


INICIJATIVE CIVILNOG DRUŠTVA OJAČANE INFORMACIJOM I SIGURNOŠĆU PODATAKA

PRAKTIČNI VODIČ ZA DIGITALNU TRANSFORMACIJU I NASTAVNI PLAN I PROGRAM O JAČANJU DIGITALNE SIGURNOSTI U CIVILNOM DRUŠTVU

PRAKTIČNI VODIČ ZA DIGITALNU TRANSFORMACIJU I NASTAVNI PLAN I PROGRAM O JAČANJU DIGITALNE SIGURNOSTI U CIVILNOM DRUŠTVU

Ankara, 2026

Ova studija je sprovedena u okviru projekta pod nazivom “INICIJATIVE CIVILNOG DRUŠTVA OJAČANE INFORMACIJAMA I BEZBEDNOŠĆU PODATAKA” (2023-1-TR01-KA220-YOU-000161230), uz podršku Turske nacionalne agencije i Evropske komisije u okviru Erasmus+ programa. Sadržaj koji je ovdje predstavljen odražava stavove autora, a ni Evropska komisija ni Turska nacionalna agencija ne mogu se smatrati odgovornim za ove stavove.



2026

Akademski savjetnik: Erman Akıllı

Dizajn naslovnice i izgled:

Urednici: Sibel Koru

Zeyneb Güşta Arık

Revizije teksta: Cenay Babaoğlu

Datum: Ankara, 2026

U današnjem svijetu koji je hiperpovezan, organizacije civilnog društva (CSO), u rasponu od nevladinih organizacija i zagovaračkih grupa do nezavisnih medija i mreža zajednice, djeluju na sve složeniji digitalni front. Dok su digitalni alati proširili doseg, efikasnost i uticaj civilnog društva, oni su istovremeno izložili organizacije povećanim rizicima sajber bezbednosti. Kako civilno društvo postaje sve digitalnije zavisno, ono također postaje digitalno ranjivije.

Širom Evrope i šire, OCD se sve više prepoznaju kao visokorizični akteri u digitalnom ekosistemu. Sajber prijetnje usmjerene na civilno društvo sada se kreću od phishinga, ransomware-a, špijunskog softvera i napada uskraćivanja usluge do sofisticiranog nadzora koji sponzorira država s ciljem utišavanja neslaganja i podrivanja demokratskih vrijednosti. Za organizacije koje često rade sa ograničenim tehničkim kapacitetom, ali upravljaju osjetljivim ličnim i organizacijskim podacima, digitalna nesigurnost predstavlja ne samo operativne rizike već i egzistencijalne.

U tom kontekstu, digitalna sigurnost više nije čisto tehnički problem. To je kritično za misiju. Sposobnost organizacija civilnog društva da bezbedno rade na mreži je neodvojiva od njihove sposobnosti da zaštite slobodu izražavanja, transparentnost, odgovornost i zajednice kojima služe. Jačanje digitalne sigurnosti u civilnom društvu, stoga, zahtijeva više od ad hoc tehničkih popravki. Zahtijeva strukturirano učenje, strateško planiranje i praktične smjernice koje se mogu implementirati u stvarnim organizacijskim okruženjima.

Odgovarajući na ovu potrebu, pokrenut je projekat KA220 Erasmus+ "Inicijative civilnog društva ojačane informacijom i sigurnošću podataka" kao zajednički napor više zemalja da se poboljšaju kapaciteti digitalne sigurnosti organizacija civilnog društva. Jedan od centralnih ishoda ovog projekta je sadašnja publikacija, koja namjerno okuplja dvije komplementarne funkcije u jednom tomu.

Ova knjiga je osmišljena i kao nastavni plan i program i kao praktični vodič.
S jedne strane, funkcionira kao strukturirani digitalni sigurnosni nastavni plan i program za civilno društvo, nudeći koherentan put učenja koji progresivno gradi znanje – od razumijevanja pejzaža digitalne prijetnje do razvoja organizacijskih politika i mehanizama odgovora na incidente. Struktura orijentisana na nastavni plan i program čini je pogodnom za upotrebu u obuci, radionicama, programima izgradnje kapaciteta i aktivnostima obuke u različitim nacionalnim kontekstima.

S druge strane, knjiga služi kao praktični vodič, pružajući konkretne smjernice koje organizacije mogu direktno primijeniti u svom svakodnevnom radu. Umjesto da ostane na nivou teorije, on

prevodi principe sajber bezbjednosti u praktične korake, kontrolne liste, primjere i okvire donošenja odluka prilagođene stvarnosti OCD-a i inicijativa na bazi koje rade s ograničenim resursima.

Kombinacijom ove dvije dimenzije, knjiga premošćuje kritični jaz između učenja i implementacije. Omogućava čitaocima ne samo da razumiju *zašto* digitalna sigurnost je važna, ali također *kako* da bi ga operacionalizirali unutar svojih organizacija. Čitaoci mogu pristupiti knjizi uzastopno kao nastavnom planu i programu, ili selektivno kao referentni vodič koji se bavi specifičnim izazovima kao što su osiguranje komunikacija, zaštita podataka, procjena rizika ili izgradnja interne kulture digitalne sigurnosti.

Napisana u pristupačnom, ali akademski utemeljenom stilu, publikacija se oslanja na iskustvo zasnovano na projektima, uvid u polje i uspostavljene najbolje prakse u sajber sigurnosti i izgradnji kapaciteta civilnog društva. Njegova modularna struktura omogućava prilagođavanje različitim organizacionim potrebama, tehničkim nivoima i nacionalnim regulatornim okruženjima.

Na kraju, ovaj kombinovani nastavni plan i program i vodič imaju za cilj da osnaže organizacije civilnog društva da preuzmu vlasništvo nad svojom digitalnom sigurnošću. Podstičući i znanje i praktične sposobnosti, podržava OCD u jačanju njihove otpornosti, zaštiti njihove digitalne infrastrukture i nastavku njihovog suštinskog rada sa većim samopouzdanjem i održivošću u sve spornijem digitalnom prostoru.

SETA, Ankara/Türkiye

TABELA SADRŽAJA:

CILJ PROJEKTA 1.1:

"Inicijative civilnog društva ojačane sigurnošću informacija i podataka" je projekat KA220 Erasmus+ koji koordinira SETA (Türkiye) i implementira se u saradnji sa partnerskim organizacijama iz Sjeverne Makedonije, Norveške, Bosne i Hercegovine, Belgije i Türkiyea. Projekat je finansirala Evropska komisija preko Turske nacionalne agencije i osmišljen je da se pozabavi rastućim izazovima sa kojima se suočavaju organizacije civilnog društva u sve digitalizovanijem okruženju.

Primarni cilj projekta bio je poboljšanje digitalne pismenosti, svijesti o sajber sigurnosti i kapaciteta zaštite podataka u civilnom društvu, uz istovremeno promoviranje uključivanja, raznolikosti i jednakog pristupa digitalnim vještinama. Tokom svoje implementacije, projekat je podržavao i pojedince i institucije u navigaciji procesima digitalne transformacije i jačanju njihove otpornosti na sajber prijetnje, dezinformacije i dezinformacije.

U okviru ovog okvira, projekat je proizveo niz značajnih intelektualnih i praktičnih rezultata. To je uključivalo sveobuhvatnu **Nastavni plan i program digitalne sigurnosti za civilno društvo,** moduli obuke za digitalnu pismenost i sajber sigurnost, osiguravajući da procesi digitalne transformacije budu dostupni i inkluzivni. Osim toga, a **Praktični vodič za digitalnu transformaciju** razvijen je da pomogne organizacijama civilnog društva u planiranju, implementaciji i održavanju efikasnih strategija digitalne transformacije.

Nadalje, projekat je razvio softverski baziran **Online centar za testiranje digitalne sigurnosti za OCD** da procijeni spremnost organizacije civilnog društva za sajber bezbjednost. Platforma omogućava OCD-ovima da procijene svoje nivoe digitalne sigurnosti, uključujući aspekte kao što su prakse zaštite podataka, konfiguracije sigurnosti sistema i sigurno korištenje online alata (npr., strukture domena, korištenje HTTPS-a i osnovne zaštite digitalne infrastrukture). Kroz ovaj alat, organizacije su u mogućnosti da identifikuju ranjivosti, podignu svest o postojećim rizicima i podrže procese izgradnje i poboljšanja digitalne bezbednosti zasnovane na dokazima.

Osim svojih obrazovnih rezultata, projekat je također generirao materijale i kampanje za podizanje svijesti fokusirane na sigurne i odgovorne digitalne prakse. Štaviše, uspeo je da uspostavi snažnu mrežu međunarodne saradnje među partnerskim zemljama, postavljajući

temelje za izgradnju dugoročnih kapaciteta, razmenu znanja i kontinuiranu saradnju u oblasti digitalne bezbednosti civilnog društva.

1.2 PARTNER PROJEKTA:

FONDACIJA ZA POLITIČKA, EKONOMSKA I SOCIJALNA ISTRAŽIVANJA SETA (KOORDINATOR)

Fondacija za politička, ekonomska i društvena istraživanja (SETA) je neprofitni think tank fokusiran na proizvodnju tačnih i ažuriranih analiza o nacionalnim, regionalnim i međunarodnim pitanjima. Cilj mu je informirati kreatore politike i javnost o političkim, ekonomskim, društvenim i kulturnim dešavanjima u istorijskom i kulturnom kontekstu. Kao institucija koja preporučuje istraživanje i politiku, SETA podstiče međunarodni dijalog, spajajući različite perspektive kroz naučne standarde. Doprinosi informisanom donošenju odluka od strane vlade, civilnog društva i poslovnih lidera kroz istraživačke izvještaje, publikacije, konferencije i preporuke politike. SETA usvaja interdisciplinarni pristup, prepoznajući međuzavisnost političkih, ekonomskih i socio-kulturnih pitanja, i nastoji promovirati viziju ukorijenjenu u miru, pravdi, jednakosti i vladavini prava. Njegova misija je obogaćivanje strateških debata i pružanje nezavisnih, autoritativnih uvida donosiocima odluka u javnom i privatnom sektoru.

FONDACIJA ZA POLITIČKA, EKONOMSKA I SOCIJALNA ISTRAŽIVANJA SETA BRISEL

SETA fondacija za politička, ekonomska i društvena istraživanja je neprofitni istraživački institut fokusiran na inovativne studije vezane za nacionalna, regionalna i međunarodna pitanja sa sjedištem u Briselu. Njegov cilj je da proizvede tačna znanja i analize u politici, ekonomiji i društvu, istovremeno informišući kreatore politike i javnost o evoluirajućim političkim, ekonomskim, društvenim i kulturnim uslovima. Podstiče međunarodni dijalog okupljajući različite perspektive kroz istraživačke izvještaje, publikacije, konferencije i preporuke za politiku. Fondacija ima za cilj da podrži informirano donošenje odluka u Turskoj tako što će liderima javnog i privatnog sektora pružiti autoritativne informacije i analize. SETA's interdisciplinarni istraživački pristup bavi se međuzavisnošću političkih, ekonomskih i socio-kulturnih pitanja, nastojeći da ostvari viziju zasnovanu na miru, pravdi, jednakosti i vladavini prava.

ANKA UDRUŽENJE ZA BUDUĆNOST I INOVACIJE

ANKA je inovativna i dinamična nevladina Organizacija (NVO) sa sjedištem u Istanbulu. Osnovan u maju 2019. godine, fokusira se na poboljšanje mentalnog, fizičkog i ekonomskog

blagostanja pojedinaca nudeći alternativne sportske aktivnosti, obuku, inicijative i mogućnosti. ANKA ima za cilj integraciju tehnologije i obrazovanja, pružajući rješenja koja dodaju vrijednost pojedincima i društvu. Organizacija ima stručnost u razvoju mobilnih aplikacija, umjetnoj inteligenciji, web tehnologijama, upravljanju projektima i 3D modeliranju. Njegovi članovi dolaze iz različitih profesionalnih sredina, uključujući preduzetništvo, softver, tehnologiju, zdravlje i obrazovanje. Osim toga, ANKA organizira obrazovne, kulturne i društvene aktivnosti kako bi se uključila omladina i njegovala aktivan, zdrav život. Organizacija nastoji kontinuirano razvijati svoje vještine u softverskom sektoru i doprinijeti procesima cjeloživotnog učenja kroz inovativna tehnološka rješenja.

UDRUŽENJE BOSANSKIH PREDSTAVNIKA ZA VRIJEDNE MOGUĆNOSTI (BRAVO)

Bosansko predstavničko udruženje za vrijedne mogućnosti (BRAVO) je dinamična nevladina organizacija sa sjedištem u Bosni i Hercegovini, fokusirana na osnaživanje pojedinaca i zajednica kroz obrazovanje, razvoj vještina i izgradnju kapaciteta. Njegova misija naglašava društvenu inkluziju, kulturnu razmjenu i održivi razvoj. BRAVO posluje u različitim sektorima, uključujući osnaživanje mladih, ekološku svijest, poduzetništvo i tehnologiju. Ima posvećen tim plaćenog osoblja i volontera koji sarađuju na brojnim projektima. BRAVO je organizovao programe razmene mladih kako bi promovisao međukulturalno razumevanje i lični rast, istovremeno podržavajući održivost životne sredine kroz inovativne projekte. Pomaže budućim poduzetnicima mentorstvo i resurse, fokusirajući se na društveni utjecaj. Osim toga, BRAVO nudi radionice digitalnih vještina, kao što su programiranje i web razvoj, pomažući pojedincima da poboljšaju svoj lični i profesionalni rast tehnologije.

TEHNOLOGIJA ZA TOMORROW'S BETTERMENT (TTB)

Technology for Tomorrow's Betterment (TTB) je nevladina organizacija sa sjedištem u Norveškoj, posvećena pružanju obrazovanja i obuke u tehnologiji i digitalnim vještinama promovirati održivu budućnost. Osnovan u oktobru6, 2019, od strane studenata u Trondhajmu, TTB ima za cilj da poveća učešće mladih u zajednici nudeći mogućnosti za stjecanje znanja i korisnih vještina. Sa timom od 15 plaćenog osoblja i brojnim volonterima, TTB implementira

projekte u obrazovanju, okolišu i poduzetništvu. Organizacija se fokusira na digitalne inovacije, rad mladih i integraciju digitalnih alata. Ključne aktivnosti uključuju edukaciju o digitalnim vještinama, ekološke inicijative i podršku poduzetnicima, posebno u tehnologiji i održivosti. TTB cijeni otvorenost, saradnju, hrabrost i brigu, njegujući održivo, etičko i društveno odgovorno okruženje. Bavi se regionalnom i međunarodnom saradnjom.

TÜRKIYE YOUTH FOUNDATION (TÜGVA)

Osnovana 2014. godine, Türkiye Youth Foundation (TÜGVA) je jedan od najvećih Türkiye's CSO-a, sa timom od preko 100 profesionalaca i 300.000 volontera. Nudi radionice robotskog kodiranja u 39 gradova i upravlja sa 42 spavaonice. Fondacija posluje sa 10 koordinatora u različitim oblastima, uključujući sport, prava žena, preduzetništvo, medije, obrazovanje, kulturu i razvoj karijere. Njegova primarna misija je podrška sveobuhvatnom razvoju mladih, fokusirajući se i na fizičko i na mentalno blagostanje, posebno u Türkiyeu. Fondacija ima za cilj osnažiti mlade ljude da postanu inovativni, produktivni i vrijedni članovi društva. Sa više od 200 završenih nacionalnih i međunarodnih projekata, njegova vizija je da kultiviše generacije sposobne da obnove i unaprede civilizaciju kroz kontinuirano samousavršavanje i kulturno obogaćivanje.

ZDRUZENIE NA GRAGJANI MAKEDONSKA ASOCIJACIJA ZA COVECKI RESURSI SKOPLJE (MHRA)

Makedonsko udruženje ljudskih resursa (MHRA) je neprofitna, nevladina nacionalna organizacija fokusirana na razvoj vještina radne snage, promociju ljudskog kapitala i standardizaciju neformalnog obrazovanja. Članstvo MHRA's uključuje preko 120 aktivnih pojedinačnih članova, prvenstveno žena, i više od 600 pasivnih članova iz oblasti ljudskih resursa, zajedno sa preko 60 kompanija iz javnog i privatnog sektora. Udruženje djeluje kao otvorena platforma koja integriše pojedince u svim fazama karijere, uključujući menadžere ljudskih resursa, konsultante, zaposlene i studente. Uključen je u oblikovanje politika koje se odnose na poslovna, obrazovna i socio-ekonomska pitanja na nacionalnom i lokalnom nivou. Zvaničnik članica Evropske asocijacije za upravljanje ljudima (EAPM) od 2012. godine, MHRA takođe prihvata volontiranje kao osnovnu vrednost u svojim lokalnim i međunarodnim inicijativama.

2. PRAKTIČNI VODIČ ZA DIGITALNU TRANSFORMACIJU

2.1 POGLAVLJE 1: DIGITALNA SIGURNOST ZA CSOS

Šta je digitalna sigurnost?

Digitalna sigurnost, poznata i kao sajber sigurnost, je praksa zaštite digitalnih informacija, uređaja i druge imovine od neovlaštenog pristupa ili štete. Obuhvaća mjere za zaštitu ličnih podataka, računa, datoteka, pa čak i finansijskih sredstava pohranjenih ili prenesenih na mreži. U suštini, digitalna sigurnost ima za cilj osigurati povjerljivost, integritet i dostupnost informacija (često sažeto kao "CIA trijad" – **Povjerljivost, Integritet, Dostupnost).**

Zašto je digitalna sigurnost važna?

U današnjem svijetu koji je hiperpovezan, gotovo svaka organizacija i pojedinac se oslanjaju na digitalne sisteme. Za OCD i nevladine organizacije, ovo oslanjanje uključuje komunikaciju sa zainteresovanim stranama, upravljanje informacijama o donatorima i pružanje usluga. Zaštita ovih digitalnih aktivnosti je kritična. Sajber napadi mogu poremetiti operacije, narušiti osjetljive podatke i oštetiti povjerenje koje donatori i zajednice polažu u organizaciju. Na primjer, kršenje podataka u Australijskom Crvenom križu 2016. godine otkrilo je lične podatke preko 550.000 davalaca krvi zbog ljudske greške (neosigurana rezervna datoteka). Incident ne samo da je pokrenuo pitanja o praksi podataka organizacije, već je doveo i do gubitka povjerenja donatora, ilustrirajući kako sajber incidenti mogu naštetiti stvarnim ljudima i narušiti povjerenje javnosti u misiju CSO's.

Važno je da su neprofitne organizacije sve više na meti sajber kriminalaca, pa čak i hakera koje podržava država. Microsoftov izvještaj je otkrio da su humanitarni i ljudski organizatori drugi najciljaniji sektor sajber napada na nacionalne države, koji čine 31% takvih obavijesti o napadima u 2025. Studija neprofitnih organizacija sa sjedištem u Ženevi iz 2023. otkrila je da je 41% doživjelo sajber napad posljednjih godina. Ipak, više od polovine tih OCD-a nije imalo poseban budžet za sajber sigurnost, a 70% smatra da im nedostaju vještine i otpornost da odgovore na napade. Ove brojke naglašavaju da digitalna sigurnost više nije opciona, već imperativ za OCD. Bez adekvatnih mjera zaštite, sajber incidenti mogu zaustaviti kritične usluge, ugroziti podatke korisnika i ugroziti finansiranje narušavanjem reputacije organizacije.

Štaviše, digitalna sigurnost je usko povezana sa fizičkom sigurnošću i ljudskim pravima u radu civilnog društva. Aktivisti, novinari i OCD često se suočavaju s digitalnim prijetnjama

usmjerenim na nadzor ili zastrašivanje. Kršenje ili hakiranje može razotkriti osjetljive komunikacije ili identitete partneri i korisnici, potencijalno dovodeći živote ili sredstva za život u opasnost. Stoga je ulaganje u digitalnu sigurnost ulaganje u ukupnu otpornost i pouzdanost jednog rad organizacije.

Šta znači digitalna sigurnost za OCD?

Za organizacije civilnog društva, *digitalna sigurnost* znači zaštita informacija I tehnologije koja omogućava njihove društvene misije. OCD-ovi rutinski prikupljaju i pohranjuju osjetljive podatke – od ličnih podataka pristalica i osoblja do strateških planova i istraživanja. Osiguravanje povjerljivosti i integriteta ovih podataka je najvažnije tako da oni ne ispovijedaju da padnu u pogrešne ruke ili da im se manipuliše. Na primjer, zagovaračka grupa će možda morati osigurati kontakt liste aktivista ili dokaze o kršenju ljudskih prava. Ako su takve informacije procurile ili izmijenile zlonamjerni akteri, to bi moglo ugroziti pojedince ili potkopati uzrok.

Digitalna sigurnost za OCD također uključuje zaštitu svakodnevnih operacija. Mnoge organizacije se oslanjaju na e-poštu, aplikacije za razmjenu poruka i platforme u oblaku za koordinaciju aktivnosti. Ako su ti računi ugroženi, napadači bi mogli poremetiti komunikaciju ili se lažno predstavljati za CSO. U jednom stvarnom slučaju, sistem e-pošte dobrotvornih organizacija hakovan je putem phishing e-pošte s prilogom za zlonamjerni softver, što je dovelo do napada ransomware-a koji je šifrirao server organizacije. Napadači su tražili otkupninu u zamjenu za ključ za dešifriranje. Budući da je CSO nedavno imao sigurnosne kopije podataka i odlučio je da ne plati, uspjeli su vratiti većinu svojih podataka, ali je oko dvije sedmice informacija trajno izgubljeno. Ovaj incident ilustruje i prijetnju i važnost spremnosti: bez jakih rezervnih kopija i plana odgovora, ishod je mogao biti daleko gori.

Za grupe civilnog društva koje djeluju u osjetljivim političkim okruženjima, digitalna sigurnost preuzima dodatno značenje zaštite sigurnosti svojih članova i zajednica kojima služe. Represivni entiteti mogu koristiti sajber sredstva da špijuniraju OCD ili ih ciljaju dezinformacijama. Stoga digitalna sigurnost za OCD često naglašava alate za poboljšanje privatnosti (kao što je šifriranje za e-poštu i poruke) i sigurne komunikacijske kanale kako bi se spriječio nadzor. Kao što Liberties, evropska organizacija za građanske slobode, napominje: OCD

koji koriste digitalne alate za aktivizam suočavaju se s jedinstvenim prijetnjama i moraju potaknuti kulturu "digitalne samoodbrane" koja pokriva ljude, procese i tehnologiju. U praktičnom smislu, to znači obuku osoblja i volontera sigurnosna svijest, uspostavljanje jasnih politika (na primjer, o rukovanju ličnim podacima ili korištenju sigurnih aplikacija) i kontinuirano ažuriranje tehničke zaštite.

Konačno, *digitalna sigurnost za OCD* radi se o održavanju povjerenja. Donatori i korisnici očekuju da organizacije budu dobri upravitelji informacija. Dobro objavljen sajber incident može poljuljati povjerenje javnosti i odvratiti ljude od angažmana ili doprinosa. Na primjer, nakon što je ranije spomenuto curenje podataka Crvenog križa, organizacija je primijetila pad davanja krvi i morala je raditi na obnovi povjerenja. Davanjem prioriteta digitalnoj sigurnosti, OCD pokazuju svoju posvećenost odgovornosti i privatnosti, što su osnovne vrijednosti u sektoru civilnog društva.

Uobičajene digitalne prijetnje i rizici do OCD-a

OCD se suočavaju sa mnogim istim sajber rizicima kao i preduzeća i pojedinci, ali često sa manje resursa za njihovo rješavanje. Neke uobičajene prijetnje uključuju:

- **Hakeri i zlonamjerni softver:** Napadači mogu pokušati da se infiltriraju u mrežu ili uređaje CSO's kako bi ukrali podatke ili ometali usluge. To se može dogoditi putem zlonamjernog softvera (zlonamjernog softvera kao što su virusi, špijunski softver ili ransomware) koji se isporučuje putem priloga e-pošte, štetnih linkova ili zaraženih USB diskova. Ransomware je posebno štetan zlonamjerni softver koji šifrira datoteke i zahtijeva plaćanje. Pogodio je organizacije svih veličina, od malih neprofitnih organizacija do čitavih gradskih vlasti. Ako CSO nema jaku odbranu protiv zlonamjernog softvera i sigurnosne kopije podataka, napad ransomware-a mogao bi efikasno paralizirati njegove operacije.
- **Phishing and Social Engineering:** Phishing je taktika u kojoj napadači šalju lažne e-poruke ili poruke koje izgledaju legitimno (na primjer, predstavljaju se kao kolega ili pružalac usluga) kako bi prevarili primaoce da otkriju lozinke ili preuzmu zlonamjerni softver. Phishing je jedna od najčešćih prijetnji i često ulazna tačka za veće napade. OCD-ovi su bili meta phishing prevara; na primjer, obrazovna neprofitna organizacija je zamalo izgubila sredstva kada su napadači lažirali mejlove kako bi prevarili partnera da pošalje uplatu na pogrešan bankovni

račun (oblik “kompromisa poslovne e-pošte”). Uobičajeni znakovi phishinga uključuju hitan ili alarmantan jezik, zahtjeve za osjetljivim informacijama ili blago pogrešno napisane adrese e-pošte. Socijalno inženjerstvo se također može pojaviti putem telefonskih poziva (vishing) ili tekstualnih poruka (smishing) koje se lažno predstavljaju kao pouzdani subjekti.

- **Kršenje podataka:** Kršenje podataka nastaje kada se povjerljivim informacijama pristupi ili otkrije bez odobrenja. To može biti rezultat hakovanja, zloupotrebe insajdera ili čak slučajnog izlaganja. OCD često sadrže lične podatke (npr. detalje o korisnicima, finansijsku evidenciju donatora, informacije o zdravstvenim ili pravnim predmetima) koji su privlačni napadačima ili bi mogli procuriti. Kao što je spomenuto, pogrešno konfigurirani serveri ili pohrana u oblaku mogu nenamjerno procuriti podatke – incident Crvenog križa je jedan primjer. Uticaj kršenja za OCD je ozbiljan: može dovesti do krađe identiteta za pojedince u podacima, kršenja zakona o privatnosti i štete reputaciji i pravnom položaju organizacije. Nažalost, mnoga kršenja sežu do ljudske greške. U stvari, industrijski izvještaj je otkrio da 74% kršenja uključuje “ljudski element,” kao što su greške ili žrtva krađe identiteta. Ovo naglašava potrebu za obukom i pažljivim rukovanjem podacima.
- **Neovlašteni pristup računu:** Napadači mogu ciljati na račune koje koristi osoblje CSO-a, kao što su e-pošta, društveni mediji ili platforme za prikupljanje sredstava. Krađom ili nagađenjem lozinki (ili korištenjem procurelih akreditiva od prethodnih kršenja), oni mogu oteti ove račune. Znakovi kompromisa uključuju upozorenja o prijavljivanju sa nepoznatih lokacija, nove e-poruke ili objave koje je poslao korisnik’t nije kreirao, ili nemogućnost prijavljivanja (password mijenja napadač). Na primjer, ako je službeni nalog na društvenim mrežama CSO’s hakovan, mogao bi se koristiti za širenje lažnih informacija ili prevaru sljedbenika CSO’sa. Korištenje jakih, jedinstvenih lozinki i dvofaktorske autentifikacije (o kojima se govori u poglavlju 2) ključna je odbrana od preuzimanja računa.
- **Zabrana web stranice ili DDoS:** OCD-ovi sa web stranicama koje se suočavaju s javnošću mogli bi doživjeti oštećenje (napadači koji mijenjaju sadržaj sajt’s za širenje poruka ili propagande) ili napade distribuiranog poricanja usluge (DDoS) koji preplavljuju stranicu saobraćajem kako bi je izbacili van mreže. Ove napade ponekad izvode haktivisti ili protivnici koji pokušavaju da ućutkaju glas CSO’s. Jedan CSO je otkrio da je njihova web stranica

preusmjerena na stranicu treće strane nakon što su napadači iskoristili ranjivosti, a budući da im je nedostajala nedavna podrška, trebalo je devet mjeseci da se obnovi njihova stranica. Osiguravanje da je softver web stranica ažuriran i podržano može ublažiti takve rizike.

- **Prijetnje insajderima i ljudska greška:** Ne dolaze svi rizici od anonimnih hakera. Ponekad insajderi (zaposleni ili volonteri) mogu slučajno ili namjerno uzrokovati sigurnosne incidente. Ovo bi se moglo kretati od gubitka neosiguranog laptopa koji sadrži osjetljive datoteke na pogrešno konfiguriranje baze podataka nezadovoljnom članu osoblja koji preuzima podatke prije polaska. OCD treba da vode računa o internim kontrolama pristupa i principu najmanje privilegija (davanje pristupa osoblju samo informacijama i sistemima neophodnim za njihovu ulogu). Štaviše, njegovanje organizaciona kultura sigurnosti može smanjiti greške – kada ljudi shvate zašto, na primjer, treba da se izjasni da koriste lične USB diskove ili da moraju slijediti procedure rukovanja podacima, manje je vjerovatno da će nenamjerno stvoriti ranjivosti.

Ukratko, OCD se suočavaju sa širokim spektrom digitalnih prijetnji – od svakodnevnih prevara poput krađe identiteta do ciljanijih napada sofisticiranih glumaca. Poglavlje 2 će istražiti kako početi čuvati ove rizike s osnovnim najboljim praksama. Ali čak iu ovoj uvodnoj fazi, jedna ključna tačka treba da bude jasna: prepoznavanje zajedničkih rizika je prvi korak ka njihovom upravljanju. Znajući šta može poći po zlu (bilo da se radi o ukradenoj lozinki, infekciji virusom ili dokumentu koji je procurio), organizacije i pojedinci postaju spremniji da preduzmu mjere kako bi spriječili i odgovorili na te scenarije.

Šta će ova knjiga da obezbedi?

Ovaj vodič je osmišljen da opremi organizacije civilnog društva praktičnim znanjem i vještinama za poboljšanje njihove digitalne sigurnosti. Potrebno je jednostavno, *praktičan pristup* <TAG1> sličan kursu otvorenog univerzitetskog stila – sa stvarnim primjerima, kontrolnim listama i jednostavnim vježbama za jačanje učenja. Prolazeći kroz poglavlja, čitaoci će:

- **Razumijete osnove:** You'll će naučiti terminologiju i osnovne koncepte digitalne sigurnosti (ne brini, uključujemo Pojmovnik pojmova u Dodatku za brzu referencu). Od osnovnih definicija poput onoga što je zlonamjerni softver konceptima kao što je dvofaktorska

autentifikacija, mi'll demistifikuje žargon kako biste mogli pouzdano komunicirati o sigurnosnim pitanjima.

- **Identificiraj svoje Rizike:** Knjiga će vas voditi kroz procjenu sa kojim konkretnim prijetnjama bi se vaš CSO mogao suočiti i kojoj imovini je potrebna zaštita. Kroz kratka pitanja i scenarije samoprocjene, počet ćete mapirati profil rizika svoje organizacije's (poglavlje 3).
- **Implementacija najboljih praksi:** Pružamo jasne savjete korak po korak o trenutnim akcijama – poput stvaranja jakih lozinki, osiguranja vaših uređaja i sigurnog korištenja interneta i e-poštu (poglavlje 2). Ovo su "brze pobjede" sajber sigurnosti koje drastično smanjuju vašu ranjivost kada se radi dosljedno.
- **Razviti sigurnosni plan:** Osim pojedinačnih savjeta, mi'll vam pokazuje kako sve to spojiti u jednostavan, ali efikasan digitalni sigurnosni plan za svoj CSO (poglavlje 3). Ovo uključuje prijedloge politike, planove obuke za vaš tim i metode za pravljenje rezervnih kopija i šifriranje podataka. Dostavljeni su predlošci i primjeri koji će vam pomoći da izradite ili poboljšate vlastiti plan.
- **Naučite koristiti sigurnosne alate:** Poglavlje 4 uvodi sigurnosne alate i softver prilagođene korisniku (od menadžera lozinki i antivirusnih programa do sigurnih aplikacija za razmjenu poruka). Naglašavamo alate koji se lako koriste i koji su obično dostupni, čak i uz mali budžet. Svaki alat ili metoda o kojoj se raspravlja dolazi s objašnjenjem zašto je koristan i kako započeti s njim.
- **Pripremite se za incidente:** Uprkos najboljim naporima, incidenti se mogu dogoditi. U 5. poglavlju prolazimo kroz to kako prepoznati znakove sajber incidenta (kao što su znakovi da bi vaš kompjuter mogao biti hakovan) i neposredne korake koje treba poduzeti kao odgovor. Zamislite to kao vježbu za hitne slučajeve – koji zna šta učiniti može značajno ograničiti štetu. Navodimo I resurse I kontakte za dobivanje pomoći, jer pravovremena podrška može biti presudna u krizi.
- **Naglasite saradnju:** Ključna tema u ovom vodiču je da niste sami u borbi protiv digitalne sigurnosti. Poglavlje 6 govori o moći vršnjačke podrške – kako OCD mogu pomoći jedni drugima dijeleći upozorenja, savjete, pa čak i udruživanjem resursa za obuku. Također

ukazuje na mreže i institucije (lokalne ili međunarodne) koje nude podršku, od tehnoloških volontera do linija za pomoć.

- **Pružajte kontekst stvarnog života:** U poglavlju 7 predstavljamo studije slučaja i zajedničke zamke. You'll je pročitao kratke priče o OCD-ima koji su se suočili sa sajber izazovima i načinom na koji su ih savladali, kao i česte greške koje organizacije čine (kako biste ih mogli izbjeći). Također uključujemo nekoliko jednostavnih vježbi za "test" vaše osiguranje –, na primjer, kontrolnu listu za reviziju vlastite kancelarije ili phishing kviz e-pošte za vaš tim.

Do kraja ove e-knjige trebali biste se osjećati sigurnije i osnaženo u suočavanju s digitalnom sigurnošću. Sadržaj je strukturiran tako da bude dostupan čak i ako nemate IT' pozadina. Svako poglavlje se gradi na prethodnim, a možete se odnositi i na određene dijelove po potrebi. Cilj nije da vas preko noći pretvorite u stručnjaka za kibernetičku sigurnost, već da vam pruži znanje i navike koje će značajno poboljšati vašu zaštitu od uobičajenih prijetnji. Zamislite to kao priručnik za vozača za digitalni put –, ne't, morate biti mehaničar za sigurno vožnju, ali morate naučiti pravila, koristiti prave alate (kao što su pojasevi) i ostati budni za opasnosti.

Osim toga, u svim poglavljima ćete pronaći "Da li ste znali?" sporedne napomene i kratka praksa zahtijevaju primjenu onoga što ste naučili. Uzmite trenutak da se uključite u ovo; oni su tu da učvrste vaše razumijevanje i učine iskustvo učenja interaktivnijim. Na primjer, nakon odjeljka lozinki, upit bi vas mogao zamoliti da procijenite snagu lozinke uzorka ili nakon odjeljka za sigurnosnu kopiju, kako biste razmotrili koji su podaci u vašoj organizaciji najkritičniji za podršku.

Na kraju krajeva, ono što vam ova publikacija nudi je temelj digitalne sigurnosti prilagođen kontekstu civilnog društva. Ulaganjem vremena u ova poglavlja, poduzimate važan korak ka zaštiti rada vaše organizacije i ljudi povezanih s tim. Dakle, hajde da's započne putovanje do sigurnije digitalne budućnosti za vaš CSO!

Sažetak poglavlja

Ovo poglavlje uvodi kritičnu važnost digitalne sigurnosti za OCD, naglašavajući njihovu ranjivost kao glavne mete za sajber napade zbog njihovih uloga zagovaranja. Navodi uobičajene prijetnje kao što su zlonamjerni softver, phishing, kršenje podataka, neovlašteni pristup računu,

oštećenje web stranice i DDoS napadi, naglašavajući njihov utjecaj na operacije, povjerenje i sigurnost. Primjeri iz stvarnog svijeta, kao što je kršenje podataka Australijskog Crvenog križa iz 2016., razotkrivanje 550.000 donatora' informacija i napad ransomware-a na dobrotvornu organizaciju, ilustruju posljedice neadekvatne odbrane. U poglavlju se navodi da je 31% napada nacionalne države u 2025. ciljalo na OCD, pri čemu se 41% neprofitnih organizacija sa sjedištem u Ženevi suočava s napadima, ali više od polovine nema budžete za sajber sigurnost. Naglašava da je digitalna sigurnost kritična za misiju, štiti osjetljive podatke (npr., detalje korisnika) i osigurava operativni kontinuitet. Za OCD u osjetljivim političkim okruženjima, sajber sigurnost je povezana s fizičkom sigurnošću, sprječavanjem nadzora ili dezinformacija. Poglavlje se zalaže za kulturu "digitalne samoodbrane," kombinirajući ljude, procese i tehnologiju. Postavlja pozornicu za e-knjigu uokvirivanjem sajber sigurnosti kao potrebe za preživljavanjem, a ne samo kao IT problem, i priprema čitaoce za praktična rješenja u narednim poglavljima. Ključni zaključci za poneti uključuju potrebu za svijesti, spremnošću i izgradnjom povjerenja za zaštitu CSOs' misije.

Quick Start kontrolna lista za kibernetičku sigurnost za OCD

Ova kontrolna lista pruža jednostavne, trenutne korake za poboljšanje digitalne sigurnosti vaše organizacije's. Završite ove akcije u narednoj sedmici kako biste smanjili ranjivost i izgradili osnovu za sigurno digitalno okruženje. Svaki korak je dizajniran da bude jeftin, prilagođen korisniku i efikasan za OCD sa ograničenim resursima.

1. Osigurajte svoje račune

- Omogućite autentifikaciju dva faktora (2FA): Uključite 2FA za sve kritične račune (npr., e-poštu, društvene mreže, pohranu u oblaku) danas. Koristite aplikaciju za autentifikaciju (kao što je Google Authenticator ili Authy) ili SMS kodove da dodate dodatni sloj zaštite.
    - ⇒ Provjerite postavke računa (npr. Pošta: Postavke > Sigurnost > 2-Step verifikacija).
- Kreirajte jake, jedinstvene lozinke: ažurirajte lozinke za ključne račune na najmanje 14 znakova, miješajući slova, brojeve i simbole (npr. "sunbird&glass7rain"). Koristite drugačiju lozinku za svaki račun.

⇒ Razmotrite besplatnog upravitelja lozinki kao što je Bitwarden da bezbedno generiše i pohranjuje lozinke.

- Provjerite za prekršene račune: Posjetite “Have I Been Prowned” (haveibeenpwned.com) da vidite da li su vaša e-pošta ili računi izloženi u kršenju podataka. Odmah promijenite pogođene lozinke.

⇒ Procurele akreditive mogu se koristiti za napad na vaše račune.

2. Zaštitite svoje uređaje

- Ažuriranje Softver danas: Osigurajte da se svi uređaji (računari, telefoni, tableti) I softver (npr., operativni sistemi, pretraživači, aplikacije) ažuriraju najnovijim sigurnosnim zakrpama.

⇒ Provjerite Windows Update, macOS Software Update ili postavke trgovine aplikacija za ažuriranja koja su na čekanju.

- Instalirajte Antivirusni softver: Instalirajte besplatni antivirusni program (npr., Windows Defender, Avast Free Antivirus) na svim uređajima I osigurajte da je’s aktivan I ažuriran.

⇒ Preuzmite iz pouzdanih izvora i zakažite sedmične snimke.

- Omogući zaključavanje uređaja: Postavite uređaje za automatsko zaključavanje nakon pet minuta neaktivnosti uz jaku lozinku ili PIN. Osigurajte da je enkripcija omogućena (većina modernih uređaja to ima prema zadanim postavkama).

⇒ Brave i enkripcija sprečavaju krađu podataka ako su uređaji izgubljeni ili ukradeni.

3. Sigurne komunikacije

- Koristite sigurnosne aplikacije za razmjenu poruka: Prebacite se na end-to-end šifrirane aplikacije kao što su Signal ili WhatsApp za osjetljive komunikacije. Provjeri kontakte prije dijeljenja osjetljivih informacija.

⇒ Preuzmite i omogućite poruke koje nestaju za osjetljive razgovore.

- Spot Phishing Emails: Obučite osoblje da izbjegava klik na linkove ili dijeljenje informacija u e-mailovima s hitnim jezikom, pogrešno napisanim ili nepoznatim pošiljaocima. Pažljivo provjerite adrese e-pošte.

⇒ Pređite preko linkova za provjeru URL-ova prije klikanja i prijavite sumnjive e-poruke IT-u.

4. Safeguard Data

- Back Up Critical Data: Uzmite osnovne datoteke (npr. liste donatora, projektni dokumenti) na siguran eksterni disk ili cloud servis (npr., Google Drive sa 2FA) ove sedmice.
    ⇒ Zakažite automatske sigurnosne kopije ili ručno kopirajte datoteke na sigurnu lokaciju.
- Ograničite pristup podacima: Pregledajte ko ima pristup osjetljivim podacima (npr., zajedničkim diskovima, bazama podataka). Uklonite pristup bivšem osoblju ili volonterima.
    ⇒ Ograničavanje pristupa smanjuje rizik od insajderskih prijetnji ili curenja informacija.

5. Osigurajte svoje prisustvo na mreži

- Provjerite sigurnost web stranice: Provjerite da li vaša web stranica koristi HTTPS (tražite katanac u pretraživaču). Kontaktirajte svoj web host kako biste osigurali redovne sigurnosne kopije i ažurirani softver (npr., CMS, dodaci).
    ⇒ Provjerite kod svog provajdera hostinga ili koristite besplatne alate kao što je Lets Encrypt za HTT'S.
- Sigurni računi društvenih medija: Omogućite 2FA i jake lozinke na svim nalozima OCD društvenih medija. Uklonite pristup neaktivnim adminima.
    ⇒ Štiti od otmice računa i dezinformacija.

2.2 POGLAVLJE 2: PRVI KORACI U DIGITALNOJ SIGURNOSTI

Prvi koraci u digitalnoj sigurnosti

Ovo poglavlje pokriva osnovne prakse koje svaki pojedinac u organizaciji treba slijediti radi osnovne digitalne sigurnosti. Ovi "prvi koraci" često su jednostavne navike i mjere koje pružaju značajne sigurnosne prednosti. Kako se kaže, sajber sigurnost počinje kibernetičkom higijenom – svakodnevnim rutinama i mjerama opreza koje vas čuvaju na internetu. Istražit ćemo kako stvoriti jake lozinke, pažljivo koristiti internet, osigurati komunikaciju i zaštititi svoje kompjutere i pametne telefone. Čak i ako u početku implementirate samo ove osnove, već ćete ublažiti veliki dio uobičajenih prijetnji.

Stvaranje i zaštita jakih lozinki

Jedan od najneposrednijih načina da povećate svoju digitalnu sigurnost je jačanje vaših lozinki. Lozinke su ključevi vaših računa i uređaja – ako su slabi ili kompromitovani, napadači mogu otključati sve, od vaše e-pošte do vaših bankarskih informacija. Nažalost, ljudi često ponovo koriste lozinke koje je lako zapamtiti ili biraju one koje je napadačima lako pogoditi (kao "123456" ili "lozinka"). U stvari, slabe ili ukradene lozinke ostaju vodeći uzrok kršenja sigurnosti.

Šta je jaka lozinka?

Prema smjernicama za kibernetičku sigurnost, jaka lozinka je duga, jedinstvena i složena. Sigurnosne smjernice Microsoft'sa sugeriraju najmanje 14 znakova, uključujući mješavinu slova, brojeva i simbola gornjeg i donjeg slova. Trebalo bi **ne** sadrži jednostavne lične podatke (poput imena ili datuma rođenja) ili uobičajene riječi. Dobra praksa je korištenje a *passfrase* <TAG1> niz nasumičnih riječi ili rečenice koju je lako zapamtiti, ali drugima teško pogoditi. Na primjer, "sunbird&glass7rain" je daleko jači od kratke lozinke poput "blue123", ali bi ga moglo lakše prisjetiti jer predstavlja frazu.

Jedinstvenost je kritična: svaki račun ili usluga treba da imaju svoju lozinku. Ako ponovo koristite lozinke i jedan račun se prekrši, napadači će isprobati istu lozinku na vašim drugim računima (poziva se taktika *punjenje akreditacija*). Korištenje jedinstvenih lozinki sadrži oštećenje jednog proboja. Kao što savjetuje ENISA (Agencija za kibernetičku sigurnost EU's), *izbjegavajte korištenje iste lozinke na više računa*. Također, razmislite o provjeri jesu li se pojavili vaši računi poznata kršenja podataka (web stranice poput "Have I Been Prowned"

omogućavaju vam da pretražujete svoju e-poštu u odnosu na baze podataka o kršenju). Ako je tako, odmah promijenite te lozinke.

Menadžeri lozinki: Nerealistično je zapamtiti desetine dugih, složenih lozinki. To potvrđuje gdje dolaze alati za upravljanje lozinkom. Upravitelj lozinki je aplikacija (ili sigurna usluga u oblaku) koja može generirati jake slučajne lozinke za vas i pohraniti ih u šifrirani svod, tako da morate zapamtiti samo jednu glavnu lozinku. Mnogi sigurnosni stručnjaci i agencije preporučuju korištenje upravitelja lozinki za bolju sigurnost. Na primjer, Bitwarden (kompanija za upravljanje lozinkama) pohvalila je ENISA's savjete, koji eksplicitno uključuje korištenje upravitelja lozinki za održavanje lozinki jedinstvenim i sigurnim. Popularni menadžeri lozinki uključuju Bitwarden, LastPass, 1Password i KeePass (između ostalih). Pronađite onu koja odgovara vašoj organizaciji (neke imaju besplatne verzije) i počnite je koristiti za nadogradnju svih tih slabih ili ponovljenih lozinki.

Zaštita vaših lozinki: Čak I jaka lozinka mora biti zaštićena. Nikada ne dijelite svoje lozinke preko e-pošte ili poruka i budite oprezni da bilo ko netraženo traži vašu lozinku – osoblje za legitimnu podršku (čak ni u IT kompanijama) neće trebati vašu stvarnu lozinku. Također, omogućite autentifikaciju dva faktora (2FA) na svojim računima kad god je to moguće. 2FA (također nazvan multi-faktorska autentifikacija, MFA) znači da pružate drugi dokaz identiteta prilikom prijavljivanja u –, na primjer, jednokratni kod koji se šalje na vaš telefon ili generira aplikacija za autentifikaciju ili skeniranje otiska prsta. Na ovaj način, čak i ako neko nauči vašu lozinku, vjerovatno ne može pristupiti računu bez tog drugog faktora. ENISA's vrhunski savjet uključuje korištenje "dodatnog step"-a kao što je telefonski kod ili biometrijski za prijave. Mnoge usluge (Google, Facebook, Microsoft, itd.) dozvoljavaju 2FA putem aplikacije ili SMS-a. Čini se mudrim da ovo uključite za račune e-pošte, društvene mreže, bankarstvo, pohranu u oblaku – u suštini za svaki račun koji bi bio osjetljiv ako bi bio hakovan.

Druga važna navika je promjena zadanih lozinki na uređajima ili aplikacijama. Mnogi hardverski uređaji (kao što su Wi-Fi ruteri) ili softverski alati dolaze s unaprijed postavljenim administrativnim lozinkama (često nešto generičko kao što je "admin/admin"). Ova zadana

postavka su nadaleko poznata napadačima, tako da uvijek postavite novu, snažnu lozinku tokom postavljanja. Na primjer, ako vaš CSO uspostavi novu kancelariju ruter ili online baza podataka, jedan od prvih zadataka bi trebao biti prilagođavanje pristupnih akreditiva.

Konačno, razmotrite raspored periodičnog ažuriranja lozinki. Mišljenja se razlikuju o tome koliko često treba mijenjati lozinke – neki stručnjaci kažu da česte prisilne promjene mogu imati suprotne rezultate (korisnici mogu birati jednostavnije lozinke ili samo povećati broj). Moderne smjernice sugeriraju da ako su lozinke jake i jedinstvene, morate ih promijeniti samo kada se kao osvježenje ukaže na indikaciju kompromisa ili periodično (recimo jednom godišnje). Staro pravilo promjene svaka tri mjeseca više nije težak zahtjev ako postoje druge kontrole (kao 2FA). Međutim, ako sumnjate da bi bilo koji račun mogao biti kompromitovan, odmah promijenite tu lozinku i bilo gdje drugdje ste koristili sličan.

Ukratko, jake lozinke + 2FA = moćna odbrana. Koristeći robusne, različite lozinke i dodajući drugi korak prijave, zatvorili ste vrata mnogim pokušajima upada. Zamislite to kao da zaključate svoju kuću visokokvalitetnom bravom (pasoškom) i zastojem (2FA) –, uljez bi morao poraziti oboje da bi provalio. Kao tim, ohrabrite sve u svom OCD da usvoje ove prakse. Poglavlje 3 će se dotaknuti kako provesti dobre politike lozinki u cijeloj organizaciji, ali promjena može početi tako što ćete voditi primjerom u korištenju upravitelja lozinki i 2FA za vaše račune.

Sigurno korištenje interneta: Šta treba paziti

Internet je glavna arterija informacija i komunikacije za većinu organizacija, ali može biti i izvor prijetnji ako se koristi nemarno. “Sigurni internet upotreba” odnosi se na prakticiranje opreza i pametnog ponašanja dok pregledavate web stranice, koristeći online usluge i preuzimate sadržaj. Evo ključnih principa i savjeta koje osoblje OCD-a treba slijediti:

***Provjerite legitimitet web stranice*:** Prije nego što unesete bilo kakve osjetljive informacije na web stranicu (kao što su vjerodajnice za prijavu ili lični podaci), pobrinite se da stranica bude autentična i sigurna. Provjerite da li je URL ispravan (pazite na tipografije ili čudne domene koji oponašaju stvarne) i da je veza šifrirana – naznačena https:// i ikonom katanaca u adresnoj traci pretraživača. Na primjer, https://secure.CSOportal.org je pouzdaniji od http://CSO-portal.example.com (nedostatak HTTPS-a je crvena zastava). Napadači često kreiraju lažne web stranice koje izgledaju legitimno (na primjer, stranicu koja imitira stranicu za prijavu

e-pošte) kako bi lažirali lozinke. Uvijek dvaput provjerite adresnu traku kada se prijavite. Moderni pretraživači također često ističu naziv kompanije u detaljima certifikata za glavne stranice – koristi te znakove. Kada ste u nedoumici o primljenom linku (recimo, putem e-pošte ili društvenih medija), nemojte ga direktno kliknuti. Umjesto toga, idite na službenu web stranicu putem Googlea ili zabilješki, ili lebdite preko linka da pregledate URL (bez klizanja). Ako veza izgleda sumnjivo ili se ne podudara s navodnim pošiljaocem (npr., e-mail tvrdi da je iz vaše banke, ali URL je neka nepovezana domena), vjerovatno je zlonamjeran.

Razmislite prije nego što kliknete ili preuzmete: Zlonamjerne veze i preuzimanja su primarno sredstvo za zlonamjerni softver. Budite oprezni kada pregledate nepoznate stranice ili kada je to potrebno za preuzimanje datoteka. Pop-up prozori koji vas pozivaju da preuzmete "codec" ili "ažuriranje" za gledanje sadržaja često su zamke. Ako vam je potreban određeni softver ili dokument, preuzmite ga iz uglednog izvora (na primjer, softver sa službene stranice dobavljača ili dobro poznate trgovine aplikacijama). Izbjegavajte preuzimanje piratskog softvera ili medija – osim pravnih problema, takve datoteke često skrivaju zlonamjerni softver. Također, onemogući automatska preuzimanja u postavkama pretraživača; kontrola znači da možete otkazati bilo šta nenamjerno. Ako vaš pretraživač ili sigurnosni alat upozorava da stranica može biti nesigurna, obratite pažnju na upozorenje i napustite stranicu. Slično, budite skeptični prema ekstenzijama pretraživača ili dodacima nepoznatih izdavača. Instalirajte samo dodatke koji su vam zaista potrebni i iz službenih web trgovina, budući da zlonamjerna ekstenzija može pratiti vašu aktivnost ili ubrizgati oglase/viruse.

Koristi sigurne veze (Wi-Fi i VPN): Prilikom povezivanja na internet, posebno izvan ureda, budite svjesni sigurnosti mreže. Javne Wi-Fi mreže (kao i one u kafićima, aerodromima, itd.) mogu biti rizične jer bi napadači na istoj mreži mogli presresti vaš saobraćaj. Ako morate koristiti javni Wi-Fi, izbjegavajte pristup osjetljivim računima osim ako je veza šifrirana (tražite HTTPS). Čak i tada, pametan napadač bi mogao postaviti odmetničko Wi-Fi hot spot sa primamljivim imenom ("Free Airport WiFi") kako bi namamio korisnike. Dobra praksa je korištenje VPN-a (virtuelna privatna mreža) kada ste na mrežama bez povjerenja. VPN kreira šifrirani tunel za sav vaš internet promet, što uvelike smanjuje mogućnost prisluškivanja. Mnoge organizacije pružaju VPN pristup za rad na daljinu; ako to čini vaš, osigurajte da znate kako ga

koristiti. Ako ne, razmislite o korištenju renomirane komercijalne VPN usluge prilikom putovanja ili rada s javnih prostora. Osim toga, pobrinite se da vaš kućni ili uredski Wi-Fi bude osiguran snažnom lozinkom i koristi WPA2 ili WPA3 enkripciju. Promijenite zadanu administrativnu lozinku na svom ruteru kao što je spomenuto i onemogućite daljinsko upravljanje osim ako nije apsolutno potrebno.

Budite oprezni s vezama e-pošte i linkovima: Iako će se o mejlovima više raspravljati u sljedećem odjeljku, vrijedi napomenuti kao dio sigurnih internet navika koje klikom na linkove u e-mailovima ili na web stranicama zahtijeva oprez. Uobičajena prevara na mreži su lažna upozorenja poput "Vaš kompjuter je zaražen! Kliknite ovdje da skenirate" –, oni često dovode do zlonamjernog softvera. Slično, izbjegavajte škljocanje na baner oglase ili iskačuće kopije tvrdeći da ste nešto osvojili ili da vam je potrebno hitno ažuriranje. Ovo su pokušaji društvenog inženjeringa da se uhvati u koštac sa radoznalošću ili strahom. Imajte na umu izreku: ako nešto na mreži zvuči previše dobro (ili previše zastrašujuće) da bi bilo istinito, to je vjerovatno prevara. Na primjer, online oglas koji kaže: "Dobijte grant od 5.000 dolara sada – ograničeno vrijeme!" treba da izazove sumnju. Obučite se da prepoznate ovu taktiku i ne reagujete impulsivno.

Zaštitite lične i organizacione informacije: Pazite na informacije koje javno dijelite na web stranicama i društvenim mrežama, jer se mogu koristiti protiv vas u sajber napadima. Napadači često prikupljaju detalje sa profila na društvenim mrežama ili web stranica kako bi izradili uvjerljivije phishing e-poruke (praksa koja se zove phishing koplja kada je visoko ciljana). Na primjer, ako vaša stranica CSO's navodi e-poštu i interese osoblja, neko bi vam mogao poslati e-poštu pozivajući se na te informacije kako bi zaslužio vaše povjerenje. Stoga ograničite ono što otkrijete o unutrašnjim stvarima na javnim forumima. Prilikom popunjavanja web obrazaca, razmislite da li su svi traženi podaci neophodni. Ako stranica traži djevojačko prezime ili druge lične podatke vaše majke bez jasne potrebe, razmislite dva puta. Iz perspektive privatnosti, koristite postavke privatnosti na društvenim mrežama kako biste ograničili ko može vidjeti vaše objave. A za organizaciju, osigurajte da direktoriji ili osjetljivi dokumenti ne budu nehotice izloženi na vlastitoj web stranici. Povremeno tražite svoje ime CSO's na mreži kako

biste vidjeli koje su informacije tamo – možete uhvatiti izloženi dokument ili lažno predstavljanje stranice na ovaj način.

Koristite ažurirane pretraživače i sigurnosne alate: Sigurna upotreba interneta nije samo ponašanje;' se također odnosi na korištenje ažurirane tehnologije. Uvijek pokrenite najnoviju verziju vašeg web pretraživača (Chrome, Firefox, Edge, itd.), budući da ažuriranja često zakrpe sigurnosne propuste. Omogućite ugrađene sigurnosne funkcije pretraživača: većina pretraživača ima phishing i zaštitu od zlonamjernog softvera koji mogu blokirati poznate loše web stranice. Također biste trebali imati renomirani antivirus/anti-malware program aktivan na vašem uređaju, što ponekad može otkriti da li je preuzimanje ili stranica zlonamjerna. Moderna antivirusna rješenja često uključuju web zaštitu koja upozorava ili blokira ako pokušate posjetiti stranicu poznatu po phishing ili hosting zlonamjernog softvera. Na primjer, Microsoft Defender ili Avast mogu bljesnuti stranicu upozorenja ako pokušate pristupiti opasnoj stranici. Obratite pažnju na ova upozorenja; oni su tu da vas zaštite.

Sumirati, sigurno korištenje interneta uglavnom je u vezi s ostankom na oprezu i skeptično kada ste na mreži. Slično kao ulične pameti u velikom gradu –, ostajete svjesni svog okruženja i dvaput razmislite prije nego što uđete u sumnjivu uličicu – na mreži, trebali biste gledati gdje "putujete" i s kim komunicirate. Ohrabrite sve u svom timu da usvoje oprezan način razmišljanja: lebdite preko linkova prije klizanja, preuzimajte samo iz pouzdanih izvora i sa sumnjom tretirajte neželjene iskačuće ili poruke. U sljedećem odjeljku, mi'll ulazimo dublje u jedan od najčešćih načina napada, e-pošte i poruka i kako osigurati te komunikacije.

Sigurnost e-pošte i poruka

E-pošta je nezamjenjiv alat za OCD, a aplikacije za razmjenu poruka (kao što su WhatsApp, Signal ili Telegram) se široko koriste za brzu komunikaciju. Međutim, ovi kanali su česte mete sajber napada kao što su phishing, prisluškivanje i otmica računa. Ovaj odjeljak pruža smjernice o tome kako sigurnije komunicirati i izbjegavati uobičajene zamke.

Phishing Awareness: Phishing e-pošte je ranije dotaknut jer je tako preovlađujući. Ponavljati i širiti: Uvijek pažljivo pregledajte neočekivane e-poruke, posebno one koji pozivaju na hitnu akciju ili traže osjetljive informacije. Tipična phishing e-pošta može izgledati kao da

dolazi od kolege, banke ili online usluge i sadrži link do “log in” ili dodatak za otvaranje. Prije nego što kliknete na bilo koju vezu u e-poruci, provjerite pošiljaoca i metu veze. Pažljivo provjerite adresu pošiljaoca – napadači često koriste adresu koja se odbija pismom (npr. john.doe@micros0ft.com umjesto legitimne Microsoft e-pošte) ili javnom e-poštom koja ne odgovara organizaciji koja se tvrdi. Ako e-mail tvrdi da trebate resetirati lozinku ili dati informacije, on je sigurniji da ne kliknete na vezu e-pošte. Umjesto toga, idite sami na službenu web stranicu. Za priloge ne otvarajte datoteke iz nepoznatih ili nepouzdanih e-poruka. Čak i ako se osmišljava iz poznatog kontakta, ako je neočekivan i čudan (npr., nasumični dokument pod nazivom “Invoice” koji vi are’t nije očekivao), provjerite sa pošiljaocem kroz drugi kanal. Po pravilu, izbjegavajte omogućavanje makroa ili omogućavanje sadržaja u Office dokumentima osim ako niste apsolutno sigurni u njihov izvor – mnoge zlonamjerne infekcije dolaze preko Word/Excel makroa u phishing prilozima.

OCD bi trebali educirati svoje osoblje da je u redu (čak ohrabreno) biti pomalo paranoičan s e-porukama – kada su u nedoumici, provjerite. Brzi telefonski poziv ili poruka navodnom pošiljaocu mogli bi potvrditi da li su zaista poslali taj zahtjev. Bolje je provjeriti nego kliknuti i žaliti. Zapamtite, phishing nije ograničen na e-poštu; može se pojaviti i putem SMS-a (tekstualnih poruka sa lošim linkovima) ili aplikacija za razmjenu poruka. Na primjer, član osoblja može dobiti WhatsApp poruku koja izgleda kao upozorenje od online usluge plaćanja s linkom – tretirajte ih na isti način, s oprezom.

Sigurnost računa e-pošte: Budući da računi e-pošte mogu biti kapija za resetovanje drugih lozinki i sadržavanje osjetljive korespondencije, osiguranje prijave e-pošte je ključno. Koristite snažnu lozinku i 2FA za svoj nalog e-pošte (kao što je objašnjeno u 2.1) – mnogi provajderi e-pošte kao što su Gmail, Outlook ili ProtonMail podržavaju dvofaktorsku autentifikaciju putem aplikacije ili SMS-a. Ovo drastično smanjuje rizik da neko hakuje vašu e-poštu. Također, imajte na umu kada pristupate e-pošti na zajedničkim ili javnim računarima; uvijek se odjavite nakon toga i osigurajte da pretraživač ne sačuva vaše akreditive. Ako je moguće, koristite sigurne protokole e-pošte (većina modernih usluga nije u skladu s ovim): osigurajte da webmail koristi HTTPS, a ako koristite aplikaciju za klijente e-pošte (kao što su

Outlook, Thunderbird ili na svom telefonu), pobrinite se da se ona's postavi za korištenje šifriranih veza (SSL/TLS) za primanje (IMAP/POP) i slanje (SMTP). Vaša IT podrška ili dokumentacija o provajderima može potvrditi ove postavke.

Razmotrite enkripciju e-pošte za visoko osjetljive komunikacije. Standardne e-poruke nisu end-to-end šifrirane, što u teoriji znači da sadržaj e-pošte mogu čitati nenamjerne strane (kao što su provajderi e-pošte ili bilo ko ko dobije pristup računu). Za osjetljive podatke, možete koristiti alate kao što su PGP/GPG e-mail enkripcija ili prebaciti na sigurne platforme za razmjenu poruka za taj razgovor. Međutim, PGP može biti složen za svakodnevnu upotrebu, tako da je druga strategija korištenje sigurne podjele datoteka za osjetljive priloge umjesto stavljanja povjerljivog teksta u tijelo e-pošte. Neke usluge e-pošte fokusirane na CSO ili poslovni paketi nude ugrađenu enkripciju ili barem mogućnost zaštite e-pošte ili priloga od lozinki. Ako je tvoj organizacija se bavi izuzetno osjetljivim informacijama (slučajevi ljudskih prava, na primjer), trebali biste se konsultovati sa stručnjakom za digitalnu sigurnost o postavljanju radnog toka šifriranja.

Sigurne aplikacije za razmjenu poruka: Mnogi OCD koriste instant poruke za brze razgovore i koordinaciju. On's je važan za odabir aplikacija za razmjenu poruka koje nude end-to-end enkripciju (E2EE), što osigurava da samo korisnici koji komuniciraju (i niko između, čak ni pružatelj usluga) mogu čitati poruke. WhatsApp, na primjer, ima E2EE po defaultu za razgovore, kao i Signal i Telegram's "tajni chats" (napomena: Telegram cloud chats nisu E2EE prema zadanim postavkama). Signal se široko preporučuje u zajednici civilnog društva za osjetljive komunikacije jer je otvorenog koda, E2EE, i ima snažnu praksu privatnosti. Drugi je **Žica**, koji je takođe siguran i evropski usklađen sa GDPR. **Threema** i **Element (Matrica)** jesu li to druge sigurne opcije za razmjenu poruka koje koriste neke grupe za ljudska prava. Specifičan izbor aplikacije može ovisiti o vašem kontekstu i onome što koriste vaši kolege, ali opće pravilo je: izbjegavajte kanale otvorenog teksta (SMS tekstovi ili nešifrirane e-poruke) za osjetljive stvari i migrirajte u šifriranu aplikaciju gdje je to izvodljivo.

Čak i kod šifriranih aplikacija, imajte na umu metapodatke (koji s kim razgovara, kada). Većina E2EE aplikacija i dalje otkriva neke metapodatke servisu (iako Signal to pokušava minimizirati). Za izuzetno osjetljive operacije, mogli bi se koristiti alati koji su više fokusirani na

anonimnost poput *Sjednica* ili koristite poruke preko Tora, ali to su napredni scenariji. Za opću upotrebu CSO-a, mainstream E2EE aplikacija će znatno poboljšati sigurnost u poređenju sa nešifriranim kanalima.

Također, zaključajte svoje aplikacije za razmjenu poruka: Koristite funkcije zaključavanja aplikacija ili PIN uređaja tako da ako je vaš telefon izgubljen ili ukraden, neko ne može samo otvoriti vaše razgovore. Omogućite poruke koje nestaju za vrlo osjetljive razgovore – mnoge aplikacije omogućavaju vam da postavite poruke na auto-delete nakon određenog vremena (Signal, WhatsApp, itd.). Na taj način, ako neko kompromituje vaš račun kasnije, prethodne poruke možda već nestanu.

Čuvajte se prevara poruka: Phishing prevare ne zloupotrebljavaju samo e-poštu. Možda ćete dobiti lažne poruke putem SMS-a ili aplikacija koje vas traže da kliknete na link (često skraćeni URL-ovi) ili da nešto prosledite. Primjer je “WhatsApp code” prevara: dobijate SMS sa kodom za prijavu koji niste zatražili, a zatim odmah WhatsApp poruku od prijatelja koji kaže: “I’m ako imaš problema, molim te pošalji mi kod koji si upravo dobio.” Taj prijatelj’s nalog je vjerovatno hakovan, a napadač pokušava da iskoristi vaš kod da preuzme vaš WhatsApp. Lekcija: nikada ne dajte kodove za verifikaciju drugima i budite sumnjičavi prema hitnom, čudni zahtjevi na chatu, čak i ako od prijatelja.

Prilozi i Cloud Linkovi: Umjesto da pričvrste dokumente e-poštom, mnogi su prešli na cloud linkove (npr., Google Drive, Dropbox, OneDrive linkove). Ovo je zgodno, ali imaju svoje sigurnosne razloge. Ako pošaljete link za dijeljenje oblaka, osigurajte da je on dostupan samo namjeravanim ljudima (koristite privatne veze ili eksplicitno dodajte njihove e-poruke) i razmislite o određivanju datuma isteka veze. Ako dobijete vezu u oblaku, budite oprezni kao i kod bilo koje veze – pobrinite se da ona osnuje iz legitimnog domena usluge u oblaku i da ste to očekivali. Taktika phishinga može poslati link koji izgleda kao Google Drive datoteka, ali vodi do lažne stranice za prijavu. Uvijek potvrdite ako je potrebno, i idealno, pristupite zajedničkim diskovima preko poznatog interfejsa (npr., prijavite se u svoj Google Drive direktno da vidite da li je datoteka podijeljena s vama).

Higijena e-pošte i najbolje prakse: Još nekoliko brzih savjeta: Koristite filtere za neželjenu poštu – modernih usluga e-pošte radi pristojan posao hvatanja većine

smeća/phishinga. Ipak, povremeno provjerite svoju fasciklu za neželjenu poštu za lažne pozitivne rezultate, ali don't komunicirajte s e-porukama u neželjenoj pošti osim ako niste sigurni da su sigurni. Don't ne odjavljuje neželjene e-poruke osim ako nisu iz renomiranih izvora; Klikom na "unssubscribe" o istinski neželjenim e-porukama možete potvrditi neželjenim licima da je vaša adresa aktivna. Bolje je samo izbrisati ih. Prilikom slanja e-poruka velikim grupama, koristite BCC da zaštitite primaoce' adrese od svih (spriječavajući slučajno curenje kontakt lista). I razmislite o omogućavanju upozorenja o prosljeđivanju e-pošte ili upozorenja o prijavi ako ih vaš provajder nudi, tako da znate da li se dogodi bilo kakva neobična aktivnost (na primjer, Gmail vas može obavijestiti ako se nova prijava dogodi s novog uređaja).

Praćenjem ovih praksi, vaša organizacija može značajno smanjiti rizik od pada žrtve na napade zasnovane na e-pošti ili porukama. Budući da je e-pošta često prva kontaktna tačka za napadače, ovladavanje sigurnošću e-pošte donosi veliku sigurnosnu isplatu. Zamislite to kao sigurnu vožnju: većinu vremena, "putevi" (internet) su u redu, ali morate nositi svoj pojas (2FA), poslušati signale (upozorenja o sumnjivim vezama) i ostati pažljivi kako biste izbjegli nesreće.

Osnovni savjeti za osiguranje računara i telefona

Laptopovi, desktop računari i pametni telefoni su radni konji bilo koje moderne organizacije. Oni također pohranjuju mnogo osjetljivih podataka i mogu biti ulazne tačke za napadače ako nisu osigurani. Ovaj odjeljak pruža osnovne savjete kako bi ovi uređaji bili sigurni od uobičajenih prijetnji. Mnogi od ovih savjeta spadaju u rutinsko održavanje i razumnu upotrebu – digitalni ekvivalent zaključavanja vaših vrata i redovnim promjenama ulja.

Držite softver ažuriranim: Osigurajte da svi vaši uređaji' operativni sistemi i aplikacije budu u toku s najnovijim sigurnosnim zakrpama. Ažuriranja softvera često popravljaju ranjivosti koje napadači mogu iskoristiti. Uključite automatska ažuriranja gdje god je to moguće –, na primjer, omogućite Windows Update ili macOS' automatska ažuriranja, a isto radite i na svom iPhone/Android telefonu za sistem i aplikacije. Također, redovno ažurirajte svoje aplikacije (preglednici, kancelarijski programi, itd.); mnogi će se javiti kada je ažuriranje dostupno – ne ignorišite te upite. Za svaki softver koji ne osmisli auto-update, postavite podsjetnik koji se ponavlja da provjerite ažuriranja ili koristite centralizirani alat za upravljanje ako je dostupan.

Zapamtite da ovo uključuje dodatke za pretraživače i okvire kao što su Java ili Adobe Reader, koji su istorijski bili putevi za zlonamjerni softver ako su zastarjeli. Ažurirani uređaj je očvrsnuo uređaj.

Instalirajte zaštitu od antivirusa/anti-Malvera: Koristite renomiranu antivirusnu otopinu na svojim računarima (i razmotrite jednu od renomiranih aplikacija za mobilnu sigurnost i za Android uređaje). Moderni antivirusni softver pruža zaštitu u realnom vremenu, što znači da će aktivno skenirati datoteke i pratiti ponašanje sistema kako bi blokirao zlonamjerni softver. Windows 10/11 dolazi sa ugrađenim Microsoft Defenderom, koji je prilično dobar za osnovnu upotrebu ako se ažurira. Mogu se razmotriti i opcije trećih strana (plaćene ili besplatne) kao što su Avast, Bitdefender i ESET, itd. Ključno je imati nešto i svakodnevno ažurirati svoje definicije virusa. Izbjegavajte korištenje više antivirusnih programa odjednom (mogu se sukobiti). Na telefonima, iPhone uređajima općenito nisu potrebne odvojene AV aplikacije zbog načina na koji je iOS dizajniran, ali Android telefoni mogu imati koristi od aplikacije protiv zlonamjernog softvera, posebno ako ponekad instalirate aplikacije izvan službene Play Store-a. Međutim, najbolja odbrana za telefone je instaliranje aplikacija samo iz pouzdanih trgovina aplikacija i provjeravanje dozvola za aplikacije – aplikacije za baterijsku lampu, na primjer, ne bi trebala't vidjeti vaše kontakte ili poruke.

Još jedna stvar: nikad ne onemogućite svoj sigurnosni softver iz pogodnosti. Ako blokira radnju, istražite zašto umjesto da je jednostavno isključite. Takođe, nemojte instalirati piratski softver, kao što je spomenuto – osim legalnosti, napuknuti softver često dolazi u paketu sa trojanima koji antivirusni softver može, ali ne mora uhvatiti.

Koristite Device Locks and Encryption: Uvijek zaključajte svoje uređaje PIN-om, lozinkom ili biometrijskom bravom (otisak prsta, prepoznavanje lica) kada se ne koriste. Postavite kratko vremensko ograničenje automatskog zaključavanja (npr., zaključavanje ekrana nakon pet minuta neaktivnosti ili manje). Ovo sprečava neovlašćeni pristup ako neko fizički dobije vaš uređaj. Ako se CSO laptop ukrade iz automobila ili se telefon izgubi na konferenciji, jak ekran za zaključavanje može zaštititi podatke od znatiželjnih očiju –, ali samo ako je' na mjestu. Za laptope razmotrite enkripciju punog diska. Moderni operativni sistemi to često imaju po defaultu: Windows ima BitLocker (Pro izdanja) ili Device Encryption, a macOS ima FileVault.

Kada su omogućeni, čak i ako se hard disk ukloni, podaci ostaju šifrirani bez ključa za dešifriranje (obično vezani za vašu lozinku za prijavu). Na pametnim telefonima, iOS i Android podržavaju enkripciju uređaja (novije verzije se podrazumevano šifriraju kada koristite PIN/password). Provjerite da li je enkripcija omogućena, posebno na starijim verzijama Androida gdje je možda bila opciona. Šifrovanje je ključno za osjetljive podatke; na primjer, ako se laptop koji sadrži podatke učesnika za studiju izgubi, ali šifrira, podaci ostaju sigurni, a incident je problem izgubljenog uređaja, a ne kršenje podataka.

Redovne rezervne kopije: Iako su sigurnosne kopije prvenstveno mjera oporavka podataka, one su također sigurnosna mjera –, one vam omogućavaju da se oporavite od ransomware-a ili gubitka uređaja bez prestanka na iznudu ili potpuni gubitak. Poglavlje 3 će detaljno opisati strategije sigurnosne kopije, ali kao osnovni savjet: redovno rezervišete važne datoteke i držite sigurnosne kopije na sigurnoj lokaciji odvojenoj od vašeg računara (spoljni pogon se čuva bezbedno ili usluga sigurnosne kopije u oblaku). Povremeno testirajte te sigurnosne kopije kako biste osigurali da možete vratiti podatke. Za mobilne uređaje razmislite o praćenju važnih fotografija/doka (telefoni se mogu podesiti da se vrate u oblak ili računar). U slučaju krađe telefona, barem vaši podaci ne nestaju zauvijek.

Sigurna instalacija aplikacija/programa: Ugradite softver iz pouzdanih izvora. Na računarima to obično znači službenu web stranicu softvera ili poznatu prodavnicu aplikacija (kao što je Microsoft Store ili Mac App Store). Na telefonima koristite Google Play Store, Apple App Store ili F-Droid (za Android aplikacije otvorenog koda). Budite oprezni sa besplatnim uslužnim programima sa nepoznatih web stranica – ako vam je potreban PDF pretvarač ili video plejer, na primjer, istražite renomiranu umjesto preuzimanja prve stvari koju pronađete. Neki zlonamjerni programi maskiraju se kao korisni alati. Također, tokom instalacije obratite pažnju na upite i odbijete sve ponude za ugradnju dodatnih traka s alatima ili promjenu pretraživača (uobičajeno u besplatnim instalaterima). Ovo nisu baš sigurnosne prijetnje, ali oni uznemiravaju vaš sistem i mogu uvesti ranjivosti ili probleme s privatnošću.

Sigurna konfiguracija i postavke: Uzmite trenutak da konfigurišete osnovne sigurnosne postavke na svojim uređajima. Na primjer, na Windows-u osigurajte da se zaštitni zid uključi (obično je po defaultu). Vatrozid pomaže u blokiranju neželjenih ulaznih veza. Većina korisnika

neće morati da ga prilagodi izvan zadanog zadatka, ali bi trebao ostati omogućen. Na svom ruteru, pobrinite se da je firewall/NAT uključen i daljinski administrator isključen (kao što je spomenuto na sigurnom internetu). Na pametnim telefonima provjerite postavke privatnosti za svaku aplikaciju – onemogućava nepotrebne dozvole (da li je igri potreban pristup vašem mikrofonu? Vjerovatno ne). I Android i iOS vam omogućavaju da pogledate koje dozvole svaka aplikacija ima i opozovete one koji izgledaju pretjerano.

Fizička sigurnost uređaja: Digitalna sigurnost je da nije važna samo digitalni – uređaji za fizičko osiguranje. Don't ostavlja laptope ili telefone bez nadzora na javnim mjestima. U kancelariji, imate politiku zaključavanja ekrana kada se udaljite od svog stola (Windows i Mac imaju prečice za ovo). Ako putujete, pazite na laptope na aerodromskom obezbjeđenju ili u taksiju – mnoga kršenja su jednostavno izgubljeni uređaji s osjetljivim informacijama. Također, razmislite o ekranima privatnosti za laptope ako često radite u javnosti (kako biste spriječili surfanje na ramenu na ekranu). Za desktop računare, posebno ako vaš CSO ima kancelariju dostupnu posetiocima ili zajedničke prostore, zaključavanje serverskih soba ili korišćenje kablovskih brava za opremu može odvratiti krađu.

Upotreba upravljanja mobilnim uređajima (MDM) za organizacije: Ako vaš CSO ima kapacitet (ili kako raste), možete implementirati MDM rješenje. MDM softver omogućava organizaciji da provodi sigurnosne politike na telefonima i laptopima centralno –, na primjer, zahtijevajući PIN, gurajući automatska ažuriranja ili daljinski brišući uređaj ako se odluči izgubiti. Čak i bez formalnog MDM-a, barem osigurajte da možete daljinski brisati uređaje: za telefone, usluge kao što su Find My iPhone ili Android's Find My Device mogu daljinski locirati i izbrisati izgubljeni telefon. Za laptope, ako koristite Windows povezan sa Microsoft računom ili poslovnim alatima, postoje ponekad slične opcije. U najmanju ruku, znajte kako promijeniti lozinke i poništiti sesije za račune na izgubljenom uređaju (na primjer, ako vaš volonter izgubi telefon koji je imao pristup e-poruci CSO's, odmah promijenite tu lozinku e-pošte i potpišite sve sesije).

Plan neuspjeha: Ponekad hardver ne uspijeva ili se pokvari. Iako nisu "sajber napad," ovi događaji mogu uzrokovati gubitak podataka ili zastoj. Osnovni savjet: koristite pouzdan antivirus, ali i držite neke alate za oporavak praktičnim (kao što je čisti USB stick za pokretanje s

antivirusnim ili sistemskim alatima za popravku). I osigurajte da važne datoteke nisu't pohranjene isključivo na jednom laptopu; ako hardver ne uspije, imate rezervne kopije ili sinhronizaciju.

Primjenom ovih temeljnih savjeta stvarate osnovni nivo zaštite za svoje lične i radne uređaje. Zamislite to kao osiguranje "krajnjih tačaka" – svaki telefon ili PC je krajnja tačka koja se može iskoristiti ako je slaba, ali zajedno čine vaše CSO's digitalno okruženje. Napadač će često ići na najlakšu metu. Ove mjere (ažuriranja, antivirusni, jake konfiguracije) uklanjaju nisko visi voće, prisiljavajući protivnike da rade mnogo teže ili ih idealno u potpunosti odvraćaju. On se zalaže analogno kućnoj sigurnosti: zaključavate vrata, postavljate dimne alarme i možda imate psa – ništa od ovoga ne garantuje sigurnost, ali oni uvelike smanjuju rizike i pružaju upozorenja. U sajber sigurnosti, vaš ažurirani, dobro konfigurirani uređaj sa sigurnosnim softverom je poput doma s bravama i alarmima – daleko manje privlačan uljezima od netaktovanog, nezaštićenog sistema.

Sa ličnim i sigurnosnim navikama uređaja, sada prelazimo na organizacioni nivo: razvijanje plana i kulture u vašem OCD-u koji podržava digitalnu sigurnost. Sljedeće poglavlje će se pozabaviti kako procijeniti rizike i stvoriti jednostavno, ali efikasno **Plan digitalne sigurnosti** prilagođen vašim potrebama CSO's.

Sažetak poglavlja

Poglavlje 2 pruža pristupačan uvod u fundamentalne koncepte kibernetičke sigurnosti prilagođene organizacijama civilnog društva, fokusirajući se na CIA trijadu: povjerljivost, integritet i dostupnost. Povjerljivost osigurava da podaci (npr. evidencija donatora) ostanu privatni, integritet sprječava neovlaštene promjene, a dostupnost održava sisteme dostupnim. Poglavlje koristi običan jezik i primjere relevantne za OCD, kao što je osiguranje lista kontakata aktivista, da objasni ove principe. Uvodi modeliranje prijetnji, proces za identifikaciju rizika i određivanje prioriteta zaštite, čineći ga relevantnim za resurse ograničene organizacije. Praktične najbolje prakse uključuju jake lozinke, dvofaktorsku autentifikaciju (2FA) i opreznu upotrebu interneta. Poglavlje naglašava jeftina rješenja, kao što su besplatni menadžeri lozinki (npr. Bitwarden), za rješavanje budžetskih ograničenja CSOs'. Također naglašava ljudski element, napominjući da 74% kršenja uključuje greške poput pada na phishing prevare.

Podsticanjem svijesti, OCD mogu ublažiti rizike bez tehničke stručnosti. Poglavlje podstiče početak jednostavnim koracima (npr. ažuriranje softvera) za izgradnju sigurnosne fondacije. Povezuje digitalnu sigurnost sa misijama CSOs', objašnjavajući kako zaštita podataka podržava povjerenje i odgovornost. Na primjer, kompromitovana baza podataka donatora mogla bi narušiti povjerenje javnosti, kao što se vidi u prošlim incidentima. Poglavlje postavlja praktičan ton za e-knjigu, opremajući čitaocima temeljno znanje da efikasno implementiraju sigurnosne mjere.

Korak-by-Step vodič za provođenje osnovne procjene rizika

Ovaj vodič pruža strukturirani proces za OCD da završe šablon procjene rizika, s primjerima prilagođenim uobičajenim sredstvima OCD-a kao što su baze podataka donatora i volonterski zapisi. Koraci su dizajnirani da budu dostupni organizacijama sa ograničenom tehničkom ekspertizom, usklađujući se sa naglaskom na nastavnom planu i programu. Naglašava praktične okvire (Modul 2) i smjernice e-knjige's o procjeni rizika (poglavlje 5).

Korak 1: Identificirajte kritična digitalna sredstva

- Šta učiniti: Navedite digitalnu imovinu (podaci, sistemi, računi) bitnu za vaše CSO's operacije. Fokusirajte se na ono što bi poremetilo vašu misiju ili naštetilo dionicima ako je kompromitovano.
- Kako to učiniti: Okupiti mali tim (npr., vodstvo, programsko osoblje, IT žarište) da razmišlja. Razmotrite podatke (npr. liste donatora, informacije o korisnicima), sisteme (npr., e-poštu, web stranicu) i račune (npr., društvene mreže, skladištenje u oblaku).

  Primjer:

  - Baza podataka donatora: tabela ili CRM sistem koji sadrži imena donatora, kontakt podatke i iznose donacija.
  - Volunteer Records: Datoteke s imenima volontera, kontakt informacijama i rasporedima pohranjenim na zajedničkoj platformi za vožnju ili oblak.
  - Računi e-pošte: Nalozi osoblja Gmail ili Outlook koji se koriste za komunikaciju sa dionicima.

Korak 2: Identificirajte prijetnje svakoj imovini

- Šta učiniti: Za svaku imovinu navedite potencijalne prijetnje (npr., hakiranje, phishing, zlonamjerni softver, ljudsku grešku) koje bi to mogle ugroziti.
- Kako to učiniti: Razgovarajte o tome kako napadači mogu ciljati na imovinu ili šta može poći po zlu (npr., slučajno curenje, krađa uređaja). Pozivajte na uobičajene prijetnje iz e-knjige (poglavlje 1.3), kao što su phishing, kršenje podataka ili ransomware.

  Primjer:

  - Baza podataka donatora:

        - Prijetnja: Kršenje podataka putem phishinga (napadač prevari osoblje da otkrije vjerodajnice za prijavu).
        - Prijetnja: Ransomware šifrira bazu podataka.
    - Volunteer Records:
        - Prijetnja: Neovlašten pristup zbog slabih lozinki ili zajedničkih akreditiva.
        - Prijetnja: Gubitak podataka ako je laptop ukraden.

Korak 3: Procijenite vjerovatnoću svake prijetnje

- Šta učiniti: Ocijenite koliko je vjerovatno da će se svaka prijetnja dogoditi na skali od 1 (rijetko) do 5 (skoro sigurno).
- Kako to učiniti: Razmotrite faktore kao što su vaša vidljivost u organizaciji civilnog društva, prošli incidenti ili uobičajeni trendovi napada (npr. phishing je široko rasprostranjen). Koristite lokalni kontekst ako je dostupan (npr., čest phishing u svom regionu).

  Primjer:
    - Baza podataka donatora:
        - Phishing: Vjerovatnoća = 3 (moguća, jer je phishing uobičajen, ali vaše osoblje ima određenu obuku).
        - Ransomware: Vjerovatnoća = 2 (Nevjerovatno, ako je antivirus na mjestu, ali nije nemoguće).
    - Volunteer Records:
        - Neovlašteni pristup: Vjerovatnoća = 4 (Vjerovatno, ako su lozinke slabe ili pristup nije ograničen).
        - Krađa laptopa: Vjerovatnoća = 2 (Nevjerovatno, ali moguće u terenskim operacijama).

Korak 4: Procjenite Utjecaj svake prijetnje

- Šta učiniti: Ocijeniti ozbiljnost posljedica prijetnje na skali od 1 (nisko) do 5 (teško), uzimajući u obzir poremećaj misije, gubitak podataka ili štetu reputaciji.

- Kako uradi to: Razmislite o najgorem scenariju (npr. pravnim pitanjima, gubitku povjerenja, šteti korisnicima). Referencirajte primjere e-knjige's, kao što je kršenje australskog Crvenog križa (poglavlje 1.1).

  Primjer:

  - Baza podataka donatora:
    - Phishing/Breach: Uticaj = 5 (Teško, zbog izloženosti donatorskim podacima, GDPR kazne, gubitak povjerenja).
    - Ransomware: Impact = 4 (visok, jer bi se operacije mogle zaustaviti bez rezervnih kopija).
  - Volunteer Records:
    - Neovlašćen pristup: Uticaj = 4 (Visoko, jer kršenje privatnosti volontera može naštetiti reputaciji).
    - Krađa laptopa: Uticaj = 3 (umjereno, ako su podaci šifrirani, ali oporavak je skup).

Korak 5: Izračunajte ocjene rizika i dajte prioritet

- Šta učiniti: Pomnožiti vjerovatnoću po uticaju da biste dobili ocjenu rizika (1-25). Viši rezultati ukazuju na rizike kojima je potrebna hitna pažnja.
- Kako to učiniti: Koristite predložak za izračunavanje rezultata i sortiranje rizika od najviših do najnižih. Prvo se fokusirajte na rješavanje rizika s visokim rezultatom.

  Primjer:

  - Baza podataka donatora:
    - Phishing: 3 x 5 = 15 (Visoki prioritet).
    - Ransomware: 2 x 4 = 8 (Umjereni prioritet).
  - Volunteer Records:
    - Neovlašćen pristup: 4 x 4 = 16 (Visoki prioritet).
    - Krađa laptopa: 2 x 3 = 6 (niski prioritet).

Korak 6: Razvijajte korake ublažavanja

- Šta da uradi: Navedite specifične, djelotvorne korake za sprječavanje ili smanjenje svake prijetnje, fokusirajući se na jeftine, praktične mjere.
- Kako to učiniti: Izvucite iz nastavnog plana i programa (Modul 1-5) i e-knjige (Poglavlja 2-4) za rješenja kao što su 2FA, enkripcija ili obuka. Osigurajte da su koraci izvodljivi za vaše resurse CSO's.

  Primjer:

  - Baza podataka donatora:
    - Phishing: Omogućite 2FA pristup bazi podataka, šifrirajte datoteke i obučite osoblje za otkrivanje phishing-a.
    - Ransomware: Postavite sedmične sigurnosne kopije na siguran oblak, instalirajte ažurirani antivirusni softver.
  - Volunteer Records:
    - Neovlašćen pristup: Koristite jake lozinke, ograničite pristup ovlašćenom osoblju i revidirajte dozvole mjesečno.
    - Krađa laptopa: Omogući šifriranje uređaja, koristite alate za daljinsko brisanje za izgubljene uređaje.

Korak 7: Pregled i ažuriranje

- Šta učiniti: Dodijelite članu tima da pregleda procjenu rizika godišnje ili nakon velikih promjena (npr. novi softver, promjene osoblja). Ažurirajte predložak po potrebi.
- Kako to učiniti: Zakažite sastanak revizije kako biste provjerili jesu li se promijenile imovine, prijetnje ili koraci ublažavanja. Ažuriranja dokumenata kako bi se osiguralo da plan ostane relevantan.

  Primjer: Nakon implementacije 2FA, vjerovatnoća neovlaštenog pristupa volonterskim evidencijama pada na 2, smanjujući rezultat rizika na 8. Ažurirajte predložak u skladu s tim.

2.3 POGLAVLJE – 3: DIGITALNI SIGURNOSNI PLANOVI ZA CSO

Plan digitalne sigurnosti za OCD

Nakon što smo pokrili individualne prakse, okrećemo se širem organizacionom pristupu. Plan digitalne sigurnosti je strateška i operativna mapa puta za to kako će vaš CSO zaštititi svoju digitalnu imovinu i odgovoriti na prijetnje. Ne mora biti komplikovan ili dugačak dokument. U stvari, koncizan plan koji svi razumiju često je bolji od glomazne politike koja se nalazi na polici. Ovo poglavlje vas vodi kroz kreiranje osnovnog sigurnosnog plana, fokusirajući se na **četiri ključna elementa:** – Prepoznavanje vaših rizika,

– Formulira plan odgovarajućim mjerama,

– svijest o izgradnji kroz obuku,

– Zaštita vaših podataka putem rezervnih kopija i sigurnog skladištenja.

Prepoznavanje Riska: Kakve prijetnje vaša organizacija suočava?

Svaka organizacija ima jedinstven profil rizika u zavisnosti od svojih aktivnosti, podataka i protivnika. Prvi korak u razvoju sigurnosnog plana je da **identificiraj I procijeni te rizike** <TAG1> u suštini, za izvođenje jednostavne procjene digitalnog rizika. Ovo ne ukazuje na to da zahtijeva napredni stepen; to znači sistematsko razmišljanje o tome šta bi moglo poći po zlu i koliko bi loše moglo naštetiti vašim operacijama ako jeste.

Identificirajte svoju imovinu i podatke: Počnite tako što ćete navesti važna digitalna sredstva i informacije koje posjeduje vaš CSO. To uključuje: hardver (računari, telefoni, serveri), softver i usluge (računi e-pošte, web stranice, cloud diskovi, baze podataka) i podatke (liste članova, finansijske evidencije, istraživački podaci, komunikacije, itd.). Postavljajte pitanja poput: Koji bi podaci izazvali najveću štetu ako bi se objavili? Koji su sistemi kritični za naš svakodnevni rad? Na primjer, OCD koji pruža pravnu pomoć može dati prioritet dosijeima o slučajevima klijenata i komunicirati sa advokatima kao kritičnom imovinom za zaštitu (zbog povjerljivosti). Razvojni CSO bi mogao identificirati svoju bazu podataka donatora i podatke o istraživanju na terenu kao vitalne. Znati šta su vaši "krunski dragulji" pomoći će da fokusirate svoje sigurnosne napore.

Identificirajte potencijalne prijetnje i aktere prijetnje: Zatim razmislite ko ili šta bi moglo naštetiti vašoj organizaciji's digital infrastruktur. Neke uobičajene prijetnje su neselektivne –

npr., nasumični sajber kriminalci koji šire ransomware radi profita, što bi moglo pogoditi svakoga. Drugi bi mogli biti više ciljani: možda kompanije ili pojedinci koji se protive vašem zagovaranju, ili čak nadzor vlade ako radite na osjetljivim pitanjima. Navedite kategorije prijetnji: hakeri koji traže finansijsku dobit, insajderi (osoblje ili volonteri) koji bi slučajno ili namjerno mogli ugroziti sigurnost i prijetnje specifične za vaš kontekst (na primjer, kampanja OCD-a protiv korupcije mogla bi privući ciljani phishing ili pokušaje hakovanja telefona od strane pogođenih strana). Također razmotrite fizičke prijetnje digitalnoj imovini, kao što je krađa opreme ili uništenje zbog katastrofa (poplava, požar – one također mogu uzrokovati IT prekide, zbog čega su potrebne sigurnosne kopije van lokacije).

Za svaku prijetnju razmislite o mogućim scenarijima: *Kako* može li se ta prijetnja manifestirati? Na primjer:

- Cyber kriminalac bi mogao pokušati hakirati vašu web stranicu kako bi je deaktivirao ili koristio za distribuciju zlonamjernog softvera.
- Neprijateljski glumac može poslati phishing e-poruke vašem osoblju, pokušavajući ukrasti lozinke i pročitati vaše e-poruke.
- Malver poput ransomware-a mogao bi zaraziti kompjuter osoblja, šifrirati datoteke i zahtijevati otkupninu, kao što je objašnjeno u prethodnim poglavljima.
- Volonter bi mogao izgubiti laptop sa nešifriranim osjetljivim podacima.
- Nezadovoljni bivši zaposlenik bi i dalje mogao imati pristup računu ako se offboarding nije pravilno obavio, što predstavlja rizik od krađe podataka ili sabotaže.

Procjenite vjerovatnoću i uticaj: Nisu svi rizici jednaki. Iako bi neki događaji mogli biti vrlo malo vjerojatni, ali katastrofalni ako bi se dogodili, drugi bi mogli biti vjerovatno, ali manji u utjecaju. Za svaki identifikovani scenario rizika, ocjenjivati koliko je vjerovatno da će se to dogoditi (nizak, srednji, visok) i kakav bi bio uticaj ako se dogodi (nizak, srednji, visok uticaj). Na primjer, *phishing napadi* vrlo su vjerovatni (velika vjerovatnoća) i mogu imati veliki utjecaj (ako se ukradu vjerodajnice računa) – tako da se osnuje visok rizik koji zahtijeva snažno ublažavanje. S druge strane, *hardverski kvar* prilično je vjerovatno tokom vremena (na kraju disk ne uspije), ali

ako imate rezervne kopije, utjecaj je nizak, tako da ukazuje na umjereni rizik kojim upravljate rezervnim kopijama. Ili *ciljano hakovanje koje sponzorira država* možda će imati veliki uticaj (mogli bi da naprave dubok kompromis), ali ako osmislite mali lokalni CSO bez kampanja visokog profila, vjerovatnoća bi mogla biti mala – i dalje vrijedan neke zaštite, ali ne i vaš fokus broj 1.

Ova vrsta kvalitativne procjene vam pomaže da date prioritet. Kao što jedan vodič fokusiran na OCD sugeriše, razumevanje sajber rizici I saznanje šta treba zaštititi su prvi koraci ka efektivnoj sigurnosti. Mogli biste ih čak uokviriti kao pitanja kao što je vodič Liberties': "Koja su naša najvažnija digitalna imovina? Ko bi ih mogao pokušati napasti I zašto? Šta bi se dogodilo da je X imovina prekršena ili nedostupna?" Dovedite svoj tim u ovo razmišljanje – različito osoblje moglo bi naglasiti različite zabrinutosti (npr. zabrinutost finansijskog službenika u vezi s vjerodajnicama za bankovne račune, zabrinutost službenika za komunikacije zbog hakovanja društvenih medija, itd.).

Razmotrite pravne i usklađene rizike: OCD takođe moraju razmišljati o propisima kao što su zakoni o zaštiti podataka. U EU, na primjer, GDPR zahtijeva od organizacija da zaštite lične podatke i prijave povrede. Dakle, jedan rizik od lošeg obezbjeđenja je pravno nepoštivanje i novčane kazne. Ako se vaš CSO bavi donatorima' ili korisnicima' ličnim podacima, kršenje bi moglo značiti kršenje zakona o privatnosti. Dakle, uključite usklađenost u razmišljanju o riziku – npr., "rizik od curenja ličnih podataka – utjecaj uključuje štetu pojedincima + zakonske kazne." Taj rizik bi očigledno bio veliki uticaj, a ako imate mnogo ličnih podataka, možda i srednje verovatnoće, koji opravdavaju jake kontrole.

Rizici dokumenata i ranga**:** Zapišite registar kratkog rizika – čak i jednostavnu tabelu scenarija rizika, vjerovatnoće, uticaja i trenutnih mjera. Rangirajte ih prema nivou rizika (neka kombinacija vjerovatnoće i utjecaja). Ovo će voditi gdje rasporediti resurse. Na primjer, možete rangirati "Phishing napad što dovodi do kompromisa računa" kao najvećeg rizika, dok bi "DDoS napad na web stranicu" mogao biti niži ako vaša stranica nije kontroverzna i ima zaštitu u oblaku. Ili "Insider koji slučajno curi podatke putem Google Drive link" može biti srednji rizik za rukovanje putem kontrole obuke i pristupa.

Apetit rizika: Takođe je dobro prepoznati to *nijedna organizacija ne može eliminirati svaki rizik*. Dio upravljanja rizikom je odlučivanje koji je nivo rizika prihvatljiv s obzirom na vaše resurse. Ovo se često naziva vašim "apetitom za rizikom." Mali OCD može prihvatiti rizik da nema IT sigurnosni tim 24/7 i umjesto toga se fokusirati na osnovnu odbranu i vanjsku podršku kada je to potrebno. Cilj je smanjiti rizike na nivo koji vam odgovara. Za visoke rizike implementirate jaka ublažavanja; za niže, možda bazičnije ili ih pratite tokom vremena.

Do kraja ove faze prepoznavanja rizika, trebali biste imati jasniju sliku o tome gdje se nalazite. Na primjer, možete zaključiti: *Naše najveće ranjivosti su phishing I slabe lozinke (visok rizik), plus zastarjeli softver na našoj web stranici (srednji rizik) i niska svijest među volonterima (doprinos rizicima). Imamo umjereni rizik od izgubljenih uređaja (ponekad dijelimo laptope), ali ako omogućimo enkripciju, to može propasti. Vjerovatno nismo posebno na meti nacionalnih država, ali rješavamo osjetljive informacije zajednice koje se moraju čuvati u tajnosti.* Ovi uvidi postavljaju teren za izradu vašeg sigurnosnog plana – u suštini, plan će se pozabaviti ovim identifikovanim rizicima odgovarajućim mjerama.

Znajući da vaša organizacija's digitalne slabe tačke i prijetnje koje će ih najvjerovatnije iskoristiti, možete efikasno planirati odbranu. Ovaj pristup je u skladu s konceptom donošenja odluka zasnovanog na riziku – osnovnim principom koji se preporučuje u okvirima kibernetičke sigurnosti. Osigurava da se fokusirate na ono što je najvažnije, umjesto da pokušavate sve raditi svuda. Sada, imajući na umu ovu sliku rizika,' nastavlja sa izgradnjom plana koji pokriva politike i prakse za ublažavanje ovih rizika.

Izgradnja jednostavnog plana digitalne sigurnosti

Sa vašim identifikovanim rizicima, sledeći korak je formulisanje plana za upravljanje i ublažavanje tih rizika. Plan digitalne sigurnosti za OCD obično uključuje politike, procedure i kontrole koje se bave glavnim područjima rizika, kao i obrise uloga i odgovornosti. Don't se ne zastrašuje terminom "plan" –, može biti jednostavan kao kontrolna lista ili kratki dokument. Ključno je da to bude praktično i prilagođeno vašoj organizaciji.

Sigurnosna politika i upravljanje: Počnite uspostavljanjem nekih vodičkih politika. Ovo može biti kratak odjeljak u kojem se navodi posvećenost organizacije digitalnoj sigurnosti i

osnovnim pravilima koja svi treba slijediti. Na primjer, imajte politiku lozinki (npr. zahtijeva jake lozinke određene dužine i 2FA na svim kritičnim računima – možete se odnositi na Odjeljak 2.1 za specifičnosti), politiku prihvatljive upotrebe (npr., smjernice o korištenju radnih uređaja i interneta u odgovarajuće svrhe, ne instaliranje neovlaštenog softvera, itd.) i Politika zaštite podataka (npr., pravila o rukovanju ličnim podacima, slijedeći zakonske zahtjeve kao što je GDPR i klasifikacija osjetljivosti na podatke). ENISA savjetuje da se jasne politike kibernetičke sigurnosti trebaju napisati i prenijeti zaposlenima, navodeći kako se od njih očekuje da se ponašaju s ICT resursima i koje posljedice postoje zbog nepoštivanja. Na primjer, vaša politika može reći da osoblje mora ne dijelite lozinke računa i morate odmah prijaviti svaki sumnjivi pokušaj krađe identiteta na IT žarišnu tačku.

Ako je vaš CSO mali, mogli biste ubaciti mnoge stvari u jedan opći politički dokument – koji se dobro manifestira. Važan dio je dodjela odgovornosti. Odlučite ko je u vašem timu zadužen za nadzor sigurnosti (mogao bi biti izvršni direktor ili službenik koji odgovara tehnologiji koji postaje "sigurnosna tačka osoba"). ENISA's SME vodič napominje da je dodjela odgovornosti za upravljanje za sajber sigurnost ključni element uspjeha. Dakle, eksplicitno nazovite ulogu: npr. Operativni menadžer će služiti kao službenik za sigurnost informacija, odgovoran za koordinaciju sigurnosnih napora i osiguravanje implementacije politika." Ako imate odbor ili rukovodstvo, pobrinite se da podrže ovaj plan – podrška liderstvu je ključna za kupovinu od svih.

Radnje upravljanja rizikom: Za svaki identifikovani veći rizik (od 3.1), ocrtajte šta ćete učiniti po tom pitanju. Ovo efektivno postaje srž vašeg plana:

- Na primjer, ako je "phishing" glavni rizik, vaš plan može uključivati radnje kao što su implementacija 2FA na e-pošti (već se raspravlja), provođenje obuke za podizanje svijesti o phishingu (vidi 3.3) i postavljanje procedura za provjeru neobičnih zahtjeva (kao što je finansijski proces potvrđivanja transakcije).
- Ako je "zastarjeli softver" bio rizik, vaš plan bi uključivao održavanje inventara ključnog softvera i rasporeda ili odgovornosti za ažuriranja (možda osoba sa sigurnosnom tačkom ili vanjska IT podrška osigurava ažuriranja mjesečno).

- Ako je identificirano “kršenje podataka o ličnom info” riziku: mjere plana kao što je ograničavanje pristupa tim podacima (samo određeni ljudi mogu pristupiti osjetljivim fasciklama), korištenje enkripcije za posebno osjetljive datoteke i postojanje procedure odgovora na incident (u slučaju da dođe do kršenja, kako zadržati i obavijestiti – više o tome u poglavlju 5).
- Ako “gubitak rizika od uređaja”: planirajte enkripciju punog diska i daljinsko brisanje kao što je spomenuto, plus možda dnevnik prijavljivanja/isključivanja uređaja za zajedničke uređaje.

Plan odgovora na incidente: Dobar plan, čak I jednostavan, predviđa da stvari mogu poći po zlu. Dakle, uključite osnovnu proceduru odgovora na incidente: ako dođe do incidenta s sajber sigurnošću (kao što je infekcija zlonamjernog softvera, sumnjivi hak, itd.), kome bi osoblje trebalo da se javi i kojim koracima ćete poduzeti? Poglavlje 5 to detaljno pokriva, ali u vašem planu, samo ocrtajte uloge: npr., “Svo osoblje mora odmah prijaviti svaki sumnjivi sigurnosni incident [Name/Role]. Izolirat ćemo pogođene računare iz mreže, procijeniti obim I kontaktirati [IT podršku ili vanjskog stručnjaka], ako je potrebno. Također ćemo obavijestiti rukovodstvo i, ako su lični podaci uključeni, pripremiti se da obavijestimo pogođene stranke i vlasti u skladu sa zakonom.” To što ste pisali znači da u žaru krize imate referencu da slijedite, što može uštedjeti dragocjeno vrijeme i smanjiti paniku.

Kontrole pristupa i upravljanje računom: Plan bi trebao definirati kako upravljate korisničkim nalozima i pristupom. Ovo može uključivati održavanje liste ko ima pristup sistemima, korištenje principa najmanje privilegije (dajte ljudima pristup samo onome što im je potrebno) i, što je važno, procedure za osoblje/dobrovoljce na brodu i van ukrcavanja. Na primjer, kada neko napusti organizaciju, vaš plan mora osigurati da njihovi računi budu odmah onemogućeni ili promijenjene lozinke. Mnogi sigurnosni incidenti se dešavaju jer bivši zaposleni ili partneri i dalje imaju aktivne akreditive. Uključuje korake kao što je “Po odlasku osoblja, IT će opozvati pristup e-pošti, cloud diskovima i svim zajedničkim lozinkama u roku od 24 sata.” Ako koristite zajedničke račune ili generičke prijave (pokušajte ih minimizirati), imajte plan da rutinski mijenjate te lozinke ili kada neko sa znanjem ode.

Upravljanje trećim stranama: Prepoznajte da vaša sigurnost također ovisi o bilo kojim uslugama treće strane ili izvođačima koje koristite. Ako ste identificirali "prodavaca" kao rizik (npr. vanjsku IT podršku ili provajdera u oblaku koji hostuje vašu bazu podataka), uključite mjere za upravljanje tim. ENISA's smjernice sugeriraju da se osigura da svi dobavljači koji imaju pristup osjetljivim podacima ispunjavaju sigurnosne zahtjeve i imaju ugovorne sporazume o sigurnosti. U jednostavnom planu, to bi moglo značiti provjeru da je svaka usluga u oblaku koju koristite renomirana i usklađena sa standardima zaštite podataka, te da imate sigurnosne kopije neovisne o njima ako je potrebno. Također, ako unajmite web programera ili IT konsultanta, osigurajte da potpišu sporazum o poštivanju vaših sigurnosnih politika (kao što je da ne koristite svoje akreditive negdje drugdje ili da podatke držite povjerljivim).

Osnovne kontrole implementacije: Rezimirajte konkretne kontrole koje ćete implementirati (neke se preklapaju sa savjetima iz poglavlja 2, ali ovdje ih formalizirate):

- **Sigurnost uređaja**: "All organizacioni laptopi će imati omogućen antivirusni i zaštitni zid, a uključen je i enkripcija punog diska (BitLocker/FileVault). Automatsko zaključavanje ekrana će biti postavljeno na 10 minuta neaktivnosti."
- **Sigurnost lozinki**: "Politika lozinke Enforce: najmanje 12 znakova, bez uobičajenih riječi, jedinstvenih po računu. Ohrabruje se upotreba upravitelja lozinki i biće postavljena za osoblje. 2FA će biti omogućena na kritičnim računima (e-pošta, finansijski sistemi, itd.)."
- **Podudaranje podataka**: "Kritični podaci (npr., baza podataka donatora, programske datoteke) će biti podržani sedmično kako bi se [osigurao oblak/šifrirani vanjski disk]. Odmarališta za testiranje će se provoditi kvartalno."
- **Sigurna konfiguracija**: "Osigurajte da se promijene zadane lozinke za svu opremu. Onemogući nepotrebne usluge na našoj web stranici i ažuriraj ih. Pregledajte privilegije korisnika periodično kako biste uklonili višak administrativnih prava."
- **Šifrovanje podataka u tranzitu**: "Koristi šifrirane kanale za osjetljive komunikacije (npr., Signal za povjerljive poruke ili PGP e-poštu za određene

kontakte što je izvodljivo). Naša web stranica ima SSL certifikat (HTTPS) i mi ćemo provesti njegovu upotrebu tako da su korisnički podnesci šifrirani."

Dok navodite kontrole, izbjegavajte jezik koji se smatra previše općim ili nemogućim za mjerenje ("We će spriječiti sve napade" – nerealnim). Umjesto toga, fokusirajte se na kontrole koje se mogu djelovati. Može pomoći da se koristi okvir kao kontrolna lista –, na primjer, CIS Controls (popularna lista osnovnih sajber praksi) ili ISO 27001 domeni za inspiraciju. Ali sve to prilagodite onome što možete implementirati.

Vremenski okvir i održavanje: Navedite koliko često će se sam plan revidirati i ko će ga održati. Tehnologija i prijetnje se razvijaju, pa možda, "Ovaj sigurnosni plan će biti revidiran i ažuriran svake godine (ili kad god dođe do velike promjene u našem IT-u) od strane [Role]." Također, kao što implementirate, možda nećete sve odjednom. U redu je dati prioritet akcijama u fazama. Vaš plan bi mogao imati odjeljak "Action Plan" gdje izlažete trenutne korake (npr., omogućite 2FA na e-pošti u roku od 1 mjeseca, zakažite obuku sljedećeg mjeseca, implementirajte sigurnosne kopije za Q3, itd.). Ovo to pretvara iz pravedne politike u projekat sa rokovima.

Komunikacija i provedba: Plan funkcionira samo ako ljudi znaju za to i on se provodi. Nakon izrade, podijelite ga sa svim osobljem i volonterima. Možda održite kratak sastanak kako biste objasnili ključne tačke ("we sada imamo politiku, ovdje se potvrđuje šta to znači za vaš svakodnevni rad"). Dobijte povratne informacije – možda neko vidi prazninu ili ima prijedlog. Uključite u plan ili prateće materijale posljedice za nepoštivanje na prijateljski način – npr., "Ako se politike ne poštuju, to može rezultirati disciplinskim mjerama, ali imamo za cilj da podržimo sve u postizanju ovih najboljih praksi kroz obuku i resurse." Ovo daje ton da je sigurnost dio posla svih koji podržavaju, a ne samo IT stvar. Dobra analogija Instituta CyberPeace: tretirati sajber sigurnost ne kao izolirani IT trošak već kao **enabler** za tvoju misiju. Ugrađivanjem sigurnosti u svakodnevne procese, osiguravate kontinuitet i povjerenje u svoje operacije.

Da biste ilustrirali, zamislite mali odlomak iz sigurnosnog plana CSO's za okoliš:

- **Rizik**: Phishing e-pošte osoblja – **Ublažavanje**: obavezan 2FA za e-poštu, obuka o prepoznavanju phishinga (predvođen IT volonterom) i kreiranje protokola za izvještavanje za sumnjive e-poruke.

- **Rizik**: Gubitak prijenosnih računala na terenu – **Ublažavanje**: omogućeno šifriranje cijelog diska, svakodnevno sinhroniziranje podataka u oblak kada je internet dostupan, zaključavanje koda uređaja na mjestu.
- **Rizik**: Oštećenje web stranice – **Ublažavanje**: redovna ažuriranja od strane web hosta, korištenje sigurnosnog dodatka ili usluge, sigurnosne kopije sadržaja stranice, planiraju brzo obnoviti ako su hakirani.
- **Politika**: Svi novi volonteri moraju dobiti osnovnu sigurnosnu orijentaciju i potpisati ugovor o korištenju IKT-a (koji pokriva ne dijeljenje računa, itd.).
- **Odgovornost**: Dodijeljena Jane Doe (program menadžer) kao koordinatorica sigurnosti za praćenje i vođenje ovih akcija.

Preslikavanjem akcija na rizike I dodjeljivanjem ko šta radi, vaš plan postaje djelotvoran. Možda će biti duga samo nekoliko stranica, ali to je u redu. Brevitacija može biti moćna ako se jasno ukaže. U stvari, ENISA's SME vodič destiluje savjete u 12 koraka visokog nivoa koji služe kao mini-plan za preduzeća (stvari poput "Develop dobre kulture sajber sigurnosti – dodjeljuju odgovornost," "plan za incidente," i "Secure rezervne kopije"). Mnogi od njih se ovdje ogledaju. Završni dio planiranja je implementacija tih mjera I podsticanje svijesti, što nas vodi do sljedećeg dijela. Održavajte svoj nacrt plana korisnim dok razgovaramo o obuci i kulturi, budući da to često ukazuje na jednu od komponenti plana.

Obuka za podizanje svijesti za osoblje i volontere

Čak i najbolji sigurnosni plan na papiru može propasti ako ljudi u organizaciji budu na brodu ili upućeni. Ljudsko ponašanje je kritičan faktor u digitalnoj sigurnosti – kao što je ranije navedeno, značajna većina kršenja uključuje ljudski element (greške ili društveni inženjering). Stoga je edukacija vašeg tima i izgradnja kulture sigurnosne svijesti jedna od najutjecajnijih stvari koje možete učiniti. Zamislite svoje osoblje i volontere kao prvu liniju odbrane (ili obrnuto, najslabiju vezu ako niste obučeni). Ovaj odjeljak opisuje kako stvoriti i održati efikasnu obuku o svijesti o sigurnosti u kontekstu OCD.

Počnite sa osnovama: Obuka ne mora biti previše tehnička. U stvari, često se bolje fokusira na osnovne do's i don'ts, pravi primjeri i interaktivna diskusija. Pokrijte uobičajene prijetnje na

načine na koje se ljudi mogu povezati. Na primjer, pokažite kako izgleda phishing e-mail (možda pokažite stvarnu phishing e-poštu koju dezinficirate za obuku) i natjerajte ljude da ističu crvene zastavice (loša gramatika, adresa čudnog pošiljaoca, neočekivana vezanost, itd.). Razgovarajte o scenariju: "Ako dobijete e-mail od direktora u kojem tražite hitan transfer novca, šta biste trebali učiniti?" (Odgovor: uvijek provjerite telefonskim pozivom ili licem u lice prije nego što djelujete, jer bi to mogla biti prevara prijevara izvršnog direktora). Ove praktične vježbe pomažu osoblju da shvati kako bi se napad mogao odigrati i kako mirno odgovoriti. ENISA preporučuje da se fokus treninga fokusira na **situacije iz stvarnog života** to MSP lice, što se odnosi i na OCD. Odrasli učenici često bolje razumiju koncepte kroz scenarije i priče nego kroz apstraktna pravila.

Ključne teme koje uključuju: U najmanju ruku, obratite se temama iz poglavlja 2 u obrascu za obuku:

- Sigurna praksa lozinki i korištenje upravitelja lozinki.
- Kako omogućiti i koristiti 2FA (možda live demo postavljanja aplikacije za autentifikaciju).
- Prepoznavanje phishing e-poruka, sumnjivih veza i šta učiniti (nemoj se kliknuti, prijaviti).
- Pravilno rukovanje osjetljivim informacijama (npr., korištenje šifriranih alata za povjerljive podatke, ne korištenje lične e-pošte za radni sadržaj, itd.).
- Sigurnost uređaja: važnost ažuriranja, neugradnja neovlaštenih aplikacija, zaključavanje ekrana i oprez s USB diskovima (nepoznati USB štapići mogu biti opasni).
- Upozorenje na društvenim mrežama: ne dijeljenje informacija osjetljivih na posao na Facebooku/Twitteru, paziti na društveni inženjering (kao što neko zove pretvarajući se da je IT podrška).
- Incidenti izvještavanja: naglasite kulturu bez krivice. Ljudi bi se trebali osjećati ugodno izvještavati ako su kliknuli na nešto loše ili izgubili uređaj, umjesto da ga kriju. Jasno stavite do znanja da je brzo izvještavanje ključno i da neće biti kažnjeni za iskrenu grešku – prioritet je riješiti problem.

Interaktivna i OCSO-ing obuka: Svjesnost nije jednokratni događaj. Planirajte da imate sesije osvježavanja ili barem periodične podsjetnike. Mnoge organizacije rade godišnju sigurnosnu obuku. Ali između toga, možete podijeliti savjete na sastancima osoblja ili poslati "sigurnosni savjet mjesečne e-pošte. Na primjer, u oktobru (Mjesec svijesti o kibernetičkoj sigurnosti, koji ENISA često promovira u EU), možete održati zabavan kviz ili podijeliti kratki video o sigurnosti. Obuka ne mora biti suva. Neki OCD pozivaju stručnjaka za sigurnost ili koriste besplatne online module (postoje mnogi besplatni kursevi podizanja svijesti o sajber sigurnosti i video snimci usmjereni na neprofitne organizacije i mala preduzeća).

Razmislite i o korištenju vanjskih resursa: ako imate IT partnera ili ako se osnuje lokalni tehnološki univerzitet, ponekad oni mogu pomoći u davanju radionice. Postoje i neprofitne inicijative koje nude besplatne radionice cyber svijesti civilnom društvu (na primjer, organizacije kao što su TechSoup ili CyberPeace Builders volonteri mogu pomoći u održavanju obuka).

Poseban fokus za ključne uloge: Krojački dijelovi treninga do uloga. Vašem finansijskom službeniku će možda trebati dublja obuka o uočavanju prijevare s fakturama ili osiguravanju bankarskih prijava (jer su CSO prevareni putem lažnih faktura ili "imitacija izvršnog direktora" e-poruke da šalju novac prevarantima). Vaše komunikacijsko osoblje koje se bavi društvenim mrežama možda će trebati savjete o izbjegavanju preuzimanja računa (kao što je korištenje 2FA i opreznost prema phishing DM-ovima). Liderstvo bi također trebalo razumjeti svoju ulogu – rukovodioci su često mete krađe identiteta (trik e-pošte "boss"), tako da bi trebali dobro ponašanje modela (kao da nikada ne tražite osjetljive informacije ili transfere samo e-poštom bez verifikacije). Također, osigurajte da volonteri ili kratkoročno osoblje dobiju barem mini ukrcavanje u obezbjeđenje, jer možda neće pohađati formalnu obuku osoblja. Lista za varanje na jednoj stranici ili brzi brifing o "do's i don'ts" kada se pridruže mogu pomoći.

Stvaranje kulture ispitivanja: Ohrabrite sve da se ispovijeda u redu da dovode u pitanje stvari koje izgledaju off. Na primjer, ako volonter dobije neobičnu IT instrukciju za koju ne vjeruju da nije siguran, treba da pitaju. Pobrinite se da znaju koga da pitaju – eg., "Ako primate bilo kakvu sumnjivu komunikaciju ili niste sigurni u datoteku ili vezu, kontaktirajte našu IT žarišnu tačku (ili koordinatora sigurnosti) u [kontaktu]." Ovo seže do Microsoftovih savjeta: sajber sigurnost je a *timski sport*, i ako nešto vidite, recite nešto savjetniku od povjerenja. Ako neko misli da je

možda napravio sigurnosnu grešku, kao što je klik na lošu vezu, trebao bi se osjećati sigurno da to odmah prijavi umjesto da se boji krivice. Brza reakcija često može spriječiti ili minimizirati štetu (kao što je isključivanje računara ako se sumnja na zlonamjerni softver).

Mjerenje i jačanje: Pomaže da se procijeni koliko dobro vaša obuka radi. Jedan od načina je provođenje internih phishing testova (ako resursi dozvoljavaju): poslati bezopasnu "lažnu phishing" e-poštu osoblju nakon treninga da vidi ko klikne. Oni koji to urade mogu dobiti nježan trening praćenja. Ali ako ste vrlo mala organizacija, neformalni Q&A i diskusije bi mogle biti dovoljne da osjetite razumijevanje. Čak i pitajući na sastanku osoblja, "Šta biste uradili ako dobijete prilog e-pošte od nekoga koga ne poznajete?" a odgovori sluha mogu otkriti razumijevanje. Pojačajte poruke objavljivanjem kratke liste sigurnosnih savjeta na oglasnoj tabli ili Slack kanalu. Neke organizacije čak uključuju sigurnost u preglede ili rutine učinka osoblja ("Did da li ste završili godišnji sigurnosni kviz?"), ali u OCD-ovima je lakši pristup često dovoljan osim ako se ne pridržavate izuzetno osjetljivih podataka.

Ostanite informisani i podijelite ažuriranja: Pejzaž prijetnje se mijenja. Ako postanete svjesni nove relevantne prijetnje, ažurirajte svoj tim. Na primjer, ako kolega iz OCD-a prijavi phishing kampanju usmjerenu na organizacije u vašem sektoru, upozorite svoje osoblje: "Heads-up, postoji phishing e-mail koji se kreće okolo i tvrdi da je iz finansijera – ne kliknite ni na jednu takvu e-poštu i obavijestite nas ako ga primite." Biti dio CSO mreža ili sigurnosnih grupa za razmjenu informacija (kao što ćemo vidjeti Poglavlje 6) može pružiti takve informacije koje možete prenijeti. Ovo održava sigurnosnu svijest aktuelnom i pokazuje osoblju da su prijetnje stvarne i da se dešavaju u njihovoj okolini, a ne samo teorijske.

Da rezimiramo, obuka za podizanje svijesti pretvara vaše ljude iz potencijalnih obaveza u imovinu u vašem sigurnosnom položaju. Kako kaže jedan slogan kibernetičke sigurnosti, "Vaši zaposleni su vaš najbolji zaštitni zid." Podsticanjem znanja i budnim načinom razmišljanja, uvelike smanjujete šanse za skupu grešku. Zapamtite, sama tehnologija nije dovoljna – čak se i najjači zaštitni zid može zaobići ako korisnik nesvjesno pusti napadača unutra. Ali dobro obučen tim, podržan pozitivnom sigurnosnom kulturom, može zaustaviti mnoge incidente prije nego što počnu ili ih uhvatiti ranije. Ovo osnaživanje ljudskih faktora je u središtu otporne digitalne sigurnosti civilnog društva.

Zaštita vaših podataka: rezervna i sigurna pohrana

Podaci se često opisuju kao “lifeblood” organizacija. Za OCD, podaci mogu uključivati informacije o korisnicima, nalaze istraživanja, detalje o donatorima, finansijsku evidenciju, izvještaje o projektima, fotografije i još mnogo toga. Zaštita ovih podataka nije samo sprečavanje neovlašćenog pristupa (povjerljivosti), već i osiguravanje da se on ne izgubi (dostupnost) i da se ne mijenja nepropisno (integritet). U ovom odjeljku fokusiramo se na dva osnovna aspekta zaštite podataka: redovne sigurnosne kopije i sigurno skladištenje (fizički i u oblaku).

Važnost rezervnih kopija: Zamislite najgore scenarije – napad ransomware-a šifrira sve vaše datoteke, ili vatra/poplava uništava vaše kancelarijske kompjutere, ili pripravnik slučajno briše ključnu fasciklu. U svakom od ovih slučajeva, nedavna rezerva može bukvalno spasiti vašu organizaciju. Rezervna kopija je zasebna kopija vaših podataka koja se čuva na drugom mediju (i po mogućnosti na drugoj lokaciji) iz kojeg možete vratiti ako je potrebno. Bez rezervnih kopija, bilo koji od gore navedenih scenarija mogao bi značiti nepovratan gubitak. Sa rezervnim kopijama, imate sigurnosnu mrežu.

Evo najboljih praksi rezervnih kopija, od kojih su mnoge u skladu sa standardnim savjetima:

Redovna frekvencija: Redovno podržavate svoje važne podatke. “Regularly” ovisi o tome koliko se često podaci mijenjaju i koliko su kritični. Za prilično statične podatke, sedmično bi moglo biti dovoljno; za podatke koji se brzo mijenjaju (kao što su dnevni dnevni zapisi programa ili aktivne baze podataka), dnevno ili čak više puta dnevno može biti bolje. Odredite svoj cilj tačke oporavka (RPO): koliko podataka možemo priuštiti da izgubimo? Ako se ispovijeda dan koji vrijedi, onda su dnevne sigurnosne kopije u redu. Ako bi gubitak čak jednog sata podataka bio katastrofalan, imajte za cilj češće snimke.

Automatiziraj: Ljudski zavisni rezervni procesi često ne uspijevaju zbog zaborava ili zauzetosti. Koristi automatska rezervna rješenja kada je to moguće. Na primjer, postavite svoj server datoteka ili NAS da se svake večeri vraća na eksterni disk u 2 sata ujutro Ili koristite usluge sigurnosne kopije u oblaku (kao što su Backblaze, Acronis, itd.) koje rade kontinuirano ili po rasporedu. Mnoge usluge pohrane u oblaku, kao što su Google Drive ili OneDrive, također

čuvaju prethodne verzije datoteka, koje mogu poslužiti kao oblik sigurnosne kopije za uređivanje datoteka ili brisanje.

Više kopija i van lokacije: Pratite nešto poput pravila 3-2-1: 3 kopije podataka (primarni + dvije rezervne kopije), na 2 različita medija, od kojih je 1 izvan lokacije. Ovo bi moglo biti pretjerano za vrlo mali OCD, ali ideja je zdrava. Možete, na primjer, imati jednu rezervnu kopiju na vanjskom tvrdom disku u kancelariji i drugu šifriranu rezervnu kopiju u cloud servisu. Van lokacije znači da ako kancelarija izgori, rezervna kopija van lokacije (ili oblaka) je sigurna. Cloud rezervne kopije su inherentno izvan lokacije. Ako koristite fizičke medije, razmislite o pohranjivanju vožnje u kući člana odbora's ili sef, povremeno je ažurirajući.

Osigurajte svoje sigurnosne kopije: Rezervna kopija je kopija vaših osjetljivih podataka, zato je zaštitite. Ako koristite eksterni disk, šifrirajte taj pogon (mnogi rezervni alati ili OS poput Windows BitLocker mogu šifrirati eksterne diskove). Ako koristite sigurnosnu kopiju u oblaku, osigurajte da usluga šifrira podatke (većina ih šifrira, ali možete odabrati i šifrirati datoteke prije učitavanja radi dodatne sigurnosti). Ograničite ko može pristupiti rezervnim kopijama. Na primjer, don't ostavlja rezervni disk stalno priključen na sistem koji osmišljava online – ako ga pogodi ransomware, mogao bi i to šifrirati. U idealnom slučaju, sigurnosne kopije koje nisu stalno povezane (offline sigurnosne kopije) su imune na zlonamjerni softver u vašoj mreži. Ako koristite mrežni pogon za sigurnosne kopije, osigurajte da ima verziju ili neku zaštitu koju malware može't može odmah pokvariti stare sigurnosne kopije.

Test Restauratori: Rezervne kopije malo znače ako ne priznaju da rade kada je to potrebno. Najmanje nekoliko puta godišnje testirajte proces obnove. Pokušajte povratiti datoteku iz sigurnosne kopije i vidjeti da li se otvara ispravno. Radite vatrogasnu vježbu: "Šta ako je naš glavni zajednički pogon umro – možemo li sinoć lako vratiti rezervnu kopiju na novi uređaj?" Testiranje će otkriti sve probleme kao što su oštećena rezervna kopija, nedostajući ključevi za šifriranje ili procedure koje treba poboljšati. Mnoge organizacije su u krizi otkrile da su njihove rezervne kopije bile nepotpune ili da su tiho propale davno – don't je dozvolio da se to dogodi vama.

Procedure za rezervnu kopiju dokumenta: Zapiši šta je potkrijepljeno, kako I gdje. Također imajte na umu ko je odgovoran za nadgledanje rezervnih kopija i kako izvršiti oporavak.

Na primjer: “Naša baza podataka donatora Salesforce je podržana vlastitim dnevnim izvozom Salesforce’s i dodatno ručnim izvozom Johna 1. mjeseca na šifrovani USB disk.” Ako John ode, neko drugi to može pročitati i nastaviti praksu. Takođe, dokumentirani akreditivi potrebni za sigurnosne kopije (sigurno, naravno), tako da se ne trudite da pronađete lozinku tokom hitne obnove.

Sigurna kontrola skladištenja i pristupa: Osim rezervnih kopija, zaštita podataka također znači sigurno čuvanje u svakodnevnoj upotrebi. Ovo uključuje i fizičku memoriju (kao što su štampane datoteke, USB diskovi i serveri) i rješenja za pohranu u oblaku:

Fizičke datoteke i uređaji: Ako imate osjetljive informacije u fizičkom obliku (papirni dokumenti, USB štapići, vanjski tvrdi diskovi), pohranite ih u zaključane ormare ili sef. Don’t ostavlja dokumente sa ličnim podacima koji leže na stolovima. Na primjer, volonterske registracijske listove ili obrasce korisnika treba odnijeti kada se ne koriste aktivno. Podijeljeni osjetljivi dokumenti prije odlaganja. Za uređaje, kao što je objašnjeno, koristite enkripciju punog diska tako da ako se računar ili disk izgubi, podacima se ne pristupa lako. Zadržite inventar uređaja – zna ko ima koji laptop ili telefon. Ako uređaj sadrži osjetljive podatke, razmotrite politike da se ne ostavlja na nesigurnim mjestima (npr., zaključan u kancelarijskoj ladici ili odveden kući od strane osoblja i čuvan). Tokom putovanja, možda koristite filtere ekrana za privatnost i držite uređaje kod sebe (ne možete provjeriti laptope u prtljagu ako je moguće).

Cloud Storage (Google Drive, Dropbox, itd.): Cloud usluge su vrlo zgodne i imaju ugrađenu redundantnost, ali ih morate pravilno konfigurirati radi sigurnosti. Prvo, omogućite 2FA na računima u oblaku da spriječi neovlaštene prijave. Drugo, pažljivo upravljajte dijeljenjem dozvola. Umjesto da otvoreno podijelite cijelu vožnju, podijelite fascikle/dosije samo sa određenim ljudima kojima je potreban pristup. Povremeno pregledajte ko ima pristup onome što je u vašem Google Driveu ili Dropbox – uklanja svakoga kome više nije potreban (uključujući eksterne saradnike čiji su projekti okončani). Budite oprezni sa “udjelom putem link” funkcija; ako kreirate javnu vezu do datoteke, teoretski, svako ko pronađe tu vezu može joj pristupiti (neki sistemi sada nude veze zaštićene lozinkom ili veze koje ističu; koristite ih ako je potrebno). Za visoko osjetljive datoteke, razmislite o korištenju enkripcija na strani klijenta prije učitavanja

(neki alati se integrišu sa Dropbox/Google Drive kako bi šifrirali datoteke lokalno tako da čak i ako neko hakuje vaš račun u oblaku, vidi besprekorno bez vašeg ključa).

ENISA's smernice o oblaku za mala i srednja preduzeća odražavaju ove tačke: razumejte jedinstvene rizike oblaka i osigurajte da odaberete ugledne provajdere. Oni posebno primjećuju da se osigura korištenje provajdera koji se zalažu za kršenje zakona u vezi sa podacima (poput GDPR ograničenja za pohranjivanje ličnih podataka izvan EU bez zaštitnih mjera). Na primjer, ako vaš CSO posluje u EU i pohranjuje lične podatke, trebali biste provjeriti gdje vaš provajder u oblaku pohranjuje podatke i eventualno potpisati Ugovore o obradi podataka. Ako koristite usluge kao što su Dropbox ili Google, pogledajte njihovu usklađenost i možda se odlučite za one sa serverima u regijama u kojima vjerujete ili koristite evropsku alternativu ako je potrebno.

Šifrovanje u tranzitu i u mirovanju: Osigurajte da podaci budu šifrirani ne samo na diskovima već i prilikom prijenosa. Većina provajdera u oblaku radi šifrirane podatke u mirovanju na svojim serverima i koristi HTTPS za transfere, što je dobro. Ako sami hostujete bilo kakve podatke (kao što je NAS na licu mjesta dostupan preko interneta), postavite VPN ili barem osigurajte da su web veze iznad HTTPS-a. Također, za izuzetno osjetljive informacije, možete slojevito šifrirati –, na primjer, šifrirati dokument lozinkom prije učitavanja čak i na šifrirani fascikl u oblaku (dvostruka enkripcija). Ovo bi moglo biti relevantno za, recimo, liste aktivista u neprijateljskoj regiji.

Segmentacija podataka: Ne bi svi u OCD trebali automatski imati pristup svim podacima. Koristite kontrole pristupa podacima o segmentima. Na primjer, HR dosijei ili medicinske informacije osoblja mogu biti ograničene samo na osoblje HR-a. Finansijska evidencija je samo za finansiranje tima. Projektne datoteke samo onima na tom projektu, itd. Mnoge platforme u oblaku dozvoljavaju nivoe dozvole i pristup zasnovan na grupi. Na ovaj način, ako je jedan korisnički račun kompromitovan, napadač ne priznaje nužno da dobije sve, samo ono čemu bi taj korisnik mogao pristupiti. Također smanjuje rizik interne zloupotrebe – ljudi ne mogu njuškati o podacima koji nisu povezani s njihovom ulogom.

Plan za zadržavanje i uništavanje podataka: Dio sigurne memorije nije čuvanje podataka duže nego što je potrebno. Stare čvrste diskove sa zamenjenih računara treba bezbedno obrisati ili uništiti (jednostavno brisanje datoteka nije dovoljno; koristite softver za

prepisivanje ili fizički uništavanje diska). Isto je I za USB štapiće koji se više ne koriste. Ako vaš CSO akumulira decenije ličnih podataka bez potrebe, razmislite o politici arhiviranja ili brisanja starih zapisa. Ovo smanjuje količina osjetljivih informacija koje bi mogle biti izložene u kršenju i usklađene su s principima zakona o zaštiti podataka (minimizirajte zadržavanje podataka). Na primjer, ako ste vodili obuku prije pet godina i još uvijek imate lične kopije učesnika, odlučite da li vam je to zaista potrebno sada.

Redundantnost i poslovni kontinuitet: Rezervne kopije osiguravaju kontinuitet podataka, ali razmišljaju i o operativnom kontinuitetu. Ako se vaš uredski server sruši, sigurnosna kopija podataka je prvi korak, ali drugi korak je vraćanje funkcionalnosti. Vaš plan može uključivati rezervni uređaj ili kvar u oblaku. Za mnoge male OCD, rad od usluga u oblaku za kritične funkcije (e-pošta, dokumenti, itd.) inherentno pruža kontinuitet – možete nastaviti raditi s bilo kojeg mjesta na drugom uređaju ako neko ne uspije. Ali identificirajte bilo koju tačku neuspjeha. Ako samo jedna osoba zna kako pristupiti rezervnim kopijama, to je rizik – unakrsnog treniranja nekog drugog ili ga dokumentirati, kao što je spomenuto.

Primjer implementacije: Pretpostavimo da vaš CSO ima zajednički disk na NAS uređaju u kancelariji za sve projektne datoteke. Uvodite noćnu rezervnu kopiju tog NAS-a na šifrovani eksterni HDD koji vaš direktor nosi kući vikendom (u redu). Osim toga, kritični podfameri se sinkroniziraju na siguran oblak (kao što je Google Drive ili Nextcloud) u realnom vremenu radi saradnje i sigurnosti izvan lokacije. Zakazujete sigurnosne kopije svoje baze podataka donatora iz svog CRM-a i preuzimate kopiju mjesečno, koju šifrirate i pohranjujete u oblaku. Za fizičke datoteke kao što su potpisani obrasci za pristanak korisnika, skenirate ih i učitavate (tako da su potvrđeni podržani) i držite originale u zaključanom ormariću. Za sve laptope osigurate da je BitLocker uključen i svaki ima BIOS/firmware lozinku tako da lopovi mogu lako pokrenuti s USB-a kako bi zaobišli enkripciju. Jednom u četvrtini, simulirate scenario gubitka podataka kako biste osigurali da se možete vratiti iz svojih rezervnih kopija.

Radeći sve ovo, postižete otpornost: čak i ako sajber katastrofa udari ili hardver ne uspije, vaši podaci su sigurni i možete nastaviti rad uz minimalne smetnje. CyberPeace Institute je istakao da neprofitne organizacije treba da vide sajber sigurnost (i šire, mjere zaštite podataka) kao da im omogućavaju da bezbedno iskoriste tehnologiju za društveni uticaj. Sigurni podaci i

sigurnosne kopije znače da možete prihvatiti digitalne alate bez stalnog straha od gubitka kritičnih informacija.

U zaključku, sigurnosne kopije i sigurno skladištenje su poput pojasa i vazdušnih jastuka vaše digitalne operacije –, nadate se da ih nikada nećete trebati u hitnim slučajevima, ali ako to učinite, mogu spasiti vašu organizaciju od katastrofalnih gubitaka. Kombinirajte to s proaktivnim mjerama iz ranijih odjeljaka (kao što su higijena lozinki i kontrole pristupa) i kreirate snažan štit za svoje CSO's informaciona sredstva. Zatim ćemo istražiti neke od alata koji se lako koriste koji mogu dodatno ojačati vašu sigurnost u praksi, dopunjujući plan i politike koje smo uspostavili.

Sažetak poglavlja

Ovo poglavlje nudi praktične smjernice za OCD-ove za osiguranje komunikacija i osjetljivih podataka, kritičnih za svakodnevne operacije i povjerenje. Pokriva enkripciju za e-poštu, razmjenu poruka i pohranu podataka, preporučujući alate kao što su Signal za sigurne razgovore i HTTPS za web promet. Naglašene su jake kontrole pristupa, kao što su robusne lozinke i 2FA, kako bi se spriječio neovlašteni pristup nalozima kao što su e-pošta ili platforme u oblaku (npr. Google Drive). Poglavlje zagovara redovne sigurnosne kopije kako bi se osigurale lokacije (npr. šifrirani diskovi) za oporavak od ransomware-a ili gubitka podataka, navodeći slučaj u kojem su sigurnosne kopije spasile CSO od napada ransomware-a. Sigurne metode dijeljenja datoteka, poput šifriranih usluga u oblaku, istaknute su kako bi se zaštitili podaci korisnika. Poglavlje se bavi usklađenošću sa GDPR-om, naglašavajući zakonito rukovanje podacima i pristanak. Uključuje korake koji se mogu djelovati, kao što je omogućavanje 2FA na Gmailu ili korištenje besplatnih alata za šifriranje, čineći ga dostupnim za netehničko osoblje. Primjeri, poput hakovanja putem e-pošte od strane dobrotvorne organizacije putem phishinga, naglašavaju potrebu za budnošću. Poglavlje također pokriva sigurne video konferencije i prakse društvenih medija, osiguravajući da OCD mogu bezbedno komunicirati u udaljenim ili visokorizičnim okruženjima. Sprovođenjem ovih mjera, OCD čuvaju osjetljive informacije, održavaju operativni kontinuitet i grade povjerenje donatora.

Cybersecurity Planirajte Godišnju listu za pregled i ažuriranje za OCD

Ova kontrolna lista osigurava da vaš CSO's plan kibernetičke sigurnosti ostane aktuelan i efikasan razmatranjem imovine, prijetnji, politika i strategija odgovora na incidente godišnje ili nakon značajnih promjena (npr. novih sistema, fluktuacije osoblja). Završavanje ovih koraka održava snažan digitalni sigurnosni stav kako bi se zaštitila vaša misija i dionici:

1. Pregled i ažuriranje digitalnih sredstava

☐ Identificirajte novu ili promijenjenu digitalnu imovinu (npr., novu bazu podataka donatora, pohranu u oblaku, naloge društvenih medija) dodanu od posljednje recenzije.

☐ Uklonite zastarjelu imovinu (npr. ukinuti softver, stare račune e-pošte) iz plana.

☐ Primjer: Dodano je novi CRM sistem za upravljanje donatorima? Uključite ga u procjenu rizika. Ušao u staru bazu podataka volontera? Izvadi ga iz plana.

2. Procjenite nove prijetnje ili prijetnje koje se razvijaju

☐ Pregledajte nedavne trendove kibernetičke sigurnosti ili prijetnje relevantne za OCD (npr., povećani phishing, ransomware ili lokalni nadzorni rizici).

☐ Konsultujte lokalne resurse (npr., nacionalni CERT, OCD mreže) ili globalne izvještaje (npr. Microsoft's CSO statistiku napada) za ažuriranja.

☐ Ažurirajte predložak procjene rizika kako biste odražavali nove prijetnje ili promjene vjerovatnoće/utjecaj.

☐ Primjer: Primijećeno povećanje phishing e-poruka usmjerenih na OCD u vašoj regiji? Povećajte rezultat vjerovatnoće za phishing u procjeni rizika.

3. Pregledajte nedavne incidente ili bliske promašaje

☐ Dokumentirajte sve incidente kibernetičke sigurnosti ili skoro promašaje (npr. phishing pokušaji, upozorenja na zlonamjerni softver) od posljednjeg pregleda.

☐ Analizirajte šta je prošlo dobro i šta nije uspjelo u vašem odgovoru (npr., jesu li rezervne kopije radile? Da li je incident odmah prijavljen?).

☐ Ažurirajte plan sa naučenim lekcijama za poboljšanje budućih odgovora.

☐ Primjer: Član osoblja kliknuo je na phishing vezu, ali je 2FA spriječio pristup. Dodajte napomenu za pojačanje 2FA obuke i ažuriranje filtera e-pošte.

4. Procedure o odgovoru na incidente ažuriranja

☐ Provjerite da plan odgovora na incident uključuje trenutne korake, uloge i odgovornosti (npr., koji otkriva, sadrži, komunicira).

☐ Liste za kontakt ažuriranja za interne odgovore (npr., IT osoblje, rukovodstvo) i eksternu podršku (npr., lokalni CERT, pravni savjetnik).

☐ Testirajte plan vježbom na stolu (npr. simulirajte napad ransomware-a) kako biste identificirali praznine.

☐ Primjer: Novi IT menadžer? Ažurirajte njihovu ulogu voditelja odgovora na incident. Stari kontakt sa CERT-om zastario? Zamijenite trenutne detalje.

5. Provjerite sigurnosne politike i usklađenost

☐ Pregledajte i ažurirajte sigurnosne politike (npr. prihvatljiva upotreba, zaštita podataka, BYOD) kako biste odražavali nove alate, propise ili prakse.

☐ Potvrdite usklađenost sa zakonima o zaštiti podataka (npr., GDPR, lokalnim propisima) i procedurama ažuriranja ako je potrebno (npr., obrasci za pristanak, izvještavanje o kršenju).

☐ Primjer: GDPR zahtijeva obavještenje o kršenju u roku od 72 sata. Osigurajte da vaša politika uključuje ovaj vremenski okvir i određeni kontakt za izvještavanje.

6. Provjeri tehničke protekcije

☐ Revizijske sigurnosne mjere (npr. 2FA, antivirusni, rezervne kopije, enkripcija) kako bi se osiguralo da su aktivne i ažurirane na svim uređajima i računima.

☐ Provjerite nove sigurnosne funkcije u alatima (npr. platforme u oblaku, provajderi e-pošte) i omogućite ih ako je primjenjivo.

☐ Primjer: Google Workspace je dodao novu sigurnosnu funkciju za zajedničke diskove? Omogućite to i ažurirajte kontrole pristupa.

7. Plan obuka osoblja i svijest

☐ Postavite obuku o sajber sigurnosti ili osvježenje (npr., svijest o phishingu, upravljanje lozinkom) za svo osoblje i volontere.

☐ Uključite nove teme zasnovane na nedavnim prijetnjama ili incidentima (npr., phishing vođen umjetnom inteligencijom, sigurnost oblaka).

☐ Primjer: Nakon lokalnog naleta ransomware-a, dodajte 30-minutnu sesiju o prepoznavanju znakova upozorenja ransomware-a.

8. Zakup testiranja i oporavak

☐ Provjerite da li rezervne kopije rade po planu i sigurno se pohranjuju (npr. šifrirani oblak ili vanjski disk).

☐ Provedite test vraćanja rezervne kopije kako biste osigurali da se podaci mogu brzo i precizno povratiti.

☐ Primjer: Vratite uzorak datoteke iz prošlomjesečne rezervne kopije kako biste potvrdili da je' dostupan i netaknut.

9. Angažirajte Liderstvo i zainteresovane strane

☐ Kratko vodstvo u ažuriranom planu i svim potrebama resursa (npr., budžet za nove alate, vrijeme za obuku).

☐ Podijelite ključna ažuriranja sa dionicima (npr. donatorima, partnerima) kako biste ojačali povjerenje u svoje sigurnosne prakse.

☐ Primjer: Obavijestite donatore da ste potvrdili ojačanu zaštitu podataka kako biste bili u skladu sa GDPR-om, poboljšavajući transparentnost.

10. Dokument i Prilog Sljedeća recenzija

☐ Zabilježite sva ažuriranja u planu kibernetičke sigurnosti i pohranite ga na sigurnu, pristupačnu lokaciju (npr. šifrirani zajednički disk).

☐ Zakažite sljedeći godišnji pregled ili pokrenite pregled nakon velikih promjena (npr. novi softver, kancelarijski potez).

☐ Primjer: Postavite godišnji podsjetnik kalendara da ponovite ovaj proces.

2.4 POGLAVLJE 4: KORISNIČKI SIGURNOSNI ALATI

Korisnik-prijateljski sigurnosni alati

Do sada smo se izjasnili o praksama i planiranju. U ovom poglavlju fokusiramo se na alate i tehnologije koje mogu olakšati implementaciju sigurnosti. Dobra vijest je da ne't ne morate biti tehnološki čarobnjak ili ulagati u vrlo skupa rješenja kako biste dobili solidan nivo zaštite. Ima ih mnogo **korisnički prilagođeni, isplativi alati** dostupan – često dizajniran imajući na umu neprofitne organizacije ili mala preduzeća – koji može značajno poboljšati vašu digitalnu sigurnost. We'll prolazi kroz kategorije alata: identifikacija sigurnih aplikacija, sigurnih pomagala za pretraživanje, osiguranje pohrane u oblaku i alata za zaštitu vaših računara i telefona. Svaki pododjeljak uvodi ključne alate ili metode, s naglaskom na praktičnost i jednostavnost korištenja.

Prepoznavanje sigurnih aplikacija

Uz bezbroj dostupnih softvera i aplikacija, kako znate koji su "siguran"? Ovdje navodimo neke kriterije i primjere koji će vam pomoći da odaberete aplikacije koje daju prioritet sigurnosti i privatnosti.

Šta čini aplikaciju sigurnom? Sigurna aplikacija obično ima sljedeće atribute:

- Dolazi od uglednog programera ili izvora i aktivno se održava (redovito ažuriran radi ispravljanja grešaka).
- Koristi enkripciju za zaštitu podataka u tranzitu i mirovanju (posebno važno za aplikacije za komunikaciju i skladištenje).
- Ima dobru kontrolu pristupa (npr. omogućava snažnu autentifikaciju, možda 2FA za račune).
- Ima evidenciju o odgovoru na ranjivosti (programeri izdaju zakrpe) i idealno je da je prošao sigurnosne revizije.
- Aplikacija poštuje privatnost (doesn't prikuplja prekomjerne podatke ili služi sumnjive oglase koji bi mogli ubrizgati zlonamjerni softver).

Na primjer, aplikacije za razmjenu poruka kao što je Signal smatraju se sigurnim jer su softver otvorenog koda (svako može pregledati kod za backdoor), koristiti end-to-end enkripciju prema zadanim postavkama i ne prikuplja metapodatke nepotrebno. S druge strane, neke besplatne aplikacije mogu čini se zgodnim, ali može biti nesiguran –, na primjer, aplikacija za nasumično dijeljenje datoteka koja nije šifrirana ili menadžer lozinki bez 2FA opcije bi bio manje siguran od alternativa.

Odabir softvera za ključne zadatke*:* Evo nekih zajedničkih kategorija aplikacija sa sigurnim preporukama:

***Upravljanje lozinkama*:** Koristite namjensku aplikaciju za upravljanje lozinkom kao što je spomenuto. Dobre opcije uključuju Bitwarden (otvoreni izvor, baziran na oblaku, besplatan za osnovnu upotrebu), LastPass (popularan, ima slobodan nivo, iako je imao proboj 2022., što naglašava potrebu za korištenjem jakih glavnih lozinki), 1Password (plaćen, prilagođen korisniku) ili KeePass (otvoreni izvor, offline). Oni imaju snažnu enkripciju za sigurno pohranjivanje vaših vjerodajnica za prijavu, a mnogi podržavaju 2FA za otključavanje trezora. Oni također mogu generirati slučajne lozinke za vas. Korištenje bilo kojeg od njih je daleko superiornije od držanja lozinki u tabeli ili njihove ponovne upotrebe.

Sigurna poruka i e-pošta: Za razmjenu poruka, kao što je objašnjeno: Signal za većinu sigurnih razgovora; WhatsApp je također end-to-end šifriran (i široko se koristi, iako je u vlasništvu Mete, ima jake osnove šifriranja). Žica ili Threema mogu biti dobri za organizacijsku upotrebu ako želite rješenje koje je domaćin Europi. Za e-poštu, ako vam je potrebna veća sigurnost, razmotrite provajdere kao što su ProtonMail ili Tutanota, koji nude end-to-end enkripciju (posebno za interne e-poruke ili e-poruke između korisnika iste usluge). Ako se držite Gmail ili Outlook.com, oni su razumno sigurni ako se koriste sa 2FA, ali osjetljive e-poruke bi se mogle bolje poslati putem šifriranog kanala ili korištenjem alata kao što je GnuPG/PGP za enkripciju (iako je PGP složen u praksi).

Antivirus/Anti-Malware: Koristite dobro poznata, dobro recenzirana antivirusna rješenja kao što je spomenuto. Windows Defender (ugrađen na Windows 10/11) je čvrsta osnovna linija i bez muke. Ako želite treću stranu: Avast, AVG, Bitdefender, Kaspersky

(zapažajući da neki imaju zabrinutost kod Kasperskyja zbog porijekla, ali tehnički jaki), ESET, itd. Mnogi od njih imaju besplatne verzije za osnovnu zaštitu. Odaberite jedan koji se ne zalaže previše usporavajući vaš sistem i ima dobru stopu detekcije (nezavisne AV testne laboratorije to mogu voditi). Neka bude ažurirano.

Zaštita zaštitnog zida i mreže: Za većinu, ugrađeni OS zaštitni zid je u redu. Ako vam je potrebno više kontrolnih i vizuelnih znakova (za napredne korisnike), alati kao što su ZoneAlarm ili TinyWall na Windows-u mogu ponudite upravljanje zaštitnim zidom na nivou aplikacije u prijateljskom interfejsu. Na ruteru, osigurajte da je njegov zaštitni zid uključen. Neki CSO se odlučuju za hardverske zaštitne zidove ili UTM uređaje ako imaju kancelarijsku mrežu, ali oni mogu biti složeni; često, dobar ruter (sa ažuriranim firmverom) djeluje kao osnovni zaštitni zid. Ako upravljate web-stranicom, korištenje usluge kao što je Cloudflare ili vaši host's sigurnosni dodaci mogu pružiti zaštitni zid protiv napada na internetu.

Sigurni pretraživači i proširenja: Koristite moderan siguran pretraživač (Chrome, Firefox, Edge, Brave). Svi su prilično sigurni; Hrabri je poznat po neispunjenosti privatnosti (blokiranje trackera). Firefox je otvorenog koda i vrlo je konfigurisan za privatnost. Chrome je vrlo robustan u sigurnosti (Google Project Zero smatra eksploatacije i zakrpe agresivnim), ali šalje podatke Googleu (iako uglavnom benigne statistike upotrebe). Edge je također dobar (izgrađen na Chromes motoru sa Microsoft sigurnosnim karakteristikama). Možete poboljšati bilo koji pretraživač sa ekstenzijama: npr., HTTPS Everywhere (sada uglavnom suvišan od većine web stranica auto-HTTPS, ali osigurava enkripciju kada je to moguće), uBlock Origin ili Privacy Badger za blokiranje zlonamjernih oglasa i tragača (što također smanjuje rizik od malvertiziranja), a pretraživač's vlastiti pop-up bloker i anti-phishing filter bi trebali biti uključeni. Neki koriste NoScript (blokira sve skripte prema zadanim postavkama), ali taj's je napredovao i može razbijati stranice; on je opcioni za korisnike moći zabrinute zbog napada zasnovanih na skriptama. Osigurajte da kliknite na igru za Flash/Java (većina pretraživača sada u potpunosti onemogući Flash, što je dobro).

VPN usluge: Ako vaš tim često koristi javni Wi-Fi ili radi na daljinu, korištenje VPN-a može dodati sigurnost. A *dobar* VPN usluga šifrira vaš internet promet i može spriječiti njuškanje lokalne mreže. Također skriva vaš IP, koji može dodati privatnost. Međutim, koristite

samo renomirane plaćene/besplatne (neki besplatni VPN-ovi su uhvaćeni kako rade suprotno od privatnosti – reklama za evidentiranje ili ubrizgavanje). Alternativno, ako imate IT mogućnost, možete postaviti vlastiti VPN na server u oblaku za svoj tim. Jednostavnije: mnogi ruteri sada podržavaju stvaranje VPN-a za kućne kancelarije kako bi osoblje moglo bezbedno da se vrati na kancelarijsku mrežu kada je u inostranstvu.

Alati za šifriranje diska: Pored ugrađene enkripcije OS-a, postoje alati kao što je VeraCrypt (besplatni nasljednik TrueCrypt-a otvorenog koda) koji mogu kreirati šifrirane kontejnere ili šifrirati cijele diskove. Korisno ako želite šifrirati USB štapiće ili kreirati šifrirani fascikl (kontejnerski fajl) koji možete pohraniti bilo gdje (čak i oblak) i znati da je siguran. VeraCrypt je malo tehničar ali dobro dokumentovano. Postoje i jednostavnije aplikacije za trezor za telefone i računare koje štite lozinku i šifriraju specifične datoteke (npr. 7-Zip može kreirati šifrirane arhive za datoteke).

Sigurne alternative i ažuriranja: Kao dio prepoznavanja sigurnih aplikacija, ponekad to znači zamjenu rizične aplikacije sigurnijom alternativom. Na primjer, ako neko koristi zastarjelu verziju aplikacije za koju se zna da ima ranjivosti (recimo, stari CMS za web stranicu ili stari Adobe Acrobat), ažurirajte je ili prebacite na alternative (kao što je korištenje Chrome's PDF preglednik ili SumatraPDF umjesto starog Adobe Reader-a, koji je bio uobičajena meta za malver). Zamijenite softver za kraj života (kao što je Windows 7, koji više ne dobija ažuriranja – nadogradnju na Windows 10/11 ili koristite lagani Linux ako su budžeti ograničenje).

Mobilne aplikacije: Na telefonima instalirajte aplikacije samo iz službenih trgovina aplikacija, kako je naglašeno. Za sigurnu komunikaciju, opet Signal, WhatsApp (uz oprez u vezi sa rezervnim kopijama, jer WhatsApp sigurnosne kopije u oblaku mogu biti nešifrirane osim ako se ne odlučite za njihovu novu šifriranu rezervnu funkciju). Za sigurno skladištenje na telefonima, koristite ugrađene sigurnosne funkcije fascikle (Samsung Secure Folder) ili aplikacije poput **KeePassDX** da Android upravlja lozinkama van mreže.

Trening na alatima: Uvođenje novih aplikacija je dobro samo ako ih ljudi pravilno koriste. Dakle, dio uvođenja bilo kojeg alata (poput upravitelja lozinki ili VPN-a) je davanje kratkog tutorijala ili lista za varanje. Mnogi alati su intuitivni, ali početne smjernice osiguravaju

pravilnu upotrebu (npr., pokazujući kako sigurno dijeliti lozinke preko menadžera, a ne putem e-pošte).

Pažljivim odabirom i korištenjem sigurnih aplikacija smanjujete ranjivosti. Međutim, održavajte ravnotežu: "najsigurniji" ponekad znači manje prilagođen korisniku, što može dovesti do rješenja koja uvode rizik (kao da je sigurna aplikacija za razmjenu poruka previše glomazna, osoblje bi se moglo vratiti korištenju otvorene e-pošte radi pogodnosti). Odaberite alate koje vaš tim može udobno usvojiti – često, mainstream alati konfigurirani dobro pružaju sigurnost i upotrebljivost. Na primjer, Google Workspace ili Microsoft 365, ako se postavi sa 2FA i odgovarajućim administrativnim kontrolama, nude snažnu sigurnost za e-poštu/dokove i prilagođeni su korisniku. Možda nisu tako zaključani kao neka niša rješenja, ali ako ljudi zapravo slijede sigurnosne prakse na njima, mogu biti dovoljni i lakši za integraciju.

U suštini, prepoznavanje sigurnih aplikacija znači raditi malo domaće zadaće prije instaliranja nečeg novog i favoriziranja onih poznatih po sigurnosti. Mnoge organizacije civilnog društva dijele liste preporučenih alata (kao što je Front Line Defenders' Security-in-a-Box, koji nudi vodiče za alate). U sljedećim odjeljcima, we'll ističe specifične oblasti (pregledanje weba, oblak, uređaji) s određenim savjetima i alatima za svaki.

Sigurnije pregledavanje na internetu

Pregledavanje weba je tako uobičajena aktivnost da je lako zaboraviti potencijalne opasnosti. Ovaj odjeljak se temelji na praksama sigurne upotrebe interneta iz poglavlja 2, sada se fokusirajući na alate i postavke pretraživača koji mogu učiniti web surfovanje sigurnijim i privatnijim.

Sigurnosne postavke pretraživača: Prvo, osigurajte da konfigurišete ugrađene sigurnosne funkcije svog web pretraživača:

- Neka pretraživač bude ažuriran (najviše auto-update po defaultu; nemojte to onemogućiti).
- Omogućite phishing i zaštitu od zlonamjernog softvera (preglednici kao što su Chrome, Firefox i Edge imaju to po defaultu, koji provjerava posjećene URL-ove u odnosu na poznate loše liste i pokazuje veliko crveno upozorenje ako se sumnja da je stranica za phishing ili sadrži zlonamjerni softver).

- Uključite “Do Not Track” (iako ga u velikoj mjeri savjetuju, neke stranice ga poštuju).
- Razmislite o korištenju funkcija sandbox-a u pretraživaču ili izolacije lokacije ako su dostupne (Chrome ima izolaciju lokacije kako bi ublažio određene napade – obično prema zadanim postavkama za domene visokog rizika).
- U Chromeu također možete koristiti “Enhanced Safe Browsing” način rada, koji dijeli više podataka s Googleom za poboljšanu procjenu prijetnje (opciono ako vjerujete Googleu u tim podacima).

Blokatori oglasa i blokeri skripti: Kao što je navedeno, mnoge zlonamjerne infekcije se javljaju putem malvertiziranja ili zlonamjernih skripti na kompromitovanim stranicama. Korištenje renomiranog proširenja za blokator oglasa kao **uBlock Origin** ili **Adblock Plus** pomaže ne samo privatnosti i estetici, već i sigurnosti tako što prekida uobičajene vektore za isporuku zlonamjernog softvera. Ova proširenja blokiraju poznate ad domene i mogu spriječiti učitavanje sumnjivih skripti. Orijentisani na privatnost kao **Privacy Badger** (od EFF-a) naučite blokirati tragače i često ubijate zlonamjerni sadržaj treće strane u tom procesu. Ako ste veoma zabrinuti ili posećujete rizične lokacije, **NoScript** (Firefox) ili **ScriptSafe** (Chrome) može blokirati sve skripte prema zadanim postavkama – vrlo siguran, ali zahtijeva ručnu bijelu listu za legitimno mjesto funkcionalnost, koja može biti opterećujuća osim ako niste tehnički upućeni. Možda ćete koristiti lakši pristup: **Firefox** u strogom načinu poboljšane zaštite praćenja ili **Hrabar** pretraživač, koji podrazumevano blokira mnoge skripte i oglase.

Sigurne veze i proširenja: Uvijek pokušajte koristiti HTTPS verzije web stranica. The *HTTPS Everywhere* proširenje (od EFF) automatski preusmjerava na HTTPS kada je to moguće, iako ovih dana većina glavnih lokacija ionako nije u skladu sa HTTPS-om. Ikona kataloga pretraživača je vaš prijatelj – kliknite na njega kako biste pregledali detalje certifikata ili barem kako biste osigurali da je prisutna za bilo koju stranicu na kojoj unosite lozinke ili osjetljive podatke. Ako često koristite javni Wi-Fi, razmislite o proširenju kao što je **HTTPS Everywhere** (ako ne koristite VPN) da biste osigurali enkripciju ili samo budite oprezni ručno. Neki moderni pretraživači (Chrome, Firefox) sada označavaju ne-HTTPS stranice koje imaju oblike kao “Not sefe” u adresnoj traci – je poslušao to upozorenje.

Motori za pretragu i praćenje: Google pretraga je moćna, ali prati upite. Ako želite izbjeći ciljane oglase ili profilisanje, razmislite **DuckDuckGo** kao tvoj zadani pretraživač. Ne prati pretrage i ima pristojne rezultate za opšte upite. Također nudi proširenje koje ocjenjuje prakse privatnosti stranica i provodi enkripciju. Alternativno, **Početna stranica** daje Google rezultate, ali uklanja identifikacijske informacije. Oni mogu malo poboljšati privatnost bez mnogo žrtvovanja u kvaliteti pretraživanja.

Izbjegavanje rezultata otrovane pretrage: Ponekad se zlonamjerne stranice ili stranice za krađu identiteta pojavljuju u rezultatima pretraživanja (npr., lažne web stranice za podršku tehnologiji). Obučite osoblje da bude oprezno kada klikne na nejasne rezultate pretraživanja i možda se držite poznatih web stranica za preuzimanja (npr., nabavite softver iz službenog izvora, a ne sa nasumične stranice za agregiranje). Korištenje ekstenzije kao što je **Web of Trust (WOT)** ili **Bitdefender TrafficLight** može dati ikone reputacije pored rezultata pretraživanja, što ukazuje da li zajednica/algoritam – smatra stranicu sigurnom, iako su sami takvi alati imali kontroverze (Pronađeno je da WOT prikuplja korisničke podatke, pa koristite s oprezom).

Privatni način pretraživanja: Koristite "Incognito" ili privatni način rada u pretraživačima kada je to prikladno –, on't vas čini anonimnim na internetu, ali ne čuva kolačiće, povijest ili keš nakon što ga zatvorite. Ovo je korisno ako se prijavljujete u uslugu na zajedničkom računaru ili samo želite osigurati da ne ostanu ostaci određene sesije (kao što je testiranje kako vaša web stranica pojavljuje se novom korisniku). Napomena: Ne predstavlja sigurnosni alat sam po sebi protiv vanjskih prijetnji, ali može spriječiti druge korisnike istog računara da njuškaju vaše sesije.
Tor Browser za anonimno pretraživanje: Za situacije u kojima vam je potrebna anonimnost na visokom nivou ili da zaobiđete lokalnu internet cenzuru, the **Tor Browser** je alat koji treba uzeti u obzir. On usmjerava vaš promet kroz Tor mrežu, skrivajući vaš IP i šifrirajući promet unutar mreže (iako saobraćaj izlazi na odredište nešifrirano osim ako ne koristi HTTPS). OCD, novinari i aktivisti ponekad koriste Tor da dođu do blokiranih lokacija ili izbjegnu nadzor. Loša strana je što je sporija, a neka mjesta blokiraju izlazne čvorove Tor. Ali to bi mogao biti dio vašeg alata u represivnim okruženjima ili za osjetljiva istraživanja. Koristite samo službeni Tor Browser iz torproject.org i shvatite njegove smjernice za korištenje (npr. ne najavite instalirati dodatne dodatke za pretraživač u Tor Browser, ne otvarajte dokumente dok su na mreži jer mogu zaobići

Tor, itd.). Ako nije potreban za vaš kontekst, dobro konfigurirani normalni pretraživač s VPN-om mogao bi biti dovoljan.

Razmatranja izbora pretraživača: Korištenje raznolikosti pretraživača ponekad može koristiti aktivnosti sandbox-a. Na primjer, možete koristiti jedan pretraživač isključivo za prijavljivanje na osjetljive račune (i uz minimalna proširenja, samo sigurnosna), a drugi za povremeno pretraživanje. Na taj način, slučajni može imati sve eksperimentalne ekstenzije ili povremeno može posjetiti manje sigurne stranice, dok "sigurni pretraživač" (recimo, Firefox) pažljivo tretirate (nema nepotrebnih ekstenzija, strogih postavki, samo idete na poznate stranice poput vaše banke, e-mail, itd.). Ovo ograničava izlaganje kritičnih kolačića ili podataka sesije.

Integracija e-pošte/vebe: Mnoge moderne usluge e-pošte će otvoriti veze ili priloge u nekoj vrsti sandbox-a ili sigurnog gledatelja (Google ima svoj "zaštićeni pogled" za dodatke, Outlook Web ima sigurne veze ako je omogućen od strane admina). Ako imate te funkcije, držite ih na sebi; dodaju dodatni sloj, otvarajući sadržaj u kontroliranom okruženju.

Održavajte dodatke i dodatke ažurirane ili ih uklonite: Dodaci pretraživača kao što su Flash ili Java, kao što je spomenuto, treba da budu deinstalirani ako je moguće. Većini web stranica više nisu potrebne. Ako vam je apsolutno potreban Flash ili drugi iz nekog razloga, postavite ih na "Ask da aktiviraju" kako se ne bi automatski pokrenuli. Uklonite bilo koju neiskorištenu ekstenziju pretraživača; zadržite samo one kojima vjerujete i trebaju, jer zlonamjerne ili kompromitovane ekstenzije mogu oteti pregledavanje.

Označavanje pouzdanih lokacija: Podstičite korištenje oznaka/omilje za važne stranice (kao što je prijava platforme za donacije ili vladini portali koje koristi vaš CSO). Ovo pomaže u izbjegavanju čučnjanja greške u kucanju (slučajno odlazak na vaš bankovni sigurnosni.com umjesto na youbank.com). Takođe ubrzava prepoznavanje – korisnika kliknu na poznato obeležje, a ne na retipiranje ili guglanje sajta svaki put (što bi ih moglo odvesti zalutalo).

Obrazovanje o pop-up-upovima i prevarama: Nijedan alat u potpunosti ne zaustavlja prevare poput "tehnološke podrške" pop-up-a koji kažu: "Imate virus, nazovite ovaj broj." Dakle, zadržite svijest: ako dođe do takvog iskačuća, ili preuzimanje iznenada počne, zatvorite pretraživač ili karticu. Moderni pretraživači blokiraju većinu iskačućih prozora, ali ih neki oglasi

simuliraju. Korištenje blokatora oglasa uglavnom ih eliminira. Također, moderni operativni sistemi imaju pameti: Windows 10's SmartScreen će često blokirati poznata zlonamjerna preuzimanja ili vas upozoriti ako aplikacija nije't koja se obično preuzima.

Kombinacijom ovih alata i postavki, svakodnevno pregledavanje postaje znatno sigurnije. Cilj je slojevita odbrana – jedno proširenje može blokirati loš oglas, pretraživač može upozoriti na obmanjujuću stranicu, a vaš oprez čini ostalo. Ako nešto sklizne, vaš antivirus bi ga mogao uhvatiti pri preuzimanju. Nijedan sloj nije siguran, ali zajedno uvelike smanjuju rizik.

Cloud Storage: Google Drive, Dropbox i njihova sigurnost

Usluge skladištenja u oblaku kao što su Google Drive, Dropbox, Microsoft OneDrive i drugi revolucionirale su način na koji OCD sarađuju i pohranjuju podatke. Oni nude praktičnost i podršku po defaultu, ali također uvode sigurnosna razmatranja. Ovaj odjeljak objašnjava kako bezbedno koristiti ove usluge.

Kontrola pristupa i podjele postavki: Jedan od najvećih rizika sa skladištenjem u oblaku je slučajno preterano deljenje. Uvijek provjeri kako dijeliš datoteke ili mape. Podrazumevano, držite dokumente privatnim za svoju organizaciju ili određene korisnike. Na primjer, Google Drive omogućava dijeljenje na "Svako sa link" – koristi to samo kada je potrebno i razmotri dodavanje lozinke ili isteka (Google' ne nudi lozinku na linkovima, ali OneDrive za poslovanje i Dropbox radi za plaćene račune). Umjesto toga, radije dijelite sa određenim e-mailovima ljudi koji se odnose na ljude (oni će se izjasniti da se prijave, što je sigurnije). Dropbox i Google prikazuju ikone koje ukazuju na to da li se fascikla dijeli – se upoznajte s tim indikatorima i periodično ih revidirate. Google's **"dijeli sa me"** sekcija i Dropbox's zajednička lista fascikli mogu pomoći u pregledu onoga što's otvara.

Ako vaš CSO koristi G Suite/Google Workspace ili Microsoft 365, iskoristite prednosti administrativnih postavki: možete ograničiti eksterno dijeljenje ili ga barem pratiti. Možda ograničiti ko može dijeliti eksterno ili postaviti zadanu postavku koja dijeli vezu izvan organizacija je isključena. Na taj način zaposlenik mora namjerno nadjačati da javno dijeli. Ako koristite lični/besplatni Google nalog, budite posebno oprezni, jer oni nemaju nadzor administratora, a možete nehotice izložiti datoteku svijetu.

Omogući dvofaktorsku autentifikaciju na računima u oblaku: Više puta smo naglašavali 2FA i navodi da je ključno za pohranu u oblaku jer bi kršenje vašeg računa moglo razotkriti mnogo podataka. Google, Dropbox, Microsoft, Box, itd., svi podržavaju 2FA (obično putem aplikacija za autentifikaciju ili SMS-a). Osigurajte da svaki korisnik u vašem timu sa pristupom to uradi. Mnoga kršenja se dešavaju jer se ukrade vjerodajnice za prijavu, ali 2FA bi spriječila napadača da kratko.

Upravljanje uređajima i daljinska cijev: Koristite opcije za upravljanje uređajima. Na primjer, Dropbox i OneDrive navode sve povezane uređaje (računari, telefoni). Ako se uređaj izgubi ili neko ode, možete se daljinski odvezati i, u slučaju Dropbox's, čak i daljinski obrisati datoteke koje su postavljene na lokalnu. Google Drive (Backup i Sync ili novi Drive for desktop) ne't sasvim briše lokalne datoteke jer su obično samo u kešu, ali je opoziv pristupa i dalje važan. Google's admin panel (za Workspace) može obrisati podatke sa korisničkog's Drive-a na mobilnom uređaju ako postavite upravljanje uređajima. Čak i ako možete da osmislite automatsko brisanje, promenu lozinke i potpisivanje svih sesija (obično bezbednosna postavka naloga) pomaže da se osigura da izgubljeni laptop može da potvrdi sinhronizaciju novih podataka ili se računu ne može pristupiti.

Šifrovanje osjetljivih podataka: Kao što je ranije spomenuto, dok ove usluge šifriraju podatke na svojim serverima, one drže ključeve (osim određenih proizvoda kao što su MEGA ili SpiderOak, koji su end-to-end šifrirani, ali se rjeđe koriste). Ako imate posebno osjetljive podatke koje're stavljate u Google Drive ili Dropbox, mogli biste dodati vlastiti sloj enkripcije. Opcije:

- Koristite alate kao **VeraCrypt** da napraviš šifrovani kontejner I pohraniš tu datoteku na Drive/Dropbox. Onda ti treba VeraCrypt da ga otvori sa lozinkom. Neuspjesi: cijeli kontejner mora ponovo sinhronizirati kada se promijeni, a istovremena suradnja unutar njega nije jednostavna.
- Koristiti **7-Zip** ili **WinZip** da šifrirate određene datoteke prije učitavanja ako ih planirate dijeliti izvana. Koristite snažnu lozinku i podijelite tu lozinku putem drugog kanala.

- Neke usluge u oblaku nude šifrirani “trezor” ili “scover” kao funkciju (npr. Dropbox Professional ima trezor). Znajte svoje karakteristike alata’s.
- Ako koristite Office 365, možete primijeniti oznake osjetljivosti koje šifriraju datoteke tako da ih samo određeni računi mogu otvoriti (ovo je ipak naprednija funkcija preduzeća).
- Ako koristite Google, izbjegavajte stavljanje izuzetno osjetljivog sadržaja u tekst Google Docs-a osim ako nije potrebno, jer Google tehnički može pristupiti njemu. Možda koristite offline šifrirane formate i samo ih pohranite tamo ili koristite nešto poput **Kriptomator** <TAG1> alat dizajniran za šifriranje datoteka na strani klijenta prije sinhronizacije s oblakom (to stvara virtuelni disk; datoteke ubačene su šifrirane, a zatim sinkronizirane). Kriptomator dobro radi sa Dropboxom, Google Driveom, itd., i ne’t zahtijeva poseban serverski softver (oblak samo vidi gibberish datoteke). Za OCD koji rukuje visoko povjerljivim informacijama, to može biti vrijedno implementacije za podskup podataka.

Monitoring i upozorenja: Neke usluge omogućavaju praćenje aktivnosti. Na primjer, Dropbox prikazuje dnevnik dijeljenja događaja i prijava na stranici računa. Administrator Google Workspacea može postaviti upozorenja za stvari kao što su “datoteka koja se dijeli izvana ili ” sumnjivi pokušaj prijave.“ Ako je dostupno, konfigurirajte ih. Čak i na ličnim računima, Google Account Security će vas upozoriti na nove prijave uređaja – obratite pažnju na te e-poruke ili upite (“Did ste se samo prijavili sa X uređaja?”).

Obrazovati o socijalnom inženjerstvu: Napadači možda neće direktno hakovati Google, ali bi vas mogli nazvati. Primjer: dobijate e-poštu koja izgleda kao udio Google Drivea od kolege, ali ona zapravo osmišljava pametno prikrivenu phishing vezu koja vodi do lažne Google prijave. Google Drive phishing je poznata taktika – jer ljudi vjeruju da Drive/Docs dijele e-poštu. Dakle, provjerite neočekivane dionice prije nego što se prijavite preko njih. Google se poboljšao dodavanjem sigurnosnih skeniranja Docs-u, ali je potreban oprez. Slično, don’t ne unosi svoju lozinku u bilo koji neočekivano iskačući – bolje idite na drive.google.com ručno ako je potaknut.

Istorija verzije i zaštita ransomware-a: Jedna od prednosti skladištenja u oblaku je istorija verzije. Ako ransomware šifrira vaše lokalne datoteke i one se sinhroniziraju s oblakom

kao besmislice, usluge poput Dropboxa i OneDrivea zadržavaju starije verzije nekoliko dana. Mogli biste vratiti prethodne verzije mnogih datoteka (Dropbox Pro čak ima opciju proširene istorije verzije). Upoznajte se s tim procesom. OneDrive (poslovni) također ima "Restore sve datoteke u odnosu na prethodnu vreme" funkciju kako bi se masovno oporavio nakon događaja ransomware-a. Znajte da se tamo manifestuje, ali prevencija je ključna da joj ne treba.

Korištenje organizacionih računa u odnosu na lični: Ako je moguće, koristite račun kojim upravlja organizacija za pohranu u oblaku, a ne gomilu ličnih računa. Na primjer, s Google Workspaceom za neprofitne organizacije (koji je često besplatan/diskontrorisan za OCD), dobijate upravljane račune (kao [name]@CSO.org) sa Driveom. Na taj način podaci mogu biti u vlasništvu organizacije, a možete ih kontrolirati ako neko ode. Lični računi povezuju podatke sa pojedincima, što može biti neuredno ako osoba nastavi dalje. Također, Google Workspace i Microsoft 365 za organizacije imaju bolje sigurnosne kontrole po dizajnu od besplatnih naloga. Pogledajte te neprofitne ponude (Google for Nonprofits, Microsoft za neprofitne organizacije), jer mogu značajno povećati sigurnost (i saradnju) uz niske ili nikakve troškove.

Redovne revizije: Uzmite vremena, možda tromjesečno ili dva puta godišnje, da revidirate svoje pogone u oblaku. Uklonite stare podatke koji vam više nisu potrebni (smanjuje izloženost). Provjerite postavke dijeljenja na kritičnim fasciklama. Uklonite pristup korisnicima kojima više nije potreban. Ovo održavanje osigurava da vaše okruženje u oblaku ostane uredno i sigurno.

Ukratko, usluge kao što su Google Drive i Dropbox mogu biti sigurne za OCD ako se koriste mudro: zaštititi račune uz snažnu autentifikaciju, pažljivo podijeliti konfiguraciju i možda dodati dodatnu enkripciju za visoko osjetljive datoteke. Prednosti pogodnosti i saradnje su ogromne, tako da se uglavnom radi o korištenju sigurnosnih funkcija alata u potpunosti. Većina incidenata na ovim platformama događa se zbog ljudske greške (kao što je javno dijeljenje veze greškom ili korištenje slabe lozinke) umjesto da provajderi budu provaljeni. Obraćajući se tim ljudskim faktorima i tehničkim okruženjima, možete pouzdano iskoristiti oblak.

Zaštita vašeg telefona I računara

U ranijim odjeljcima razgovarali smo o općoj sigurnosnoj praksi uređaja. Ovdje ćemo se uključiti u neke specifične alate i postavke kako bismo dodatno osigurali vaše računare i mobilne uređaje, budući da su to krajnje tačke u kojima pristupate svim svojim digitalnim resursima.

Osigurajte da je FDE omogućen na svim laptopima i mobilnim uređajima. Na modernim računarima, ovo često zahtijeva samo uključivanje:

- Windows 10/11: Koristi **BitLocker** (na Pro izdanjima) ili šifriranje uređaja kod kuće (ako je dostupno). Jednom uključen, šifrira cijeli disk i vezuje dešifriranje na vašu lozinku/PIN (i TPM čip). BitLocker također može šifrirati USB diskove (možete koristiti BitLocker To Go za to).
- macOS: Uključi se **FileVault** u sigurnosnim postavkama; on osmišljava jedan klik za šifriranje Mac's diska.
- Linux: Ako koristite Linux, instalirajte pomoću LUKS enkripcije omogućene ili koristite alat kao što je kriptosetup. Mnogi distroi prilagođeni korisniku omogućavaju omogućavanje šifriranja tokom instalacije.
- Android: Većina modernih Android uređaja šifrira po defaultu skladištenje (posebno od Androida 7.0+). Samo se pobrinite da postavite jak PIN/password/obrazac, jer je enkripcija jaka samo kao ekran za zaključavanje.
- iPhone/iPads: Oni su automatski hardverski šifrirani sve dok postavljate lozinku. Dakle, uvijek koristite lozinku (i Touch/Face ID za praktičnost, ali to's je zaključano na šifru kao sigurnosna kopija).

Sigurnosne aplikacije mobilnih uređaja: Za Android, razmislite o instaliranju renomirane sigurnosne aplikacije. Opcije: **Google Play Protect** ugrađene su i skeniraju aplikacije (pobrinite se da se's omogući u postavkama Play Store-a). AV treće strane kao **Avast Mobile**, **Bitdefender Mobile**, ili **Pazi** mogu dodati zaštitu od phishinga i funkcije pronalaska mog telefona. Oni također mogu skenirati za zlonamjerne aplikacije izvan onoga što Play Protect nalazi (iako je Google's pristojan). Za iOS, odvojene sigurnosne aplikacije su manje potrebne zbog sandboxinga (iako aplikacije poput Lookout-a mogu pomoći u lociranju telefona ili provjeri da li je vaš iOS slomljen).

***Nađi moj uređaj*:** Uvijek omogućite usluge pronalaženja i daljinskog brisanja:

- Android: Koristi **Nađi moj uređaj** (gugla usluga) – i's obično uključuje ako imate Google nalog na telefonu. Testirajte ga (Google "pronađite moj uređaj" i pogledajte da li je vaš telefon pronađen).
- Samsung uređaji takođe imaju **Nađi moj mobilni,** što može biti alternativa sa više funkcija.
- iPhone: Pobrinite se **Nađi moj iPhone** je uključen (u iCloud postavkama). Ovo vam omogućava da locirate ili izbrišete izgubljeni telefon.
- Laptopovi: Razmotrite softver za praćenje laptopa ako je krađa zabrinjavajuća. PreyProject (Prey) ima besplatan plan za do tri uređaja i može pomoći u lociranju izgubljenog/ukradenog laptopa, pa čak i fotografiranju ili slanju poruka. Neki poslovni laptopi imaju ugrađenu anti-krađu (kao što je Computrace/LoJack). Ali čak i bez specijalizovanog softvera, ako se laptop izgubi, odmah promenite lozinke za račune kojima je imao pristup, a ako je bio šifrovan, barem znate da su podaci sigurni.

Firewall na računarima: Windows Firewall je podrazumevano uključen – ga zadrži. U tišini radi svoj posao, blokirajući neželjeni ulazni saobraćaj. Također ga možete koristiti za blokiranje određenih aplikacija odlaznih ako je potrebno (manje uobičajeno za CSO scenario). Na Macu, uključite zaštitni zid u sigurnosnim preferencijama. Vjerovatno vam nije potreban softver za zaštitne zidove trećih strana; ugrađeni su u redu i izbjegavajte zbunjujuće upute koje bi manje tehnološkog nadzora moglo ionako dozvoliti.

Firmware i BIOS sigurnost: Za potrebe visoke sigurnosti, razmislite o postavljanju BIOS/UEFI lozinke na laptopove (tako da pokretanje sa vanjskih medija ili izmjena postavki pokretanja zahtijeva lozinku). Također omogući Secure Boot (da spriječi rootkits). Ovi koraci sprečavaju napadača sa fizičkim pristupom da, recimo, pokrene živi OS kako bi zaobišao sigurnost vašeg sistema. Uz to, ako imate FDE i snažnu lozinku, ionako ne bi trebali ući. Ali BIOS lozinka dodaje sloj protiv neovlaštenog pristupa ili korištenja mašine.

Ažuriranje uređaja Automatizacija: Razgovarali smo o ažuriranjima OS-a; dodatno:

- Održavajte aplikacije ažuriranim, npr., osigurajte da je Microsoft Office ili LibreOffice ažuriran (Ured obično automatski ažurira putem Office 365 ako to imate, inače provjerite ažuriranje Windows Update ili Office's).
- PDF čitač: Ako koristite Acrobat Reader, ažurirajte ga. Ili koristite sigurniji čitač kao **SumatraPDF** ili vaš pretraživač' PDF preglednik, koji su jednostavniji I manje iskorišteni.
- Java: Ako ga morate imati, postavite ga za automatsko ažuriranje. Ako vam ne bude potrebno, potpuno ga deinstalirajte.
- Na telefonima ažurirajte aplikacije putem Play Store/App Store kad god su dostupna ažuriranja (mogu se automatski ažurirati na Wi-Fi kako bi bila bez napora).

Onemogući nepotrebne karakteristike: Neiskorištena otvorena vrata se mogu zatvoriti:

- Na Windows-u, ako vam ne potvrde potrebne funkcije kao što su RDP (Remote Desktop) ili dijeljenje datoteka, isključite ih kako biste smanjili površinu napada.
- Na telefonima, imajte na umu Bluetooth i NFC –, držite ih podalje kada se ne koriste (Bluetooth napadi su sada manje uobičajeni s zakrpama, ali to je i dalje dobra higijena, posebno na javnim mjestima).
- Uklonite aplikacije za bloatware na telefone koje ne koristite, posebno one koje bi mogle raditi u pozadini ili imati dozvole (neki Android telefoni dolaze s unaprijed instaliranim aplikacijama koje bi mogle rudariti podatke).
- Na bilo kojem sistemu, don't se prijavljuje kao administrator za svakodnevnu upotrebu. Imajte standardni korisnički nalog za rutinski rad i administrativni nalog za instaliranje softvera. Na ovaj način, ako radi zlonamjerni softver, možda neće imati administrativna prava da izvrši duboke promjene. Doduše, mnogi ljudi to ignorišu, ali to je preporučena praksa na Windows i Linux. Na Macu, početni korisnik je admin, ali Mac će potaknuti eskalaciju lozinke, koja djeluje slično kao i privilegije razdvajanja.

Koristite dobar sigurnosni softverski apartman: Ako je budžet dozvoljen ili su besplatne opcije dovoljne, koristite dobro zaokruženi sigurnosni paket. Na primjer, **Microsoft Defender** zapravo uključuje ne samo anti-malware već i pristup kontrolisanom folderu (zaštita od resomvera koja sprečava nepoznate aplikacije da uređuju vaše dokumente) i zaštitu zasnovanu na oblaku ako se uključi. Paketi trećih strana mogu uključivati upravitelja lozinki, VPN probnu verziju, itd. Ulažu samo ako su vam potrebni ti dodaci; u suprotnom, slojeviti pojedinačni alati rade.

Sigurnost e-pošte na uređaju: Ako koristite klijent e-pošte kao što su Outlook ili Thunderbird, osigurajte da se ažurira. Budite oprezni s tim koje priloge otvarate. Moderni klijenti e-pošte imaju malo sandboxinga (Outlook, na primjer, neće učitati slike ili pokrenuti makroe prema zadanim postavkama, i upozorava da li aplikacija pokušava pristupiti podacima e-pošte). Don't omogućava "da omogući programski pristup" osim ako nije potrebno nekom integracijom.

Fizičke zaštite: Laptops – razmišljajte o korištenju Kensington kabla za zaključavanje ako ga ostavite u zajedničkom prostoru (da odvratite oportunističku krađu). Za telefone koristite zaštitne futrole i možda štitnike za ekran privatnosti ako se javno bavite osjetljivim informacijama (prevencija surfanja ramenom).

Rezervne kopije podataka za uređaje: Razgovarali smo o rezervnim kopijama, ali jedan aspekt: za mobilne uređaje, rezervišete i svoje podatke (oblikovanje u oblaku ili ručni). Za iPhone uređaje koristite iCloud ili lokalne iTunes sigurnosne kopije; za Android, koristite Google's backup usluge ili aplikacije za kritične podatke. Na taj način izgubljeni uređaj ne znači izgubljene podatke, a možete daljinski obrisati bez oklijevanja, znajući da je sačuvan.

Oznaka protiv krađe: Ponekad su najjednostavnija rješenja najbolja: označite svoje uređaje kontakt informacijama. Osoba koja pronađe izgubljeni uređaj može ga vratiti ako je lako (kao naljepnica koja kaže "Ako se pronađe, pozovite [CSO broj]"). Ovo je više savjet za oporavak nego sigurnost, ali može spasiti dan.

Plan zamjene uređaja: Imajte jednostavan plan ako je uređaj kompromitovan ili zastario. Na primjer, ako računar više ne prima ažuriranja (Windows 7, stari Android), postupno

ga ukinite ili izolirajte iz osjetljivih zadataka. Možda ga koristiti van mreže ako je potrebno za nešto naslijeđe. Ali ulažete u zadržavanje hardvera u podržanom životu radi sigurnosti.

Koristeći gore navedene metode i alate na svojim telefonima i računarima, kreirate snažan odbrambeni perimetar oko svojih ličnih i radnih podataka. Zamislite svoj uređaj kao siguran trezor:'ve ga je zaključao (snažna prijava), uznemirio (antivirus i zaštitni zid), pojačao ga (ažuriranja i šifriranje) i postavio način da locirate ili uništite sadržaj ako se uzme (pronađite moj uređaj, daljinsko brisanje). S takvim mjerama, čak i ako se pojave prijetnje, ili ih blokirate ili ste spremni odgovoriti bez katastrofalnog gubitka.

Ovim se završava poglavlje o alatima. Usvajanjem sigurnih aplikacija (4.1), prakticiranjem sigurnog pregledavanja (4.2), pravilnim korištenjem pohrane u oblaku (4.3) i uređaja za utvrđivanje (4.4), vaš OCD hoće imajte mnogo jači stav digitalne sigurnosti. Zatim ćemo razgovarati šta da radimo ako, uprkos svemu ovome, sajber pitanje se dešava – jer nijedna odbrana nije 100% savršena, plan odgovora je od vitalnog značaja.

Sažetak poglavlja

Poglavlje 4 fokusira se na osiguranje tehnologije na koju se OCD oslanjaju, uključujući računare, mreže i web stranice. Preporučuje ažuriranje softvera za zakrpe ranjivosti, korištenje antivirusnih alata (npr. Avast Free) za borbu protiv zlonamjernog softvera i osiguranje Wi-Fi mreže pomoću WPA2/WPA3 enkripcije. Za web stranice savjetuje omogućavanje HTTPS-a, redovnih rezervnih kopija i ažuriranje sistema upravljanja sadržajem (npr., WordPress) kako bi se spriječilo oštećenje ili DDoS napadi. Studija slučaja web stranice CSO's koja preusmjerava na stranicu treće strane zbog zastarjelog softvera ilustruje rizike. Poglavlje promoviše VPN-ove (npr. ProtonVPN) za sigurne veze na javnom Wi-Fi-ju, vitalnom za terensko osoblje. Naglašava jeftina rješenja, poput besplatnog HTTPS-a preko Let's Encrypt-a, kako bi odgovarala CSO budžetima. Netehničko osoblje se vodi kako bi provjerilo postavke (npr., provjerilo ima li HTTPS katanaca) bez potrebe za IT stručnošću. Poglavlje također pokriva šifriranje uređaja i jake lozinke za zaštitu od krađe ili gubitka. Osiguranjem infrastrukture, OCD sprečavaju poremećaje i povrede podataka, osiguravajući kontinuitet misije. Poglavlje osmišljava praktične korake, poput zakazivanja automatskih ažuriranja, čini implementaciju jednostavnom, usklađujući se s ciljem e-knjige's pristupačne sajber sigurnosti.

Kontrolna lista sigurnosti računa društvenih medija za OCD

Ova kontrolna lista pomaže organizacijama civilnog društva da osiguraju svoje naloge na društvenim mrežama (npr. Twitter/X, Facebook, Instagram) kako bi zaštitili svoje prisustvo i reputaciju na mreži od otmice, dezinformacija ili neovlaštenog pristupa. Ovi koraci su dizajnirani za programsko osoblje i volontere sa minimalnom tehničkom stručnošću koju treba završiti za jedan ili dva sata. Radite kroz svaki predmet, provjeravajte završene zadatke. Ako niste sigurni, pitajte svog menadžera društvenih medija, IT kontakt ili podršku platforme za pomoć. Podijelite nalaze sa svojim timom kako biste održali sigurno prisustvo na mreži.

1. Omogući dvofaktorsku autentifikaciju (2FA)

☐ Uključite 2FA za sve naloge na društvenim mrežama da zahtijevaju drugi korak provjere (npr., kod koji se šalje na vaš telefon ili aplikaciju).

☐ Platformski savjeti:

- Twitter/X: Idite na postavke > Privatnost i sigurnost > Autentifikacija dva faktora. Odaberite aplikaciju za autentifikaciju (npr. Google Authenticator) ili SMS.
- Facebook: Navigacija na postavke > Sigurnost i prijava > Autentifikacija dva faktora. Odaberite aplikaciju za autentifikaciju ili tekstualnu poruku.
- Instagram: Idite na postavke > Sigurnost > Autentifikacija dva faktora. Omogućite autentifikaciju zasnovanu na aplikacijama ili SMS-u.

☐ Primjer: Hakirani CSO Twitter nalog objavio je lažne poruke. 2FA je spriječio dalji neovlašteni pristup.

☐ Prijavite se na svaki račun, omogućite 2FA i testirajte ga pomoću uređaja za svoj tim’s.

2. Koristi jake, jedinstvene lozinke

☐ Ažurirajte lozinke na najmanje 14 znakova, miješajući slova, brojeve i simbole (npr. “sunbird&glass7rain”). Koristite drugačiju lozinku za svaki račun.

☐ Razmislite o besplatnom menadžeru lozinki (npr. Bitwarden) za sigurno pohranjivanje lozinki.

☐ Platformski savjeti:

- Twitter/X: Ažuriranje u postavkama > Promijenite lozinku. Izbjegavajte ponovno korištenje lozinki sa drugih platformi.
- Facebook: Idite na postavke > Sigurnost i prijava > Promijenite lozinku. Osigurajte da se manifestira jedinstvenim na osnovu e-pošte ili drugih naloga.
- Instagram: Navigacija na postavke > Sigurnost > Lozinka. Koristite šifru za lakše pamćenje.

☐ Primjer: CSO's Instagram je kompromitovan zbog ponovo korištene lozinke e-pošte. Jedinstvena lozinka je popravila problem.

☐ Promijenite lozinke za sve račune i pohranite ih u upravitelj lozinki.

3. Uklonite račune za nenamještene štednje

☐ Provjerite ko ima administratora ili urednika pristup vašim nalozima na društvenim mrežama i uklonite bivše osoblje, volontere ili neaktivne korisnike.

☐ Platformski savjeti:

- Twitter/X: Idite na postavke > Pretplate kreatora > Upravljajte timom za pregled i uklanjanje administratora.
- Facebook: Navigacija na podešavanja stranica > Uloge stranica za vidjeti i izbrisati nepotrebne uspomene ili urednike.
- Instagram: Provjerite postavke > Ovlaštene aplikacije ili poslovne postavke > Korisnici da odustanu od pristupa neiskorištenim nalozima.

☐ Primjer: Bivši administratorski pristup volonterskog direktora korišten je za objavljivanje neovlaštenog sadržaja. Uklanjanje starih dimina spriječilo je ponavljanje.

☐ Pitajte svog menadžera društvenih medija: "Možemo li pregledati i ukloniti zastarjele administrativne račune?"

4. Postavite i provjerite e-poštu/fon

☐ Osigurajte da svaki račun ima trenutnu e-poštu za oporavak ili broj telefona koji kontrolira osoblje od povjerenja za oporavak računa ako je zaključan ili hakovan.

- Platformski savjeti:
    - Twitter/X: Ažuriranje u postavkama > Vaš račun > Informacije o računu. Provjerite da li je e-mail za oporavak aktivan.
    - Facebook: Idite na Postavke > Sigurnost i prijava > Kontakt za dodavanje ili ažuriranje e-pošte/telefona za oporavak.
    - Instagram: Navigacija na postavke > Sigurnost > Oporavak računa za potvrdu važeće e-pošte ili telefona.

☐ Primjer: CSO je povratio hakovani Facebook nalog koristeći e-poštu za oporavak. Bez toga, oporavak je trajao nedeljama.

☐ Dodajte ili ažurirajte detalje oporavka i testirajte tražeći kod za oporavak.

5. Aktivnost računa za praćenje

☐ Redovno provjerite neobične aktivnosti (npr. postove koje ste kreirali, prijave sa nepoznatih lokacija).

☐ Omogućite upozorenje o prijavi gdje je to dostupno za obavještenje o sumnjivoj aktivnosti.

☐ Platformski savjeti:

- Twitter/X: Provjerite postavke > Privatnost i sigurnost > Povezani računi za nepoznate uređaje ili aplikacije.
- Facebook: Idite na postavke > Sigurnost i prijava > Gdje ste se prijavili za pregled aktivnih sesija. Omogućite upozorenje o prijavi.
- Instagram: Navigacija na postavke > Sigurnost > Logiranje aktivnosti za pregled lokacija za prijavu i omogućavanje obavještenja.

☐ Primjer: CSO je uočio prijavu iz druge zemlje i zaključao račun prije nego što je šteta učinjena.

☐ Pregledajte dnevnike aktivnosti sedmično i prijavite čudno ponašanje uz podršku platforme.

6. Ograničite pristup aplikaciji treće strane

☐ Uklonite pristup aplikacijama ili alatima trećih strana (npr. alatima za planiranje, analitičkim aplikacijama) koji se više ne koriste ili ne vjeruju.

☐ Platformski savjeti:

- Twitter/X: Idite na postavke > Privatnost i sigurnost > Povezani računi za ukidanje dozvola za prijavu.
- Facebook: Navigacija na postavke > Aplikacije i web stranice za uklanjanje neiskorištenih ili sumnjivih aplikacija.
- Instagram: Provjerite postavke > Sigurnost > Aplikacije i web stranice za ukidanje pristupa potrebnim aplikacijama.

☐ Primjer: Aplikacija za zakazivanje sa zastarjelim pristupom korištena je za objavljivanje neželjene pošte na CSO's Twitteru. Opozivni pristup ga je popravio.

☐ Pregledajte i uklonite nepotrebne veze aplikacija u postavkama računa.

7. Željezničko osoblje za bezbednu upotrebu društvenih medija

☐ Podsjetite osoblje i volontere da ne dijele akreditive računa, kliknu na sumnjive veze ili objavljuju osjetljive podatke (npr. informacije o donatorima) na društvenim mrežama.

☐ Podijelite savjet: “Log sa računa na zajedničkim ili javnim uređajima.”

☐ Primjer: Volonter je objavio osjetljive detalje kampanje na javnoj objavi na Instagramu. Trening je sprečio buduće greške.

☐ Pošaljite e-poštu timu: “Never dijeli prijave na društvenim mrežama. Prijavite se nakon upotrebe na zajedničkim uređajima.”

8. Plan za dezinformacije ili otmice

☐ Razviti jednostavan plan odgovora za hakovane naloge ili dezinformacije (npr. izvještaj platforme, objaviti pojašnjenje sljedbenicima).

☐ Održavajte nacrt izjave spremnim: “Naš račun je kompromitovan. Molimo vas da zanemarite nedavne objave. We’re rješava ovo.”

☐ Platformski savjeti:

- Twitter/X: Prijavite hakove putem pomoći.twitter.com/forme/sigurnost.
- Facebook: Koristite facebook.com/hakiran da prijavite kompromitovane naloge.
- Instagram: Izveštaj pitanja putem Postavki > Pomoć > Izveštaj hakovanog računa.

☐ Primjer: CSO je brzo razjasnio hakovanu objavu na Facebooku, smanjujući širenje dezinformacija.

☐ Nacrtajte izjavu o odgovoru i sačuvajte linkove podrške platformi za brzi pristup.

POGLAVLJE 5: UZORCI SCENARIJA INCIDENTA SA KIBERNETIČKOM SIGURNOŠĆU

Šta da učiniš ako doživiš kiberincident

Uprkos najboljim naporima u prevenciji, incidenti se i dalje mogu dogoditi. Brz, miran i metodičan odgovor može značajno smanjiti štetu uzrokovanu sajber incidentom. Ovo poglavlje vas vodi kroz prepoznavanje znakova incidenta, neposrednih koraka koje treba poduzeti, koga kontaktirati za pomoć i kako obnoviti sigurnost nakon toga. U suštini, to je vaš plan hitne akcije za digitalno carstvo.

Prepoznavanje znakova sajber napada

Što prije shvatiš da nešto nije u redu, brže ćeš odgovoriti. Sajber napadi se mogu manifestovati na različite načine; neki očigledni, neki suptilni. Evo uobičajenih crvenih zastavica koje mogu ukazivati na problem:

Ransomware poruka ili zaključani ekran: Vrlo jasan znak – vaš računar iznenada prikazuje poruku da su vaše datoteke šifrirane ili zahtijeva otkupninu za otključavanje vašeg sistema. Možda ne možete otvoriti datoteke, a možda imaju čudne ekstenzije. Često se pozadina može promijeniti na instrukcije, ili se pojavi prozor koji navodi datoteke i upute za plaćanje. Ako vidite ovo, to je gotovo sigurno napad ransomware-a.

Upozorenja na antiviruse ili lažni AV pop-up: Ako vaš antivirus uhvati nešto, shvatite to ozbiljno. Suprotno tome, ako vidite skitni pop-up koji tvrdi “Vaš kompjuter je zaražen! Kliknite ovdje da skenirate,” i on’ nije iz vašeg AV-a već web stranice, to je taktika da vas namamite da instalirate zlonamjerni softver. Prepoznajte razliku: vaš stvarni AV softver će imati svoje poznato sučelje i vjerovatno neće projicirati putem nasumične reklame za pretraživač.

Neočekivano ponašanje alata ili pretraživača: Odjednom, vaš pretraživač ima nove trake sa alatima, ili vaš početni/tražni motor promijenjen bez vašeg unosa, ili pretrage preusmjeravaju na neobične stranice. Ovo sugerira da je instaliran adver ili zlonamjerni softver. Slično, česti pop-up oglasi kada ste u’ offline-u ili na stranicama koje ih inače ne prikazuju mogu ukazivati na infekciju.

Nepoznati programi ili procesi: Primjećujete aplikaciju koju nikada niste instalirali. Ili vaš računar’s fan radi visoko, i on je’ spor, a Task Manager/Activity Monitor pokazuje nepoznate procese koji zakrče CPU. Neki zlonamjerni softver može raditi nevidljivo, ali mnogi će trošiti

resurse (poput kriptominera, čineći vaš sistem sporim). Ako vidite program otvoren nakratko, onda nestanite ili nove ikone na desktopu, istražite.

Vaši prijatelji dobijaju čudne poruke od vas: Ako kolege ili prijatelji kažu da su od vas dobili čudnu e-poštu ili poruku na društvenim mrežama koju niste poslali, vaš račun bi mogao biti ugrožen. Primjeri: neželjene e-poruke s vaše adrese ili vaš WhatsApp koji šalje sumnjivu vezu u grupnim razgovorima. Ovo je znak da je ili vaš uređaj ili taj račun preuzet.

Lozinka ne radi: Vrlo alarmantan znak je ako se odjednom ne možete prijaviti na račun jer je lozinka promijenjena (a vi je niste promijenili). Ako je vaša poznata ispravna lozinka odbijena, a oporavak računa ukazuje na promjenu, pretpostavite kršenje tog računa.

Neobična mrežna ili sistemska aktivnost: Ovo može biti teže primijetiti za prosječnog korisnika, ali ako imate alat za mrežni monitor ili IT administrator: primjeri su porast izlaznog saobraćaja, nepoznati uređaji na mreži ili svjetlo na tvrdom disku stalno trepće kada' ne radite ništa (može značiti da se podaci eksfiltriraju ili da virus skenira vaše datoteke). Također provjerite upozorenja zaštitnog zida (ako ih ima) ili dnevnike Windows Defendera za ponovljene blokirane radnje.

Datoteke nestale ili izmijenjene: Ako otkrijete da se datoteke brišu ili se sadržaj mijenja bez objašnjenja, to se odnosi na. Napadač može obrisati ili neovlastiti podatke. Također, ako vidite datoteke koje imaju iskrivljena imena ili ekstenzije poput zaključanih ili šifriranih, to ukazuje na ransomware.

Čudan kursor ili kontrola: U ekstremnim slučajevima, ako se vaš miš kreće sam ili se prozori otvaraju i vi to ne činite, neko može imati daljinski upravljač (kao da radi daljinski desktop ili RAT malver). Isključite se s interneta odmah ako se to dogodi.

Sistemska upozorenja ili kreme za krah: Ponovljeni padovi ili plavi ekrani mogu biti samo problemi hardvera/softvera, ali ponekad rootkits ili duboki zlonamjerni softver uzrokuju nestabilnost. Ako je počeo da se dešava zajedno sa drugim znakovima, smatrajte zlonamjerni softver mogućnošću.

Redirekcije pretraživača: Ako, kada pokušate posjetiti zajedničke stranice (poput banke ili Gmaila), stalno se preusmjeravate na malo drugačiji URL ili neočekivano vidite upozorenja o

certifikatu, možda ćete imati zlonamjerni softver ili otmicu DNS-a. Na primjer, pokušaj da se ide na facebook.com, ali uvijek slijetanje na stranicu koja ne izgleda kako treba znači probleme.

U praksi se mnogi od ovih znakova preklapaju. Na primjer, napad ransomware-a će proizvesti šifrirane datoteke (koje možete predstaviti), vjerovatno tekstualnu datoteku otkupnine u svakoj fascikli, a možda i promijenjenu tapetu na desktopu koja je najavljuje. Kompromisi sa phishing računom često se otkrivaju kada vas drugi informišu o čudnim porukama ili kada dobijete upozorenja o prijavi sa neobičnih mjesta.

Ako sumnjate u problem, ali niste sigurni, pogriješite na strani opreza:

- Ako se osnuje potencijalni virus, pokrenite potpuno antivirusno skeniranje.
- Ako bi račun mogao biti ugrožen, pokušajte se prijaviti sa drugog sigurnog uređaja i promijeniti lozinku ako još uvijek možete ili pogledajte zapise aktivnosti računa.
- Pazite na korištenje mreže (na Windows 10, možete vidjeti korištenje mreže po aplikaciji iu Task Manageru).
- Ako vaš uređaj ima alat za dijagnostičko ili sigurnosno skeniranje (kao što je Windows Security ili treća strana), koristite ga.

Ključ je da ostanete na oprezu. Jedna praksa OCD-a je da ohrabri osoblje da progovori ako se “njihov kompjuter ponaša čudno.” Bolje je istražiti lažne alarme nego propustiti pravi proboj. Don’t je dozvolio da potencijalna stigma prestane sa izvještavanjem; u sigurnosnoj obuci, naglasite da je pravovremeno izvještavanje kritično i da se oni neće kriviti za izazivanje zabrinutosti.

Sada kada znate šta treba tražiti, sljedeći korak je da djelujete brzo kada se nešto čini pogrešnim. Sljedeći odjeljci će pokriti korake trenutnog odgovora, koga pozvati u pomoć i kako se oporaviti.

Odziv korak po korak: Šta učiniti kada nešto krene po zlu

U trenutku kada shvatite da se sajber incident možda dešava, on je ključan za poduzimanje namjernih koraka za obuzdavanje i istragu problema. Paničarenje ili činjenje pogrešne stvari (kao što je odmah plaćanje otkupnine ili brisanje dokaza) može pogoršati stvari. Evo vodiča korak po korak koji je u skladu sa standardnim fazama odgovora na incidente (identificirajte, obuzdajte, iskorijenite, oporavite se) u pojednostavljenom smislu za CSO okruženje:

1. **Don't Panic, procijenite situaciju:** Udahnite i pokušajte razumjeti šta se dešava. Koji su znakovi I opseg? Na primjer, da li se jedan kompjuter ponaša čudno ili više puta? Je li problem s računom ili problem s uređajem? Identifikacija prirode incidenta vodi sljedeće korake. Zabilježite ono što ste primijetili (vrijeme, simptomi). Ako je potrebno, brzo napravite fotografije ili snimke ekrana sumnjivih poruka ili ekrana za greške pomoću telefona (koristite dokaze i kasnije pitajte stručnjake).

2. **Disconnect Pogođeni sistemi:** Ako sumnjate na aktivni zlonamjerni softver, posebno ako se podaci mogu ukrasti ili ako je više sistema zaraženo, odmah izolujte mašinu iz mreže. Isključite Ethernet kabl ili isključite Wi-Fi. Ovo sprečava širenje (npr. neki crvi ili ransomware pokušavaju da skoče na mrežne diskove) i zaustavlja daljinski upravljač ili eksfiltraciju podataka. Međutim, nemojte isključiti sistem osim ako ne morate – jednostavno isključiti mrežu. Postoje nijanse: isključivanje zaustavlja zlonamjerni softver, ali također može izbrisati nestabilne dokaze. Za većinu scenarija CSO-a, on je u redu da ga ostavite i isključite, a zatim pokrenete skeniranje. Ali ako ransomware aktivno šifrira datoteke pred vašim očima, možda ćete brzo krenuti da ga zaustavite. Koristite prosuđivanje; kada ste u nedoumici, isključenje mreže je dobar prvi potez.

3. **Osigurajte svoje račune:** Ako je nalog ugrožen (poput e-pošte ili društvenih medija), **pokušaj povratiti kontrolu**. Koristite tokove oporavka računa: odmah resetujte lozinke. Potpišite sve aktivne sesije (mnoge usluge imaju "dnevnik od svih uređaja" funkcija). Omogućite 2FA ako već ne (čak i ako haker još uvijek ima sesiju, kada ih izbacite, 2FA će pomoći da se zaustavi ponovna prijava). Obavijestite kolege da je račun kompromitovan, pa bi sve nedavne poruke trebali tretirati kao potencijalno lažne. Ako ne možete povratiti pristup (haker

je promijenio lozinku i zaključao vas), odmah kontaktirajte podršku provajdera usluga's kako biste prijavili preuzimanje računa.

4. **Obavijestite osobu zaduženu (i moguće svakoga):** Prema vašem sigurnosnom planu (iz poglavlja 3), trebali biste imati tačku ili tim za incidente. Obavijesti ih odmah. Ako si ti ta osoba, okupi relevantne ljude. Na primjer, ako je zajednički server pogođen, upozorite sve korisnike da ga ne koriste do daljnjeg. Ako je jedan zaposlenik's PC zaražen, možda ćete upozoriti druge da ne otvaraju e-poruke tog računara, itd. **Ne čuvaj tajnost incidenta** <TAG1> skrivanje može pogoršati štetu. Brza komunikacija omogućava drugima da budu oprezni ili poduzimaju zaštitne korake (kao što je promjena lozinki ako je potrebno). Također, ako imate IT podršku (u kući ili ugovoreni), pozovite ih ranije. Oni mogu početi pomagati u tehnološkim mjerama ili dubljim analizama.

5. **Sadržajte štetu:** Osim isključivanja mreže, evo koraka zadržavanja:
    - Ako je zlonamjerni softver na računaru, pokrenite antivirusno skeniranje u sigurnom načinu, ako je moguće, ili koristeći disk za spašavanje koji se može pokrenuti. Ovo može staviti u karantin zlonamjerni softver, zaustavljajući daljnju štetu. Međutim, prvo obuzdajte (neto isključeno), a zatim skenirajte – don't skeniranje dok ste još uvijek na mreži ako aktivni napadač možda gleda ili bi se dodatna korisna opterećenja mogla preuzeti.
    - Ako je ransomware I datoteke su šifrirane, identificirajte je li prestao ili još uvijek radi. Ubijte sumnjive procese preko Task Managera ako ih vidite (neki koriste očigledna imena, drugi su nasumični). Ali u ovoj fazi, vjerovatno je enkripcija brzo urađena. Zadržavanje tada znači karantin tog računara i ne dodirivanje datoteka (tako da forenzički stručnjaci ili alati za dešifriranje mogu pokušati da se oporave).
    - Ako je web stranica napadnuta (ukinuta ili hakovana), skinite je van mreže ako možete (npr. postavite stranicu za održavanje ili zamolite domaćina da privremeno suspenduje) kako biste spriječili daljnju štetu posjetiteljima i dali vam vremena da popravite.

- Za kršenje e-pošte, osim promjene lozinke, razmislite o kontaktima e-pošte kako biste ih upozorili na potencijalni phishing koji je došao s vašeg računa.
- Ako su podaci procurili (kao što nalazite svoju bazu podataka na stranici za pastu), ograničite pristup tim sistemima dok ne shvatite putanju eksploatacije i zakrpite je.

6. **Dokument Sve:** Kao što radite gore navedeno, vodite bilješke. Zapiši vremena, radnje koje si poduzeo I tko je obaviješten. Ako pronađete sumnjivi fajl ili ime procesa, obratite pažnju. Ova dokumentacija pomaže kasnije u oporavku, izvještavanju i poboljšanju vašeg sigurnosnog plana. It's također korisno ako uključujete policiju ili profesionalca za reagovanje na incidente; oni će se izjasniti da znaju slijed događaja.

7. **Potražite pomoć ako je potrebno:** Don't okleva da dobije pomoć izvana. Ako imate kontakt za sajber sigurnost (možda ih drugi CSO's IT, stručnjak za volontere ili telefon za pomoć u sajber sigurnosti), nazovite ih. Mnoge zemlje također imaju CERT (Computer Emergency Response Teams) koji mogu pomoći ili savjetovati čak i male organizacije. Postoje i besplatni resursi zajednice; na primjer, u slučaju ransomware-a, možete provjeriti web stranicu "No More Ransom" da vidite postoji li alat za dešifriranje za vaš soj. Ali primijenite samo renomirane alate – za bilo koji online savjet, osigurajte da je legitiman. Ako niste sigurni, pitajte svoje pouzdane IT savjetnike.

8. **Rezervišite dokaze (posebno za ozbiljne incidente):** Ako bi incident mogao uključivati zločin (npr., namjerni hak, značajnu krađu), kasnije možete uključiti policiju. U takvim slučajevima, očuvanje dnevnika i dokaza je ključno. Izbjegavajte brisanje sistemskih zapisa ili brisanje sistema dok se problem ne shvati i riješi. Ako morate obnoviti sistem, razmislite o tome da prvo napravite sliku diska. U manje kritičnim slučajevima, dokazi su i dalje korisni za učenje – npr., zadržavanje phishing e-pošte koja je nekoga prevarila, proučavanje i edukaciju drugih.

9. **Iskorijenite prijetnju:** Jednom sadržani, rad na uklanjanju. Za zlonamjerni softver: koristite AV da ga potpuno uklonite, ili u tvrdoglavim slučajevima, preformatirajte/ponovo instalirajte OS (početak svježeg je najsigurniji način ako imate rezervne kopije i on se ne navodi previše težak). Za kompromitovane račune: dvostruka provjera bez backdoor-a (kao što je

osiguranje u e-poruci da napadač nije postavio nova pravila prosljeđivanja kako bi tajno prosljeđivao poštu, često zanemaren trik). Provjerite druge račune jer ponekad jedan kred dobije mnogo –, na primjer, ako pretraživač sačuva lozinke, napadač bi ih mogao zgrabiti, tako da ćete možda morati promijeniti i druge račune' lozinke.

Ako je incident bio ranjivost (kao što je vaša web stranica imala zastarjeli dodatak koji je iskorišten), zakrpite ga ili uklonite. Ako je lažni insajder bio problem, očigledno, uklonite njihov pristup.

10. **Oporavite se i obnovite:** Nakon eliminacije neposredne prijetnje, počnite se vraćati u normalu:

- Vratite izgubljene ili oštećene podatke iz rezervnih kopija. Provjerite da li su sigurnosne kopije čiste (preskočite ih sa AV prije nego što se obnovi ako je moguće).
- Pažljivo spojite sisteme. Na primjer, nakon čišćenja računara, vratite ga na mrežu i pratite ako se nastavi bilo kakav sumnjivi izlazni saobraćaj (ako to učini, možda zlonamjerni softver nije u potpunosti nestao).
- Ako ponovo date račune ili promijenite akreditive, pobrinite se da svi ponovo mogu pristupiti onome što im je potrebno, s novim sigurnim lozinkama.
- Ako su operacije zaustavljene (kao što ste isključili server), koordinirajte ga kako biste ga pokrenuli tokom van špica za testiranje, osiguravajući da nema preostalog kompromisa.

11. **Komunicirajte ažuriranja:** Obavijestite osoblje o tome šta se dogodilo i šta se radi. Transparentnost gradi povjerenje I saradnju. Također, ako je relevantno, informirajte vanjske dionike prema potrebi (pogledajte sljedeći odjeljak o tome koga kontaktirati, npr., donatore ako su njihovi podaci provaljeni, itd.). Međutim, općenito, interna pitanja se mogu držati internim osim ako ne postoji potreba ili obaveza da se izvještava izvana.

Kroz ovaj proces, zadržite stav učenja, a ne krivice. Napadi se dešavaju najboljima od nas. Fokusirajte se na rješavanje i sprječavanje ponavljanja, a ne na to ko se zadržava ko je šta kliknuo (osim korištenja tih informacija za poboljšanje treninga).

Ovaj strukturirani odgovor – identifikuje, sadrži, iskorijenjuje, vraća – zrcala smjernice stručnjaka. Za male OCD-ove korake može učiniti jedna osoba koja nosi mnogo šešira, ali princip ostaje.

Zatim, hajde da detaljnije ispitamo kome ćete možda morati da pozovete ili da se javite, jer rukovanje incidentom može uključivati više strana nego samo vaša organizacija.

Kome se obratiti za pomoć: podrška resursima i dobijanje pomoći

Kada se bavite sajber incidentom, ne morate to sami da rešite. Postoji nekoliko mjesta i ljudi kojima možete obratiti pomoć, savjete i izvještavanje. Here's pregled resursa podrške:

Unutrašnji tim i IT podrška: Prvo, unutar vaše organizacije, uključite svakoga ko je odgovoran za IT ili sigurnost (vaše "techie" osoblje/dobrovoljač, ili osobu koja je postavila vaše sisteme). Ako imate pružaoca usluga kojim upravlja IT ili dobrovoljnog IT savjetnika, odmah ih kontaktirajte i opišite situaciju. Vjerovatno su vidjeli slične probleme i mogu ih voditi tehnički koraci. Čak I tehnološki pametan član odbora ili partner organizacija's IT osoba može biti vrijedan saveznik u štipanju.

Peer Networks i drugi OCD: Razmislite o diskretnom kontaktu sa sestrinskim organizacijama ili mrežama. Često, mreže OCD (na primjer, mreža za ljudska prava ili krovna organizacija OCD) mogu imati zajedničke resurse ili barem kolektivno znanje. Možda znaju za uobičajene prijetnje u vašem sektoru ili regiji i imaju preporuke (kao "Da, dva druga CSO-a su dobila istu phishing e-poštu; evo's ono što smo uradili"). Saradnja može biti moćna ovdje. Međutim, odmjerite koliko detalja podijeliti izvana – čuva osjetljive specifičnosti za pouzdane kontakte kako biste izbjegli bilo kakav rizik reputacije do službenog.

Pomoćne linije za kibernetičku sigurnost za civilno društvo: Postoje inicijative posebno za pomoć civilnom društvu u hitnim slučajevima digitalne sigurnosti. Značajan je **Access Now's Digital Security Helpline**, koji pruža besplatnu pomoć 24 sata dnevno, 7 sati, organizacijama civilnog društva, aktivistima I novinarima širom svijeta. Oni mogu pomoći u slučajevima kao što su napadi na web stranicu, kompromisi na računima, itd., često premošćujući stručne volontere ili dajući prilagođene smjernice. Ako se nađete u ozbiljnoj situaciji izvan svojih kapaciteta, ne ustručavajte se da pošaljete e-poštu ili nazovete takvu liniju za pomoć (Access Now's je [zaštićen e-pošti]). Oni održavaju povjerljivost i koriste se za rješavanje hitnih slučajeva.

Drugi primjer: **CyberPeace Institute's CyberPeace Builders** program nudi besplatnu pomoć u sajber sigurnosti od strane korporativnih volontera organizacijama civilnog društva. Ako ste već upisani ili povezani s njima, koristite taj kanal. Ako ne, možda nešto što treba uzeti u obzir za budućnost.

Sprovođenje zakona: Ovo zavisi od prirode incidenta:

- Ako se radi o značajnoj kršenju podataka koja uključuje krađu ličnih podataka ili namjerni hak, mogli biste razmisliti o obavještavanju lokalnih organa za provođenje zakona ili jedinice za sajber kriminal. Oni mogu istražiti, posebno ako je novac donatora ili osjetljive informacije ukraden, ili ako postoji iznuda (poput zahtjeva ransomware-a). Međutim, iskustva se razlikuju – na nekim mjestima, policija je od pomoći; u drugim, možda neće dati prioritet ili imati stručnost.
- U zemljama sa zakonima o obaveznom obavještavanju o kršenju (kao što je GDPR u EU, organima za zaštitu podataka moraju se prijaviti ozbiljna kršenja ličnih podataka u roku od 72 sata), trebali biste slijediti te propise. To znači informisanje relevantnih podataka Zaštitno tijelo, ako je primjenjivo, i moguće je da je uticalo na pojedince (više o tome u sljedećem odjeljku).
- Ako sumnjate da je napadač iz određene regije ili postoji obrazac koji utiče na više organizacija, policija bi ih mogla sastaviti.
- Napomena: Ako vaš CSO radi na osjetljivim pitanjima u zemlji u kojoj vlasti možda nisu prijateljske ili bi mogle zloupotrijebiti te informacije (na primjer, ako bi napad mogao biti sponzoriran od strane države), vi ćete se izjasniti pažljivo da biste izmjerili angažiranje organa za provođenje zakona. U takvim slučajevima, konsultacije sa međunarodnim tijelima (kao što je možda CERT u neutralnoj zemlji ili samo korištenje CSO linija za pomoć) mogu se u početku preferirati.

Nacionalni CERT/CSIRT: Mnoge zemlje imaju Tim za kompjuterski hitan odgovor (CERT) ili CSIRT, često pod gov ili akademskim kišobranom. Ponekad pomažu organizacijama (ne samo kritičnoj infrastrukturi). Neki imaju posebno oružje za mala preduzeća ili neprofitne organizacije. Na primjer, **CERT-ovi u EU** često odgovara na incidente i može davati savjete ili

koordinira sa organima za provođenje zakona. Ako imate kontakt ili možete lako prijaviti putem njihove web stranice, to bi moglo biti korisno. Oni također mogu upozoriti druge ili pratiti širenje kampanje zlonamjernog softvera.

Donatori ili partneri: Ako su uključeni podaci o projektu ili donatoru, ili ako je pogođena isporuka usluge, možda ćete morati obavijestiti partnere. Na primjer, ako vodite zajednički projekat i hakeri naruše web stranicu projekta, govoreći partneru iz drugog CSO-a da osigura da su svjesni i da mogu pomoći, ili barem nisu zatečeni nespremni. Donatori bi mogli imati zahtjeve za izvještavanje ako su sredstva pogođena (recimo, finansijska prevara). S druge strane podrške, neki donatori (posebno veći ili oni koji finansiraju kapacitete za sajber sigurnost) mogu imati resurse da vam pomognu. Ali pažljivo upravljajte komunikacijom – se fokusira na ono što se radi kako biste to riješili, a ne samo problem, kako biste zadržali povjerenje.

Osiguranje: Ako imate sajber osiguranje ili opću odgovornost koja pokriva sajber incidente, obavijestite osiguravajuću telefonsku liniju za incidente što je prije moguće (često je potrebna za pokriće). Oni mogu poslati profesionalne odgovore na incidente ili voditi sljedeće korake. Mnoge polise osiguranja zahtijevaju koordinaciju osiguravača za stvari kao što je plaćanje odluka o otkupninini. Ako nemate osiguranje, ovo se očigledno ne primjenjuje.

Resursi zajednice i interneta: Postoje online forumi kao što je **Reddit r/cybersecurity ili r/tech support** ili **StackExchange Security** gdje profesionalci ponekad pomažu. Ali budite oprezni da ne otkrivate osjetljive detalje na javnim forumima. Umjesto toga, mogli bi se pretraživati ti forumi kako bi se vidjelo da li su se drugi nosili s specifičnim zlonamjernim softverom ili greškom (često je neko objavio o toj specifičnoj bilješci o otkupninini ili ponašanju virusa, što može dati tragove o ispravkama). Web stranice kao **BleepingComputer** imaju namjenske odjeljke za pomoć u uklanjanju zlonamjernog softvera i specifične teme podrške ransomware-u, koje često moderiraju stručnjaci koji pomažu žrtvama besplatno. Često sarađuju i sa projektom NoMoreRansom. Ako idete tim putem, slijedite njihove smjernice (često traže objavljivanje log datoteka, itd. –, ali' ne rade ništa što vam nije ugodno; možda koristite pseudonim ako javno raspravljate o svom slučaju).

Kada i kako informirati pogođene pojedince/javnost: Ovo je više "koji treba obavijestiti i": ako procure lični podaci korisnika ili dionika, etička i eventualno pravna dužnost mogla bi vas

natjerati da obavijestite te pojedince kako bi se mogli zaštititi (npr., promijeniti svoje lozinke ako je njihov e-mail procurio, pazite na krađu identiteta). Izrada takvih komunikacija može biti nezgodna; trebalo bi da bude iskren, apologetski i da pruži smernice (kao ". Doživeli smo bezbednosni incident u kojem je vaša adresa e-pošte možda bila izložena. Budite oprezni prema sumnjivim e-mailovima i razmislite o promjeni lozinke ako je ponovo koristite ..."). Ako niste sigurni, konsultujte se sa savjetnikom za komunikacije ili pravnikom –, želite da postignete pravi ton i ne želite nehotice pogrešno priznati odgovornost, itd.

Psihološka podrška: Ovo može zvučati van teme, ali ozbiljan incident može biti stresan. Ljudi se mogu osjećati povrijeđeno ili krivo (osoba koja je kliknula na phishing mogla bi se osjećati užasno). On se ističe vrijednim rješavanja morala. Osigurajte da svi znaju da se greške dešavaju i fokusirajte se na napredovanje. Ako je pod ekstremnim stresom, možda napravite kratku pauzu ili naterajte nekoga da razgovara (čak i odricanje od kolege u drugom OCD-u koji je prošao kroz slično iskustvo može biti ohrabrujuće). Nakon što se stvari riješe, razmislite o sjednici o zaduženju koja podržava: razgovarajte o tome šta se dogodilo i kako pomoći jedni drugima da se nose i ojačaju.

U svim komunikacijama sa vanjskim subjektima, vodi evidenciju o tome koga ste kontaktirali i kada, i o bilo kojim brojevima slučaja/referenca ili datim savjetima. Ovo je dio dokumentacija i pomaže u praćenju.

Konačno, koristite ove kanale podrške ne samo tokom incidenta, već i nakon toga da se poboljšate. Na primjer, linija za pomoć Access Now mogla bi savjetovati koje korake treba poduzeti u budućnosti kako bi se izbjeglo ponavljanje, ili CERT može vam poslati njihov izvještaj i preporuke.

Sigurnost vraćanja: Koraci do oporavka

Nakon obuzdavanja incidenta i dobijanja pomoći, završna faza je vraćanje sistema u normalan rad i implementaciju mjera kako bi se spriječilo ponavljanje. Oporavak se ne odnosi samo na vraćanje podataka, već i na vraćanje povjerenja da je vaše okruženje ponovo čisto i sigurno.

Čisti i obnovljeni sistemi: Ako su bilo koje mašine zaražene, nakon uklanjanja zlonamjernog softvera, procijenite da li je potpuno vraćanje OS-a opravdano. Stručnjaci za sigurnost često sugeriraju da je za ozbiljne kompromise (poput rootkita ili nepoznatog zlonamjernog softvera) brisanje i rekonstrukcija najsigurniji način da se osigura da je sistem čist. Da, to potvrđuje dugotrajno vraćanje aplikacija i vraćanje datoteka, ali daje mir da nema skrivenih backdoor-a. Ako odlučite da to ne učinite, barem pokrenite više alata za skeniranje (jedan AV bi mogao propustiti nešto drugo ulov). Alati kao što su Malwarebytes, HitmanPro, itd., mogu se pokrenuti pored vašeg glavnog AV-a za drugo mišljenje. Osi se pobrinite da se OS potpuno zakrpi nakon čišćenja.

Za račune, nakon povratka pristupa, pregledajte postavke računa: da li je napadač postavio bilo kakva pravila prosljeđivanja, dodao e-poruke za oporavak ili 2FA uređaje? (Ovo je uobičajeno: npr., Gmail haker može dodati svoju e-poštu kao e-poštu za oporavak, pa čak i nakon promjene lozinke, pokušavaju povratiti račun.) Uklonite sve takve neovlaštene promjene. Provjerite filtere pošte, lozinke za aplikacije, povezane aplikacije – u osnovi sve u postavkama računa što bi moglo omogućiti nastavak pristupa.

Ako je web stranica hakovana, nakon što popravite ranjivost i restaurirate sadržaj, razmislite o premještanju na sigurniji host ili dodajte zaštitni zid web aplikacije (WAF). Moguće je da izvršite sigurnosnu reviziju koda ako je to prilagođena stranica. Također, promijenite sve baze podataka i FTP lozinke u slučaju da budu ugrožene.

Vratite podatke iz rezervnih kopija: Vratite sve izgubljene podatke. Na primjer, ako ste morali obrisati PC, izvadite njegove korisničke datoteke iz sigurnosne kopije (ali ih prvo skenirajte, samo u slučaju da zaražena datoteka vreba u dokumentima). Ako je baza podataka obrisana ili šifrirana, povratite najnoviju rezervnu kopiju. Testirajte da su obnovljeni podaci netaknuti i da sistemi koji ih koriste rade kako treba. Ponekad rezervne kopije nisu svježe koliko bismo željeli, tako da možete izgubiti malo posla. Nakon oporavka, neka osoblje brzo provjeri da li nešto nedostaje iz jaza, i ako jeste, vidi može li se ponovo ući ili ponovo prikupiti.

Ako je ransomware bio uključen i nemate rezervne kopije, oporavak je teži. Stručnjaci za konsultacije ili NoMoreRansom za alate za dešifriranje – ponekad postoje besplatna rješenja za određene ransomware sojeve. Plaćanje otkupnine se općenito obeshrabruje (obezbeđuje

kriminalce i nema garancije), ali neke organizacije čine taj težak izbor. Angažirajte policiju prije plaćanja, jer ponekad imaju ključeve ili mogu savjetovati. Ako na kraju dođe do gubitka podataka, planirajte kako obnoviti te podatke (možda kontaktirajte partnere da vam pošalju kopije datoteka koje imaju, itd.).

Poboljšanje i ažuriranje sigurnosnih mjera: Nakon proboja, mora se ojačati obrana. Ovo je "naučena" faza, gdje zakrpate rupe koje su iskorištene:

- Ako se radilo o phishingu, potrebno je očito više obuke i možda tehničkih kontrola (kao što je bolji filter za neželjenu poštu ili MFA provođenje). Na primjer, provedite da svi računi e-pošte imaju omogućeno 2FA i možda implementirajte upozorenje e-poštom za eksterne pošiljaoce (neki sistemi stavljaju "[eksterni]" u temu ako pošta dođe spolja, kako bi pomogla u uočavanju lažiranja).
- Ako je to bila slaba lozinka ili ponovo korištena akreditacija, pojačajte politiku lozinki (duža, jedinstvena) i razmislite o korištenju upravitelja lozinki u cijeloj organizaciji kako biste to pomogli. I definitivno 2FA o svemu kritičnom.
- Ako je zlonamjerni softver došao putem softvera bez zakrpe, osigurajte da se ažuriranja primjenjuju brže. Možda koristite alat za praćenje nedostajućih zakrpa ili se pretplatite na sigurnosne biltene relevantne za vaš softver.
- Ako je određena usluga bila izložena (kao otvoreni RDP port koji je dobio grubu silu), zatvorite je ili stavite iza VPN-a.
- Provjerite da li su vaša pravila zaštitnog zida pooštrena, nepotrebne usluge onemogućene (kao što smo pokrili u 4.4).
- Razmislite o segmentiranju svoje mreže ili podataka: npr., u budućnosti držite sigurnosne kopije na uređaju koji nije uvijek povezan tako da ga ransomware ne može pogoditi, ili odvojite osjetljive podatke na disk kojem ne mogu svi pristupiti.
- Implementacija boljeg praćenja: možda omogućiti evidentiranje sistema i postaviti upozorenja (postoje besplatni alati za praćenje dnevnika ili čak samo Windows Prosljeđivanje događaja za gledanje određenih događaja kao što je više neuspjelih prijava).

- Planirajte formalnu proceduru odgovora na incident ako nemate jedan – koji u osnovi zapisuje šta ste uradili ovog puta i poboljšava ga za sljedeći put (dio ažuriranja sigurnosnog plana).

Komunicirajte sa zainteresovanim stranama: Ako ste morali obavijestiti ljude o incidentu, nastavite jednom riješeno. Na primjer, obavijestite svoj odbor ili donatore: "Iskusili smo X, poduzeli smo korake Y i sada su operacije obnovljene. Implementiramo Z kako bismo osigurali da se ovo ne ponovi." Ova sigurnost i odgovornost mogu ojačati povjerenje ako se rade transparentno i kompetentno. Isto tako, ako su volonteri ili korisnici ranije bili obaviješteni da budu oprezni, kasnije ih obavijestite da je problem riješen: npr. Naša web stranica je sada sigurna i ponovo na mreži. Hvala na strpljenju."

Psihološki oporavak: Nakon proboja, moral tima bi mogao biti pogođen. Ljudi bi se mogli osjećati nelagodno ("Are, sigurni smo da hakeri još uvijek nisu u?") ili kriv. Imajte sastanak za razgovor kako biste otvoreno razgovarali o tome šta se dogodilo i tretirali ga kao priliku za učenje, a ne kao lov na vještice. Pohvalite brzo izvještavanje ili radnje koje su ograničile štetu. Možda imate malu radionicu 'naučene lekcije' u kojoj ažurirate sve o tome koje su nove mjere na snazi, što će ih također uvjeriti da su stvari sada sigurnije. Ton bi trebao biti: suočili smo se s izazovom i savladali ga, sada smo odlučni.

Dokumentacija i izvještavanje: Napišite interni izvještaj o incidentu – čak i ako je samo stranica. Vremenski okvir dokumenta, osnovni uzrok (ako je poznato), preduzete radnje i preporuke. Ovo je korisno za pamćenje (šest mjeseci kasnije, mogli biste zaboraviti detalje koji su važni ako se dogodi nešto slično) i za bilo kakve vanjske poslove. Ako je potrebno propisom (npr., GDPR), podnesete taj formalni izvještaj nadležnom tijelu, uključujući te detalje. Ako koordinirate sa kišobranom organizacija ili imaju obavezu prema donatorima (neki grantovi zahtijevaju prijavljivanje ozbiljnih događaja kao dio upravljanja rizikom), koristite interni izvještaj za odgovarajuću komunikaciju.

Planovi testiranja i ažuriranja: Kada je sve normalno, savršeno je vrijeme da poboljšate svoj sigurnosni plan i odgovor na incidente. Ažurirajte svoje kontakt liste (možda ste shvatili da nemate SerT's broj zgodan – sada sačuvajte ga). Ako bi određeni alat pomogao da se to otkrije ili zaustavi ranije, razmislite o implementaciji toga. Čak razmislite o provođenju male

“vatrogasne vježbe” u budućem –, na primjer, testirajte vraćanje rezervnih kopija ili imate simulirani phishing test da vidite da li se novi trening drži.

Zapamti to **potpuni oporavak uključuje vraćanje povjerenja**. Poverenje vašeg osoblja u sisteme, poverenje spoljnih partnera u vaše upravljanje. Transparentnost, akcija i praćenje pomažu u obnovi tog povjerenja. To pokazuje da ste to shvatili ozbiljno I poboljšali.

Konačno, vrijedi podijeliti znanje (bez osjetljivih detalja) sa zajednicom ako je prikladno. Na primjer, ako ste otkrili novu prevaru usmjerenu na OCD, upozorenje drugih putem mailing liste ili mreže može spriječiti da postanu žrtve – pozitivan ishod vašeg iskušenja.

Pomirično prolazeći kroz ove korake oporavka, ne samo da vraćate normalnost, već se idealno pojavljujete sa snažnijim sigurnosnim stavom. Mnoge organizacije smatraju da je kršenje bio poziv na buđenje koji ih je na kraju ostavio bolje pripremljenim za budućnost (iako je uvijek bolje poboljšati se bez bola incidenta!).

U ovom trenutku, mi smo sami pokrili kako da se nosi sa incidentima. Zatim ćemo se odlučiti da pređemo na moć saradnje i zajednice u očuvanju sigurnosti, što je često nedovoljno iskorišten aspekt sajber sigurnosti za civilno društvo.

Sažetak poglavlja

Ovo poglavlje naglašava ljudsku stranu sajber sigurnosti, zalažući se za kulturu svjesnu sigurnosti kroz obuku i politiku. Ističe da 74% kršenja uključuje ljudske greške, kao što je phishing, što obrazovanje osoblja čini kritičnim. OCD-ovi se vode za izvođenje osnovne obuke o sajber sigurnosti, pokrivanje upravljanja lozinkama i uočavanje phishing e-poruka, koristeći vježbe poput phishing kvizova. Poglavlje pruža savjete o izradi prihvatljivih politika korištenja uređaja i podataka, osiguravajući jasna pravila za osoblje i volontere. Takođe navodi protokole za incidente izvještavanje, podsticanje brze komunikacije za suzbijanje kršenja. Primjeri uključuju osoblje za obuku civilnog društva da prijavi sumnjive mejlove, sprečavajući napad zlonamjernog softvera. Poglavlje naglašava ulogu liderstva u modeliranju sigurnih praksi (npr. korištenje 2FA) kako bi se legitimizirali napori. Preporučuje nagrađivanje budnosti, poput hvale osoblja za prijavu phishinga, kako bi se ojačale navike. Ugrađivanjem sigurnosti u svakodnevne tokove rada, OCD stvaraju otpornu kulturu. Fokus poglavlja’s na jednostavne, inkluzivne prakse

osigurava dostupnost za svo osoblje, usklađujući se sa modelom "voza-trenera" i ciljem e-knjige’s podsticanja dugoročnih sigurnosnih navika.

Non- Kontrolna lista za sigurnost tehničkih stranica za OCD

Ova kontrolna lista ovlašćuje programsko osoblje i volontere da provjere i poboljšaju sigurnost web stranice vašeg CSO'sa bez potrebe za tehničkom stručnošću. Ovi koraci pomažu u zaštiti vaše web stranice od napada (npr., defacement, DDoS) i osiguravaju da ona ostane pouzdana platforma za vašu misiju:

1. Provjerite da li vaša web stranica koristi HTTPS

☐ Posjetite svoju web stranicu i potražite ikonu katanaca u adresnoj traci pretraživača's (prije URL-a) ili "https://" na početku adrese.

☐ Ako vidite "http://" ili "Not Secure" upozorenje, kontaktirajte svoj web host kako biste omogućili HTTPS (npr. zatražite besplatan Let's Encrypt certifikat).

☐ Primjer: Vaša stranica je "www.CSOexample.org". Osigurajte da adresna traka pokazuje "https://www.CSOexample.org" sa katanac.

☐ Ako HTTPS nedostaje, pošaljite e-poštu svom web hostu: "Molimo omogućite HTTPS za našu web stranicu."

2. Potvrdite redovne sigurnosne kopije

☐ Pitajte svog web hosta ili menadžera web stranice da li je vaša web stranica redovno podržana (npr., svakodnevno ili sedmično) i gdje se čuvaju sigurnosne kopije (npr., oblak ili vanjski server).

☐ Zahtijevajte vraćanje testa kako biste osigurali da rezervne kopije funkcioniraju (npr., pitajte, "Možete li vratiti našu stranicu na verziju prošle sedmice's?").

☐ Primjer: Vaša web stranica je isključena nakon napada. Nedavna rezerva vam omogućava da ga brzo vratite.

☐ Kontaktirajte svog domaćina: "Imamo li automatske sigurnosne kopije web stranica? Koliko često se rade?"

3. Provjerite ažuriranja softvera web stranice

☐ Provjerite sa svojim web hostom ili menadžerom web stranice ako se sistem upravljanja sadržajem (CMS, npr., WordPress, Joomla) i dodaci/teme redovno ažuriraju.

☐ Pitajte da li su ažuriranja automatska ili ih neko provjerava mjesečno.

☐ Primjer: Zastarjeli dodatak WordPress-a doveo je do hakovanja CSO's stranice. Redovna ažuriranja to sprečavaju.

☐ Pošaljite e-poštu svom domaćinu: "Da li su naši CMS i dodaci ažurirani? Ako ne, molimo omogućite automatske ažuriranja."

4. Sigurni pristup administratorima

☐ Osigurajte da samo osoblje od povjerenja ima pristup administratoru web stranice. Provjerite kod svog menadžera web stranice da uklonite pristup bivšem osoblju ili volonterima.

☐ Provjerite da admin nalozi koriste jake lozinke (npr. 14+ znakova, kao što je "sunbird&glass7rain") i dvofaktorsku autentifikaciju (2FA).

☐ Primjer: Stara prijava bivšeg volontera's korištena je za klevetu lokacije. Uklanjanje neiskorištenih računa to sprečava.

☐ Pitajte svog menadžera web stranice: "Ko ima pristup administratoru? Možemo li ukloniti stare račune i omogućiti 2FA?"

5. Provjerite za sumnjive promjene web stranice

☐ Posjetite svoju web stranicu i potražite neobičan sadržaj (npr. čudan tekst, nepoznate slike ili preusmjeravanje na druge stranice).

☐ Prijavite bilo kakvo čudno ponašanje svom web hostu ili IT kontaktu odmah.

☐ Primjer: početna stranica CSO's preusmjerena na stranicu za prevare zbog hakovanja. Rano izvještavanje ga je brzo popravilo.

☐ Pregledajte svoju stranicu i zabilježite bilo šta neobično. Kontaktirajte svog domaćina: “Naša stranica ima [izdanje]; molimo istražite.”

6. Zaštita od DDoS napada

☐ Pitajte svog web voditelja da li pružaju DDoS (Distributed Denial of Service) zaštitu kako bi vaš sajt bio na mreži tokom saobraćajnih poplava.

☐ Potvrdite da li su osnovne zaštite (npr. Cloudflare’s besplatni plan) omogućene.

☐ Primjer: Stranica za ljudska prava CSO’s je isključena tokom DDoS napada. Besplatna DDoS zaštita ga je održavala.

☐ Pošaljite e-poštu svom domaćinu: “Imamo li DDoS zaštitu? Možemo li omogućiti besplatnu uslugu kao što je Cloudflare?”

7. Ograničite javni pristup osjetljivim stranicama

☐ Provjerite jesu li osjetljive stranice web stranice (npr. prijava administratora, interni dokumenti) zaštićene lozinkom ili skrivene od pogleda javnosti.

☐ Zamolite svog menadžera web stranice da ograniči pristup samo ovlaštenim korisnicima.

☐ Primjer: lista donatora CSO’s slučajno je objavljena. Zaštita lozinkom stranice riješila je problem.

☐ Pitajte: “Jesu li osjetljive stranice poput zaštićenih administrativnih prijava? Možemo li dodati lozinke ako je potrebno?”

8. Osoblje voza za bezbednu upotrebu web stranice

☐ Podsjetite osoblje i volontere da ne dijele administrativne akreditive ili ne objavljuju osjetljive informacije (npr. podatke o donatorima) na web stranici.

☐ Podijelite brzi savjet: “Uvijek se odjavite iz administrativnog panela web stranice nakon upotrebe.”

☐ Primjer: Član osoblja podijelio je administrativnu lozinku u e-poruci, što je dovelo do hakovanja. Trening to sprečava.

☐ Pošaljite e-poštu timu: “Never dijeli detalje o prijavi web stranice. Odjavite se nakon uređivanja stranice.”

POGLAVLJE 6: SARADNJA I PODRŠKA DIGITALNOJ SIGURNOSTI

Jači zajedno: Saradnja i podrška

Digitalna sigurnost nije samo individualni ili organizacioni napor; to je kolektivni poduhvat. Organizacije civilnog društva mogu imati velike koristi od zajedničkog rada, dijeljenja znanja i podrške jedna drugoj suočene s sajber prijetnjama. U ovom poglavlju raspravljamo o tome kako saradnja može poboljšati sigurnost – od razmjene informacija sa vršnjačkim OCD-ovima i izgradnje kulture sigurnosti u zajednici, do edukacije javnosti i prisluškivanja lokalnih i međunarodnih mreža podrške.

Dijeljenje informacija sa drugim OCD

Nijedan OCD nije ostrvo, posebno u digitalnom carstvu. Često napadi ili rizici koji ciljaju na jednu organizaciju mogu uticati i na druge u istom sektoru ili regionu. Dijeljenjem informacija o prijetnjama i najboljim praksama, OCD mogu kolektivno poboljšati svoju odbranu.

Zašto dijeliti? Možda postoji oklijevanje da se sigurnosni incidenti podijele iz sramote ili straha da će to otkriti ranjivost. Međutim, koristi obično nadmašuju rizike kada se rade u pravom okruženju. Ako je vaš CSO postao žrtva phishing kampanje, obavještavanje drugih može im pomoći da izbjegnu tu zamku. Slično je komšijskom satu: ako je jedna kuća na meti prevare, upozoravaju komšije. U sajber sigurnosti, ovaj koncept **dijeljenje informacija** formaliziran je u nekim sektorima preko ISAC-a (Centri za razmjenu i analizu informacija). Dok formalni ISAC postoje za industrije kao što su finansije ili zdravlje, OCD mogu stvoriti vlastite neformalne krugove ili grupe za razmjenu.

Šta i kako podijeliti:

- **Upozorenja o prijetnjama:** Ako naiđete na određenu phishing e-poštu, zlonamjernu datoteku ili sumnjivi pristup (kao što je neko imitirao donatora), možete podijeliti indikatore: npr., “. Primili smo e-poštu sa adrese X sa subjektom Y koji je bio zlonamjeran. Budite na vidikovcu.” Dajte dovoljno detalja da ga drugi prepoznaju. Neke mreže civilnog društva postavile su liste e-pošte ili sigurne grupe za ćaskanje za takva upozorenja.

- **Taktika i lekcije:** Nakon što doživite incident ili čak vježbu, podijelite ono što ste naučili, možda anonimizirajući osjetljive dijelove. Na primjer, mogli biste podijeliti: “Mi smo implementirali dvofaktorsko autorstvo na sve naše račune i blokirao je višestruke neovlaštene pokušaje prijave. Vrijedilo je truda.” Ovo motivira druge da usvoje slične mjere.
- **Politike i materijali za obuku:** Promjena resursa kao što su politike sigurnosti uzorka ili klizni špilovi za obuku može biti obostrano korisna. Jedan CSO bi mogao imati sjajnu osnovnu “Cybersecurity 101 za prezentaciju osoblja” koju bi mogli distribuirati drugima za prilagođavanje, umjesto da svi ponovo osmisle točak.
- **Kontakti za pomoć:** Ako imate dobro iskustvo sa konsultantom za sigurnost ili IT volonterom, možda ćete podijeliti taj kontakt sa kolegom iz OCD-a u nevolji (uz dozvolu, naravno). Slično, ako član OCD-a pohađa radionicu o sajber sigurnosti ili webinar, može prenijeti ključne stvari za poneti vršnjacima koji nisu mogli prisustvovati.
- **Zajedničke vježbe:** Moguće je organizirati zajedničke događaje poput sigurnosne obuke za više organizacija ili čak simulirane phishing vježbe među nekoliko OCD-a. Ovo ne samo da poboljšava vještine, već i podstiče povjerenje među učesnicima.

Izgradnja povjerenja za dijeljenje: Sigurnosni podaci su osjetljivi. Da biste iskreno podijelili (“we je hakovan X metodom, izgubljen Y data”), potrebno vam je povjerenje da vršnjaci neće zloupotrebiti te informacije ili oštro suditi. Uspostaviti normu povjerljivosti. Možda prvo formirate malu, pouzdanu grupu (kao unutar koalicije ili radne grupe OCD-a koji se poznaju) prije nego što se povećate šire. Neke zajednice uspostavljaju pravilo Chatham House (možete koristiti informacije, ali ne otkrivaju ko je to rekao). Neki čak mogu pažljivo potpisati jednostavan memorandum o rukovanju zajedničkim informacijama. Vremenom, kako se dešavaju korisne razmjene, povjerenje raste.

Upotreba platformi: Neke platforme i alati mogu olakšati sigurno dijeljenje:

- Šifrovane liste e-pošte (koristeći usluge ili PGP ako svi učesnici mogu da upravljaju njime, iako je PGP nezgodan).
- Grupe za razmjenu poruka o Signalu ili sličnim aplikacijama za brzo praćenje hitnih problema.

- Moguće je da koristite platformu kao **Raketa. Chat** ili **Matrica/Element** da bi stvorili zatvoreni forum za OCD (samohodne ili pouzdane servere) gdje mogu razgovarati o sigurnosnim temama daleko od očiju javnosti.
- Neke mreže bi mogle biti partner sa CERT-ovima kako bi ih nahranile anonimnim informacijama i zauzvrat dobile savjete.

Uspješni primjeri: Bilo je inicijativa kao što je **"CyberPeace Cafe"** ili CSO sastanci o sigurnosti. Takođe, takođe **NetHope** (konzorcij humanitarnih organizacija civilnog društva) radi na zajedničkim smjernicama za kibernetičku sigurnost i informacijama o incidentima, tretirajući infrastrukturu civilnog društva kao kritičnu. Druga je "Organizacija za razmjenu i analizu informacija (ISAO) za koncept CSOs" koji su neki iznijeli. U Evropi, u okviru projekata EU (kao što je možda kontekst ovog nastavnog plana i programa), partnerski OCD-ovi mogli bi postaviti zajednički dnevnik incidenata ili Slack kanal posebno u tu svrhu.

Dijeljenjem pravovremenih informacija, OCD mogu **transformiši napad na jednog u rano upozorenje za sve**. Takođe efikasno koristi oskudnu stručnost –, jedna IT osoba u vodećem OCD-u može efikasno služiti kao savetnik nekoliko partnera kroz razmenu znanja.

Izgradnja zajednice za sigurnost

Osim reaktivne razmjene informacija, OCD mogu proaktivno stvoriti kulturu zajednice koja daje prioritet digitalnoj sigurnosti. Zajednica koja podržava može udružiti resurse, potaknuti učenje i pojačati zagovaranje boljih sigurnosnih alata i politika.

Mreža sigurnosnih šampiona: Identificirajte ljude unutar lokalnog civilnog društva koji imaju interes ili vještine za sajber sigurnost. Oni bi mogli biti tehničko osoblje, volonteri s IT iskustvom ili simpatični akademici. Formirajte lokalnu "sigurnosnu šampionsku grupu" koja se sastaje povremeno (čak i virtuelno) kako bi razgovarala o pitanjima i rješenjima. Ovi šampioni tada mogu djelovati kao tačkaste osobe u svojim organizacijama. Na primjer, možda jedan IT službenik CSO-a uči druge kako da očvrsnu svoje Wi-Fi mreže, dok drugi koji je saznao za GDPR dijeli savjete o usklađenosti.

Radionice i događaji obuke: Organizujte treninge u zajednici, pozivajući više OCD. Možda tromjesečna radionica o temama kao što su "Using Password Managers," "Securing

Mobile Communications," ili "How to Respond to the Cyberincident" – od kojih veliki dio dolazi iz sadržaja ove knjige's. Zajedničkom obukom, osoblje OCD ne samo da stiče znanje već i upoznaje vršnjake, što može činiti osnovu povjerenja za razmjenu informacija o kojima smo razgovarali. Često možete natjerati stručnjake (sa univerziteta, kompanija ili državnih CERT-ova) da dođu na ove radionice niski ili nikakvi troškovi za neprofitne organizacije kao dio CSR-a ili društveno korisnog rada. Postoji moć u brojevima –, korporativni trener možda neće napraviti besplatnu sesiju za jedan OCD pet ljudi, ali za kolektivnu publiku od 50 od raznih organizacija civilnog društva, mogli bi.

Podrška vršnjacima i mentorstvo: Ohrabrite sistem prijatelja: možda uparite manji OCD koji nema IT podršku sa većim OCD koji ima IT odjel za neko mentorstvo. Na primjer, OCD koji je uspješno implementirao sigurnost oblaka može mentorirati još jedan upravo početak. Ovo može biti neformalno, ali pruža brzu pomoć kada je to potrebno ("Hey, kako ste implementirali 2FA za svo osoblje? Možete li nam pokazati?").

Podešavanje resursa: Razmotrite zajedničku nabavku ili razmjenu alata. Grupa OCD-a može dobiti veliki popust na sigurnosni softver ili podijeliti pretplatu (u skladu sa uslovima licence). Alternativno, ako CSO ima rezervni server ili sigurnosni uređaj, možda drugi mogu koristiti kapacitet na njemu. U nekim kontekstima, OCD su uspostavili zajedničke IT usluge (kao što je uobičajeni sigurni server e-pošte ili zajednički IT helpdesk u tri ili četiri organizacije) kako bi zajednički priuštili kvalitetniju sigurnost nego što bi svaka mogla pojedinačno.

Zagovaranje zajednice: Takođe postoji uloga za OCD da se kolektivno zalažu za bolje uslove sajber bezbednosti. Na primjer, lobiranje kod donatorske zajednice za financiranje izgradnje kapaciteta kibernetičke sigurnosti ili tjeranje dobavljača softvera da ponude bolje neprofitne cijene ili funkcije (neke neprofitne koalicije natjerale su Microsoft ili Google da uključe besplatne sigurnosne dodatke za OCD). Osim toga, podizanje svijesti s provajderima internetskih usluga ili vlastima o prijetnjama civilnom društvu (poput sofisticiranih aktivista za ciljanje phishinga) može dovesti do širih zaštitnih mjera. Zamislite koncept "civilnog društva kao kritičnu infrastrukturu" koju je NetHope opisao – udruživanjem, OCD-ovi mogu tvrditi da im je potrebna zaštita slična vladi ili industriji i na taj način privući podršku.

Solidarnost u odgovoru na incidente: Kada se dogodi veliki incident (kao što je OCD pogođen ozbiljnim napadom ili se suočava sa uznemiravanjem na mreži, itd.), zajednica je jača pred njom. Drugi OCD mogu pomoći u ljudstvu, podijeliti teret javnih poruka ili pružiti privremene usluge. Postoje slučajevi, npr., kada je jedna grupa za ljudska prava napadnuta DDoS, drugi su odražavali sadržaj svoje web stranice kako bi bio dostupan (kao što je digitalna solidarnost). Takva kooperativna odbrana pokazuje protivnike da će napad na jednog okupiti mnoge druge, što može biti odvraćanje.

Dijeljenje priča o uspjehu: U izgradnji pozitivne zajednice, dijele i priče o uspjehu (kao što će biti istaknuto u Poglavlju 7). Ako se jedan OCD uspješno odbranio od pokušaja krađe identiteta zahvaljujući treningu, proslavite to u biltenu zajednice. Motiviše sve da se ulaganje u sigurnost isplati. Prepoznajte i zahvalite onima koji pomažu drugima u sigurnosti (možda na godišnjoj konferenciji OCD-a, pohvalite onog IT volontera koji besplatno putuje oko instaliranja antivirusa u različitim OCD-ovima –, takva vrsta podizanja morala podstiče kontinuiranu podršku).

Razvijanjem usko povezane zajednice oko sigurnosti, OCD se kreću od izolovanih, ranjivih ciljeva do otporne mreže. Napadači (bilo kriminalci ili opresivni režimi) često se oslanjaju na odabir izolovanih organizacija; ujedinjeni front znači da se informacije o njihovoj taktici brzo šire, a odgovori se mogu koordinirati. Kako jedna maksima ide, “Postoji sigurnost u solidarnosti.”

Informisanje javnosti: Podizanje svijesti o digitalnoj sigurnosti

OCD često služe kao edukatori i zagovornici u zajednici. Digitalna sigurnost nije samo interno pitanje; mnogi ljudi s kojima radite (korisnici, članovi zajednice, aktivisti, itd.) također bi mogli imati koristi od bolje sigurnosne svijesti. Proširujući znanje o digitalnoj sigurnosti na svoju širu zajednicu, pomnožite utjecaj i pomažete u stvaranju sigurnijeg okruženja civilnog društva.

Radionice i obuka zajednice: Razmislite o održavanju javnih radionica ili webinara o osnovnoj digitalnoj sigurnosti za svoju publiku. Na primjer, ako ste osnovali omladinsku organizaciju, pokrenite sesiju na “Staying Safe on Social Media” za tinejdžere i njihove roditelje, pokrivajući postavke privatnosti, cyber maltretiranje, phishing, itd. Ako radite sa braniteljima ljudskih prava, možda obuku o sigurnoj komunikaciji (koristeći Signal, izbjegavajući nadzor). Ove sesije se mogu integrisati u vaše redovno programiranje. Mnogi OCD-ovi već rade obuku o

srodnim temama (npr., medijskoj pismenosti, privatnosti na mreži) – možete uključiti module iz ovog nastavnog plana i programa. Pružanje takvog obrazovanja ne samo da pomaže zajednici, već i pozicionira vaš OCD kao lidera u rješavanju savremenih pitanja, što može ojačati vašu reputaciju i povjerenje.

Razvijajte jednostavne obrazovne materijale: Mogli biste kreirati ili prilagoditi letke, infografiju ili postove na blogu na sigurnosnim savjetima i javno ih podijeliti. Na primjer, jednoznačni pod nazivom "5 načina zaštite sebe na mreži" s lakim koracima (koristite jake lozinke, ne kliknite na sumnjive veze, ažurirajte softver, itd.), koje distribuirate na događajima ili na društvenim mrežama. Vizuelno, netehničko jezik najbolje funkcionira za javnu publiku. Možete prilagoditi sadržaj iz nacionalnih kampanja podizanja svijesti o sajber sigurnosti (Materijali mjeseca kibernetičke sigurnosti u oktobru često su besplatno dostupni na više jezika putem ENISA-e ili drugih). Osigurajte da su materijali na lokalnom jeziku i kontekstualno relevantni (milione lokalne prevare koje ljudi vide, kontakti lokalne podrške). Ovo bi se također moglo vezati za vas misija organizacije – npr., OCD o pravima potrošača koji podučava o izbjegavanju online prijevara.

***Kampanje za javnu svijest*:** Ako resursi dozvole, pokrenite kampanju oko digitalne sigurnosti. Ovo bi se moglo vezati za nešto poput Sigurnijeg dana interneta ili nekog relevantnog lokalnog razvoja (recimo, porast SMS prevara u vašem području). Koristite svoje komunikacijske kanale da redovno podsjetite pratioce na sigurnost (tweet sigurnosni savjeti, podijelite vijesti o trenutnim prevarama na koje treba paziti, itd.). Neki OCD-ovi su partneri sa telekom kompanijama ili medijima kako bi emitovali sigurnosne PSA poruke. Čak i kampanja malih razmjera, poput objavljivanja sedmičnog "Security Tip Tuesday" na vašoj Facebook stranici, može polako podići svijest.

Leverage Media and Storytelling: Ljudi razumiju kroz priče. Ako je prikladno, podijelite anonimne priče o digitalnim incidentima i kako su oni prevaziđeni (možda kao dio bloga ili razgovora). Na primjer, priča o tome kako je e-mail vođe zajednice hakovan i korišten za slanje lažnih poruka i šta je naučeno iz toga. Može humanizirati problem i upozoriti druge da budu oprezni. Mediji bi također mogli biti zainteresovani ako postoji trend (kao što je sve veće ciljanje

organizacija civilnog društva ili aktivista na mreži); intervju sa vašim OCD-om na tu temu može naglasiti važnost digitalne sigurnosti široj publici.

Lobi za bolje politike i podršku: Na višem nivou informišite javnost i kreatore politike o potrebama civilnog društva u sajber bezbednosti. OCD se mogu kolektivno zalagati za vladine programe koji pomažu OCD-ovima u sajber sigurnosti (neke zemlje imaju programe grantova ili poseban kontakt sa CERT-om). Također se zalažete za sigurnost prilagođenu korisniku u tehnološkim proizvodima – npr., gurajući softverske kompanije da osiguraju sigurne postavke kao zadane kako bi korisnici bili sigurniji bez potrebe za opsežnom stručnošću. U EU, na primjer, postoje dijalozi o zaštiti civilnog društva od sajber prijetnji; glasovi CSOs' na tim forumima osiguravaju da ih mjere politike uključuju (poput finansiranja i obuke).

Saradnja sa školama I bibliotekama: Možda će biti partner s lokalnim obrazovnim institucijama ili bibliotekama kako bi ugostili zajedničke sesije o digitalnoj pismenosti i sigurnosti. Mnoge javne biblioteke održavaju časove računara; ponuda sigurnosnog segmenta mogla bi biti dobrodošla. Škole sve više moraju da predaju onlajn bezbednost; OCD sa ekspertizom mogu podržati taj nastavni plan i program. Pomažući u obrazovanju mladih i šire javnosti, gradite društvo koje je svjesnije sigurnosti, koje indirektno štiti i vaše OCD (manje kompromitovanih ličnih računa koji bi mogli dovesti do krađe krađe vaše organizacije itd.).

Podsticaj izvještavanje i dijalog: Pozovite javnost s kojom se bavite da prijavi sajber kriminal ili sumnjive incidente. Mnogi pojedinci pate tiho ili se previše stide (kao da je neko pao na prevaru). Stvorite klimu u kojoj ljudi mogu tražiti pomoć –, možda vaš CSO može poslužiti kao posrednik koji će ih voditi policiji ili telefonskim linijama ako su žrtve uznemiravanja ili prijevare na mreži. Neki OCD preuzimaju ulogu zagovornika digitalnih prava, naglašavajući pitanja poput privatnosti ili nadzora u društvu, koja su u korelaciji sa sigurnosnom svijesti.

U skladu sa svojom misijom: Krojačko obrazovanje javne sigurnosti u skladu sa vašom misijom koherentnosti. Na primjer, ako se vaš CSO bavi pravima žena i znate da se aktivistkinje suočavaju s uznemiravanjem na mreži, fokusirajte svijest o tome i kako se nositi s tim (blokirati/prijavljivati funkcije, održavati privatnost). Ako ste ekološki OCD, mogli biste naglasiti kako se lažne informacije šire na mreži i osnovne prakse verifikacije – susjednu sigurnosnu temu (integritet informacija).

Obavještavajući javnost, OCD obavljaju dvostruku uslugu: štiteći svoje birače i jačajući vlastitu sigurnost podizanjem cjelokupnog sigurnosnog "higijenskog" okruženja u kojem posluju. Stvara vrli ciklus u kojem je manja vjerovatnoća da će svjesna zajednica biti vektor ili žrtva kibernetičara.

Ukratko, znanje je moć, a OCD, kao pouzdani entiteti zajednice, dobro su u poziciji da šire tu moć.

Lokalni i međunarodni resursi podrške

Pored vršnjačke saradnje i javne svijesti, postoje formalni resursi za podršku dostupni OCD-ima na lokalnom, regionalnom i međunarodnom nivou. Znajući šta je ovo a kako im pristupiti može pružiti prijeko potrebnu pomoć, posebno kada se suočite s sofisticiranim prijetnjama ili su vam potrebni resursi izvan vaših kapaciteta.

Lokalni resursi:

- **Nacionalne agencije za kibernetičku sigurnost/CERT:** Kao što je ranije spomenuto, mnoge zemlje imaju nacionalni CERT (Tim za hitne slučajeve računara) ili agenciju za sajber sigurnost koja nudi smjernice. Neki imaju programe fokusirane na OCD ili mala preduzeća. Na primjer, Nacionalni centar za kibernetičku sigurnost Ujedinjenog Kraljevstva (NCSC) pruža besplatne smjernice, pa čak i neke besplatne usluge (kao što su web provjera, provjera pošte) za poboljšanje sigurnosti organizacija. Provjerite ima li vaš country's CERT pristup ili resurse na vašem jeziku (često objavljuju biltene upozorenja koje možete slijediti).
- **Jedinice za sajber kriminal za provođenje zakona:** Ako se suočite s problemima poput online prijevare, uznemiravanja ili ciljanog napada, lokalne policijske sajber jedinice mogu pomoći. Neke zemlje imaju posebne jedinice koje rade sa civilnim društvom (posebno u kontekstu zaštite novinara ili aktivista). Izgradite vezu ako je moguće – možda pozove službenika da govori na forumu OCD o izvještavanju o sajber incidentima, tako da demistificirate proces.
- **Akademske institucije:** Lokalni univerziteti, posebno oni sa IT ili odsjecima za kibernetičku sigurnost, mogu biti saveznici. Profesori ili studenti mogu preuzeti sigurnost OCD kao dio istraživačkih ili volonterskih projekata. Na primjer, univerzitetski IT klub može izvršiti

sigurnosnu reviziju za vaš OCD kao klasni projekat (uz vaš pristanak i pod nadzorom). Neki univerziteti vode klinike za kibernetičku sigurnost ili imaju inkubatore za rješenja socijalne tehnologije.

- **Lokalni uredi tehnoloških kompanija:** Velike tehnološke kompanije često imaju lokalno prisustvo i programe korporativne društvene odgovornosti (CSR). Ponekad vode radionice digitalne pismenosti ili sigurnosti (Googleova online sigurnosna obuka, Metina kampanja digitalne pismenosti, itd.). Pristupite im da uključite svoje osoblje ili korisnike OCD-a u te besplatne treninge. Oni također mogu donirati ili sniziti sigurnosne proizvode. Na primjer, Cisco je donirao hardver zaštitnog zida nekim neprofitnim organizacijama kroz partnerstva.
- **Organizacije za podršku OCD:** Entiteti kao što su tehnološke federacije ili udruženja (npr. TechSoup – globalni CSO koji pruža sniženi softver, uključujući sigurnosne pakete; u Evropi, možda postoji Evropska mreža sigurnosti civilnog društva itd.). TechSoup, konkretno, nudi ne samo softver već I resursi za izgradnju kapaciteta, a ponekad i webinari o sigurnosti. Nacionalne mreže OCD-a mogu imati i radne grupe na ICT-u, gdje možete dobiti savjete.

Međunarodni resursi:

- **Access Now-ova linija za digitalnu sigurnost:** Već spomenut, to je globalno dostupan tim za brzo reagovanje civilnog društva 24 sata dnevno. Djeluju na više jezika (24/7 na engleskom, španskom, francuskom i drugim jezicima). Oni mogu pomoći u bilo čemu, od smjernica za uklanjanje zlonamjernog softvera do ublažavanja DDoS-a do povrata računa. Besplatno je I povjerljivo.
- **CyberPeace Institute:** Ova organizacija ne samo da analizira sajber napade na civilno društvo, već i koordinira pomoć. Njihov program CyberPeace Builders ima volontere tehnoloških kompanija koje nude pro-bono pomoć OCD-ima širom svijeta. Možete se prijaviti da budete korisnik njihovog programa, koji bi vam mogao dati ponavljajuću stručnost, poput pomoći u uspostavljanju sigurne infrastrukture ili politika.
- **Međunarodne slobode izražavanja/Krpe za prava digitalnih prava:** Grupe kao što su Front Line Defenders, The Engine Room, EFF (Electronic Frontier Foundation) i druge često objavljuju vodiče ili vas mogu povezati sa stručnjacima. Na primjer, Front Line Defenders

ima “Digital Protection” program i Security in a Box komplet alata prilagođen braniteljima ljudskih prava (sa alatima i taktikama).

- **Programi finansirani donatorima:** Ponekad postoje projekti koje finansiraju donatori posebno za podizanje sajber otpornosti civilnog društva. Na primjer, u EU su postojali projekti pod Erasmus+ ili CEF-om koji se fokusiraju na poboljšanje digitalnih vještina, uključujući sigurnost za neprofitne organizacije (kao što je možda projekat KA220 u vašem naslovu jedan). Pazite na pozive ili mreže u okviru takvih projekata; često proizvode alate, treninge domaćina ili nude konsultacije za OCD koji učestvuju.
- **Forumi i konferencije:** Na međunarodnom nivou, konferencije kao što su RightsCon, Internet Governance Forum (IGF) ili regionalne konferencije o sajber sigurnosti ponekad imaju tragove civilnog društva. Učešće vas može povezati sa globalnom zajednicom I resursima. RightsCon se posebno odnosi na digitalna prava i sigurnost za aktiviste. Mnoge sesije daju korisne savjete ili dovode do finansijera koji bi mogli podržati vaša sigurnosna poboljšanja.
- **Mogućnosti finansiranja:** Međunarodne fondacije prepoznale su sajber sigurnost kao kritičan kapacitet za civilno društvo. Na primjer, Ford fondacija i Fond za otvorenu tehnologiju odobrili su sredstva za inicijative CSO za sajber sigurnost. EU ima linije finansiranja u okviru programa kao što su Horizon ili Digital Europe koji bi mogli podržati izgradnju kapaciteta ako budete partneri ili se prijavite. Ako vam je potrebna ozbiljna nadogradnja (kao što je zapošljavanje osoblja IT sigurnosti ili preuređenje IT infrastrukture), razmislite o integraciji toga u prijedloge grantova za osnovnu podršku. Opravdajte to kao neophodno ublažavanje rizika – mnogi donatori su sada svjesniji i mogli bi odobriti budžet za to.

Relevantnost jezika i kulture: Kada tražite pomoć, pokušajte je pronaći u svom jeziku ili kontekstu ako je moguće. Globalni resursi su odlični, ali mogu biti na engleskom ili previše općenito. Zbog toga su važni lokalni stručnjaci i prevođenje međunarodnih vodiča na lokalne jezike. Ako je, recimo, vaš CSO u Türkiyeu (ubrzo vidim vremensku zonu Istanbula), korištenje lokalnog turskog resursa (poput turskog CERT savjeta ili obuke o digitalnoj sigurnosti na turskom) moglo bi biti jednostavnije za osoblje. Ako ne možete pronaći neki resurs na svom jeziku, možda volontirajte da prevedete relevantni vodič – koji je sam doprinos zajednice.

Tehnološke donacije: Uz podršku, imajte na umu da stvari poput Googlea za neprofitne organizacije nude besplatni G Suite, Microsoft za neprofitne organizacije nudi besplatne O365 licence, Okta nudi besplatna rješenja za jednokratnu prijavu, a neki dobavljači sigurnosti imaju neprofitne programe donacija (npr. NortonLifeLock pruža neke CSO podrška). Ovo može smanjiti prepreke u troškovima korištenja vrhunskih sigurnosnih alata.

Ostanite ažurirani: Pejzaž prijetnji se razvija. Neka bude navika da pratite neke sigurnosne vijesti ili se pridružite mailing listama (neke su kurirane za OCD). Na primjer, CIVICUS mailing lista za kibernetičku sigurnost (ako postoji) ili jednostavno praćenje vjerodostojnih izvora na društvenim mrežama (npr., @enisa_eu na Twitteru za vijesti iz EU ili blogove lokalnih firmi za kibernetičku sigurnost).

Ukratko, nisi sam. Postoji mreža podrške od lokalnog do globalnog. Proaktivno povezivanje sa ovim resursima u mirnim vremenima (ne samo tokom krize) je vrijedno truda. Uspostavite odnose sa ključnim kontaktima (znajte koga biste nazvali u 22 sata ako nešto pođe po zlu). I jednako, kada steknete znanje ili resurse, doprinesite ovim mrežama –, to je ono što ih čini robusnim i dostupnim za sljedeći OCD koji je potreban.

Koristeći saradnju (odjeljak 6.1, 6.2), obrazujući javnost (6.3) i posežući za sistemima podrške (6.4), OCD mogu transformirati digitalnu sigurnost iz zastrašujuće solo bitke u napor koji podržava zajednica. U sljedećem poglavlju pogledat ćemo konkretne primjere i uobičajene zamke kako bismo dalje učili iz iskustva iz stvarnog svijeta.

Sažetak poglavlja

Poglavlje 6 pruža okvire za OCD da proaktivno identifikuju rizike i pripreme se za sajber incidente. Vodi organizacije da procijene kritičnu imovinu (npr., baze podataka donatora) i ranjivosti, koristeći jednostavne šablone procjene rizika za određivanje prioriteta prijetnji kao što su phishing ili ransomware. Poglavlje opisuje kreiranje plana odgovora na incidente, sa detaljima o koracima za otkrivanje, zadržavanje, komunikaciju i oporavak. Na primjer, OCD sa planom odgovora može brzo vratiti podatke nakon napada ransomware-a, minimizirajući štetu. Naglašava dokumentovanje incidenata koje treba naučiti od njih i ažuriranje planova godišnje. Poglavlje se bavi pravilom obavještenja o kršenju od 72 sata, osiguravajući usklađenost. Praktični koraci uključuju dodjeljivanje uloga (npr., službenik za zaštitu podataka) i planove testiranja putem stolnih vježbi. Fokus poglavlja na pripremu pomaže OCD-ovima da se brzo oporave, smanjujući operativnu i reputacijsku štetu. Nudeći jasne, jeftine okvire, ovlašćuje netehničko osoblje da doprinese otpornosti, usklađujući se s misijom e-knjige's kako bi sajber sigurnost bila ostvariva za organizacije ograničene resursima.

Predlog politike zaštite podataka za OCD

Naziv organizacije: [Ubaci ime OCD]

Efektivni datum: [Insertni datum]

Posljednje ažurirano: [Insert Date ili "N/A za početnu politiku"]

Ova politika zaštite podataka opisuje kako [CSO Name] prikuplja, pohranjuje, pristupa i štiti lične podatke kako bi se osigurala privatnost, sigurnost i usklađenost sa važećim zakonima (npr., GDPR, [Zakon o zaštiti lokalnih podataka o istraživanju]). Primjenjuje se na svo osoblje, volontere i partnere koji rukuju ličnim podacima, štiteći povjerenje naših korisnika, donatora i dionika.

Ova politika pokriva sve lične podatke (npr. imena, kontakt podatke, zdravstvene ili finansijske informacije) kojima upravlja [CSO Name], uključujući podatke koji se odnose na korisnike, donatore, osoblje i volontere.

1. Prikupljanje podataka

Prikupljamo samo lične podatke neophodne za našu misiju I programe, dobijamo informirani pristanak gdje je to potrebno. Podaci se prikupljaju zakonito, transparentno i u određene svrhe.

Procedure:

⇒ Jasno objasnite zašto se podaci prikupljaju i kako će se koristiti prije prikupljanja (npr. putem obrazaca za pristanak ili obavještenja o privatnosti).

⇒ Sakupite minimalne podatke za postizanje svrhe (princip minimizacije podataka).

⇒ Dokumentirajte svrhu prikupljanja i dobijte saglasnost gdje je to primjenjivo (npr., potpisani obrasci, online kontrolne kutije).

2. Data Storage

Sigurno pohranjujemo lične podatke, koristeći enkripciju I zaštićene sisteme, kako bismo spriječili neovlašteni pristup, gubitak ili krađu.

Procedure:

⇒ Pripremite podatke na sigurnim platformama (npr. šifrirane cloud usluge kao što je Google Drive sa 2FA ili zaključane fizičke datoteke).

⇒ Šifrirajte osjetljive podatke u mirovanju (npr. na laptopima, vanjskim diskovima) i u tranzitu (npr., koristeći HTTPS ili sigurnu e-poštu).

⇒ Održavajte redovne sigurnosne kopije (npr., sedmično na siguran oblak ili vanjski disk) kako biste osigurali oporavak podataka.

⇒ Postavljanje podataka sigurno kada više nisu potrebni (npr. isjeckani papirni zapisi, koriste sigurne alate za brisanje za digitalne datoteke).

3. Kontrola pristupa

Pristup ličnim podacima ograničen je na ovlašteno osoblje kojem je potrebna za svoju ulogu, slijedeći princip najmanje privilegija.

Procedure:

⇒ Dodijelite pristup na osnovu radnih uloga (npr. samo menadžeri programa pristupaju podacima korisnika).

⇒ Koristite jake lozinke i dvofaktorsku autentifikaciju (2FA) za sve račune s pristupom ličnim podacima.

⇒ Redovno revidirati dozvole za pristup (npr. mjesečno) kako bi se uklonio pristup bivšem osoblju ili volonterima.

⇒ Željezničko osoblje i volonteri o sigurnom rukovanju podacima (npr. ne dijele lozinke, odjavljuju se nakon upotrebe).

4. Breach Reporting

Odmah otkrivamo, odgovaramo i prijavljujemo kršenje podataka kako bismo minimizirali štetu i ispunili zakonske obaveze (npr. GDPR' pravilo 72-satnog obavještenja).

Procedure:

⇒ Odredite službenika za zaštitu podataka ili lice tačke (npr. [Umetno ime/ulog]) za rješavanje kršenja.

⇒ Prijavite sumnje na kršenje odmah određenoj osobi (npr. putem e-pošte [Insert Email]).

⇒ Obavijestite nadležno tijelo za zaštitu podataka (npr. [Umjesti naziv lokalne uprave umetanje u 72 sata ako kršenje rizikuje da nanese štetu pojedincima.

⇒ Informisati pogođene pojedince (npr., korisnike, donatore) ako je potrebno, dajući jasne smjernice o sljedećim koracima.

⇒ Dokumentirajte sva kršenja i odgovore za poboljšanje buduće prevencije (npr., procjenu rizika ažuriranja).

5. Odgovornosti

Liderstvo: Odobrenje i finansiranje implementacije politike (npr., budžet za obuku, alate).
Osoblje i volonteri: Pratite ovu politiku, odmah prijavite pitanja i pohađajte obuku za zaštitu podataka.
Službenik za zaštitu podataka/Zajednička osoba: Nadgledajte usklađenost politike, upravljajte kršenjima i koordinirajte godišnje preglede.

6. Usklađenost i pregled

Usklađenost: Ova politika je u skladu sa GDPR-om i [Zakonom o zaštiti lokalnih podataka umetanja]. Nepoštivanje može rezultirati disciplinskim ili zakonskim kaznama.
Pregledajte i ažurirajte ovu politiku svake godine ili nakon značajnih promjena (npr. nove programe, propise). Sljedeća recenzija: [Insert Date, npr., novembar 2026.].
Svo osoblje i volonteri prolaze obuku za zaštitu podataka na brodu i svake godine.

7. Kontakt

Za pitanja ili za prijavu kršenja, kontakt: [Poslužitelj za zaštitu podataka umetanja/ime osobe sa bočnim zarezom, e-pošta, telefon].
Lokalno tijelo za zaštitu podataka: [Insert Name and Contact Info, npr., “Türkiye’s Personal Data Protection Authority (KVKK), [kontaktni detalji]”.

Odobreno sa: [Ubaci ime liderstva/Role, npr., izvršni direktor]

Datum: [Insert Date]

Bilješke o prilagođavanju: Zamijenite vlasnike mjesta (npr. [Znak OSO], [Zakon o zaštiti lokalnih podataka]) detaljima svoje organizacije. Dodajte lokalne zahtjeve za usklađenost ili specifične alate po potrebi.

2.7 POGLAVLJE 7: SIGURNOSNI USPJESI U CSOS-U

Prave priče: Sigurnosni uspjesi u OCD

Okreće se ohrabrujući da sazna kako su vršnjačke organizacije prevazišle sigurnosne izazove. Evo nekoliko anonimnih, ali realističnih scenarija koji pokazuju pozitivne rezultate zahvaljujući dobrim sigurnosnim praksama:

Phishing Attempt by Training: OCD za ljudska prava u istočnoj Evropi primio je e-mail koji je izgledao kao udio Google Docs-a od kolege. Budući da je osoblje prošlo obuku za podizanje svijesti o phishingu, jedan član tima je primijetio da nešto nije u redu (e-mail pošiljaoca je malo pogrešno napisan) i nije kliknuo na link. Umjesto toga, upozorila je IT žarišnu tačku. Potvrdili su da je to bio pokušaj krađe akreditiva. Kao rezultat toga, nijedan račun nije kompromitovan. Ovo je pojačalo vrijednost obuke –, direktor CSO-a je na sljedećem sastanku osoblja istakao kako je oprez zaposlenika potvrdio sve, pretvarajući ga u trenutak za učenje. Uspjeh je bio u tome što je napad spriječen nultom štetom, zahvaljujući osoblju za uzbunu.

Ransomware Attack Preživio zbog rezervnih kopija: Srednjoveliki zdravstveni CSO u Africi je jednog jutra pogodio ransomware – osoblje je pronašlo svoje datoteke šifrirane i otkupninu na svojim ekranima. U početku je bio haos. Međutim, organizacija je imala robustan sistem rezervnih kopija: svi kritični podaci su bili podržani do eksternog servera svake noći. Za nekoliko sati, njihov IT konsultant je izolovao zaražene mašine, obrisao ih, ponovo instalirao softver i vratio podatke iz prethodne noćne rezervne kopije. Izgubili su najviše jedan dan rada na nekoliko dokumenata. Nisu platili otkupninu i prijavili su incident. Ovo iskustvo se pretvorilo u priču o sigurnosnom uspjehu koju dijele – njihova ulaganja u rezervnu kopiju i planiranje oporavka se isplatila, dokazujući koliko je to važno. Kasnije su čak predstavili ovaj slučaj na webinaru, ohrabrujući druge OCD-ove da implementiraju offline sigurnosne kopije.

Sigurnosni planovi osjetljivi na komunikaciju: Koalicija za zagovaranje organizirala je kampanju u zemlji s velikim nadzorom. Sumnjali su da se nadzire njihova komunikacija. Pod vodstvom konsultanta za digitalnu sigurnost, prešli su na korištenje end-to-end šifriranih poruka (Signal) i e-pošte s PGP-om za najosjetljivije priloge. Tokom kampanje primijetili su pokušaje protivnika da preduzmu svoju strategiju, ali kritični detalji nikada nisu procurili. Analiza nakon kampanje sugerira da od njihovog prelaska na siguran komunikacije, opozicija je izgubila svoju "unutar znanja" prednost. Koalicija pripisuje sigurne alate za očuvanje njihovih planova i

doprinos uspjehu kampanje's. Očvrsnuo je njihovu posvećenost korištenju šifriranih kanala za buduće operacije i poslužio kao primjer drugima u njihovoj mreži.

Otmica lažnih računa od dva faktora: OCD za ženska prava u Južnoj Aziji imao je jedan od Gmail naloga svog osoblja na meti e-pošte za krađu identiteta. Osoblje je slučajno ušlo u njenu lozinku na lažnoj Google stranici za prijavu. Ta lozinka je otišla napadaču. Ubrzo nakon toga, napadač iz druge zemlje pokušao je da se prijavi na svoj Google nalog —, ali pošto je CSO nametnuo dvofaktorsku autentifikaciju na svim računima, prijava je tražila kod za verifikaciju sa njenog telefona. Napadač to nije imao, pa je bio zaustavljen hladan. Google je upozorio korisnika na blokirani pokušaj prijave. Odmah je shvatila šta se dogodilo, prijavila i promijenila lozinku. Na kraju, 2FA je ono što je moglo biti ozbiljan proboj pretvorilo u puki strah bez nanošenja štete. Ovaj pravi incident zaista se vratio kući cijelom timu zašto su se vredele te pomalo dosadne upute za 2FA. Bio je to dan olakšanja i pobjede za njihove sigurnosne mjere.

Saradnja u zajednici Zaustavljena DDoS: Mreža ekoloških OCD-a pokrenula je kampanju koja je izazvala bijes nekih protivnika, koji su potom pokrenuli napad distribuiranog poricanja usluge (DDoS) na zajedničku web stranicu mreže's (preplavivši ga saobraćajem kako bi ga izbacili van mreže). Pojedinačno, OCD su imali ograničene IT resurse da to ublaže. Međutim, putem kanala tehnološke solidarnosti, jedan lider OCD-a brzo je zatražio pomoć. Partnerska organizacija u tehnološkoj kompaniji dogovorila je privremenu upotrebu svoje DDoS usluge zaštite (Cloudflare), a drugo IT osoblje CSO's pomoglo je preusmjeravanju stranice kroz tu zaštitu. U roku od nekoliko sati, web stranica je ponovo pokrenuta uprkos suočavanju s napadom, a kampanja je nastavljena. Ovaj zajednički odgovor bila je priča o uspjehu koja ilustruje kako podrška saveznika može suprotstaviti čak i velikim sajber prijetnjama. To ih je također naučilo da nakon toga postave uvijek na Cloudflare zaštitu. Kasnije su napisali ovaj slučaj na blogu kako bi se zahvalili onima koji su pomogli i vodili druge o ophođenju sa DDoS-om.

Ove priče pokazuju da čak i kada su OCD na meti sajber prijetnji, **spremnost i brza akcija mogu dovesti do uspješne odbrane ili brzog oporavka**. Zajedničke niti uključuju: prethodno ulaganje u sigurnosne mjere (trening, sigurnosne kopije, 2FA), brzo prepoznavanje i odgovor, te

korištenje mreža podrške. Dijeljenjem i proučavanjem takvih uspjeha, OCD mogu naučiti šta zaista funkcionira i steći povjerenje da oni, također, može podnijeti slične situacije.

Uobičajene greške i kako ih spriječiti

Učenje iz tuđih grešaka (ili naših) ključno je za poboljšanje sigurnosti. Evo nekih čestih zamki na kojima se OCD susreću, zajedno sa strategijama da ih se izbjegne:

Korištenje slabih ili neispravnih lozinki: Možda je najrasprostranjenija greška pridržavanje jednostavnih lozinki (kao što su "123456", "lozinka") ili ostavljanje zadanih lozinki nepromijenjenim na uređajima (npr., ruteri često dolaze sa "admin/admin"). Ovo je poklon napadačima. Prevencija: Uspostaviti politiku lozinki koja zahtijeva jake, jedinstvene lozinke i koristiti upravitelje lozinki za njihovo rukovanje. Tokom treninga, pokažite primjere loših i dobrih lozinki. I kad god postavljate novi hardver/softver, odmah promijenite zadane akreditive (i bezbedno ih dokumentirajte). Provedite povremene revizije – koriste alat ili skriptu da provjerite ima li bilo koji račun slabe lozinke (neki organi koriste baze podataka o kršenju ili alate za reviziju). Naglasite 2FA da kompenzirate svaku slabu lozinku koja proklizne.

Kliknuti prije razmišljanja (Phishing Success): Mnoga kršenja počinju tako što neko klikne na zlonamjernu vezu ili vezanost bez nadzora. Greška djeluje na impuls e-pošte ili poruke (posebno na one koji izazivaju hitnost ili radoznalost) umjesto da provjeravaju autentičnost. Prevencija: obuka, obuka, obuka. Pokrenite simulirane phishing testove kako biste identificirali kome je potrebno više prakse. Ohrabrite kulturu u kojoj je u redu usporavati i provjeriti zahtjeve – npr., "Ako se e-mail čini hitnim i traži novac ili akreditive, u redu je (u stvari ohrabreno) da provjerite s pozivom ili odvojenom 3email." Pružajte jednostavne kontrolne liste: pažljivo provjerite adresu pošiljaoca, potražite pravopisne greške, ne preuzimajte neočekivane dodatke, itd. Osim toga, tehnička odbrana poput dobrih filtera za neželjenu poštu i skeniranja veze pomažu u filtriranju očigledne prijevare.

***Neuspješno ažuriranje softvera*:** Uobičajeni scenario: web stranica OCD-a radi na WordPressu, ali nije ažurirala dodatke za godinu dana, a napadač iskorištava poznatu grešku da je ublaži. Ili računarski računari i dalje pokreću starije verzije OS-a sa netaktiranim ranjivostima. Greška je odlaganje ili ignorisanje ažuriranja (ponekad iz straha da bi to moglo nešto slomiti, ponekad samo zaboraviti). Prevencija: Omogući automatska ažuriranja gdje god je to izvodljivo.

Na sistemima koji ne mogu automatsko ažuriranje, dodijelite nekome zadatak da provjerava mjesečno. Koristite alate koji agregiraju potrebe ažuriranja (čak i jednostavno uključite “Check za ažuriranja” obavještenja). Za web stranice razmotrite upravljani hosting koji upravlja ažuriranjima ili se pretplatite na liste za sigurnosnu poštu dodataka. Naglasite “patch Tuesday” ili neku rutinu. Ako resursi dozvoljavaju, zadržite inventar kritičnog softvera i pratite njihov status zakrpe (postoje besplatni skeneri koji ističu zakrpe koje nedostaju). Također, raspršite mitove poput “ažuriranja usporavajući moj kompjuter” pokazujući sigurnosni rizici ne ažuriranja.

Ne odustajanje (ili testiranje rezervnih kopija): Neke organizacije shvataju važnost rezervnih kopija tek nakon gubitka podataka. Greške uključuju nepoduzimanje podrške uopće ili rezervne kopije, ali ne i testiranje (tada otkrivanje da su nepotpune ili oštećene kada je to potrebno). Prevencija: Implementirati rezervnu strategiju 3-2-1 (više kopija, različiti mediji, jedan van lokacije). Zakažite rezervne kopije i automatizirajte ih. Što je još važnije, redovno se obnavljaju testovi. Jednostavna bušilica: nasumično odaberite datoteku i pokušajte je vratiti iz rezervne kopije kako biste osigurali da proces funkcionira. Također, osigurajte da su same sigurnosne kopije osigurane (šifrirane i nedostupne normalnoj mreži, tako da ih ransomware ne može pogoditi). Mnogi su naučili na teži način da sigurnosna kopija na mrežnom disku dostupna svima nije sigurna od malvera za šifriranje. Rješenja: offline sigurnosne kopije ili barem verzije rezervnih kopija u oblaku su imune na enkripciju.

Pretjerani privilegija i zajednički računi: Greška: davanje svim korisnicima administrativnih prava “jer je lakše” ili dijeljenje jedne prijave među nekoliko ljudi radi pogodnosti. Ovo može dovesti do velikih problema – jedna osoba može nenamjerno instalirati zlonamjerni softver sa administrativnim pravima, ili preminuli zaposlenik još uvijek zna lozinku zajedničkog računa. A odgovornost se gubi kada se računi dijele (ne možete reći ko je šta uradio). Prevencija: Primijenite princip najmanje privilegije. Kreirajte pojedinačne račune za sve i dajte im samo pristup koji im je potreban. Koristite dozvole zasnovane na ulogama za datoteke I sisteme. Da, to je malo početnije podešavanje, ali moderni sistemi čine prilično jednostavnim upravljanje korisnicima. Također, imajte jasnu kontrolnu listu za ukrcavanje/offboarding tako da se pristup odobrava i sistematski ukida. Za administrativne zadatke, imajte poseban

administrativni nalog – ne pretražujete web ili čitajte e-poštu kao administratorski korisnik. Na taj način, čak i ako je korisnik prevaren, šteta bi mogla biti sadržana na nivou korisnika.

Ignoriranje sigurnosnih upozorenja ili najboljih praksi: Ljudi ponekad ignorišu ta upozorenja pretraživača ("This sajt sertifikat nije pouzdano") ili onemogućuju bezbednosne funkcije jer izgledaju dosadan (Pustite me da isključim zaštitni zid kako bih ovu aplikaciju pokrenuo). To može otvoriti vrata za napad. Drugi primjer: korištenje zastarjelo, nesigurni protokoli (poput FTP-a umjesto SFTP-a) iz navike. Prevencija: Obrazovati o tome zašto postoje upozorenja. Na primjer, objasnite šta znači upozorenje o certifikatu i da može ukazivati na lažno mjesto ili prisluškivanje. Napravite okruženje u kojem ako sigurnosna mjera blokira nešto, umjesto da ga onesposobi, osoblje traži odgovarajuća rješenja (kao što je dodavanje izuzetka ako je to poznato sigurno interno mjesto, itd.). Pružajte smjernice: ako antivirusni signal označi datoteku, nemojte ga samo izbjeljivati iz frustracije – kontaktirajte IT da analizirate da li je zaista siguran. Napišite jednostavna interna često postavljana pitanja: "Ako vidite sigurnosno upozorenje, uradite X." Također, kada postavljate nove alate, uradite to bezbedno od početka kako osoblje neće biti u iskušenju da koristi nesigurne radne grupe.

Plan odgovora na nedostatak incidenata: Mnogi OCD-ovi su uhvaćeni ravnih nogu tokom incidenta – ne znajući koga da nazove ili koje korake da preduzme, što gubi dragoceno vreme. Greška: nema unaprijed definiranog plana incidenta ili vježbi. Prevencija: Razviti osnovni plan odgovora na incidente (kao što je učinjeno u Poglavlju 5) i osigurati da svi znaju njegove osnove. To bi mogao biti samo jedan pejdžer: "Ako se dogodi nešto čudno: isključite se s interneta, nazovite ovu osobu, itd." Također, napravite barem stolnu vježbu: razgovarajte kroz hipotetički "Šta ako nas ransomware udari, šta bismo radili?" uočiti praznine. Imati plan smanjuje greške tokom pravih kriza, kao što je isključivanje pogrešnog sistema ili panika.

Svjestan ovih uobičajenih grešaka, OCD može poduzeti proaktivne mjere kako bi izbjegao upad u te zamke. Često su male promjene u ponašanju ili politici one koje čine veliku razliku – poput navike primjene ažuriranja ili dvostruke provjere prije klizanja. Ohrabrite filozofiju koja "**svi su dionici u sigurnosti,"** dakle, greške se mogu uhvatiti ili spriječiti kolektivnom marljivošću (npr., recenzija sumnjivih mejlova – "Hey kolega, da li vam ovo izgleda legalno?" može zaustaviti grešku).

Ukratko: ojačajte slabe lozinke, razmislite prije klizanja, sve ažurirajte, pažljivo rezervišete, ograničite privilegije, obratite pažnju na upozorenja i planirajte najgore. Izbjegavanje ovih uobičajenih grešaka dramatično će poboljšati vaš sigurnosni stav uz prilično malu cijenu.

Testirajte svoju sigurnost: jednostavne vježbe

On navodi jednu stvar koju treba pročitati o sigurnosti; drugo je to sprovesti u praksu. Evo nekoliko jednostavnih samoprocjena i vježbi koje vi (i vaš tim) možete učiniti kako biste procijenili i poboljšali svoju sigurnosnu spremnost. Zamislite ih kao "sigurnosne vježbe" ili preglede:

Phishing Drill: Napravite bezopasnu "lažnu phishing e-poštu" kako biste testirali svijest u svom timu. Na primjer, pošaljite e-poštu sa neorganizacijske adrese, ali koristite svoje ime za organe na ekranu, s subjektom kao što je "Urgent ažuriranje zahtijevalo je" i link do Google obrasca (koji samo kaže "Čestitke, ovo je bio test!"). Vidi ko klikne ili šalje informacije. Cilj je edukativan, a ne gotcha: nakon toga, otkrijte ga i razgovarajte o tragovima da je bio šaljiv (možda mala razlika u adresi, hitan ton, itd.). Ako je malo njih palo na to, odličan – ako neki jesu, koristite ga kao nježnu priliku za trening. Alternativno, koristite besplatne alate kao što je Google's phishing kviz ili Phishing Simulation alati (neki AV paketi imaju ovu funkciju) na kontroliran način.

Provjera snage lozinke: Pogledajte neke lozinke (bez traženja od bilo koga da razotkrije svoje, možete simulirati uobičajene obrasce). Koristite mjerač snage lozinke (mnogi online, npr., Passwordmeter.com) za testiranje uzorka tipičnih lozinki u odnosu na preporučene. Bolje, ako koristite upravitelj lozinki, pogledajte da li prijavljuje slabe/ponovno korištene lozinke –, mnogi imaju funkciju sigurnosne revizije. Kao vježba, neka svi kreiraju snažnu šifru od četiri nasumične riječi (npr. "karavan tiger dance") i testiraju njegovu snagu u odnosu na nešto poput "Winter2020!" – rezultati često pokazuju da je šifraza jača i lakša za pamćenje. Ovo pojačava dobre navike kreiranja lozinki.

Rezervna pomoć: Testirajte svoju rezervnu kopiju. Simulirajte scenario: "Izgubili smo datoteku X, šta da radimo?" Zapravo, idite na svoju rezervnu lokaciju, dohvatite datoteku I otvorite je da bude netaknuta. Ili odaberite datum i pretvarajte se da morate sve vratiti na to kako je tada bilo – možete li preuzeti podršku tog datuma? Vrijeme koliko je potrebno da se obnovi reprezentativni skup podataka. Ovo ne samo da provjerava sigurnosne kopije, već vas i priprema za stvarne incidente otkrivajući da li su upute/kreditacije za sigurnosne kopije lako

dostupne. Možda dodijelite nekom drugom (ne uobičajenoj IT osobi) da isproba vraćanje koristeći samo dokumentirane korake da vidi da li je proces dovoljno jasan.

Revizija sigurnosti uređaja: Uradite brzu reviziju računara i telefona u vašem uredu (uz dozvolu, naravno). Provjera: Da li je sav OS ažuriran (otvoreni Windows Update ili ekvivalent, pogledajte posljednji datum ažuriranja)? Da li antivirus radi I ažurira? Jesu li vatreni zidovi upaljeni? Da li neki uređaji i dalje koriste zadane lozinke (npr., prijavite se na uredski ruter i pogledajte da li zadani kreditori rade – ako da, velika zastavica da je promijene)? Pogledajte da li se ekrani automatski zaključavaju kada su u praznom hodu. Možete napraviti jednostavnu kontrolnu listu i ocijeniti svaki računar. Zatim riješite sve pronađene probleme i proslavite ako je većina stvari osigurana prema zadanim postavkama (otvrđuje vaše konfiguracijske prakse).

Test spoof e-pošte: Zanimljiva vježba: pokazati koliko lako može biti lažirati e-poštu, izazvati skepticizam. Korištenje kontroliranog okruženja (poput usluge koja omogućava slanje e-poruka sa prilagođene adrese koju posjedujete, ili čak samo modificiranje imena “From” u Gmailu), pošaljite sebi e-poštu koja izgleda da dolazi iz, recimo, “[zaštićene e-pošte]” (ali dolazi iz druge domene). Pokažite osoblju kako, na prvi pogled, izgleda uvjerljivo, ali zaglavlja e-pošte ili stvarna adresa pokazuju istinu. Ova vježba često šokira ljude, a nakon toga pažljivije provjeravaju adrese e-pošte.

Čišćenje dozvola: Uzmite jednu zajedničku fasciklu ili Google Drive i reviziju ko ima pristup. Možda ćete otkriti da bivši dobrovoljci još uvijek imaju pristup, ili su neki dosijei nehotice podijeljeni na javne veze. Kao “mini vježba,” ukida svaki nepotreban pristup i dokumentira ga. To je kao proljetno čišćenje za prava pristupa. Ovo služi kao podsjetnik da se to povremeno radi.

Incident Role-play: Odaberite scenario (kao što je “laptop ukraden iz cafe” ili “ransomware na server”) i verbalno prođite kroz to kako biste odgovorili (koga nazvati, koje korake treba poduzeti). Igra uloga sa osobljem: igra se uspaničeni korisnik, drugi IT responder, itd. Ova skromna proba može ukazati na praznine (“Oh, mi zapravo nemamo broj banke koji bi bio zgodan za pozivanje i zamrzavanje računa ako je e-pošta kompromitovana,” ili “Shvaćamo da ne znamo administrativnu lozinku našoj web stranici po memoriji ako je LastPass nedostupan.”). Bolje je sada saznati nego za vrijeme prave krize.

Svaka vježba treba da bude jednostavna i ne dugotrajna, već vrlo pronicljiva. Zamislite to kao vatrogasnu vježbu za sajber prijetnje – koju praktikujete u okruženju s niskim ulozima tako da u stvarnim hitnim slučajevima znate šta učiniti i osjećate se manje anksiozno jer ste ranije radili nešto slično.

Nakon svake vježbe, otvoreno razgovarajte o rezultatima bez krivice. Ako je nešto pošlo po zlu (npr., polovina tima je pala na phishing testu), tretirajte to kao kolektivno učenje: možda je phishing e-mail bio zaista podmukao – sada svi znaju da budu oprezni s tim trikom sljedeći put. Ako vježba otkrije ozbiljnu slabost, zahvalite procesu na otkrivanju i posvetite se njenom popravljanju.

Redovno izvođenje takvih vježbi održava sigurnost u glavama ljudi i njeguje kulturu kontinuiranog poboljšanja. To demistificira sigurnost (jer aktivno radite stvari, a ne samo da slušate politiku). Može čak biti zabavno na način – neke organizacije ga ga gamificiraju, nudeći male nagrade onima koji uočavaju ribe ili imaju najmanje problema u reviziji.

Integracija digitalne sigurnosti u dnevnu rutinu

Krajnji cilj je da dobre sigurnosne prakse postanu druga priroda – samo normalan dio načina na koji vi i vaša organizacija radite. Evo savjeta o neprimjetnom tkanju digitalne sigurnosti u svakodnevni život u OCD:

Započnite dan sa sigurnošću na umu: Podsticati jednostavne jutarnje navike. Na primjer, kada pokrenete svoj računar, neka prvo instalira ažuriranja prije nego što skoči na posao (zgrabite kafu dok ažurira umjesto da pogodite “postpone”). Ili provjerite bilo kakva sigurnosna obavještenja (kao što je “Windows Defender: nema problema koji su pronašli” ili upit za ažuriranje softvera) i obratite im se rano. Ovo osigurava da počnete raditi u sigurnom stanju umjesto da ignorišete te male štitove i znakove uzvika na radnoj traci.

Upravitelj lozinki svaki dan: Učinite korištenje upravitelja lozinki rutinskim dijelom procesa prijave. Ako se pravilno postavi, može automatski ispuniti akreditive – tako da osoblje brzo vidi korist (brže prijavu, nema problema s resetiranjem lozinke) i jednostavno postaje način na koji se prijavljuju. Dnevni rutinski pomak je od “zapamtite ili zapisate lozinke” do “menadžera otključavanja jednom sa jakom lozinkom, a zatim kliknite da se prijavite posvuda.” Vremenom neće zamisliti život bez njega. Neki menadžeri također traže ažuriranje slabih lozinki

– možda dodijele nekoliko minuta svakog petka kako bi ažurirali jednu označenu lozinku. Pomalo po malo, svi računi dobijaju jače lozinke.

Podsjetnici tima i kultura: Uključivanje obezbjeđenja vodi u redovne sastanke tima ili interne biltene. Na primjer, na sedmičnom sastanku, jedna tačka dnevnog reda mogla bi biti jednominutni sigurnosni savjet ili vijest (npr. "FYI, trenutno postoji WhatsApp prevara; ne zaboravite da ne dijelite kodove za verifikaciju"). Ovo normalizuje razgovor. Ne mora dominirati, samo rutinska prijava. Neki CSO su postavili poster "Security Tip of the Month" na zidu ili Slack kanalu, koji pasivno održava svijest na dnevnom vidiku.

Kreteni za zaključavanje i čisti stolovi: Neka vam je navika da zaključate svoj računar (Win+L na Windows, Ctrl+Cmd+Q na Mac) kad god se povučete – čak i na minut. Ako svi to rade, to je normalno, ne paranoično. Isto je i sa održavanjem osjetljivih papira ili USB diskova koji ne leže okolo (stara politika "čistog stola"). Lakše je u rutini ako ga vežete za nešto: npr., na kraju dana, posljednja stvar: rezervne datoteke, zaključajte sve ormare, provjerite da li ste se prijavili iz sistema –, onda znate da ste postavljeni. Možda napravite štampanu kontrolnu listu za sigurno zatvaranje ureda (digitalno i fizičko) koju osoblje prati svakodnevno dok to ne postane druga priroda.

Integrirajte sigurnost u radnim tokovima: Kakvi god alati da koristite, koristite njihove sigurnosne funkcije prema zadanim postavkama. Primjer: ako dijelite datoteku putem oblaka, rutinski koristite "udio sa određenim ljudima", a ne link. Potrebno je možda 10 sekundi više da se otkuca njihov e-mail, ali ako to postane jedini način na koji ljudi dijele, to je normalno. Ili zakažite periodične preglede dozvola kao dio zatvaranja projekta: npr., kada se projekat završi, dio kontrolne liste za završetak je "pregled i uklonite svaki vanjski pristup iz fascikli projekta." Na taj način, sigurnosno održavanje se uvlači u životni ciklus upravljanja projektom.

Ažuriranje u utorak (ili izabrani dan): Mnoge organizacije planiraju kada obavljaju poslove održavanja. Možda u utorak ujutro, IT/određena osoba osigurava da se OS i aplikacije ažuriraju na svim uređajima ili svaki korisnik provjerava ažuriranja telefona sedmično. Ako se očekuje i zakaže, to se neće smatrati prekidom, već rutinskim (kao što je zalijevanje biljaka svakog ponedjeljka, ažuriramo sisteme). Cloud usluge se ažuriraju, ali možda mjesečno provjerite administrativnu konzolu za bilo kakva upozorenja ili nove sigurnosne funkcije koje će

omogućiti (pružaoci često dodaju nove sigurnosne postavke; dobro je odvojiti vrijeme za redovnu integraciju njih).

Kontinuirano učenje: Ohrabrite osoblje da povremeno pohađa online kurseve ili kvizove veličine zalogaja. Možda svi rade jedan modul online sigurnosnog kursa po kvartalu (neki su interaktivni i kratki). Ako dodijelite, recimo, sat vremena rada za to, to pokazuje organizacijsku posvećenost. Ovo održava znanje svježim i signalizira da je sigurnost dio profesionalnog razvoja, a ne opcioni posao.

Olovo po primjeru: Liderstvo bi trebalo otvoreno modelirati sigurnosno ponašanje. Ako režiser uvijek koristi 2FA token i hvali se, "Volim koliko je to sigurno i lako, slijede drugi". Ako rukovodstvo padne na prevare ili koristi slabe prakse, drugi će podsvjesno misliti da je to u redu. Dakle, integrirajte ga u top – npr., ako član osoblja šalje osjetljive podatke putem lične e-pošte, menadžer bi ga trebao nježno ispraviti: "Molimo koristite naš službeni račun ili šifrirajte tu datoteku – tako radimo stvari ovdje." Vremenom se grupne norme menjaju.

Automatizacija harnessa: Jedan od načina da imate sigurnost bez svakodnevnih ljudskih napora je automatizacija. Na primjer, postavite sve računare da se automatski zaključaju nakon pet minuta mirovanja –, a zatim se osoblje prilagođava tom obrascu (i možda nalazi pet minuta prekratko, tako da se proaktivno zaključavaju kada izađu, a ne da budu zaključani usred rečenice). Koristite automatske ažuriranja, automatska skeniranja (proglasite AV puna skeniranja za vrijeme pauze za ručak sedmično). Ovo smanjuje oslanjanje na memoriju ili motivaciju – sistem podržava rutinu. Slično, korištenje jednog rješenja za prijavu (SSO), ako je dostupno, može integrirati sigurnost (jedna jaka prijava otključava više aplikacija, tako da se korisnici uvijek prijavljuju s tom jednom robusnom metodom umjesto da žongliraju slabijim).

Nagrada i pojačanje: Pozitivno pojačanje pomaže navikama. Razmotrite male nagrade ili priznanje za dobro sigurnosno ponašanje. Primjer: "Security Star of the Month" za nekoga ko je prijavio phishing e-poštu ili došao na ideju za poboljšanje sigurnosti. Čak i samo pohvale javnosti, "Hvala Alice što je primijetila neobičan e-mail – veliku pažnju na detalje!" ohrabruje sve da budu pažljivi. To pokazuje da je sigurnosna svjesnost cijenjena, a ne samo očekivana.

Ugrađivanjem ovih praksi u svakodnevne tokove rada, digitalna sigurnost prestaje biti sporadičan projekat i postaje dio organizacijske kulture. Novo osoblje će ga apsorbirati od prvog

dana jer “ovako radimo ovdje.” Demistificira sigurnost – to nije posebna techie stvar, dio je svačije rutinske dužnosti posla, slično kao zaključavanje vrata kancelarije ili nošenje lične značke. Vremenom ove male svakodnevne navike grade jaku tvrđavu gotovo nevidljivo. Možda čak i ne shvatite koliko ste postali sigurni jer se čini rutinskim i lakim. To je cilj: sigurnost ne kao teret, već kao integrirani aspekt rada pametniji i sigurniji svaki dan.

Sažetak poglavlja

Ovo poglavlje istražuje kako OCD mogu iskoristiti saradnju i eksterne resurse za poboljšanje digitalne sigurnosti. Naglašava da se nijedna organizacija sama ne suočava sa sajber prijetnjama zalaganje za zajedničko znanje i mreže. Poglavlje naglašava besplatne alate ili alate vođene zajednicom, kao što je Google Workspace za OCD ili digitalne sigurnosne linije za pomoć, kako bi se riješila budžetska ograničenja. Podstiče pridruživanje sigurnosnim forumima i koalicijama kako bi se podijelile obavještajne informacije o prijetnjama i priče o uspjehu. Primjeri uključuju OCD-ove koji se udružuju s tehnološkim volonterima kako bi osigurali servere ili pristupili besplatnim resursima iz nacionalnih CERT-ova. Ogranak također promovira saradnju s vladom, akademskom zajednicom i tehnološkom industrijom kako bi se zalagao za sigurniji digitalni ekosistem. Povezivanjem sa vršnjacima, OCD pojačavaju svoju odbranu, kao što se vidi u slučaju kada su zajednička upozorenja zaustavila phishing kampanju. Poglavlje osmišljava praktične smjernice, poput pretplate na sigurnosne biltene, osigurava dostupnost za male OCD. U skladu je sa nastavnim planom i programom, formira model voza-trenera, podstičući pristup otpornosti i kolektivne odbrane vođen zajednicom.

3. OBRAZOVNI MODULI

Uvod i kontekst

U današnjem digitalnom dobu, organizacije civilnog društva (CSO) i nevladine organizacije (NVO) se sve više oslanjaju na digitalne alate za ispunjavanje svojih misija. Nažalost, to ih čini atraktivnim metama za sajber prijetnje. U stvari, 50% OCD-a bilo je na meti sajber napada 2025. godine, a neprofitne organizacije su sada drugi najciljaniji sektor sajber napada nacionalne države (31% svih slučajeva). Uprkos ovom riziku, mnogi OCD-ovi su nedovoljno pripremljeni – četiri od pet OCD nemaju nikakav plan sajber bezbednosti, a 70% ne smatra da imaju potrebno znanje ili veštine da odgovore na sajber napade. Ove statistike naglašavaju hitnu potrebu za jačanjem kapaciteta digitalne sigurnosti u neprofitnom sektoru.

Digitalna sigurnost nije samo IT pitanje; utiče na sposobnost organizacije's da služi svojoj zajednici. Jedno kršenje ili napad ransomware-a može poremetiti kritične usluge, ugroziti osjetljive podatke korisnika i oštetiti povjerenje javnosti. Za OCD koji rade sa ograničenim resursima, oporavak od takvih incidenata može odvratiti dragocjena sredstva i vrijeme od svoje osnovne misije. Poboljšanje digitalne sigurnosne infrastrukture civilnog društva je stoga od suštinskog značaja kako bi se osiguralo da ove organizacije mogu raditi bezbedno i efikasno.

Cilj nastavnog plana i programa

Jedan od ključnih ciljeva našeg projekta je razvoj sveobuhvatnog "kurikuluma digitalne sigurnosti za civilno društvo." Cilj je stvoriti strukturirani program obuke koji će osnažiti OCD i grupe civilnog društva znanjem i vještinama potrebnim za poboljšanje njihove infrastrukture digitalne sigurnosti. Po infrastrukturi, mislimo na cijeli spektar organizacije digitalnog sigurnosnog stava – od sigurnih tehnologija i praksi do politika i kapaciteta osoblja. Ovaj nastavni plan i program je zamišljen kao praktičan alat koji pomaže OCD-ima da nauče kako da zaštite svoje podatke, sisteme i komunikacije, čime se smanjuje njihova ranjivost na sajber prijetnje.

Ovaj cilj je u skladu sa našim projektom.' širi cilj povećanja digitalne sigurnosti širom Evrope. Gradeći kapacitete na nivou civilnog društva, zauzimamo pristup odozdo prema gore kako bismo ojačali sajber sigurnost na kontinentalnom nivou. Dobro obučeni OCD neće samo zaštititi svoje poslovanje, već će doprinijeti i sigurnijem digitalnom okruženju za zajednice kojima služe. U suštini, nastavni plan i program će biti strateški korak ka jačanju sajber

sigurnosti kroz civilno društvo, osiguravajući da to bude još manje organizacije mogu podržavati snažne prakse digitalne odbrane.

Do kraja ovog nastavnog plana i programa, učesnici će moći:

- *Identificirajte glavne prijetnje digitalnom sigurnošću organizacijama civilnog društva i objasnite osnovne zaštitne mjere.*
- *Provesti osnovnu procjenu rizika svoje organizacije's digital agets i izraditi jednostavan plan kibernetičke sigurnosti.*
- *Implementacija osnovnih sigurnosnih mjera na uređajima, mrežama I komunikacijama (npr., jake lozinke, zaštitne zidove, siguran Wi-Fi).*
- *Primijenite principe zaštite podataka i uskladite se sa relevantnim propisima o privatnosti podataka (npr., GDPR).*
- *Koristite sigurne društvene mreže i online alate za zaštitu reputacije i informacija organizacije's.*
- *Razvijajte i sprovodite osnovne politike IT bezbednosti (kao što su lozinka, sigurnosna kopija i politike prihvatljive upotrebe) i izvršite osnovnu proceduru odgovora na incidente.*

Pregled kurikuluma

"The Digital Security Curriculum for Civil Society" je strukturirani program učenja, dizajniran kao strateški alat koji organizacije civilnog društva i OCD prate kako bi ojačali svoju infrastrukturu digitalne sigurnosti. Nastavni plan i program se isporučuje kao modularni paket obuke koji projektni partneri prilagođavaju i implementiraju u svojim zemljama.

Ključne karakteristike nastavnog plana i programa uključuju:

- **Sveobuhvatni sadržaj:**

  Nastavni plan i program pokriva teme od osnovnog do naprednog nivoa, omogućavajući organizacije sa ograničenim prethodnim znanjem da postepeno grade svoje kapacitete digitalne sigurnosti korak po korak.
- **Praktični fokus:**

  Nastavni plan i program naglašava praktične vještine i scenarije iz stvarnog života, a ne teorijske pristupe. Moduli se bave praktičnim situacijama kao što su odgovor na

pokušaje krađe identiteta, osiguranje sastanaka na mreži i zaštita organizacioni podaci. Svaki modul pruža izvodljive smjernice, alate i kontrolne liste koje OCD primjenjuju direktno u svom svakodnevnom radu.

- **Prilagođavanje i lokalna režija:**
  Nastavni plan i program je osmišljen tako da bude prilagodljiv nacionalnim kontekstima. Partneri u projektu prilagođavaju primjere, studije slučaja i odabrani sadržaj lokalnim propisima, potrebama i operativnim realnostima, dok osnovni principi i ciljevi učenja ostaju dosljedni u svim partnerskim zemljama.
- **Format i dostava:**
  Materijali za obuku uključuju klizne palube, sažete tekstove objašnjenja i interaktivne komponente kao što su vježbe i kvizovi. Nastavni plan i program se isporučuje putem online formata i/ili ličnih radionica kako bi se osigurala pristupačnost za organizacije različitih veličina i tehničkih kapaciteta. Promovira se pristup vlaku-treneru, koji omogućava projektnim partnerima i lokalnim stručnjacima da pruže obuku na svojim nacionalnim jezicima.
- **Struktura orijentisana na rezultate:**
  Po završetku nastavnog plana i programa, učesnici su u mogućnosti da procijene svoj organizacija osmišljava digitalne rizike, implementira osnovne sigurnosne mjere, razvija interne politike digitalne sigurnosti i samouvjereno odgovara na uobičajene sajber prijetnje. Nastavni plan i program uključuje alate i indikatore za samoprocjenu koji omogućavaju organizacijama da procijene svoj nivo digitalne sigurnosne spremnosti.

Zašto je OCD-ovima potreban digitalni sigurnosni kapacitet?

- ***Visok rizik, niski resursi***: OCD često rukuju osjetljivim podacima (npr. ličnim podacima korisnika, donatora), ali rade na ograničenim budžetima koji ograničavaju njihove mjere kibernetičke sigurnosti. Napadači znaju da su mnogi CSO “cyberpoor, ali bogati ciljevima” – bogat podacima i fondovima, ali siromašan u odbrani.
- ***Pejzaž rastućih prijetnji***: Uz povećanu digitalizaciju (ubrzanu pandemijom) i oslanjanje na online usluge trećih strana, površina napada za OCD je porasla. U porastu su phishing, zlonamjerni softver, ransomware i DDoS napadi na civilno društvo.

- ***Nedostatak svijesti i obuke***: Mnogi zaposleni i lideri civilnog društva nisu imali formalnu obuku o sajber sigurnosti. Oko 90% neprofitnih organizacija ne obučava redovno osoblje za kibernetičku higijenu. Ovaj jaz dovodi do nesigurnih praksi (poput slabih lozinki ili pada na phishing prevare) koje protivnici iskorištavaju.
- ***Nema formalnih politika***: Bez smjernica, malo organizacija civilnog društva uspostavlja sigurnosne politike ili planove odgovora na incidente – ostavljajući ih bez kormila tokom incidenta. Gotovo 80% OCD-a nema politiku/plan sajber sigurnosti. Nastavni plan i program može pomoći organizacijama da kreiraju ove interne politike i strategije odgovora.
- ***Regulatorni pritisak***: Zakoni o zaštiti podataka kao što je EU's General Data Protection Regulation (GDPR) – the world's najsveobuhvatniji zakon o zaštiti podataka – zahtijevaju od organizacija da zaštite lične podatke. OCD moraju poštovati baš kao što to rade kompanije, ili rizikovati pravne i reputacijske posljedice. Izgradnja znanja o takvim propisima je ključni dio kapaciteta digitalne sigurnosti.
- Ovi izazovi naglašavaju zašto je neophodan namjenski nastavni plan i program. On će se pozabaviti jazom u znanju, promovirati kulturu sigurnosti i pružiti OCD-ovima mapu puta za razvoj vlastitih planova, politika i zaštite kibernetičke sigurnosti.

Ciljajte publiku i zainteresovane strane

Primarnu ciljnu grupu nastavnog plana i programa čine organizacije civilnog društva (OCD) i nevladine organizacije, uključujući sljedeće profile:

- ***Osoblje za rukovođenje i upravljanje OCD:***

  Pojedinci odgovorni za organizaciona strategija, upravljanje rizicima i raspodjela resursa, koji zahtijevaju jasno razumijevanje rizika digitalne sigurnosti i institucionalnih odgovornosti.
- ***IT osoblje ili tehničke vokalne tačke:***

  Osoblje odgovorno za implementaciju tehničkih sigurnosnih mjera i podršku sigurnim digitalnim praksama unutar organizacija.
- ***Programsko i operativno osoblje:***

  Za to su potrebni članovi osoblja koji upravljaju dnevnim tokovima podataka,

informacijama o korisnicima, finansijskim podacima i digitalnom komunikacijom jaka svijest o sigurnim digitalnim praksama.

- ***Volonteri i terenski štab:***
  Pojedinci koji koriste organizacioni uređaji ili rukovanje osjetljivim informacijama u terenskim postavkama i trebaju smjernice o sigurnom digitalnom ponašanju.
- ***Partnerske mreže i organizacije zajednice:***
  Organizacije koje rade u saradnji ili koalicijama sa OCD, osiguravajući da se prakse digitalne bezbednosti prošire na institucionalne mreže.

Zainteresovane strane uključene u razvoj i implementaciju nastavnog plana i programa uključuju partnerske organizacije projekta iz zemalja učesnica i stručnjake za sajber sigurnost i digitalnu sigurnost. Ulaz specijalizovanih stručnjaka i institucija osigurava da je nastavni plan i program u skladu sa međunarodno priznatim najboljim praksama u digitalnoj sigurnosti i zaštiti podataka.

Ključni moduli i teme u nastavnom planu i programu

Nastavni plan i program je organizovan u nekoliko modula, od kojih se svaki fokusira na kritični aspekt digitalne bezbednosti. Ispod je pregled ključnih tema koje planiramo uključiti:

1. Osnove digitalne sigurnosti: Razumijevanje pejzaža prijetnje i osnovne higijene – Uvodi zašto je digitalna sigurnost važna za OCD. Prekriva vrste prijetnji (malver, phishing, hacking, DDoS, itd.), aktere prijetnji (kriminalci, neprijateljske vlade koje ciljaju civilno društvo) i fundamentalne najbolje prakse. Naglasak na stvaranju sigurnosnog načina razmišljanja i osnovnih navika (jake lozinke, korištenje dvofaktorske autentifikacije, redovna ažuriranja softvera, izbjegavanje sumnjivih e-poruka).

2. Procjena rizika i planiranje: Procjena organizacionih rizika i kreiranje sigurnosnog plana – vodi CSO kroz identifikaciju njihove digitalne imovine i ranjivosti. Kako provesti jednostavnu procjenu rizika (šta imamo da bi drugi mogli napasti? Kako su to mogli učiniti? Kakve su posljedice?). Ovaj modul će navesti organizacije da izrade ili poboljšaju svoj plan kibernetičke sigurnosti (pošto trenutno 80% nedostaje jedan) – uključujući politike za rukovanje podacima, kontrolu pristupa i proceduru odgovora na incidente.

3. Osiguravanje uređaja i infrastrukture: Zaštita računara, mreža i web stranica – Fokusira na osiguranje tehnologije koju koristi CSO. Teme uključuju sigurnost uređaja (antivirus, enkripciju uređaja, konfiguraciju sigurnog uređaja), sigurnu upotrebu Wi-Fi i mreža, korištenje VPN-ova kada je to prikladno, i osiguranje web stranica (osnove sigurnosti web hostinga, rezervnih kopija, korištenje HTTPS-a, zaštita od defakcije ili DDoS-a). Pravi primjeri napada (npr, slučaj deplasmana web stranice koji je mjesecima isključivao OCD) ilustrirat će važnost ovih mjera.

4. Sigurna komunikacija i saradnja: Safe Email, Messaging i Remote Work – uči kako bezbedno komunicirati kako interno tako i sa spoljnim zainteresovanim stranama. Prekriva sigurnost e-pošte (prepoznavanje phishinga, korištenje šifrirane e-pošte ili sigurnih provajdera e-pošte), aplikacije za razmjenu poruka (izabir sigurnih aplikacija kao što je Signal, omogućavanje end-to-end enkripcije) i sigurno dijeljenje datoteka. Također se bavi izazovima rada na daljinu: korištenje sigurnih veza, zaštita video konferencija i upravljanje računima/kreditima kada radite od kuće ili u pokretu.

5. Zaštita podataka i usklađenost privatnosti: Zaštita podataka i razumijevanje pravnih obaveza – naglašava zaštitu osjetljivih podataka koje CSO prikupljaju (korisnički podaci, podaci o donatorima, itd.). Uvodi principe zaštite podataka: minimiziranje podataka, šifriranje podataka u mirovanju i u tranzitu, sigurno skladištenje/poduzimanje i pravilno odlaganje podataka. Istaknut ćemo relevantne zakone kao što je GDPR – vodeći okvir zaštite podataka u Evropi – i šta usklađenost podrazumijeva za OCD (npr., dobijanje pristanka, osiguranje ličnih podataka, kršenje izvještaja). Ovaj modul osigurava organizacijama da shvate i etičke i pravne odgovornosti u rukovanju podacima.

6. Sigurnost prisustva na društvenim mrežama i na mreži: Zaštita organizacijske reputacije i računa – Mnogi OCD se oslanjaju na društvene mreže za širenje. Ova tema pokriva osiguranje naloga na društvenim mrežama (jake lozinke, autor dva faktora, pristup zasnovan na ulozi za više menadžera), zaštitu od otmice naloga i bavljenje onlajn uznemiravanjem ili kampanjama

dezinformacija. Također uključuje smjernice o upravljanju sadržajem web stranice, sigurnosti i sigurnom ponašanju na mreži koje štite reputaciju CSO's.

7. Razvoj sigurnosne kulture: Obuka osoblja, politike i odgovor na incidente – Fokusira se na ljudske faktore i organizacione mjere. Kako kultivirati kulturu u kojoj svaki član osoblja razumije svoju ulogu u sajber sigurnosti. Smjernice o pisanju jednostavnih IT sigurnosnih politika (prihvatljiva politika korištenja, pravila o donošenju uređaja, itd.), provođenje redovnih obuka o svijesti osoblja (od tada OCSOing obuka je od vitalnog značaja da se 90% osoblja spreči da bude slaba karika) i da se uspostavi plan odgovora na incidente (koraci koje treba preduzeti ako dođe do kršenja, uloge i odgovornosti, komunikaciona strategija tokom sajber krize). We'll također pokriva osnove prijavljivanja incidenata vlastima i učenja iz incidenata

Strategija implementacije nastavnog plana i programa

Razvoj i implementacija ovog nastavnog plana i programa sprovedeni su kao zajednički i fazni proces.

Pregled i lokalizacija nastavnog plana i programa:

Nakon pripreme početnog nacrta, projektni partneri su pregledali materijale nastavnog plana i programa kako bi osigurali njihovu relevantnost za lokalni kontekst. Tokom ove faze, partneri su predložili adaptacije kao što je prevođenje ključne terminologije, uključivanje studija slučaja specifičnih za zemlju i usklađivanje preporuka sa nacionalnim zakonodavstvom i zajedničkom praksom. Kao rezultat toga, nastavni plan i program je strukturiran sa osnovnim okvirom dopunjenim opcionim lokaliziranim odjeljcima za svaku zemlju učesnicu.

Obuka pilota:

Nastavni plan i program je pilotiran malom grupom učesnika OCD-a u odabranim partnerskim zemljama. Implementacija pilota je isporučena ili kao kratki segmenti modula (otprilike 15–20 minuta po modulu) ili kao cjelodnevna radionica. Povratne informacije prikupljene tokom ove faze fokusirale su se na jasnoću, dužinu i praktičnu korisnost sadržaja, a nastavni plan i program je u skladu s tim dorađen.

Sesije voza-trenera:

Kako bi se osigurala skalabilnost i održivost, organizovane su sesije vozova-trenera za projektne partnere i određene predstavnike OCD-a u svakoj zemlji. Ove sesije su pokrivale ne samo sadržaj nastavnog plana i programa, već i vođene tehnike facilitacije, interaktivne vježbe i upite za diskusiju, omogućavajući trenerima da samouvjereno isporuče materijal široj publici.

Poziv na OCD (Zgrada kapaciteta):

Nakon faze obuke, partnerske organizacije su sprovele treninge na nacionalnom nivou za lokalne organe civilnog društva i aktere civilnog društva. Ove obuke su se izvodile putem webinara, ličnih seminara ili su integrisane u postojeće aktivnosti izgradnje kapaciteta. Ovisno o lokalnim potrebama, treninzi su strukturirani kao pojedinačni moduli od 15–20 minuta ili kombinovani u duže radionice koje pokrivaju više modula.

Resursi i OCSOing Podrška:

Svi materijali nastavnog plana i programa i prateći priručnik sastavljeni su i podijeljeni u pristupačnim formatima, prvenstveno kao PDF resursi koji se mogu preuzeti. Osim toga, uspostavljen je online komunikacijski kanal koji omogućava učesnicima i trenerima da postavljaju pitanja, razmjenjuju iskustva i dijele ažuriranja vezana za nove prijetnje ili dobre sigurnosne prakse. Ovo okruženje za vršnjačko učenje podržalo je nastavak angažmana izvan formalnih treninga**.**

Monitoring i evaluacija:

Tokom procesa implementacije sprovedene su aktivnosti praćenja i evaluacije kako bi se procenio uticaj nastavnog plana i programa. Indikatori su uključivali broj obučenih OCD-a, uočene promjene između procjena prije i nakon obuke i kvalitativne povratne informacije o organizacijskim poboljšanjima (kao što je usvajanje politika kibernetičke sigurnosti ili novih procedura zaštite podataka). Ovi nalazi su integrisani u opšti okvir praćenja projekta's kako bi se osiguralo da nastavni plan i program efektivno doprinese jačanju prakse digitalne bezbednosti među organizacijama koje učestvuju.

Prateći ovaj pristup, proces razvoja i implementacije nastavnog plana i programa bio je inkluzivan i iterativan, što je rezultiralo konačnim proizvodom koji je bio dobro prilagođen potrebama organizacija civilnog društva u različitim nacionalnim kontekstima**.**

3.1 MODUL 1: OSNOVE DIGITALNE SIGURNOSTI – RAZUMIJEVANJE PEJZAŽA PRIJETNJE I OSNOVNE HIGIJENE

Do kraja ovog modula, učesnik će moći:

- *Objasnite zašto je digitalna sigurnost ključna za OCD i identificirajte osnovne kiberneginske prakse.*
- *Prepoznajte uobičajene sajber prijetnje (malver, phishing, DDoS, itd.) usmjerene na civilno društvo.*
- *Primijenite osnovne sigurnosne navike (jake lozinke, dvofaktorska autentifikacija, ažuriranja softvera, budnost protiv sumnjivih e-poruka).*

Ciljevi učenja:

- Podignite svijest o tome zašto je digitalna sigurnost ključna za OCD i specifične sajber prijetnje usmjerene na civilno društvo.
- Identificirajte uobičajene vrste sajber napada (npr. zlonamjerni softver, phishing, hacking, DDoS) i aktere prijetnji (kriminalne grupe, neprijateljske vlade) s kojima se mogu suočiti OCD.
- Usvojite osnovne najbolje prakse i navike kibernetičke sigurnosti (npr., stvarajući jake lozinke, omogućavajući dvofaktorsku autentifikaciju, ažuriranje softvera i prepoznavanje sumnjivih komunikacija).

Ključne teme:

- Važnost digitalne sigurnosti za OCD – kako kibernenticidi mogu poremetiti operacije i ugroziti osjetljive podatke.
- Pregled pejzaža prijetnje: uobičajeni tipovi napada kao što su zlonamjerni softver, phishing, hacking, DDoS, itd., i njihova sve veća učestalost protiv civilnog društva.
- Glumci prijetnji koji ciljaju na OCD: od sajber kriminalaca koji traže finansijsku dobit do neprijateljskih grupa koje podržava država s ciljem nadzora ili ometanja aktivnosti OCD-a.
- Osnovne prakse kiberhigijene: korištenje jakih lozinki i upravitelja lozinki, omogućavanje dvofaktorske autentifikacije, održavanje ažuriranja softvera/antivirusa i opreznost uz sumnjive e-poruke ili linkove.

- Izgradnja sigurnosnog načina razmišljanja među osobljem – ohrabruje budnost i kulturu u kojoj svi preuzimaju odgovornost za digitalnu sigurnost.

Uzorci aktivnosti ili vježbe:

- **Prijetnja Brainstorm:** Učesnici navode potencijalne sajber prijetnje svojoj organizaciji i razgovaraju o tome kako bi svaka prijetnja mogla utjecati na njihov rad.
- **Izazov lozinkom:** Polaznici procjenjuju snagu lozinki za uzorke i uče kako kreirati i upravljati jakim lozinkama (npr., lozinkama, koristeći upravitelj lozinkom).
- **Phishing Quiz:** Sadašnji primjer e-pošte (neki phishing, neki legitimni) i imaju učesnike da identifikuju crvene zastavice koje ukazuju na pokušaj phishinga.
- **Diskusija o studiji slučaja:** Opišite nedavni lokalni sajber incident koji utiče na OCD – Analizirajte šta se dogodilo u ovom incidentu i razgovarajte o tome koje su to osnovne sigurnosne mjere mogle spriječiti.

Primjer studije slučaja Modula 1: Phishing Attack on the Community CSO

- **Kontekst:** OCD male zajednice koji pruža hranu i pomoć ugroženim populacijama oslanja se na platforme za donacije putem e-pošte i interneta. Osoblje je imalo minimalnu obuku o sajber sigurnosti i oslanja se samo na osnovnu sigurnost e-pošte.
- **Problem:** Jednog jutra, finansijski službenik CSO's primio je e-mail sa hitnim zvukom od nekoga ko se pretvarao da je glavni donator. E-mail je sadržavao sumnjivu vezu za ažuriranje detalja plaćanja. Policajac je kliknuo na link i ušao u akreditive za prijavu za web stranicu bankovnog računa CSO's, nesvjestan da se radi o phishing stranici. Za nekoliko sati, neovlašćeno povlačenje je izvršeno sa računa CSO's, ukupno hiljade dolara. OCD je morao privremeno obustaviti rad dok je vraćao sredstva i osiguravao račune.
- **Ishod:** Nakon incidenta, OCD je pregledao ovaj sigurnosni neuspjeh uz pomoć volontera koji poznaje tehnologiju. Odmah su implementirali osnovne mjere kibernetičke higijene: provođenje jakih, jedinstvenih lozinki i omogućavanje dvofaktorske autentifikacije na svim računima. Takođe su započeli redovnu obuku osoblja o prepoznavanju phishing e-poruka (tražeći kucanje, provjeravajući adrese

pošiljaoca, itd.). U narednim mjesecima, OCD je uspješno izbjegao slične prevare i vratio povjerenje donatorima tako što je bio transparentan u pogledu poboljšanja.

Pitanja diskusije:

- *Koja je osnovna praksa kibernetičke sigurnosti mogla spriječiti phishing napad u ovom slučaju?*
- *Zašto je član osoblja pao na phishing e-poštu i koji koraci bi mogli pomoći osoblju da prepozna takve prevare u budućnosti?*
- *Kako se OCD oporavio od incidenta i koje mjere su poduzeli za jačanje sigurnosti nakon toga?*

Procjena modula 1

- Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Modul 1 – procjena: kratka pitanja

1. Zašto je digitalna sigurnost posebno važna za organizacije civilnog društva? (Ukratko objasnite kako sajber incidenti mogu uticati na operacije ili korisnike OCD.)
2. Navedi dvije uobičajene sajber prijetnje koje često ciljaju na OCD. (Primjer: phishing, malware, DDoS, itd.)
3. Šta je phishing, i kako obično pokušava prevariti korisnike? (Objasnite osnovnu metodu u jednoj ili dvije rečenice.)
4. Navedite dvije osnovne prakse kiberhigijene koje pomažu u sprečavanju kompromisa računa. (Primjer: jake lozinke, dvofaktorska autentifikacija, redovna ažuriranja.)
5. Spomenite jedan jasan znak upozorenja da bi e-mail mogao biti pokušaj krađe identiteta. (Primjer: hitan jezik, adresa sumnjivog pošiljaoca, neočekivane veze ili prilozi.)

Praktičan zadatak: Identifikacija rizika od krađe

Učesnicima se daje kratak uzorak e-pošte (ili scenarija) koji se odnosi na rad OCD-a (npr., ažuriranje donacije, poruka o finansijeru ili interni zahtjev).

Od učesnika se traži da:

- Odlučite da li je poruka legitimna ili sumnjiva.
- Identificirajte najmanje dva znaka upozorenja (crvene zastavice) u poruci.
- Napišite jednu konkretnu radnju koju bi trebali poduzeti umjesto da kliknu na link ili direktno reaguju (npr, verifikujemo preko drugog kanala, javi se supervizoru).

Kriterijumi procjene:

- Ispravno identifikuje e-poštu kao sumnjivu ili rizičnu,
- Tačno ukazuje na najmanje dvije crvene zastavice
- Predlaže odgovarajući siguran odgovor.

3.2 MODUL 2: PROCJENA RIZIKA I PLANIRANJE – PROCJENA ORGANIZACIONI RIZICI I STVARANJE SIGURNOSNOG PLANA

Do kraja ovog modula, učesnik će moći:

- *Identificirajte kritičnu digitalnu imovinu organizacije i potencijalne ranjivosti.*
- *Provesti osnovnu procjenu rizika procjenom vjerovatnoće i utjecaja prijetnji tim sredstvima.*
- *Nacrtajte jednostavan plan kibernetičke sigurnosti ili politiku koja pokriva rukovanje podacima, kontrolu pristupa i pregled odgovora na incident.*

Ciljevi učenja:

- Razumijete kako identificirati organizaciju's kritična digitalna sredstva (podaci, sistemi, računi) i potencijalne ranjivosti.
- Provesti osnovnu procjenu rizika za procjenu prijetnji toj imovini i potencijalnog uticaja na organizaciju.
- Razvijajte ili poboljšajte plan/politiku kibernetičke sigurnosti za OCD, pokrivajući ključne oblasti kao što su procedure rukovanja podacima, kontrole pristupa i spremnost za odgovor na incidente.

Ključne teme:

- Identifikacija digitalnih sredstava I podataka: mapiranje informacija I sistema koje CSO koristi (npr., baze podataka donatora, naloga e-pošte, web stranica) I zašto bi oni mogli biti ciljani.
- Ranjivosti i prijetnje: razumijevanje kako uočiti slabosti (zastarjeli softver, nedostatak rezervnih kopija, itd.) i zamišljanje scenarija prijetnji (Šta bi napadači mogli ciljati? Kako su to mogli učiniti? Kakve su posljedice?).
- Proces procjene rizika: procjena vjerovatnoće i utjecaja različitih scenarija prijetnji i davanje prioriteta rizicima za prvo rješavanje.
- Stvaranje plana sajber sigurnosti: izrada nacrta organizacijaal sigurnosna politika koja pokriva prakse zaštite podataka, kontrolu pristupa korisniku i proceduru odgovora na incidente (posebno važna jer ~80% OCD trenutno nema formalni sigurnosni plan).

- Održavanje plana ažuriranim: dodjeljivanje odgovornosti za periodično preispitivanje i ažuriranje sigurnosnog plana kao organizacija raste ili se mijenja krajolik prijetnje.

Uzorci aktivnosti ili vježbe:

- **Inventar imovine:** Učesnici navode ključna digitalna sredstva (npr., baze podataka, račune e-pošte, uređaje, usluge u oblaku) na koje se njihov CSO oslanja i identifikuje koje su osjetljive informacije povezane sa svakim.
- **Mapiranje rizika:** Za svaku navedenu imovinu, grupa identifikuje moguće prijetnje ili scenarije neuspjeha i ocjenjuje njihovu vjerovatnoću i utjecaj (stvaranje jednostavne matrice rizika za vizualizaciju rizika visokog prioriteta).
- **Razvoj plana:** Radeći u timovima, učesnici sastavljaju osnovni nacrt plana kibernetičke sigurnosti za uzorak OCD. Ovo bi trebalo da uključuje odeljke o politikama rukovanja podacima, koji imaju pristup njima, i korake koje treba preduzeti ako dođe do bezbednosnog incidenta. Timovi tada dijele svoje planove za povratne informacije.
- **Lokalni scenario rizika:** (Primeri scenarija slučaja uključeni su u odjeljke za lokalizaciju specifične za zemlju.) Učesnici raspravljaju o ovom scenariju i razmišljaju o tome kako bi ublažili rizik, koristeći elemente sigurnosnog plana (politike, preventivne mjere, koraci odgovora).

Studija slučaja modula 2: Ignorisana ranjivost vodi do gubitka podataka

Kontekst: CSO srednje veličine upravlja internim serverom koji pohranjuje podatke donatora i korisnika. Oni znaju da je server važan, ali nemaju formalnu dokumentaciju o njegovim rezervnim kopijama ili rizicima. Osoblje je pretpostavilo da su podaci sigurni jer se “ništa loše nije dogodilo prije.”

Problem: Iznenadni talas struje uzrokovan obližnjom olujom oštetio je serverski hardver CSO’s, oštetivši podatke. Budući da server nije bio podržan mjesecima, svi donatorski zapisi, projektni fajlovi i finansijski podaci su izgubljeni. OCD je bio primoran da prekine svoje programe nedeljama. Donatori su morali da preprodaju informacije, a mnogi zapisi nisu mogli biti pronađeni, što je dovelo do zabune i gubitka povjerenja.

Ishod: Shvativši ozbiljnost ovog neuspjeha, OCD je izvršio detaljnu procjenu rizika uz pomoć izvana. Identificirali su ključna sredstva (baze podataka, web stranica, nalozi e-pošte) i prijetnje

(gubitak snage, kvar hardvera, sajber napadi). Dali su prioritet ulaganju u rezervnu kopiju izvan lokacije sistem I postavljanje redovnog rezervnog rasporeda. OCD je izradio osnovni plan kibernetičke sigurnosti, uključujući procedure za sigurnosne kopije podataka i oporavak. Kasnije, kada su se desili manji sistemski problemi, uspešno su vratili podatke iz rezervnih kopija bez prekida.

Pitanja diskusije:

- *Koji su bili znaci upozorenja da je OCD bio ranjiv prije katastrofe?*
- *Koje elemente treba da OCD uključi u svoj novi plan kibernetičke sigurnosti kako bi spriječio sličan gubitak?*
- *Kako je izvođenje procjene rizika pomoglo OCD-u da poboljša svoju sigurnost i operacije?*

Procjena modula 2

Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Modul 2 – procjena: kratka pitanja

- Šta se smatra digitalnim sredstvom u kontekstu OCD? (Dajte dva primjera.)
- Zašto je rizično da se organizacija osloni na pretpostavku da se “ništa loše nije dogodilo prije nego što je”?
- Koja su dva glavna faktora procijenjena u osnovnoj procjeni rizika? (Nakratko objašnjeno.)
- Navedi dvije uobičajene ranjivosti koje mogu povećati rizike kibernetičke sigurnosti u OCD.
- Zašto je važno redovno pregledavati i ažurirati plan kibernetičke sigurnosti?

Praktični zadatak: Osnovna vježba procjene rizika

Od učesnika se traži da završe sljedeće korake za hipotetički ili pravi OCD:

- Lista jedan kritični digitalni adut (npr., baza podataka donatora, sistem e-pošte, web stranica)

- Identificirajte jednu moguću prijetnju toj imovini (npr., nestanak struje, phishing napad, hardverski kvar)
- Ukratko opišite jednu preventivnu mjeru koja bi mogla smanjiti rizik (npr., sigurnosne kopije, kontrole pristupa, dvofaktorsku autentifikaciju).

Kriterijumi procjene:

- Sredstvo je jasno identifikovano,
- Prijetnja je realna I relevantna,
- Predložena preventivna mjera je prikladna.

3.3 MODUL 3: OSIGURANJE UREĐAJA I INFRASTRUKTURE – ZAŠTITA RAČUNARA, MREŽA I WEB STRANICA

Do kraja ovog modula, učesnik će moći:

- *Implementacija najboljih praksi za osiguranje računara i mobilnih uređaja (instaliranje ažuriranja, anti-malware i enkripcije).*
- *Povjerljiva I zaštita organizacijskih mreža (sigurni Wi-Fi, korištenje VPN-ova za daljinski pristup).*
- *Poboljšajte sigurnost web stranice i servera (omogućite HTTPS, izvršite redovne sigurnosne kopije i branite se od uobičajenih napada kao što su defacement ili DDoS).*

Ciljevi učenja:

- Implementirati najbolje prakse za osiguranje računara I mobilnih uređaja (npr., instaliranje softvera protiv zlonamjernog softvera, omogućavanje šifriranja uređaja I pravilno konfiguriranje sigurnosnih postavki).
- Zaštitite organizacione mreže i pristup internetu putem sigurnih Wi-Fi praksi i korištenja sigurnih veza (kao što su VPN-ovi za daljinski pristup).
- Ojačati sigurnost web stranice CSO's i online infrastrukture korištenjem modernih mjera zaštite (HTTPS, sigurnosne kopije, DDoS zaštita, itd.) i razumijevanjem kako odgovoriti na uobičajene napade.

Ključne teme:

- Sigurnosne osnove uređaja: instaliranje i ažuriranje antivirusnog/anti-malver softvera na svim računarima, omogućavanje zaštitnih zidova i korištenje šifriranja diska na laptopima i pametnim telefonima kako bi se spriječila krađa podataka.
- Sigurna konfiguracija uređaja: provođenje jakih lozinki/PIN-ova za prijavu uređaja, uklanjanje ili onemogućavanje nepotrebnih aplikacija i usluga i redovna primjena sigurnosnih zakrpa ili ažuriranja.
- Osnove mrežne sigurnosti: sigurna upotreba Wi-Fi mreže (koristeći pouzdane mreže, osiguranje kancelarijskog Wi-Fi-ja sa jakim lozinkama i enkripcijom) i kada koristiti VPN-ove za šifrirane veze (posebno na javnim mrežama).

- Sigurnost web stranica i servera: održavanje ažuriranog softvera web stranice (CMS, dodaci), korištenje HTTPS-a za šifriranje web prometa, izvođenje redovnih rezervnih kopija podataka sa stranice i implementacija zaštite od uobičajenih napada kao što su defacement ili DDoS.
- Primjeri infrastrukturnih napada u stvarnom svijetu: na primjer, slučaj otkopavanja web stranice koji je mjesecima isključio CSO, naglašavajući važnost proaktivne odbrane.

Uzorci aktivnosti ili vježbe:

- **Revizija sigurnosti uređaja:** Koristeći kontrolnu listu, učesnici pregledaju uređaj za uzorke (ili svoj vlastiti, ako je prikladno) za osnovnu sigurnosnu zaštitu – provjeru instalacije i ažuriranja antivirusnih virusa, status zaštitnog zida, omogućeno šifriranje i nedavna sigurnosna ažuriranja.
- **Wi-Fi Safety Demo:** Trener pokazuje rizike korištenja neosiguranog javnog Wi-Fi-ja (npr., koliko je lako njuškati u saobraćaju). Zatim razgovarajte o koracima za sigurnost: konfiguriranje sigurne Wi-Fi mreže za dom/kancelariju i korištenje VPN-a ili sigurnih aplikacija kada ste na javnim mrežama.
- **Web stranica Security Review:** Predstavite fiktivni scenario CSO web stranice s nekoliko sigurnosnih nedostataka (zastarjeli softver, bez HTTPS-a, slaba administrativna lozinka). Male grupe identifikuju probleme i preporučuju popravke za poboljšanje sigurnosti web stranice's.
- **Lokalna studija slučaja:** Opišite lokalni slučaj kršenja web stranice CSO ili sajber napada – Diskuss šta se dogodilo u ovom incidentu i koje preventivne mjere (iz modula's ključne teme) mogu pomoći da se izbjegne takav događaj u budućnosti.

  Studija slučaja modula 3: Zabrana web stranice i prekid usluge

  Kontekst: OCD vodi javnu web stranicu za ažuriranja programa i prikupljanje sredstava. Stranica je izgrađena na sistemu upravljanja sadržajem otvorenog koda (CMS). Tehničkim održavanjem upravljao je jedan volonter koji je povremeno ažurirao lokaciju.

  Problem: Hakeri su iskoristili zastarjeli dodatak na web stranici CSOs', narušivši početnu stranicu i zamijenivši je političkom porukom. OCD nije odmah primijetio promjenu jer osoblje nije redovno provjeravalo lokaciju. Oštećenje je ostalo nekoliko dana, što je

izazvalo zabunu među pristalicama i privremeno odvraćalo donatore. Posjetioci su vidjeli neprikladan sadržaj i kredibilitet organizacije's oštećen je. Osim toga, hakeri su dobili pristup datotekama web stranice's, što je izazvalo zabrinutost u vezi sa sigurnošću podataka donatora (iako nije potvrđeno kršenje).

Ishod: Nakon što je otkrio problem, CSO je isključio web stranicu radi čišćenja i uklonio zlonamjerni sadržaj. Ažurirali su CMS i sve dodatke najnovijim verzijama. Ubuduće, CSO je implementirao redovne sigurnosne kopije stranica i zakazane sedmične provjere svoje web stranice. Takođe su prešli na upravljanog provajdera hostinga sa automatskim ažuriranjima i HTTPS enkripcijom. U narednim mjesecima, stranica je ostala sigurna, a OCD je povratio povjerenje transparentnom komunikacijom o incidentu i koracima koji su poduzeti da se to spriječi.

Pitanja diskusije:

- *Kako je softver mogao ažurirati i redovne sigurnosne kopije promijenile ishod ovog napada?*
- *Koje je neposredne korake trebalo da CSO preduzme kada je primetio da je web stranica pokvarena?*
- *Koje dugoročne mjere je OCD implementirao kako bi osigurao svoju web infrastrukturu?*

Procjena modula 3

Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Modul 3 – procjena

Kratka pitanja

1. Zašto je enkripcija uređaja važna za laptope i pametne telefone koje koriste CSO? *(Odgovori u jednoj ili dvije rečenice.)*

2. Navedi dvije osnovne sigurnosne mjere koje treba omogućiti na svim organizacionim uređajima.
3. Koji su glavni rizici korištenja neosiguranog javnog Wi-Fi-ja bez dodatne zaštite?
4. Zašto zastarjeli CMS dodaci predstavljaju ozbiljan sigurnosni rizik za web stranice CSO?
5. Kako redovne sigurnosne kopije smanjuju utjecaj narušavanja web stranica ili sajber napada?

Praktični zadatak: osnovni uređaj ili provjera sigurnosti web stranice

Učesnici biraju jednu od sljedećih opcija:

Opcija A – Sigurnost uređaja

- Lista **tri sigurnosne mjere** trenutno se primjenjuje na jedan radni uređaj (računar ili pametni telefon)
  (npr. antivirusni, enkripcija, zaključavanje ekrana, ažuriranja)
- Identifikovati **jedna nestala ili slaba mjera** i ukratko navedite kako se to može poboljšati.

Opcija B – sigurnost web stranice

- Identifikovati **dvije osnovne sigurnosne kontrole** to bi trebalo biti na mjestu a CSO web. *(npr., HTTPS, redovna ažuriranja, sigurnosne kopije, jake admin lozinke)*
- Kratko objasniti **jedan rizik** ako se ove kontrole ne implementiraju.

Kriterijumi procjene:

- Identifikovane mjere su relevantne za modul.
- Rizici ili poboljšanja su realni i jasno objašnjeni.

Zahtjev za donošenje:
Učesnik mora ispravno identificirati najmanje dvije važeće sigurnosne mjere i jednu povezanu opasnost ili poboljšanje.

3.4 MODUL 4: SIGURNA KOMUNIKACIJA I SARADNJA – SIGURNA E-POŠTA, PORUKE I RAD NA DALJINU

Do kraja ovog modula, učesnik će moći:

- *Prepoznajte i izbjegavajte uobičajene prijetnje zasnovane na e-pošti (kao što je phishing) i primijenite sigurne prakse e-pošte (jake lozinke, 2FA).*
- *Koristite sigurne poruke i alate za razmjenu datoteka koji pružaju enkripciju.*
- *Implementacija sigurnih praksi rada na daljinu (koristeći VPN-ove na javnim mrežama, osiguravanje virtuelnih sastanaka lozinkama).*

Ciljevi učenja:

- Prepoznajte i izbjegavajte uobičajene prijetnje zasnovane na e-pošti (kao što su phishing prevare) i primijenite sigurne prakse e-pošte u svakodnevnom radu.
- Odaberite i koristite sigurne komunikacijske alate za razmjenu poruka i dijeljenja datoteka (npr. end-to-end šifrirane aplikacije, platforme za sigurnu saradnju s dokumentima) za zaštitu osjetljivih informacija.
- Implementacija sigurnosnih mjera za rad na daljinu i virtuelnu saradnju (koristeći sigurne mreže, zaštitu online sastanaka i upravljanje računima/uređajima prilikom rada van lokacije).

Ključne teme:

- **Sigurnost e-pošte:** Kako uočiti pokušaje krađe identiteta (npr., sumnjive pošiljaoce ili linkove, hitne, neobične zahtjeve) i važnost korištenja jakih lozinki i 2FA za račune e-pošte. Ako se razmjenjuju osjetljivi podaci, razmotrite šifrirane usluge e-pošte ili dodatke.
- **Sigurna poruka:** Odabir pouzdanih aplikacija za razmjenu poruka koje nude end-to-end enkripciju (na primjer, Signal ili drugi sigurni glasnici) i omogućavanje sigurnosnih funkcija kao što su poruke koje nestaju. Smjernice o verifikaciji kontakata i ne dijeljenju osjetljivih informacija o nesigurnim kanalima.
- **Dijeljenje datoteka i saradnja:** Korištenje sigurne pohrane u oblaku ili usluga dijeljenja datoteka koje nude enkripciju. Prakse poput zaštite osjetljivih dokumenata ili korištenja platformi dizajniranih za sigurnu saradnju kada radite sa vanjskim partnerima.

- **Zaštitne mjere rada na daljinu:** Najbolje prakse za rad izvan ureda, uključujući korištenje VPN-ova na mrežama bez povjerenja, osiguranje kućnih Wi-Fi rutera, zaštitu virtuelnih prostora za sastanke (koristeći čekaonice, lozinke za sastanke, ograničavanje dijeljenja ekrana) i upravljanje radnim uređajima koji se koriste na daljinu.
- **Balansiranje sigurnosti i pristupačnosti:** Osiguravanje da su sigurnosne mjere (kao što su kontrole šifriranja i pristupa) dovoljno prilagođene korisniku da će ih osoblje dosljedno koristiti i pružanje obuke o bilo kojem novom komunikacijskom alatu uvedenom iz sigurnosnih razloga.

Uzorci aktivnosti ili vježbe:

- **Vježbanje phishing Email:** Fasilitator dijeli uzorke e-poruka sa grupom. Učesnici moraju odlučiti za svakog da li on predstavlja legitimnu e-poštu ili pokušaj krađe identiteta i istaći tragove koji su informirali o njihovoj odluci.
- **Poređenje aplikacija za razmjenu poruka:** Prelomite se u male grupe; svaka grupa pregledava različitu aplikaciju za razmjenu poruka (npr., WhatsApp, Signal, Telegram) i izvještava o svojim sigurnosnim funkcijama (šifriranje, dvofaktorska autentifikacija, itd.) i svim ograničenjima. Razgovarajte koje su aplikacije najprikladnije za različite vrste komunikacija OCD-a.
- **Sigurno postavljanje video poziva:** Demonstracija uživo o postavljanju online sastanka sa odgovarajućom sigurnošću: omogućavanje čekaonice, zahtijevanje lozinke za sastanke, ograničavanje dijeljenja ekrana učesnika, itd. Nakon demo-a, učesnici vježbaju konfiguriranje ovih postavki ili razgovaraju o iskustvima osiguravanja vlastitih sastanaka.
- **Diskusija o lokalnom kontekstu:** [Ubacite siguran komunikacijski alat popularan u vašoj zemlji ili relevantan zakon o šifriranju] – raspravljajte o tome kako ovaj lokalni kontekst utječe na komunikacijsku sigurnost CSO's. Na primjer, ako se određena šifrirana aplikacija široko koristi lokalno, kako je CSO može iskoristiti? Ako postoje lokalni propisi o šifriranju ili skladištenju podataka, kako oni utiču na izbore komunikacije?

Studija slučaja Modul 4: Udaljeni prekid e-pošte na rad

Kontekst: Tokom humanitarne krize, terenski službenik CSO's radi na daljinu iz kafića koristeći javni Wi-Fi za slanje izvještaja o situaciji u sjedište. Organizacija koristi e-poštu za svakodnevnu komunikaciju, ali ne provodi šifrirane veze za udaljene korisnike.

Problem: Sajber kriminalac na istoj javnoj Wi-Fi mreži presreo je neošifrirani promet e-pošte Officer's. Napadač je dobio vjerodajnice za prijavu kada se policajac prijavio na CSO's e-mail nalog. Sljedećeg dana, napadač se lažno predstavljao kao policajac, šaljući lažne mejlove donatorima tražeći hitna sredstva za lažni projekat. Jedan donator je prebacio novac na račun napadača's prije nego što je prevara otkrivena. OCD je izgubio sredstva i morao je da objasni prevaru donatorima.

Ishod: Kao odgovor, OCD je implementirao sigurne komunikacijske prakse. Od svih zaposlenih koji rade na daljinu se tražilo da koriste VPN ili HTTPS za pristup e-pošti, a dvofaktorska autentifikacija je omogućena na nalozima e-pošte. OCD je također usvojio šifriranu aplikaciju za razmjenu poruka za interne komunikacije. Komunicirali su s donatorima o provjeravanju budućih zahtjeva i poboljšanoj obuci e-pošte za osoblje (spotiranje laži putem e-pošte, ne korištenje javnog Wi-Fi-ja bez zaštite). Nakon ovih mjera nije bilo daljnjih incidenata.

Pitanja diskusije:

- *Kakve ranjivosti je CSO's prakse rada na daljinu imala u ovom slučaju?*
- *Kako su VPN-ovi i dvofaktorska autentifikacija mogli spriječiti napadača da dobije pristup?*
- *Koje korake je OCD preduzeo nakon kršenja kako bi zaštitio komunikacije i povjerenje donatora?*

Procjena modula 4

Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Modul 4 – procjena

5 Kratkih pitanja

1. Koja su dva uobičajena znaka da bi e-mail mogao biti pokušaj krađe identiteta? *(Nakratko odgovori.)*
2. Zašto je dvofaktorska autentifikacija (2FA) posebno važna za naloge e-pošte koje koriste OCD?
3. Navedi jednu sigurnu funkciju za razmjenu poruka koja pomaže u zaštiti osjetljivih komunikacija.
4. S kojim rizicima se suočava OCD kada osoblje radi na daljinu koristeći javni Wi-Fi bez zaštite?
5. Kako osiguranje online sastanaka (npr., lozinke, čekaonice) može smanjiti sigurnosne rizike?

Praktični zadatak: Sigurna provjera komunikacije

Učesnici obavljaju sljedeći zadatak pojedinačno ili u parovima:

1. **Izaberi jedan komunikacijski kanal** koristi tvoj CSO
   (e-pošta, aplikacija za razmjenu poruka, platforma za razmjenu datoteka ili alat za video sastanke).
2. Kratak odgovor:
   - **Trenutno postoji jedna mjera sigurnosti**
     (npr. 2FA omogućeno, šifrirano slanje poruka, lozinke za sastanke)
   - **Jedno poboljšanje** to bi moglo ojačati sigurnost
     (npr., omogućavanje korištenja VPN-a, prelazak na šifriranu aplikaciju, ograničavanje prava pristupa)
3. Objasniti **jedna ili dvije rečenice** kako bi ovo poboljšanje smanjilo rizik.

Kriterijumi procjene:

- Odabrani kanal je relevantan za komunikaciju OCD
- Sigurnosne mjere i poboljšanja su realni,
- Objašnjenje pokazuje razumijevanje sigurnih komunikacijskih praksi.

3.5 MODUL 5: ZAŠTITA PODATAKA I USKLAĐENOST PRIVATNOSTI – ZAŠTITA PODATAKA I RAZUMIJEVANJE PRAVNIH OBAVEZA

Do kraja ovog modula, učesnik će moći:

- *Identificirajte osjetljive podatke koje OCD prikuplja i objasnite zašto ih morate zaštititi.*
- *Primijenite ključne prakse zaštite podataka (minimalizacija podataka, enkripcija, sigurno skladištenje, redovne sigurnosne kopije i sigurno odlaganje).*
- *Razumije i ocrtava pravne obaveze CSO's prema zakonima o zaštiti podataka (kao što je GDPR) i kako osigurati usklađenost.*

Ciljevi učenja:

- Prepoznajte vrste osjetljivih podataka (npr. lične podatke korisnika, podatke o donatorima) koje CSO prikupljaju i zašto je ključno zaštititi takve podatke.
- Primijenite ključne principe zaštite podataka – uključujući minimizaciju podataka, enkripciju (za podatke u mirovanju i u tranzitu), sigurno skladištenje/poduzimanje i pravilno odlaganje podataka – kako biste poboljšali privatnost i sigurnost.
- Razumije pravne obaveze i okvire za zaštitu podataka, kao što su EU's GDPR i ekvivalentni nacionalni zakoni o zaštiti podataka, i kako osigurati da CSO poštuje ove propise.

Ključne teme:

- **Identifikacija osjetljivih podataka:** Ono što se računa kao lični ili osjetljivi podaci u kontekstu OCD (imeni, adrese, informacije o zdravstvenim ili pravnim slučajevima, itd.), i rizici ako takvi podaci procure.
- **Principi zaštite podataka:** Praktični koraci za minimiziranje podataka (sakupljanje samo onoga što je zaista potrebno), šifriranje podataka u mirovanju (npr., datoteke na diskovima) i u tranzitu (koristeći SSL/HTTPS za prijenos podataka), sigurna rješenja za pohranu podataka (fizički i oblačni), održavanje redovnih rezervnih kopija i pravilno brisanje podataka koji' više nisu potrebni.

- **Pravni okviri:** Pregled glavnih zakona o zaštiti podataka –, na primjer, GDPR (Opšta regulativa o zaštiti podataka) kao vodeći okvir u Evropi i [Insert your country's regulativa zaštite podataka ovdje]. Ključne obaveze uključuju dobijanje informisanog pristanka za prikupljanje podataka, obezbeđivanje ličnih podataka putem tehničkih i organizacione mjere i zahtjevi za obavještenje o kršenju.
- **Etičko rukovanje podacima:** Osim pravnih pravila, naglašavajući etičku odgovornost za zaštitu privatnosti pojedinaca'. Rasprava o posljedicama kršenja podataka za OCD, uključujući štetu korisnicima, gubitak povjerenja, zakonske kazne i štetu reputaciji.
- **Usklađenost sa izgradnjom u praksi:** Kako OCD mogu razviti jednostavne politike privatnosti, smjernice za rukovanje podacima i obučiti osoblje o ovim politikama. Uvod u koncepte kao što su službenici za zaštitu podataka (ako su relevantni) ili sporazumi o rukovanju podacima kada radite sa partnerima.

Uzorci aktivnosti ili vježbe:

- **Vježba revizije podataka:** Učesnici nabrajaju vrste ličnih podataka koje njihov OCD prikuplja ili obrađuje i mapiraju gdje se ti podaci pohranjuju (baze podataka, tabele, e-pošta, usluge u oblaku). Zatim razgovaraju za svaku stavku: ko ima pristup, kako se trenutno štiti i sve praznine koje primjećuju.
- **Šifrovanje Demo:** Trener demonstrira šifriranje datoteke uzorka ili fascikle (ili korištenje alata za šifriranje za e-poštu/tekst). Učesnici uče kako šifrovani podaci izgledaju i praktikuju šifriranje i dešifriranje dijela podataka o testiranju, naglašavajući važnost upravljanja ključem/lozinkom.
- **Pregled politike:** Obezbedite predložak ili primer jednostavne politike zaštite podataka ili Obaveštenja o privatnosti. U malim grupama, učesnici identifikuju kako se ovaj dokument bavi zahtjevima GDPR-a i razmatraju koje bi promjene bile potrebne da bi se uskladilo sa [Ovdje potvrdite regulativu zaštite podataka svoje zemlje]. Svaka grupa može predstaviti jednu ključnu tačku koju će'd uključiti u svoju vlastitu politiku CSO's.
- **Diskusija o pravnom usklađivanju:** Pregledajte kontrolnu listu radnji za usklađenost sa GDPR-om (npr., imenovanje odgovorne osobe, formulare za pristanak, plan kršenja podataka). Učesnici raspravljaju o tome koje stavke na listi imaju i koje moraju

implementirati. Naglasite sve dodatne korake koje zahtijeva nacionalni zakon (npr., registriranje podataka zaštitno tijelo ako to zahtijeva [Potvrdite regulativu zaštite podataka svoje zemlje.]).

Studija slučaja modula 5: Kršenje baze podataka donatora

Kontekst: Međunarodna pomoć CSO održava bazu podataka informacija o donatorima (ime, kontakt podaci, istorija donacija) i podatke o korisnicima (osjetljive zdravstvene informacije). Podaci se pohranjuju na internom mrežnom disku dostupnom programskom osoblju.

Problem: Tokom nadogradnje sistema, administrator je slučajno razotkrio fasciklu baze podataka donatora na javnoj vezi za dijeljenje datoteka u oblaku bez šifriranja ili kontrole pristupa. Haker je otkrio link I preuzeo cijelu listu donatora. Lične informacije hiljada donatora (ime, e-mailovi i iznosi donacija) procurile su na internet. OCD je bio primoran da obavijesti donatore o kršenju kako to zahtijeva zakon. Nekoliko donatora je povuklo podršku, navodeći gubitak povjerenja. OCD se također suočio sa ispitivanjem jer nije pravilno obezbedio podatke.

Ishod: Nakon kršenja, OCD je revidirao svoje prakse rukovanja podacima. Šifrovali su sve osjetljive podatke u mirovanju i tranzitu, te ograničili pristup bazi podataka implementacijom jakih kontrola pristupa. Također su primijenili minimizaciju podataka uklanjanjem nepotrebnih ličnih podataka iz javnih datoteka. OCD je imenovao službenika za zaštitu podataka da nadgleda usklađenost i izradio jasnu politiku privatnosti. Obuka je data osoblju o pravilnom rukovanju podacima, a buduće dijeljenje je obavljeno sigurnim vezama i lozinkama. OCD je povratio povjerenje od svojih donatora tako što je brzo pooštrio sigurnost i transparentno izvijestio o poboljšanjima.

Pitanja diskusije:

- *Koji su propusti u zaštiti podataka doveli do ovog kršenja i kako su mogli biti spriječeni?*
- *Koje prakse zaštite podataka (iz ovog modula's teme) je CSO usvojio nakon incidenta?*
- *Koje zakonske obaveze je OCD morao da se pozabavi ovim kršenjem, i zašto je usklađenost važna za OCD?*

Procjena modula 5

Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Procjena modula 5

Kratka pitanja

1. Koje vrste ličnih ili osjetljivih podataka obično prikupljaju OCD i zašto se ovi podaci moraju zaštititi?
2. Objasnite princip minimizacije podataka i dajte jedan praktičan primjer kako a CSO mogu ga primijeniti.
3. Koja je razlika između šifriranja podataka u mirovanju I šifriranja podataka u tranzitu?
4. Prema GDPR-u (ili ekvivalentnim nacionalnim zakonima o zaštiti podataka), šta je a CSO potrebno je da se uradi u slučaju povrede ličnih podataka?
5. Zašto je etičko rukovanje podacima važno za OCD osim zakonskog poštovanja? Spominje jednu potencijalnu posljedicu neuspjeha da se podaci pravilno zaštite.

Praktični zadatak: pregled zaštite mini podataka

Od učesnika se traži da završe sljedeći zadatak:

- Identifikovati **jedna vrsta ličnih ili osjetljivih podataka** prikupljeno od strane njihovog CSO (npr., evidencija korisnika, podaci o kontaktu sa donatorima, informacije o osoblju).
- Ukratko opišite:
    - Gdje se ovi podaci pohranjuju (npr., kompjuter, usluga u oblaku, e-pošta, papirne datoteke)
    - Ko ima pristup tome,
    - Jedno poboljšanje koje bi se moglo napraviti kako bi se bolje zaštitili ovi podaci (npr., enkripcija, ograničen pristup, minimizacija podataka).

Učesnici bi trebali predstaviti svoje odgovore **za tri do pet kratkih metaka** ili o njima kratko raspravljati u malim grupama.

3.6 **MODUL 6: DRUŠTVENI MEDIJI I SIGURNOST PRISUSTVA NA INTERNETU – ŠTITI ORGANIZACIONU REPUTACIJU I NALOGE**

Do kraja ovog modula, učesnik će moći:

- *Primijenite sigurnosne mjere za zaštitu naloga na društvenim mrežama CSO's (jake, jedinstvene lozinke, dvofaktorska autentifikacija, ograničene uloge administratora).*
- *Efikasno odgovorite na incidente na društvenim mrežama (otmica računa ili lažno predstavljanje) slijedeći procedure izvještavanja i komunikacije.*
- *Implementirajte najbolje prakse za održavanje sigurnog prisustva na mreži (redovna ažuriranja web stranice/CMS, smjernice osoblja za objavljivanje i reagovanje na dezinformacije).*

Ciljevi učenja:

- Implementacija sigurnosnih mjera za zaštitu naloga na društvenim mrežama CSO's (snažna autentifikacija, nadgledani pristup, redovne revizije postavki naloga).
- Razvijajte strategije za zaštitu organizacije. Naglašava prisustvo i reputaciju na mreži, uključujući kako odgovoriti na otmicu računa, lažno predstavljanje ili napade dezinformacija.
- Primijenite najbolje prakse za upravljanje sadržajem web stranica i osoblje koje provodi online kako biste osigurali dosljedno i sigurno organizacijsko predstavljanje na internetu.

Ključne teme:

- **Sigurnost naloga na društvenim mrežama:** Osiguravanje svih organizacionih naloga na društvenim mrežama koristi snažne, jedinstvene lozinke i omogućava dvofaktorsku autentifikaciju. Upravljanje više administratora bezbedno (koristeći kontrole pristupa zasnovane na ulozi ili karakteristike timske saradnje, umesto da dele lozinke).
- **Praćenje i oporavak računa:** Držati na oku aktivnosti računa (tako da je svaki neovlašteni pristup rano uhvaćen) i znati kako povratiti račune ako su ugroženi (razumijevanje procesa podrške platformi za hakovane račune).
- **Rukovanje otmicom i lažno predstavljanje:** Koraci koje treba poduzeti ako je CSO's račun otet ili ako se lažni nalozi lažno predstavljaju kao CSO –, uključujući mehanizme

izvještavanja o društvenim mrežama platforme, komunikacija sa pristalicama kako bi se razjasnile dezinformacije i ponovno preuzimanje kontrole nad računima.

- **Suočavanje s uznemiravanjem na mreži i dezinformacijama:** Taktike za reagovanje na trolove ili koordinirane kampanje uznemiravanja (npr., dokumentovanje zlostavljanja, korištenje blok/izvještajnih funkcija, politika moderiranja za komentare). Kako se suprotstaviti dezinformacijama ili kleveti na internetu činjeničnim porukama bez pojačavanja lažnih tvrdnji.
- **Sigurnost web stranica i upravljanja sadržajem:** Održavanje web stranice CSO's sigurnim i renomiranim – redovno ažuriranje web stranice CMS/plugins, korištenje sigurnih lozinki za admine stranice, ograničavanje ko može objavljivati sadržaj i proces brzog ispravljanja ili uklanjanja netačnog ili neovlaštenog sadržaja.
- **Upravljanje reputacijom:** Osoblje za obuku i volonteri na smjernicama za predstavljanje organizacije na mreži (lične politike korištenja društvenih medija, šta ne objavljivati o poslu, kako odgovoriti ako vide dezinformacije), kako bi se održalo pozitivno i sigurno prisustvo na mreži za OCD.

Uzorci aktivnosti ili vježbe:

- **Provjera sigurnosti računa:** Učesnici sprovode brzu reviziju jednog od naloga na društvenim mrežama CSOs's. Oni provjeravaju da li je 2FA omogućen, lozinke su jake/nedavno ažurirane, informacije o kontaktu s oporavkom su tačne i samo ovlašteni ljudi imaju pristup. Zatim kreiraju listu obaveza za sva potrebna poboljšanja.
- **Igra uloga incidenta:** Simulirajte scenario u kojem je otet službeni nalog na društvenim mrežama CSO's ili lažni nalog širi lažne informacije o organizaciji. Tim mora odlučiti o planu hitne akcije: ko će komunicirati s javnošću, kako upozoriti platformu i sljedbenike i koje korake da osigura ili povrati račun. Nakon igranja uloga, razgovarajte o tome šta je prošlo dobro i šta bi se moglo poboljšati u njihovom odgovoru.
- **Plan odgovora na uznemiravanje:** U grupama, učesnici izrađuju jednostavan protokol za rukovanje onlajn kampanjama uznemiravanja ili mržnje. Ovo može uključivati korake poput: nemojte se javno upuštati u ljutnju, dokumentirati uvredljive postove, prijaviti ih

platformi, upozoriti CSO's menadžment i podržava svako ciljano osoblje. Grupe dijele svoje planove i razgovaraju o zajedničkim elementima.

- **Lokalni primjer rasprave:** [Opišite nedavni incident povezan s lokalnim društvenim medijima koji uključuje OCD] – Analizirajte šta se dogodilo i kako bi snažna sigurnosna praksa društvenih medija i plan odgovora na incidente mogli pomoći u upravljanju ili sprječavanju takve situacije.

Studija slučaja modula 6: Otmica računa društvenih medija

Kontekst: OCD za zaštitu životne sredine koristi društvene mreže (Twitter i Facebook) da angažuje donatore i podeli vesti o kampanji. Više članova osoblja ima pristup računima sa zajedničkim lozinkama, a niko ne prati blisku aktivnost prijave.

Problem: Jednog jutra, CSO's Twitter nalog je počeo da objavljuje zapaljive političke poruke koje nisu povezane sa misijom CSO's. Sljedbenici su bili zbunjeni, a neki su optužili OCD da zauzima politički stav. Objave su bile djelo hakera koji je dobio pristup nakon što je jedan član osoblja ponovo koristio zajedničku lozinku. Do trenutka kada je osoblje shvatilo kršenje, pristalice su retvitovale poruke, uzrokujući štetu reputaciji. Trebalo je nekoliko sati da se povrati pristup kroz proces podrške platforme's, tokom kojeg su se negativni utisci proširili na internet.

Ishod: OCD je izvršio odgovor na incident tako što je odmah objavio pojašnjenje na svim kanalima, izvinjavajući se zbog kršenja. Resetovali su sve lozinke društvenih medija i omogućili dvofaktorsku autentifikaciju na svim nalozima. Oni su također uspostavili pristup zasnovan na ulogama (dodjeljivanje specifičnih administrativnih naloga umjesto dijeljenja lozinki). Osoblje je pregledalo i ažuriralo sadržaj web stranice kako bi osiguralo da nema zastarjelih informacija. OCD je uspostavio politiku za svakodnevno praćenje aktivnosti računa. Kao rezultat toga, uspjeli su obnoviti normalnu komunikaciju, a kasnije su čak dobili podršku da budu transparentni. Nove sigurnosne mjere spriječile su daljnje pokušaje otmice.

Pitanja diskusije:

- *Koji su bili ključni neuspjesi koji su omogućili otmicu računa?*
- *Kako je OCD odgovorio da ublaži štetu, kako tehnološki tako i u komunikacijama?*

- *Koja sigurnosna poboljšanja je OCD implementirao kako bi zaštitio svoje prisustvo na društvenim mrežama u budućnosti?*

Procjena modula 6

Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Procjena modula 6

Kratka pitanja

1. Zašto je važno da OCD koriste jake, jedinstvene lozinke i dvofaktorsku autentifikaciju na nalozima društvenih medija?
2. Koji rizici mogu nastati dijeljenjem lozinki za račune na društvenim mrežama među više članova osoblja?
3. Koje neposredne korake treba a CSO uzmimo da li je njegov nalog na društvenim mrežama otet ili kompromitovan?
4. Kako dezinformacije na mreži ili lažno predstavljanje mogu uticati a CSO's reputacija i povjerenje javnosti?
5. Zašto je važno imati jasne smjernice osoblja za ponašanje na mreži i predstavljanje organizacije?

Praktični zadatak: Pregled sigurnosti društvenih medija

Od učesnika se traži da završe sljedeći zadatak:

- Izaberi jedan službeni nalog na društvenim mrežama njihovog OCD (ili hipotetičkog OCD).
- Ukratko opišite:
    - Da li je dvofaktorska autentifikacija omogućena,
    - Kako se trenutno upravlja pristupom (zajedničke lozinke u odnosu na pristup zasnovan na ulozi),

- Jedna konkretna akcija koja bi mogla poboljšati sigurnost ili praćenje ovog računa.

Učesnici bi trebali sumirati svoje odgovore u tri pet kratkih metaka ili o njima kratko raspravljati u malim grupama.

3.7 MODUL 7: RAZVOJ SIGURNOSNE KULTURE – OBUKE OSOBLJA, POLITIKE I ODGOVORA NA INCIDENTE

Do kraja ovog modula, učesnik će moći:

- *Podsticati kulturu svjesnu sigurnosti u organizaciji uključivanjem vodstva i osoblja.*
- *Razvijajte osnovne politike IT sigurnosti (npr., prihvatljiva upotreba, BYOD, pravila lozinke) i planirajte redovnu sigurnosnu obuku za svo osoblje.*
- *Kreirajte i uvježbajte jednostavan plan odgovora na incidente (definirajući uloge, korake i komunikaciju) za efikasno rješavanje kibernetičkih incidenata.*

Ciljevi učenja:

- Hranite kulturu koja je svjesna sigurnosti unutar OCD-a, gdje svaki član osoblja razumije svoju ličnu ulogu u održavanju sajber sigurnosti.
- Razvijajte osnovne politike IT sigurnosti (npr., prihvatljiva upotreba tehnologije, donosite pravila uređaja) i implementirajte redovne programe obuke osoblja za jačanje dobrih sigurnosnih praksi.
- Uspostavite i uvježbajte plan odgovora na incidente kako bi organizacija mogla efikasno odgovoriti na incidente kibernetičke sigurnosti (očigledno definišući korake, uloge i komunikacijske kanale).

Ključne teme:

- **Izgradnja kulture sajber sigurnosti:** Kako dobiti angažman rukovodstva i osoblja za sigurnosne inicijative. Stvaranje okruženja u kojem se zaposleni osjećaju odgovornim za zaštitu podataka i sistema, umjesto da sigurnost vide samo kao posao IT osobe.
- **Osnovne sigurnosne politike:** Izrada jednostavnih, jasnih politika koje postavljaju očekivanja za sigurnu upotrebu tehnologije. Primjeri uključuju Politiku prihvatljive upotrebe (ono što je dozvoljeno/zabranjeno na radnim uređajima i računima), smjernice BYOD-a (donošenje-svoj uređaj) ako osoblje koristi lične uređaje za rad i pravila za kreiranje i upravljanje lozinkama.

- **Kontinuirana svijest i obuka osoblja:** Važnost OCSOing obrazovanje (radionice, bilteni, testovi simulacije krađe identiteta) kako bi sigurnosno znanje ostalo svježe. Napominjući da je redovna obuka od vitalnog značaja jer neobučeno osoblje može postati najslabija karika u sigurnosti.
- **Planiranje odgovora na incidente:** Ključne komponente plana odgovora na incident – kako otkriti i prijaviti incident, neposredne korake za suzbijanje problema (npr. isključivanje pogođenih računara), uloge i odgovornosti (koji vodi odgovor, koji komunicira sa dionicima) i kako održati operacije tokom poremećaja.
- **Izvještavanje i učenje iz incidenata:** Smjernice o tome kada i kako prijaviti sajber incidente vlastima ili regulatorima (posebno ako su uključeni lični podaci) i provesti pregled nakon incidenta kako bi se poboljšala buduća otpornost.

Uzorci aktivnosti ili vježbe:

- **Radionica pisanja politike:** Učesnici kreiraju nacrt za jednu kratku sigurnosnu politiku relevantnu za njihov OCD (na primjer, Politika prihvatljive upotrebe kancelarijskih računara ili Politika mobilnih uređaja). Svaka grupa piše nekoliko ključnih pravila, a zatim dijeli sa svima, pozivajući na povratne informacije kako bi se osiguralo da su politike jasne i djelotvorne.
- **Vježba o svijesti o sigurnosti:** Organizirajte lažnu phishing vježbu ili iznenadni "USB drop" (ostavljajući USB fleš disk kao da je pronađen, da vidite da li ga neko uključuje). Nakon toga, razgovarajte o rezultatima: kako je osoblje reagovalo? Koje su bile crvene zastavice? Koristite ovo kao priliku za učenje za jačanje bodova obuke u sigurnom okruženju.
- **Tabletop odgovora na incidente:** Predstavite hipotetički incident kibernetičke sigurnosti (npr. napad ransomware-a koji šifrira podatke o CSO-u). Neka tim prođe kroz svoj odgovor korak po korak: kako da identifikuje obim problema, koga prvo zovu, kako komuniciraju sa osobljem, a možda i sa javnošću, i kako da povrate sisteme ili podatke? Nakon vježbe, izvještaj o tome šta je prošlo dobro i koje uloge ili korake treba pojašnjenje u njihovom planu.

- **Informacije o lokalnom izvještavanju:** [Ovdje uključite svoj country's mehanizam za izvještavanje o sajber incidentima ili relevantan kontakt s autoritetima] – Pobrinite se da učesnici budu svjesni kako prijaviti ozbiljan incident kibernetičke sigurnosti u svom lokalnom kontekstu (na primjer, obavještavanje nacionalnog CERT ili policija) i raspravljaju o svim zakonskim zahtjevima za prijavljivanje kršenja koji se primjenjuju na OCD u njihovoj zemlji.

Studija slučaja modula 7: Neosigurani USB koji vodi do izbijanja zlonamjernog softvera

Kontekst: Kancelarija OCD-a omogućila je osoblju da koristi lične USB diskove na radnim računarima. Nije bilo pisane politike ili obuke o uklonjivoj upotrebi medija. Novi volonter je često koristio svoj USB stick.

Problem: Jednog dana, član osoblja pronašao je USB disk na parkingu kancelarije (vjerovatno ga je neko ispustio). Zanimljivi, uključili su ga u svoj kancelarijski računar i otvorili dokument na njemu. USB je zaražen zlonamjernim softverom. Malver se brzo proširio preko mreže CSO's, šifrirajući datoteke na više računara. Podaci CSO's bili su nedostupni, a operacije su prekinute. Nedostatak plana odgovora na incident izazvao je zabunu: niko nije znao ko će voditi odgovor ili koga obavijestiti.

Ishod: Nakon što je obuzdao epidemiju isključivanjem pogođenih mašina, CSO je angažovao IT stručnjaka da povrati podatke iz nedavnih rezervnih kopija. Shvatili su da su sigurnosne kopije pomogle da se obnovi većina podataka. OCD je zatim implementirao stroge politike: napisana je formalna politika prihvatljive upotrebe (zabranjena upotreba neodobrenih USB diskova i potrebna skeniranje bilo kojeg vanjskog medija), a cijelo osoblje je prošlo obuku o prepoznavanju sumnjivih uređaja i dodataka. Oni su također razvili jednostavan plan odgovora na incidente, dodjeljujući timu za reagovanje i jasne korake koje treba slijediti u budućem incidentu (uključujući koga prvo nazvati i kako komunicirati sa dionicima). Kasnije, tokom manjeg incidenta s phishingom, OCD ga je uspješno obuzdao koristeći novi plan, minimizirajući štetu.

Pitanja diskusije:

- *Koje su politike ili prakse nedostajale koje su dozvoljavale da se ovaj incident dogodi?*

- *Kako su nedavne sigurnosne kopije i tim za reagovanje uticali na ishod incidenta?*
- *Koje nove mjere I planove je OCD implementirao nakon tog događaja, I zašto su oni važni za sprječavanje budućih incidenata?*

Napomena o procjeni modula 7

Ovaj modul će biti procijenjen sa pet kratkih pitanja I jedan mali zadatak. Za prolaz je potreban minimalni rezultat od 70%.

Procjena modula 7

Kratka pitanja

1. Šta znači "sigurnosna kultura" a CSO kontekst, i zašto je učešće osoblja neophodno za njegovu izgradnju?
2. Zašto su osnovne politike IT sigurnosti (kao što su prihvatljiva upotreba ili BYOD politike) važne za OCD?
3. Kako redovna obuka osoblja i aktivnosti podizanja svijesti mogu smanjiti rizike kibernetičke sigurnosti u organizaciji?
4. Koji su ključni elementi jednostavnog plana odgovora na incident a CSO?
5. Zašto je važno pregledati i učiti iz incidenata kibernetičke sigurnosti nakon što se dogode?

Praktični zadatak: Akcioni plan za mini sigurnosnu kulturu

Od učesnika se traži da završe sljedeći zadatak:

- Identificirajte jednu konkretnu akciju koju bi njihov OCD mogao poduzeti kako bi ojačao svoju sigurnosnu kulturu (npr., uvođenje jednostavne politike prihvatljive upotrebe, organiziranje godišnje sigurnosne obuke ili definiranje kontakt osobe koja reaguje na incident).
- Ukratko opišite:
    - Ko bi bio odgovoran za ovu akciju,
    - Kako bi to bilo saopšteno osoblju,
    - Kako bi to pomoglo u sprečavanju ili smanjenju incidenata kibernetičke sigurnosti.

Učesnici bi svoje odgovore trebali predstaviti u tri do pet kratkih tačaka ili o njima nakratko razgovarati u malim grupama.

3.8 MODUL 8: NAPREDNE TEME – PRIJETNJE I ALATI U NASTAJANJU

Do kraja ovog modula, učesnik će moći:

- *Prepoznajte sofisticirane sajber prijetnje (kao što su ciljani phishing i lažiranje) i primijenite metode verifikacije (kao što je potvrđivanje zahtjeva putem alternativnih kanala).*
- *Na odgovarajući način koristite napredne sigurnosne alate (npr., hardverske sigurnosne ključeve za kritične račune, praćenje mreže za anomalije, resurse inteligencije prijetnji).*
- *Plan za organizaciona sigurnosna poboljšanja (kao što je postavljanje upravitelja lozinki preduzeća ili sistema za detekciju upada) zasnovan na kapacitetu i potrebama CSO's.*

Ciljevi učenja:

- Upoznajte se s novim ili sofisticiranim sajber prijetnjama (kao što su napredne tehnike phishinga ili lažni napadi) i naučite metode verifikacije kako biste im se suprotstavili.
- Istražite napredne sigurnosne alate i prakse koje mogu dodatno poboljšati zaštitu, uključujući sigurnost zasnovanu na hardveru (npr., sigurnosne ključeve), praćenje mreže i inteligenciju prijetnji, prilagođenu potrebama CSOs'.
- Razmislite o tome kako implementirati sigurnosna poboljšanja u cijeloj organizaciji kao što su upravitelji lozinki preduzeća ili sistemi za detekciju upada, razumijevanje kada su ove napredne mjere prikladne za kapacitet CSO's.

Ključne teme:

- **Sofisticirani phishing & lažiranje:** Razumijevanje napada socijalnog inženjeringa na visokom nivou (e-poruke o prijevari CEO-a, klonirane web stranice, itd.) i tehnika učenja za provjeru komunikacije (na primjer, provjera sumnjivih zahtjeva putem sekundarnog kanala ili korištenje digitalnih potpisa).
- **Hardverski sigurnosni ključevi:** Uvod u tokene fizičke autentifikacije (kao što su U2F/FIDO2 ključevi) kao alternativa SMS-u ili aplikaciji 2FA. Kako rade na sprječavanju

preuzimanja računa (2FA otporan na ribolov) i razmatranja za njihovo raspoređivanje osoblju.

- **Monitoring mreže i otkrivanje upada:** Osnovni koncepti kako je OCD mogao pratiti svoju mrežu zbog neobične aktivnosti. Objašnjavanje alata kao što su sistemi za detekciju upada (IDS) ili sistemi za prevenciju upada (IPS) jednostavnim terminima i kako upozoravaju amine na potencijalna kršenja.
- **Sigurnosni alati za cijelu organizaciju:** Implementacija naprednih alata kao što su upravitelji lozinki za cijelu organizaciju (kako bi se osiguralo da svo osoblje koristi jake, jedinstvene lozinke) ili korištenje upozorenja o obavještavanju o prijetnjama/zajedničkim upozorenjima kako bi se ažurirali o novim prijetnjama relevantnim za civilno društvo.
- **Prilagođavanje vašem kontekstu:** Naglašavajući da su ove napredne mjere opcione i da ih treba proširiti na tehničku ekspertizu i resurse CSO's. Smjernice o tome kako odlučiti koji napredni alati su vrijedni usvajanja i osigurati da osoblje bude obučeno da ih efikasno koristi.

Uzorci aktivnosti ili vježbe:

- **Scenario krađe govora:** Fasilitator predstavlja primjer visoko ciljanog pokušaja krađe identiteta (na primjer, e-mail koji izgleda kao da je iz poznatog finansijera koji traži prijenos). Učesnici praktikuju korak verifikacije (kao što je pozivanje službenog broja telefona pošiljaoca's ili provjera zaglavlja e-pošte) umjesto da odgovaraju putem e-pošte. Razgovarajte o tome kako ovaj pristup može osujetiti sofisticirane prevare.
- **Hardverski ključ Demo:** Učesnici mogu vidjeti ili isprobati hardverski sigurnosni ključ. Trener prolazi kroz registraciju ključa na račun, a zatim se prijavljuje koristeći ključ. Ako je moguće, dozvolite volonterima da pokušaju proces na demo nalogu kako bi demistificirali kako ovi uređaji rade i istakli njihove sigurnosne prednosti.
- **Mini lov na prijetnje:** Obezbedite pojednostavljeni mrežni dnevnik ili primer upozorenja iz hipotetičkog sistema za detekciju upada (IDS). Neka učesnici pregledaju unose kako bi uočili bilo šta sumnjivo (npr., nepoznatu IP adresu koja više puta pokušava prijavu u

neparnim satima). Ovo daje okus načina na koji alati za praćenje mreže mogu otkriti anomalije.

- **Diskusija o lokalnoj relevantnosti:** [Insert primjer napredne prijetnje ili alata za kibernetičku sigurnost koji je privukao pažnju u vašoj zemlji] – raspravljajte o tome da li je ova prijetnja ili alat nešto zbog čega bi se OCD trebao brinuti ili razmotriti korištenje. Kako lokalni resursi (poput nacionalnih savjeta CSIRT-a ili zajednica kibernetičke sigurnosti) mogu pomoći CSO-u da se uhvati u koštac s takvim naprednim prijetnjama?

Studija slučaja modula 8: Prijem prijevara izvršnog direktora

Kontekst: OCD je upravljao velikim projektom grantova sa više međunarodnih donatora. Osoblje ima iskustvo u osnovnoj sigurnosti, ali se nije bavilo visoko ciljanim napadima. Organizacija je nedavno predstavila hardverske sigurnosne ključeve za ključne menadžere i pregledala napredne sigurnosne alate.

Problem: Finansijski službenik CSO's primio je hitnu e-poštu navodno od izvršnog direktora, tražeći veliki prijenos žice novom dobavljaču za nabavku projekta. E-mail je izgledao legitimno bez očiglednih znakova za krađu identiteta. Policajac je trebao nastaviti kada su se sjetili da provjere zahtjev. Zvali su direktora u uredu. Direktor je, iznenađen, rekao da nije poslao nikakav e-mail. Odmah su shvatili da je to sofisticirani pokušaj lažiranja e-pošte (CEO prevara). Budući da su hardverski sigurnosni ključevi bili na snazi za račune direktora, napadač nije kompromitovao prijavu direktora; to je u potpunosti bila lažna e-pošta.

Ishod: Osoblje OCD-a blokiralo je sve daljnje mejlove sa adrese napadača i prijavilo pokušaj prevare. Kako bi spriječio buduće pokušaje, OCD je održao brifing o provjeravanju neobičnih zahtjeva (koristeći odvojene kanale) i ažurirao svoju kontrolnu listu odgovora na incidente kako bi uključio korake za sumnju na phishing. Također su odlučili da šire unose sigurnosne ključeve za račune visoke privilegije. Zahvaljujući ovim mjerama, OCD je izbjegao bilo kakav finansijski gubitak i povećao povjerenje osoblja da se napredni phishing napadi mogu otkriti i spriječiti.

Pitanja diskusije:

- *Kako je CSO otkrio i spriječio pokušaj prevare prije nego što su sredstva izgubljena?*

- *Koju su ulogu hardverski sigurnosni ključevi i postupak verifikacije odigrali u ovom scenariju?*
- *Koja su napredna sigurnosna poboljšanja (iz ovog modula) da li je OCD odlučio da ih sprovede kao rezultat ovog incidenta?*

Procjena modula 8

Ovaj modul će biti procijenjen sa pet kratkih pitanja i jednim malim zadatkom. Za prolaz je potreban minimalni rezultat od 70%.

Procjena modula 8

Kratka pitanja

1. Šta čini napredne phishing ili lažiranje napada opasnijim od osnovnih pokušaja krađe identiteta?
2. Šta je prevara generalnog direktora i zašto su OCD posebno ranjivi na ovu vrstu napada?
3. Kako se hardverski sigurnosni ključevi razlikuju od tradicionalnih metoda provjere autentičnosti dva faktora i zašto se smatraju otpornim na phishing?
4. Koja je svrha mrežnog praćenja ili sistema za detekciju upada u organizaciji?
5. Zašto bi OCD pažljivo procijenili svoje kapacitete i potrebe prije implementacije naprednih sigurnosnih alata?

Praktični zadatak: Napredna provjera pripravnosti za prijetnje

Od učesnika se traži da završe sljedeći zadatak:

- Identifikovati **jedna napredna pretnja** relevantno za njihov OCD (npr., prevara izvršnih direktora, ciljani phishing, lažiranje računa).
- Ukratko opišite:
    - Jedan korak osoblja za verifikaciju treba da preduzme pre nego što postupi po sumnjivim zahtevima,
    - Jedan napredni sigurnosni alat ili praksa koji bi mogao pomoći u smanjenju rizika (npr., hardverski sigurnosni ključevi, menadžeri lozinki, procedure verifikacije),
    - Da li je ova mjera trenutno izvodljiva za njihov OCD i zašto.

Učesnici bi svoje odgovore trebali predstaviti u tri do pet kratkih tačaka ili o njima nakratko razgovarati u malim grupama.

4. PRAVNI I REGULATORNI OKVIRI U ZEMLJI

4.1 Pravni i regulatorni okvir u Türkiyeu i prijedlozi za OCD u Türkiyeu

Obim Zakona o zaštiti ličnih podataka (KVKK) i njegov uticaj na OCD

Zakon br. 6698 o zaštiti ličnih podataka (KVKK) je primarni zakon koji reguliše obradu ličnih podataka u Türkiyeu. Zakon se primjenjuje na sva fizička i pravna lica koja obrađuju lične podatke, uključujući javne institucije, organizacije privatnog sektora i organizacije civilnog društva (CSO) (Uprava za ličnu zaštitu podataka [KVKK], 2020).

OCD obično prikupljaju i obrađuju lične podatke koji se odnose na njihove članove, volontere, donatore i zaposlene. Takvi podaci mogu uključivati imena, kontakt podatke, fotografije, iznose donacija i zapise o učešću u događajima. Stoga, OCD-ovi također imaju obaveze kao kontrolori podataka prema KVKK.

Prema Zakonu, lični podaci se mogu obrađivati samo u specifične, eksplicitne i legitimne svrhe, a moraju se brisati ili anonimizirati kada svrha obrade prestane. OCD moraju djelovati u skladu sa ovim principima u svim procesima prikupljanja podataka, od obrazaca za članstvo do digitalnih kampanja.

Koraci koje OCD moraju poduzeti da bi se uskladili sa KVKK

Glavni koraci koje bi OCD trebali slijediti kako bi se osiguralo usklađenost sa KVKK uključuju:

1. **Priprema inventara podataka:** OCD treba da identifikuju i dokumentuju koje lične podatke obrađuju, u koje svrhe, koliko dugo se podaci zadržavaju i sa kim se dele.
2. **Dobivanje eksplicitne saglasnosti:** Eksplicitni pristanak se mora dobiti za obrade aktivnosti koje nisu zakonski obavezne (npr. promotivne e-poruke). Pristanak se mora slobodno davati, informisati i ponovo raspolagati u bilo kom trenutku.
3. **Obaveza informacija:** Pojedinci čiji se lični podaci prikupljaju moraju se pismeno informisati o tome ko obrađuje njihove podatke, u koje svrhe, na kojima se nalaze pravni razlozi i koja su njihova prava.
4. **Mjere sigurnosti podataka:** Moraju se implementirati fizičke (zaključani ormarići), digitalne (šifriranje, antivirusni softver, ograničenja pristupa) i organizacijske (ugovori o povjerljivosti, obuka za podizanje svijesti) mjere.

5. **VERBIS Registracija:** OCD čije su aktivnosti ograničene isključivo na svoje članove, volontere i donatore izuzete su od registracije VERBIS-a. Međutim, od OCD-a sa ekonomskim preduzećem se traži da se registruju u sistemu (KVKK, 2020).

Kršenja i sankcije KVKK

KVKK predviđa administrativne kazne i, u nekim slučajevima, krivične sankcije u slučaju kršenja (KVKK, 2020). Ako OCD ne ispune svoje obaveze sigurnosti podataka, mogu se suočiti sa značajnim kaznama u slučajevima kršenja podataka, neovlaštenog dijeljenja podataka ili propusta da obavijeste prekršaje.

Od 2024. godine administrativne kazne se kreću od 25.000 TL (569 dolara) do 1.800.000 TL, u zavisnosti od prirode kršenja. Na primjer, nepojavljivanje kod VERBIS-a od strane OCD-a koji podliježe obavezi registracije predstavlja ozbiljan prekršaj.

Odbor KVKK uveo je sankcije I OCD. Udruženje je 2020. godine kažnjeno nakon žalbe u vezi sa neovlašćenom komunikacijom SMS-a, jer nije dalo izričit pristanak i nije izbrisalo lične podatke. Ovo pokazuje da su OCD podliježu revizijama i mjerama izvršenja prema zakonu.

Obaveze o zakonu i obaveštavanju o sajber bezbednosti

Zakon br. 7545 o sajber sigurnosti stupio je na snagu od 2025. godine i pokriva sve institucije koje pružaju usluge u digitalnom okruženju, bez razlike između javnih i privatnih subjekata (Službeni glasnik, 2024.). U okviru ovog okvira, OCD takođe podležu obavezama obaveštenja o incidentima.

U slučaju povrede podataka, infekcije zlonamjernim softverom, sajber napada ili identifikacije kritične ranjivosti unutar sistema CSO’s, incident se mora prijaviti Direkciji za kibernetičku sigurnost povezanoj s turskim predsjedništvom u roku od najviše 48 sati.

Nepoštivanje može rezultirati administrativnim kaznama počevši od 1.000.000 TL i, u određenim slučajevima, krivičnim sankcijama kao što je zatvor za odgovorna lica. Ovom uredbom utvrđuje se temeljna obaveza sigurnosti I transparentnosti za sve OCD.

Nacionalna strategija kibernetičke sigurnosti i uloga OCD

Nacionalna strategija kibernetičke sigurnosti i akcioni plan 2024–2028 je glavni dokument koji definira viziju digitalne sigurnosti Türkiye. Dokument dodjeljuje posebne uloge javnim institucijama, privatnom sektoru i OCD (Ministarstvo saobraćaja i infrastrukture, 2023).

Ključna očekivanja od OCD-a uključuju podizanje svijesti javnosti, promoviranje individualne digitalne sigurnosne pismenosti i provođenje aktivnosti digitalne pismenosti za ugrožene grupe kao što su djeca i starije osobe.

Nadalje, strategija naglašava važnost učešća civilnog društva i podstiče OCD da sprovode kampanje i aktivnosti obuke u saradnji sa javnim institucijama.

Pravni status digitalnih alata

Kao dio digitalne transformacije, od OCD-a se može tražiti da koriste određene digitalne alate. Prema Zakonu br. 5070 o elektronskim potpisima, elektronski potpisi imaju istu zakonsku valjanost kao i rukom pisani potpisi. Odluke odbora, ugovori i zvanična prepiska stoga mogu biti potpisani elektronskim putem (Uprava za informacione i komunikacione tehnologije, 2023).

OCD sa ekonomskim preduzećem ili prekoračenjem određenih pragova prometa mogu biti podložni obavezama e-glasova (e-Fatura) i e-arhiva (e-Aršajeva). Uprava za prihode objavljuje godišnje saopštenja u kojima se navode primjenjivi pragovi (Uprava prihoda, 2024.).

Registrovana elektronska pošta (KEP) je još jedan preferirani metod za zvanična obaveštenja, posebno da bi se osigurala pravna valjanost. Koristeći sve ove alate, OCD moraju osigurati ne samo tehničku adekvatnost već i punu usklađenost sa relevantnim pravnim okvirom.

Digitalna sigurnost za male i srednje veličine OCD-a u Türkiyeu

Uvod

Sljedećih pet originalnih slučajeva pripremljeno je za potrebe obuke i zasnovano je na realističnim digitalnim sigurnosnim rizicima i iskustvima malih i srednjih organizacija civilnog društva (CSO) koje djeluju u Türkiyeu. Svaki slučaj jasno predstavlja strukturu OCD-a, doživljenog incidenta, tehničku ili ljudsku ranjivost, posljedice i lekcije koje se mogu izvući za druge OCD. Svi OCD su anonimno predstavljeni u ovoj studiji.

LOKALNE STUDIJE SLUČAJA OD TÜRKRIYEA

Slučaj 1: Glavobolja izazvana lažnom trakom za e-poštu

Ovaj OCD je malo obrazovno udruženje koje posluje sa samo četiri zaposlena i nekoliko volontera, sa ciljem da pruži stipendije i obrazovnu podršku lokalnim studentima. Njegove digitalne operacije se uglavnom oslanjaju na komunikaciju putem e-pošte, kancelarijski softver i koordinaciju zasnovanu na WhatsApp-u sa volonterima. The organizacija nema posebnog člana IT osoblja, a zaposleni uglavnom koriste svoje lične laptope za posao.

"One day, e-mail sa temom "Ministry Education Grant" stiže u udruženje's general info@... inbox. U poruci se tvrdi da je organizaciji dodijeljen grant za koji se prijavila i traži da se pridruženi PDF fajl otvori za više detalja. Uzbuđen vijestima, projektni službenik preuzima i otvara prilog bez provjere njegove autentičnosti. Datoteka se ne otvara kako treba, ali zlonamjerni softver se tiho instalira na računaru."

Glavna ranjivost u ovom slučaju je ljudska greška i nedostatak svijesti. Član osoblja nije prošao obuku o sajber sigurnosti i nije pažljivo ispitao adresu pošiljaoca, jezične greške i sumnjivu privrženost. To su bili jasni pokazatelji phishing e-pošte osmišljene da se lažno predstavlja kao zvanična institucija.

U roku od jednog dana, zajednički nalozi e-pošte koje su koristili projektni službenik i odbor su kompromitovani. Napadači su slali lažne poruke tražeći novac donatorima i partnerima. Komunikacija je prekinuta, povjerenje je poljuljano, a neke pristalice su privremeno obustavile angažman. U srednjem roku, the organizacija je morala uložiti vrijeme i trud da povrati kredibilitet i unutrašnji moral.

Naučene lekcije i preporuke

Phishing napadi su jedna od najčešćih sajber prijetnji za OCD. Svo osoblje i volonteri treba biti obučeni za identifikaciju sumnjivih mejlova. Adrese pošiljaoca, priloge i hitne zahtjeve uvijek treba provjeriti. Treba implementirati osnovne prakse kiberhigijene i dvofaktorsku autentifikaciju za kritične račune.

Slučaj 1: Glavobolja izazvana lažnom trakom za e-poštu

Relevantni modul(i)

- Modul 4: Uobičajene sajber prijetnje (Fishing & Malware)
- Modul 5: Zaštita podataka i usklađenost privatnosti
- Modul 7: Razvoj sigurnosne kulture

Kako se ovaj slučaj može koristiti u obuci

- **Primjer podizanja svijesti (Modul 4):**
  Ovaj slučaj se može uvesti na početku modula kao a **realističan scenarij phishinga** ciljanje malih OCD. Treneri mogu zamoliti učesnike da identifikuju crvene zastavice u e-poruci (pošiljajte adresu, privrženost, hitnost, jezičke greške) prije nego što otkriju ishod.
- **Diskusija o ljudskim greškama (Modul 7):**
  Koristite ovaj slučaj da naglasite da sajber sigurnost nije samo tehnički problem već i a **pitanje ljudskog ponašanja**. Dobro funkcionira kao početak diskusije o tome zašto je obuka osoblja i volontera kritična, posebno u malim organizacijama civilnog društva bez IT osoblja.
- **Refleksija sigurnosti računa (Modul 5):**
  Slučaj može podržati diskusiju o **zaštita od naloga e-pošte**, uključujući dvofaktorsku autentifikaciju i upravljanje pristupom, povezujući phishing napade sa širim rizicima zaštite podataka.

Predložena metoda:

Grupna diskusija + “Šta biste radili drugačije?” vježba.

Slučaj 2: Preuzimanje računa na društvenim mrežama

Ovaj slučaj uključuje CSO za prava žena srednjih veličina sa otprilike 20 članova osoblja i volontera. Organizacija aktivno koristi platforme društvenih medija kao što su Instagram, X (bivši Twitter) i Facebook za zagovaranje i javni angažman. Računima uglavnom upravlja službenik za komunikacije, iako volonteri povremeno doprinose. Nije omogućena dvofaktorska autentifikacija.

Jednog jutra, neobične objave se pojavljuju na službenom Instagram nalogu organizacije’s. Slika profila i biografija su promijenjeni, a lažni sadržaj vezan za ulaganja dijeli se sa pratiocima. Članovi i sljedbenici upozoravaju organizaciju da je račun hakovan.

Službenik za komunikacije ponovo je koristio istu lozinku na više platformi. Kršenje podataka na drugoj usluzi razotkrilo je lozinku, omogućavajući napadačima pristup nalogu na društvenim mrežama. Odsustvo dvofaktorske autentifikacije dodatno je olakšalo preuzimanje. Osim toga, organizaciji je nedostajao unaprijed definiran plan odgovora na krizu.

Račun je privremeno obustavljen dok su pokrenute procedure oporavka. Sljedbenici su upozoreni putem alternativnih kanala. Iako je pristup na kraju obnovljen, došlo je do štete po reputaciju, a neki sljedbenici su izgubili povjerenje. Kao odgovor, organizacija je ojačala politiku lozinki i aktivirala dvofaktorsku autentifikaciju.

Naučene lekcije i preporuke

Nalozi na društvenim mrežama česte su mete sajber napada. Snažne, jedinstvene lozinke i dvofaktorska autentifikacija su od suštinskog značaja. Treba izbjegavati ponovnu upotrebu lozinki, a osoblje koje upravlja društvenim medijima trebalo bi proći ciljanu obuku o svijesti o sigurnosti.

Slučaj 2: Preuzimanje računa na društvenim mrežama

Relevantni modul(i)

- **Modul 6: Socijalni mediji i sigurnost prisutnosti na mreži**
- **Modul 7: Razvoj sigurnosne kulture**

Kako se ovaj slučaj može koristiti u obuci

- **Osnovna studija slučaja (Modul 6):**
  Ovaj slučaj je idealan kao **primarna studija slučaja** kada se predaje sigurnost društvenih medija. Treneri mogu prošetati učesnike kroz incident korak po korak i mapirati propuste u nedostajućim kontrolama (ponovna upotreba lozinke, ne 2FA, bez plana odgovora).
- **Vježba odgovora na incidente (Modul 7):**
  Slučaj se može transformisati u scenario igranja uloga u kojem učesnici odlučuju kako da komuniciraju sa pratiocima, prijave kršenje platformi i povrate račun.
- **Ciljana diskusija o obuci:**
  Ističite da je osoblju odgovornom za komunikaciju i zagovaranje potrebna specijalizirana sigurnosna svijest, a ne samo opća obuka.

Predložena metoda:
Analiza slučaja + igra uloga odgovora na incidente.

Slučaj 3: Trošak gubitka podataka i nedostatak rezervnih kopija

Prakse tipa, skale i digitalnog rada OCD

Ovaj slučaj se odnosi na mali ekološki OCD sa tri stalno zaposlena člana osoblja i nekoliko volontera. Projektni dokumenti se pripremaju na ličnim laptopima i dijele se putem usluga u oblaku. Međutim, kritični podaci kao što su liste donatora i finansijska evidencija pohranjeni su samo na Director’s desktop računaru, bez redovnih rezervnih kopija.

Nakon nestanka struje, računar Director’s ne uspijeva ponovo pokrenuti zbog oštećenja na tvrdom disku. Pokušaji lokalnog povrata podataka su neuspješni, a profesionalne usluge oporavka podataka preporučuju se po visokoj cijeni bez zagarantovanog uspjeha.

Nije bilo sajber napada; incident je rezultat lošeg upravljanja podacima i odsustva rezervne strategije. Pohranjivanje kritičnih podataka na jednom uređaju i korištenje zastarjelog hardvera značajno je povećalo rizik od gubitka podataka.

OCSOing projekti su prekinuti, a izgubljeni su važni izvještaji, finansijski dokumenti i kontakt liste. Osoblje je provelo sedmice pokušavajući rekonstruirati podatke koji nedostaju. Povjerenje donatora i partnera je pogođeno, a finansijski gubici su nastali zbog napora za oporavak i poremećenih projekata.

Naučene lekcije i preporuke

Redovne sigurnosne kopije podataka su neophodne za organizacioni kontinuitet. Rezervne kopije treba pohraniti na više platformi i periodično testirati. Hardver treba ažurirati, a treba koristiti sisteme zaštite snage.

Slučaj 3: Trošak gubitka podataka i nedostatak rezervnih kopija

Relevantni modul(i)

- **Modul 5: Zaštita podataka i usklađenost privatnosti**
- **Modul 7: Razvoj sigurnosne kulture**

Kako se ovaj slučaj može koristiti u obuci

- **Primjer upravljanja podacima (Modul 5):**
  Ovaj slučaj je efikasan za objašnjenje da ne uključuju svi sigurnosni incidenti hakere. Treneri ga mogu koristiti za uvođenje strategija sigurnosne kopije, dostupnosti podataka i organizacioni kontinuitet.
- **Vježba procjene rizika:**
  Od učesnika se može tražiti da navedu kritične podatke u svojim OCD i identifikuju da li postoje slične pojedinačne tačke kvara.
- **Diskusija o odgovornosti za liderstvo (Modul 7):**
  Slučaj pokazuje zašto su zaštita podataka i sigurnosne kopije upravljanje-odgovornosti nivoa, ne samo tehnički zadaci.

Predložena metoda:
Vođeni odraz + aktivnosti revizije mini podataka.

Slučaj 4: Opasnost od slabih lozinki i zajedničkih računa

Ovaj scenario uključuje fondaciju srednje veličine koja podržava osobe sa invaliditetom. Oko 15 članova osoblja i volontera koristi zajedničke račune e-pošte i sistema za svakodnevne operacije, oslanjajući se na jedno korisničko ime i lozinku na više platformi.

Donator's prijavite se da primate sumnjive poruke u kojima se traži novac. Istraga otkriva da je bivši volonter još uvijek imao pristup zajedničkim računima jer lozinke nikada nisu promijenjene nakon njihovog odlaska. Ove akreditive su kasnije neovlaštene osobe zloupotrebile.

Slabe i zajedničke lozinke, ponovna upotreba lozinki i odsustvo procedura opoziva pristupa stvorili su ozbiljan sigurnosni jaz. The organizaciji su nedostajale jasne politike za upravljanje digitalnim pristupom kada osoblje ili volonteri odu.

Lozinke su odmah promijenjene, a donatori su obaviješteni. Iako je neposredna šteta bila ograničena, došlo je do štete po reputaciju. U srednjem roku, organizacija je uvela jače politike lozinki, pojedinačne korisničke naloge i sesije podizanja svijesti osoblja.

Svaki račun bi trebao imati snažnu, jedinstvenu lozinku. Zajedničke račune treba izbjegavati gdje je to moguće, a prava pristupa moraju se preispitati i odmah opozvati kada osoblje ode. Jasne interne politike su neophodne.

Slučaj 4: Opasnost od slabih lozinki i zajedničkih računa

Relevantni modul(i)

- **Modul 6: Socijalni mediji i sigurnost prisutnosti na mreži**
- **Modul 7: Razvoj sigurnosne kulture**
- **Modul 8: Napredne teme (Pristup i kontrole računa)**

Kako se ovaj slučaj može koristiti u obuci

- **Ilustracija jaza u politici (Modul 7):**
  Ovaj slučaj jasno pokazuje rizike od nestanka **politike upravljanja pristupom**, posebno procedure van ukrcaja, kada osoblje ili volonteri odu.
- **Računovodstvena sigurnosna diskusija (Modul 6):**
  Treneri mogu povezati ovaj slučaj sa značajem pojedinačnih računa, jakih lozinki i pristupa zasnovanog na ulogama <TAG1> posebno za komunikaciju putem e-pošte i donatora.

- **Uvod u kontrolu naprednog pristupa (Modul 8):**
  Slučaj može poslužiti kao most za naprednije prakse kao što su revizije računa, menadžeri lozinki i upravljanje privilegijama.

Predložena metoda:
Vježba izrade politike zasnovana na slučajevima (npr., "Šta bi kontrolna lista van ukrcaja trebala uključivati?").

Trainer's Note (Sporno dodati na kraju sekcije)

Ove lokalne studije slučaja su dizajnirane da:

- Odrazite realne rizike s kojima se suočavaju OCD u Türkiyeu
- Podsticati vršnjačko učenje i diskusiju,
- Demonstrirajte da incidenti s sajber sigurnošću često proizlaze iz jednostavnih problema koji se mogu spriječiti
- Pojačajte važnost politika, obuke i pripravnosti, a ne samo tehnologije.

Treneri se ohrabruju da prilagode dubinu diskusije u zavisnosti od organizacione veličine učesnika', digitalne zrelosti i uloga.

Praktične politike digitalne sigurnosti i predlošci za OCD

Uvod

Ovaj dokument predstavlja praktične predloške politike koji se mogu koristiti za jačanje kapaciteta digitalne sigurnosti malih i srednjih organizacija civilnog društva (CSO) u Türkiyeu. Predlošci su dizajnirani da budu jednostavni, djelotvorni i usklađeni sa nacionalnim zakonodavstvom (Zakon o zaštiti ličnih podataka – KVKK, Zakon o kibernetičkoj sigurnosti) i međunarodnim dobrim praksama (NIST, ENISA, Tactical Tech).

1. Politika prihvatljive upotrebe (AUP)

Svrha:

Promovirati odgovornu upotrebu organizacioni digitalni alati, pristup internetu i informacioni sistemi.

Odredbe politike:

- Svo osoblje će koristiti digitalne resurse organizacije isključivo u svrhu rada.
- Lozinke moraju biti pojedinačne i ne smiju se dijeliti s drugima.
- Ilegalni sadržaj se ne može pohraniti, pristupiti ili distribuirati kroz organizacione sisteme.
- Upotreba društvenih medija ne smije naštetiti reputaciji organizacije's.
- Nijedan podatak ne može biti prebačen izvan organizacije bez prethodnog odobrenja menadžmenta.

Napomena:

Ova politika stupa na snagu nakon što je potpisano od strane osoblja tokom ukrcavanja i mora se revidirati svake godine. (ENISA, 2021)

2. Plan odgovora na incidente (IRP)

Svrha:

Da bi se osigurao brz i efikasan odgovor na potencijalne incidente digitalne sigurnosti.

Koraci:

1. Osoba koja otkrije incident odmah obavještava određena ovlaštenja unutar organizacije.
2. Vlast određuje vrstu incidenta (phishing, malware, kršenje podataka).
3. Pogođeni sistemi su izolovani (uklonjeni iz mreže ako je potrebno).
4. Sačuvani su svi digitalni dnevnici i zapisi vezani za incident.
5. Incident je prijavljen Direkciji za kibernetičku sigurnost u roku od najviše 48 sati (Službeni glasnik, 2024.).

6. Provodi se evaluacija nakon incidenta, a procedure se ažuriraju u skladu s tim.

Napomena:

Ovaj plan je zasnovan na Zakonu br. 7545 o sajber sigurnosti i NIST SP 800-61 Rev. 2.

3. Osnovni postupak zaštite podataka

Svrha:

Da bi se osiguralo da se lični podaci obrađuju unutar OCD njime se upravlja u skladu sa KVKK.

Implementacija:

- Svaka aktivnost obrade podataka mora imati jasnu svrhu i biti u skladu sa principom minimizacije podataka.
- Lični podaci se ne mogu obrađivati bez izričitog pristanka, osim ako nije drugačije dozvoljeno zakonom (KVKK, 2020).
- Za svaku aktivnost dijeljenja podataka mora se dokumentirati razlog dijeljenja, primalac i trajanje.
- Mora se uspostaviti politika zadržavanja podataka i uništavanja; lični podaci se moraju izbrisati ili anonimizirati kada više nisu potrebni.
- Zapisi zasnovani na papiru moraju se pohraniti u zaključane ormariće, a digitalni podaci moraju biti zaštićeni šifriranim fasciklama.

Napomena:

Preporučuje se da organizacija imenuje internog kontrolora podataka ili odgovornu osobu.

4. Protokol o podjeli kredita i uređaja

Svrha:

Regulisati sigurnu upotrebu i dijeljenje lozinki, korisničkih naloga i digitalnih uređaja unutar organizacija.

Pravila:

- Lozinke se moraju pojedinačno dodijeliti i ne smiju se zapisivati.

- Na zajedničkim uređajima, svaki korisnik se mora prijaviti na poseban račun i ne smije dijeliti lozinke.
- Prenos podataka na eksterne uređaje (npr, osobni laptopi) su zabranjeni.
- Upotreba USB diskova ili eksternih uređaja za pohranu je dozvoljena samo uz odobrenje upravljanja.

Napomena:

Organizacije mogu dodatno definirati politiku autentifikacije (npr. višefaktorsku autentifikaciju).

5. Obaveza digitalne sigurnosti (Staff / Volunteers)

Tekst posvećenosti (uzorak):

“Po ovom dokumentu, preduzimam da koristim digitalne sisteme i alate koje pruža [Naziv organizacije] isključivo u okviru mojih dužnosti i sa dužnom pažnjom. Priznajem svoju odgovornost da ispunim sve obaveze vezane za sigurnost organizacionih podataka.”

"Bu belgeyle, [Kurum Adı] tarafından tahsis edilen dijital sistem ve araçları yalnızca görev kapsamımda ve dikkatli biçimde kullanacağımı taahhüt ederim. Kurum içi verilerin güvenliği için üzerime düşen yükümlükleri yerine geriveceğimi kabul ederim."

Napomena:

Ovu obavezu treba potpisati svi članovi osoblja i volonteri i zadržati u svojim kadrovskim dosijeima.

Kontrolne liste digitalne sigurnosti za OCD

Kako bi se ojačala digitalna sigurnost malih i srednjih organizacija civilnog društva (CSO) koje djeluju u Türkiyeu, u nastavku su predviđene četiri odvojene kontrolne liste. Ove liste se sastoje od jednostavnih i praktičnih stavki koje korisnici sa ograničenim tehničkim znanjem mogu lako primijeniti. Svaka kontrolna lista sažima osnovne sigurnosne korake u skladu sa važećim zakonskim propisima. Cilj je povećati sigurnosnu svijest u svakodnevnim digitalnim operacijama i osigurati spremnost za potencijalne hitne slučajeve.

1. Osnovna kontrolna lista digitalne sigurnosti

☐ Da li svi korisnici koriste jake I jedinstvene lozinke?

☐ Da li su automatske zaključavanje ekrana omogućene na računarima I mobilnim telefonima?

☐ Da li je ažurirani antivirusni softver instaliran na svim uređajima?

☐ Da li se sav softver I aplikacije redovno ažuriraju?

☐ Da li su važni dokumenti redovno podržani (spoljni pogon ili skladištenje u oblaku)?

☐ Da li su svi korisnici oprezni prilikom otvaranja priloga e-pošte?

☐ Da li se prati upotreba vanjskih ili ličnih uređaja?

2. Kontrolna lista spremnosti za odgovor na incidente

☐ Da li je osoba odgovorna za digitalnu sigurnost određena?

☐ Je li jasno definisano kome I kako treba prijaviti incidente?

☐ Da li svo osoblje ima osnovna znanja o identifikaciji incidenata (phishing, malware, itd.)?

☐ Jesu li kritični dokumenti I sistemi potkrijepljeni?

☐ Postoji li pisana procedura nakon incidenta?

☐ Da li je osoblje svjesno pravila obavještenja od 48 sati? (Zakon br. 7545)

3. Kontrolna lista sigurnosti društvenih medija

☐ Da li samo ovlašćene osobe imaju pristup nalozima na društvenim mrežama?

☐ Da li je dvofaktorska autentifikacija (2FA) omogućena na svim računima?

☐ Jesu li lozinke jake i ne koriste se ponovo na drugim platformama?

☐ Je li jasno ko upravlja računima i u koju svrhu?

☐ Da li sadržaj podliježe prethodnom odobrenju prije dijeljenja?

☐ Da li se nadziru sumnjivi prijave ili neuobičajena povećanja brojača?

4. Novi štab /Kontrolna lista za sigurnost informacija volontera

☐ Da li novi članovi osoblja ili volonteri dobijaju digitalnu sigurnosnu orijentaciju?

☐ Da li je potpisana Politika prihvatljive upotrebe?

☐ Da li su preuzete obaveze u vezi sa obradom ličnih podataka?

☐ Da li su prava pristupa ograničena isključivo na obaveze posla?

☐ Da li se organizacioni računi koriste umesto ličnih računa?

☐ Da li je usklađenost sa organizacionim lozinkama i politikama uređaja osigurana?

4.2 Pravni I regulatorni okvir u Bosni I Hercegovini I prijedlozi za OCD u BiH

Pravni I regulatorni kontekst u Bosni I Hercegovini (BiH)

Zaštitom ličnih podataka u Bosni i Hercegovini upravlja **Zakon o zaštiti ličnih podataka (Zakon o zaštttiti lichnih podataka)**. nadležni nadzorni organ je **Agencija za zaštitu ličnih podataka Bosne I Hercegovine (AZLP)**. Iako Opća uredba EU o zaštiti podataka (GDPR) nije direktno primjenjiva u BiH, mnogi programi koje finansira EU I međunarodni donatori zahtijevaju standarde usklađene s GDPR-om. Kao rezultat toga, organizacione prakse I smjernice u BiH sve više odražavaju osnovne principe GDPR-a, poput zakonitosti, minimizacije podataka, odgovornosti I sigurnosti obrade.

Bosna I Hercegovina još uvijek nema jedinstveni, sveobuhvatni nacionalni zakon o kibernetičkoj sigurnosti. U tom kontekstu, od organizacija civilnog društva (OCD) se prvenstveno očekuje da osiguraju digitalnu sigurnost kroz mehanizme unutrašnjeg upravljanja, uključujući jasno definisane uloge i odgovornosti, politike interne informacione bezbednosti i dokumentovane procedure koje se dosljedno primenjuju u svakodnevnim operacijama.

Nacionalne institucije i mehanizmi podrške za kibernetičke incidente

Nekoliko javnih institucija pruža podršku, koordinaciju ili istražne funkcije u slučaju incidenata kibernetičke sigurnosti u Bosni i Hercegovini. To uključuje **CERT BiH**, koji je odgovoran za podršku odgovoru na incidente, rana upozorenja i praćenje prijetnji, kao i za **Ministarstvo sigurnosti BiH – Sektor kibernetičke sigurnosti**, koji pruža koordinaciju i smjernice na nivou politike. Izvještavanje i istragu o sajber kriminalu rješava **Državna agencija za istrage i zaštitu (SIPA)** kroz specijalizirane jedinice, uz jedinice za kibernetički kriminal entiteta I kantonalne policije odgovorne za operativne istrage na lokalnom nivou.

Pejzaž kibernetske prijetnje za OCD u BiH

Organizacije civilnog društva u BiH najčešće se suočavaju s kibernetskim prijetnjama vezanim za phishing napade usmjerene na organizacijske finansije, grantove I donatorsku komunikaciju. Incidenti sa ransomware-om i trajni gubitak podataka su također česti, često zbog nedostajućih ili neadekvatnih praksi sigurnosne kopije. Impersonacijski i napadi socijalnog

inženjeringa se sve više primjećuju putem platforme za razmjenu poruka kao što su WhatsApp i Viber, dok deplasman web stranice predstavlja poseban rizik za organizacije koje rade na politički ili društveno osjetljivim pitanjima. Osim toga, krađa akreditiva povezana s korištenjem neosiguranih javnih Wi-Fi mreža ostaje problem koji se ponavlja.

Operativna realnost organizacija civilnog društva u BiH I Rationale za pojednostavljeni pristup

U praksi, mnogi OCD u Bosni I Hercegovini se u velikoj mjeri oslanjaju na lične laptope I mobilne telefone za organizacioni rad I koriste platforme kao što su Gmail, Google Workspace I društvene mreže kao svoje primarne operativne alate. Namjenski IT ili cybersecurity osoblje su rijetke, a neformalne prakse kao što je dijeljenje lozinki unutar timova su još uvijek uobičajene.

S obzirom na ovu stvarnost, nastavni plan i program usvaja namjerno pojednostavljen i pragmatičan pristup. Prioritet daje jeftine i lako primjenjive sigurnosne mjere, pruža praktične šablone i dokumente spremne za korištenje, a fokusira se na jasne kontrolne liste korak po korak dizajnirane za netehničko osoblje, a ne na složena tehnička rješenja.

Usklađenost sa okvirima evropske politike

Iako Bosna I Hercegovina nije članica Evropske unije, mnoge organizacije civilnog društva rade u okviru programa koje finansira EU I okvira evropskih politika. Ovaj nastavni plan i program je stoga usklađen sa osnovnim GDPR principima, posebno pristupom zasnovanim na riziku, kao i sa širom evropskom svešću o sajber bezbednosti i strategijama izgradnje kapaciteta. Usklađivanje je praktično, a ne legalističko, fokusirajući se na svakodnevnu implementaciju i organizacijsko ponašanje umjesto na formalne zahtjeve usklađenosti.

Pristup zasnovan na riziku i logika politike

Okviri evropske politike naglašavaju proporcionalnost, kontekstualnu svijest i procjenu uticaja. Nastavni plan i program primjenjuje ovu logiku dajući prioritet visokorizičnim sredstvima i aktivnostima, izbjegavajući pretjerano složene kontrole ili kontrole koje intenzivno

koriste resurse, te fokusirajući se na ljudske i realistične sigurnosne prakse koje se mogu održati u okruženjima OCD-a.

ISO-inspirisana logika (pojednostavljena)

Čak i bez formalne certifikacije, OCD mogu imati koristi od pojednostavljenih principa inspirisanih standardima ISO sigurnosti informacija. To uključuje identifikaciju ključnih organizacionih sredstava, primjenu osnovnih principa kontrole pristupa, uspostavljanje strukturiranih procesa upravljanja incidentima i promoviranje kontinuiranog poboljšanja kroz pregled i učenje. Ovaj pristup podržava postepeno jačanje organizacione zrelosti i otpornosti tokom vremena.

Lokalne studije slučaja iz Bosne I Hercegovine

Slučaj 1: Fishing Link koji vodi do preuzimanja punog računa

Ovaj slučaj uključuje omladinsku organizaciju civilnog društva sa sjedištem u Sarajevu. Organizacija djeluje s malim timom i u velikoj mjeri se oslanja na zajedničke inboxove e-pošte i platforme društvenih medija kao što su Facebook i Instagram za komunikaciju, koordinaciju i javni pristup. Lozinke se dijele interno i nije omogućena dvofaktorska autentifikacija. Član osoblja primio je poruku Facebook Messengera koja je, čini se, došla od pouzdanog partnera u projektu. U poruci je tražena potvrda detalja za zajedničku aktivnost i uključena je veza. Član osoblja kliknuo je na link i ušao u akreditive organizacije za e-poštu's. U roku od nekoliko minuta, napadač je dobio pristup zajedničkom sandučetu e-pošte i povezanim nalozima na društvenim mrežama. Podaci o kontaktu za oporavak su promijenjeni, a donatorima su poslani lažni zahtjevi za plaćanje.

Incident je omogućen višestrukim slabostima, uključujući zajedničke lozinke, ponovnu upotrebu lozinki na platformama, nedostatak dvofaktorske autentifikacije i pretjerane administrativne privilegije za sve korisnike. Poruka je bila pouzdana bez nezavisne provjere. Kratkoročno, organizacija je izgubila pristup svojim nalozima e-pošte i društvenih medija, ometajući komunikaciju i aktivnosti prikupljanja sredstava. Prevarne poruke oštetile su povjerenje

donatora. U srednjem roku, OCD je morao uložiti značajno vrijeme u oporavak računa i obnovu kredibiliteta.

Naučene lekcije i preporuke

Svi organizacioni nalozi treba da koriste jedinstvene lozinke kojima se upravlja preko upravitelja lozinki i da imaju omogućenu dvofaktorsku autentifikaciju. Administrativne privilegije moraju biti ograničene, a osjetljive zahtjeve uvijek treba provjeriti putem sekundarnog komunikacijskog kanala.

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 1 – Osnove kibernetičke sigurnosti:**
  Koristi se kao ključni primjer za ilustraciju phishing napada, krađe akreditiva i brzog preuzimanja računa.
- **Modul 4 – Uobičajene sajber prijetnje (Fishing & Malware):**
  Demonstrira kako društveni inženjering iskorištava povjerenje i nedostatak verifikacije.
- **Modul 7 – Razvoj sigurnosne kulture:**
  Podržava diskusiju o svijesti osoblja, higijeni lozinki i važnosti dvofaktorske autentifikacije.

Predložena upotreba:
Analiza slučaja praćena identifikacijom crvenih zastavica i preventivnim kontrolama mapiranja.

Slučaj 2: WhatsApp/Imperation Viber koji vodi do finansijskog gubitka

Ovaj slučaj se odnosi na CSO srednje veličine koji često koristi WhatsApp i Viber za internu koordinaciju i finansijsku komunikaciju. Osjetljive odluke se često rješavaju neformalno putem aplikacija za razmjenu poruka.

Napadač je kreirao WhatsApp ili Viber nalog koristeći ime i profilnu fotografiju pravog koordinatora projekta. Napadač je kontaktirao finansijsko osoblje sa hitnom porukom u kojoj se

navodi da su se podaci banke promijenili i zatražio je hitno korištenje novog IBAN-a. Zahtjev je obrađen bez provjere.

The organizacija se oslanjala na platforme za neformalne poruke za osjetljive finansijske odluke i nije imala mehanizme sekundarne verifikacije. Nije bilo zahtjeva za višečlano odobrenje za finansijske transakcije.

Sredstva su prebačena napadaču i nisu se mogla povratiti. Incident je rezultirao finansijskim gubitkom i unutrašnjim problemima, kao i zabrinutošću za reputaciju donatora i partnera.

Finansijske razmjene nikada ne bi trebale biti odobrene putem platformi za razmjenu poruka. Svi zahtjevi vezani za plaćanje moraju se provjeriti putem službenih kanala, kao što su potpisani mejlovi iz organizacijske domene ili telefonski pozivi na poznate brojeve. Za značajne finansijske transakcije trebalo bi implementirati pravilo o odobrenju za dvije osobe.

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 2 – Communication and Social Engineering:**
  Primarni slučaj koji ilustruje imitiranje i manipulaciju zasnovanu na hitnosti putem platformi za razmjenu poruka.
- **Modul 7 – Razvoj sigurnosne kulture:**
  Ističe potrebu za internim pravilima, procedurama verifikacije i zajedničkom odgovornošću za finansijske odluke.

Predložena upotreba:
Vježba igranja uloga na verifikaciji hitnih finansijskih zahtjeva i primjeni pravila odobrenja za dvije osobe.

Slučaj 3: Credential Theft putem javnog Wi-Fi-ja

Ovaj slučaj uključuje OCD koji omogućava volonterima da rade na daljinu koristeći lične uređaje. Cloud usluge kao što su Gmail i Google Drive su centralne za svakodnevne operacije i ne postoji formalna politika koja reguliše daljinski pristup ili sigurnost uređaja.

Volonter je radio od cafe koristeći besplatni javni Wi-Fi i prijavljen u organizaciju's e-mail i cloud storage. Uređaju su nedostajala nedavna sigurnosna ažuriranja, a lozinke su sačuvane u pretraživaču. Ubrzo nakon toga, otkriveni su nepoznati prijave, a preuzete su i liste kontakata donatora. Odgovor je odgođen zbog nejasnih procedura prijavljivanja.

Organizacija je omogućila pristup osjetljivim nalozima preko neosiguranog javnog Wi-Fi-ja, koristila zastarjele uređaje i dozvoljavala lozinke sačuvane u pretraživaču. Takođe nije postojao jasan interni mehanizam za izveštavanje o incidentima.

Otkriveni su osjetljivi podaci, a povjerenje donatora je dovedeno u opasnost. Odgođeni odgovor povećao je potencijalni uticaj kršenja.

Osjetljivim nalozima ne treba pristupiti putem javnog Wi-Fi-ja bez VPN-a. Uređaji moraju biti ažurirani, funkcije automatskog povezivanja onemogućene, a procedure prijavljivanja incidenata jasno su saopštene svim osobljem i volonterima.

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 3 – uređaji i sigurnost infrastrukture:**
  Osnovni primjer za rizike vezane za javni Wi-Fi, netaktovane uređaje i nesigurno skladištenje akreditiva.
- **Modul 7 – Razvoj sigurnosne kulture:**
  Pojačava važnost jasnih procedura prijavljivanja incidenata i svijesti osoblja.

Predložena upotreba:
Grupna diskusija praćena vježbom kontrolne liste o sigurnim praksama rada na daljinu.

Slučaj 4: Ransomware putem e-mail veza

Ovaj slučaj se odnosi na regionalno OCD koje koristi laptope zajedničkih ureda i razmjenu dokumenata zasnovanih na e-poruci. Backup prakse su bile neformalne i nisu se održavale nikakve kompenzacije van mreže. Primljen je e-mail koji liči na izvještaj donatora, a član osoblja otvorio je prilog na a zajednički laptop. Ubrzo nakon toga, fajlovi su postali nedostupni, a na ekranu se pojavila poruka o otkupninini. The organizacija je vjerovala izgledu pošiljaoca, nije imala pravila filtriranja vezanosti i nije održavala offline ili izolirane sigurnosne kopije. Finansijska evidencija i projektna dokumentacija su trajno izgubljeni. OCSOing projekti su prekinuti, a troškovi oporavka su nastali. OCD bi trebali održavati barem jednu offline sigurnosnu kopiju i koristiti usluge u oblaku s omogućenom istorijom verzije. Makro-omogućene i izvršne priloge treba ograničiti, a osoblje treba obučiti da ne otvara neželjene datoteke.

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 4 – Common cyber prijetnje (Malware & Ransomware):**
  Demonstrira kako se ransomware širi putem priloga e-pošte i utjecaja nedostajućih rezervnih kopija.
- **Modul 5 – Zaštita podataka i usklađenost privatnosti:**
  Ističe dostupnost podataka, rezervne obaveze i rizici organizacionog kontinuiteta.

Predložena upotreba:

Diskusija zasnovana na scenariji o rezervnim strategijama i “šta biste prvo uradili?” koraci odgovora.

Slučaj 5: Otpuštena Facebook stranica zbog zajedničkih prijava

Nekoliko omladinskih organizacija podijelilo je jednu prijavu na Facebook među osobljem i volonterima za upravljanje javnim stranicama. Pristup nije pregledan kada su volonteri napustili organizaciju. Bivši volonter je zadržao pristup zajedničkom računu i kasnije ga je zloupotrebio. Facebook stranica je oteta i korištena za objavljivanje lažnih poruka i političkog sadržaja. Zajedničke akreditive, nedostatak pristupa zasnovanog na ulozi i nepovlačenje pristupa kada je osoblje otišlo stvorili su veliki sigurnosni jaz. Reputacija organizacije's je narušena, a donatori su kontaktirali CSO kako bi potvrdili legitimitet objavljenog sadržaja. Oporavak je zahtijevao vrijeme i javno pojašnjenje.

Naučene lekcije i preporuke

Treba izbjegavati zajedničke prijave. Pristup se mora odobriti kroz karakteristike uloga platforme, dvofaktorska autentifikacija treba da bude obavezna za administratore, a prava pristupa moraju se redovno revidirati.

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 6 – Social Media and Online Presence Security:**
  Primarni slučaj zajedničkih akreditiva, pristupa zasnovanog na ulozi i procedura oporavka računa.
- **Modul 7 – Razvoj sigurnosne kulture:**
  Podržava diskusije o politici o procedurama opoziva pristupa i vanboardinga.
- **Modul 8 – napredne teme (praksa kontrole uspjeha):**
  Može se referencirati prilikom uvođenja jačeg upravljanja računom i administrativne kontrole.

Predložena upotreba:
Vježba izrade politike zasnovana na slučajevima koja se fokusira na upravljanje pristupom društvenim mrežama.

PRAKTIČNI ŠABLONI I KONTROLNE LISTE Za organizacije civilnog društva (CSO) u Bosni I Hercegovini

ANEKS 1 – POLITIKA PRIHVATLJIVE UPOTREBE (AUP)

Predložak za male I srednje organizacije civilnog društva u BiH

Naslov dokumenta: Politika prihvatljive upotrebe (AUP)

Aplikacije za: svo osoblje, volonteri, pripravnici, vanjski konsultanti

1. Svrha

   Ova politika definira pravila za sigurno i odgovorno korištenje CSO uređaja, korisničkih naloga i podataka.
2. Računi i lozinke

- Koristite jedinstvene lozinke za svaki račun.
- Ne dijelite lozinke putem chat grupa, aplikacija za razmjenu poruka ili e-pošte.
- Omogućite dvofaktorsku autentifikaciju (2FA) za e-poštu, pohranu u oblaku i administrativne naloge društvenih medija.
- Koristite upravitelj lozinki gdje je to moguće.

3. Uređaji (Laptops i mobilni telefoni)

- Zaključajte sve uređaje sa PIN-om, lozinkom ili biometrijskom zaštitom.
- Omogući automatska ažuriranja sistema I sigurnosti.
- Prijavite izgubljene ili ukradene uređaje u roku od 1 sat do voditelja incidenta.

4. E-mail i linkovi

- Ne otvarajte neočekivane priloge ili veze.
- Uvijek provjerite promjene banke ili plaćanja putem telefonskog poziva na poznati broj.
- Tretirajte hitne poruke ili poruke zasnovane na pritisku kao visok rizik.

5. Wi-Fi i daljinski rad

- Izbjegavajte korištenje javnog Wi-Fi-ja za administratore ili osjetljive račune.
- Koristi mobilni hotspot ili VPN ako je dostupan.

- Onemogući automatsko povezivanje na Wi-Fi mreže.

6. Social Media

- Koristite uloge stranica umjesto zajedničkih prijava.
- Zadrži minimalni broj administratora.
- Uklonite pristup odmah kada član osoblja ili volonter ode.

7. Rukovanje podacima

- Sakupite samo neophodne lične podatke.
- Snimite lične podatke samo na odobrenim lokacijama (npr. CSO cloud drajv).
- Ne pohranjujte korisničke podatke na lične uređaje bez šifriranja.

8. Izvještavanje o incidentima

   Svaki sumnjivi sigurnosni ili podatkovni incident mora se odmah prijaviti korištenjem Plana odgovora na incidente CSO.

Odobreno: _____

DATUM: _____

Sljedeći datum pregleda: _____

ANEKS 2 – PLAN ODGOVORA NA INCIDENTE (IRP)

Pojednostavljeno – za male OCD

Naslov dokumenta: Plan odgovora na incidente (pojednostavljeno)

1. Šta je incident

   Incident je svaki događaj koji prijeti računima, uređajima, podacima ili reputaciji CSO-a, uključujući phishing, preuzimanje računa, zlonamjerni softver, ransomware ili curenje podataka.

2. Uloge i odgovornosti (punite imena)

   Incident olovo: _____

   Komunikacija olovo: _____

   IT podrška (unutrašnji/vanjski): _____

   Odobrenje upravljanja: _____

3. Prvih 15 minuta – neposredne akcije

- Isključite zahvaćeni uređaj sa Wi-Fi-ja ili interneta.
- Uzmite snimke ekrana i zabilježite vrijeme i pogođene račune.
- Informišite interni tim: “Ne kliknite na linkove. Incident pod revizijom.”
- Prvo osigurajte račun e-pošte (promijenite lozinku i omogućite 2FA).

4. Prvih 60 minuta – sadržaja

- Preuredite lozinke ovim redoslijedom: e-pošta, pohrana u oblaku, društveni mediji, bankarstvo ili finansijski alati.
- Zabilježi sve nepoznate ili sumnjive sesije.
- Uklonite nepoznate admine, aplikacije i integracije.
- Provjerite pravila prosljeđivanja e-pošte.

5. Procjena (Isti dan)

- Šta se desilo?

- Na koje podatke može uticati (donatori, korisnici, maloljetnici)?
- Na koje sisteme I račune utiče?

6. Eksterno izvještavanje (Kada se zatraži)

- CERT BiH za podršku incidentima I upozorenja.
- SIPA ili policijske jedinice za sajber kriminal ako se sumnja na sajber kriminal.
- Konsultujte AZLP zahtjeve ako je vjerovatno kršenje ličnih podataka i poduzmu radnje dokumenata.

7. Komunikacijska pravila

- Samo voditelj komunikacija izdaje vanjske izjave.
- Dijelite samo činjenice.
- Obavijesti donatore ili partnere ako je potrebno.

8. Oporavak

- Vratite sisteme iz rezervnih kopija.
- Ažuriraj sve uređaje.
- Osoblje za ponovno obuku o tipu incidenta.

9. Pregled nakon akcije (u roku od 7 dana)

- Koja kontrola nije uspjela?
- Šta se mora promijeniti (2FA, pristupne uloge, rezervne kopije, trening)?
- Politika ažuriranja i kontrolne liste.

ANEKS 3 – PRAVILNIK O ZAŠTITI PODATAKA (UNUTRAŠNJI)

Jednostavan interni pravilnik za OCD

Naslov dokumenta: Pravilo o zaštiti podataka (Interno)

1. Obim

   Ovaj pravilnik se odnosi na sve lične podatke koje obrađuje OCD.

2. Osnovna pravila zaštite podataka

- Procesni podaci zakonito i pošteno.
- Sakupite samo ono što je potrebno (minimalizacija podataka).
- Čuvajte podatke samo koliko god je potrebno.
- Mjere zaštite aplikacija kao što su kontrola pristupa, sigurnosne kopije i 2FA.

3. Odobrene lokacije za skladištenje podataka

   CSO cLOUND drajv: _____

   CSO sistem e-pošte: _____

   Lokalna šifrovana fascikla (ako je potrebno): _____

4. Kontrola pristupa

- Samo osoblje kome trebaju podaci može im pristupiti.
- Uklonite pristup u roku od 24 sata kada neko ode.

5. Osjetljivi podaci i maloljetnici

   Prilikom obrade podataka maloljetnika, primijenite strože kontrole i ograničite pristup.

6. Dijeljenje podataka

- Podijelite podatke samo putem odobrenih kanala.
- Ne dijelite liste korisnika putem WhatsApp-a ili Vibera.
- Koristite datoteke zaštićene lozinkom za osjetljive podatke.

7. Rukovanje incidentima

   Svako za koje se sumnja da je došlo do povrede podataka odmah pokreće Plan odgovora na incidente.

Odobreno: _____

DATUM: _____

Sljedeći datum pregleda: _____

ANEKS 4 – PRAKTIČNE KONTROLNE LISTE

Za BiH OCD sa niskim IT kapacitetima

Kontrolna lista A – Basic Digital Security Checklist (Starter Pack)

Računi

- 2FA omogućeno za e-poštu, oblak i adinove na društvenim mrežama.
- Korištene jedinstvene lozinke.
- Lozinke se ne dijele u grupama za ćaskanje.

Uređaji

- Zaključavanje ekrana omogućeno.
- Uključena su automatska ažuriranja.
- Antivirusni ili sistemski branič je aktivan.

Wi-Fi i daljinski rad

- Wi-Fi za goste je odvojen od Wi-Fi-ja za osoblje.
- Nema administratora koji se prijavljuje na javni Wi-Fi bez vruća tačka ili VPN.

Podaci i rezervne kopije

- Omogućena istorija Cloud verzije.
- Dostupna sedmična rezerva (jedna offline kopija ako je moguće).
- Pristup se odmah uklanja kada neko ode.

Social Media

- Korištene uloge na stranici.
- Samo 1–2 administratora.
- E-mail i telefon za oporavak pripadaju OCD-u.

Kontrolna lista B – kontrolna lista za izvještavanje o incidentima (unutrašnje)

Kada sumnjate u incident

- Isključite pogođeni uređaj sa interneta.
- Uzmite snimke ekrana i zabilježite vrijeme.
- Obavijestite voditelja incidenta odmah.
- Promijenite lozinku e-pošte i omogućite 2FA.
- Provjerite nepoznate prijave i pravila prosljeđivanja e-pošte.
- Identificirajte pogođene podatke (donatori, korisnici, maloljetnici).
- Odlučite da li je potrebno vanjsko izvještavanje (CERT BiH, SIPA, policija, AZLP).

Rekord minimalnih incidenata

Datum I vrijeme detektovan: _____

Detektiva: _____

Šta se dogodilo (kratki opis): _____

Pogođeni računi ili sistemi: _____

Uslikani postupci: _____

Dokazi pohranjeni u: _____

Završeno vanjsko izvještavanje (da/ne): _____

4.3 Pravni, regulatorni i operativni okvir za OCD u Sjevernoj Makedoniji

Pravni i regulatorni okvir u Sjevernoj Makedoniji

Evropski parlament i Vijeće Evropske unije usvojili su 27. aprila 2016. Uredbu (EU) 2016/679 o zaštiti prirodnih lica u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka, ukidajući Direktivu 95/46/EC. Ovo je označilo početak sveobuhvatnog reformskog procesa u oblasti zaštite ličnih podataka. Nakon dvogodišnjeg prelaznog perioda, Uredba je postala primjenjiva širom Evropske unije 25. maja 2018. godine.

Ova Uredba, koja se obično naziva GDPR, u potpunosti je transponovana u Republici Sjevernoj Makedoniji usvajanjem Zakona o zaštiti ličnih podataka, koji je stupio na snagu 24. februara 2020. godine.

Zakon o zaštiti ličnih podataka reguliše sedam osnovnih principa za obradu ličnih podataka:

- zakonitost, pravičnost, i transparentnost,
- ograničenje svrhe,
- minimiziranje podataka,
- tačnost,
- ograničenje skladištenja,
- integritet i povjerljivost,
- odgovornost.

Nevladine organizacije, kao kontrolori podataka, moraju primijeniti sve principe kumulativno u svakom slučaju obrade ličnih podataka i tokom cijelog životnog ciklusa podataka. Neprimjena bilo kojeg od ovih principa predstavlja kršenje Zakona o zaštiti ličnih podataka. Glavni organ nadležan za sprovođenje I nadzor Zakona o zaštiti ličnih podataka je Agencija za zaštitu ličnih podataka.

Osim toga, u oblasti sajber bezbjednosti, Zakon o sigurnosti mrežnih i informacionih sistema, usvojen u julu 2025. godine, predstavlja prvi sveobuhvatni pravni okvir koji reguliše sajber sigurnost u Sjevernoj Makedoniji. Zakon je usklađen sa Evropskom direktivom NIS2 i ima

za cilj uspostavljanje visokog i zajedničkog nivoa zaštite mrežnih i informacionih sistema u javnom i privatnom sektoru.

Ministarstvo digitalne transformacije i Nacionalni tim za odgovor na kompjuterske incidente (MKD-CIRT), koji djeluju u okviru Agencije za elektronske komunikacije, odgovorni su za praćenje, koordinaciju i reagovanje na incidente kibernetičke sigurnosti. Od značaja za privatni sektor, uključujući nevladine organizacije, je prelazni period implementacije koji traje do 2027. godine, tokom kojeg se očekuje da će svi subjekti progresivno poštovati obaveze koje donosi zakon.

Uobičajene prijetnje i nedavni incidenti koji utiču na OCD

Nevladine organizacije u Sjevernoj Makedoniji, slično drugim sektorima, vrlo su osjetljive na prijetnje sajber sigurnosti. Ključni izazov je toliki kibernecidenti ostaju nepriznati ili neprijavljeni, što rezultira nedostatkom sveobuhvatnih i pouzdanih podataka o incidentima. Dok značajan broj organizacija izvještava o informisanju o zakonskim promjenama i prilagođavanju njihove operativne prakse u skladu s tim, dostupni podaci pokazuju da mnoge organizacije nisu usvojile interne akte o zaštiti ličnih podataka i da nisu imenovale službenika za zaštitu ličnih podataka.

Nadalje, udio osoblja OCD-a koji je prošao formalnu obuku o zaštiti ličnih podataka ostaje vrlo nizak. S obzirom na to da OCD često rade sa ograničenim finansijskim resursima i suočavaju se sa poteškoćama u izdvajanju sredstava za obuku osoblja, preporučuje se da se uspostave strukturirani mehanizmi saradnje između Agencije za zaštitu ličnih podataka i nevladinog sektora kako bi se olakšao pristup mogućnostima obuke.

Glavni faktor rizika za OCD je njihov ograničeni budžet za ulaganje u zaštitu podataka i sajber sigurnost. Mnoge manje organizacije i dalje koriste nelicencirani ili zastarjeli softver, što značajno povećava njihovu izloženost sajber prijetnjama. Istovremeno, nekoliko priručnika a na makedonskom jeziku dostupni su dokumenti s uputama koji mogu podržati OCD u jačanju njihove digitalne sigurnosti.

Najidentifikovanije prijetnje uključuju:

• ne provjeravanje pošiljalaca prije klikanja na linkove ili otvaranja poruka,
• ograničena upotreba upravitelja lozinki i česta ponovna upotreba sličnih lozinki,
• nepravilne ili odsutne prakse sigurnosnog kopiranja podataka,
• korištenje nelicenciranog i zastarjelog softvera,
• nedovoljno sigurnosne mjere za mobilne uređaje,
• Vrlo nisko usvajanje dvofaktorske autentifikacije.

Nacionalna podrška i resursi

Nekoliko nacionalnih institucija, uključujući Agenciju za zaštitu ličnih podataka, Ministarstvo digitalne transformacije i Agenciju za elektronske komunikacije, pružaju podršku i smjernice OCD-ovima koji imaju za cilj poboljšanje digitalne sigurnosti i zaštite podataka. Ipak, potrebni su dalji institucionalni napori, uključujući sistematsko planiranje i inicijative koje finansira država.

Podrška se također pruža kroz projekte civilnog društva koje prvenstveno finansiraju strani donatori za povećanje digitalne pismenosti među OCD i opštom populacijom. Značajan primjer je projekat "CyberShield: Osnaženi građani za sajber otpornost," u okviru kojeg su 2025. godine isporučene tri obuke o sajber sigurnosti za organizacije koje rade s marginaliziranim grupama. Kao nastavak, razvijeni su planovi digitalne sigurnosti za šest organizacija civilnog društva. Ovi prilagođeni planovi imaju za cilj da osiguraju sistematsku implementaciju praksi sajber sigurnosti, poboljšanje organizacijske otpornosti i indirektno poboljšanje isporuke usluga krajnjim korisnicima.

Uprkos ovim pozitivnim primjerima, ograničeno finansiranje znači da samo mali broj OCD može imati koristi od takvih inicijativa. Dok je nekoliko priručnika I materijala za podizanje svijesti dostupno u makedonskom, šira I održivija saradnja između njih javne vlasti I OCD su neophodni za proširenje pristupa obuci I aktivnostima izgradnje kapaciteta. Posebno su potrebni povećano finansiranje i ciljani programi za podršku direktnom obrazovanju i obuci osoblja OCD.

Kulturni i operativni kontekst OCD u Sjevernoj Makedoniji

Većina OCD-a u Sjevernoj Makedoniji radi na modelu zasnovanom na donatorima i projektima i obično ima male administrativne i operativne timove ili se u velikoj mjeri oslanja na volontere. Organizacioni rad se često obavlja pomoću ličnih uređaja i široko dostupnih digitalnih usluga kao što su Google Workspace, Dropbox ili Microsoft 365, često bez odgovarajućeg licenciranja.

Inicijative za obuku i izgradnju kapaciteta bi se stoga trebale fokusirati na praktične i realistične mjere, uključujući:

- prednosti korištenja licenciranih proizvoda i usluga,
- "Think Before You Click" kampanje podizanja svijesti,
- redovne sigurnosne kopije podataka i informacija,
- aktivna i dosljedna upotreba dvofaktorske autentifikacije,
- osiguranje mobilnih uređaja i upravljanje njihovom upotrebom,
- Odgovorne prakse lozinki,
- Efikasna upotreba rješenja zasnovanih na oblaku,
- Povećana svijest o praksama dijeljenja podataka.

Nivo digitalne pismenosti u Sjevernoj Makedoniji i dalje je nedovoljan, uključujući i sektor OCD. Potrebna su dodatna sredstva, resursi i koordinirani napori da se postigne viši nivo digitalne sigurnosti. Ove napore treba prevesti u konkretne programe i planove praktične akcije prilagođene stvarnim potrebama i kapacitetima organizacija civilnog društva.

Aneksi i templati spremni za upotrebu (Sjeverna Makedonija)

ANNEX 1 – Pejzaž digitalne sigurnosti za OCD u Sjevernoj Makedoniji

Ovaj aneks odražava pravnu, institucionalnu i operativnu stvarnost koja utiče na organizacije civilnog društva u Severnoj Makedoniji i podržava lokalizaciju nastavnog plana i programa.

Threat Landscape

• Phishing napadi putem e-pošte i lažnih institucionalnih poruka,
• Incidenti sa ransomware-om i gubitak podataka zbog nedostajućih rezervnih kopija,
• Zloupotreba neosiguranih ličnih podataka,
• Rizici vezani za korištenje ličnih laptopa i mobilnih uređaja.

Operativni izazovi

• Niska upotreba upravitelja lozinki i česta ponovna upotreba lozinki,
• Nepravilne rutine za sigurnosno kopiranje podataka ili nedostaju,
• Upotreba nelicenciranog ili zastarjelog softvera,
• Nedovoljno obezbeđenje mobilnih uređaja,
• Ograničeno usvajanje dvofaktorske autentifikacije,
• Nedostatak namjenskog finansiranja za mjere digitalne sigurnosti.

Predložak: 10 Osnovnih koraka za povećanje digitalne zaštite

Za OCD u Sjevernoj Makedoniji preporučuju se sljedeći osnovni koraci:

• Instalirajte i redovno ažurirajte antivirusni i anti-malware softver,
• Primijenite odmah ažuriranja sistema i softvera
• Koristite jake i jedinstvene lozinke za svaki račun,
• Izbjegavajte otvaranje priloga iz nepoznatih ili sumnjivih izvora
• Unesite osjetljive podatke samo na šifrirane web stranice,
• Obavlja redovne sigurnosne kopije organizacionih podataka,
• Koristite odvojene adrese e-pošte za različite svrhe
• Sprečite phishing ručnim kucanjem adresa web stranice,

• Uklonite zastarjele ili nepodržane aplikacije
• Obradite lične i organizacione podatke oprezno.

Predlog – internih operativnih pravila za digitalnu bezbednost

Svaki OCD treba da usvoji jednostavan interni dokument koji definiše pravila digitalne bezbednosti za osoblje, volontere i posetioce. Dokument bi trebao uključivati:

• Koristite jedinstvene lozinke za svaki račun,
• Ne dijelite lozinke putem chat aplikacija ili e-pošte
• Omogućite dvofaktorsku autentifikaciju za e-poštu, pohranu u oblaku i administrativne naloge društvenih medija,
• Koristite upravitelj lozinki gdje je to moguće,
• Zaključaj sve uređaje sa PIN-ovima ili lozinkama
• Omogući automatska ažuriranja,
• Odmah prijavite izgubljene ili ukradene uređaje
• Provjeri sve zahtjeve za banke I promjene plaćanja,
• Koristi mobilni žarišta kada radite izvan prostorija OCD
• Dodijelite pristup društvenim medijima samo putem platformskih uloga,
• Držite broj administratora na minimumu,
• Sakupite I pohranite samo neophodne lične podatke,
• Odmah prijavite svaki sigurnosni incident navedenom odgovornom licu.

Predložak – Plan odgovora na incidente (pojednostavljeni)

Kada se dogodi ili se sumnja na incident digitalne sigurnosti, moraju se poduzeti sljedeći koraci:

- Isključite zahvaćeni uređaj iz mreže
- Sačuvajte dokaze vezane za incident,
- Obavijesti interni tim,
- Prvo osigurajte račun e-pošte promjenom lozinki i omogućavanjem 2FA

- Preuredite lozinke za sve pogođene račune,
- Log nepoznate ili sumnjive sesije,
- Uklonite nepoznate administratore i povezane aplikacije, prijavite incidente MKD-CIRT-u,
- Prijavite sumnjivi sajber kriminal policijskim jedinicama za sajber kriminal,
- Konsultirajte Agenciju za zaštitu ličnih podataka ako se sumnja na kršenje podataka
- Procjenite utjecaj incidenta i vratite sisteme iz rezervnih kopija,
- Ažurirajte uređaje I softver,
- Osoblje za prekvalifikaciju,
- Ažurirajte interne politike i kontrolne liste ako je potrebno.

Praktične kontrolne liste za OCD u Sjevernoj Makedoniji

ANNEX 1 – Pejzaž digitalne sigurnosti za OCD u Sjevernoj Makedoniji

Ovaj aneks opisuje pravni, institucionalni i operativni kontekst koji utiče na organizacije civilnog društva (OCD) u Severnoj Makedoniji. Podržava lokalizaciju nastavnog plana i programa digitalne sigurnosti odražavajući zajedničke rizike, kapacitete i praktične potrebe OCD-a koji posluju u zemlji.

Threat Landscape

Organizacije civilnog društva u Sjevernoj Makedoniji obično se suočavaju s sljedećim prijetnjama digitalnom sigurnošću:

- phishing napadi putem e-pošte i lažnih institucionalnih poruka
- incidenti ransomware-a i gubitak podataka zbog nedostajućih ili neadekvatnih rezervnih kopija
- zloupotreba ili izlaganje neosiguranih ličnih podataka
- rizici vezani za korišćenje ličnih laptopa I mobilnih uređaja za organizacioni rad

Operativni izazovi

U praksi, mnogi OCD u Sjevernoj Makedoniji doživljavaju sljedeće izazove:

- Niska upotreba upravitelja lozinki i česta ponovna upotreba lozinki,
- Nepravilne rutine za sigurnosno kopiranje podataka ili nedostaju,
- Upotreba nelicenciranog ili zastarjelog softvera,
- Nedovoljno obezbeđenje mobilnih uređaja,
- Ograničeno usvajanje dvofaktorske autentifikacije,
- Nedostatak namjenskog finansiranja za mjere digitalne sigurnosti.

Deset osnovnih koraka za povećanje digitalne zaštite

Sljedeći osnovni koraci preporučuju se organizacijama civilnog društva u Sjevernoj Makedoniji da poboljšaju svoje digitalno sigurnosno držanje:

1. Instalirajte i redovno ažurirajte antivirusni i anti-malware softver.
2. Primijenite ažuriranja sistema i softvera odmah kada su dostupna.
3. Koristite jake i jedinstvene lozinke za svaki račun.
4. Izbjegavajte otvaranje priloga iz nepoznatih ili sumnjivih izvora.
5. Unesite osjetljive podatke samo na šifrirane web stranice (HTTPS).
6. Obavlja redovne sigurnosne kopije organizacionih podataka.
7. Koristite odvojene adrese e-pošte za različite svrhe (npr. administraciju, projekte, javnu komunikaciju).
8. Sprečite phishing ručnim kucanjem adresa web stranice umjesto klikom na linkove.
9. Uklonite zastarjele ili nepodržane aplikacije s uređaja.
10. Bavite se ličnim i organizacionim podacima oprezno u svakom trenutku.

Interna operativna pravila za digitalnu sigurnost

Svaki OCD treba da usvoji jednostavan interni dokument koji definiše pravila digitalne bezbednosti za osoblje, volontere i posetioce. U najmanju ruku, ovaj dokument bi trebao uključivati sljedeća pravila:

- ☐ Koristite jedinstvene lozinke za svaki račun.
- ☐ Ne dijelite lozinke putem chat aplikacija ili e-pošte.
- ☐ Omogućite dvofaktorsku autentifikaciju za račune e-pošte, pohrane u oblaku i administratora društvenih medija.
- ☐ Koristite upravitelj lozinki gdje je to moguće.
- ☐ Zaključajte sve uređaje sa PIN-ovima, lozinkama ili biometrijskom zaštitom.
- ☐ Omogući automatsko ažuriranje sistema I aplikacija.
- ☐ Odmah prijavite izgubljene ili ukradene uređaje.

- ☐ Provjeri sve zahtjeve za banke I promjene plaćanja putem sekundarnog kanala.
- ☐ Koristi mobilni žarišta kada radite izvan prostorija OCD.
- ☐ Dodijelite pristup društvenim medijima samo putem funkcija uloga platforme.
- ☐ Držite broj administratora na minimumu.
- ☐ Sakupite I pohranite samo neophodne lične podatke.
- ☐ Odmah prijavite svaki sigurnosni incident navedenom odgovornom licu.

Plan odgovora na incidente za OCD u Sjevernoj Makedoniji

Kada se dogodi ili se sumnja na incident digitalne sigurnosti, treba poduzeti sljedeće korake kako bi se:

1. Isključite zahvaćeni uređaj iz mreže.
2. Sačuvajte dokaze vezane za incident (pucnjeve ekrana, dnevnici, poruke).
3. Obavijestite interni tim i imenovanu odgovornu osobu.
4. Prvo osigurajte račun e-pošte promjenom lozinki i omogućavanjem dvofaktorske autentifikacije.
5. Preuredite lozinke za sve pogođene račune.
6. Zabilježite nepoznate ili sumnjive aktivne sesije.
7. Uklonite nepoznate administratore i povezane aplikacije.
8. Prijavite incidente da **MKD-CIRT**.
9. Prijavite sumnjivi sajber kriminal policijskim jedinicama za sajber kriminal.
10. Konsultant **Agencija za zaštitu ličnih podataka** ako se sumnja na kršenje ličnih podataka.
11. Procijenite uticaj incidenta.
12. Vratite sisteme i podatke iz rezervnih kopija gdje je to moguće.
13. Ažurirajte uređaje I softver.
14. Osoblje za prekvalifikaciju i volonteri ako je potrebno.
15. Ažurirajte interne politike i kontrolne liste na osnovu naučenih lekcija.

ANEKS 2: Osnovna kontrolna lista digitalne sigurnosti

Aktivnost/Mjera	Provjereno (Y/N)
2FA omogućeno za sve online prodajne kuće	
Jedinstvene lozinke koje se koriste za različite račune	
Lozinke se ne dijele u digitalnom obliku	
Zaključavanje ekrana je omogućeno na svim uređajima	
Uključena su automatska ažuriranja	
Antivirus omogućen i ažuriran	
Wi-Fi osoblja odvojen od gostiju	
Omogućeni rezervni podaci	
Različite uloge na stranicama na društvenim mrežama	
E-mail/telefon za oporavak pripada CSO-u	
Upotreba Wi-Fi administrativnih uređaja na vrućoj tački u javnosti	
Zatvoren I isključen sav uređaj nakon posla	

ANEKS 3: Kontrolna lista za izvještavanje o incidentima

Aktivnost/Mjera	**Provjereno (Y/N)**
Pogođeni uređaji isključeni s interneta	
Dokazi iz napada su uzeti	
Promijenjena e-pošta i druge lozinke društvenih medija	
Identifikovani pogođeni podaci	
Nepoznati dimini/aplikacije uklonjene	
Omogućeno 2FA	
Interni tim je obaviješten o tome šta se dogodilo	
Podaci o bankama i plaćanju su onemogućeni sa uređaja	
Odgovorna vlast/institucija je obaviještena o napadu	

Pravni i regulatorni okvir u Norveškoj i prijedlozi za OCD u Norveškoj

Pravni i regulatorni okvir u Norveškoj

Organizacije civilnog društva (CSO) koje posluju u Norveškoj podliježu Općoj uredbi EU o zaštiti podataka (GDPR) i Norveškom zakonu o ličnim podacima (Persopplysningsloven), koji uključuje i dopunjuje GDPR u norveški zakon. Ovi pravni okviri se odnose na sve organizacije koje obrađuju lične podatke, uključujući neprofitne i volonterske organizacije, bez obzira na veličinu. Kompetentno nadzorno tijelo je Datatilsynet, norveško tijelo za zaštitu podataka.

Norveški OCD obično obrađuju lične podatke koji se odnose na korisnike, članove, volontere, donatore, zaposlene i, u mnogim slučajevima, ranjive grupe. Takvi podaci mogu uključivati imena, kontakt podatke, finansijske informacije, podatke vezane za zdravlje, evidenciju slučajeva ili osjetljive pozadinske informacije. Kao kontrolori podataka, od OCD-a se traži da budu u skladu sa osnovnim principima zakona o zaštiti podataka.

Ključne zakonske obaveze uključuju:

Zakonita osnova za obradu: Svi lični podaci moraju se obrađivati na važećem pravnom osnovu kao što su pristanak, legitimna kamata, ugovorna potreba ili zakonska obaveza.

Informisani pristanak (gdje je primjenjivo): Pristanak se mora slobodno davati, specifičan, informisan i revokabilan.

Transparentnost: Pojedinci moraju biti obaviješteni o tome kako se njihovi podaci prikupljaju, koriste, pohranjuju, dijele i zadržavaju putem jasnih obavijesti o privatnosti.

Minimizacija podataka i ograničenje svrhe: Samo podaci koji su striktno neophodni za definisane svrhe mogu se prikupljati i zadržavati.

Sigurnost obrade: OCD moraju implementirati odgovarajuće tehničke i organizacione mjere za zaštitu ličnih podataka od neovlaštenog pristupa, gubitka ili zloupotrebe.

Zadržavanje i brisanje podataka: Lični podaci se ne smiju pohraniti duže nego što je potrebno; moraju se definirati periodi zadržavanja i rutine brisanja.

Upravljanje procesorima: Pisani ugovori o obradi podataka moraju se održavati sa svim provajderima eksternih usluga koji rukuju ličnim podacima.

Međunarodni prijenosi podataka: Lični podaci bi se po mogućnosti trebali pohraniti u EU/EEA. Transferi u treće zemlje zahtijevaju važeće zaštitne mjere kao što su standardne ugovorne klauzule (SCC) i dodatne mjere.

Obavijest o lomu: Kršenja ličnih podataka moraju se procijeniti odmah i, gdje je to potrebno, prijaviti Datatilsynetu u roku od 72 sata.

Datatilsynet je više puta identifikovao zajedničke izazove među norveškim OCD-ovima, uključujući nejasne rutine pristanka, nesigurno skladištenje u oblaku izvan EU/EEA, nedostatak dokumentovanih internih procedura i prekomerno zadržavanje podataka.

Etičke odgovornosti u zaštiti podataka

Osim zakonskih obaveza, norveški OCD imaju etičku dužnost da zaštite privatnost, dostojanstvo i sigurnost pojedinaca čije podatke obrađuju. Mnogi OCD rade s ljudima u ranjivim situacijama – kao što su izbjeglice, djeca, žrtve nasilja ili politički izloženi pojedinci – gdje izloženost podacima može dovesti do ozbiljne lične štete.

Kršenje podataka može rezultirati:

- Šteta korisnicima I volonterima
- Gubitak donatora, partnera i povjerenja javnosti,
- Pravne posljedice I finansijske kazne,
- Oštećenje reputacije i operativni poremećaj.

Etičko rukovanje podacima, dakle, zahtijeva pristup predostrožnosti: prikupljanje minimalnih potrebnih podataka, njihovo efikasno zaštitu i dijeljenje samo kada je to strogo potrebno.

Usklađenost zgrada u dnevnu praksu

Za mnoge norveške OCD, posebno one koji se oslanjaju na volontere i ograničene IT kapacitete, usklađenost mora biti praktična i održiva.

Efikasna implementacija uključuje:

- Određivanje odgovornog lica za zaštitu podataka I digitalnu sigurnost, čak I ako je na pola radnog vremena ili u kombinaciji s drugom ulogom.
- Razvijanje kratkih i pristupačnih internih dokumenata kao što su Politika zaštite podataka i smjernice za rukovanje podacima.

- Implementacija rutina kontrole pristupa, uključujući pojedinačne korisničke naloge, pristup zasnovan na ulozi i pravovremeno uklanjanje neaktivnih korisnika.
- Odabir sigurnih rješenja za pohranu podataka, po mogućnosti usluga u oblaku zasnovanih na EU/EEA za lične podatke.
- Osiguravanje sporazuma o obradi podataka postoji sa svim vanjskim provajderima.
- Pružanje redovne obuke za podizanje svijesti za osoblje i volontere o phishingu, lozinkama i sigurnom rukovanju podacima.
- Održavanje jednostavne rutine odgovora na incidente koja pokriva identifikaciju, zadržavanje, dokumentaciju i eskalaciju.
- Ugradnja ovih rutina u svakodnevne operacije pomaže da se osigura da je usklađenost kontinuirana, a ne reaktivna.

Studije slučaja iz Norveške

Studija slučaja 1: Ciljani ribolov tokom kampanje prikupljanja sredstava (Oslo, 2023)

Godine 2023., mali humanitarni OCD sa sjedištem u Oslu doživio je ciljanu kampanju phishinga tokom svoje godišnje akcije prikupljanja sredstava. Attackers su kreirali lažnu verziju stranice za donacije CSO's i poslali e-poruke pristalicama tvrdeći da je organizacija "ažurirala svoj sistem plaćanja." Nekoliko donatora je ušlo u detalje svoje kartice prije nego što je OCD saznao za prevaru. Incident je oštetio povjerenje donatora i zahtijevao je značajno vrijeme i napore da se riješe problemi s bankama i pogođenim pristalicama.

Osnovna kombinacija sigurnosnih mjera – kao što je dvofaktorska autentifikacija na nalozima e-pošte, praćenje domena i obuka osoblja o phishing crvenim zastavicama – mogla je smanjiti utjecaj incidenta ili u potpunosti spriječiti napad.

Pitanja diskusije:

- Koje su bile glavne ranjivosti iskorištene u ovom incidentu?
- Koji su znaci upozorenja mogli ukazivati da su e-mailovi i stranica za donacije lažni?
- Koje osnovne mjere digitalne sigurnosti su mogle spriječiti ili ograničiti štetu?

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 1 – Osnove kibernetičke sigurnosti:**
  Koristi se kao temeljni primjer phishing-a i eksploatacije povjerenja usmjerene na donatore i pristalice.
- **Modul 4 – Zajedničke sajber prijetnje (Fishing & Social Engineering):**
  Demonstrira napredne tehnike phishinga, uključujući lažne web stranice i lažno predstavljanje.
- **Modul 6 – Social Media and Online Presence Security:**
  Može se referencirati kada se raspravlja organizaciona reputacija, povjerenje javnosti i sigurne online prakse prikupljanja sredstava.
- **Modul 7 – Razvoj sigurnosne kulture:**
  Podržava diskusiju o svijesti osoblja, protokolima komunikacije donatora i preventivnoj obuci.

Predložena upotreba:

Analiza slučaja praćena grupnom vježbom o identifikaciji phishing crvenih zastavica u komunikacijama prikupljanja sredstava i dizajniranju sigurne kontrolne liste za komunikaciju donatora.

Studija slučaja 2: Zabrana web stranice zbog zastarjelog plugina (Bergen, 2022)

2022. godine, mali CSO za ljudska prava sa sjedištem u Bergenu je oštetio svoju web stranicu WordPress nakon što su napadači iskoristili zastarjeli dodatak. Početna stranica je zamijenjena političkom propagandom, a organizacija je izgubila pristup administratoru. Budući da CSO nije imao nedavne sigurnosne kopije web stranice, obnavljanje stranice trajalo je više od dvije sedmice i zahtijevalo je vanjsku tehničku pomoć. Incident je poremetio komunikaciju sa volonterima i donatorima i izazvao zabrinutost za reputaciju.

Rutinska ažuriranja softvera, jake administratorske lozinke, dvofaktorska autentifikacija i automatizirane sigurnosne kopije značajno bi smanjile utjecaj napada**.**

Pitanja diskusije:

- Kakve su tehničke I organizacione slabosti doprinijele ovom incidentu?
- Kako je nedostatak rezervnih kopija uticao na sposobnost organizacije da se oporavi
  - Koje preventivne mjere o kojima se raspravlja u modulu's ključne teme mogle bi pomoći u izbjegavanju sličnih incidenata u budućnosti?

Praktične kontrolne liste digitalne sigurnosti i zaštite podataka za OCD u Norveškoj

Relevantni modul(i) i upotreba u nastavnom planu i programu

- **Modul 3 – uređaji i sigurnost infrastrukture:**
  Osnovni slučaj koji ilustruje rizike vezane za zastarjeli softver i nesigurnu infrastrukturu web stranica.
- **Modul 5 – Zaštita podataka i usklađenost privatnosti:**
  Ističe važnost dostupnosti podataka, integriteta i rezervnih kopija za organizacioni kontinuitet.

- **Modul 6 – Social Media and Online Presence Security:**
  Relevantno za diskusije o integritetu web stranice, upravljanju reputacijom i kontroli sadržaja.
- **Modul 7 – Razvoj sigurnosne kulture:**
  Podržava svijest o zajedničkoj odgovornosti za ažuriranja i održavanje, a ne samo "IT zadatke."

Predložena upotreba:

Diskusija zasnovana na scenarija praćena praktičnom vježbom kontrolne liste o održavanju web stranice, rutinama ažuriranja i planiranju rezervnih kopija.

ANEX-1: Pravna i GDPR kontrolna lista usklađenosti za OCD u Norveškoj

☐ Svi lični podaci koje organizacija obrađuje su identifikovani i dokumentovani.

☐ Definira se i bilježi zakonita osnova za svaku procesorsku aktivnost.

☐ Dostupna je i saopštena Obavijest o privatnosti/Politika zaštite podataka.

☐ Mehanizmi pristanka su jasni i revokabilni gdje je to potrebno.

☐ Periodi zadržavanja podataka su definisani i primenjeni.

☐ Ugovori o obradi podataka postoje sa svim vanjskim pružaocima usluga.

☐ Lični podaci se pohranjuju unutar EU/EEA ili štite važećim zaštitnim mjerama.

☐ Postoji rutina obavještavanja o kršenju podataka, a poznato je pravilo od 72 sata.

ANEKS-2. Osnovna kontrolna lista digitalne sigurnosti

☐ Snažne, jedinstvene lozinke se koriste za sve organizacione račune.

☐ U upotrebi je upravitelj lozinki.

☐ Autentifikacija sa dva faktora je omogućena na nalozima e-pošte, oblaka i društvenih medija.

☐ Uređaji su zaštićeni zaključavanjem ekrana i jakim PIN-ovima/prolaznim riječima.

☐ Operativni sistemi i aplikacije se automatski ažuriraju.

☐ Softver protiv virusa/anti-malvera je instaliran i ažuriran.

☐ Kritički podaci se redovno i bezbedno podržavaju.

ANEKS -3. Kontrolna lista upravljanja oblakom i računom

☐ Koriste se pojedinačni korisnički nalozi; izbjegavaju se zajedničke prijave.

☐ Prava pristupa su zasnovana na ulozi i ograničena na neophodnost.

☐ Neaktivni računi se odmah uklanjaju.

☐ Dozvole za pristup oblaku se periodično revidiraju.

☐ Osjetljivi fajlovi se dijele s ograničenjima i ograničenjima isteka.

☐ Dnevnici aktivnosti su omogućeni tamo gdje su dostupni.

ANEKS-4. Kontrolna lista društvenih medija i online prisutnosti

☐ Dvofaktorska autentifikacija je omogućena na svim nalozima na društvenim mrežama.

☐ Uloge administratora se dodjeljuju pojedinačno.

☐ Adrese e-pošte za oporavak i brojevi telefona su ažurirani.

☐ Liste administratora se redovno pregledavaju.

☐ Postoji plan odgovora za otmicu ili lažno predstavljanje računa.

☐ Web stranica CMS i dodaci se redovno ažuriraju.

ANEKS-5. Kontrolna lista odgovora i izvještavanja o incidentima

☐ Određena je sigurnosno odgovorna osoba.

☐ Osoblje zna kako interno prijaviti sumnjive incidente.

☐ Postoji pisana procedura odgovora na incident.

☐ Dokazi i dnevnici se čuvaju nakon incidenata.

☐ Ozbiljni sajber incidenti se prijavljuju NorCERT-u kada je to prikladno.

☐ Lična kršenja podataka prijavljena su Datatilsynetu kada je to potrebno.

☐ Naučene lekcije su dokumentovane i procedure ažurirane.

ANEKS-6. Kontrolna lista za svijest o osoblju i volonterima

☐ Novo osoblje i volonteri dobijaju sigurnosnu i privatnost.

☐ Priznate su politike prihvatljive upotrebe i zaštite podataka.

☐ Obezbeđena je redovna obuka za osveženje.

☐ Postoje jasna pravila za korištenje ličnih uređaja za rad OCD.

☐ Osjetljivi podaci se ne dijele nesigurnim kanalima.

Prijedlozi i praktične preporuke

Norveški OCD bi trebali dati prioritet jednostavnim, dobro dokumentiranim rutinama u odnosu na složena tehnička rješenja. Kombinacijom jasnih internih politika, osnovnih tehničkih mjera zaštite, redovne obuke i etičke svijesti, organizacije mogu značajno smanjiti svoje digitalne rizike uz održavanje usklađenosti sa GDPR i norveškim zakonom.

Dodatni norveško-specifični bodovi za koje bi trebalo biti svjesni

1. Volonterska prekretnica i upravljanje životnim ciklusom pristupa

Norveški OCD se u velikoj mjeri oslanjaju na kratkoročne volontere, pripravnike i osoblje sa skraćenim radnim vremenom. Jedan od najčešćih rizika koje su prijavili Datatilsynet i NSM je neuspjeh da se ukine pristup kada pojedinci napuste organizaciju.

Šta bi OCD trebalo da znaju:

- Svaki brod mora imati odgovarajuću kontrolnu listu van ukrcaja,
- Računi, pristup e-pošti, fascikle u oblaku i uloge na društvenim mrežama moraju se odmah ukloniti,
- Zajednički računi dramatično povećavaju rizik u volonterskim organizacijama,
- Ova tačka jača modul 7 (Sigurna kultura i politike).

2. Nacionalni brojevi identiteta i osjetljivi identifikatori

Neki norveški OCD obrađuju fødselsnummer (broj nacionalnog identiteta), zdravstvene podatke, informacije vezane za azil ili pravne detalje slučaja.

Zašto je to važno:

- Ovi tipovi podataka zahtijevaju više standarde zaštite prema GDPR-u
- Skladištenje u neosiguranim tabelama ili općim fasciklama u oblaku je praksa visokog rizika,
- Šifrovanje i stroga kontrola pristupa su od suštinskog značaja,
- Ovo se prirodno uklapa u modul 5 (Zaštita podataka i privatnost), ali se može unakrsno referencirati u treningu Modula 7.

3. Cloud Services i Schrems II Awareness

Mnogi norveški OCD koriste globalne usluge u oblaku (Google, Microsoft, Dropbox) bez razumijevanja implikacija prijenosa podataka.

Realnost specifična za Norvešku:

- Datatilsynet očekuje da će CSO biti svjesni rezidentnosti podataka EU/EEA,
- Transferi izvan EU/EEA zahtijevaju zaštitne mjere (SCC + procjena rizika),
- "Koristimo velikog provajdera" nije dovoljno opravdanje,
- Ovo jača modul 8 (napredne teme) pravno-tehničkim uglom.

4. Koordinacija između NorCERT-a i Datatilsynet-a

OCD često brkaju koga da prijave šta.

OCD-ovi jasne razlike bi trebali znati:

- NorCERT (NSM): ozbiljni incidenti kibernetičke sigurnosti (ransomware, preuzimanje računa, prekid usluge),
- Datatilsynet: kršenja ličnih podataka (GDPR – u roku od 72 sata),
- Neki incidenti zahtijevaju oba obavještenja,
- Ovo je ključni dodatak modulu 7 (Incident Response & Reporting).

5. Psihološka sigurnost i "kultura izvještavanja No-Blame"

Norveška organizaciona kultura snažno cijeni povjerenje i ravne hijerarhije –, ali to može imati suprotne rezultate ako se osoblje plaši sramote.

Najbolja praksa:

- Osoblje treba odmah ohrabriti da prijavi greške (kliknuta phishing link, izgubljeni uređaj),
- Kultura bez krivice smanjuje štetu i poboljšava vrijeme odgovora,
- Ovo je važan kulturni sloj za modul 7 koji ide dalje od tehničkih kontrola.

6. Odgovornost odbora i nadzor upravljanja

U Norveškoj se sve više očekuje da odbori OCD-a razumiju digitalni rizik kao dio dobrog upravljanja.

Šta daske treba da znaju:

- Cyber sigurnost i zaštita podataka su pitanja upravljanja, a ne samo IT pitanja
- Odbori bi trebali odobriti osnovne sigurnosne politike i planove odgovora na incidente
- Ozbiljni incidenti mogu imati pravne i reputacijske posljedice po vodstvo
- Ovo se može dodati kao napomena o upravljanju prema modulu 7 ili modulu 8.

7. Civilno društvo kao strateška meta

Norveški OCD koji rade na demokratiji, ljudskim pravima, vanjskoj politici ili međunarodnoj pomoći smatraju se strateškim ciljevima, a ne nasumičnim žrtvama.

Implikacije:

- Napadi mogu biti uporni, suptilni i vođeni inteligencijom
- Nisu sve prijetnje usmjerene na novac. Neki imaju za cilj nadzor ili poremećaj
- Svjesnost o brifinzima prijetnji NSM-a je kritična
- Ovo pojačava modul 1 i modul 8 sa modelom prijetnje specifičnim za Norvešku.

DODATAK

Dodatak 1: Pojmovnik ključnih pojmova

- ***Antivirus (AV):*** *Softver koji detektuje i uklanja zlonamjerni softver (virusi, trojani, itd.) sa računara. Primjer: Windows Defender ili Avast.*
- ***Backup:*** *Dodatna kopija podataka pohranjenih odvojeno u svrhu oporavka, npr., čuvanje datoteka na vanjskom tvrdom disku ili cloud servisu tako da se mogu vratiti ako se izgube originali.*
- ***Napad grubih snaga:*** *Metoda u kojoj napadači isprobavaju mnogo lozinki ili ključeva dok se ne pronađe ispravna. Jake lozinke i politike zaključavanja pomažu u odbrani od ovoga.*
- ***Kršenje podataka:*** *Incident u kojem se osjetljivim informacijama pristupa ili otkriva bez odobrenja. Može se pojaviti hakiranjem, izgubljenim uređajima itd.*
- ***Šifrovanje:*** *Proces pretvaranja podataka u kodirani format koji je nečitljiv bez ključa. Štiti povjerljivost informacija (npr. HTTPS šifrira web promet).*
- ***Vatrozid:*** *Uređaj ili softver za mrežnu sigurnost koji prati i filtrira dolazni i odlazni mrežni saobraćaj na osnovu sigurnosnih pravila. Može blokirati neovlašteni pristup uz omogućavanje legitimne komunikacije.*
- ***Malver:*** *Zlonamjeran softver dizajniran da šteti ili iskorištava sisteme. Uključuje viruse, ransomware, špijunski softver, itd. Često se isporučuju putem priloga e-pošte ili zlonamjernih web stranica.*
- ***Multi-Factor Authentication (MFA / 2FA):*** *Korištenje više od jedne metode verifikacije za prijavu (npr., lozinka + jednokratni kod na telefonu). Dramatično poboljšava sigurnost računa.*
- ***Phishing:*** *Lažan pokušaj (obično putem e-pošte) da se pojedinci prevare da otkriju osjetljive informacije ili instaliraju zlonamjerni softver predstavljajući se kao pouzdani entitet. Fishing kopljem odnosi se na ciljane pokušaje određenih pojedinaca ili organizacija.*

- ***Ransomware:*** *Malver koji šifrira podatke žrtve i zahtijeva plaćanje ključa za dešifriranje. Ako ne postoje sigurnosne kopije, žrtve se suočavaju s pritiskom da plate hakerima da povrate pristup.*
- ***Socijalno inženjerstvo:*** *Taktike koje manipulišu ljudima da otkriju povjerljive informacije ili da izvode radnje koje ugrožavaju sigurnost. Phishing je jedan oblik; drugi uključuju pretekst ili mamljenje. Iskorištava ljudsko povjerenje i radoznalost.*
- ***VPN (virtuelna privatna mreža):*** *Alat koji kreira šifrirani tunel preko interneta od vašeg uređaja do servera, štiteći podatke u tranzitu i maskirajući vašu IP adresu. Korisno na javnom Wi-Fi-ju za sigurnu vezu.*
- ***Ranjivost:*** *Slabost u softveru, hardveru ili proceduri koju napadači mogu iskoristiti da dobiju neovlašteni pristup ili izvrše neovlaštene radnje. Patching rješava poznate ranjivosti.*
- ***Wi-Fi enkripcija (WPA2/WPA3):*** *Sigurnosni protokoli za bežične mreže koji šifriraju promet između uređaja I rutera. Pobrinite se da vaš Wi-Fi koristi barem WPA2 sa jakom šifrom za propust kako biste spriječili prisluškivanje.*

Dodatak II: Predložak politike lozinki (primjer)

Svrha: Uspostaviti zahtjeve za kreiranje, korištenje i upravljanje lozinkama za zaštitu informacionih sistema organizacije's.

Obim: Ova politika se odnosi na svo osoblje, volontere i izvođače [ime organizacije] koji koriste IT sisteme (uključujući računare, e-poštu, aplikacije i web stranice) za organizacioni rad.

Izjave o politici:

- *Sve korisničke lozinke moraju biti dugačke najmanje 12 znakova, miješajući slova, brojeve i posebne simbole u gornjem i donjem dijelu slova.*
- *Zadane lozinke moraju se mijenjati odmah nakon prve upotrebe.*
- *Lozinke se ne smiju dijeliti između pojedinaca ili zapisivati na nesigurnim lokacijama.*

- *Dvofaktorska autentifikacija (2FA) je potrebna za sav daljinski pristup organizacionim sistemima i za račune e-pošte.*
- *Lozinke za kritične sisteme (finansijske, donatorske baze podataka) moraju se mijenjati svakih 90 dana.*
- *Korisnici ne smiju ponovo koristiti lozinke koje su korištene na drugim (javnim) nalozima ili koje su procurile u kršenju.*
- *Ako se sumnja da je lozinka ugrožena, ona se mora odmah promijeniti, a službenik za IT/sigurnosnu zaštitu mora biti obaviješten.*

Uloge i odgovornosti:

- *Korisnici moraju poštovati ova pravila i prijaviti svaki sumnjivi kompromis.*
- *IT osoblje će provoditi pravila lozinke putem tehničkih kontrola (npr. upravitelji lozinki, zaključavanja računa nakon neuspjelih pokušaja).*
- *Službenik sigurnosti će pregledati usklađenost i ažurirati politiku svake godine.*

Sprovođenje: Kršenje ove politike može rezultirati oduzimanjem privilegija pristupa ili drugim disciplinskim mjerama.

Dodatak III: Backup Policy Template (Primjer)

Svrha: Kako bi se osiguralo da se kritični podaci redovno podržavaju i da se mogu vratiti u slučaju gubitka, korupcije ili katastrofe.

Obim: Primjenjuje se na sve podatke pohranjene na organizacijskim serverima, radnim stanicama i uređajima za pohranu mreže na [ime organizacije].

Izjave o politici:

- *Kritički podaci (zapisi donatora, finansijske datoteke, baze podataka projekata, itd.) moraju biti podržani barem svakodnevno.*
- *Rezervne kopije bi trebale uključivati sistemske konfiguracije i aplikacije potrebne za obnavljanje operacija.*
- *Rezervne kopije moraju biti sigurno pohranjene izvan lokacije ili u zasebnom skladištu u oblaku kako bi se spriječio gubitak od lokalnih incidenata.*
- *Potpune sigurnosne kopije se izvode sedmično, sa inkrementalnim rezervnim kopijama dnevno (ili češće za visoko osjetljive podatke).*
- *Provjere integriteta rezervne kopije i restauracije testova moraju se obavljati mjesečno kako bi se osiguralo da se podaci mogu povratiti.*
- *Zadržavanje: Zadržati najmanje jednu punu sedmicu dnevnih rezervnih kopija na licu mjesta, a mjesečna puna rezervna kopija arhivirana je van lokacije najmanje godinu dana.*
- *Pristup rezervnim podacima je ograničen samo na ovlašteno IT ili upravljačko osoblje.*

Uloge i odgovornosti:

- *IT osoblje mora konfigurirati i pratiti automatizirane sigurnosne kopije prema ovom rasporedu.*
- *Određeni Backup administrator će dokumentirati procedure sigurnosne kopije i provjeriti završetak i integritet rezervne kopije.*
- *Svo osoblje je odgovorno za čuvanje kritičnih radnih datoteka na određenim lokacijama koje su uključene u raspored rezervnih kopija.*

Sprovođenje: Nepoštivanje može rezultirati gubitkom podataka i u skladu s tim će se pozabaviti upravljanjem [ime organizacije].

Dodatak IV: Predložak inventara imovine (primjer)

ID imovine	Ime imovine	Kategorija	Vlasnik/Odjel	Lokacija	Nivo osjetljivosti	Zahtjev za zaštitu	Bilješke
A001	Donor Database	Softver/Podaci	Direktor programa	Na licu mjesta	Visoko	Šifrirano, zaštićeno lozinkom	Sadrži PII donatora
A002	Finansijski server	Hardver/Server	IT Department	Data Center	Visoko	Redovne sigurnosne kopije, 2FA za pristup	Podržava računovodstveni softver
A003	Laptops	Hardver/Device	Razno osoblje	Ured/Field	Srednji	Prisilna šifriranje diska, lozinka	Svaki uređaj ima identifikacionu oznaku
A004	Web stranica	Softver	Komunikacije	Cloud-hosted	Srednji	HTTPS omogućen, ažurirani CMS	Web stranica koja se odnosi na javnost
A005	CRM softver	Softver	Menadžer podataka	Oblak	Visoko	Pristup zasnovan na ulogama, dnevne rezervne kopije	Informacije o korisniku traga

(Napomena: 'Nivo osjetljivosti' može biti nizak/srednji/visok. 'Pretresena zaštita' opisuje sigurnosne mjere za svaku imovinu.)

Dodatak V: Jednostavan predložak matrice rizika (primjer)

	Uticaj: Nizak (1)	**Uticaj: Srednji (2)**	**Uticaj: Visok (3)**
Vjerovatnoća: Visoka (3)	Visok rizik (3×1)	Kritički rizik (3×2)	Kritički rizik (3×3)
Vjerovatnoća: Srednji (2)	Srednji rizik (2×1)	Visok rizik (2×2)	Kritički rizik (2×3)
Vjerovatnoća: Niska (1)	Nizak rizik (1×1)	Srednji rizik (1×2)	Visok rizik (1×3)

- **Nivoi rizika:** Izračunajte rizik množenjem vjerovatnoće i rezultata udara. Na primjer, scenario ocijenjen Likeliod=3 (visok) i Impact=2 (srednji) daje ocjenu rizika od 6 (kritični rizik).
- Iskoristite ovu matricu da prvo date prioritet rješavanju scenarija većeg rizika (kritično > visoko > srednje > nisko).

ZAKLJUČAK

Digitalna sigurnost nije jednokratni projekat ili kutija koju treba provjeriti – to je OCSOing obaveza. Dok zaključujemo ovu e-knjigu, želimo da reafirmišemo centralnu lekciju koja je odjeknula kroz svako poglavlje: očuvanje naših organizacija civilnog društva na sigurnom na internetu zahtijeva kontinuiranu pažnju, adaptaciju i brigu. Pejzaž sajber prijetnji o kojem smo razgovarali na početku se stalno razvija, a napadači svakodnevno traže nove načine za probijanje odbrane. Ono što danas osiguramo može biti testirano novom taktikom sutra.

Ova realnost znači da digitalna sigurnost mora dugo ostati na našem radaru, što je sastavni dio našeg planiranja i operacija kao budžetiranja ili upravljanja programom. Ne možemo sebi priuštiti da sajber sigurnost tretiramo kao naknadnu misao; nego bi to trebalo postati uobičajeni dio načina na koji radimo. Ulozi su jednostavno previsoki – kada jedan uspješan hak može razotkriti osjetljive podatke korisnika ili izbaciti iz kolosijeka kampanju zagovaranja, budnost u digitalnoj sigurnosti je dio i paket ispunjenja naših misija. Znanje i strategije koje ste stekli iz ove e-knjige su osnova za izgradnju. Ubuduće, sigurnost će značiti redovno ponovno razmatranje ovih tema, ažuriranje vaše prakse kako se pojavljuju nove prijetnje (i rješenja) i njegovanje okruženja u kojem je učenje o sigurnosti kontinuirani proces. Ukratko, rad digitalne sigurnosti nikada nije "završen,", ali nije ni nepremostiv. Sa svakim korakom koji preduzmete da ojačate svoju organizaciju's cyber odbrane, doprinosite otpornijem civilnom društvu.

Održavanje sigurnosti postalo lako: Jedan ključni zaključak je da sigurnost ne mora biti previše komplikovana. Često se radi o dosljednom činjenju jednostavnih stvari. Koristite jake, jedinstvene lozinke (i upravitelj lozinki). Obavještavajte svoj softver. Razmislite dvaput prije nego kliknete na neočekivane veze. Redovno podržavate svoje podatke. Ove osnovne prakse, kada su ukorijenjene, nose veliki postotak prijetnji. Kao što smo vidjeli, mnogi napadi uspijevaju zbog zanemarenih osnova –, tako da brigom o njima zatvorite zajednička vrata koja napadači iskorištavaju.

Prilagođavanje novim izazovima: Digitalni svijet će se nastaviti mijenjati. Prije pet godina, ransomware nije bio tako dominantan; danas je to najveća prijetnja. U budućnosti bismo se mogli boriti s napadima na alate umjetne inteligencije ili sofisticiranijim deepfake

phishingom. Vaš OCD bi trebao ostati prilagodljiv i nastaviti učiti. Pretplatite se na odgovarajući sigurnosni feed ili se pridružite zajednici tamo gdje se raspravlja o novim prijetnjama – na taj način, dobijate rano upozorenje o novim pitanjima. Razmotrite periodičnu obuku za osvježavanje ili nove module za osoblje kada nešto značajno promijeni (na primjer, ako mobilni zlonamjerni softver poraste, uradite posebnu sesiju o tome). Prihvatite način razmišljanja kontinuiranog poboljšanja, tretirajući svaki skoro promašaj ili incident kao priliku za učenje za dalje jačanje odbrane.

Mudro dodjela resursa: Sigurnost je ulaganje u održivost vaše organizacije. Može zahtijevati određeni budžet (za bolju opremu, softver ili vrijeme obuke) i pažnju upravljanja. Ali kao što je pokazano, trošak neosiguranja (kršenja, zastoj, izgubljeno povjerenje) je daleko veći. Plan sigurnosti u vašoj dugoročnoj strategiji – npr. uključuje liniju grantova za ažuriranja tehnologije ili obuku. Usluge bez poluge ili snižene za OCD (postoje mnoge, od besplatnog Google Workspacea do doniranih zaštitnih zidova) kao što je objašnjeno u Poglavlju 6. Također, razmislite o određivanju osobe sigurnosne tačke (čak i ako ne i s punim radnim vremenom) koja prati sigurnosne zadatke i razvoje – da neko odgovara osigurava da ne propadne kroz pukotine.

Podrška rukovodstva: Održiva sigurnost treba podršku rukovodstva. Kada lideri daju prioritet sigurnosti – modeliranjem dobrih praksi i dodjeljivanjem resursa –, to šalje jasnu poruku da je to važno za sve. Također se suprotstavlja bilo kakvom odbijanju (kao “, da li zaista moramo da se zamaramo ovim?”): ako se direktor prijavljuje sa 2FA i prisustvuje istim treninzima, to legitimira trud. Dakle, osigurajte da je vaš menadžerski tim u potpunosti na brodu, pa čak i da se zalaže za sigurnosne inicijative.

Angažirajte svoj cijeli tim**:** Sigurna budućnost zavisi od toga da li će svi igrati ulogu. Od najnovijeg pripravnika do članova odbora, svaka osoba ima ulogu u lancu. Održavajte sigurnost inkluzivnom: potaknite pitanja, ne tvrdite greške u stidu, budnost nagrade. Neke organizacije uključuju sigurnosnu kompetenciju u pregledima performansi ili opisima poslova, naglašavajući da je to očekivanje za sve uloge. Osnažujući osoblje – dajući im znanje i alate –, u suštini ste uzgajali ljudski zaštitni zid oko svog CSO-a. Kao što jedna izreka kaže, “sigurnosna svijest korisnika je najjeftiniji i najefikasniji zaštitni zid koji možete imati.”

Gledati unaprijed s optimizmom: Može biti lako osjećati se zastrašeno sajber prijetnjama, ali zapamtite da znanje i priprema snažno naginju ravnotežu u vašu korist. Mnogi OCD širom svijeta, čak i oni s nedostatkom sredstava, uspješno su se branili proaktivnim i ujedinjenim. Čitajući ovu e-knjigu i implementirajući njene smjernice, poduzeli ste važan korak ka osiguravanju svoje digitalna budućnost organizacije. To je putovanje –, doći će do neravnina i eventualno incidenata –, ali svaki korak koji sada preduzmete smanjuje utjecaj njih i ubrzava vaš oporavak.

U svijetu u kojem je civilno društvo ponekad posebno na meti sajber napada, vaša posvećenost digitalnoj sigurnosti je također posvećenost vašoj stvari i ljudima kojima služite. To znači da se vaš važan rad može nastaviti bez izbacivanja iz kolosijeka zbog poremećaja koji se mogu spriječiti. To znači da povjerenje koje ljudi stavljaju u vas – za rukovanje svojim podacima ili pojačavanje njihovih glasova – je dobro utemeljen.

Kao što zaključimo, hajde da nadoknadimo nekoliko dugoročnih sigurnosnih navika za uzgoj:

- *Redovno ponovo pogledajte svoju procjenu rizika i ažurirajte svoj sigurnosni plan (barem godišnje ili kada se dogode velike promjene).*
- *Nastavite učiti – pohađajte taj webinar, pročitajte taj vodič, podijelite uvide sa vršnjacima.*
- *Ostanite povezani – ne izolujte svoje sigurnosne napore; budite dio zajednice koja uči i brani se zajedno.*
- *Budite spremni – održavajte svoj plan odgovora na incidente i testirajte ga povremeno kako bi bio spreman ako je potrebno.*
- *Ostanite oprezni –, ali ne i uplašeni. Uz dobre prakse, možete biti sigurni i mirni, ne zabrinuti zbog digitalnih prijetnji.*

Ka sigurnoj budućnosti: Učinivši digitalnu sigurnost sastavnim dijelom svakodnevnih operacija i kulture vašeg OCD-a, u dobroj ste poziciji da se suočite s budućnošću. Izazovi će se nesumnjivo pojaviti, ali imate alate, znanje i podršku da ih prevaziđete. Čineći to, štitite ne samo svoju organizaciju, već i doprinosite sigurnijem digitalnom okruženju za šire civilno društvo.

Kretanje naprijed, posvetiti se kontinuiranom poboljšanju. Proslavite svoje sigurnosne pobjede (čak i male poput “niko nije pao na phishing u ovoj četvrtini!” ili “uspješno smo obnovili podatke

iz backup-a nakon manjeg serverskog crash"). Naučite iz bilo kakvih neuspjeha. I uvijek zapamtite zašto: siguran OCD može bolje ispuniti svoju misiju i ostvariti pozitivan utjecaj bez prekida.

Otpornost na izgradnju je još jedna tema koju smo naglasili i zaslužuje da bude ponovo pod stresom ovdje na kraju. Otpornost znači ne samo pokušaj sprječavanja napada već i osiguravanje vašeg organizacija se može oporaviti ako nešto krene po zlu. On se bavi rezervnim kopijama kako bi napad ransomware-a ne bi osakatio vaše operacije, o planovima odgovora kako bi se phishing incident mogao obuzdati i naučiti od njega, te o kultiviranju organizacijskog načina razmišljanja koji na neuspjehe gleda kao na prilike za poboljšanje. Dok nastavljate sa svojim radom, zapamtite da svaki izazov može učiniti vas jačim ako se susretnete s pripremom i razmišljanjem. Ako dođe do sigurnosnog incidenta, koristite ga kao iskustvo učenja da poboljšate svoju politiku i obuku. Proslavite napredak koji ste've postigli – na primjer, okrećući taj "80% organizacija bez sigurnosnog plana" statistiku na svoju glavu u svom kontekstu postavljanjem snažnog plana. I nastavi da obrazuješ sebe I svoj tim. Polje digitalne sigurnosti se brzo razvija, ali postoji više resursa nego ikad (od kojih smo mnogi naveli u poglavlju 7 i dodacima) kako bismo vas obavještavali. Razmislite o periodičnim radionicama osvježavanja, pretplatite se na upozorenja ili biltene o sajber sigurnosti za neprofitne organizacije i ohrabrite mlađe osoblje ili volontere s IT interesima da preuzmu uloge "šampiona digitalne sigurnosti" unutar vaše organizacije. Kontinuirano učenje je kamen temeljac otpornosti. Održava vas okretnim i spremnim da upoznate sve što vam digitalni svijet baci.

Gledajući unaprijed, ostajemo optimistični i usmjereni naprijed prema budućnosti civilnog društva u digitalnom dobu. Da, izazovi su značajni – sajber napadi postaju sve sofisticiraniji i moramo ostati na nogama. Ali napredak postignut čak iu proteklih nekoliko godina je ohrabrujući. Sve više organizacija se budi do važnosti digitalne sigurnosti, a strukture podrške polako ali sigurno jačaju. Vidimo razvoj alata i usluga prilagođenih neprofitnim organizacijama, povećanu svijest među donatorima i institucijama o finansiranju potreba za sajber bezbjednošću i veću globalnu pažnju na koncept "digitalne otpornosti" za zajednice. Svako poglavlje ove e-knjige ne samo da je ponudilo smjernice upozorenja, već je i naglasilo mogućnosti – da pretvori tehnologiju u našu korist, da inovira u tome kako se štitimo i

oblikujemo digitalno okruženje koje podržava naše vrijednosti. Kao što smo primijetili, sajber prijetnje će nastaviti da se razvijaju, ali i naša odbrana. Premošćivanjem preostalih praznina u znanju i kapacitetu, jačanjem partnerstava i održavanjem sajber sigurnosti a prioritet za one kojima je najpotrebniji, možemo stvoriti sigurniji digitalni ekosistem gdje civilno društvo može nastaviti svoj kritični rad bez straha.

Na kraju, želimo da vam ostavimo osnažujuću misao: svaki napor koji uložite u digitalnu sigurnost je ulaganje u slobodu i integritet vašeg rada i ljude kojima služite. Svaka nova politika lozinki, svaka šifrirana baza podataka, svaka sesija obuke osoblja –, sve se zbrajaju u jači štit koji štiti ljudska prava, socijalnu pravdu i inicijative za dobrobit zajednice širom svijeta. Činjenica da ste pročitali ovu e-knjigu i bavili se ovim temama pozitivan je korak ka sigurnijoj budućnosti. Ohrabrujemo vas da ovu posvećenost prenesete naprijed. Podijelite ono što ste’ve naučili sa kolegama i partnerskim organizacijama. Održavajte razgovor o digitalnoj sigurnosti živim na svojim strateškim sastancima i sesijama planiranja. Zagovarajte za resurse i podršku koja vam je potrebna – bilo da je to’ finansiranje bolje infrastrukture ili jednostavno vrijeme dodijeljeno osoblju da nauči i implementira sigurnosne mjere – jer je digitalna sigurnost vrijedna toga. Stav koji gleda na budućnost je da ugrađivanjem sigurnosti u naš svakodnevni rad činimo više od samo zaštite naših organizacija; omogućavamo im da napreduju. Sigurna organizacija civilnog društva može govoriti glasnije, djelovati hrabrije i doseći dalje, znajući da se njen glas ne može lako ušutkati digitalnim prijetnjama.

Jedan od najhrabrijih uvida iz projekta KA220 i ove e-knjige je da nismo sami u suočavanju s ovim izazovima. U stvari, saradnja je jedna od naših najjačih sredstava. Ako postoji jedna poruka koju treba prenijeti, to je da smo zajedno sigurniji. Sajber prijetnje se često mogu osjećati izolovano –, mala neprofitna organizacija može se osjećati nadmašeno sofisticiranom hakeru –, ali kolektivna moć civilnog društva, koje radi zajedno, može nagnuti ravnotežu. Tokom ovog projekta, inspirisani smo primjerima organizacija koje se udružuju kako bi podijelile stručnost, mrežama digitalnih volontera koji su im pružili ruku i partnerstvima koja su se formirala preko granica kako bi se pozabavila zajedničkim sigurnosnim pitanjima. Put do digitalne sigurnosti nije usamljen; to je zajedničko putovanje. Otvorenom komunikacijom o prijetnjama i incidentima, dijeljenjem alata i priča o uspjehu, te podržavanjem jedni drugih kroz

hitne slučajeve, organizacije civilnog društva pojačavaju svoje odbrambene sposobnosti. Štaviše, široka saradnja izvan neprofitnog sektora je neophodna. Moramo nastaviti sa sklapanjem partnerstava sa saveznicima u vladi, akademskoj zajednici i tehnološkoj industriji koji su posvećeni zaštiti otvorenog i sigurnog interneta koji civilno društvo oslanja se na. Kao što su stručnjaci i globalni sajber lideri primijetili, odbrana rizičnih grupa efektivno "zahtijeva ulaganje u rješenja za kibernetičku sigurnost, saradnju među dionicima i inovativne modele finansiranja za dugoročnu otpornost". Nema nijednog organizacija – bez obzira na to koliko – ima dobre resurse može se pozabaviti svim aspektima samo digitalne sigurnosti. Biće potrebna zajednica prakse, koja obuhvata različite sektore i stručnost, kako bi se osiguralo da zaštitne mjere budu dostupne, efikasne i održive dugoročno. Ohrabrujem vas da potražite ove saradnje: pridružite se sigurnosnim forumima i koalicijama, uključite se u inicijative koje nude pomoć u sajber sigurnosti OCD-ovima i ne ustručavate se obratiti kolegama za pomoć ili ponuditi svoju. Jačanjem ovih veza, mi stvaramo ujedinjeni front koji može brzo odgovoriti na prijetnje I spriječiti da mala pitanja postanu velike krize.

Hvala vam što ste dio ovog putovanja za razvoj digitalne sigurnosne infrastrukture kroz civilno društvo. Zaključak ovog udžbenika nije kraj, već početak – početne tačke novih inicijativa, razgovora i saradnje koje će se nastaviti izvan ovih stranica. Ostanite radoznali, budite na oprezu i ostanite ujedinjeni. Zajedno ćemo izgraditi digitalno okruženje u kojem civilno društvo nije samo sigurno već i osnaženo da iskoristi tehnologiju u odbrani uzroka koje nam je drago. Sa otpornošću, saradnjom i kontinuiranim učenjem kao našim vodičima, idemo naprijed u budućnost u kojoj organizacije poput vaše mogu samouvjereno prihvatiti inovacije i potaknuti društvene promjene, podržane snažnim temeljima digitalne sigurnosti. Neka's nastavi ovaj važan rad – naše zajednice računaju na njega, a alati i saveznici koji su nam potrebni su na dohvat ruke. Ovdje se poziva na sigurnije, jače i osnaženije civilno društvo u digitalnoj eri.

Praktični vodič za digitalnu transformaciju i nastavni plan i program o jačanju digitalne sigurnosti u civilnom društvu kreiran je sa jednom jasnom svrhom: da digitalnu sigurnost učini ostvarivom, razumljivom i djelotvoran za svakog organizacija, bez obzira na veličinu ili tehničke kapacitete. Dok idete naprijed, nadamo se da ovaj vodič služi ne samo kao resurs već i kao pratilac na vašem putu ka jačim, sigurnijim digitalnim praksama.

Digitalna otpornost raste korak po korak, kroz svijest, saradnju i konzistentnost. Integracijom ovih praksi u svoj svakodnevni rad, ne samo da štitite podatke i komunikaciju, već i branite ljudska prava, povjerenje i demokratske vrijednosti u digitalnom dobu.

Ostanite svjesni. Ostanite otporni. Ostani siguran.