сите да бидат внимателни. Тоа покажува дека внимателноста кон безбедноста се цени, а не само се очекува.

Со вградување на овие практики во секојдневните работни процеси, дигиталната безбедност престанува да биде спорадичен проект и станува дел од организациската култура. Новиот персонал ќе ја апсорбира од првиот ден затоа што „вака работиме тука“. Тоа ја демистифицира безбедноста – не е нешто посебно технолошко, туку дел од рутинските работни обврски на секого, слично како заклучување на вратата од канцеларијата или носење лична значка. Со текот на времето, овие мали дневни навики речиси невидливо градат силна тврдина. Можеби дури и не сфаќате колку сте станале безбедни затоа што се чувствува рутински и лесно. Тоа е целта: безбедноста не како товар, туку како интегриран аспект на работењето попаметно и побезбедно секој ден.

Резиме на поглавјето

Ова поглавје истражува како граѓанските организации можат да ја искористат соработката и надворешните ресурси за подобрување на дигиталната безбедност. Нагласува дека ниедна организација не се соочува сама со сајбер закани, застапувајќи се за споделено знаење и мрежи. Поглавјето ги истакнува бесплатните или алатките управувани од заедницата, како што се Google Workspace за граѓански организации или телефонските линии за помош за дигитална безбедност, за справување со буџетските ограничувања. Го охрабрува приклучувањето кон безбедносните форуми и коалиции за споделување информации за закани и успешни приказни. Примерите вклучуваат партнерство на граѓански организации со технолошки волонтери за обезбедување сервери или пристап до бесплатни ресурси од националните CERT-ови. Поглавјето, исто така, промовира соработка со владата, академијата и технолошките индустрии за застапување за побезбеден дигитален екосистем. Со поврзување со врсници, граѓанските организации ја засилуваат својата одбрана, како што се гледа во случај кога споделените предупредувања спречија фишинг кампања. Практичните упатства на поглавјето, како што е претплатата на безбедносни билтени, обезбедуваат пристапност за малите граѓански организации. Се усогласува со моделот „обучи го обучувачот“ од наставната програма, поттикнувајќи пристап управуван од заедницата кон отпорност и колективна одбрана.

3. ОБРАЗОВНИ МОДУЛИ

Вовед и контекст

Во денешната дигитална доба, организациите на граѓанското општество (ГО) и невладините организации (НВО) сè повеќе се потпираат на дигитални алатки, за да ги

исполнат своите мисии. За жал, ова ги прави да бидат привлечни цели за сајбер закани. Всушност, 50% од ГО беа цел на сајбер напад во 2025 година, а непрофитните организации сега се вториот најподложен сектор од страна на сајбер напади од национални држави (31% од сите случаи). И покрај овој ризик, многу ГО се недоволно подготвени – четири од пет ГО немаат никаков план за сајбер безбедност, а 70% не сметаат дека ги имаат потребните знаења или вештини за да одговорат на сајбер напади. Овие статистики ја нагласуваат итната потреба од зајакнување на дигиталниот безбедносен капацитет во непрофитниот сектор.

Дигиталната безбедност не е само ИТ прашање; таа влијае на способноста на организацијата да ѝ служи на својата заедница. Еднократното кршење на правата или нападот со ransomware може да ги наруши критичните услуги, да ги компромитира чувствителните податоци на корисниците и да ја наруши јавната доверба. За граѓанските организации кои работат со ограничени ресурси, закрепнувањето од вакви инциденти може да ги одвлече драгоцените средства и време од нивната основна мисија. Затоа, подобрувањето на дигиталната безбедносна инфраструктура на граѓанското општество е од суштинско значење за да се обезбеди дека овие организации можат да работат безбедно и ефикасно.

Цел на наставната програма

Една од клучните цели на нашиот проект е да се развие сеопфатна „Наставна програма за дигитална безбедност за граѓанското општество“. Целта е да се создаде структурирана програма за обука што ќе ги оспособи граѓанските организации и групите на граѓанското општество со знаењето и вештините потребни за подобрување на нивната дигитална безбедносна инфраструктура. Под инфраструктура, подразбираме цел спектар на дигиталната безбедносна позиција на една организација – од безбедни технологии и практики до политики и капацитети на персоналот. Оваа наставна програма е замислена како практичен сет алатки што ќе им помогне на граѓанските организации да научат како да ги заштитат своите податоци, системи и комуникации, со што ќе ја намалат нивната ранливост на сајбер закани.

Оваа цел е во согласност со поширокаата цел на нашиот проект за зголемување на дигиталната безбедност низ цела Европа. Со градење капацитети на ниво на граѓанското општество, ние користиме пристап од долу нагоре за зајакнување на сајбер безбедноста на континентално ниво. Добро обучените граѓански организации не само што ќе ги заштитат своите операции, туку ќе придонесат и за побезбедна дигитална средина за заедниците на кои им служат. Во суштина, наставната програма ќе биде стратешки чекор кон зајакнување на сајбер безбедноста преку граѓанското општество, осигурувајќи дека дури и помалите организации можат да одржуваат силни практики за дигитална одбрана.

До крајот на оваа наставна програма, учесниците ќе можат да:

- *Ги идентификуваат главните закани за дигиталната безбедност за граѓанските организации и да ги објаснат основните заштитни мерки.*
- *Спроведат основна проценка на ризикот на дигиталните средства на нивната организација и да изготват едноставен план за сајбер безбедност.*

- *Ги имплементираат основните безбедносни мерки на уредите, мрежите и комуникациите (на пр. силни лозинки, заштитни ѕидови, безбедни Wi-Fi мрежи).*
- *Ги применуваат принципите за заштита на податоците и да ги почитуваат релевантните прописи за приватност на податоците (на пр. GDPR).*
- *Користат безбедни социјални медиуми и онлајн алатки за да го заштитат угледот и информациите на организацијата.*
- *Развијат и спроведуваат основни политики за ИТ безбедност (како што се политики за лозинка, резервна копија и прифатлива употреба) и да спроведат основна постапка за одговор на инциденти.*

Преглед на наставната програма

„Наставната програма за дигитална безбедност за граѓанското општество“ е структурирана програма за учење, дизајнирана како стратешки сет алатки што организациите на граѓанското општество и граѓанските организации го следат за да ја зајакнат својата инфраструктура за дигитална безбедност. Наставната програма се спроведува како модуларен пакет за обука што партнерите во проектот го адаптираат и го спроведуваат во своите земји.

Клучните карактеристики на наставната програма вклучуваат:

- **Сеопфатна содржина:**
  Наставната програма опфаќа теми од основно до напредно ниво, овозможувајќи им на организациите со ограничено претходно знаење постепено да го градат својот капацитет за дигитална безбедност чекор по чекор.
- **Практичен фокус:**
  Наставната програма нагласува практични вештини и сценарија од реалниот живот, наместо теоретски пристапи. Модулите се занимаваат со практични ситуации како што се реагирање на обиди за фишинг, обезбедување онлајн состаноци и заштита на организациските податоци. Секој модул обезбедува практични упатства, алатки и контролни листи што граѓанските организации ги применуваат директно во нивното секојдневно работење.
- **Прилагодување и локална релевантност:**
  Наставната програма е дизајнирана да биде прилагодлива на националните контексти. Партнерите во проектот ги прилагодуваат примерите, студиите на случај и избраната содржина на локалните регулативи, потреби и оперативни реалности, додека основните принципи и целите на учењето остануваат конзистентни во сите земји-партнери.
- **Формат и испорака:**
  Материјалите за обука вклучуваат слајдови, концизни објаснувачки текстови и интерактивни компоненти како што се вежби и квизови. Наставната програма се спроведува преку онлајн формати и/или работилници со физичко присуство за да се обезбеди пристапност за организации од различни големини и технички капацитети. Се промовира пристап „обучи го обучувачот“, овозможувајќи им на партнерите во проектот и на локалните експерти да ја спроведуваат обуката на нивните национални јазици.

- **Структура ориентирана кон резултати:**
  По завршувањето на наставната програма, учесниците се способни да ги проценат дигиталните ризици на нивната организација, да имплементираат основни безбедносни мерки, да развијат внатрешни политики за дигитална безбедност и самоуверено да одговорат на вообичаените сајбер закани. Наставната програма вклучува алатки и индикатори за самооценување што им овозможуваат на организациите да го проценат нивото на подготвеност за дигитална безбедност.

Зошто на граѓанските организации им е потребен капацитет за дигитална безбедност?

- ***Висок ризик, ниски ресурси:*** ГО често ракуваат со чувствителни податоци (на пр. лични податоци на корисници, донатори), но работат со ограничени буџети што ги ограничуваат нивните мерки за сајбер безбедност. Напаѓачите знаат дека многу ГО се „сиромашни со сајбер-безбедност, но богати со целни цели“ - богати со податоци и средства, но сиромашни со одбрана.
- ***Растечки пејзаж на закани:*** Со зголемената дигитализација (забрзана од пандемијата) и потпирањето на онлајн услуги од трети страни, површината на напади врз граѓанските организации се зголеми. Фишинг, малициозен софтвер, рансомвер и DDoS напади врз граѓанското општество се во пораст.
- ***Недостаток на свест и обука:*** Многу вработени и лидери на граѓански организации немаат формална обука за сајбер безбедност. Околу 90% од непрофитните организации не редовно ги обучуваат вработените за сајбер хигиена. Овој јаз води до небезбедни практики (како слаби лозинки или напаѓање со фишинг измами) што ги искористуваат противниците.
- ***Нема формални политики:*** Без насоки, малку граѓански организации воспоставуваат безбедносни политики или планови за одговор на инциденти - оставајќи ги без кормило за време на инцидент. Речиси 80% од граѓанските организации немаат политика/план за сајбер безбедност. Наставната програма може да им помогне на организациите да ги креираат овие внатрешни политики и стратегии за одговор.
- ***Регулаторен притисок:*** Законите за заштита на податоци, како што е Општата регулатива за заштита на податоци (GDPR) на ЕУ – најсеопфатниот закон за заштита на податоци во светот – бараат од организациите да ги заштитат личните податоци. Граѓанските организации мора да се придржуваат исто како што прават компаниите, или ризикуваат правни и репутациски последици. Градењето знаење за ваквите регулативи е клучен дел од капацитетот за дигитална безбедност.
- Овие предизвици истакнуваат зошто е неопходна наменска наставна програма. Таа ќе се справи со јазот во знаењето, ќе промовира култура на безбедност и ќе им обезбеди на граѓанските организации патоказ за развој на сопствени планови, политики и заштита за сајбер безбедност.

Целна публика и засегнати страни

Примарната целна група на наставната програма ја сочинуваат организациите на граѓанското општество (ГО) и невладините организации, вклучувајќи ги следниве профили:

- ***Раководство и менаџмент на граѓанските организации:***
  Поединци одговорни за организациската стратегија, управувањето со ризици и

распределбата на ресурсите, на кои им е потребно јасно разбирање на дигиталните безбедносни ризици и институционалните одговорности.

- ***ИТ персонал или технички контактни точки:***
  Персонал одговорен за спроведување на технички безбедносни мерки и поддршка на безбедни дигитални практики во рамките на организацијата.
- ***Програмски и оперативен персонал:***
  Членовите на персоналот кои управуваат со дневниот тек на податоци, информациите за корисниците, финансиските евиденции и дигиталната комуникација бараат силна свест за безбедните дигитални практики.
- ***Волонтери и теренски персонал:***
  Поединци кои користат организациски уреди или ракуваат со чувствителни информации на терен и имаат потреба од насоки за безбедно дигитално однесување.
- ***Партнерски мрежи и организации во заедницата:***
  Организации кои работат во соработка или во коалиции со граѓански организации, осигурувајќи се дека практиките за дигитална безбедност се протегаат низ институционалните мрежи.

Заинтересираните страни вклучени во развојот и имплементацијата на наставната програма се партнерските организации на проектот од земјите учеснички и експерти за сајбер безбедност и дигитална безбедност. Влезот од специјализирани експерти и институции гарантира дека наставната програма е усогласена со меѓународно признатите најдобри практики во дигиталната безбедност и заштитата на податоците.

Клучни модули и теми во наставната програма

Наставната програма е организирана во неколку модули, секој од нив фокусиран на критичен аспект на дигиталната безбедност. Подолу е даден преглед на клучните теми што планираме да ги вклучиме:

1. Основи на дигиталната безбедност: Разбирање на пејзажот со закани и основна хигиена – Воведува зошто дигиталната безбедност е важна за граѓанските организации. Опфаќа видови закани (малициозен софтвер, фишинг, хакирање, DDoS итн.), актери на закана (криминалци, непријателски настроени влади кои го таргетираат граѓанското општество) и фундаментални најдобри практики. Акцентот е на создавање безбедносен начин на размислување и основни навики (силни лозинки, користење двофакторска автентикација, редовни ажурирања на софтверот, избегнување сомнителни е-пораки).

2. Проценка на ризик и планирање: Проценка на организациските ризици и креирање план за безбедност – Ги води граѓанските организации низ идентификување на нивните дигитални средства и ранливости. Како да се спроведе едноставна проценка на ризикот (што имаме што другите би можеле да го нападнат? Како би можеле да го направат тоа? Кои се последиците?). Овој модул ќе ги води организациите кон изготвување или подобрување на нивниот план за сајбер безбедност (бидејќи во моментов 80% од нив немаат таков) – вклучувајќи политики за ракување со податоци, контрола на пристап и постапка за одговор на инциденти.

3. Обезбедување на уреди и инфраструктура: Заштита на компјутери, мрежи и веб-страници – Се фокусира на обезбедување на технологијата што ја користи CSO. Темите

вклучуваат безбедност на уредот (антивирус, енкрипција на уреди, безбедна конфигурација на уредот), безбедна употреба на Wi-Fi и мрежи, користење на VPN кога е соодветно и обезбедување на веб-страници (основи на безбедност на веб-хостинг, резервни копии, користење HTTPS, заштита од оштетување или DDoS). Вистински примери на напади (на пр., случај на оштетување на веб-страница што го остави CSO офлајн со месеци) ќе ја илустрираат важноста на овие мерки.

4. Безбедна комуникација и соработка: Безбедна е-пошта, пораки и работа од далечина – Ве учи како безбедно да комуницирате и внатрешно и со надворешни засегнати страни. Опфаќа безбедност на е-пошта (препознавање фишинг, користење шифрирана е-пошта или безбедни даватели на услуги за е-пошта), апликации за пораки (избор на безбедни апликации како Signal, овозможување енкрипција од крај до крај) и безбедно споделување датотеки. Исто така, се справува со предизвиците на далечинската работа: користење безбедни врски, заштита на видео конференции и управување со сметки/акредитиви при работа од дома или во движење.

5. Заштита на податоци и усогласеност со прописите за приватност: Заштита на податоци и разбирање на законските обврски – ја нагласува заштитата на чувствителните податоци што ги собираат граѓанските организации (податоци за корисници, информации за донатори, итн). Воведува принципи на заштита на податоците: минимизирање на податоците, енкрипција на податоците во мирување и во пренос, безбедно складирање/резервна копија и правилно отстранување на податоците. Ќе ги истакнеме релевантните закони како што е GDPR – водечка рамка за заштита на податоците во Европа – и што подразбира усогласеноста за граѓанските организации (на пр. добивање согласност, обезбедување на лични податоци, пријавување на прекршувања). Овој модул им обезбедува на организациите да ги разберат и етичките и законските одговорности при ракување со податоци.

6. Безбедност на социјалните медиуми и онлајн присуство: Заштита на организацискиот углед и сметки – Многу граѓански организации се потпираат на социјалните медиуми за информирање. Оваа тема опфаќа обезбедување на сметките на социјалните медиуми (силни лозинки, двофакторска авторизација, пристап базиран на улоги за повеќе менаџери), заштита од киднапирање на сметки и справување со онлајн вознемирување или кампањи за дезинформации. Исто така, вклучува упатства за управување со содржината на веб-страницата, безбедност и безбедно онлајн однесување што ја штити репутацијата на граѓанските организации.

7. Развивање на безбедносна култура: Обука на персоналот, политики и одговор на инциденти – Фокусот е на човечки фактори и организациските мерки. Како да се негува култура каде што секој член на персоналот ја разбира својата улога во сајбер безбедноста. Упатство за пишување едноставни политики за ИТ безбедност (политика за прифатлива употреба, правила за „донесете го вашиот сопствен уред“ итн.), спроведување редовни обуки за подигање на свеста за персоналот (бидејќи обуката за оCSO е од витално значење за да се спречи 90% од персоналот да биде слабата алка) и воспоставување план за одговор

на инциденти (чекори што треба да се преземат доколку се случи прекршок, улоги и одговорности, стратегија за комуникација за време на сајбер криза). Исто така, ќе ги опфатиме основите на пријавување инциденти до властите и учење од инцидентите.

Стратегија за имплементација на наставната програма

Развојот и имплементацијата на оваа наставна програма беа спроведени како колаборативен и фазен процес.

Преглед на наставната програма и локализација:

По подготовката на првичниот нацрт, партнерите во проектот ги разгледаа материјалите за наставната програма за да се осигурат дека се релевантни за локалните контексти. Во текот на оваа фаза, партнерите предложија адаптации како што се преведување на клучна терминологија, вклучување на студии на случаи специфични за земјата и усогласување на препораките со националното законодавство и вообичаените практики. Како резултат на тоа, наставната програма беше структурирана со основна рамка дополнета со опционални локализирани делови за секоја земја учесничка.

Обука за пилот програми:

Наставната програма беше пилотирана со мала група учесници од граѓански организации во одбрани партнерски земји. Пилот-имплементацијата беше спроведена или како кратки модуларни сегменти (приближно 15-20 минути по модул) или како целодневна работилница. Повратните информации собрани во текот на оваа фаза се фокусираа на јасноста, должината и практичната корисност на содржината, а наставната програма беше соодветно подобрена.

Сесии за обука на обучувачи:

За да се обезбеди скалираност и одржливост, беа организирани сесии за обука на обучувачи за партнерите во проектот и на назначените претставници на граѓанските организации во секоја земја. Овие сесии ги опфатија не само содржината на наставната програма, туку и техниките за водечка фасилитација, интерактивни вежби и дискусии, овозможувајќи им на обучувачите со сигурност да го достават материјалот до поширокаата публика.

Имплементација кај граѓанските организации (градење капацитети):

По фазата на обука на обучувачи, партнерските организации спроведоа обуки на национално ниво за локални граѓански организации и актери од граѓанското општество. Овие обуки беа спроведени преку вебинари, семинари со физичко присуство или интегрирани во постојните активности за градење капацитети. Во зависност од локалните потреби, обуките беа структурирани како индивидуални модули од 15-20 минути или комбинирани во подолги работилници што опфаќаа повеќе модули.

Ресурси и поддршка за OCSOing:

Сите материјали за наставната програма и придружниот прирачник беа собрани и споделени во достапни формати, првенствено како PDF ресурси што можат да се преземат.

Покрај тоа, беше воспоставен и онлајн комуникациски канал за да им се овозможи на учесниците и обучувачите да поставуваат прашања, да разменуваат искуства и да споделуваат новости поврзани со новите закани или добрите безбедносни практики. Оваа средина за врсници за учење поддржуваше континуирано ангажирање надвор од формалните обуки.

Мониторинг и евалуација:

Во текот на целиот процес на имплементација, беа спроведени активности за следење и евалуација, за да се процени влијанието на наставната програма. Индикаторите вклучуваа број на обучени граѓански организации, промени забележани помеѓу проценките пред и по обуката и квалитативни повратни информации за организациските подобрувања (како што се усвојување политики за сајбер безбедност или нови процедури за заштита на податоци). Овие наоди беа интегрирани во целокупната рамка за следење на проектот, за да се осигури дека наставната програма ефикасно придонесува за зајакнување на практиките за дигитална безбедност меѓу организациите учеснички.

Следејќи го овој пристап, процесот на развој и имплементација на наставната програма беше инклузивен и итеративен, што резултираше со финален производ, кој беше добро прилагоден на потребите на организациите на граѓанското општество во различни национални контексти.

3.1 МОДУЛ 1: ОСНОВИ НА ДИГИТАЛНАТА БЕЗБЕДНОСТ – РАЗБИРАЊЕ НА ПЕЈЗАЖОТ СО ЗАКАНИ И ОСНОВНА ХИГИЕНА

До крајот на овој модул, учесникот ќе може да:

- *Објасни зошто дигиталната безбедност е клучна за граѓанските организации и да ги идентификуваосновните практики за сајберхигиена.*
- *Ги препознае вообичаените сајбер закани (малициозен софтвер, фишинг, DDoS итн.) насочени кон граѓанското општество.*
- *Применува основни безбедносни навики (силни лозинки, двофакторска автентикација, ажурирања на софтвер, внимателност кон сомнителни е-пораки).*

Цели на учење:

- Подигнување на свеста за тоа зошто дигиталната безбедност е клучна за граѓанските организации и за специфичните сајбер закани насочени кон граѓанското општество.
- Идентификување на вообичаените видови сајбер напади (на пр. малициозен софтвер, фишинг, хакирање, DDoS) и закани (криминални групи, непријателски настроени влади) со кои може да се соочат граѓанските организации.
- Усвојување на фундаментални најдобри практики и навики за сајбер безбедност (на пр. креирање силни лозинки, овозможување двофакторска автентикација, ажурирање на софтверот и препознавање на сомнителни комуникации).

Клучни теми:

- Важноста на дигиталната безбедност за граѓанските организации – како сајбер инцидентите можат да ги нарушат операциите и да ги компромитираат чувствителните податоци.
- Преглед на пејзажот на закани: вообичаени видови напади како малициозен софтвер, фишинг, хакирање, DDoS итн., и нивната зголемена инциденца против граѓанското општество.
- Заканувачки актери насочени кон граѓанските организации: од сајбер криминалци кои бараат финансиска добивка до непријателски групи поддржани од државата кои имаат за цел да ги надгледуваат или попречуваат активностите на граѓанските организации.
- Основни практики за сајбер хигиена: користење силни лозинки и менаџер за лозинки, овозможување двофакторска автентикација, ажурирање на софтверот/антивирусот и претпазливост со сомнителни е-пораки или линкови.
- Градење безбедносен менталитет кај персоналот – поттикнување на будност и култура каде што секој презема одговорност за дигиталната безбедност.

Примери за активности или вежби:

- **Брејнсторминг на закани:** Учесниците ги наведуваат потенцијалните сајбер закани за нивната организација и дискутираат како секоја закана би можела да влијае на нивната работа.
- **Предизвик за лозинка:** Присутните ја оценуваат јачината на примероците на лозинки и учат како да креираат и управуваат со силни лозинки (на пр. лозинки, користејќи менаџер за лозинки).
- **Квиз за фишинг: Се** презентираат примери на е-пораки (некои фишинг, некои легитимни) и учесниците идентификуваат црвени знамиња што укажуваат на обид за фишинг.
- **Дискусија за студија на случај: Се** опишува неодамнешен локален сајбер инцидент што ги погодил граѓанските организации – се анализира што се случило во овој инцидент и се дискутира кои основни безбедносни мерки можеби го спречиле.

Пример за студија на случај од Модул 1: Напад со фишинг врз граѓанска организација во заедницата

- **Контекст:** Мала граѓанска организација во заедницата која обезбедува храна и помош за ранливото население се потпира на е-пошта и на платформи за онлајн донации. Персоналот има минимална обука за сајбер безбедност и се потпира само на основна безбедност на е-поштата.
- **Проблем:** Едно утро, финансискиот службеник на CSO добил итна е-пошта од некој што се преправал дека е голем донатор. Е-поштата содржела сомнителна врска за ажурирање на деталите за плаќање. Службеникот кликнал на врската и ги внел податоците за најавување на веб-страницата на банкарската сметка на CSO, несвесен дека станува збор за фишинг страница. За неколку часа, од сметката на CSO биле извршени неовластени подигнувања средства, во вкупен износ од илјадници долари. CSO морал привремено да ги запре операциите додека да ги поврати средствата и да ги обезбеди сметките.
- **Исход:** По инцидентот, Организацискиот орган за заштита на лични податоци (ОЗО) го разгледа овој безбедносен пропуст со помош на технолошки искусен волонтер. Тие веднаш имплементираа основни мерки за сајбер хигиена: спроведување силни, уникатни лозинки и овозможување двофакторска автентикација на сите сметки. Тие исто така започнаа со редовна обука на персоналот за препознавање на фишинг е-пораки (барање печатни грешки, проверка на адреси на испраќачи итн.). Во следните месеци, ОЗО успешно избегна слични измами и ја врати довербата кај донаторите преку транспарентност во врска со подобрувањата.

Прашања за дискусија:

- *Која основна сајбер-безбедносна практика можеше да го спречи фишинг нападот во овој случај?*

- *Зошто вработениот наседна на фишинг е-поштата и кои чекори би можеле да му помогнат на персоналот да препознае вакви измами во иднина?*
- *Како ОЗО закрепна од инцидентот и какви мерки презеде за зајакнување на безбедноста потоа?*

Модул 1 Проценка

- Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 1 – Проценка: Кратки прашања

ошто дигиталната безбедност е особено важна за организациите на граѓанското општество? (Накратко објаснете како сајбер инцидентите можат да влијаат врз работењето на граѓанските организации или врз корисниците.)

аведете две вообичаени сајбер закани кои често ги таргетираат организациите на граѓански организации. (Пример: фишинг, малициозен софтвер, DDoS итн.)

то е фишинг и како обично се обидува да ги измами корисниците? (Објаснете го основниот метод во една или две реченици.)

аведете две основни практики за сајбер-хигиена кои помагаат да се спречи компромитирањето на сметката. (Пример: силни лозинки, двофакторска автентикација, редовни ажурирања.)

аведете еден јасен предупредувачки знак дека е-поштата може да биде обид за фишинг. (Пример: итен јазик, сомнителна адреса на испраќачот, неочекувани врски или прилози.)

Практична задача: Идентификација на ризик од фишинг

На учесниците им се дава краток примерок на е-пошта (или сценарио) поврзан со работата на ГО (на пр., ажурирање за донација, порака за финансиер или внатрешно барање).

Од учесниците се бара да:

- Одлучат дали пораката е легитимна или сомнителна.
- Идентификуваат најмалку два предупредувачки знаци (црвени знамиња) во пораката.
- Напишат една конкретна акција што треба да ја преземат наместо да кликнат на линкот или директно да одговорат (на пр., да потврдат преку друг канал, да пријават кај претпоставен).

Критериуми за оценување:

- Правилно ја идентификува е-поштата како сомнителна или ризична,
- Правилно посочува најмалку две црвени знамиња,
- Предлага соодветен безбеден одговор.

3.2 МОДУЛ 2: ПРОЦЕНКА НА РИЗИЦИ И ПЛАНИРАЊЕ – ПРОЦЕНКА НА ОРГАНИЗАЦИСКИ РИЗИЦИ И КРЕИРАЊЕ НА БЕЗБЕДНОСЕН ПЛАН

До крајот на овој модул, учесникот ќе може да:

- *Ги идентификува ги критичните дигитални средства на организацијата и потенцијалните ранливости.*
- *Спроведе основна проценка на ризикот преку проценка на веројатноста и влијанието на заканите врз тие средства.*
- *Нацрта едноставен план или политика за сајбер безбедност што опфаќа ракување со податоци, контрола на пристап и план за одговор на инциденти.*

Цели на учење:

- Разбирање како да ги идентификувате критичните дигитални средства на организацијата (податоци, системи, сметки) и потенцијалните ранливости.
- Спроведување основна проценка на ризикот за да ги процените заканите за тие средства и потенцијалното влијание врз организацијата.
- Развивање или подобрување на план/политика за сајбер безбедност за ООП, опфаќајќи клучни области како што се процедури за ракување со податоци, контроли на пристап и подготвеност за одговор на инциденти.

Клучни теми:

- Идентификување на дигиталните средства и податоци: мапирање на тоа кои информации и системи ги користи ГО (на пр. бази на податоци за донатори, е-пошта сметки, веб-страници) и зошто тие би можеле да бидат цел на напади.
- Ранливости и закани: разбирање како да се забележат слабостите (застарен софтвер, недостаток на резервни копии итн.) и замислување сценарија за закани (Што би можеле да целат напаѓачите? Како би можеле да го сторат тоа? Кои се последиците?).
- Процес на проценка на ризик: проценка на веројатноста и влијанието на различни сценарија на закани и приоритизација на ризиците што треба да се решат први.
- Создавање план за сајбер безбедност: изготвување на политика за безбедност на организацијата што опфаќа практики за заштита на податоци, контрола на пристап на корисниците и постапка за одговор на инциденти (особено важно бидејќи ~80% од граѓанските организации моментално немаат формален план за безбедност).
- Ажурирање на планот: доделување одговорност за периодично прегледување и ажурирање на безбедносниот план како што расте организацијата или се менува пејзажот на закани.

Примери за активности или вежби:

- **Инвентар на средства:** Учесниците ги наведуваат клучните дигитални средства (на пр. бази на податоци, сметки за е-пошта, уреди, услуги во облак) на кои се потпира нивната организација за граѓански организации и идентификуваат кои чувствителни информации се поврзани со секоја од нив.
- **Мапирање на ризик:** За секое наведено средство, групата идентификува можни закани или сценарија за дефекти и ја оценува нивната веројатност и влијание (креирајќи едноставна матрица на ризик за визуелизација на ризиците со висок приоритет).

- **Развој на план:** Работејќи во тимови, учесниците изготвуваат основен план за сајбер безбедност за примерок на граѓанска организација. Ова треба да вклучува делови за политиките за ракување со податоци, кој има пристап до нив и чекорите што треба да се преземат доколку се случи безбедносен инцидент. Потоа тимовите ги споделуваат своите планови за повратни информации.
- **Локалон ризично сценарио:** (Примери за сценарија на случаи се вклучени во деловите за локализација специфични за земјата.) Учесниците дискутираат за ова сценарио и размислуваат како би го ублажиле ризикот, користејќи елементи од безбедносен план (политики, превентивни мерки, чекори за одговор).

Студија на случај за Модул 2: Игнорираната ранливост води до губење податоци
Контекст: Средна организација за граѓански организации управува со внатрешен сервер на кој се чуваат податоци за донаторот и корисникот. Тие знаат дека серверот е важен, но немаат формална документација за неговите резервни копии или ризици. Персоналот претпоставувал дека податоците се безбедни бидејќи „ништо лошо не се случило претходно".
Проблем: Ненадеен пренапон на струја предизвикан од бура во близина го оштети хардверот на серверот на CSO, оштетувајќи ги податоците. Бидејќи серверот немаше резервна копија со месеци, сите записи на донаторите, датотеките на проектот и финансиските податоци беа изгубени. CSO беше принудена да ги запре своите програми со недели. Донаторите мораа повторно да испраќаат информации, а многу записи не можеа да се вратат, што доведе до конфузија и губење на довербата.
Исход: Сфаќајќи ја сериозноста на овој дефект, CSO спроведе темелна проценка на ризикот со надворешна помош. Тие ги идентификуваа клучните средства (бази на податоци, веб-страница, сметки за е-пошта) и заканите (прекин на електрична енергија, хардверски дефекти, сајбер напади). Тие дадоа приоритет на инвестирањето во систем за резервни копии надвор од локацијата и поставувањето редовен распоред за резервни копии. CSO изготви основен план за сајбер безбедност, вклучувајќи процедури за резервни копии и за обновување на податоците. Подоцна, кога се појавија помали системски проблеми, тие успешно ги вратија податоците од резервни копии без прекин.
Прашања за дискусија:

- *Кои беа предупредувачките знаци дека ГО беше ранлива пред катастрофата?*
- *Кои елементи треба да ги вклучи ГО во својот нов план за сајбер безбедност за да се спречи слична загуба?*
- *Како вршењето проценка на ризикот ѝ помогна на ГО да ја подобри својата безбедност и работење?*

Модул 2 Проценка
Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 2 – Проценка: Кратки прашања

- Што се смета за дигитален ресурс во контекст на граѓанска организација? (Наведете два примера).

- Зошто е ризично за една организација да се потпира на претпоставката дека „ништо лошо не се случило претходно“?
- Кои се двата главни фактори што се оценуваат во основната проценка на ризикот? (Објаснете накратко).
- Наведете две вообичаени ранливости што можат да ги зголемат ризиците од сајбер безбедност кај граѓанските организации.
- Зошто е важно редовно да се прегледува и ажурира планот за сајбер безбедност?

Практична задача: Основна вежба за проценка на ризик

Од учесниците се бара да ги завршат следните чекори за хипотетичка или реална ГО:

- Да наведат еден критичен дигитален ресурс (на пр. база на податоци за донатори, систем за е-пошта, веб-страница),
- Да идентификуваат една можна закана за тој имот (на пр. прекин на електричната енергија, фишинг напад, хардверски дефект),
- Накратко да опишат една превентивна мерка што би можела да го намали ризикот (на пр. резервни копии, контроли на пристап, двофакторска автентикација).

Критериуми за оценување:

- Имотот е јасно идентификуван,
- Заканата е реална и релевантна,
- Предложената превентивна мерка е соодветна.

3.3 МОДУЛ 3: ОБЕЗБЕДУВАЊЕ НА УРЕДИ И ИНФРАСТРУКТУРА – ЗАШТИТА НА КОМПЈУТЕРИ, МРЕЖИ И ВЕБ-СТРАНИЦИ

До крајот на овој модул, учесникот ќе може да:

мплементира најдобри практики за заштита на компјутерите и мобилните уреди (инсталирање ажурирања, заштита од малициозен софтвер и енкрипција).

онфигурира и да ги заштити организациските мрежи (безбеден Wi-Fi, користење VPN за далечински пристап).

а подобри безбедноста на веб-страницата и серверот (овозможување HTTPS, правете редовни резервни копии и заштитете се од вообичаени напади како што се уништување на профилот или DDoS).

Цели на учење:

- Имплементирање најдобри практики за обезбедување на компјутери и мобилни уреди (на пр. инсталирање на софтвер против малициозен софтвер, овозможување на енкрипција на уредот и правилно конфигурирање на безбедносните поставки).
- Заштитување на организациските мрежи и пристапот до интернет преку безбедни Wi-Fi практики и користење на безбедни врски (како што се VPN мрежи за далечински пристап).
- Зајакнување на безбедноста на веб-страницата и онлајн инфраструктурата на ГО со користење на современи мерки за заштита (HTTPS, резервни копии, DDoS заштита итн.) и разбирање како да се одговори на вообичаени напади.

Клучни теми:

- Основни безбедносни мерки на уредот: инсталирање и ажурирање на антивирусен/ софтвер на сите компјутери, овозможување на заштитни ѕидови и користење енкрипција на дискови на лаптопи и паметни телефони за да се спречи кражба на податоци.
- Безбедна конфигурација на уредот: создавање силни лозинки/ПИН кодови за најавување на уредот, отстранување или оневозможување на непотребни апликации и услуги и редовно применување безбедносни закрпи или ажурирања.
- Основи на мрежна безбедност: безбедна употреба на Wi-Fi (користење доверливи мрежи, обезбедување канцелариски Wi-Fi со силни лозинки и енкрипција) и кога да се користат VPN мрежи за енкриптирани врски (особено на јавни мрежи).
- Безбедност на веб-страницата и серверот: одржување на ажуриран софтвер на веб-страницата (CMS, додатоци), користење на HTTPS за шифрирање на веб-сообраќајот, вршење редовни резервни копии на податоците на страницата и имплементирање заштита од вообичаени напади како што се уништување на идентитетот или DDoS.
- Примери од реалниот свет за напади во инфраструктурата: на пример, случај на оштетување на веб-страницата што ја остави граѓанската организација офлајн со месеци, што ја нагласува важноста на проактивната одбрана.

Примери за активности или вежби:

- **Ревизија на безбедноста на уредот:** Користејќи листа за проверка, учесниците проверуваат примерок од уредот (или својот, доколку е соодветно) за основна безбедносна заштита – проверуваат дали има инсталација и ажурирања на антивирусниот софтвер, статус на заштитен sид, овозможено шифрирање и неодамнешни безбедносни ажурирања.
- **Демонстрација за безбедност на Wi-Fi:** Обучувачот ги демонстрира ризиците од користење на необезбеден јавен Wi-Fi (на пр., колку е лесно да се шпионира сообраќајот). Потоа дискутирајте за чекорите за да останете безбедни: конфигурирање на безбедна Wi-Fi мрежа за дома/канцеларија и користење VPN или безбедни апликации кога сте на јавни мрежи.
- **Преглед на безбедноста на веб-страницата:** Презентирајте сценарио за фиктивна веб-страница на ГО со неколку безбедносни недостатоци (застарен софтвер, недостаток на HTTPS, слаба администраторска лозинка). Мали групи ги идентификуваат проблемите и препорачуваат решенија за подобрување на безбедноста на веб-страницата.
- **Локална студија на случај:** Опишете локален случај на оштетување на веб-страницата на граѓанска организација или сајбер напад – Дискутирајте што се случило во овој инцидент и кои превентивни мерки (од клучните теми на модулот) би можеле да помогнат да се избегне таков настан во иднина.

Студија на случај за Модул 3: Деформирање на веб-страницата и прекин на услугата

Контекст: Граѓанска организација управува со јавна веб-страница за ажурирања на програмите и собирање средства. Страницата е изградена на систем за управување со содржини со отворен код (CMS). Техничкото одржување го вршеше еден волонтер кој повремено ја ажурираше страницата.

Проблем: Хакерите искористиле застарен додаток на веб-страницата на ГО, оштетувајќи ја почетната страница и заменувајќи ја со политичка порака. ГО не ја забележале промената веднаш бидејќи персоналот не ја проверувал редовно страницата. Оштетувањето продолжило неколку дена, предизвикувајќи забуна кај поддржувачите и привремено одвраќајќи ги донаторите. Посетителите виделе несоодветна содржина, а кредибилитетот на организацијата бил нарушен. Дополнително, хакерите добиле пристап до датотеките на веб-страницата, што предизвикало загриженост за безбедноста на податоците на донаторите (иако не е потврдено никакво кршење на безбедноста).

Исход: Откако го откри проблемот, CSO ја исклучи веб-страницата за чистење и ја отстрани злонамерната содржина. Го ажурираа CMS и сите додатоци на најновите верзии. Во иднина, CSO имплементираше редовни резервни копии на страницата и закажа неделни проверки на својата веб-страница. Тие исто така преминаа на управуван давател на хостинг услуги со автоматски ажурирања и HTTPS енкрипција. Во следните месеци, страницата остана безбедна, а CSO ја врати довербата преку транспарентно комуницирање за инцидентот и чекорите преземени за да го спречи.

Прашања за дискусија:

ако ажурирањето на софтверот и редовните резервни копии можеа да го променат исходот од овој напад?
ои итни чекори требало да ги преземе ГО откако го забележале оштетувањето на веб-страницата?
ои долгорочни мерки ги спроведе ГО за да ја обезбеди својата веб-инфраструктура?

Модул 3 Проценка
Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 3 – Проценка

Кратки прашања

ошто е важна енкрипцијата на уредите за лаптопите и паметните телефони што ги користат граѓанските организации?
(Одговорете во една или две реченици.)
аведете две основни безбедносни мерки што треба да бидат овозможени на сите организациски уреди.
ои се главните ризици од користење на необезбеден јавен Wi-Fi без дополнителна заштита?
ошто застарените CMS додатоци претставуваат сериозен безбедносен ризик за веб-страниците на CSO?
ако редовните резервни копии го намалуваат влијанието на оштетувањето на веб-страницата или сајбер нападите?

Практична задача: Основна проверка на безбедноста на уредот или веб-страницата

Учесниците избираат една од следниве опции:

Опција А – Безбедност на уредот

- Наведете три безбедносни мерки што моментално се применуваат на еден работен уред (компјутер или паметен телефон)
  (на пр. антивирус, енкрипција, заклучување на екранот, ажурирања)
- Идентификувајте една мерка што недостасува или е слаба и накратко наведете како би можела да се подобри.

Опција Б – Безбедност на веб-страницата

- Идентификувајте две основни безбедносни контроли што треба да бидат воспоставени за веб-страницата на една ГО.

(на пр. HTTPS, редовни ажурирања, резервни копии, силни администраторски лозинки)

- Накратко објаснете еден ризик доколку овие контроли не се имплементираат.

Критериуми за оценување:

- Идентификуваните мерки се релевантни за модулот.
- Ризиците или подобрувањата се реални и јасно објаснети.

Полагање на барања:
Учесникот мора правилно да идентификува најмалку две валидни безбедносни мерки и еден поврзан ризик или подобрување.

3.4 МОДУЛ 4: БЕЗБЕДНА КОМУНИКАЦИЈА И СОРАБОТКА – БЕЗБЕДНА Е-ПОШТА, ПОРАКИ И РАБОТА ОД ДАЛЕЧИНА

До крајот на овој модул, учесникот ќе може да:

и препознае и избегнува вообичаените закани базирани на е-пошта (како што е фишинг) и да применува безбедни практики за е-пошта (силни лозинки, 2FA).

ористи алатки за безбедни пораки и споделување датотеки што овозможуваат енкрипција.

мплементира безбедни практики за работа од далечина (користење VPN мрежи на јавни мрежи, обезбедување виртуелни состаноци со лозинки).

Цели на учење:

- Препознавање и избегнување вообичаени закани базирани на е-пошта (како што се фишинг измами) и применување безбедни практики за е-пошта во секојдневната работа.
- Изберање и користење безбедни алатки за комуникација за пораки и споделување датотеки (на пр. апликации со енкриптирање од крај до крај, платформи за безбедна соработка со документи) за да ги заштитите чувствителните информации.
- Спроведување безбедносни мерки за работа од далечина и виртуелна соработка (користење безбедни мрежи, заштита на онлајн состаноци и управување со сметки/уреди при работа надвор од локацијата).

Клучни теми:

- **Безбедност на е-пошта:** Како да се препознаат обиди за фишинг (на пр. сомнителни испраќачи или линкови, итни, необични барања) и важноста од користење силни лозинки и 2FA за е-пошта сметки. Доколку се разменуваат чувствителни податоци, размислете за шифрирани е-пошта услуги или додатоци.
- **Безбедно испраќање пораки:** Избирање на доверливи апликации за пораки кои нудат енкрипција од крај до крај (на пример, Signal или други безбедни пораки) и овозможување на безбедносни функции како што е исчезнување на пораките. Упатство за проверка на контакти и несподелување чувствителни информации преку небезбедни канали.
- **Споделување датотеки и соработка:** Користење на безбедно складирање во облак или услуги за споделување датотеки што нудат енкрипција. Практики како заштита на чувствителни документи со лозинка или користење платформи дизајнирани за безбедна соработка при работа со надворешни партнери.
- **Заштитни мерки за работа од далечина:** Најдобри практики за работа надвор од канцеларијата, вклучително и користење VPN мрежи на недоверливи мрежи, обезбедување на домашни Wi-Fi рутери, заштита на виртуелни простори за состаноци (користење чекални, лозинки за состаноци, ограничување на споделувањето на екранот) и управување со работните уреди што се користат од далечина.

- **Балансирање на безбедноста и пристапноста:** Обезбедување дека безбедносните мерки (како што се енкрипција и контрола на пристап) се доволно лесни за користење за персоналот постојано да ги користи и обезбедување обука за секоја нова алатка за комуникација воведена од безбедносни причини.

Примери за активности или вежби:

- **Вежба за фишинг е-пошта:** Фасилитаторот споделува примероци од е-пошта со групата. Учесниците мора да одлучат за секоја од нив дали станува збор за легитимна е-пошта или обид за фишинг и да ги истакнат индициите што влијаеле врз нивната одлука.
- **Споредба на апликации за пораки:** Поделете се во мали групи; секоја група разгледува различна апликација за пораки (на пр. WhatsApp, Signal, Telegram) и известува за нејзините безбедносни карактеристики (енкрипција, двофакторска автентикација итн.) и сите ограничувања. Дискутирајте кои апликации се најсоодветни за различни видови комуникации со граѓански организации.
- **Безбедно поставување видео повик:** Демонстрација во живо за поставување онлајн состанок со соодветна безбедност: овозможување на чекалната, барање лозинка за состанокот, ограничување на споделувањето на екранот од страна на учесниците итн. По демото, учесниците вежбаат конфигурирање на овие поставки или дискутираат за искуствата со обезбедување на сопствените состаноци.
- **Дискусија за локален контекст:** [Вметнете алатка за безбедна комуникација популарна во вашата земја или релевантен закон за енкрипција] – Дискутирајте како овој локален контекст влијае врз безбедноста на комуникацијата на организацијата за заштита на лични податоци (CSO). На пример, ако одредена енкриптирана апликација е широко користена локално, како може организацијата за заштита на лични податоци да ја искористи? Ако постојат локални прописи за енкрипција или складирање на податоци, како тие влијаат врз изборот на комуникација?

Студија на случај од Модул 4: Пробивање на е-пошта за време на далечинска работа

Контекст: За време на хуманитарна криза, теренски службеник на граѓанска организација работи од далечина од кафуле користејќи јавен Wi-Fi за да испраќа извештаи за ситуацијата до седиштето. Организацијата користи е-пошта за секојдневна комуникација, но не спроведува шифрирани врски за далечински корисници.

Проблем: Сајбер криминалец на истата јавна Wi-Fi мрежа го пресретнал нешифрираниот сообраќај на е-пошта на службеникот. Напаѓачот ги добил акредитивите за најавување кога службеникот се најавил на е-пошта сметката на CSO. Во текот на следниот ден, напаѓачот се претставил како службеник, испраќајќи лажни е-пораки до донатори барајќи итни средства за лажен проект. Еден донатор префрлил пари на сметката на напаѓачот пред да биде откриена измамата. CSO изгубил средства и морал да им ја објасни измамата на донаторите.

Исход: Како одговор на тоа, ОГО имплементираше практики за безбедна комуникација. Од сите вработени кои работеа од далечина се бараше да користат VPN или HTTPS за пристап до е-пошта, а беше овозможена двофакторска автентикација на е-пошта сметките. ОГО, исто така, усвои апликација за шифрирани пораки за внатрешна комуникација. Тие

комуницираа со донаторите за проверка на сите идни барања и подобрена обука за е-пошта за персоналот (откривање лажни е-пораки, некористење јавен Wi-Fi без заштита). По овие мерки не се случија понатамошни инциденти.

Прашања за дискусија:

акви ранливости имаа практиките за работа од далечина на ГО во овој случај?

ако VPN мрежите и двофакторската автентикација можеа да го спречат напаѓачот да добие пристап?

акви чекори презеде ГО по пробивот на безбедноста за да ги заштити комуникациите и довербата на донаторите?

Модул 4 Проценка

Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 4 – Проценка

5 кратки прашања

ои се два вообичаени знаци дека е-поштата може да биде обид за фишинг?
(Одговорете кратко.)
ошто двофакторската автентикација (2FA) е особено важна за е-пошта сметките што ги користат граѓанските организации?
аведете една функција за безбедни пораки што помага во заштитата на чувствителните комуникации.
о какви ризици се соочуваат граѓанските организации кога персоналот работи од далечина користејќи јавен Wi-Fi без заштита?
ако може обезбедувањето онлајн состаноци (на пр. лозинки, чекални) да ги намали безбедносните ризици?

Практична задача: Проверка на безбедна комуникација

Учесниците ја завршуваат следната задача индивидуално или во парови:

зберете еден комуникациски канал користен од вашата ГО
(е-пошта, апликација за пораки, платформа за споделување датотеки или алатка за видео состаноци).
акратко одговорете:

оментално е во сила една безбедносна мерка
(на пр. овозможено 2FA, шифрирани пораки, лозинки за состаноци)
дно подобрувањешто би можело да ја зајакне безбедноста
(на пр., овозможување на употреба на VPN, префрлување на шифрирана апликација, ограничување на правата за пристап)

бјаснете во една или две реченици како ова подобрување би го намалило ризикот.

Критериуми за оценување:

- Избраниот канал е релевантен за комуникацијата со ГО,
- Безбедносните мерки и подобрувања се реални,
- Објаснувањето покажува разбирање на практиките за безбедна комуникација.

3.5 МОДУЛ 5: ЗАШТИТА НА ПОДАТОЦИ И УСОГЛАСЕНОСТ СО ПРАВИЛАТА ЗА ПРИВАТНОСТ – ЗАШТИТА НА ПОДАТОЦИТЕ И РАЗБИРАЊЕ НА ЗАКОНСКИТЕ ОБВРСКИ

До крајот на овој модул, учесникот ќе може да:

и Идентификувачувствителните податоци што ги собира ГО и да објаснизошто тие мора да бидат заштитени.

рименуваклучни практики за заштита на податоци (минимизирање на податоци, енкрипција, безбедно складирање, редовни резервни копии и безбедно отстранување).

и разбира и објаснува законските обврски на ГО според законите за заштита на податоци (како што е GDPR) и како да се обезбеди усогласеност.

Цели на учење:

- Препознавање на видовите чувствителни податоци (на пр., лични информации за корисниците, евиденција за донаторите) што ги собираат граѓанските организации и зошто е клучно да се заштитат таквите податоци.
- Применување на клучните принципи за заштита на податоците – вклучувајќи минимизирање на податоците, енкрипција (за податоци што се во мирување и во пренос), безбедно складирање/резервна копија и правилно отстранување на податоците – за подобрување на приватноста и безбедноста.
- Разбирање на законските обврски и рамки за заштита на податоците, како што се GDPR на ЕУ и еквивалентните национални закони за заштита на податоците, и како да се обезбеди дека граѓанската организација за заштита на податоците се придржува до овие регулативи.

Клучни теми:

- **Идентификување на чувствителни податоци:** Што се смета за лични или чувствителни податоци во контекст на граѓанска организација (имиња, адреси, информации за здравјето или правниот случај итн.) и ризиците доколку таквите податоци протекуваат.
- **Принципи за заштита на податоци:** Практични чекори за минимизирање на податоците (собирање само на она што е навистина потребно), шифрирање на податоците во мирување (на пр. датотеки на дискови) и во пренос (користење SSL/HTTPS за пренос на податоци), безбедни решенија за складирање на податоци (физичко и во облак), одржување редовни резервни копии и правилно бришење на податоците што повеќе не се потребни.
- **Правни рамки:** Преглед на главните закони за заштита на податоците – на пример, GDPR (Општа регулатива за заштита на податоците) како водечка рамка во Европа и [Вметнете ја регулативата за заштита на податоците на вашата земја тука]. Клучните

обврски вклучуваат добивање информирана согласност за собирање податоци, обезбедување на лични податоци преку технички и организациски мерки и барања за известување за прекршување.

- **Етичко ракување со податоци:** Надвор од законските правила, нагласување на етичката одговорност за заштита на приватноста на поединците. Дискусија за последиците од кршење на податоците за граѓанските организации, вклучувајќи штета на корисниците, губење на довербата, законски казни и оштетување на угледот.
- **Вградување на усогласеноста во пракса:** Како граѓанските организации можат да развијат едноставни политики за приватност, упатства за ракување со податоци и да обучат персонал за овие политики. Вовед во концепти како службеници за заштита на податоци (доколку се релевантни) или договори за ракување со податоци при работа со партнери.

Примери за активности или вежби:

- **Вежба за ревизија на податоци:** Учесниците ги набројуваат видовите лични податоци што ги собира или ракува нивната ГО и мапираат каде се складираат тие податоци (бази на податоци, табеларни пресметки, е-пошта, услуги во облак). Потоа дискутираат за секоја ставка: кој има пристап, како е заштитен во моментов и какви било празнини што ги забележуваат.
- **Демо за енкрипција:** Обучувачот демонстрира шифрирање на примерок од датотека или папка (или користење на алатка за шифрирање за е-пошта/текстуални пораки). Учесниците учат како изгледаат шифрираните податоци и вежбаат шифрирање и дешифрирање на дел од тест податоците, нагласувајќи ја важноста на управувањето со клучеви/лозинки.
- **Преглед на политиката:** Обезбедете образец или пример за едноставна Политика за заштита на податоци или Известување за приватност. Во мали групи, учесниците идентификуваат како овој документ ги опфаќа барањата на GDPR и разгледуваат какви промени би биле потребни за да се усогласат со [Вметнете ја регулативата за заштита на податоци на вашата земја овде]. Секоја група може да презентира една клучна точка што би ја вклучила во политиката на својата граѓанска организација.
- **Дискусија за правна усогласеност:** Прегледајте ја листата за проверка на активности за усогласеност со GDPR (на пр., назначување одговорно лице, поседување формулари за согласност, план за повреда на податоци). Учесниците дискутираат кои ставки од листата ги имаат воспоставено, а кои треба да ги спроведат. Нагласете ги сите дополнителни чекори што ги бара националното законодавство (на пр. регистрирање кај орган за заштита на податоци доколку е потребно според [Вметнете ја регулативата за заштита на податоци на вашата земја овде]).

Студија на случај за Модул 5: Пробивање на базата на податоци на донатори

Контекст: Меѓународна хуманитарна организација одржува база на податоци со информации за донаторите (имиња, контакт информации, историја на донации) и податоци за корисниците (чувствителни здравствени информации). Податоците се чуваат на внатрешен мрежен диск достапен за персоналот на програмата.

Проблем: За време на надградба на системот, администратор случајно ја откри папката со базата на податоци на донаторите на врска за споделување датотеки во јавен облак без енкрипција или контрола на пристап. Хакер ја откри врската и ја презеде целата листа на донатори. Личните податоци на илјадници донатори (имиња, е-пошта и износи на донации) беа објавени на интернет. Организацијата за заштита на лични податоци (ГЗО) беше принудена да ги извести донаторите за прекршувањето на правилата, како што е пропишано со закон. Неколку донатори ја повлекоа поддршката, наведувајќи ја загубата на доверба. ГЗО, исто така, се соочи со критики поради тоа што не ги обезбеди податоците правилно.
Исход: По пробивот, Организациската организација за заштита на податоци ги ревидираше своите практики за ракување со податоци. Ги шифрираше сите чувствителни податоци во мирување и во пренос, и го ограничи пристапот до базата на податоци со спроведување силни контроли за пристап. Тие, исто така, применија минимизирање на податоците со отстранување на непотребни лични податоци од јавните досиеја. Организациската организација за заштита на податоци назначи службеник за заштита на податоци за да ја надгледува усогласеноста и да изготви јасна политика за приватност. На персоналот му беше дадена обука за правилно ракување со податоци, а идното споделување се вршеше со безбедни врски и лозинки. Организациската организација за заштита на податоци ја врати довербата кај своите донатори со брзо заострување на безбедноста и транспарентно известување за подобрувањата.

Прашања за дискусија:

ои пропусти во заштитата на податоците доведоа до ова кршење на правилата и како можеа да се спречат?
ои практики за заштита на податоци (од темите на овој модул) ги усвои граѓанската организација по инцидентот?
ои законски обврски ги имаше ГО за да се справи со ова прекршување и зошто усогласеноста е важна за ГО?

Модул 5 Проценка
Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 5 Проценка

Кратки прашања

акви видови лични или чувствителни податоци најчесто собираат граѓанските организации и зошто овие податоци мора да бидат заштитени?
бјаснете го принципот на минимизирање на податоците и наведете еден практичен пример за тоа како една граѓанска организација може да го примени.
оја е разликата помеѓу шифрирање на податоци во мирување и шифрирање на податоци во транзит?

поред GDPR (или еквивалентни национални закони за заштита на податоци), што треба да направи една граѓанска организација во случај на повреда на лични податоци?
ошто е важно етичкото ракување со податоци за граѓанските организации, покрај усогласеноста со законските одредби? Наведете една потенцијална последица од несоодветната заштита на податоците.

Практична задача: Мини преглед на заштитата на податоците

Од учесниците се бара да ја извршат следната задача:

- Идентификување еден вид лични или чувствителни податоци собрани од нивната ГО (на пр., евиденција за корисници, контакт информации за донатори, информации за персоналот).
- Накратко да опишат:
  аде се складираат овие податоци (на пр. компјутер, услуга во облак, е-пошта, хартиени датотеки),
  ој има пристап до тоа,
  дно подобрување што може да се направи за подобра заштита на овие податоци (на пр. енкрипција, ограничен пристап, минимизирање на податоците).

Учесниците треба да ги презентираат своите одговори во три до пет кратки точки или накратко да ги дискутираат во мали групи.

3.5 МОДУЛ 5: ЗАШТИТА НА ПОДАТОЦИ И УСОГЛАСЕНОСТ СО ПРАВИЛАТА ЗА ПРИВАТНОСТ – ЗАШТИТА НА ПОДАТОЦИТЕ И РАЗБИРАЊЕ НА ЗАКОНСКИТЕ ОБВРСКИ

До крајот на овој модул, учесникот ќе може да:

и идентификува чувствителните податоци што ги собира ГО и да објасни зошто тие мора да бидат заштитени.

рименува клучни практики за заштита на податоци (минимизирање на податоци, енкрипција, безбедно складирање, редовни резервни копии и безбедно отстранување).

и разбира и објаснува законските обврски на ГО според законите за заштита на податоци (како што е GDPR) и како да се обезбеди усогласеност.

Цели на учење:

- Препознавање на видовите чувствителни податоци (на пр. лични информации за корисниците, евиденција за донаторите) што ги собираат граѓанските организации и зошто е клучно да се заштитат таквите податоци.
- Применување на клучните принципи за заштита на податоците – вклучувајќи минимизирање на податоците, енкрипција (за податоци што се во мирување и во пренос), безбедно складирање/резервна копија и правилно отстранување на податоците – за подобрување на приватноста и безбедноста.
- Разбирање на законските обврски и рамки за заштита на податоците, како што се GDPR на ЕУ и еквивалентните национални закони за заштита на податоците, и како да се обезбеди дека граѓанската организација за заштита на податоците се придржува до овие регулативи.

Клучни теми:

- **Идентификување чувствителни податоци:** Што се смета за лични или чувствителни податоци во контекст на граѓанска организација (имиња, адреси, информации за здравјето или правниот случај итн.) и ризиците доколку таквите податоци протекуваат.
- **Принципи за заштита на податоци:** Практични чекори за минимизирање на податоците (собирање само на она што е навистина потребно), шифрирање на податоците во мирување (на пр., датотеки на дискови) и во пренос (користење SSL/HTTPS за пренос на податоци), безбедни решенија за складирање на податоци (физичко и во облак), одржување редовни резервни копии и правилно бришење на податоците што повеќе не се потребни.
- **Правни рамки:** Преглед на главните закони за заштита на податоците – на пример, GDPR (Општа регулатива за заштита на податоците) како водечка рамка во Европа и [Вметнете ја регулативата за заштита на податоците на вашата земја овде]. Клучните обврски вклучуваат добивање информирана согласност за собирање податоци, обезбедување лични податоци преку технички и организациски мерки и барања за известување за прекршување.
- **Етичко ракување со податоци:** Надвор од законските правила, нагласување на етичката одговорност за заштита на приватноста на поединците. Дискусија за

последиците од кршење на податоците за граѓанските организации, вклучувајќи штета на корисниците, губење на довербата, законски казни и оштетување на угледот.

- **Вградување на усогласеноста во пракса:** Како граѓанските организации можат да развијат едноставни политики за приватност, упатства за ракување со податоци и да обучат персонал за овие политики. Вовед во концепти како службеници за заштита на податоци (доколку се релевантни) или договори за ракување со податоци при работа со партнери.

Примери за активности или вежби:

- **Вежба за ревизија на податоци:** Учесниците ги набројуваат видовите лични податоци што ги собира или ракува нивната ГО и мапираат каде се складираат тие податоци (бази на податоци, табеларни пресметки, е-пошта, услуги во облак). Потоа дискутираат за секоја ставка: кој има пристап, како е заштитен во моментов и какви било празнини што ги забележуваат.
- **Демо за енкрипција:** Обучувачот демонстрира шифрирање на примерок од датотека или папка (или користење алатка за шифрирање за е-пошта/текстуални пораки). Учесниците учат како изгледаат шифрираните податоци и вежбаат шифрирање и дешифрирање на дел од тест податоците, нагласувајќи ја важноста на управувањето со клучеви/лозинки.
- **Преглед на политиката:** Обезбедете образец или пример за едноставна Политика за заштита на податоци или Известување за приватност. Во мали групи, учесниците идентификуваат како овој документ ги опфаќа барањата на GDPR и разгледуваат какви промени би биле потребни за да се усогласат со [Вметнете ја регулативата за заштита на податоци на вашата земја овде]. Секоја група може да презентира една клучна точка што би ја вклучила во политиката на својата граѓанска организација.
- **Дискусија за правна усогласеност:** Прегледајте ја листата за проверка на активности за усогласеност со GDPR (на пр. назначување одговорно лице, поседување формулари за согласност, план за повреда на податоци). Учесниците дискутираат кои ставки од листата ги имаат воспоставено, а кои треба да ги спроведат. Нагласете ги сите дополнителни чекори што ги бара националното законодавство (на пр., регистрирање кај орган за заштита на податоци доколку е потребно според [Вметнете ја регулативата за заштита на податоци на вашата земја овде]).

Студија на случај за Модул 5: Пробивање на базата на податоци на донатори

Контекст: Меѓународна хуманитарна организација одржува база на податоци со информации за донаторите (имиња, контакт информации, историја на донации) и податоци за корисниците (чувствителни здравствени информации). Податоците се чуваат на внатрешен мрежен диск достапен за персоналот на програмата.

Проблем: За време на надградба на системот, администратор случајно ја откри папката со базата на податоци на донаторите на врска за споделување датотеки во јавен облак без енкрипција или контрола на пристап. Хакер ја откри врската и ја презеде целата листа на донатори. Личните податоци на илјадници донатори (имиња, е-пошта и износи на донации) беа објавени на интернет. Организацијата за заштита на лични податоци (ГЗО)

беше принудена да ги извести донаторите за прекршувањето на правилата, како што е пропишано со закон. Неколку донатори ја повлекоа поддршката, наведувајќи ја загубата на доверба. ГЗО, исто така, се соочи со критики поради тоа што не ги обезбеди податоците правилно.

Исход: По пробивот, Организациската организација за заштита на податоци ги ревидираше своите практики за ракување со податоци. Ги шифрираше сите чувствителни податоци во мирување и во пренос, и го ограничи пристапот до базата на податоци со спроведување силни контроли за пристап. Тие, исто така, применија минимизирање на податоците со отстранување на непотребни лични податоци од јавните досиеја. Организациската организација за заштита на податоци назначи службеник за заштита на податоци за да ја надгледува усогласеноста и изготви јасна политика за приватност. На персоналот му беше дадена обука за правилно ракување со податоци, а идното споделување се вршеше со безбедни врски и лозинки. Организациската организација за заштита на податоци ја врати довербата кај своите донатори со брзо заостручање на безбедноста и транспарентно известување за подобрувањата.

Прашања за дискусија:

ои пропусти во заштитата на податоците доведоа до ова кршење на правилата и како можеа да се спречат?

ои практики за заштита на податоци (од темите на овој модул) ги усвои граѓанската организација по инцидентот?

ои законски обврски ги имаше ГО за да се справи со ова прекршување и зошто усогласеноста е важна за ГО?

Модул 5 Проценка

Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 5 Проценка

Кратки прашања

акви видови лични или чувствителни податоци најчесто собираат граѓанските организации и зошто овие податоци мора да бидат заштитени?

бјаснете го принципот на минимизирање на податоците и наведете еден практичен пример за тоа како една граѓанска организација може да го примени.

оја е разликата помеѓу шифрирање на податоци во мирување и шифрирање на податоци во транзит?

поред GDPR (или еквивалентни национални закони за заштита на податоци), што треба да направи една граѓанска организација во случај на повреда на лични податоци?

ошто е важно етичкото ракување со податоци за граѓанските организации, покрај усогласеноста со законските одредби? Наведете една потенцијална последица од несоодветната заштита на податоците.

Практична задача: Мини преглед на заштитата на податоците

Од учесниците се бара да ја извршат следната задача:

- Да идентификуваат еден вид лични или чувствителни податоци собрани од нивната ГО (на пр. евиденција за корисници, контакт информации за донатори, информации за персоналот).
- Накратко да опишат:

  аде се складираат овие податоци (на пр. компјутер, услуга во облак, е-пошта, хартиени датотеки),

  ој има пристап до тоа,

  дно подобрување што може да се направи за подобра заштита на овие податоци (на пр. енкрипција, ограничен пристап, минимизирање на податоците).

Учесниците треба да ги презентираат своите одговори во три до пет кратки точки или накратко да ги дискутираат во мали групи.

3.6 МОДУЛ 6: БЕЗБЕДНОСТ НА СОЦИЈАЛНИТЕ МЕДИУМИ И ОНЛАЈН ПРИСУСТВО – ЗАШТИТА НА ОРГАНИЗАЦИСКАТА РЕПУТАЦИЈА И НА СМЕТКИТЕ

До крајот на овој модул, учесникот ќе може да:

рименува безбедносни мерки за заштита на сметките на социјалните медиуми на ГО (силни, уникатни лозинки, двофакторска автентикација, ограничени администраторски улоги).

фикасно да реагира на инциденти на социјалните медиуми (киднапирање на сметка или лажно претставување) преку следење на процедурите за пријавување и комуникација.

мплементира најдобри практики за одржување на безбедно онлајн присуство (редовни ажурирања на веб-страницата/CMS, упатства за персоналот за објавување и реагирање на дезинформации).

Цели на учење:

- Спроведување безбедносни мерки за заштита на сметките на социјалните медиуми на ГО (силна автентикација, следен пристап, редовни ревизии на поставките на сметката).
- Развивање стратегии за заштита на онлајн присуството и репутацијата на организацијата, вклучително и како да се одговори на напади со киднапирање на сметка, лажно претставување или дезинформации.
- Применување најдобри практики за управување со содржината на веб-страницата и однесување на персоналот онлајн за да се обезбеди доследно и безбедно претставување на организацијата на интернет.

Клучни теми:

- **Безбедност на профилот на социјалните медиуми:** Обезбедување дека сите организациски сметки на социјалните медиуми користат силни, уникатни лозинки и

имаат овозможено двофакторско автентикација. Безбедно управување со повеќе администратори (користење контроли за пристап базирани на улоги или функции за тимска соработка, наместо споделување лозинки).

- **Следење и обновување на сметката:** Следење на активноста на сметката (за рано да се открие секој неовластен пристап) и познавање како да се вратат сметките ако се компромитирани (разбирање на процесите за поддршка на платформата за хакирани сметки).
- **Справување со киднапирање и лажно претставување:** Чекори што треба да се преземат ако сметката на граѓанска организација е хакирана или ако лажните сметки се претставуваат како граѓанска организација – вклучувајќи механизми за пријавување на социјалните платформи, комуникација со поддржувачите за разјаснување на дезинформациите и враќање на контролата врз сметките.
- **Справување со онлајн вознемирување и дезинформации:** Тактики за одговор на тролови или координирани кампањи за вознемирување (на пр., документирање на злоупотреба, користење функции за блокирање/пријавување, политика за модерирање на коментари). Како да се спротивставиме на дезинформациите или клеветите на интернет со фактички пораки без засилување на лажни тврдења.
- **Безбедност на веб-страницата и управувањето со содржини:** Одржување на безбедноста и на репутацијата на веб-страницата на ГО – редовно ажурирање на CMS/додатоците на веб-страницата, користење безбедни лозинки за администраторите на страницата, ограничување кој може да објавува содржина и воспоставување процес за брзо коригирање или отстранување на неточна или неовластена содржина.
- **Управување со репутација:** Обука на персоналот и волонтерите за упатствата за претставување на организацијата онлајн (политики за користење на лични социјални медиуми, што да не се објавува за работата, како да се реагира доколку видат дезинформации), со цел одржување на позитивно и безбедно онлајн присуство за ГО.

Примери за активности или вежби:

- **Проверка на безбедноста на сметката:**Учесниците вршат брза ревизија на сметките на социјалните медиуми на една од организациите за заштита на лични податоци (CSO). Тие потврдуваат дали е овозможен 2FA, дали лозинките се силни/неодамна ажурирани, дали информациите за контакт за обновување се точни и дали само овластени лица имаат пристап. Потоа креираат список на задачи за сите потребни подобрувања.
- **Играње улоги со инциденти:** Симулирајте сценарио каде што официјалниот профил на социјалните медиуми на граѓанска организација е хакиран или лажен профил шири лажни информации за организацијата. Тимот мора да одлучи за итен план за дејствување: кој ќе комуницира со јавноста, како да ја извести платформата и следбениците и кои чекори ќе бидат преземени за да се обезбеди или врати профилот. По играњето со улоги, дискутирајте што поминало добро и што би можело да се подобри во нивниот одговор.

- **План за одговор на вознемирување:** Во групи, учесниците изготвуваат едноставен протокол за справување со онлајн вознемирување или кампањи на омраза. Ова може да вклучува чекори како што се: не се вклучувајте јавно во гнев, документирајте ги навредливите објави, пријавете ги на платформата, известете го менаџментот на ГО и поддржете ги сите вработени кои се цел на тоа. Групите ги споделуваат своите планови и дискутираат за заедничките елементи.
- **Локална дискусија за пример:** [Опишете неодамнешен локален инцидент поврзан со социјалните медиуми во кој е вклучена граѓанска организација] – Анализирајте што се случило и како постоењето робусни практики за безбедност на социјалните медиуми и план за одговор на инциденти би можеле да помогнат во управувањето или спречувањето на таква ситуација.

Студија на случај од Модул 6: Киднапирање на профили на социјални медиуми
Контекст:Една граѓанска организација за животна средина користи социјални медиуми (Твитер и Фејсбук) за да ангажира донатори и да споделува новости од кампањата. Повеќе членови на персоналот имаат пристап до сметките со заеднички лозинки и никој не ја следи внимателно активноста за најавување.
Проблем: Едно утро, Твитер профилот на ГО почна да објавува провокативни политички пораки неповрзани со мисијата на ГО. Следбениците беа збунети, а некои ја обвинија ГО дека зазема политички став. Објавите беа дело на хакер, кој добил пристап откако еден член на персоналот повторно употребил заедничка лозинка. Додека персоналот го сфатил пробивот, пораките биле ретвитувани од поддржувачите, предизвикувајќи штета на угледот. Потребни беа часови за повторно добивање пристап преку процесот на поддршка на платформата, за кое време негативните впечатоци се шират на интернет.
Исход: Операторот за безбедност на информациите (ОК) реагираше на инцидентот со веднаш објавување разјаснување на сите канали, извинувајќи се за прекршувањето. Ги ресетираа сите лозинки на социјалните мрежи и овозможија двофакторска автентикација на сите сметки. Тие, исто така, поставија пристап базиран на улоги (доделувајќи специфични администраторски сметки наместо споделување лозинки). Персоналот ја прегледа и ја ажурира содржината на веб-страницата за да се осигури дека нема застарени информации. Операторот за безбедност воспостави политика за дневно следење на активноста на сметките. Како резултат на тоа, тие беа во можност да ја вратат нормалната комуникација, а подоцна дури и добија поддршка за транспарентност. Новите безбедносни мерки спречија понатамошни обиди за киднапирање.
Прашања за дискусија:

ои беа клучните неуспеси што дозволија да се случи киднапирањето на сметката?

ако реагираше ГО за да ја ублажи штетата, и технолошки и во комуникациите?

ои безбедносни подобрувања ги имплементираше CSO за да го заштити своето присуство на социјалните медиуми во иднина?

Модул 6 Проценка

Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 6 Проценка

Кратки прашања

ошто е важно граѓанските организации да користат силни, уникатни лозинки и двофакторска автентикација на сметките на социјалните медиуми?
акви ризици можат да произлезат од споделувањето лозинки за сметки на социјалните медиуми меѓу повеќе членови на персоналот?
ои итни чекори треба да ги преземе една граѓанска организација ако нејзината сметка на социјалните медиуми е хакирана или компромитирана?
ако онлајн дезинформациите или лажното претставување можат да влијаат на угледот и јавната доверба на една граѓанска организација?
ошто е важно да има јасни упатства за персоналот за онлајн однесување и претставување на организацијата?

Практична задача: Преглед на безбедноста на социјалните медиуми

Од учесниците се бара да ја извршат следната задача:

- Да изберат **еден официјален профил на социјалните мрежи** на нивната ГО (или хипотетичка ГО).
- Накратко да опишат:
  - али е овозможена двофакторска автентикација,
  - ако се управува пристапот моментално (споделени лозинки наспроти пристап базиран на улоги),
  - дна конкретна акција што би можела да ја подобри безбедноста или следењето на оваа сметка.

Учесниците треба да ги сумираат своите одговори **во три-пет кратки точки** или накратко дискутирајте ги во мали групи.

3.7 МОДУЛ 7: РАЗВИВАЊЕ НА БЕЗБЕДНОСНА КУЛТУРА – ОБУКА НА ПЕРСОНАЛОТ, ПОЛИТИКИ И РЕАГИРАЊЕ НА ИНЦИДЕНТИ

До крајот на овој модул, учесникот ќе може да:

егува култура на безбедност во организацијата преку ангажирање на раководството и персоналот.

азвива основни политики за ИТ безбедност (на пр., прифатлива употреба, BYOD, правила за лозинка) и планирајте редовна обука за безбедност за сите вработени.

оздаде и вежба едноставен план за одговор на инциденти (дефинирање на улоги, чекори и комуникација) за ефикасно справување со сајбер инциденти.

Цели на учење:

- Негување култура на безбедносно свесна личност во рамките на ГО, каде што секој член на персоналот ја разбира својата лична улога во одржувањето на сајбер безбедноста.
- Развивање основни политики за ИТ безбедност (на пр., прифатлива употреба на технологија, правила „донесете го вашиот сопствен уред“) и имплементирајте редовни програми за обука на персоналот за зајакнување на добрите безбедносни практики.
- Воспоставување и вежбање план за одговор на инциденти за да може организацијата ефикасно да реагира на инциденти со сајбер безбедност (јасно дефинирајќи ги чекорите, улогите и комуникациските канали).

Клучни теми:

- **Градење култура на сајбер безбедност:** Како да се добие согласност од раководството и ангажман на персоналот за безбедносни иницијативи. Создавање средина каде што вработените се чувствуваат одговорни за заштитата на податоците и системите, наместо да ја гледаат безбедноста исклучиво како работа на ИТ лицето.
- **Основни безбедносни политики:** Изготвување едноставни, јасни политики што поставуваат очекувања за безбедно користење на технологијата. Примерите вклучуваат Политика за прифатлива употреба (што е дозволено/забрането на работните уреди и сметки), упатства за донесување на сопствени уреди (BYOD) доколку персоналот користи лични уреди за работа и правила за креирање и управување со лозинки.
- **Континуирана свест и обука на персоналот:** Важноста на едукацијата за oCSO (работилници, билтени, тестови за симулација на фишинг) за одржување свежо знаење за безбедноста, забележувајќи дека редовната обука е од витално значење бидејќи необучениот персонал може да стане најслабата алка во безбедноста.
- **Планирање за одговор на инциденти:** Клучни компоненти на планот за одговор на инциденти – како да се открие и пријави инцидент, итни чекори за справување со проблемот (на пр. исклучување на засегнатите компјутери), улоги и одговорности

(кој го води одговорот, кој комуницира со засегнатите страни) и како да се одржат операциите во функција за време на прекини.

- **Известување и учење од инциденти:** Упатства за тоа кога и како да се пријават сајбер инциденти кај властите или регулаторите (особено ако се вклучени лични податоци) и спроведување преглед по инцидентот за подобрување на идната отпорност.

Примери за активности или вежби:

- **Работилница за пишување политики:** Учесниците креираат нацрт за една кратка безбедносна политика, релевантна за нивната организација за граѓански услуги (на пример, Политика за прифатлива употреба за канцелариски компјутери или Политика за мобилни уреди). Секоја група пишува неколку клучни правила, а потоа ги споделува со сите, барајќи повратни информации за да се осигури дека политиките се јасни и применливи.
- **Вежба за подигнување на безбедносната свест:** Организирајте симулирана вежба за фишинг или изненадувачко „пуштање на USB“ (оставајќи USB флеш драјв како да е пронајден, за да видите дали некој ќе го вклучи). Потоа, дискутирајте ги резултатите: како реагираше персоналот? Кои беа црвените знамиња? Искористете го ова како можност за учење за зајакнување на точките за обука во безбедна средина.
- **Маса за одговор на инциденти:** Презентирајте хипотетички инцидент со сајбер безбедност (на пр. напад со ransomware што ги криптира податоците на CSO). Нека тимот го разгледа својот одговор чекор по чекор: како го идентификуваат обемот на проблемот, кого прво повикуваат, како комуницираат со персоналот и евентуално со јавноста и како ги обновуваат системите или податоците? По вежбата, разговарајте за тоа што поминало добро и кои улоги или чекори треба да се разјаснат во нивниот план.
- **Информации за локално известување:** [Вметнете го механизмот за пријавување на сајбер инциденти во вашата земја или контактот на надлежниот орган овде] – Погрижете се учесниците да бидат свесни како да пријават сериозен инцидент на сајбер безбедност во нивниот локален контекст (на пример, известување на национален CERT или органи за спроведување на законот) и дискутирајте за сите законски барања за пријавување на прекршувања што важат за граѓанските организации во вашата земја.

Студија на случај од Модул 7: Необезбеден USB што води до појава на малициозен софтвер

Контекст: Канцеларијата на една граѓанска организација им дозволи на вработените да користат лични USB-уреди на работните компјутери. Немаше писмена политика или обука за употреба на преносливи медиуми. Еден нов волонтер често користеше сопствен USB-уред.

Проблем: Еден ден, еден член на персоналот пронашол USB-уред на паркингот во канцеларијата (веројатно некој го испуштил). Љубопитни, го вклучиле во нивниот канцелариски компјутер и отвориле документ на него. Тој USB-уред бил заразен со малициозен софтвер. Малициозниот софтвер брзо се проширил низ мрежата на CSO, криптирајќи датотеки на повеќе компјутери. Податоците на CSO биле недостапни, а

операциите биле прекинати. Недостатокот на план за одговор на инциденти предизвикал конфузија: никој не знаел кој ќе го води одговорот или кого да извести.
Исход: Откако ја локализираше епидемијата со исклучување на засегнатите машини, CSO ангажираше ИТ специјалист за да ги врати податоците од неодамнешните резервни копии. Тие сфатија дека резервните копии помогнаа во враќањето на повеќето податоци. Потоа, CSO имплементираше строги политики: беше напишана формална Политика за прифатлива употреба (со која се забранува употреба на неодобрени USB-дискови и се бара скенирање на кој било надворешен медиум), а целиот персонал помина обука за препознавање на сомнителни уреди и приклучоци. Тие исто така развија едноставен план за одговор на инциденти, назначувајќи тим за одговор и јасни чекори што треба да се следат во иден инцидент (вклучувајќи кого прво да се повика и како да се комуницира со засегнатите страни). Подоцна, за време на помал инцидент со фишинг, CSO успешно го локализираше користејќи го новиот план, минимизирајќи ја штетата.

Прашања за дискусија:

ои политики или практики недостасуваа што дозволија да се случи овој инцидент?
ако неодамнешните резервни копии и тимот за реагирање влијаеја врз исходот од инцидентот?
ои нови мерки и планови ги спроведе ГО по настанот и зошто се тие важни за спречување на идни инциденти?

Белешка за проценка на Модул 7
Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 7 Проценка

Кратки прашања

то значи „безбедносна култура“ во контекст на ГО и зошто вклучувањето на персоналот е од суштинско значење за нејзино градење?
ошто основните политики за ИТ безбедност (како што се политиките за прифатлива употреба или политиките за внесување на производи во системот) се важни за граѓанските организации?
ако можат редовните обуки на персоналот и активностите за подигнување на свеста да ги намалат ризиците од сајбер безбедноста во една организација?
ои се клучните елементи на едноставен план за одговор на инциденти за ГО?
ошто е важно да се разгледаат и да се учи од инцидентите поврзани со сајбер безбедноста откако ќе се случат?

Практична задача: Мини акционен план за безбедносна култура

Од учесниците се бара да ја извршат следната задача:

- Да идентификуваат една конкретна акција што нивната ГО би можела да ја преземе за да ја зајакне својата безбедносна култура (на пр. воведување едноставна Политика за прифатлива употреба, организирање годишна обука за безбедност или дефинирање лице за контакт за одговор на инциденти).
- Накратко да опишат:
  - ој би бил одговорен за оваа акција,
  - ако би им било соопштено на вработените,
  - ако тоа би помогнало во спречувањето или намалувањето на инцидентите поврзани со сајбер безбедноста.

Учесниците треба да ги презентираат своите одговори во три до пет кратки точки или накратко да ги дискутираат во мали групи.

3.8 МОДУЛ 8: НАПРЕДНИ ТЕМИ – НОВИ ЗАКАНИ И АЛАТКИ

До крајот на овој модул, учесникот ќе може да:

репознава софистицирани сајбер закани (како насочен фишинг и лажирање) и да применува методи за верификација (како што е потврдување на барања преку алтернативни канали).

оодветно да користи напредни безбедносни алатки (на пр. хардверски безбедносни клучеви за критични сметки, мрежно следење за аномалии, ресурси за разузнавање за закани).

ланира подобрувања на организациската безбедност (како што е распоредување менаџери за лозинки во претпријатијата или системи за откривање на упади) врз основа на капацитетот и потребите на организацијата за заштита на лични податоци.

Цели на учење:

- Запознавање со новите или софистицирани сајберзакани (како што се напредните техники на фишинг или напади со лажирање) и учење методи за верификација за да им се спротивставите на нив.
- Истражување напредни безбедносни алатки и практики што можат дополнително да ја подобрат заштитата, вклучувајќи безбедност базирана на хардвер (на пр. безбедносни клучеви), следење на мрежата и разузнавање за закани, прилагодени на потребите на организациите на граѓанскиот сектор.
- Размислување како да се имплементираат безбедносни подобрувања на ниво на целата организација, како што се менаџери за лозинки на претпријатието или

системи за откривање на упади, разбирајќи кога овие напредни мерки се соодветни за капацитетот на ГО.

Клучни теми:

- **Софистициран фишинг и лажирање:** Разбирање на напади од социјален инженеринг на високо ниво (измами на извршни директори, клонирани веб-страници итн.) и учење техники за проверка на комуникациите (на пример, проверка на сомнителни барања преку секундарен канал или користење на дигитални потписи).
- **Хардверски безбедносни клучеви:** Вовед во токени за физичка автентикација (како U2F/FIDO2 клучеви) како алтернатива на SMS или апликација 2FA,како тие функционираат за да спречат преземање на сметки (2FA отпорни на фишинг) и размислувања за нивно распоредување кај персоналот.
- **Мониторинг на мрежата и откривање на упади:** Основни концепти за тоа како една организација за заштита на лични податоци (CSO) може да ја следи својата мрежа за необични активности. Објаснување на алатки како системи за откривање на упади (IDS) или системи за спречување на упади (IPS) на едноставен начин и како тие ги алармираат администраторите за потенцијални прекршувања.
- **Безбедносни алатки за целата организација:** Имплементирање напредни алатки како што се менаџери за лозинки за целата организација (за да се обезбеди дека сите вработени користат силни, уникатни лозинки) или користење на информации за закани/известувања од заедницата за да се биде во тек со новите закани релевантни за граѓанското општество.
- **Прилагодување на вашиот контекст:** Нагласување дека овие напредни мерки се опционални и треба да се прилагодат на техничката експертиза и ресурсите на ГО. Упатство за тоа како да се одлучи кои напредни алатки вреди да се усвојат и обезбедување обучен персонал за нивно ефикасно користење.

Примери за активности или вежби:

- **Сценарио за фишинг со копје:** Фасилитаторот презентира пример за високо насочен обид за фишинг (на пример, е-пошта што изгледа како да е од познат финансиер со кој се бара трансфер). Учесниците вежбаат чекор за верификација (како јавување на официјалниот телефонски број на испраќачот или проверка на заглавието на е-поштата) наместо да одговараат преку е-пошта. Дискутирајте како овој пристап може да спречи софистицирани измами.
- **Демонстрација на хардверски клуч:** Учесниците можат да видат или да пробаат хардверски безбедносен клуч. Обучувачот води низ процесот на регистрирање на клучот на сметката, а потоа и низ процесот на најавување со клучот. Доколку е можно, дозволете им на волонтерите да го пробаат процесот на демо сметка за да разберат како функционираат овие уреди и да ги истакнат нивните безбедносни придобивки.
- **Мини лов на закани:** Обезбедете поедноставен мрежен дневник или пример за известување од хипотетички систем за откривање на упади (IDS). Учесниците нека ги испитаат записите за да забележат нешто сомнително (на пр. непозната IP-адреса

што прави повеќекратни обиди за најавување во непарни часови). Ова дава претстава за тоа како алатките за следење на мрежата можат да откријат аномалии.

- **Дискусија за локална релевантност:** [Вметнете пример за напредна закана или алатка за сајбер безбедност што привлече внимание во вашата земја] – Дискутирајте дали оваа закана или алатка е нешто за што ГО треба да биде загрижена или да размисли да го користи. Како локалните ресурси (како што се националните CSIRT совети или заедниците за сајбер безбедност) можат да ѝ помогнат на ГО да се справи со ваквите напредни закани?

Студија на случај од Модул 8: Спречен обид за измама од извршен директор

Контекст: Една граѓанска организација управуваше со голем проект за грантови со повеќе меѓународни донатори. Вработените имаат искуство во основната безбедност, но не се справувале со високо насочени напади. Организацијата неодамна воведе хардверски безбедносни клучеви за менаџерите на клучеви и разгледа напредни безбедносни алатки.

Проблем: Финансискиот службеник на CSO добил итна е-пошта наводно од извршниот директор, со која се бара голем банкарски трансфер до нов добавувач за материјали за проектот. Е-поштата изгледала легитимно, без очигледни знаци на фишинг. Службеникот се спремал да продолжи кога се сетиле да го потврдат барањето. Го повикале директорот во канцеларијата. Директорот, изненаден, рекол дека не испратил никакаква е-порака. Веднаш сфатиле дека станува збор за софистициран обид за лажирање на е-пошта (измама на извршен директор). Бидејќи за сметките на директорот биле поставени хардверски безбедносни клучеви, напаѓачот не го компромитирал најавувањето на директорот; тоа било целосно лажна е-пошта.

Исход: Персоналот на CSO ги блокираше сите понатамошни е-пораки од адресата на напаѓачот и го пријави обидот за измама. За да се спречат идните обиди, CSO одржа брифинг за проверка на необични барања (користејќи посебни канали) и ја ажурираше својата листа за проверка за одговор на инциденти за да вклучи чекори за сомневање за фишинг. Тие, исто така, одлучија пошироко да ги воведат безбедносните клучеви за сметки со високи привилегии. Благодарение на овие мерки, CSO избегна каква било финансиска загуба и ја зголеми довербата на персоналот дека напредните фишинг напади можат да се откријат и спречат.

Прашања за дискусија:

ако ГО го откри и спречи обидот за измама пред да се изгубат средствата?

аква улога играа безбедносните клучеви на хардверот и постапката за верификација во ова сценарио?

ои напредни безбедносни подобрувања (од овој модул) одлучи CSO да ги имплементира како резултат на овој инцидент?

Модул 8 Проценка

Овој модул ќе биде оценет со пет кратки прашања и една мала задача. За положување е потребен минимален резултат од 70%.

Модул 8 Проценка

Кратки прашања

то ги прави напредните фишинг или лажни напади поопасни од основните обиди за фишинг?
то е измама на извршни директори и зошто граѓанските организации се особено ранливи на овој вид напад?
о што се разликуваат хардверските безбедносни клучеви од традиционалните методи за двофакторска автентикација и зошто се сметаат за отпорни на фишинг?
оја е целта на системите за мониторинг на мрежата или за детекција на упади во една организација?
ошто граѓанските организации треба внимателно да ги проценат своите капацитети и потреби пред да имплементираат напредни безбедносни алатки?

Практична задача: Напредна проверка на подготвеност за закана

Од учесниците се бара да ја извршат следната задача:

- Идентификувајте **една напредна закана** релевантна за нивниот CSO (на пр. измама од извршен директор, подложност на фишинг, лажирање на сметки).
- Накратко опишете:
  ден чекор за верификација што треба да го преземе персоналот пред да дејствува по сомнителни барања,
  дна напредна безбедносна алатка или практика што би можела да помогне во намалувањето на ризикот (на пр. хардверски безбедносни клучеви, менаџери за лозинки, процедури за верификација),
  или оваа мерка е изводлива за нивната ГО во моментов и зошто.

Учесниците треба да ги презентираат своите одговори во три до пет кратки точки или накратко да ги дискутираат во мали групи.

4. ПРАВНИ И РЕГУЛАТОРНИ РАМКИ ЗАСНОВАНИ НА ДРЖАВАТА

4.1 Правна и регулаторна рамка во Турција и предлози за граѓанските организации во Турција

Опсег на Законот за заштита на лични податоци (KVKK) и неговото влијание врз граѓанските организации

Законот бр. 6698 за заштита на лични податоци (KVKK) е примарното законодавство што ја регулира обработката на лични податоци во Турција. Законот се однесува на сите физички и правни лица кои обработуваат лични податоци, вклучувајќи ги јавните институции, организациите од приватниот сектор и организациите на граѓанското општество (ОЗО) (Одговор за заштита на лични податоци [KVKK], 2020).

ГО обично собираат и обработуваат лични податоци поврзани со нивните членови, волонтери, донатори и вработени. Таквите податоци може да вклучуваат имиња, контакт информации, фотографии, износи на донации и евиденција за учество на настани. Затоа, ГО имаат и обврски како контролори на податоци според KVKK.

Според Законот, личните податоци можат да се обработуваат само за специфични, експлицитни и легитимни цели и мора да се избришат или анонимизираат откако ќе престане целта на обработката. Граѓанските организации мора да дејствуваат во согласност со овие принципи во сите процеси на собирање податоци, од формулари за членство до дигитални кампањи.

Чекори што граѓанските организации мора да ги преземат за да се усогласат со KVKK

Главните чекори што треба да ги следат граѓанските организации за да обезбедат усогласеност со KVKK вклучуваат:

одготовка на инвентар на податоци: ГО треба да идентификуваат и документираат кои лични податоци ги обработуваат, за кои цели, колку долго се чуваат податоците и со кого се споделуваат.

обивање експлицитна согласност: За активностите за обработка кои не се законски обврзувачки (на пр. промотивни е-пораки) мора да се добие експлицитна согласност. Согласноста мора да биде слободно дадена, информирана и отповиклива во секое време.

бврска за информации: Поединците чии лични податоци се собираат мора да бидат писмено информирани за тоа кој ги обработува нивните податоци, за кои цели, врз кои законски основи и кои се нивните права.

ерки за безбедност на податоците: Мора да се спроведат физички (заклучени кабинети), дигитални (енкрипција, антивирусен софтвер, ограничувања на пристап) и организациски (договори за доверливост, обука за подигање на свеста) мерки.

егистрација на VERBIS: Граѓанските организации чии активности се ограничени исклучиво на нивните членови, волонтери и донатори се ослободени од регистрација во VERBIS. Сепак, граѓанските организации со економско претпријатие се должни да се регистрираат во системот (KVKK, 2020).

Прекршувања и санкции на KVKK

КВКК предвидува административни казни, а во некои случаи и кривични санкции во случај на прекршувања (КВКК, 2020). Доколку граѓанските организации не ги исполнат своите обврски за безбедност на податоците, тие може да се соочат со значителни казни во случаи на прекршување на податоците, неовластено споделување на податоци или непријавување на прекршоци.

Од 2024 година, административните казни се движат од 25.000 TL (569 американски долари) до 1.800.000 TL, во зависност од природата на прекршокот. На пример, нерегистрирањето во VERBIS од страна на граѓанска организација која е предмет на обврска за регистрација претставува сериозен прекршок.

Управниот одбор на КВКК, исто така, воведе санкции врз граѓанските организации. Во 2020 година, едно здружение беше казнето по жалба за неовластена СМС комуникација, бидејќи не даде експлицитна согласност и не ги избриша личните податоци. Ова покажува дека граѓанските организации се предмет на ревизии и мерки за спроведување согласно законот.

Закон за сајбер безбедност и обврски за известување

Законот бр. 7545 за сајбер безбедност стапи на сила во 2025 година и ги опфаќа сите институции што обезбедуваат услуги во дигитални средини, без разлика помеѓу јавни и приватни субјекти (Службен весник, 2024). Во оваа рамка, граѓанските организации се исто така предмет на обврски за известување за инциденти.

Во случај на повреда на податоци, инфекција со малициозен софтвер, сајбер напад или идентификување на критична ранливост во системите на организацијата за граѓански организации, инцидентот мора да се пријави до Дирекцијата за сајбер безбедност поврзана со турското претседателство во рок од максимум 48 часа.

Непочитувањето може да резултира со административни казни почнувајќи од 1.000.000 лири, а во одредени случаи и со кривични санкции како што е затворска казна за одговорните лица. Оваа регулатива воспоставува фундаментална обврска за безбедност и транспарентност за сите граѓански организации.

Национална стратегија за сајбер безбедност и улогата на граѓанските организации

Националната стратегија и акциониот план за сајбер безбедност 2024–2028 е главниот документ што ја дефинира визијата на Турција за дигитална безбедност. Документот им доделува специфични улоги на јавните институции, приватниот сектор и граѓанските организации (Министерство за транспорт и инфраструктура, 2023).

Клучните очекувања за граѓанските организации вклучуваат подигање на јавната свест, промовирање на индивидуална писменост за дигитална безбедност и спроведување активности за дигитална писменост за ранливи групи како што се децата и постарите лица.

Понатаму, стратегијата ја нагласува важноста на учеството на граѓанското општество и ги охрабрува граѓанските организации да спроведуваат кампањи и обуки во соработка со јавните институции.

Правен статус на дигиталните алатки

Како дел од дигиталната трансформација, од граѓанските организации може да се бара да користат одредени дигитални алатки. Според Законот бр. 5070 за електронски потписи, електронските потписи имаат иста правна важност како и рачно напишаните потписи. Затоа, одлуките на одборот, договорите и официјалната кореспонденција може да се потпишуваат електронски (Управа за информациски и комуникациски технологии,

Граѓанските организации со економско претпријатие или кои надминуваат одредени прагови на обрт може да бидат предмет на обврски за е-фактура (е-Фатура) и е-архива (е-

Аршив). Управата за приходи објавува годишни соопштенија во кои ги наведува применливите прагови (Управа за приходи, 2024).

Регистрираната електронска пошта (КЕР) е уште еден преферирани метод за официјални известувања, особено за да се обезбеди правна важност. При користењето на сите овие алатки, граѓанските организации мора да обезбедат не само техничка соодветност, туку и целосна усогласеност со релевантната законска рамка.

Дигитална безбедност за мали и средни граѓански организации во Турција

Вовед

Следните пет оригинални случаи се подготвени за цели на обука и се засноваат на реални дигитални безбедносни ризици и искуства на мали и средни организации на граѓанското општество (ГО) кои работат во Турција. Секој случај јасно ја претставува структурата на ГО, доживеаниот инцидент, вклучената техничка или човечка ранливост, последиците и лекциите што можат да се извлечат за другите ГО. Сите ГО се претставени анонимно во оваа студија.

ЛОКАЛНИ СТУДИИ НА СЛУЧАЈ ОД ТУРЦИЈА

Случај 1: Главоболка предизвикана од лажна стапица за е-пошта

Оваа граѓанска организација е мала образовна асоцијација која работи само со четири вработени и неколку волонтери, со цел да обезбеди стипендии и образовна поддршка за локалните студенти. Нејзините дигитални операции се потпираат главно на комуникација преку е-пошта, канцелариски софтвер и координација со волонтери преку WhatsApp. Организацијата нема посветен член на ИТ персоналот, а вработените генерално ги користат своите лични лаптопи за работа.

„Еден ден, во сандачето за општи информации на здружението пристигнува е-пошта со наслов „Грант за образование од Министерството“. Во пораката се тврди дека на организацијата ѝ е доделен грант за кој аплицирала и се бара да се отвори прикачената PDF-датотека за повеќе детали. Возбуден од веста, службеникот на проектот ја презема и ја отвора прикачената датотека без да ја потврди нејзината автентичност. Датотеката не се отвора правилно, но на компјутерот е тивко инсталиран малициозен софтвер“.

Главната ранливост во овој случај е човечката грешка и недостатокот на свест. Вработениот не поминал обука за сајбер безбедност и не успеал внимателно да ја испита адресата на испраќачот, јазичните грешки и сомнителниот прилог. Ова беа јасни индикатори за фишинг е-пошта дизајнирана да се претстави како официјална институција.

Во рок од еден ден, споделените е-поштенски сметки што ги користеле службеникот на проектот и одборот биле компромитирани. Напаѓачите испраќале лажни пораки со барање пари до донатори и партнери. Комуникацијата била нарушена, довербата била разнишана, а некои поддржувачи привремено го прекинале својот

ангажман. На среден рок, организацијата морала да инвестира време и труд за да го врати кредибилитетот и внатрешниот морал.

Научени лекции и препораки

Фишинг нападите се едни од најчестите сајбер-закани за граѓанските организации. Сите вработени и волонтери треба да бидат обучени да идентификуваат сомнителни е-пораки. Адресите на испраќачите, прилозите и итните барања секогаш треба да се проверуваат. Треба да се имплементираат основни практики за сајбер-хигиена и двофакторска автентикација за критични сметки.

Случај 1: Главоболка предизвикана од лажна стапица за е-пошта

Релевантен(и) модул(и)

- Модул 4: Чести сајбер-закани (фишинг и малициозен софтвер)
- Модул 5: Заштита на податоци и усогласеност со прописите за приватност
- Модул 7: Развивање на безбедносна култура

Како овој случај може да се користи во обуката

- **Пример за подигање на свеста (Модул 4):**
  Овој случај може да се претстави на почетокот на модулот како реално сценарио за фишинг насочено кон мали граѓански организации. Обучувачите можат да ги замолат учесниците да идентификуваат црвени знамиња во е-поштата (адреса на испраќачот, прилог, итност, јазични грешки) пред да го откријат исходот.
- **Дискусија за човечки грешки (Модул 7):**
  Користете го овој случај за да нагласите дека сајбер безбедноста не е само техничко прашање, туку и прашање на човековото однесување. Тој функционира добро како повод за дискусија за тоа зошто обуката на персоналот и на волонтерите е критична, особено во малите граѓански организации без ИТ персонал.
- **Рефлексија за безбедноста на сметката (Модул 5):**
  Случајот може да поддржи дискусија за заштита на е-пошта сметка, вклучувајќи двофакторска автентикација и управување со пристап, поврзувајќи ги фишинг нападите со пошироки ризици од заштита на податоците.

Предложен метод:
Групна дискусија + вежба „Што би направиле поинаку?“.

Случај 2: Преземање на сметка на социјалните медиуми

Овој случај вклучува граѓанска организација за права на жените со средна големина со приближно 20 членови на персоналот и волонтери. Организацијата активно користи платформи на социјалните медиуми како што се Instagram, X (порано Twitter) и Facebook за застапување и јавно ангажирање. Сметките главно ги управува службеник за комуникации, иако волонтерите повремено придонесуваат. Не е овозможена двофакторска автентикација.

Едно утро, на официјалниот Инстаграм профил на организацијата се појавуваат необични објави. Профилната слика и биографијата се променети, а со следбениците се споделува измамничка содржина поврзана со инвестиции. Членовите и следбениците ја известуваат организацијата дека профилот е хакиран.

Службеникот за комуникации ја користел истата лозинка на повеќе платформи. Нападот на податоците на друга услуга ја открил лозинката, дозволувајќи им на напаѓачите пристап до сметката на социјалните медиуми. Отсуството на двофакторска автентикација дополнително го олесни преземањето. Дополнително, на организацијата ѝ недостасувал однапред дефиниран план за одговор на кризи.

Сметката беше привремено суспендирана додека беа започнати процедурите за обновување. Следбениците беа предупредени преку алтернативни канали. Иако пристапот на крајот беше вратен, дојде до оштетување на репутацијата, а некои следбеници ја изгубија довербата. Како одговор на тоа, организацијата ги зајакна политиките за лозинки и активираше двофакторска автентикација.

Научени лекции и препораки

Сметките на социјалните медиуми се чести мети на сајбер напади. Силните, уникатни лозинки и двофакторската автентикација се од суштинско значење. Треба да се избегнува повторната употреба на лозинки, а персоналот што управува со социјалните медиуми треба да добие целна обука за подигање на свеста за безбедноста.

Случај 2: Преземање на сметка на социјалните медиуми

Релевантен(и) модул(и)

- **Модул 6: Социјални медиуми и безбедност на онлајн присуство**
- **Модул 7: Развивање на безбедносна култура**

Како овој случај може да се користи во обуката

- **Основна студија на случај (Модул 6):**
  Овој случај е идеален како примарна студија на случај при предавање безбедност на социјалните медиуми. Обучувачите можат да ги водат учесниците низ инцидентот чекор по чекор и да ги мапираат неуспесите со недостасувачките контроли (повторна употреба на лозинка, без 2FA, без план за одговор).
- **Вежба за одговор на инциденти (Модул 7):**
  Случајот може да се трансформира во сценарио со играње улоги каде што учесниците одлучуваат како да комуницираат со следбениците, да го пријават пробивот на платформата и да ја вратат сметката.
- **Дискусија за целна обука:**
  Нагласете дека персоналот одговорен за комуникација и застапување има потреба од специјализирана безбедносна свест, а не само општа обука.

Предложен метод:
Анализа на случај + играње улоги при одговор на инциденти.

Случај 3: Цената на губењето на податоци и недостатокот на резервни копии

Вид, обем и дигитални работни практики на граѓанските организации

Овој случај се однесува на мала граѓанска организација за животна средина со тројца вработени со полно работно време и неколку волонтери. Проектните документи се подготвуваат на лични лаптопи и се споделуваат преку услуги во облак. Сепак, критичните податоци како што се листите на донатори и финансиските записи се чуваат само на десктоп компјутерот на директорот, без редовни резервни копии.

По прекин на струја, компјутерот на директорот не може да се рестартира поради оштетување на тврдиот диск. Обидите за локално враќање на податоците се неуспешни, а се препорачуваат професионални услуги за враќање на податоци со висока цена без загарантиран успех.

Немаше сајбер напад; инцидентот е резултат на лошо управување со податоци и отсуство на стратегија за резервна копија. Складирањето на критични податоци на еден уред и користењето на застарен хардвер значително го зголеми ризикот од губење на податоци.

Проектите беа прекинати, а важни извештаи, финансиски документи и контакт листи беа изгубени. Персоналот помина недели обидувајќи се да ги реконструира недостасувачките податоци. Довербата од донаторите и партнерите беше засегната, а се случија и финансиски загуби поради напорите за закрепнување и прекинатите проекти.

Научени лекции и препораки

Редовните резервни копии на податоците се од суштинско значење за континуитетот на организацијата. Резервните копии треба да се чуваат на повеќе платформи и периодично да се тестираат. Хардверот треба да се ажурира, а треба да се користат и системи за заштита од напојување.

Случај 3: Цената на губењето на податоци и недостатокот на резервни копии

Релевантен(и) модул(и)

- **Модул 5: Заштита на податоци и усогласеност со прописите за приватност**
- **Модул 7: Развивање на безбедносна култура**

Како овој случај може да се користи во обуката

- **Пример за управување со податоци (Модул 5):**
  Овој случај е ефикасен за објаснување дека не сите безбедносни инциденти вклучуваат хакери. Обучувачите можат да го користат за да воведат стратегии за резервна копија, достапност на податоци и организациски континуитет.

- **Вежба за проценка на ризик:**
  Од учесниците може да се побара да ги наведат критичните податоци во своите сопствени организации за граѓански организации и да идентификуваат дали постојат слични поединечни точки на неуспех.
- **Дискусија за одговорност на лидерството (Модул 7):**
  Случајот покажува зошто заштитата на податоците и резервните копии се одговорности на ниво на менаџмент, а не само технички задачи.

Предложен метод:
Водена рефлексија + активност за мини ревизија на податоци.

Случај 4: Опасноста од слаби лозинки и споделени сметки

Ова сценарио вклучува фондација со средна големина која поддржува лица со попреченост. Околу 15 членови на персоналот и волонтери користат споделени е-пошта и системски сметки за секојдневно работење, потпирајќи се на едно корисничко име и лозинка на повеќе платформи.

Донаторот пријавува дека примил сомнителни пораки со кои бара пари. Истрагата открива дека поранешен волонтер сè уште имал пристап до споделени сметки бидејќи лозинките никогаш не биле променети по неговото заминување. Овие акредитиви подоцна биле злоупотребени од неовластени лица. Слабите и споделените лозинки, повторната употреба на лозинки и отсуството на процедури за отповикување на пристап создадоа сериозен безбедносен јаз. На организацијата ѝ недостасувале јасни политики за управување со дигиталниот пристап кога персоналот или волонтерите си заминуваат.

Лозинките беа веднаш сменети, а донаторите беа информирани. Иако непосредната штета беше ограничена, се случи штета на угледот. На среден рок, организацијата воведе построги политики за лозинки, индивидуални кориснички сметки и сесии за подигање на свеста за персоналот.

Секоја сметка треба да има силна, единствена лозинка. Споделените сметки треба да се избегнуваат секогаш кога е можно, а правата за пристап мора да се прегледаат и одземат веднаш штом персоналот ќе си замине. Јасните внатрешни политики се од суштинско значење.

Случај 4: Опасноста од слаби лозинки и споделени сметки

Релевантен(и) модул(и)

- **Модул 6: Социјални медиуми и безбедност на онлајн присуство**
- **Модул 7: Развивање на безбедносна култура**
- **Модул 8: Напредни теми (Пристап до сметка и контрола)**

Како овој случај може да се користи во обуката

- **Илустрација на јазот во политиката (Модул 7):**
  Овој случај јасно ги покажува ризиците од пропуштање на политиките за управување со пристапот, особено процедурите за исклучување од работа, кога персоналот или волонтерите си заминуваат.
- **Дискусија за безбедноста на сметката (Модул 6):**
  Обучувачите можат да го поврзат овој случај со важноста на индивидуалните сметки, силните лозинки и пристапот базиран на улоги – особено за е-пошта и комуникација со донатори.
- **Вовед во напредна контрола на пристап (Модул 8):**
  Случајот може да послужи како мост кон понапредни практики како што се ревизии на сметки, менаџери за лозинки и управување со привилегии.

Предложен метод:
Вежба за изготвување политики засновани на случаи (на пр. „Што треба да вклучува контролната листа за исклучување од работа?“).

Забелешка од тренерот (опционално за додавање на крајот од делот)

Овие локални студии на случај се дизајнирани да:

- Ги одразат реалните ризици со кои се соочуваат граѓанските организации во Турција,
- Поттикнат учење од врсници и дискусија,
- Покажат дека инцидентите со сајбер безбедност честопати произлегуваат од едноставни, спречливи проблеми,
- Ја зајакнат важноста на политиките, обуката и подготвеноста, а не само на технологијата.

Обучувачите се охрабруваат да ја прилагодат длабочината на дискусијата во зависност од големината на организацијата, дигиталната зрелост и улогите на учесниците.

Практични политики и шаблони за дигитална безбедност за граѓански организации

Вовед

Овој документ претставува практични обрасци за политики што можат да се користат за зајакнување на капацитетот за дигитална безбедност на малите и средни организации на граѓанското општество (ГО) во Турција. Обрасците се дизајнирани да бидат едноставни, практични и усогласени и со националното законодавство (Закон за заштита на лични податоци – KVKK, Закон за сајбер безбедност) и со меѓународните добри практики

1. Политика за прифатлива употреба (AUP)

Намена:
Да се промовира одговорно користење на организациските дигитални алатки, пристапот до интернет и информациските системи.

Одредби за политиката:

- Сите вработени треба да ги користат дигиталните ресурси на организацијата исклучиво за работни цели.
- Лозинките мора да бидат индивидуални и не смеат да се споделуваат со други.
- Нелегалната содржина не смее да се складира, да се пристапува до неа или дистрибуира преку организациските системи.
- Користењето на социјалните медиуми не смее да му наштети на угледот на организацијата.
- Ниту еден податок не може да се пренесува надвор од организацијата без претходна согласност од менаџментот.

Забелешка:
Оваа политика стапува на сила по потпишувањето од страна на персоналот за време на процесот на вработување и мора да се ревидира секоја година. (ENISA, 2021)

2. План за одговор на инциденти (IRP)

Намена:
За да се обезбеди брз и ефикасен одговор на потенцијални инциденти поврзани со дигиталната безбедност.

Чекори:

ицето кое го детектира инцидентот веднаш го информира надлежниот орган во организацијата.

адлежното лице го одредува типот на инцидент (фишинг, малициозен софтвер, повреда на податоци).

асегнатите системи се изолирани (доколку е потребно се отстрануваат од мрежата).

ите дигитални логови и записи поврзани со инцидентот се зачувани.

нцидентот се пријавува во Дирекцијата за сајбер безбедност во рок од максимум 48 часа (Службен весник, 2024).

е спроведува евалуација по инцидентот, а процедурите се ажурираат соодветно.

Забелешка:
Овој план се базира на Законот бр. 7545 за сајбер безбедност и NIST SP 800-61 Rev. 2.

3. Основна постапка за заштита на податоци

Намена:
Да се обезбеди дека личните податоци обработени во рамките на CSO се управуваат во согласност со KVKK.

Имплементација:

- Секоја активност за обработка на податоци мора да има јасна цел и да биде во согласност со принципот на минимизирање на податоците.
- Личните податоци не смеат да се обработуваат без изречна согласност, освен ако поинаку не е дозволено со закон (KVKK, 2020).
- За секоја активност за споделување податоци, мора да се документираат причината за споделувањето, примателот и времетраењето.
- Мора да се воспостави политика за задржување и уништување на податоци; личните податоци мора да се избришат или анонимизираат кога повеќе не се потребни.
- Хартиените записи мора да се чуваат во заклучени ормари, а дигиталните податоци мора да бидат заштитени во шифрирани папки.

Забелешка:
Се препорачува организацијата да назначи внатрешен контролор на податоци или одговорно лице.

4. Протокол за споделување на акредитиви и уреди

Намена:
Да се регулира безбедната употреба и споделување на лозинки, кориснички сметки и дигитални уреди во рамките на организацијата.

Правила:

- Лозинките мора да се доделат поединечно и не смеат да се запишуваат.
- На споделени уреди, секој корисник мора да се најави со посебна сметка и не смее да споделува лозинки.
- Преносот на податоци на надворешни уреди (на пр. лични лаптопи) е забранет.
- Употребата на USB-дискови или надворешни уреди за складирање е дозволена само со одобрение од менаџментот.

Забелешка:
Организациите можат дополнително да дефинираат политика за автентикација (на пр. повеќефакторска автентикација).

5. Обврска за дигитална безбедност (Вработени / Волонтери)

Текст на обврска (пример):
„Со овој документ, се обврзувам да ги користам дигиталните системи и алатки обезбедени од [Име на организацијата] исклучиво во рамките на моите должности и со должно внимание. Ја потврдувам мојата одговорност да ги исполнам сите обврски поврзани со безбедноста на организациските податоци“.

Забелешка:
Оваа обврска треба да ја потпишат сите членови на персоналот и волонтерите и да ја чуваат во нивните лични досиеја.

Контролни листи за дигитална безбедност за граѓанските организации

За зајакнување на дигиталната безбедност на малите и средните организации на граѓанското општество (ГО) што работат во Турција, подолу се дадени четири одделни контролни листи. Овие листи се состојат од едноставни и практични елементи што лесно можат да ги применат дури и корисници со ограничено техничко знаење. Секоја контролна листа ги сумира основните безбедносни чекори во согласност со важечките законски прописи. Целта е да се зголеми свеста за безбедноста во секојдневните дигитални операции и да се обезбеди подготвеност за потенцијални итни случаи.

1. Основна контролна листа за дигитална безбедност

☐Дали сите корисници користат силни и уникатни лозинки?
☐Дали се овозможени автоматски заклучувања на екранот на компјутерите и мобилните телефони?
☐Дали е инсталиран ажуриран антивирусен софтвер на сите уреди?
☐Дали сите софтвери и апликации редовно се ажурираат?
☐Дали редовно се прави резервна копија на важните документи (надворешен диск или складирање во облак)?
☐Дали сите корисници се претпазливи при отворање на прилози во е-пошта?
☐Дали се следи употребата на надворешни или лични уреди?

2. Контролна листа за подготвеност за одговор на инциденти

☐Дали е назначено лице одговорно за дигитална безбедност?
☐Дали е јасно дефинирано до кого и како треба да се пријават инцидентите?
☐Дали сите вработени имаат основно знаење за идентификување инциденти (фишинг, малициозен софтвер итн.)?
☐Дали е направена резервна копија на критичните документи и системи?
☐Дали постои писмена постапка по инцидентот?
☐Дали персоналот е запознаен со правилото за известување во рок од 48 часа? (Закон бр. 7545)

3. Контролна листа за безбедност на социјалните медиуми

☐Дали само овластени лица имаат пристап до сметките на социјалните медиуми?
☐Дали е овозможена двофакторска автентикација (2FA) на сите сметки?
☐Дали лозинките се силни и не се користат повторно на други платформи?
☐Дали е јасно кој ги управува сметките и за која цел?
☐Дали содржината е предмет на претходно одобрување пред да се сподели?

☐Дали се следат сомнителните најавувања или невообичаеното зголемување на бројот на следбеници?

4. Контролна листа за безбедност на информациите за нови вработени / волонтери

☐Дали новите членови на персоналот или волонтерите добиваат ориентација за дигитална безбедност?
☐Дали е потпишана Политиката за прифатлива употреба?
☐Дали се добиени обврски во врска со обработката на лични податоци?
☐Дали правата за пристап се ограничени строго на работните обврски?
☐Дали се користат организациски сметки наместо лични сметки?
☐Дали е обезбедено почитување на организациските политики за лозинка и уред?

4.2 Правна и регулаторна рамка во Босна и Херцеговина и предлози за граѓанските организации во БиХ

Правен и регулаторен контекст во Босна и Херцеговина (БиХ)

Заштитата на личните податоци во Босна и Херцеговина е регулирана со **Закон за заштита на личните податоци (Zakon o zaštiti ličnih podataka).** Надлежниот надзорен орган е **Агенцијата за заштита на лични податоци на Босна и Херцеговина (AZLP).** Иако Општата регулатива на ЕУ за заштита на податоци (GDPR) не е директно применлива во БиХ, многу програми финансирани од ЕУ и меѓународни донатори бараат стандарди усогласени со GDPR. Како резултат на тоа, организациските практики и упатства во БиХ сè повеќе ги одразуваат основните принципи на GDPR, како што се законитоста, минимизирањето на податоците, одговорноста и безбедноста на обработката.

Босна и Херцеговина сè уште нема единствен, сеопфатен национален закон за сајбер безбедност. Во овој контекст, од организациите на граѓанското општество (ГО) првенствено се очекува да обезбедат дигитална безбедност преку механизми за внатрешно управување, вклучувајќи јасно дефинирани улоги и одговорности, политики за внатрешна безбедност на информациите и документирани процедури, кои доследно се применуваат во секојдневното работење.

Национални институции и механизми за поддршка на сајбер инциденти

Неколку јавни институции обезбедуваат поддршка, координација или истражни функции во случај на инциденти поврзани со сајбер безбедноста во Босна и Херцеговина. Тие ги вклучуваат **ЦЕРТ БиХ**, кој е одговорен за поддршка за одговор на инциденти, рано предупредување и следење на закани, како и **Министерството за безбедност на БиХ – Сектор за сајбер безбедност**, кој обезбедува координација и насоки на ниво на политики. Пријавувањето и истрагата за сајбер криминал се спроведуваат од страна на **Државната агенција за истраги и заштита (SIPA)**преку специјализирани единици, заедно со единиците

за сајбер криминал на ентитетите и кантоналните полициски единици одговорни за оперативни истраги на локално ниво.

Предел на сајбер закани за граѓанските организации во БиХ

Граѓанските организации во БиХ најчесто се соочуваат со сајбер закани поврзани со фишинг напади насочени кон организациските финансии, грантовите и комуникацијата со донаторите. Инцидентите со рансомвер и трајното губење на податоци се исто така чести, честопати поради недостаток или несоодветни практики за резервна копија. Нападите со лажно претставување и социјално инженерство се забележуваат сè повеќе преку платформи за пораки како што се WhatsApp и Viber, додека деформирањето на веб-страницата претставува посебен ризик за организациите што работат на политички или социјално чувствителни прашања. Покрај тоа, кражбата на акредитиви поврзана со употребата на необезбедени јавни Wi-Fi мрежи останува постојан проблем.

Оперативна реалност на граѓанските организации во БиХ и образложение за поедноставен пристап

Во пракса, многу граѓански организации во Босна и Херцеговина во голема мера се потпираат на лични лаптопи и мобилни телефони за организациска работа и користат платформи како што се Gmail, Google Workspace и социјалните медиуми како нивни примарни оперативни алатки. Посветен персонал за ИТ или сајбер безбедност е редок, а неформалните практики како што е споделувањето лозинки во рамките на тимовите се сè уште вообичаени.

Со оглед на оваа реалност, наставната програма усвојува намерно поедноставен и прагматичен пристап. Таа дава приоритет на нискобуџетните и лесно применливи безбедносни мерки, обезбедува практични шаблони и документи готови за употреба и се фокусира на јасни, чекор-по-чекор контролни листи дизајнирани за нетехнички персонал, наместо на сложени технички решенија.

Усогласување со европските рамки на политиките

Иако Босна и Херцеговина не е членка на Европската Унија, многу граѓански организации работат во рамките на програми финансирани од ЕУ и рамки на европски политики. Затоа, оваа наставна програма е усогласена со основните принципи на GDPR, особено пристапот базиран на ризик, како и со пошироките европски стратегии за свест за сајбер безбедноста и градење капацитети. Усогласувањето е практично, а не легалистичко, фокусирајќи се на секојдневна имплементација и организациско однесување, наместо на формални барања за усогласеност.

Пристап базиран на ризик и логика на политиката

Европските рамки на политиките нагласуваат пропорционалност, контекстуална свест и проценка на влијанието. Наставната програма ја применува оваа логика преку давање приоритет на средствата и активностите со висок ризик, избегнување на премногу сложени или контроли што бараат интензивни ресурси и фокусирање на реални безбедносни практики ориентирани кон луѓето и кои можат да се одржат во рамките на граѓанското општество.

ISO-инспирирана логика (поедноставено)

Дури и без формална сертификација, граѓанските организации можат да имаат корист од поедноставените принципи инспирирани од ISO стандардите за безбедност на информациите. Тие вклучуваат идентификување на клучните организациски средства, примена на основни принципи за контрола на пристап, воспоставување структурирани процеси за управување со инциденти и промовирање на континуирано подобрување преку преглед и учење. Овој пристап поддржува постепено зајакнување на организациската зрелост и отпорност со текот на времето.

Локални студии на случај од Босна и Херцеговина

Случај 1: Фишинг линк што води до целосно преземање на сметката

Овој случај вклучува младинска организација на граѓанското општество со седиште во Сараево. Организацијата работи со мал тим и во голема мера се потпира на споделени е-пошта сандачиња и платформи на социјалните медиуми како што се Фејсбук и Инстаграм за комуникација, координација и информирање на јавноста. Лозинките се споделуваат интерно и не е овозможена двофакторска автентикација. Член на персоналот добил порака на Фејсбук Месинџер која изгледала како да доаѓа од доверлив партнер на проектот. Пораката барала потврда за деталите за заедничка активност и содржела линк. Членот на персоналот кликнал на линкот и ги внел е-поштенските акредитиви на организацијата. За неколку минути, напаѓачот добил пристап до споделеното е-поштенско сандаче и поврзаните сметки на социјалните медиуми. Контакт деталите за враќање беа променети, а до донаторите беа испратени лажни барања за плаќање.

Инцидентот беше овозможен од повеќе слабости, вклучувајќи споделени лозинки, повторна употреба на лозинки на различни платформи, недостаток на двофакторска автентикација и прекумерни административни привилегии за сите корисници. Пораката беше доверлива без независна верификација. На краток рок, организацијата го изгуби пристапот до своите сметки за е-пошта и социјални медиуми, нарушувајќи ја комуникацијата и активностите за собирање средства. Лажните пораки ја нарушија довербата на донаторите. На среден рок, организацијата мораше да инвестира значително време во обновување на сметката и обновување на кредибилитетот.

Научени лекции и препораки

Сите организациски сметки треба да користат уникатни лозинки управувани преку менаџер за лозинки и да имаат овозможена двофакторска автентикација. Административните привилегии мора да бидат ограничени, а чувствителните барања секогаш треба да се проверуваат преку секундарен комуникациски канал.

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 1 – Основи на сајбер безбедноста:**
  Користено како основен пример за илустрирање на фишинг напади, кражба на акредитиви и брзо преземање на сметка.
- **Модул 4 – Чести сајбер-закани (фишинг и малициозен софтвер):**
  Покажува како социјалниот инженеринг ја експлоатира довербата и недостатокот на верификација.
- **Модул 7 – Развивање на безбедносна култура:**
  Поддржува дискусија за свеста на персоналот, хигиената на лозинките и важноста на двофакторската автентикација.

Препорачана употреба:
Анализа на случајот проследена со идентификување на црвени знамиња и мапирање на превентивни контроли.

Случај 2: Лажно претставување преку WhatsApp/Viber што доведува до финансиска загуба

Овој случај се однесува на граѓанска организација со средна големина која често користи WhatsApp и Viber за внатрешна координација и финансиска комуникација. Чувствителните одлуки често се решаваат неформално преку апликации за пораки.

Напаѓач креирал сметка на WhatsApp или Viber користејќи го името и профилната фотографија на вистински координатор на проектот. Напаѓачот контактирал со финансискиот персонал со итна порака во која се наведува дека банкарските податоци се променети и побарал итна употреба на нов IBAN. Барањето било обработено без верификација.

Организацијата се потпираше на неформални платформи за пораки за чувствителни финансиски одлуки и немаше секундарни механизми за верификација. Немаше барање за одобрување од повеќе лица за финансиски трансакции.

Средствата му беа префрлени на напаѓачот и не можеа да бидат вратени. Инцидентот резултираше со финансиски загуби и внатрешни проблеми, како и проблеми со репутацијата кај донаторите и партнерите.

Финансиските размени никогаш не треба да се одобруваат преку платформи за пораки. Сите барања поврзани со плаќања мора да бидат потврдени преку официјални канали, како што се потпишани е-пораки од организацискиот домен или телефонски повици до познати броеви. За значајни финансиски трансакции треба да се имплементира правило за одобрување од две лица.

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 2 – Комуникација и социјален инженеринг:**
  Примарен случај што илустрира лажно претставување и манипулација базирана на итност преку платформи за пораки.
- **Модул 7 – Развивање на безбедносна култура:**
  Ја нагласува потребата од внатрешни правила, процедури за верификација и споделена одговорност за финансиските одлуки.

Препорачана употреба:
Вежба со играње улоги за проверка на итни финансиски барања и примена на правилото за одобрување од две лица.

Случај 3: Кражба на акредитиви преку јавен Wi-Fi

Овој случај вклучува граѓанска организација која им овозможува на волонтерите да работат од далечина користејќи лични уреди. Облак-услугите како што се Gmail и Google Drive се централни за секојдневното работење и не постои формална политика што го регулира далечинскиот пристап или безбедноста на уредите.

Волонтер работеше од кафуле користејќи бесплатен јавен Wi-Fi и се најавуваше на е-поштата и меморијата на облакот на организацијата. На уредот му недостасуваа неодамнешни безбедносни ажурирања, а лозинките беа зачувани во прелистувачот. Кратко потоа, беа откриени непознати најавувања и беа преземени списоци со контакти на донатори. Одговорот беше одложен поради нејасни процедури за пријавување.

Организацијата дозволуваше пристап до чувствителни сметки преку необезбеден јавен Wi-Fi, користеше застарени уреди и дозволуваше лозинки зачувани во прелистувачот. Исто така, немаше јасен внатрешен механизам за пријавување инциденти.

Чувствителни податоци беа откриени, а довербата на донаторите беше доведена во опасност. Доцнењето во одговорот го зголеми потенцијалното влијание на прекршувањето на безбедноста.

Не треба да се пристапува до чувствителни сметки преку јавен Wi-Fi без VPN. Уредите мора да се ажурираат, функциите за автоматско поврзување да се оневозможат, а процедурите за пријавување инциденти јасно да им се соопштат на сите вработени и волонтери.

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 3 – Безбедност на уреди и инфраструктура:**
  Основен пример за ризици поврзани со јавна Wi-Fi мрежа, незакрпени уреди и небезбедно складирање на акредитиви.
- **Модул 7 – Развивање на безбедносна култура:**
  Ја нагласува важноста на јасните процедури за пријавување инциденти и свеста на персоналот.

Препорачана употреба:
Групна дискусија проследена со вежба со листа за проверка за безбедни практики на работа од далечина.

Случај 4: Ransomware преку прилог во е-пошта

Овој случај се однесува на регионална граѓанска организација (ГО) која користи споделени канцелариски лаптопи и размена на документи преку е-пошта. Практиките за резервна копија беа неформални и не се правеа офлајн резервни копии. Примена е е-пошта слична на извештај од донатор, а член на персоналот го отвори прилогот на споделен лаптоп. Кратко потоа, датотеките станаа недостапни и на екранот се појави порака за откуп. Организацијата веруваше во профилот на испраќачот, немаше правила за филтрирање на прилози и не одржуваше офлајн или изолирани резервни копии. Финансиските записи и проектната документација беа трајно изгубени. Проектите за OCSO беа прекинати и беа направени трошоци за обновување. ГО треба да одржуваат барем една офлајн резервна копија и да користат услуги во облак со овозможена историја на верзии. Прилозите овозможени со макро и извршните датотеки треба да бидат ограничени, а персоналот треба да биде обучен да не отвора непобарани датотеки.

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 4 – Чести сајбер закани (малициозен софтвер и рансомвер):**
  Покажува како ransomware се шири преку прилози во е-пошта и влијанието на недостасувачките резервни копии.
- **Модул 5 – Заштита на податоци и усогласеност со прописите за приватност:**
  Ги истакнува достапноста на податоците, обврските за резервна копија и ризиците од организацискиот континуитет.

Препорачана употреба:
Дискусија базирана на сценарија за стратегиите за резервна копија и чекорите за одговор „што би направиле прво?“

Случај 5: Ограбената Фејсбук страница поради споделени најавувања

Неколку младински граѓански организации споделија едно единствено најавување на Фејсбук меѓу персоналот и волонтерите за управување со јавни страници. Пристапот не беше прегледан кога волонтерите ја напуштија организацијата. Поранешен волонтер го задржа пристапот до споделената сметка, а подоцна ја злоупотреби. Фејсбук страницата беше киднапирана и искористена за објавување лажни пораки и политичка содржина. Споделените акредитиви, недостатокот на пристап базиран на улоги и неуспехот да се поништи пристапот кога персоналот си замина создаде голема безбедносна празнина. Репутацијата на организацијата беше нарушена, а донаторите ја контактираа граѓанската организација за да ја потврдат легитимноста на објавената содржина. Закрепнувањето бараше време и јавно разјаснување.

Научени лекции и препораки

Треба да се избегнуваат споделени најавувања. Пристапот мора да се овозможи преку функциите на улогите на платформата, двофакторската автентикација треба да биде задолжителна за администраторите, а правата за пристап мора редовно да се прегледуваат.

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 6 – Безбедност на социјалните медиуми и онлајн присуство:**
  Примарен случај за споделени акредитиви, пристап базиран на улоги и процедури за враќање на сметката.
- **Модул 7 – Развивање на безбедносна култура:**
  Поддржува дискусии за политиките за поништување на пристап и процедури за исклучување од системот.
- **Модул 8 – Напредни теми (Практики за контрола на пристап):**
  Може да се користи при воведување посилно управување со сметките и административни контроли.

Препорачана употреба:
Вежба за изготвување политики засновани на случаи, фокусирана на управување со пристапот до социјалните медиуми.

ПРАКТИЧНИ ШАБЛОНИ И ЛИСТИ ЗА ПРОВЕРКА За организациите на граѓанското општество (ГО) во Босна и Херцеговина

АНЕКС 1 – ПОЛИТИКА ЗА ПРИФАТЛИВА УПОТРЕБА (AUP)
Шаблон за мали и средни граѓански организации во БиХ

Наслов на документот: Политика за прифатлива употреба (AUP)Важи за: Сите вработени, волонтери, практиканти, надворешни консултанти

ел Оваа политика ги дефинира правилата за безбедна и одговорна употреба на CSO уреди, кориснички сметки и податоци.

метки и лозинки

- Користете уникатни лозинки за секоја сметка.
- Не споделувајте лозинки преку групи за разговор, апликации за пораки или е-пошта.
- Овозможете двофакторска автентикација (2FA) за е-пошта, складирање во облак и администраторски сметки на социјалните медиуми.
- Користете менаџер за лозинки каде што е можно.

реди (лаптопи и мобилни телефони)

- Заклучете ги сите уреди со ПИН, лозинка или биометриска заштита.
- Овозможете автоматски системски и безбедносни ажурирања.
- Пријавете изгубени или украдени уреди во рок од 1 час кај раководителот на инциденти.

-пошта и линкови

- Не отворајте неочекувани прилози или линкови.
- Секогаш проверувајте ги промените во банкарската или платежната сметка преку телефонски повик на познат број.
- Третирајте ги итните пораки или пораките засновани на притисок како пораки со висок ризик.

i-Fi и работа од далечина

- Избегнувајте користење на јавен Wi-Fi за администраторски или чувствителни сметки.
- Користете мобилна точка за пристап или VPN доколку е достапна.
- Оневозможете автоматско поврзување со Wi-Fi мрежи.

оцијални медиуми

- Користете улоги на страницата наместо споделени најавувања.
- Одржувајте го минималниот број на администратори.
- Веднаш отстранете го пристапот кога член на персоналот или волонтер ќе замине.

акување со податоци

- Собирајте само потребни лични податоци.
- Чувајте ги личните податоци само на одобрени локации (на пр. CSO cloud drive).
- Не чувајте податоци за корисниците на лични уреди без енкрипција.

ријавување инциденти Секој сомнителен безбедносен или инцидент со податоци мора веднаш да се пријави со користење на Планот за одговор на инциденти на

Одобрено од: _____Датум: _____Датум на следен преглед: _____

АНЕКС 2 – ПЛАН ЗА РЕАГИРАЊЕ НА ИНЦИДЕНТИ (ПРЕ)
Поедноставено – за мали граѓански организации

Наслов на документот: План за одговор на инциденти (поедноставен)

то е инцидент? Инцидент е секој настан што ги загрозува сметките, уредите, податоците или угледот на CSO, вклучувајќи фишинг, преземање сметка, малициозен софтвер, рансомвер или протекување податоци.
логи и одговорности (Внесете ги имињата) Раководител на инцидентот: _____Раководител на комуникациите: _____ИТ поддршка (внатрешна/надворешна): _____Одобрување од менаџментот: _____
рвите 15 минути – Итни дејства

- Исклучете го засегнатиот уред од Wi-Fi или интернет.
- Направете снимки од екранот и забележете го времето и засегнатите сметки.
- Информирајте го внатрешниот тим: „Не кликнувајте на линкови. Инцидентот е во фаза на преглед“.
- Прво обезбедете ја сметката за е-пошта (променете ја лозинката и овозможете

рвите 60 минути – Задржување

- Ресетирајте ги лозинките по овој редослед: е-пошта, складирање во облак, социјални медиуми, банкарски или финансиски алатки.
- Одјавете се од сите непознати или сомнителни сесии.
- Отстранете ги непознатите администратори, апликации и интеграции.
- Проверете ги правилата за препраќање е-пошта.

роценка (истиот ден)

- Што се случи?
- Кои податоци може да бидат засегнати (донатори, корисници, малолетници)?
- Кои системи и сметки се засегнати?

адворешно известување (кога е потребно)

- CERT BiH за поддршка за инциденти и известувања.
- SIPA или полициски единици за сајбер криминал доколку се сомнева во сајбер криминал.
- Консултирајте се со барањата на AZLP доколку е веројатно нарушување на личните податоци и документирајте ги преземените мерки.

равила за комуникација

- Само раководителот за комуникации издава надворешни изјави.
- Споделувајте само факти.
- Доколку е потребно, известете ги донаторите или партнерите.

акрепнување

- Вратете ги системите од резервните копии.
- Ажурирајте ги сите уреди.
- Преобучете го персоналот за типот на инцидент.

реглед по акцијата (во рок од 7 дена)

- Која контрола не успеа?
- Што мора да се промени (2FA, улоги за пристап, резервни копии, обука)?
- Ажурирајте ги политиките и контролните листи.

АНЕКС 3 – ПРАВИЛНИК ЗА ЗАШТИТА НА ПОДАТОЦИ (ИНТЕРЕН)
Едноставен внатрешен правилник за граѓански организации

Наслов на документот: Правилник за заштита на податоци (интерен)

псегОвој правилник се однесува на сите лични податоци обработени од страна на ГО.
сновни правила за заштита на податоци

- Обработувајте податоци законски и праведно.
- Соберете го само она што е потребно (минимизирање на податоците).
- Чувајте ги податоците само онолку долго колку што е потребно.
- Применете мерки за заштита како што се контрола на пристап, резервни копии и

добрени локации за складирање на податоци на CSO облак диск: _____CSO систем за е-пошта: _____Локална шифрирана папка (доколку е потребно): _____
онтрола на пристап

- Само вработените на кои им се потребни податоците можат да пристапат до нив.
- Отстранете го пристапот во рок од 24 часа кога некој ќе замине.

увствителни податоци и малолетници – При обработка на податоци на малолетници, применувајте построги контроли и ограничете го пристапот.
поделување на податоци

- Споделувајте податоци само преку одобрени канали.
- Не споделувајте списоци на корисници преку WhatsApp или Viber.
- Користете датотеки заштитени со лозинка за чувствителни податоци.

правување со инциденти – Секое сомнително кршење на податоци веднаш го активира Планот за одговор на инциденти.

Одобрено од: _____Датум: _____Датум на следен преглед: _____

АНЕКС 4 – ПРАКТИЧНИ ЛИСТИ ЗА ПРОВЕРКА
За граѓански организации во БиХ со низок ИТ капацитет

Контролна листа А – Контролна листа за основна дигитална безбедност (почетен пакет)

Сметки

- 2FA е овозможен за администратори на е-пошта, облак и социјални медиуми.
- Користени се уникатни лозинки.
- Лозинките не се споделуваат во групите за разговор.

Уреди

- Заклучувањето на екранот е овозможено.
- Автоматските ажурирања се вклучени.
- Антивирусот или системскиот заштитник е активен.

Wi-Fi и работа од далечина

- Wi-Fi за гости е одделен од Wi-Fi за персоналот.
- Нема администраторски најавувања на јавна Wi-Fi мрежа без хотспот или VPN мрежа.

Податоци и резервни копии

- Историјата на верзии во облакот е овозможена.
- Достапна е неделна резервна копија (една офлајн копија доколку е можно).
- Пристапот се одзема веднаш штом некој ќе замине.

Социјални медиуми

- Користени улоги на страницата.
- Само 1–2 администратори.
- Е-поштата и телефонот за враќање му припаѓаат на CSO.

Контролна листа Б – Контролна листа за пријавување инциденти (внатрешна)

Кога се сомневате во инцидент

- Исклучете го засегнатиот уред од интернет.
- Направете снимки од екранот и забележете го времето.
- Веднаш известете го раководителот на инцидентот.
- Променете ја лозинката за е-пошта и овозможете 2FA.
- Проверете за непознати најавувања и правила за препраќање е-пошта.

- Идентификувајте ги засегнатите податоци (донатори, корисници, малолетници).
- Одлучете дали е потребно надворешно известување (CERT BiH, SIPA, полиција,

Минимален запис за инциденти

Датум и време на откривање: _____Откриено од: _____Што се случило (краток опис): _____Засегнати сметки или системи: _____Преземени дејствија: _____Доказ зачуван во: _____Завршено надворешно известување (да/не): _____

4.3 Правна, регулаторна и оперативна рамка за граѓанските организации во Северна Македонија

Правна и регулаторна рамка во Северна Македонија

На 27 април 2016 година, Европскиот парламент и Советот на Европската Унија ја усвоија Регулативата (ЕУ) 2016/679 за заштита на физичките лица во врска со обработката на лични податоци и за слободното движење на таквите податоци, со која се укинува Директивата 95/46/ЕЗ. Ова го означи почетокот на сеопфатен процес на реформи во областа на заштитата на личните податоци. По двегодишен транзициски период, Регулативата стана применлива низ целата Европска Унија на 25 мај 2018 година.

Оваа регулатива, попозната како GDPR, е целосно транспонирана во Република Северна Македонија преку донесување на Законот за заштита на личните податоци, кој стапи на сила на 24 февруари 2020 година.

Законот за заштита на личните податоци регулира седум основни принципи за обработка на лични податоци:

- законитост, праведност и транспарентност,
- ограничување на целта,
- минимизирање на податоците,
- точност,
- ограничување на складирањето,
- интегритет и доверливост,
- отчетност.

Невладините организации, како контролори на податоци, се должни да ги применуваат сите принципи кумулативно во секој случај на обработка на лични податоци и во текот на целиот животен циклус на податоците. Неприменувањето на кој било од овие принципи претставува прекршување на Законот за заштита на личните податоци. Главен орган одговорен за спроведување и надзор на Законот за заштита на личните податоци е Агенцијата за заштита на личните податоци.

Дополнително, во областа на сајбер безбедноста, Законот за безбедност на мрежни и информациски системи, донесен во јули 2025 година, претставува прва сеопфатна правна рамка што ја регулира сајбер безбедноста во Северна Македонија. Законот е усогласен со европската директива NIS2 и има за цел да воспостави високо и заедничко ниво на заштита на мрежните и информациските системи и во јавниот и во приватниот сектор.

Министерството за дигитална трансформација и Националниот тим за одговор на компјутерски инциденти (MKD-CIRT), кој работи во рамките на Агенцијата за електронски комуникации, се одговорни за следење, координирање и реагирање на инциденти со сајбер безбедност. Од важност за приватниот сектор, вклучително и невладините

организации, е преодниот период на имплементација што трае до 2027 година, во кој се очекува сите субјекти постепено да ги почитуваат обврските воведени со законот.

Чести закани и неодамнешни инциденти што влијаат врз граѓанските организации

Невладините организации во Северна Македонија, слично како и другите сектори, се многу ранливи на закани поврзани со сајбер безбедноста. Клучен предизвик е што многу сајбер инциденти остануваат непрепознаени или непријавени, што резултира со недостаток на сеопфатни и веродостојни податоци за инцидентите. Иако значителен број граѓански организации известуваат дека се информирани за законските измени и соодветно ги прилагодуваат своите оперативни практики, достапните податоци покажуваат дека многу организации не донеле внатрешни закони за заштита на личните податоци и не назначиле службеник за заштита на личните податоци.

Понатаму, процентот на вработени во граѓанските организации кои добиле формална обука за заштита на лични податоци останува многу низок. Со оглед на тоа што граѓанските организации често работат со ограничени финансиски ресурси и се соочуваат со тешкотии при распределбата на средства за обука на вработените, се препорачува да се воспостават структурирани механизми за соработка помеѓу Агенцијата за заштита на лични податоци и невладиниот сектор за да се олесни пристапот до можностите за обука.

Главен фактор на ризик за граѓанските организации е нивниот ограничен буџет за инвестиции во заштитата на податоци и сајбер безбедноста. Многу помали организации продолжуваат да користат нелиценциран или застарен софтвер, што значително ја зголемува нивната изложеност на сајбер закани. Во исто време, достапни се неколку прирачници и упатства на македонски јазик кои можат да им помогнат на граѓанските организации во зајакнувањето на нивната дигитална безбедност.

Најидентификуваните закани вклучуваат:• неможност за проверка на испраќачите пред кликнување на линкови или отворање пораки,• ограничена употреба на менаџери за лозинки и честа повторна употреба на слични лозинки,• неправилни или отсутни практики за резервна копија на податоци,• употреба на нелиценциран и застарен софтвер,• недоволни безбедносни мерки за мобилни уреди,• многу ниска употреба на двофакторска автентикација.

Национална поддршка и ресурси

Неколку национални институции, вклучувајќи ја Агенцијата за заштита на личните податоци, Министерството за дигитална трансформација и Агенцијата за електронски комуникации, обезбедуваат поддршка и насоки за граѓанските организации насочени кон подобрување на дигиталната безбедност и заштитата на податоците. Сепак, потребни се понатамошни институционални напори, вклучително и систематско планирање и иницијативи финансирани од државата.

Поддршка се обезбедува и преку проекти на граѓанското општество финансирани првенствено од странски донатори за зголемување на дигиталната писменост кај граѓанските организации и општата популација. Значаен пример е проектот „CyberShield: Овластени граѓани за сајбер отпорност“, во рамките на кој во 2025 година беа одржани три обуки за сајбер безбедност за организации што работат со маргинализирани групи. Како продолжение, беа развиени планови за дигитална безбедност за шест организации на граѓанското општество. Овие прилагодени планови имаат за цел да обезбедат систематско спроведување на практиките за сајбер безбедност, подобрување на организациската отпорност и индиректно подобрување на испораката на услуги до крајните корисници.

И покрај овие позитивни примери, ограниченото финансирање значи дека само мал број граѓански организации се во можност да имаат корист од ваквите иницијативи. Иако неколку прирачници и материјали за подигање на свеста се достапни на македонски јазик, неопходна е поширока и поодржлива соработка меѓу јавните власти и граѓанските организации, за да се прошири пристапот до обуки и активности за градење капацитети. Зголеменото финансирање и насочените програми се особено потребни за поддршка на директното образование и на обуката на персоналот на граѓанските организации.

Културен и оперативен контекст на граѓанските организации во Северна Македонија

Повеќето граѓански организации во Северна Македонија работат според модел базиран на донатори и проекти и обично имаат мали административни и оперативни тимови или во голема мера се потпираат на волонтери. Организациската работа често се извршува со користење на лични уреди и широко достапни дигитални услуги како што се Google Workspace, Dropbox или Microsoft 365, честопати без соодветна лиценца.

Затоа, иницијативите за обука и градење капацитети треба да се фокусираат на практични и реални мерки, вклучувајќи:
- предностите од користењето лиценцирани производи и услуги,
- кампањи за подигнување на свеста „Размислете пред да кликнете“,
- редовни резервни копии на податоци и информации,
- активна и доследна употреба на двофакторска автентикација,
- обезбедување на мобилни уреди и управување со нивната употреба,
- одговорни практики за лозинки,
- ефикасна употреба на решенија базирани на облак,
- зголемена свест за практиките за споделување податоци.

Нивоата на дигитална писменост во Северна Македонија остануваат недоволни, вклучително и во рамките на граѓанскиот сектор. Потребни се дополнителни средства, ресурси и координирани напори за да се постигне повисоко ниво на дигитална безбедност. Овие напори треба да се преточат во конкретни програми и практични акциони планови прилагодени на реалните потреби и капацитети на организациите на граѓанското општество.

Анекси и шаблони подготвени за употреба (Северна Македонија)

АНЕКС 1 – Дигитален безбедносен пејзаж за граѓанските организации во Северна Македонија

Овој анекс ги одразува правните, институционалните и оперативните реалности што влијаат врз организациите на граѓанското општество во Северна Македонија и ја поддржува локализацијата на наставната програма.

Закани
- Фишинг напади преку е-пошта и лажни институционални пораки,
- Инциденти со Ransomware и губење на податоци поради недостаток на резервни копии,
- Злоупотреба на необезбедени лични податоци,
- Ризици поврзани со употребата на лични лаптопи и мобилни уреди.

Оперативни предизвици
- Мала употреба на менаџери за лозинки и честа повторна употреба на лозинки,
- Неправилни или недостасувачки рутини за резервна копија на податоци,
- Употреба на нелиценциран или застарен софтвер,
- Недоволна безбедност на мобилните уреди,
- Ограничено усвојување на двофакторска автентикација,
- Недостаток на наменски средства за дигитални безбедносни мерки.

Шаблон: 10 основни чекори за зголемување на дигиталната заштита

Следните основни чекори се препорачуваат за граѓанските организации во Северна Македонија:
- Инсталирајте и редовно ажурирајте антивирусен и анти-малициозен софтвер,
- Веднаш применувајте системски и софтверски ажурирања,
- Користете силни и уникатни лозинки за секоја сметка,
- Избегнувајте отворање прилози од непознати или сомнителни извори,
- Внесете чувствителни податоци само на шифрирани веб-страници,
- Правете редовни резервни копии на организациските податоци,
- Користете одделни е-адреси за различни цели,
- Спречете фишинг со рачно пишување адреси на веб-страници,
- Отстранете ги застарените или неподдржаните апликации,
- Ракувајте со личните и организациските податоци со претпазливост.

Шаблон – Внатрешни оперативни правила за дигитална безбедност

Секоја ГО треба да усвои едноставен интерен документ со кој ќе се дефинираат правилата за дигитална безбедност за персоналот, волонтерите и посетителите. Документот треба да вклучува:
- Користете уникатни лозинки за секоја сметка,

• Не споделувајте лозинки преку апликации за разговор или е-пошта,
• Овозможете двофакторска автентикација за е-пошта, складирање во облак и администраторски сметки на социјалните медиуми,
• Користете менаџер за лозинки каде што е можно,
• Заклучете ги сите уреди со ПИН-кодови или лозинки,
• Овозможете автоматски ажурирања,
• Веднаш пријавете изгубени или украдени уреди,
• Проверете ги сите барања за промена на банкарски и плаќања,
• Користете мобилни жаришта кога работите надвор од просториите на ГО,
• Доделете пристап до социјалните медиуми само преку улоги на платформата,
• Одржувајте го бројот на администратори на минимум,
• Собирајте и чувајте само потребни лични податоци,
• Веднаш пријавете го секој безбедносен инцидент до назначеното одговорно лице.

Шаблон – План за одговор на инциденти (поедноставен)

Кога ќе се случи или се сомнева дека има инцидент со дигитална безбедност, мора да се преземат следниве чекори:

- Исклучете го засегнатиот уред од мрежата,
- Зачувајте докази поврзани со инцидентот,
- Информирајте го внатрешниот тим,
- Прво обезбедете ја е-поштата со промена на лозинките и овозможување на 2FA,
- Ресетирајте ги лозинките за сите засегнати сметки,
- Одјавете се од непознати или сомнителни сесии,
- Отстранете непознати администратори и поврзани апликации, пријавете инциденти на MKD-CIRT,
- Пријавете сомневање за сајбер криминал до полициските единици за сајбер криминал,
- Консултирајте се со Агенцијата за заштита на лични податоци доколку се сомневате дека е извршено нарушување на податоците,
- Проценете го влијанието на инцидентот и вратете ги системите од резервни копии,
- Ажурирајте ги уредите и софтверот,
- Направете преквалификација на персоналот,
- Ажурирајте ги внатрешните политики и контролните листи доколку е потребно.

Практични контролни листи за граѓанските организации во Северна Македонија

АНЕКС 1 – Дигитален безбедносен пејзаж за граѓанските организации во Северна Македонија

Овој анекс го опишува правниот, институционалниот и оперативниот контекст што влијае на организациите на граѓанското општество (ГО) во Северна Македонија. Тој ја поддржува

локализацијата на наставната програма за дигитална безбедност преку одразување на заедничките ризици, капацитети и практични потреби на ГО што работат во земјата.

Закани

Граѓанските организации во Северна Македонија најчесто се соочуваат со следниве закани за дигиталната безбедност:

- фишинг напади преку е-пошта и лажни институционални пораки
- инциденти со ransomware и губење на податоци поради недостаток или несоодветни резервни копии
- злоупотреба или откривање на необезбедени лични податоци
- ризици поврзани со употребата на лични лаптопи и мобилни уреди за организациска работа.

Оперативни предизвици

Во пракса, многу граѓански организации во Северна Македонија се соочуваат со следниве предизвици:

- Мала употреба на менаџери за лозинки и честа повторна употреба на лозинки,
- Неправилни или недостасувачки рутини за резервна копија на податоци,
- Употреба на нелиценциран или застарен софтвер,
- Недоволна безбедност на мобилните уреди,
- Ограничено усвојување на двофакторска автентикација,
- Недостаток на наменски средства за мерки за дигитална безбедност.

Правна и регулаторна рамка во Северна Македонија

На 27 април 2016 година, Европскиот парламент и Советот на Европската Унија ја усвоија Регулативата (ЕУ) 2016/679 за заштита на физичките лица во врска со обработката на лични податоци и за слободното движење на таквите податоци, со која се укинува Директивата 95/46/ЕЗ. Ова го означи почетокот на сеопфатен процес на реформи во областа на заштитата на личните податоци. По двегодишен транзициски период, Регулативата стана применлива низ целата Европска Унија на 25 мај 2018 година.

Оваа регулатива, попозната како GDPR, е целосно транспонирана во Република Северна Македонија преку донесување на Законот за заштита на личните податоци, кој стапи на сила на 24 февруари 2020 година.

Законот за заштита на личните податоци регулира седум основни принципи за обработка на лични податоци:
• законитост, праведност и транспарентност,
• ограничување на целта,
• минимизирање на податоците,
• точност,
• ограничување на складирањето,
• интегритет и доверливост,
• отчетност.

Невладините организации, како контролори на податоци, се должни да ги применуваат сите принципи кумулативно во секој случај на обработка на лични податоци и во текот на целиот животен циклус на податоците. Неприменувањето на кој било од овие принципи претставува прекршување на Законот за заштита на личните податоци. Главен орган одговорен за спроведување и надзор на Законот за заштита на личните податоци е Агенцијата за заштита на личните податоци.

Дополнително, во областа на сајбер безбедноста, Законот за безбедност на мрежни и информациски системи, донесен во јули 2025 година, претставува прва сеопфатна правна рамка што ја регулира сајбер безбедноста во Северна Македонија. Законот е усогласен со европската директива NIS2 и има за цел да воспостави високо и заедничко ниво на заштита на мрежните и информациските системи и во јавниот и во приватниот сектор.

Министерството за дигитална трансформација и Националниот тим за одговор на компјутерски инциденти (MKD-CIRT), кој работи во рамките на Агенцијата за електронски комуникации, се одговорни за следење, координирање и реагирање на инциденти со сајбер безбедност. Од важност за приватниот сектор, вклучително и за невладините организации, е преодниот период на имплементација што трае до 2027 година, во кој се очекува сите субјекти постепено да ги почитуваат обврските воведени со законот.

Чести закани и неодамнешни инциденти што влијаат врз граѓанските организации

Невладините организации во Северна Македонија, слично како и другите сектори, се многу ранливи на закани поврзани со сајбер безбедноста. Клучен предизвик е што многу сајбер инциденти остануваат непрепознаени или непријавени, што резултира со недостаток на сеопфатни и веродостојни податоци за инцидентите. Иако значителен број граѓански организации известуваат дека се информирани за законските измени и соодветно ги прилагодуваат своите оперативни практики, достапните податоци покажуваат дека многу организации не донеле внатрешни закони за заштита на личните податоци и не назначиле службеник за заштита на личните податоци.

Понатаму, процентот на вработени во граѓанските организации кои добиле формална обука за заштита на лични податоци останува многу низок. Со оглед на тоа што граѓанските организации често работат со ограничени финансиски ресурси и се соочуваат со тешкотии при распределбата на средства за обука на вработените, се препорачува да се воспостават структурирани механизми за соработка помеѓу Агенцијата за заштита на лични податоци и невладиниот сектор за да се олесни пристапот до можностите за обука.

Главен фактор на ризик за граѓанските организации е нивниот ограничен буџет за инвестиции во заштитата на податоци и сајбер безбедноста. Многу помали организации продолжуваат да користат нелиценциран или застарен софтвер, што значително ја зголемува нивната изложеност на сајбер закани. Во исто време, достапни се неколку прирачници и упатства на македонски јазик, кои можат да им помогнат на граѓанските организации во зајакнувањето на нивната дигитална безбедност.

Најидентификуваните закани вклучуваат:
• неможност за проверка на испраќачите пред кликнување на линкови или отворање пораки,
• ограничена употреба на менаџери за лозинки и честа повторна употреба на слични лозинки,
• неправилни или отсутни практики за резервна копија на податоци,
• употреба на нелиценциран и застарен софтвер,
• недоволни безбедносни мерки за мобилни уреди,
• многу ниска употреба на двофакторска автентикација.

Национална поддршка и ресурси

Неколку национални институции, вклучувајќи ја Агенцијата за заштита на лични податоци, Министерството за дигитална трансформација и Агенцијата за електронски комуникации, обезбедуваат поддршка и насоки за граѓанските организации насочени кон подобрување на дигиталната безбедност и заштитата на податоците. Сепак, потребни се понатамошни институционални напори, вклучително и систематско планирање и иницијативи финансирани од државата.

Поддршка се обезбедува и преку проекти на граѓанското општество финансирани првенствено од странски донатори за зголемување на дигиталната писменост кај

граѓанските организации и општата популација. Значаен пример е проектот „CyberShield: Овластени граѓани за сајбер отпорност“, во рамките на кој во 2025 година беа одржани три обуки за сајбер безбедност за организации што работат со маргинализирани групи. Како продолжение, беа развиени планови за дигитална безбедност за шест организации на граѓанското општество. Овие прилагодени планови имаат за цел да обезбедат систематско спроведување на практиките за сајбер безбедност, подобрување на организациската отпорност и индиректно подобрување на испораката на услуги до крајните корисници.

И покрај овие позитивни примери, ограниченото финансирање значи дека само мал број граѓански организации се во можност да имаат корист од ваквите иницијативи. Иако неколку прирачници и материјали за подигање на свеста се достапни на македонски јазик, неопходна е поширока и поодржлива соработка меѓу јавните власти и граѓанските организации за да се прошири пристапот до обуки и активности за градење капацитети. Зголемено финансирање и насочени програми се особено потребни за поддршка на директното образование и обука на персоналот на граѓанските организации.

Културен и оперативен контекст на граѓанските организации во Северна Македонија

Повеќето граѓански организации во Северна Македонија работат според модел базиран на донатори и проекти и обично имаат мали административни и оперативни тимови или во голема мера се потпираат на волонтери. Организациската работа често се извршува со користење на лични уреди и широко достапни дигитални услуги, како што се Google Workspace, Dropbox или Microsoft 365, честопати без соодветна лиценца.

Затоа, иницијативите за обука и градење капацитети треба да се фокусираат на практични и реални мерки, вклучувајќи:
- предностите од користењето лиценцирани производи и услуги,
- кампањи за подигнување на свеста „Размислете пред да кликнете“,
- редовни резервни копии на податоци и информации,
- активна и доследна употреба на двофакторска автентикација,
- обезбедување мобилни уреди и управување со нивната употреба,
- одговорни практики за лозинки,
- ефикасна употреба на решенија базирани на облак,
- зголемена свест за практиките за споделување податоци.

Нивоата на дигитална писменост во Северна Македонија остануваат недоволни, вклучително и во рамките на граѓанскиот сектор. Потребни се дополнителни средства, ресурси и координирани напори за да се постигне повисоко ниво на дигитална безбедност. Овие напори треба да се преточат во конкретни програми и практични акциони планови прилагодени на реалните потреби и капацитети на организациите на граѓанското општество.

Анекси и шаблони подготвени за употреба (Северна Македонија)

АНЕКС 1 – Дигитален безбедносен пејзаж за граѓанските организации во Северна Македонија

Овој анекс ги одразува правните, институционалните и оперативните реалности што влијаат врз организациите на граѓанското општество во Северна Македонија и ја поддржува локализацијата на наставната програма.

Закани
- Фишинг напади преку е-пошта и лажни институционални пораки,
- Инциденти со Ransomware и губење на податоци поради недостаток на резервни копии,
- Злоупотреба на необезбедени лични податоци,
- Ризици поврзани со употребата на лични лаптопи и мобилни уреди.

Оперативни предизвици
- Мала употреба на менаџери за лозинки и честа повторна употреба на лозинки,
- Неправилни или недостасувачки рутини за резервна копија на податоци,
- Употреба на нелиценциран или застарен софтвер,
- Недоволна безбедност на мобилните уреди,
- Ограничено усвојување на двофакторска автентикација,
- Недостаток на наменски средства за дигитални безбедносни мерки.

Шаблон: 10 основни чекори за зголемување на дигиталната заштита

Следните основни чекори се препорачуваат за граѓанските организации во Северна Македонија:
- Инсталирајте и редовно ажурирајте антивирусен и анти-малициозен софтвер,
- Веднаш применувајте системски и софтверски ажурирања,
- Користете силни и уникатни лозинки за секоја сметка,
- Избегнувајте отворање прилози од непознати или сомнителни извори,
- Внесете чувствителни податоци само на шифрирани веб-страници,
- Правете редовни резервни копии на организациските податоци,
- Користете одделни е-адреси за различни цели,
- Спречете фишинг со рачно пишување адреси на веб-страници,
- Отстранете ги застарените или неподдржаните апликации,
- Ракувајте со личните и организациските податоци со претпазливост.

Шаблон – Внатрешни оперативни правила за дигитална безбедност

Секоја ГО треба да усвои едноставен интерен документ со кој ќе се дефинираат правилата за дигитална безбедност за персоналот, волонтерите и посетителите. Документот треба да вклучува:
- Користете уникатни лозинки за секоја сметка,

• Не споделувајте лозинки преку апликации за разговор или е-пошта,
•Овозможете двофакторска автентикација за е-пошта, складирање во облак и администраторски сметки на социјалните медиуми,
• Користете менаџер за лозинки каде што е можно,
• Заклучете ги сите уреди со ПИН-кодови или лозинки,
• Овозможете автоматски ажурирања,
• Веднаш пријавете изгубени или украдени уреди,
• Проверете ги сите барања за промена на банкарски и плаќања,
• Користете мобилен хотспот кога работите надвор од просториите на ГО,
• Доделете пристап до социјалните медиуми само преку улоги на платформата,
• Одржувајте го бројот на администратори на минимум,
• Собирајте и чувајте само потребни лични податоци,
• Веднаш пријавете го секој безбедносен инцидент до назначеното одговорно лице.

Шаблон – План за одговор на инциденти (поедноставен)

Кога ќе се случи или се сомнева дека има инцидент со дигитална безбедност, мора да се преземат следниве чекори:

- Исклучете го засегнатиот уред од мрежата,
- Зачувајте докази поврзани со инцидентот,
- Информирајте го внатрешниот тим,
- Прво обезбедете ја е-поштата со промена на лозинките и овозможување на 2FA,
- Ресетирајте ги лозинките за сите засегнати сметки,
- Одјавете се од непознати или сомнителни сесии,
- Отстранете непознати администратори и поврзани апликации, пријавете инциденти на MKD-CIRT,
- Пријавете сомневање за сајбер криминал до полициските единици за сајбер криминал,
- Консултирајте се со Агенцијата за заштита на лични податоци доколку се сомневате дека е извршено кршење на податоците,
- Проценете го влијанието на инцидентот и вратете ги системите од резервни копии,
- Ажурирајте ги уредите и софтверот,
- Направете преквалификација на персоналот,
- Ажурирајте ги внатрешните политики и контролните листи доколку е потребно.

Практични контролни листи за граѓанските организации во Северна Македонија

АНЕКС 1 – Дигитален безбедносен пејзаж за граѓанските организации во Северна Македонија

Овој анекс го опишува правниот, институционалниот и оперативниот контекст што им влијае на организациите на граѓанското општество (ГО) во Северна Македонија. Тој ја

поддржува локализацијата на наставната програма за дигитална безбедност преку одразување на заедничките ризици, капацитети и практични потреби на ГО што работат во земјата.

Закани

Граѓанските организации во Северна Македонија најчесто се соочуваат со следниве закани за дигиталната безбедност:

- фишинг напади преку е-пошта и лажни институционални пораки
- инциденти со ransomware и губење на податоци поради недостаток или несоодветни резервни копии
- злоупотреба или откривање на необезбедени лични податоци
- ризици поврзани со употребата на лични лаптопи и мобилни уреди за организациска работа

Оперативни предизвици

Во пракса, многу граѓански организации во Северна Македонија се соочуваат со следниве предизвици:

- Мала употреба на менаџери за лозинки и честа повторна употреба на лозинки,
- Неправилни или недостасувачки рутини за резервна копија на податоци,
- Употреба на нелиценциран или застарен софтвер,
- Недоволна безбедност на мобилните уреди,
- Ограничено усвојување на двофакторска автентикација,
- Недостаток на наменски средства за мерки за дигитална безбедност.

Десет основни чекори за зголемување на дигиталната заштита

Следните основни чекори им се препорачуваат на граѓанските организации во Северна Македонија за да ја подобрат својата дигитална безбедносна позиција:

нсталирајте и редовно ажурирајте антивирусен и анти-малициозен софтвер.
рименувајте системски и софтверски ажурирања веднаш штом ќе бидат достапни.
ористете силни и уникатни лозинки за секоја сметка.
збегнувајте отворање прилози од непознати или сомнителни извори.
несете чувствителни податоци само на шифрирани веб-страници (HTTPS).
равете редовни резервни копии на организациските податоци.
ористете одделни е-адреси за различни цели (на пр. администрација, проекти, јавна комуникација).
пречете фишинг со рачно пишување адреси на веб-страници наместо кликнување на линкови.
тстранете ги застарените или неподдржаните апликации од уредите.
акувајте со личните и организациските податоци со претпазливост во секое време.

Внатрешни оперативни правила за дигитална безбедност

Секоја ГО треба да усвои едноставен интерен документ во кој ќе се дефинираат правилата за дигитална безбедност за персоналот, волонтерите и посетителите. Како минимум, овој документ треба да ги содржи следниве правила:

- ☐ Користете уникатни лозинки за секоја сметка.
- ☐ Не споделувајте лозинки преку апликации за разговор или е-пошта.
- ☐ Овозможете двофакторска автентикација за е-пошта, складирање во облак и администраторски сметки на социјалните медиуми.
- ☐ Користете менаџер за лозинки каде што е можно.
- ☐ Заклучете ги сите уреди со ПИН-кодови, лозинки или биометриска заштита.
- ☐ Овозможете автоматски ажурирања на системот и апликациите.
- ☐ Веднаш пријавете изгубени или украдени уреди.
- ☐ Проверете ги сите барања за промена на банкарските податоци и плаќањата преку секундарен канал.
- ☐ Користете мобилни жаришта кога работите надвор од просториите на граѓанските организации.
- ☐ Доделувајте пристап до социјалните медиуми само преку функциите за улоги на платформата.
- ☐ Ограничете го бројот на администратори на минимум.
- ☐ Собирајте и чувајте само неопходни лични податоци.
- ☐ Веднаш пријавете го секој безбедносен инцидент кај назначеното одговорно лице.

План за одговор на инциденти за граѓанските организации во Северна Македонија

Кога ќе се случи инцидент со дигитална безбедност или кога постои сомневање за него, треба да се преземат следниве чекори:

склучете го засегнатиот уред од мрежата.
ачувајте ги доказите поврзани со инцидентот (слики од екранот, логови, пораки).
нформирајте го внатрешниот тим и назначеното одговорно лице.
рво обезбедете ја е-поштата со промена на лозинките и овозможување на двофакторска автентикација.
есетирајте ги лозинките за сите засегнати сметки.
дјавете се од непознати или сомнителни активни сесии.
тстранете ги непознатите администратори и поврзаните апликации.
ријавете инциденти во MKD-CIRT.
ријавете сомневање за сајбер криминал до полициските единици за сајбер криминал.
онсултирајте се со Агенцијата за заштита на лични податоци доколку се сомневате дека е направена повреда на лични податоци.
роценете го влијанието на инцидентот.
ратете ги системите и податоците од резервни копии каде што е можно.
журирајте ги уредите и софтверот.
реквалификувајте го персоналот и волонтерите доколку е потребно.
журирајте ги внатрешните политики и контролните листи врз основа на научените лекции.

АНЕКС 1 – Дигитален безбедносен пејзаж за граѓанските организации во Северна Македонија

Овој анекс ги одразува правните, институционалните и оперативните реалности што влијаат врз организациите на граѓанското општество во Северна Македонија и ја поддржува локализацијата на наставната програма.

Закани
- Фишинг напади преку е-пошта и лажни институционални пораки,
- Инциденти со Ransomware и губење податоци поради недостаток на резервни копии,
- Злоупотреба на необезбедени лични податоци,
- Ризици поврзани со употребата на лични лаптопи и мобилни уреди.

Оперативни предизвици
- Мала употреба на менаџери за лозинки и честа повторна употреба на лозинки,
- Неправилни или недостасувачки рутини за резервна копија на податоци,
- Употреба на нелиценциран или застарен софтвер,
- Недоволна безбедност на мобилните уреди,
- Ограничено усвојување на двофакторска автентикација,
- Недостаток на наменски средства за дигитални безбедносни мерки.

Шаблон: 10 основни чекори за зголемување на дигиталната заштита

Следните основни чекори се препорачуваат за граѓанските организации во Северна Македонија:
• Инсталирајте и редовно ажурирајте антивирусен и анти-малициозен софтвер,
• Веднаш применувајте системски и софтверски ажурирања,
• Користете силни и уникатни лозинки за секоја сметка,
• Избегнувајте отворање прилози од непознати или сомнителни извори,
• Внесете чувствителни податоци само на шифрирани веб-страници,
• Правете редовни резервни копии на организациските податоци,
• Користете одделни е-адреси за различни цели,
• Спречете фишинг со рачно пишување адреси на веб-страници,
• Отстранете ги застарените или неподдржаните апликации,
• Ракувајте со личните и организациските податоци со претпазливост.

Шаблон – Внатрешни оперативни правила за дигитална безбедност

Секоја ГО треба да усвои едноставен интерен документ со кој ќе се дефинираат правилата за дигитална безбедност за персоналот, волонтерите и посетителите. Документот треба да вклучува:
• Користете уникатни лозинки за секоја сметка,
• Не споделувајте лозинки преку апликации за разговор или е-пошта,
• Овозможете двофакторска автентикација за е-пошта, складирање во облак и администраторски сметки на социјалните медиуми,
• Користете менаџер за лозинки каде што е можно,
• Заклучете ги сите уреди со ПИН-кодови или лозинки,
• Овозможете автоматски ажурирања,
• Веднаш пријавете изгубени или украдени уреди,
• Проверете ги сите барања за промена на банкарски податоци и плаќања,
• Користете мобилни жаришта кога работите надвор од просториите на ГО,
• Доделете пристап до социјалните медиуми само преку улоги на платформата,
• Одржувајте го бројот на администратори на минимум,
• Собирајте и чувајте само потребни лични податоци,
• Веднаш пријавете го секој безбедносен инцидент до назначеното одговорно лице.

Шаблон – План за одговор на инциденти (поедноставен)

Кога ќе се случи или се сомнева дека има инцидент со дигитална безбедност, мора да се преземат следниве чекори:

- Исклучете го засегнатиот уред од мрежата,
- Зачувајте докази поврзани со инцидентот,
- Информирајте го внатрешниот тим,
- Прво обезбедете ја е-поштата со промена на лозинките и овозможување на 2FA,

- Ресетирајте ги лозинките за сите засегнати сметки,
- Одјавете се од непознати или сомнителни сесии,
- Отстранете непознати администратори и поврзани апликации, пријавете инциденти на MKD-CIRT,
- Пријавете сомневање за сајбер криминал до полициските единици за сајбер криминал,
- Консултирајте се со Агенцијата за заштита на лични податоци доколку се сомневате дека е извршено кршење на податоците,
- Проценете го влијанието на инцидентот и вратете ги системите од резервни копии,
- Ажурирајте ги уредите и софтверот,
- Преквалификувајте го персоналот,
- Ажурирајте ги внатрешните политики и контролните листи доколку е потребно.

Практични контролни листи за граѓанските организации во Северна Македонија

АНЕКС 1 – Дигитален безбедносен пејзаж за граѓанските организации во Северна Македонија

Овој анекс го опишува правниот, институционалниот и оперативниот контекст што влијае на организациите на граѓанското општество (ГО) во Северна Македонија. Тој ја поддржува локализацијата на наставната програма за дигитална безбедност преку одразување на заедничките ризици, капацитети и практични потреби на ГО што работат во земјата.

Закани

Граѓанските организации во Северна Македонија најчесто се соочуваат со следниве закани за дигиталната безбедност:

- фишинг напади преку е-пошта и лажни институционални пораки,
- инциденти со ransomware и губење податоци поради недостаток или несоодветни резервни копии,
- злоупотреба или откривање необезбедени лични податоци,
- ризици поврзани со употребата на лични лаптопи и мобилни уреди за организациска работа.

Оперативни предизвици

Во пракса, многу граѓански организации во Северна Македонија се соочуваат со следниве предизвици:

- Мала употреба на менаџери за лозинки и честа повторна употреба на лозинки,
- Неправилни или недостасувачки рутини за резервна копија на податоци,
- Употреба на нелиценциран или застарен софтвер,
- Недоволна безбедност на мобилните уреди,

- Ограничено усвојување на двофакторска автентикација,
- Недостаток на наменски средства за мерки за дигитална безбедност.

Десет основни чекори за зголемување на дигиталната заштита

Следните основни чекори се препорачуваат за граѓанските организации во Северна Македонија за да ја подобрат својата дигитална безбедносна позиција:

нсталирајте и редовно ажурирајте антивирусен и анти-малициозен софтвер.
рименувајте системски и софтверски ажурирања веднаш штом ќе бидат достапни.
ористете силни и уникатни лозинки за секоја сметка.
збегнувајте отворање прилози од непознати или сомнителни извори.
несете чувствителни податоци само на шифрирани веб-страници (HTTPS).
равете редовни резервни копии на организациските податоци.
ористете одделни е-адреси за различни цели (на пр., администрација, проекти, јавна комуникација).
пречете фишинг со рачно пишување адреси на веб-страници наместо кликнување на линкови.
тстранете ги застарените или неподдржаните апликации од уредите.
акувајте со личните и организациските податоци со претпазливост во секое време.

Внатрешни оперативни правила за дигитална безбедност

Секоја ГО треба да усвои едноставен интерен документ во кој ќе се дефинираат правилата за дигитална безбедност за персоналот, волонтерите и посетителите. Како минимум, овој документ треба да ги содржи следниве правила:

- ☐ Користете уникатни лозинки за секоја сметка.
- ☐ Не споделувајте лозинки преку апликации за разговор или е-пошта.
- ☐ Овозможете двофакторска автентикација за е-пошта, складирање во облак и администраторски сметки на социјалните медиуми.
- ☐ Користете менаџер за лозинки каде што е можно.
- ☐ Заклучете ги сите уреди со ПИН-кодови, лозинки или биометриска заштита.
- ☐ Овозможете автоматски ажурирања на системот и апликациите.
- ☐ Веднаш пријавете изгубени или украдени уреди.
- ☐ Проверете ги сите барања за промена на банкарските податоци и плаќањата преку секундарен канал.
- ☐ Користете мобилни жаришта кога работите надвор од просториите на граѓанските организации.
- ☐ Доделувајте пристап до социјалните медиуми само преку функциите за улоги на платформата.
- ☐ Ограничете го бројот на администратори на минимум.
- ☐ Собирајте и чувајте само неопходни лични податоци.
- ☐ Веднаш пријавете го секој безбедносен инцидент кај назначеното одговорно лице.

План за одговор на инциденти за граѓанските организации во Северна Македонија

Кога ќе се случи инцидент со дигитална безбедност или кога постои сомневање за него, треба да се преземат следниве чекори:

склучете го засегнатиот уред од мрежата.
ачувајте ги доказите поврзани со инцидентот (слики од екранот, логови, пораки).
нформирајте го внатрешниот тим и назначеното одговорно лице.
рво обезбедете ја е-поштата со промена на лозинките и овозможување на двофакторска автентикација.
есетирајте ги лозинките за сите засегнати сметки.
дјавете се од непознати или сомнителни активни сесии.
тстранете ги непознатите администратори и поврзаните апликации.
ријавете инциденти во MKD-CIRT.
ријавете сомневање за сајбер криминал до полициските единици за сајбер криминал.
онсултирајте се со Агенцијата за заштита на лични податоци доколку се сомневате дека е направена повреда на лични податоци.
роценете го влијанието на инцидентот.
ратете ги системите и податоците од резервни копии каде што е можно.
журирајте ги уредите и софтверот.
реквалификувајте го персоналот и волонтерите доколку е потребно.
журирајте ги внатрешните политики и контролните листи врз основа на научените лекции.

АНЕКС 2: Основна контролна листа за дигитална безбедност

Активност/Мерка	Означено (Д/Н)
2FA овозможен за сите онлајн продавници	
Уникатни лозинки што се користат за различни сметки	
Лозинките не се споделуваат во дигитална форма	
Заклучувањето на екранот е овозможено на сите уреди	
Автоматските ажурирања се вклучени	
Антивирусот е овозможен и ажуриран	
Wi-Fi за персоналот одвоен од гостинот	
Овозможено е креирање резервни копии на податоци	
Различни улоги на страницата на социјалните медиуми	
Е-поштата/телефонот за враќање му припаѓаат на CSO	
Користење на Wi-Fi на администраторски уреди во јавни места преку хотспот	
Ги затворив и исклучив сите уреди по работа	

АНЕКС 3: Контролна листа за пријавување инциденти

Активност/Мерка	Означено (Д/Н)
Засегнатите уреди се исклучени од интернет	
Доказите од нападот беа земени	

Променети се лозинките за е-пошта и други социјални мрежи	
Идентификувани се засегнати податоци	
Непознати администратори/апликации се отстранети	
Овозможено 2FA	
Внатрешниот тим беше информиран за тоа што се случило.	
Банкарските и платежните детали се оневозможени на уредот	
Одговорниот орган/институција беше информиран за нападот	

Правна и регулаторна рамка во Норвешка и предлози за граѓанските организации во Норвешка

Правна и регулаторна рамка во Норвешка

Граѓанските организации (ГО) што работат во Норвешка се предмет на Општата регулатива на ЕУ за заштита на податоци (GDPR) и норвешкиот Закон за лични податоци (Personopplysningsloven), кој го вклучува и дополнува GDPR во норвешкото законодавство. Овие законски рамки се однесуваат на сите организации што обработуваат лични податоци, вклучувајќи ги непрофитните и волонтерските организации, без оглед на големината. Надлежниот надзорен орган е Datatilsynet, норвешкиот орган за заштита на податоци.

Норвешките граѓански организации најчесто обработуваат лични податоци поврзани со корисници, членови, волонтери, донатори, вработени и, во многу случаи, ранливи групи. Таквите податоци може да вклучуваат имиња, контакт информации, финансиски информации, податоци поврзани со здравјето, евиденција на случаи или чувствителни информации за позадината. Како контролори на податоци, граѓанските организации се должни да ги почитуваат основните принципи на законот за заштита на податоците.

Клучните законски обврски вклучуваат:

Законска основа за обработка: Сите лични податоци мора да се обработуваат врз основа на валидна законска основа, како што се согласност, легитимен интерес, договорна неопходност или законска обврска.

Информирана согласност (доколку е применливо): Согласноста мора да биде дадена слободно, специфична, информирана и отповиклива.

Транспарентност: Поединците мора да бидат информирани за тоа како нивните податоци се собираат, користат, складираат, споделуваат и задржуваат преку јасни известувања за приватност.

Минимизирање на податоците и ограничување на намената: Може да се собираат и чуваат само податоци што се строго неопходни за дефинирани цели.

Безбедност на обработката: ГО мора да спроведат соодветни технички и организациски мерки за заштита на личните податоци од неовластен пристап, губење или злоупотреба.

Задржување и бришење податоци: Личните податоци не смеат да се чуваат подолго од потребното; мора да се дефинираат периоди на чување и рутини за бришење.

Управување со процесорот: Писмени договори за обработка на податоци мора да се одржуваат со сите надворешни даватели на услуги кои ракуваат со лични податоци.

Меѓународни трансфери на податоци: Личните податоци по можност треба да се чуваат во рамките на ЕУ/ЕЕА. Трансферите во трети земји бараат важечки заштитни мерки како што се стандардни договорни клаузули (SCC) и дополнителни мерки.

Известување за прекршување: Прекршувањата на личните податоци мора да се проценат брзо и, доколку е потребно, да се пријават на Datatilsynet во рок од 72 часа.

„Дататилсинет“ постојано идентификуваше заеднички предизвици меѓу норвешките граѓански организации, вклучувајќи нејасни рутини за согласност, небезбедно складирање

во облак надвор од ЕУ/ЕЕА, недостаток на документирани внатрешни процедури и прекумерно задржување на податоци.

Етички одговорности во заштитата на податоците

Надвор од законските обврски, норвешките граѓански организации имаат етичка должност да ја заштитат приватноста, достоинството и безбедноста на лицата чии податоци ги обработуваат. Многу граѓански организации работат со луѓе во ранливи ситуации – како што се бегалци, деца, жртви на насилство или политички експонирани лица – каде што изложеноста на податоци може да доведе до сериозна лична штета.

Пробивањето на податоците може да резултира со:

- Штета врз корисниците и волонтерите,
- Губење на довербата на донаторот, партнерот и јавноста,
- Правни последици и финансиски казни,
- Штета на угледот и нарушување на работењето.

Затоа, етичкото ракување со податоци бара претпазлив пристап: собирање на минимално потребните податоци, нивна ефикасна заштита и нивно споделување само кога е строго потребно.

Вградување на усогласеноста во секојдневната пракса

За многу норвешки граѓански организации, особено оние кои се потпираат на волонтери и ограничен ИТ капацитет, усогласеноста мора да биде практична и одржлива.

Ефективната имплементација вклучува:

- Назначување одговорно лице за заштита на податоци и дигитална безбедност, дури и ако е со скратено работно време или во комбинација со друга улога.
- Развивање кратки и достапни интерни документи како што се Политика за заштита на податоци и упатства за ракување со податоци.
- Имплементирање рутини за контрола на пристап, вклучувајќи индивидуални кориснички сметки, пристап базиран на улоги и навремено отстранување неактивни корисници.
- Избор на безбедни решенија за складирање, по можност услуги во облак базирани на ЕУ/ЕЕА за лични податоци.
- Обезбедување договори за обработка на податоци со сите надворешни добавувачи.
- Обезбедување редовна обука за подигање на свеста за персоналот и волонтерите за фишинг, лозинки и безбедно ракување со податоци.
- Одржување едноставна рутина за одговор на инциденти што опфаќа идентификација, ограничување, документирање и ескалација.
- Вградувањето на овие рутини во секојдневните операции помага да се обезбеди континуирано, а не реактивно усогласување.

Студии на случај од Норвешка

Студија на случај 1: Подложност на фишинг за време на кампања за собирање средства (Осло, 2023)

Во 2023 година, мала хуманитарна невладина организација со седиште во Осло доживеа целна фишинг кампања за време на својата годишна акција за собирање средства. Напаѓачите создадоа лажна верзија на страницата за донации на невладината организација и испратија е-пошта до поддржувачите тврдејќи дека организацијата „го ажурирала својот систем за плаќање“. Неколку донатори ги внесоа податоците за нивната картичка пред невладината организација да стане свесна за измамата. Инцидентот ја наруши довербата на донаторите и бараше значително време и труд за решавање на проблемите со банките и засегнатите поддржувачи.

Основна комбинација од безбедносни мерки – како што се двофакторската автентикација на е-пошта сметки, следењето домени и обука на персоналот за црвени знамиња за фишинг – можеше да го намали влијанието на инцидентот или целосно да го спречи нападот.

Прашања за дискусија:

- Кои беа главните ранливости искористени во овој инцидент?
- Кои предупредувачки знаци можеа да укажуваат дека е-поштата и страницата за донации беа лажни?
- Кои основни дигитални безбедносни мерки можеби ја спречиле или ограничиле штетата?

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 1 – Основи на сајбер безбедноста:**
  Се користи како основен пример за фишинг и експлоатација на доверба насочени кон донатори и поддржувачи.
- **Модул 4 – Чести сајбер-закани (фишинг и социјален инженеринг):**
  Демонстрира напредни техники за фишинг, вклучувајќи лажни веб-страници и лажно претставување.
- **Модул 6 – Безбедност на социјалните медиуми и онлајн присуство:**
  Може да се спомене кога се дискутира за организацискиот углед, јавната доверба и безбедните практики за собирање средства преку интернет.
- **Модул 7 – Развивање на безбедносна култура:**
  Поддржува дискусија за свеста на персоналот, протоколите за комуникација со донаторите и превентивната обука.

Препорачана употреба:

Анализа на случај проследена со групна вежба за идентификување на црвени знамиња за фишинг во комуникациите за собирање средства и дизајнирање листа за проверка за безбедна комуникација со донаторите.

Студија на случај 2: Деформирање на веб-страницата поради застарен приклучок (Берген,

Во 2022 година, мала невладина организација за човекови права со седиште во Берген ја оштети својата веб-страница на WordPress откако напаѓачите искористија застарен приклучок. Почетната страница беше заменета со политичка пропаганда, а организацијата го изгуби пристапот до административниот панел. Бидејќи невладината организација немаше неодамнешни резервни копии на веб-страницата, враќањето на страницата траеше повеќе од две недели и бараше надворешна техничка помош. Инцидентот ја наруши комуникацијата со волонтерите и донаторите и предизвика проблеми со репутацијата.
Рутинските ажурирања на софтверот, силните администраторски лозинки, двофакторската автентикација и автоматизираните резервни копии значително би го намалиле влијанието на нападот.

Прашања за дискусија:

- Кои технички и организациски слабости придонесоа за овој инцидент?
- Како недостатокот на резервни копии влијаеше врз способноста на организацијата да закрепне?
    - Кои превентивни мерки дискутирани во клучните теми на модулот би можеле да помогнат во избегнувањето на слични инциденти во иднина?

Практични контролни листи за дигитална безбедност и заштита на податоци за граѓанските организации во Норвешка

Релевантен(и) модул(и) и употреба во наставната програма

- **Модул 3 – Безбедност на уреди и инфраструктура:**
  Основен случај што ги илустрира ризиците поврзани со застарен софтвер и небезбедна инфраструктура на веб-страницата.
- **Модул 5 – Заштита на податоци и усогласеност со прописите за приватност:**
  Ја нагласува важноста на достапноста на податоците, интегритетот и резервните копии за организацискиот континуитет.
- **Модул 6 – Безбедност на социјалните медиуми и онлајн присуство:**
  Релевантно за дискусии за интегритетот на веб-страницата, управувањето со репутацијата и контролата на содржината.
- **Модул 7 – Развивање на безбедносна култура:**
  Поддржува свест за споделена одговорност за ажурирања и одржување, а не само за „ИТ задачи“.

Препорачана употреба:
Дискусија базирана на сценарија, проследена со практична вежба со листа за проверка за одржување на веб-страницата, рутини за ажурирање и планирање резервни копии.

АНЕКС-1: Контролна листа за усогласеност со законите и GDPR за граѓанските организации во Норвешка

☐Сите лични податоци обработени од организацијата се идентификувани и документирани.
☐За секоја активност на обработка е дефинирана и евидентирана законска основа.
☐Достапно е и доставено Известување за приватност/Политика за заштита на податоци.
☐Механизмите за согласност се јасни и отповикливи каде што е потребно.
☐Периодите за задржување на податоци се дефинирани и применети.
☐Постојат договори за обработка на податоци со сите надворешни даватели на услуги.
☐Личните податоци се чуваат во рамките на ЕУ/ЕЕА или се заштитени со важечки заштитни мерки.
☐Постои рутина за известување за повреда на податоци, а правилото од 72 часа е познато.

АНЕКС-2. Основна контролна листа за дигитална безбедност

☐За сите организациски сметки се користат силни, уникатни лозинки.

☐Се користи менаџер за лозинки.

☐Двофакторската автентикација е овозможена на сметките за е-пошта, облак и социјални медиуми.

☐Уредите се заштитени со заклучување на екранот и силни ПИН-кодови/лозинки.

☐Оперативните системи и апликациите се ажурираат автоматски.

☐Инсталиран е и ажуриран антивирусен/антивирусен софтвер.

☐Критичните податоци се зачувуваат редовно и безбедно.

АНЕКС -3. Контролна листа за управување со облак и сметки

☐Се користат индивидуални кориснички сметки; се избегнуваат споделени најавувања.

☐Правата на пристап се засноваат на улоги и се ограничени на неопходност.

☐Неактивните сметки се отстрануваат веднаш.

☐Дозволите за пристап до облакот периодично се прегледуваат.

☐Чувствителните датотеки се споделуваат со ограничувања и рок на истекување.

☐Дневниците на активности се овозможени каде што се достапни.

АНЕКС-4. Контролна листа за социјалните медиуми и онлајн присуството

☐Двофакторската автентикација е овозможена на сите сметки на социјалните медиуми.

☐Администраторските улоги се доделуваат индивидуално.

☐Е-пошта адресите и телефонските броеви за враќање се ажурирани.

☐Администраторските листи се прегледуваат редовно.

☐Постои план за одговор во случај на киднапирање на сметка или лажно претставување.

☐CMS-от и додатоците на веб-страницата редовно се ажурираат.

АНЕКС-5. Контролна листа за одговор и пријавување на инциденти

☐Назначено е лице одговорно за безбедноста.

☐Персоналот знае како интерно да пријавува сомнителни инциденти.

☐Постои писмена постапка за одговор на инциденти.

☐Доказите и логовите се зачувуваат по инцидентите.

☐Сериозните сајбер инциденти се пријавуваат на NorCERT кога е соодветно.

☐Пробивите на лични податоци се пријавуваат на Datatilsynet кога е потребно.

☐Научените лекции се документираат, а процедурите се ажурираат.

АНЕКС-6. Контролна листа за подигнување на свеста за вработените и волонтерите

☐Новите вработени и волонтери добиваат ориентација за безбедност и приватност.

☐Прифатливата употреба и политиките за заштита на податоци се признаваат.

☐Обезбедена е редовна обука за освежување на состојбата.

☐Постојат јасни правила за користење лични уреди за работа на граѓанските организации.

☐Чувствителните податоци не се споделуваат преку небезбедни канали.

Предлози и практични препораки

Норвешките граѓански организации треба да дадат приоритет на едноставните, добро документирани рутини пред сложените технички решенија. Со комбинирање на јасни внатрешни политики, основни технички заштитни мерки, редовна обука и етичка свест, организациите можат значително да ги намалат своите дигитални ризици, а воедно да ја одржат усогласеноста со GDPR и со норвешкиот закон.

Дополнителни точки специфични за Норвешка за кои граѓанските организации треба да бидат свесни

1. Промена на волонтери и управување со животниот циклус на пристап

Норвешките граѓански организации во голема мера се потпираат на краткорочни волонтери, практиканти и персонал со скратено работно време. Еден од најчестите ризици пријавени од Datatilsynet и NSM е неуспехот да се одземе пристапот кога поединците ја напуштаат организацијата.

Што треба да знаат граѓанските организации:

- Секое вклучување во тимот мора да има соодветна листа за проверка за исклучување од тимот,
- Сметките, пристапот до е-пошта, папките во облакот и улогите на социјалните медиуми мора веднаш да се отстранат,
- Споделените сметки драматично го зголемуваат ризикот во организациите базирани на волонтери,
- Оваа точка го зајакнува Модул 7 (Безбедносна култура и политики).

2. Национални идентификациски броеви и чувствителни идентификатори

Некои норвешки граѓански организации обработуваат fødselsnummer (национални идентификациски броеви), здравствени податоци, информации поврзани со азил или детали за правни случаи.

Зошто ова е важно:

- Овие типови на податоци бараат повисоки стандарди за заштита според GDPR,
- Складирањето во необезбедени табеларни пресметки или општи папки во облакот е практика со висок ризик,
- Шифрирањето и строгата контрола на пристапот се неопходни,
- Ова природно се вклопува во Модул 5 (Заштита на податоци и приватност), но може да се вкрсти во обуката за Модул 7.

3. Облак-услуги и свест за Schrems II

Многу норвешки граѓански организации користат глобални cloud услуги (Google, Microsoft, Dropbox) без да ги разберат импликациите од преносот на податоци.

Реалност специфична за Норвешка:

- Datatilsynet очекува граѓанските организации да бидат свесни за резиденцијата на податоците од ЕУ/ЕЕА,
- Трансферите надвор од ЕУ/ЕЕА бараат заштитни мерки (SCC + проценка на ризик),
- „Користиме голем провајдер“ не е доволно оправдување,
- Ова го зајакнува Модул 8 (Напредни теми) со правно-технички агол.

4. Координација помеѓу NorCERT и Datatilsynet

ГО често се збунуваат кому што да пријават.

Јасна разлика што граѓанските организации треба да ја знаат:

- NorCERT (NSM): сериозни инциденти со сајбер безбедност (ransomware, преземање на сметка, прекин на услугата),
- Datatilsynet: прекршувања на лични податоци (GDPR – во рок од 72 часа),
- За некои инциденти се потребни и двете известувања,
- Ова е клучен додаток на Модул 7 (Реагирање и пријавување на инциденти).

5. Психолошка безбедност и култура на известување без обвинување

Норвешката организациска култура силно ја цени довербата и рамните хиерархии – но ова може да се врати како бумеранг ако персоналот се плаши од срам.

Најдобра практика:

- Персоналот треба да биде охрабрен веднаш да пријавува грешки (кликнување на фишинг линк, губење на уред),
- Културата на необвинување ја намалува штетата и го подобрува времето на одговор,
- Ова е важен културен слој за Модул 7 што оди подалеку од техничките контроли.

6. Одговорност на одборот и надзор на управувањето

Во Норвешка, од одборите на граѓанските организации сè повеќе се очекува да го разберат дигиталниот ризик како дел од доброто управување.

Што треба да знаат одборите:

- Сајбер безбедноста и заштитата на податоците се прашања од управувањето, а не само ИТ прашања
- Одборите треба да одобрат основни безбедносни политики и планови за одговор на инциденти
- Сериозни инциденти може да имаат правни последици и последици по угледот за раководството
- Ова може да се додаде како белешка за управување во рамките на Модул 7 или Модул 8.

7. Граѓанското општество како стратешка цел

Норвешките граѓански организации кои работат на демократија, човекови права, надворешна политика или меѓународна помош се сметаат за стратешки цели, а не за случајни жртви.

Импликации:

- Нападите може да бидат постојани, суптилни и водени од разузнавачки информации
- Не сите закани имаат за цел пари – некои имаат за цел надзор или нарушување на односите.
- Свеста за брифинзите за закани од страна на NSM е од клучно значење.
- Ова ги зајакнува Модул 1 и Модул 8 со модел на закана специфичен за Норвешка.

ДОДАТОК

Додаток 1: Речник на клучни термини

- ***Антивирус (AV):*** *Софтвер што открива и отстранува малициозен софтвер (вируси, тројанци итн.) од компјутерите. Пример: Windows Defender или*

- ***Резервна копија:*** *Дополнителна копија од податоците складирани одделно за цели на обновување, на пр. зачувување датотеки на надворешен тврд диск или услуга во облак за да можат да се обноват доколку се изгубат оригиналите.*
- ***Напад со брутална сила:*** *Метод каде што напаѓачите пробуваат многу лозинки или клучеви додека не ја пронајдат точната. Силните лозинки и политиките за заклучување помагаат во одбраната од ова.*
- ***Пробив на податоци:*** *Инцидент каде што е пристапено до чувствителни информации или тие се откриваат без овластување. Може да се случи преку хакирање, губење уреди итн.*
- ***Шифрирање:*** *Процес на конвертирање на податоци во кодиран формат кој е нечитлив без клуч. Ја заштитува доверливоста на информациите (на пр. HTTPS го шифрира веб-сообраќајот).*
- ***Заштитен ѕид:*** *Уред или софтвер за мрежна безбедност што ги следи и филтрира дојдовните и појдовните мрежни пораки врз основа на безбедносни правила. Може да блокира неовластен пристап, а воедно да дозволи легитимна комуникација.*
- ***Малициозен софтвер:*** *Злонамерен софтвер дизајниран да им наштети или да ги експлоатира системите. Вклучува вируси, рансомвер, шпионски софтвер итн. Често се доставува преку прилози во е-пошта или злонамерни веб-страници.*
- ***Мултифакторска автентикација (MFA / 2FA):*** *Користење на повеќе од еден метод за верификација за најавување (на пр. лозинка + еднократен код на телефон). Драматично ја подобрува безбедноста на сметката.*
- ***Фишинг:*** *Измамнички обид (обично преку е-пошта) за измама на поединци да откријат чувствителни информации или да инсталираат малициозен софтвер, претставувајќи се како доверлив субјект. Спајр фишинг се однесува на насочени обиди кон одредени поединци или организации.*

  Малициозен софтвер што ги криптира податоците на жртвата и бара плаќање за клучот за декрипција. Доколку не постојат резервни копии, жртвите се соочуваат со притисок да им платат на хакерите за да го вратат пристапот.
- ***Социјален инженеринг:*** *Тактики што манипулираат со луѓето за да откријат доверливи информации или да извршуваат дејствија што ја загрозуваат безбедноста. Фишингот е една форма; други вклучуваат изговор или мамка. Ја искористува човечката доверба и љубопитност.*
- ***VPN (Виртуелна приватна мрежа):*** *Алатка што создава шифриран тунел преку интернет од вашиот уред до сервер, заштитувајќи ги податоците во*

пренос и маскирајќи ја вашата IP адреса. Корисна на јавен Wi-Fi за безбедна врска.

- ***Ранливост:*** *Слабост во софтверот, хардверот или постапката што напаѓачите можат да ја искористат за да добијат неовластен пристап или да извршат неовластени дејства. Поправката се справува со познати ранливости.*
- ***Шифрирање на Wi-Fi (WPA2/WPA3):*** *Безбедносни протоколи за безжични мрежи кои го шифрираат сообраќајот помеѓу уредите и рутерот. Осигурајте се дека вашиот Wi-Fi користи барем WPA2 со силна лозинка за да спречите прислушкување.*

Додаток II: Шаблон за политика за лозинки (пример)

Намена: Да се утврдат барања за креирање, користење и управување со лозинки за заштита на информациските системи на организацијата.

Опсег: Оваа политика се однесува на сите вработени, волонтери и изведувачи на [Име на организација] кои користат ИТ системи (вклучувајќи компјутери, е-пошта, апликации и веб-страници) за организациска работа.

Изјави за политиката:

ите кориснички лозинки мора да бидат долги најмалку 12 знаци, мешајќи големи и мали букви, броеви и специјални симболи.

тандардните лозинки мора да се променат веднаш по првата употреба.

озинките не смеат да се споделуваат меѓу поединци или да се запишуваат на небезбедни места.

вофакторската автентикација (2FA) е потребна за сите далечински пристапи до организациските системи и за сметките на е-пошта.

озинките за критичните системи (финансиски, бази на податоци на донатори) мора да се менуваат на секои 90 дена.

орисниците не смеат повторно да користат лозинки што биле користени на други (јавни) сметки или што протекле при пробивање на информациите.

околку постои сомневање дека лозинката е компромитирана, таа мора веднаш да се промени и за тоа мора да се извести службеникот за ИТ/безбедност.

Улоги и одговорности:

орисниците мора да ги следат овие правила и да го пријават секое сомнително компромитирање.

Т персоналот ќе ги спроведува правилата за лозинки преку технички контроли (на пр. менаџери за лозинки, заклучување на сметки по неуспешни обиди).

лужбеникот за безбедност ќе ја проверува усогласеноста и ќе ја ажурира политиката годишно.

Спроведување: Прекршувањата на оваа политика може да резултираат со одземање на привилегиите за пристап или други дисциплински мерки.

Додаток III: Шаблон за политика за резервна копија (пример)

Намена: За да се осигури дека критичните податоци редовно се зачувуваат и дека можат да се обноват во случај на загуба, оштетување или катастрофа.

Опсег: Важи за сите податоци складирани на организациските сервери, работни станици и мрежни уреди за складирање во [Име на организацијата].

Изјави за политиката:

ритичните податоци (евиденција на донатори, финансиски досиеја, бази на податоци за проекти итн.) мора да се зачувуваат најмалку еднаш дневно.

езервните копии треба да вклучуваат системски конфигурации и апликации потребни за враќање на операциите.

езервните копии мора да се чуваат безбедно надвор од локацијата или во посебен складишен простор во облакот за да се спречи губење од локални инциденти.

елосните резервни копии се прават неделно, со постепени резервни копии дневно (или почесто за високо чувствителни податоци).

роверките за интегритетот на резервната копија и тест-обновувањата мора да се вршат месечно за да се осигури дека податоците можат да се обноват.

адржување: Чувајте дневни резервни копии најмалку една цела на самото место и месечна целосна резервна копија архивирана надвор од локацијата најмалку една година.

ристапот до резервните копии на податоците е ограничен само на овластен ИТ или менаџерски персонал.

Улоги и одговорности:

Т персоналот мора да ги конфигурира и да ги следи автоматските резервни копии според овој распоред.

азначениот администратор за резервни копии ќе ги документира процедурите за резервни копии и ќе го потврди завршувањето и интегритетот на резервната копија.

елиот персонал е одговорен за зачувување на критичните работни датотеки на назначените локации што се вклучени во распоредот за резервна копија.

Спроведување: Непочитувањето може да резултира со губење на податоци и соодветно ќе се реши од страна на менаџментот на [Име на организација].

Додаток IV: Шаблон за попис на средства (пример)

ИД на средство	Име на средство	Категорија	Сопственик/Одделение	Локација	Ниво на чувствителност	Потребна е заштита	Белешки
A001	База на податоци за донатори	Софтвер/Податоци	Директор на програмата	На самото место	Висок	Шифрирано, заштитено со лозинка	Содржи информации за донаторите
A002	Финансиски сервер	Хардвер/Сервер	ИТ оддел	Центар за податоци	Висок	Редовни резервни копии, 2FA за пристап	Поддржува софтвер за сметководство
A003	Лаптопи	Хардвер/Уред	Различен персонал	Канцеларија /Терен	Средно	Присилно енкрипција на диск, лозинка	Секој уред има идентификациска ознака
A004	Веб-страница	Софтвер	Комуникации	Хостирано во облак	Средно	HTTPS е овозможен, CMS е ажуриран	Веб-страница наменета за јавноста
A005	CRM софтвер	Софтвер	Менаџер на податоци	Облак	Висок	Пристап базиран на улоги, дневни резервни копии	Ги следи информациите за корисниците

(Забелешка: „Ниво на чувствителност“ може да биде Ниско/Средно/Високо. „Потребна заштита“ ги наведува безбедносните мерки за секое средство.)

Додаток V: Едноставен образец за матрица на ризик (пример)

	Влијание: Ниско (1)	**Влијание: Средно (2)**	**Влијание: Високо (3)**
Веројатност: Висока (3)	Висок ризик (3×1)	Критичен ризик (3×2)	Критичен ризик (3×3)
Веројатност: Средна (2)	Среден ризик (2×1)	Висок ризик (2×2)	Критичен ризик (2×3)
Веројатност: Ниска (1)	Низок ризик (1×1)	Среден ризик (1×2)	Висок ризик (1×3)

- **Нивоа на ризик:** Пресметајте го ризикот со множење на оценките за веројатност и влијание. На пример, сценарио оценето со Веројатност=3 (Висока) и Влијание=2 (Средна) дава оценка за ризик од 6 (Критичен ризик).
- Користете ја оваа матрица за прво да дадете приоритет на решавањето на сценаријата со повисок ризик (Критично > Високо > Средно > Ниско).

ЗАКЛУЧОК

Дигиталната безбедност не е еднократен проект или поле што треба да се означи – тоа е обврска на организациите за граѓански организации. Заклучувајќи ја оваа е-книга, сакаме повторно да ја потврдиме централната лекција што одекнува низ секое поглавје: одржувањето на безбедноста на нашите организации на граѓанското општество онлајн бара континуирано внимание, адаптација и грижа. Пејзажот на сајбер закани што го дискутиравме на почетокот постојано се развива, при што, напаѓачите секојдневно бараат нови начини да ја пробијат одбраната. Она што го обезбедуваме денес може да биде тестирано со нови тактики утре.

Оваа реалност значи дека дигиталната безбедност мора да остане на нашиот радар на долг рок, како составен дел од нашето планирање и работење како буџетирањето или управувањето со програми. Не можеме да си дозволиме да ја третираме сајбер безбедноста како дополнителна мисла; наместо тоа, таа треба да стане вообичаен дел од начинот на кој работиме. Влоговите се едноставно превисоки – кога едно успешно хакирање може да открие чувствителни податоци на корисниците или да попречи кампања за застапување, будноста во дигиталната безбедност е дел од исполнувањето на нашите мисии. Знаењето и стратегиите што ги стекнавте од оваа е-книга се основа врз која може да се гради. Во иднина, останувањето безбедно ќе значи редовно преиспитување на овие теми, ажурирање на вашите практики како што се појавуваат нови закани (и решенија) и поттикнување средина каде што учењето за безбедноста е континуиран процес. Накратко, работата на дигиталната безбедност никогаш не е „завршена“, но ниту е непремостлива. Со секој чекор што го преземате за да ја зајакнете сајбер-одбраната на вашата организација, придонесувате за поотпорно граѓанско општество.

Одржувањето на безбедноста е лесно: Еден клучен заклучок е дека безбедноста не мора да биде премногу комплицирана. Честопати, станува збор за доследно извршување на едноставните работи. Користете силни, уникатни лозинки (и менаџер за лозинки). Одржувајте го вашиот софтвер ажуриран. Размислете двапати пред да кликнете на неочекувани линкови. Редовно правете резервна копија на вашите податоци. Овие основни практики, кога се вкоренети, се справуваат со голем процент од заканите. Како што видовме, многу напади успеваат поради занемарени основи – па затоа со нивно почитување, ги затворате вообичаените врати што ги искористуваат напаѓачите.

Прилагодување на нови предизвици: Дигиталниот свет ќе продолжи да се менува. Пред пет години, ransomware не беше толку доминантен; денес тој е најголема закана. Во иднина, можеби ќе се соочиме со напади врз алатки за вештачка интелигенција или пософистициран deepfake фишинг. Вашиот CSO треба да остане прилагодлив и да продолжи да учи. Претплатете се на релевантен безбедносен канал или придружете се на заедница каде што се дискутираат нови закани – на тој начин, ќе добиете рано предупредување за нови проблеми. Размислете за периодична обука за освежување на знаењето или нови модули за персоналот кога нешто значајно ќе се промени (на пример, ако мобилниот малициозен софтвер се зголеми, направете посебна сесија за тоа). Прифатете го начинот на размислување за континуирано подобрување, третирајќи го секој инцидент или инцидент што се случил речиси како можност за учење за понатамошно зајакнување на одбраната.

Мудро распределување на ресурсите: Безбедноста е инвестиција во одржливоста на вашата организација. Можеби ќе бара одреден буџет (за подобра опрема, софтвер или време за обука) и внимание од менаџментот. Но, како што е прикажано, цената на необезбедување (пробиви, застој, изгубена доверба) е многу поголема. Планирајте ја безбедноста во вашата долгорочна стратегија – на пр. вклучете ставка во грантови за технолошки ажурирања или обука. Искористете бесплатни или намалени услуги за граѓанските организации (има многу, од бесплатен Google Workspace до донирани firewall-ови) како што е дискутирано во Поглавје 6. Исто така, размислете за назначување лице за безбедност (дури и ако не е со полно работно време) кое ги следи безбедносните задачи и развој – имањето некој одговорен осигурува дека нема да пропадне.

Поддршка од раководството: Одржливата безбедност бара поддршка од раководството. Кога лидерите ја даваат безбедноста како приоритет – преку моделирање добри практики и распределба на ресурси – тоа испраќа јасна порака дека ова е важно за сите. Исто така, се спротивставува на секој отпор (како „дали навистина треба да се мачиме со ова?“): ако директорот се најавува на 2FA и присуствува на истите обуки, тоа го легитимира напорот. Затоа, осигурајте се дека вашиот менаџерски тим е целосно вклучен во процесот, па дури и се залага за безбедносни иницијативи.

Вклучете го целиот ваш тим**:** Безбедната иднина зависи од тоа секој да игра улога. Од најновиот практикант до членовите на одборот, секоја личност има улога во синџирот. Одржувајте ја безбедноста инклузивна: охрабрувајте прашања, не срамотете ги кога грешат, наградете ја будноста. Некои организации вклучуваат безбедносна компетентност во прегледите на перформансите или описите на работните места, нагласувајќи дека тоа е очекување за сите улоги. Со овластување на персоналот – давајќи им знаење и алатки - во суштина сте изградиле човечки заштитен sид околу вашата ГО. Како што вели една поговорка, „безбедносната свест на корисниците е најевтиниот и најефикасниот заштитен sид што можете да го имате“.

Гледајќи напред со оптимизам: Може лесно да се почувствувате заплашени од сајбер заканите, но запомнете дека знаењето и подготовката силно ја навалуваат рамнотежата во ваша корист. Многу граѓански организации низ целиот свет, дури и оние со недоволно ресурси, успешно се одбранија со тоа што беа проактивни и обединети. Со читањето на оваа е-книга и спроведувањето на нејзините упатства, направивте важен чекор кон обезбедување на дигиталната иднина на вашата организација. Тоа е патување – ќе има пречки и евентуални инциденти – но секој чекор што го преземате сега го намалува влијанието на нив и го забрзува вашето закрепнување.

Во свет каде што граѓанското општество понекогаш е конкретно цел на сајбер напади, вашата посветеност на дигиталната безбедност е, исто така, посветеност на вашата кауза и луѓето на кои им служите. Тоа значи дека вашата важна работа може да продолжи без да биде попречена од пречки што може да се спречат. Тоа значи дека довербата што луѓето ја имаат во вас – за ракување со нивните податоци или за засилување на нивните гласови – е добро основана.

Како заклучок, да резимираме неколку долгорочни безбедносни навики што треба да ги развиеме:

- *Редовно проверувајте ја вашата проценка на ризик и ажурирајте го вашиот план за безбедност (најмалку еднаш годишно или кога ќе се случат поголеми промени).*
- *Продолжете да учите – присуствувајте на тој вебинар, прочитајте го тој водич, споделете сознанија со колегите.*
- *Останете поврзани – не ги изолирајте вашите безбедносни напори; бидете дел од заедницата што учи и се брани заедно.*
- *Бидете подготвени – одржувајте го вашиот план за одговор на инциденти и повремено тестирајте го за да биде подготвен доколку е потребно.*
- *Останете будни – но не и да се плашите. Со воспоставени добри практики, можете да бидете самоуверени и смирени, а не вознемирени, во врска со дигиталните закани.*

Кон сигурна иднина: Со тоа што дигиталната безбедност ќе стане составен дел од секојдневното работење и култура на вашата граѓанска организација, вие сте во добра позиција да се соочите со иднината. Несомнено ќе се појават предизвици, но вие ги имате алатките, знаењето и поддршката за да ги надминете. Правејќи го тоа, вие не само што ја заштитувате вашата организација, туку придонесувате и за побезбедна дигитална средина за поширокото граѓанско општество.

Продолжувајќи напред, посветете се на континуирано подобрување. Прославете ги вашите безбедносни победи (дури и мали како „никој не нападна фишинг овој квартал!“ или „успешно ги вративме податоците од резервна копија по мал пад на серверот“). Учете од сите неуспеси. И секогаш запомнете ја причината: безбедна организација за заштита на лични податоци може подобро да ја исполни својата мисија и да направи позитивно влијание без прекин.

Градењето отпорност е уште една тема што ја нагласивме и заслужува повторно да се нагласи овде на заклучокот. Отпорноста значи не само обид за спречување на напади, туку и осигурување дека вашата организација може да закрепне ако нешто тргне наопаку. Станува збор за тоа да имате резервни копии за нападот со ransomware да не ги осакатува вашите операции, за тоа да имате планови за одговор за да може да се контролира и да се учи од инцидентот со фишинг, како и за негување организациски начин на размислување кој ги гледа неуспесите како можности за подобрување. Додека продолжувате со вашата работа, запомнете дека секој предизвик може да ве направи посилни ако се соочите со подготовка и размислување. Ако се случи безбедносен инцидент, користете го како искуство за учење за да ги усовршите вашите политики и обука. Прославете го напредокот што сте го постигнале – на пример, превртувајќи ја статистиката „80% од организациите без план за безбедност“ наопаку во вашиот сопствен контекст со воспоставување робустен план. И продолжете да се едуцирате себеси и вашиот тим. Областа на дигиталната безбедност се развива брзо, но има повеќе ресурси од кога било досега (многу од нив ги наведовме во Поглавје 7 и додатоците) за да ве информираме. Размислете за периодични работилници за освежување на знаењето, претплатете се на известувања или билтени за сајбер безбедност за непрофитни организации и охрабрете ги помладите вработени или волонтери со ИТ интереси да преземат улоги како „шампиони за дигитална безбедност“ во

вашата организација. Континуираното учење е камен-темелник на отпорноста. Ве одржува агилни и подготвени да се соочите со сè што дигиталниот свет ви фрла на патот.

Гледајќи напред, останuваме оптимисти и гледаме напред кон иднината на граѓанското општество во дигиталното доба. Да, предизвиците се значајни – сајбер нападите стануваат сè пософистицирани и мора да останеме будни. Но, напредокот постигнат дури и во последните неколку години е охрабрувачки. Сè повеќе организации се будат за важноста на дигиталната безбедност, а структурите за поддршка полека, но сигурно се зајакнуваат. Гледаме развој на алатки и услуги прилагодени за непрофитни организации, зголемена свест кај донаторите и институциите за финансирање на потребите за сајбер безбедност и поголемо глобално внимание кон концептот на „дигитална отпорност“ за заедниците. Секое поглавје од оваа е-книга не само што понуди предупредувачки упатства, туку и ги истакна можностите – можноста да ја свртиме технологијата во наша корист, да иновираме во начинот на кој се заштитуваме и да обликуваме дигитална средина што ги поддржува нашите вредности. Како што забележавме, сајбер заканите ќе продолжат да се развиваат, но, исто така, може да се развива и нашата одбрана. Со премостување на преостанатите празнини во знаењето и капацитетот, со зајакнување на партнерствата и со тоа што сајбер безбедноста ќе биде приоритет за оние на кои им е најпотребна, можеме да создадеме побезбеден дигитален екосистем каде што граѓанското општество може да ја продолжи својата критична работа без страв.

На крајот, сакаме да ве оставиме со една охрабрувачка мисла: секој напор што го вложувате во дигиталната безбедност е инвестиција во слободата и интегритетот на вашата работа и луѓето на кои им служите. Секоја нова политика за лозинки, секоја шифрирана база на податоци, секоја обука на персоналот – сите тие создаваат посилен штит што ги штити човековите права, социјалната правда и иницијативите за благосостојба на заедницата низ целиот свет. Фактот дека ја прочитавте оваа е-книга и се вклучивте во овие теми е позитивен чекор кон побезбедна иднина. Ве охрабруваме да ја продолжите оваа посветеност. Споделете го она што сте го научиле со колегите и со партнерските организации. Одржувајте го разговорот за дигиталната безбедност жив на вашите стратешки состаноци и сесии за планирање. Застапувајте се за ресурсите и поддршката што ви се потребни – без разлика дали тоа е финансирање за подобра инфраструктура или едноставно време доделено на персоналот да учи и имплементира безбедносни мерки – затоа што дигиталната безбедност вреди. Согледувањето кон иднината е дека со вградување на безбедноста во нашата секојдневна работа, правиме повеќе отколку само да ги заштитуваме нашите организации; им овозможуваме да напредуваат. Безбедната организација на граѓанското општество може да зборува погласно, да дејствува похрабро и да стигне подалеку, знаејќи дека нејзиниот глас не може лесно да се замолчи од дигиталните закани.

Еден од најохрабрувачките сознанија од проектот КА220 и оваа е-книга е дека не сме сами во соочувањето со овие предизвици. Всушност, соработката е една од нашите најсилни предности. Ако има една порака што треба да ја пренесеме, тоа е дека сме побезбедни заедно. Сајбер заканите честопати можат да се чувствуваат изолирано – мала непрофитна организација може да се чувствува надмината во однос на софистициран хакер – но колективната моќ на граѓанското општество, работејќи заедно, може да ја навали

рамнотежата. Во текот на овој проект, бевме инспирирани од примерите на организации кои се здружуваат за да споделат експертиза, од мрежи на дигитални волонтери кои помагаат и од партнерства што се формирале преку границите за справување со заедничките безбедносни прашања. Патот до дигиталната безбедност не е осамен; тоа е споделено патување. Со отворено комуницирање за заканите и инцидентите, со споделување алатки и успешни приказни и со меѓусебно поддржување во итни случаи, организациите на граѓанското општество ги засилуваат своите одбранбени способности. Покрај тоа, широката соработка надвор од непрофитниот сектор е од суштинско значење. Треба да продолжиме да градиме партнерства со сојузници во владата, академијата и технолошката индустрија кои се посветени на заштитата на отворениот и безбеден интернет на кој се потпира граѓанското општество. Како што забележаа експертите и глобалните сајбер лидери, одбраната на ризичните групи ефикасно „бара инвестиции во решенија за сајбер безбедност, соработка меѓу засегнатите страни и иновативни модели на финансирање за долгорочна отпорност“. Ниту една организација – без разлика колку е добро обезбедена со ресурси – не може сама да се справи со сите аспекти на дигиталната безбедност. Ќе биде потребна заедница на практичари, која опфаќа различни сектори и експертиза, за да се обезбеди дека заштитните мерки се достапни, ефикасни и одржливи на долг рок. Ве охрабрувам да ги побарате овие соработки: придружете се на безбедносни форуми и коалиции, ангажирајте се во иницијативи кои нудат помош за сајбер безбедност на граѓанските организации и не двоумете се да побарате помош од колеги или да ја понудите вашата. Со зајакнување на овие врски, создаваме обединет фронт кој може брзо да одговори на заканите и да спречи малите проблеми да станат големи кризи.

Ви благодариме што сте дел од ова патување за развој на дигитална безбедносна инфраструктура преку граѓанското општество. Заклучокот од овој учебник не е крај, туку почеток – почетна точка на нови иницијативи, разговори и соработки што ќе продолжат и по овие страници. Останете љубопитни, останете будни и останете обединети. Заедно, ќе изградиме дигитална средина каде што граѓанското општество не само што е безбедно, туку и овластено да ја искористи технологијата во одбрана на каузите што ни се драги. Со отпорност, соработка и континуирано учење како наши водичи, се движиме напред во иднина каде што организации како вашата можат со сигурност да прифатат иновации и да водат општествени промени, поддржани од робусна основа на дигитална безбедност. Да продолжиме со оваа важна работа – нашите заедници сметаат на тоа, а алатките и сојузниците што ни се потребни се на дофат. На здравје за побезбедно, посилно и поовластено граѓанско општество во дигиталната ера.

Co-funded by the European Union

Практичниот водич за дигитална трансформација и наставна програма за зајакнување на дигиталната безбедност во граѓанското општество е создаден со една јасна цел: да ја направи дигиталната безбедност остварлива, разбирлива и практична за секоја организација, без оглед на големината или техничкиот капацитет. Додека се движите напред, се надеваме дека овој водич ќе ви служи не само како ресурс, туку и како придружник на вашето патување кон посилни, побезбедни дигитални практики.

Дигиталната отпорност расте чекор по чекор, преку свест, соработка и доследност. Со интегрирање на овие практики во вашата секојдневна работа, вие не само што ги заштитувате податоците и комуникацијата, туку и ги браните човековите права, довербата и демократските вредности во дигиталното доба.

Останете свесни. Останете отпорни. Останете безбедни.