Co-funded by
the European Union

SIVILSAMFUNNSINITIATIVER STYRKET MED INFORMASJONS- OG DATASIKKERHET

PRAKTISK VEILEDNING FOR DIGITAL OMVANDLING OG PENSUM FOR STYRKING AV DIGITAL SIKKERHET I SIVILSAMFUNNET

PRAKTISK VEILEDNING FOR DIGITAL OMVANDLING OG PENSUM FOR STYRKING AV DIGITAL SIKKERHET I SIVILSAMFUNNET

Ankara, 2026

Denne studien ble utført innenfor rammen av prosjektet «SIVILSAMFUNNSINITIATIVER STYRKET MED INFORMASJONS- OG DATASIKKERHET» (2023-1-TR01-KA220-YOU-000161230), støttet av det tyrkiske nasjonale byrået og Europakommisjonen under Erasmus+-programmet. Innholdet som presenteres her gjenspeiler forfatterens synspunkter, og verken Europakommisjonen eller det tyrkiske nasjonale byrået kan holdes ansvarlige for disse synspunktene.

Co-funded by
the European Union

2026

Akademisk rådgiver: Erman Akıllı

Omslagdesign og layout:

Redaktører: Sibel Koru

Zeyneb Güşta Arık

Tekstrevisjoner: Cenay Babaoğlu

Dato: Ankara, 2026

SETA

I dagens hypertilkoblede verden opererer sivilsamfunnsorganisasjoner (CSO-er), alt fra ikke-statlige organisasjoner og påvirkningsgrupper til uavhengige mediekanaler og fellesskapsnettverk, på en stadig mer kompleks digital frontlinje. Selv om digitale verktøy har utvidet sivilsamfunnets rekkevidde, effektivitet og innvirkning, har de samtidig utsatt organisasjoner for økte cybersikkerhetsrisikoer. Etter hvert som sivilsamfunnet blir mer avhengig av digital teknologi, blir det også mer sårbart digitalt.

Over hele Europa og utover dets grenser anerkjennes sivilsamfunnsorganisasjoner i økende grad som høyrisikoaktører i det digitale økosystemet. Cybertrusler rettet mot sivilsamfunnet spenner nå fra phishing, ransomware, spyware og tjenestenektangrep til sofistikert statssponset overvåking som tar sikte på å dempe avvikende meninger og undergrave demokratiske verdier. For organisasjoner som ofte opererer med begrenset teknisk kapasitet, men likevel håndterer sensitive personopplysninger og organisasjonsdata, utgjør digital usikkerhet ikke bare operasjonelle risikoer, men også eksistensielle risikoer.

I denne sammenhengen er digital sikkerhet ikke lenger en rent teknisk sak. Det er oppdragskritisk. Sivilsamfunnsorganisasjoners evne til å operere trygt på nettet er uatskillelig fra deres evne til å beskytte ytringsfriheten, åpenheten, ansvarligheten og fellesskapene de betjener. For å styrke den digitale sikkerheten i sivilsamfunnet kreves det derfor mer enn tekniske ad hoc-løsninger. Det krever strukturert læring, strategisk planlegging og praktisk veiledning som kan implementeres i virkelige organisasjonsmiljøer.

Som svar på dette behovet ble KA220 Erasmus+-prosjektet «Civilsamfunnsinitiativer styrket med informasjons- og datasikkerhet» igangsatt som en samarbeidsbasert, flerlandsinnsats for å forbedre kapasiteten til organisasjoner i sivilsamfunnet innen digital sikkerhet. Et av de sentrale resultatene av dette prosjektet er denne publikasjonen, som med vilje samler to komplementære funksjoner i én og samme bok.

Denne boken er utformet som både en læreplan og en praktisk veiledning.
På den ene siden fungerer den som et strukturert læreplan for digital sikkerhet for sivilsamfunnet, og tilbyr en sammenhengende læringsvei som bygger opp kunnskap trinnvis – fra å forstå det digitale trussellandskapet til å utvikle organisasjonspolicyer og hendelsesresponsmekanismer. Den læreplanorienterte strukturen gjør den egnet for bruk i opplæring, workshopper, kapasitetsbyggende programmer og opplæring av instruktører i ulike nasjonale kontekster.

På den annen side fungerer boken som en praktisk veiledning som gir konkrete, handlingsrettede retningslinjer som organisasjoner kan anvende direkte i den daglige driften. I stedet for å holde seg på teorinivå, omdanner den cybersikkerhetsprinsipper til praktiske trinn, sjekklister, eksempler og beslutningsrammer som er tilpasset virkeligheten til sivilsamfunnsorganisasjoner og gressrotsinitiativer som opererer med begrensede ressurser.

Ved å kombinere disse to dimensjonene bygger boken en bro over et kritisk gap mellom læring og implementering. Den gjør det mulig for leserne å forstå ikke bare *hvorfor* digital sikkerhet er viktig, men også *hvordan* de kan iverksette den i egne organisasjoner. Lesere kan tilnærme seg boken sekvensielt som et pensum, eller selektivt som en referanseveiledning som tar for seg spesifikke utfordringer som å sikre kommunikasjon, beskytte data, vurdere risikoer eller bygge en intern kultur for digital sikkerhet.

Publikasjonen er skrevet i en tilgjengelig, men likevel akademisk forankret stil, og bygger på prosjektbasert erfaring, innsikt fra feltet og etablert beste praksis innen cybersikkerhet og kapasitetsbygging i sivilsamfunnet. Den modulære strukturen gjør det mulig å tilpasse den til ulike organisasjonsbehov, tekniske nivåer og nasjonale regelverk.

Til syvende og sist tar dette kombinerte pensumet og den kombinerte veiledningen sikte på å gi sivilsamfunnsorganisasjoner muligheten til å ta eierskap over den digitale sikkerheten sin. Ved å fremme både kunnskap og praktisk kompetanse støtter den sivilsamfunnsorganisasjoner i å styrke sin motstandskraft, beskytte sin digitale infrastruktur og fortsette sitt viktige arbeid med større tillit og bærekraft i et stadig mer omstridt digitalt rom.

SETA, Ankara/Tyrkia

INNHOLDSFORTEGNELSE:

1.1 PROSJEKTMÅL:

«Civilsamfunnsinitiativer styrket med informasjons- og datasikkerhet» er et KA220 Erasmus+-prosjekt koordinert av SETA (Tyrkia) og gjennomført i samarbeid med partnerorganisasjoner fra Nord-Makedonia, Norge, Bosnia-Hercegovina, Belgia og Tyrkia. Prosjektet ble finansiert av EU-kommisjonen gjennom det tyrkiske nasjonale byrået og ble utformet for å håndtere de økende utfordringene som organisasjoner i sivilsamfunnet står overfor i et stadig mer digitalisert miljø.

Prosjektets primære mål var å forbedre digital kompetanse, bevissthet om cybersikkerhet og databeskyttelseskapasitet i sivilsamfunnet, samtidig som man fremmet inkludering, mangfold og lik tilgang til digitale ferdigheter. Gjennom hele gjennomføringen støttet prosjektet både enkeltpersoner og institusjoner i å navigere i digitale transformasjonsprosesser og i å styrke sin motstandskraft mot cybertrusler, feilinformasjon og desinformasjon.

Innenfor denne rammen produserte prosjektet en rekke betydningsfulle intellektuelle og praktiske resultater. Disse omfatter en omfattende **læreplan for digital sikkerhet for sivilsamfunnet,** opplæringsmoduler for digitale ferdigheter og cybersikkerhet, som sikrer at digitale transformasjonsprosesser er tilgjengelige og inkluderende. I tillegg ble det utarbeidet en **praktisk veiledning for digital transformasjon** for å hjelpe sivilsamfunnsorganisasjoner med å planlegge, iverksette og opprettholde effektive strategier for digital transformasjon.

Videre utviklet prosjektet et programvarebasert nettbasert **testsenter for digital sikkerhet for organisasjoner i sivilsamfunnet** for å evaluere hvor beredte de er på cybersikkerhet. Plattformen gjør det mulig for sivilsamfunnsorganisasjoner å vurdere det digitale sikkerhetsnivået sitt, herunder aspekter som databeskyttelsespraksis, systemsikkerhetskonfigurasjoner og sikker bruk av nettbaserte verktøy (f.eks. domenestrukturer, HTTPS-bruk og grunnleggende sikkerhetstiltak for digital infrastruktur). Gjennom dette verktøyet kan organisasjoner identifisere sårbarheter, øke bevisstheten om eksisterende risikoer og støtte evidensbaserte prosesser for kapasitetsbygging og forbedring innen digital sikkerhet.

Utover de pedagogiske resultatene genererte prosjektet også bevisstgjøringssmateriale og -kampanjer med fokus på trykk og ansvarlig digital praksis. Videre lyktes det med å etablere et

robust internasjonalt samarbeidsnettverk mellom partnerlandene, og la grunnlaget for langsiktig kapasitetsbygging, kunnskapsutveksling og vedvarende samarbeid innen digital sikkerhet for sivilsamfunnet.

1.2 PROSJEKTPARTNERE:

STIFTELSEN FOR POLITISK, ØKONOMISK OG SAMFUNNSFAGLIG FORSKNING, SETA (KOORDINATOR)

Stiftelsen for politisk, økonomisk og sosial forskning (SETA) er en ideell tenketank som fokuserer på å utarbeide nøyaktige og oppdaterte analyser av nasjonale, regionale og internasjonale spørsmål. Målet er å informere beslutningstakere og allmennheten om politisk, økonomisk, sosial og kulturell utvikling i en historisk og kulturell kontekst. Som en institusjon for forskning og politikanbefaling fremmer SETA internasjonal dialog og bringer ulike perspektiver sammen gjennom vitenskapelige standarder. Det bidrar til informert beslutningstaking hos myndigheter, sivilsamfunnet og bedriftsledere gjennom forskningsrapporter, publikasjoner, konferanser og politiske anbefalinger. SETA tar i bruk en tverrfaglig tilnærming som anerkjenner den innbyrdes avhengigheten mellom politiske, økonomiske og sosiokulturelle spørsmål, og søker å fremme en visjon forankret i fred, rettferdighet, likestilling og rettsstatsprinsippet. Oppdraget er å berike strategiske debatter og gi uavhengig, autoritativ innsikt til beslutningstakere i både offentlig og privat sektor.

STIFTELSEN FOR POLITISK, ØKONOMISK OG SOSIAL FORSKNING, SETA BRUSSEL

SETA Foundation for Political, Economic, and Social Research er et ideelt forskningsinstitutt med fokus på innovative studier knyttet til nasjonale, regionale og internasjonale spørsmål, og har base i Brussel. Målet er å produsere nøyaktig kunnskap og analyser innen politikk, økonomi og samfunn, samtidig som beslutningstakere og allmennheten informeres om utviklingen av politiske, økonomiske, sosiale og kulturelle forhold. Det fremmer internasjonal dialog ved å bringe ulike perspektiver sammen gjennom forskningsrapporter, publikasjoner, konferanser og politiske anbefalinger. Stiftelsen har som mål å støtte informert beslutningstaking i Tyrkia ved å gi ledere i både offentlig og privat sektor autoritative opplysninger og analyser. SETAs tverrfaglige forskningstilnærming tar for seg den innbyrdes avhengigheten mellom politiske, økonomiske og sosiokulturelle spørsmål, og streber etter en visjon basert på fred, rettferdighet, likestilling og rettsstatsprinsippet.

ANKA – FORBUND FOR FREMTID OG INNOVASJON

ANKA er en innovativ og dynamisk ikke-statlig organisasjon (frivillig organisasjon) med base i Istanbul. Organisasjonen ble etablert i mai 2019 og fokuserer på å forbedre enkeltpersoners mentale, fysiske og økonomiske velvære ved å tilby alternative sportsaktiviteter, opplæring, initiativer og muligheter. ANKA har som mål å integrere teknologi og utdanning og tilby løsninger som skaper merverdi for enkeltpersoner og samfunnet. Organisasjonen har kompetanse innen utvikling av mobilapplikasjoner, kunstig intelligens, webteknologier, prosjektledelse og 3D-modellering. Organisasjonens medlemmer kommer fra ulike yrkesbakgrunner, blant annet entreprenørskap, programvare, teknologi, helse og utdanning. I tillegg organiserer ANKA pedagogiske, kulturelle og sosiale aktiviteter for å engasjere ungdom og fremme en aktiv og sunn livsstil. Organisasjonen streber etter å kontinuerlig utvikle ferdighetene sine i programvaresektoren og bidra til livslange læringsprosesser gjennom innovative teknologiske løsninger.

BOSNISK REPRESENTATIV FORENING FOR VERDIFULLE MULIGHETER (BRAVO)

Bosnian Representative Association for Valuable Opportunities (BRAVO) er en dynamisk ideell organisasjon med base i Bosnia-Hercegovina, som fokuserer på å styrke enkeltpersoner og lokalsamfunn gjennom utdanning, kompetanseutvikling og kapasitetsbygging. Organisasjonens oppdrag legger vekt på sosial inkludering, kulturell utveksling og bærekraftig utvikling. BRAVO er virksom i ulike sektorer, inkludert styrking av ungdom, miljøbevissthet, entreprenørskap og teknologi. Organisasjonen har et dedikert team av betalte medarbeidere og frivillige som samarbeider om en rekke prosjekter. BRAVO har organisert ungdomsutvekslingsprogrammer for å fremme tverrkulturell forståelse og personlig vekst, samtidig som de støtter miljømessig bærekraft gjennom innovative prosjekter. Organisasjonen hjelper vordende gründere med veiledning og ressurser, med fokus på sosial påvirkning. I tillegg tilbyr BRAVO workshopper i digitale ferdigheter, for eksempel programmering og webutvikling, og hjelper enkeltpersoner med å forbedre sin personlige og profesjonelle vekst innen teknologi.

TTB

TTB er en ikke-statlig organisasjon med base i Norge, som er opptatt av å tilby utdanning og opplæring i teknologi og digitale ferdigheter for å fremme en bærekraftig fremtid. TTB ble etablert 6. oktober 2019 av studenter i Trondheim, og har som mål å øke ungdommens deltakelse i samfunnet ved å tilby muligheter til å tilegne seg kunnskap og nyttige ferdigheter. Med et team på 15 betalte medarbeidere og en rekke frivillige gjennomfører TTB prosjekter innen utdanning, miljø og entreprenørskap. Organisasjonen fokuserer på digital innovasjon, ungdomsarbeid og integrering av digitale verktøy. Sentrale aktiviteter omfatter opplæring i digitale ferdigheter, miljøinitiativer og støtte til gründere, særlig innen teknologi og bærekraft. TTB verdsetter åpenhet, samarbeid, mot og omsorg, og fremmer et bærekraftig, etisk og samfunnsansvarlig miljø. Organisasjonen deltar i både regionalt og internasjonalt samarbeid.

TÜRKIYE UNGDOMSSTIFTELSE (TÜGVA)

Türkiye Youth Foundation (TÜGVA) ble grunnlagt i 2014 og er en av Tyrkias største sivilsamfunnsorganisasjoner, med et team på over 100 fagfolk og 300 000 frivillige. Den tilbyr robotkodeverksteder i 39 byer og administrerer 42 sovesaler. Stiftelsen opererer med 10 koordinatorer på ulike områder, inkludert idrett, kvinners rettigheter, entreprenørskap, media, utdanning, kultur og karriereutvikling. Hovedoppgaven er å støtte ungdommens helhetlige utvikling, med fokus på både fysisk og psykisk velvære, særlig i Tyrkia. Stiftelsen har som mål å gi unge mennesker mulighet til å bli innovative, produktive og verdifulle medlemmer av samfunnet. Med mer enn 200 nasjonale og internasjonale prosjekter fullført, er visjonen å dyrke generasjoner som er i stand til å gjenoppbygge og fremme sivilisasjonen gjennom kontinuerlig selvforbedring og kulturell berikelse.

ZDRUŽENIE NA GRAGJANI MAKEDONSKA ASOCIJACIJA ZA ČOVEČKI RESURSI SKOPJE (MHRA)

Macedonian Human Resources Association (MHRA) er en ideell, ikke-statlig nasjonal organisasjon med fokus på kompetanseutvikling av arbeidsstyrken, fremming av menneskelig kapital og standardisering av uformell utdanning. MHRA har over 120 aktive individuelle medlemmer, hovedsakelig kvinner, og mer enn 600 passive medlemmer fra HR-bransjen, i tillegg til over 60 bedrifter fra både offentlig og privat sektor. Foreningen fungerer som en åpen plattform som integrerer personer på alle karrierestadier, inkludert HR-ledere, konsulenter, ansatte og studenter. Den er involvert i utformingen av retningslinjer knyttet til næringsliv,

utdanning og sosioøkonomiske spørsmål på både nasjonalt og lokalt plan. MHRA har vært offisielt medlem av European Association for People Management (EAPM) siden 2012, og omfavner også frivillig arbeid som en kjerneverdi i lokale og internasjonale initiativer.

2. PRAKTISK VEILEDNING FOR DIGITAL TRANSFORMASJON

2.1 KAPITTEL 1: DIGITAL SIKKERHET FOR CIVILSAMFUNNSORGANISASJONER

Hva er digital sikkerhet?

Digital sikkerhet, også kjent som cybersikkerhet, er praksisen med å beskytte digital informasjon, enheter og andre ressurser mot uautorisert tilgang eller skade. Den omfatter tiltak for å beskytte personopplysninger, kontoer, filer og til og med økonomiske ressurser som lagres eller overføres på nettet. I bunn og grunn tar digital sikkerhet sikte på å sikre informasjonens konfidensialitet, integritet og tilgjengelighet (ofte oppsummert som «CIA-triaden» – **C** onfidentiality, **I** ntegrity, **A** vailability).

Hvorfor er digital sikkerhet viktig?

I dagens hypertilkoblede verden er nesten alle organisasjoner og enkeltpersoner avhengige av digitale systemer. For organisasjoner i sivilsamfunnet og frivillige organisasjoner omfatter denne avhengigheten kommunikasjon med interessenter, håndtering av giverinformasjon og levering av tjenester. Det er avgjørende å beskytte disse digitale aktivitetene. Cyberangrep kan forstyrre driften, lekke sensitive data og skade tilliten givere og lokalsamfunn har til en organisasjon. For eksempel avslørte et datainnbrudd hos Australske Røde Kors i 2016 personopplysningene til over 550 000 blodgivere på grunn av en menneskelig feil (en usikret sikkerhetskopifil). Hendelsen reiste ikke bare spørsmål om organisasjonens datapraksis, men førte også til at giverne mistet tilliten, noe som illustrerer hvordan cyberhendelser kan skade virkelige mennesker og undergrave allmennhetens tillit til en sivilorganisasjons oppdrag.

Det er viktig å merke seg at ideelle organisasjoner i økende grad blir målrettet av nettkriminelle og til og med statsstøttede hackere. En Microsoft-rapport fant at humanitære organisasjoner og menneskerettighetsorganisasjoner var den nest mest utsatte sektoren for cyberangrep fra nasjonalstater, og sto for 31 % av slike angrepsmeldinger i 2025. En studie fra 2023 av ideelle organisasjoner basert i Genève avdekket at 41 % hadde opplevd et cyberangrep de siste årene. Likevel hadde over halvparten av disse organisasjonene ikke noe eget budsjett for cybersikkerhet, og 70 % følte at de manglet ferdigheter og motstandskraft til å reagere på angrep. Disse tallene understreker at digital sikkerhet ikke lenger er valgfritt, men helt nødvendig for sivilsamfunnsorganisasjoner. Uten tilstrekkelige sikkerhetstiltak kan

cyberhendelser stanse kritiske tjenester, kompromittere mottakerdata og true finansieringen ved å skade en organisasjons omdømme.

Videre er digital sikkerhet nært knyttet til fysisk sikkerhet og menneskerettigheter i sivilsamfunnets arbeid. Aktivister, journalister og sivilsamfunnsorganisasjoner utsettes ofte for digitale trusler med sikte på overvåking eller trusler. Et brudd eller et hack kan avsløre sensitiv kommunikasjon eller identiteten til partnere og mottakere, og potensielt sette liv eller levebrød i fare. Derfor er investering i digital sikkerhet en investering i den generelle motstandskraften og påliteligheten til en organisasjons arbeid.

Hva betyr digital sikkerhet for sivilsamfunnsorganisasjoner?

For organisasjoner i sivilsamfunnet betyr *digital sikkerhet* å beskytte informasjonen og teknologien som gjør det mulig for dem å utføre sine sosiale oppdrag. Sivilsamfunnsorganisasjonene innhenter og lagrer rutinemessig sensitive data – fra personopplysninger om støttespillere og ansatte til strategiske planer og forskning. Det er avgjørende å sikre disse opplysningenes konfidensialitet og integritet, slik at de ikke havner i gale hender eller blir tuklet med. For eksempel kan en påvirkningsgruppe ha behov for å sikre kontaktlister over aktivister eller bevis på menneskerettighetsbrudd. Dersom slik informasjon ble lekket eller endret av ondsinnede aktører, kunne det sette enkeltpersoner i fare eller undergrave saken.

Digital sikkerhet for sivilsamfunnsorganisasjoner innebærer også å beskytte den daglige driften. Mange organisasjoner er avhengige av e-post, meldingsapper og skyplattformer for å koordinere aktiviteter. Dersom disse kontoene kompromitteres, kan angripere forstyrre kommunikasjonen eller utgi seg for å være CSO-en. I ett virkelig tilfelle ble e-postsystemet til en veldedig organisasjon hacket gjennom en phishing-e-post med et skadevarevedlegg, noe som førte til et løsepengevirusangrep som krypterte organisasjonens server. Angriperne krevde løsepenger i bytte mot dekrypteringsnøkkelen. Ettersom sivilsamfunnsorganisasjonen hadde nylige sikkerhetskopier av data og valgte å ikke betale, klarte de å gjenopprette de fleste av dataene sine, men omtrent to ukers informasjon gikk tapt for alltid. Denne hendelsen illustrerer både trusselen og viktigheten av beredskap: Uten solide sikkerhetskopier og en beredskapsplan kunne utfallet ha blitt langt verre.

For sivilsamfunnsgrupper som opererer i sensitive politiske miljøer, får digital sikkerhet en ekstra betydning i form av å beskytte sikkerheten til medlemmene og fellesskapene de betjener. Repressive enheter kan bruke cybermidler til å spionere på sivilsamfunnsorganisasjoner eller rette desinformasjon mot dem. Derfor legger digital sikkerhet for organisasjoner i sivilsamfunnet ofte vekt på verktøy som forbedrer personvernet (som kryptering av e-poster og meldinger) og sikre kommunikasjonskanaler for å forhindre overvåking. Som Liberties, en europeisk organisasjon for borgerrettigheter, bemerker: Sivilsamfunnsorganisasjoner som bruker digitale verktøy for aktivisme, står overfor unike trusler og må fremme en kultur for «digitalt selvforsvar» som omfatter mennesker, prosesser og teknologi. I praksis innebærer dette å lære opp ansatte og frivillige i sikkerhetsbevissthet, etablere klare retningslinjer (for eksempel for håndtering av personopplysninger eller bruk av sikre apper) og kontinuerlig oppdatere tekniske beskyttelsestiltak.

Til slutt handler *digital sikkerhet for organisasjoner for sivilsamfunnet* om å opprettholde tillit. Givere og mottakere forventer at organisasjoner er gode forvaltere av informasjon. En cyberhendelse som får mye omtale, kan rokke ved allmenhetens tillit og avskrekke folk fra å engasjere seg eller bidra. Etter Røde Kors' datalekkasje som ble nevnt tidligere, observerte organisasjonen for eksempel en nedgang i blodgiving og måtte arbeide for å gjenoppbygge tilliten. Ved å prioritere digital sikkerhet viser organisasjoner i sivilsamfunnet at de er opptatt av ansvarlighet og personvern, som er kjerneverdier i sivilsamfunnssektoren.

Vanlige digitale trusler og risikoer for sivilsamfunnsorganisasjoner

Civilsamfunnsorganisasjoner står overfor mange av de samme cyberrisikoene som bedrifter og enkeltpersoner, men har ofte færre ressurser til å håndtere dem. Noen vanlige trusler omfatter:

- **Hackere og skadevare:** Angripere kan prøve å infiltrere en sivilsamfunnsorganisasjons nettverk eller enheter for å stjele data eller forstyrre tjenester. Dette kan skje gjennom skadevare (skadelig programvare som virus, spionprogrammer eller løsepengevirus) som leveres via e-postvedlegg, skadelige lenker eller infiserte USB-minnepinner. Løsepengevirus er en spesielt skadelig type skadevare som krypterer filer og krever betaling. Den har rammet organisasjoner av alle størrelser, fra små ideelle

organisasjoner til hele bymyndigheter. Dersom en sivilorganisasjon mangler sterke forsvar mot skadevare og sikkerhetskopier av data, kan et løsepengevareangrep effektivt lamme driften.

- **Phishing og sosial manipulering:** Phishing er en taktikk der angripere sender falske e-poster eller meldinger som virker legitime (for eksempel ved å utgi seg for å være en kollega eller en tjenesteleverandør) for å lure mottakerne til å oppgi passord eller laste ned skadevare. Phishing er en av de mest utbredte truslene og ofte inngangspunktet for større angrep. Civilsamfunnsorganisasjoner har vært mål for phishing-svindel. For eksempel mistet en ideell utdanningsorganisasjon nesten finansiering da angripere forfalsket e-poster for å lure en partner til å sende en betaling til feil bankkonto (en form for «kompromittering av bedrifts-e-post»). Vanlige tegn på phishing inkluderer presserende eller alarmerende språk, forespørsler om sensitiv informasjon eller e-postadresser med små stavefeil. Sosial manipulering kan også skje via telefonsamtaler (vishing) eller tekstmeldinger (smishing) der angriperen utgir seg for å være en pålitelig aktør.
- **Datainnbrudd:** Et datainnbrudd inntreffer når det gis uautorisert tilgang til eller utleveres konfidensiell informasjon. Dette kan skyldes hacking, insidermisbruk eller til og med utilsiktet eksponering. Civilsamfunnsorganisasjoner innehar ofte personopplysninger (f.eks. opplysninger om mottakere, giveres økonomiske opplysninger, helseopplysninger eller opplysninger om rettssaker) som er attraktive for angripere eller som kan lekkes. Som nevnt kan feilkonfigurerte servere eller skylagring utilsiktet lekke data – Røde Kors-hendelsen er ett eksempel. Konsekvensene av et datainnbrudd for en sivilorganisasjon er alvorlige: Det kan føre til identitetstyveri for personene i dataene, krenke personvernlovgivningen og skade organisasjonens omdømme og juridiske stilling. Dessverre kan mange datainnbrudd spores tilbake til menneskelige feil. Faktisk fant en bransjerapport ut at 74 % av datainnbruddene involverer et «menneskelig element», for eksempel feil eller å bli offer for phishing. Dette understreker behovet for opplæring og forsiktig håndtering av data.
- **Uautorisert konto tilgang:** Angripere kan rette seg mot kontoene som CSO-ansatte bruker, for eksempel e-post, sosiale medier eller innsamlingsplattformer. Ved å stjele eller gjette passord (eller bruke lekkede tilgangsopplysninger fra tidligere brudd), kan de kapre disse kontoene. Tegn på at kontoen er kompromittert kan være påloggingsvarsler fra ukjente

steder, nye e-poster eller innlegg som brukeren ikke har opprettet, eller manglende evne til å logge på (passordet er endret av en angriper). Hvis for eksempel en sivilorganisasjons offisielle konto på sosiale medier blir hacket, kan den brukes til å spre falsk informasjon eller svindle sivilorganisasjonens følgere. Bruk av sterke, unike passord og tofaktorautentisering (beskrevet i kapittel 2) er viktige forsvarsmekanismer mot kontoovertakelser.

- **Skjending av nettsteder eller DDoS:** Civilsamfunnsorganisasjoner med offentlige nettsteder kan oppleve skjending (angripere endrer innholdet på nettstedet for å spre meldinger eller propaganda) eller DDoS-angrep (Distributed Denial of Service) som oversvømmer nettstedet med trafikk for å få det til å gå offline. Disse angrepene utføres noen ganger av hacktivister eller motstandere som prøver å dempe stemmen til en sivilsamfunnsorganisasjon. Én sivilsamfunnsorganisasjon oppdaget at nettstedet deres hadde blitt omdirigert til et tredjepartsnettsted etter at angripere utnyttet sårbarheter, og fordi de manglet en nylig sikkerhetskopi, tok det ni måneder å gjenoppbygge nettstedet. Å sikre at nettstedsprogramvaren er oppdatert og sikkerhetskopiert, kan redusere slike risikoer.
- **Insidertrusler og menneskelige feil:** Ikke alle risikoer kommer fra anonyme hackere. Noen ganger kan insidere (ansatte eller frivillige) forårsake sikkerhetshendelser ved et uhell eller med vilje. Dette kan variere fra å miste en usikret bærbar PC som inneholder sensitive filer, til feilkonfigurering av en database, til at en misfornøyd medarbeider laster ned data før avreise. Civilsamfunnsorganisasjoner bør være oppmerksomme på interne tilgangskontroller og prinsippet om minst mulig privilegium (kun gi ansatte tilgang til informasjonen og systemene som er nødvendige for rollen deres). Videre kan fremming av en organisasjonskultur preget av sikkerhet redusere feil – når folk for eksempel forstår hvorfor de ikke bør bruke personlige USB-minnepinner eller må følge prosedyrer for datahåndtering, er det mindre sannsynlig at de utilsiktet skaper sårbarheter.

Oppsummert står sivilsamfunnsorganisasjoner overfor et bredt spekter av digitale trusler – fra daglige svindelforsøk som phishing til mer målrettede angrep fra sofistikerte aktører. Kapittel 2 kommer til å utforske hvordan man kan begynne å beskytte seg mot disse risikoene ved hjelp av grunnleggende beste praksis. Men selv på dette innledende stadiet bør ett sentralt punkt være klart: Å anerkjenne de vanlige risikoene er det første skrittet mot å håndtere dem. Ved å vite

hva som kan gå galt (enten det er et stjålet passord, en virusinfeksjon eller et lekket dokument), blir organisasjoner og enkeltpersoner bedre forberedt på å iverksette tiltak for å forhindre og reagere på disse scenariene.

Hva vil denne boken gi?

Denne veiledningen er utformet for å gi organisasjoner i sivilsamfunnet praktisk kunnskap og ferdigheter for å forbedre den digitale sikkerheten sin. Den tar i bruk en enkel, *praktisk tilnærming* – i likhet med et kurs i åpen universitetsstil – med virkelige eksempler, sjekklister og enkle øvelser for å forsterke læringen. Ved å gå gjennom kapitlene kommer leserne til å:

- **Forstå det grunnleggende:** Du kommer til å lære terminologien og kjernekonseptene innen digital sikkerhet (ta det med ro – vi har tatt med en ordliste i vedlegget som du kan bruke som hurtigreferanse). Fra grunnleggende definisjoner som hva skadevare er, til begreper som tofaktorautentisering – vi avmystifiserer sjargongen slik at du trygt kan kommunisere om sikkerhetsspørsmål.
- **Identifisere risikoene dine:** Boken veileder deg gjennom en vurdering av hvilke spesifikke trusler sivilsamfunnsorganisasjonen din kan stå overfor, og hvilke ressurser som trenger beskyttelse. Gjennom korte spørsmål og scenarier for egenvurdering kan du begynne å kartlegge organisasjonens risikoprofil (kapittel 3).
- **Implementere beste praksis:** Vi gir tydelige, trinnvise råd om umiddelbare tiltak – for eksempel hvordan du oppretter sterke passord, sikrer enhetene dine og bruker internett og e-post på en trygg måte (kapittel 2). Dette er «hurtiggevinstene» innen cybersikkerhet, som reduserer sårbarheten din drastisk når de utføres konsekvent.
- **Utvikle en sikkerhetsplan:** I tillegg til individuelle tips, viser vi deg hvordan du kan samle alt i en enkel, men effektiv digital sikkerhetsplan for sivilsamfunnsorganisasjonen din (kapittel 3). Dette omfatter forslag til retningslinjer, opplæringsplaner for teamet ditt og metoder for sikkerhetskopiering og kryptering av data. Det finnes maler og eksempler som kan hjelpe deg med å utarbeide eller forbedre din egen plan.
- **Lær å bruke sikkerhetsverktøy:** Kapittel 4 introduserer brukervennlige sikkerhetsverktøy og programvare (fra passordbehandlere og antivirusprogrammer til sikre

meldingsapper). Vi legger vekt på verktøy som er enkle å bruke og allment tilgjengelige, selv med et lite budsjett. Hvert verktøy eller hver metode som omtales, kommer med en forklaring på hvorfor det/den er nyttig og hvordan du kommer i gang med det/den.

- **Forbered deg på hendelser:** Til tross for at du gjør ditt beste, kan hendelser inntreffe. I kapittel 5 går vi gjennom hvordan du kan gjenkjenne tegn på en cyberhendelse (for eksempel tegn på at datamaskinen din kan være hacket), og de umiddelbare tiltakene du bør iverksette som respons. Tenk på det som en nødøvelse – å vite hva du skal gjøre kan begrense skaden betydelig. Vi oppfører også ressurser og kontakter for å få hjelp, fordi rettidig støtte kan være avgjørende i en krise.
- **Legg vekt på samarbeid:** Et sentralt tema i denne veiledningen er at du ikke er alene om å håndtere digital sikkerhet. Kapittel 6 omhandler kraften i støtte fra likemenn – hvordan organisasjoner i sivilsamfunnet kan hjelpe hverandre ved å dele advarsler, tips og til og med samle ressurser til opplæring. Det peker også på nettverk og institusjoner (lokale eller internasjonale) som tilbyr støtte, fra tekniske frivillige til hjelpetelefoner.
- **Gi kontekst fra det virkelige liv:** I kapittel 7 presenterer vi casestudier og vanlige fallgruver. Du kommer til å lese korte historier om civilsamfunnsorganisasjoner som har stått overfor cyberutfordringer og hvordan de overvant dem, samt om vanlige feil organisasjoner gjør (slik at du kan unngå dem). Vi inkluderer også noen enkle øvelser for å «teste» sikkerheten din – for eksempel en sjekkliste for å revidere ditt eget kontor eller en phishing-e-postquiz for teamet ditt.

På slutten av denne e-boken bør du føle deg tryggere og mer kompetent i håndteringen av digital sikkerhet. Innholdet er strukturert slik at det er tilgjengelig selv om du ikke har bakgrunn fra IT-bransjen. Hvert kapittel bygger på de foregående, og du kan også henvise til bestemte avsnitt etter behov. Målet er ikke å gjøre deg til en cybersikkerhetsekspert over natten, men å gi deg kunnskap og vaner som vil forbedre beskyttelsen din mot vanlige trusler betydelig. Tenk på det som en førerhåndbok for den digitale veien – du trenger ikke å være mekaniker for å kjøre trygt, men du må lære reglene, bruke riktig utstyr (som sikkerhetsbelter) og være oppmerksom på farer.

I tillegg finner du «Visste du at?»-sidnoter og korte øvelsesoppgaver i alle kapitlene sidnotater og korte øvelsesoppfordringer for å anvende det du har lært. Ta deg tid til å engasjere deg i disse – de er der for å styrke forståelsen din og gjøre læringsopplevelsen mer interaktiv. Etter avsnittet om passord kan du for eksempel bli bedt om å vurdere styrken til et eksempel på et passord, eller etter avsnittet om sikkerhetskopiering kan du bli bedt om å vurdere hvilke data i organisasjonen din som er viktigst å sikkerhetskopiere.

Til syvende og sist tilbyr denne publikasjonen deg et grunnlag innen digital sikkerhet som er skreddersydd for sivilsamfunnskonteksten. Ved å investere tid i disse kapitlene tar du et viktig skritt mot å beskytte organisasjonens arbeid og personene som er knyttet til den. La oss derfor begynne reisen mot en tryggere digital fremtid for sivilsamfunnsorganisasjonen din!

Kapittelsammendrag

Dette kapitlet introduserer den kritiske betydningen av digital sikkerhet for sivilsamfunnsorganisasjoner, og fremhever sårbarheten deres som primære mål for cyberangrep på grunn av deres påvirkningsroller. Det skisserer vanlige trusler som skadevare, nettfisking, datainnbrudd, uautorisert konto tilgang, skade på nettsteder og DDoS-angrep, og legger vekt på hvordan disse påvirker driften, tilliten og sikkerheten. Eksempler fra den virkelige verden, for eksempel datainnbruddet i den australske Røde Kors' databaser i 2016, som avslørte opplysninger om 550 000 givere, og et løsepengevirusangrep mot en veldedig organisasjon, illustrerer konsekvensene av utilstrekkelige forsvar. Kapitlet bemerker at 31 % av nasjonalstatsangrepene i 2025 var rettet mot sivilsamfunnsorganisasjoner, og at 41 % av de ideelle organisasjonene i Genève sto overfor angrep, men at over halvparten mangler budsjetter for cybersikkerhet. Det understrekes at digital sikkerhet er oppdragskritisk, og at den beskytter sensitive data (f.eks. opplysninger om mottakere) og sikrer driftskontinuitet. For sivilsamfunnsorganisasjoner i sensitive politiske miljøer er cybersikkerhet knyttet til fysisk sikkerhet, og forhindrer overvåking eller desinformasjon. Kapitlet taler for en kultur for «digitalt selvforsvar» som kombinerer mennesker, prosesser og teknologi. Det legger grunnlaget for e-boken ved å ramme inn cybersikkerhet som en overlevelsesnødvendighet, og ikke bare et IT-problem, og forbereder leserne på praktiske løsninger i de påfølgende kapitlene. Blant de

viktigste punktene er behovet for bevissthet, beredskap og tillitsbygging for å beskytte sivilsamfunnsorganisasjonenes oppdrag.

Hurtigstart-sjekkliste for cybersikkerhet for organisasjoner i sivilsamfunnet

Denne sjekklisten inneholder enkle, umiddelbare tiltak for å forbedre organisasjonens digitale sikkerhet. Gjennomfør disse tiltakene i løpet av den neste uken for å redusere sårbarheter og legge grunnlaget for et sikkert digitalt miljø. Hvert trinn er utformet for å være rimelig, brukervennlig og effektivt for sivilsamfunnsorganisasjoner med begrensede ressurser.

1. Sikre kontoene dine

- Aktiver tofaktorautentisering (2FA): Aktiver 2FA for alle kritiske kontoer (f.eks. e-post, sosiale medier, skylagring) i dag. Bruk en autentiseringsapp (for eksempel Google Authenticator eller Authy) eller SMS-koder for å legge til et ekstra beskyttelseslag.
    - ⇒ Kontroller kontoinnstillingene (f.eks. Gmail: Innstillinger > Sikkerhet > To-trinns verifisering).
- Opprett sterke, unike passord: Oppdater passordene for viktige kontoer slik at de består av minst 14 tegn, med en blanding av bokstaver, tall og symboler (f.eks. «sunbird&glass7rain»). Bruk et forskjellig passord for hver konto.
    - ⇒ Vurder en gratis passordbehandler som Bitwarden for å generere og lagre passord på en sikker måte.
- Se etter kontoer som er utsatt for datainnbrudd: Gå til «Have I Been Pwned» (haveibeenpwned.com) for å se om e-posten eller kontoene dine har blitt utsatt for datainnbrudd. Endre berørte passord umiddelbart.
    - ⇒ Lekkede påloggingsopplysninger kan brukes til å angripe kontoene dine.

2. Beskytt enhetene dine

- Oppdater programvare i dag: Sørg for at alle enheter (datamaskiner, telefoner, nettbrett) og programvare (f.eks. operativsystemer, nettlesere, apper) er oppdatert med de nyeste sikkerhetsoppdateringene.
    - ⇒ Sjekk Windows Update, macOS Software Update eller App Store-innstillingene for ventende oppdateringer.

- Installer antivirusprogramvare: Installer et gratis antivirusprogram (f.eks. Windows Defender, Avast Free Antivirus) på alle enheter og sørg for at det er aktivt og oppdatert.
    ⇒ Last ned fra pålitelige kilder og planlegg ukentlige skanninger.
- Aktiver enhetslås: Konfigurer enheter til å låses automatisk etter fem minutters inaktivitet med et sterkt passord eller en PIN-kode. Sørg for at kryptering er aktivert (de fleste moderne enheter har dette som standard).
    ⇒ Låser og kryptering forhindrer datatyveri dersom enheter mistes eller blir stjålet.

3. Sikker kommunikasjon

- Bruk sikre meldingsapper: Bytt til ende-til-ende-krypterte apper som Signal eller WhatsApp for sensitiv kommunikasjon. Verifiser kontakter før du deler sensitiv informasjon.
    ⇒ Last ned og aktiver forsvinende meldinger for sensitive chatter.
- Oppdag phishing-e-poster: Opplær personalet til å unngå å klikke på lenker eller dele informasjon i e-poster med presserende språk, stavefeil eller ukjente avsendere. Kontroller e-postadresser nøye.
    ⇒ Hold musepekeren over lenker for å verifisere nettadresser før du klikker, og rapporter mistenkelige e-poster til IT-avdelingen.

4. Beskytt data

- Sikkerhetskopier kritiske data: Sikkerhetskopier viktige filer (f.eks. giverlister, prosjektdokumenter) til en sikker ekstern harddisk eller skytjeneste (f.eks. Google Drive med 2FA) denne uken.
    ⇒ Planlegg automatiske sikkerhetskopier eller kopier filer manuelt til et sikkert sted.
- Begrens datatilgang: Gjennomgå hvem som har tilgang til sensitive data (f.eks. delte stasjoner, databaser). Fjern tilgangen til tidligere ansatte eller frivillige.
    ⇒ Begrensning av tilgang reduserer risikoen for insidertrusler eller lekkasjer.

5. Sikre tilstedeværelsen din på nettet

- Kontroller nettstedssikkerheten: Kontroller at nettstedet ditt bruker HTTPS (se etter hengelåsen i nettleseren). Kontakt webverten din for å sikre regelmessige

sikkerhetskopier og oppdatert programvare (f.eks. innholdsstyringssystem, programtillegg).

⇒ Sjekk med vertstjenesteleverandøren din eller bruk gratis verktøy som Let's Encrypt for HTTPS.

- Sikre kontoer på sosiale medier: Aktiver 2FA og sterke passord på alle CSO-kontoer på sosiale medier. Fjern tilgang for inaktive administratorer.

  ⇒ Beskytter mot kontokapring og feilinformasjon.

2.2 KAPITTEL 2: FØRSTE TRINN INN I DIGITAL SIKKERHET

Første trinn innen digital sikkerhet

Dette kapittelet omhandler den grunnleggende praksisen som hver enkelt person i en organisasjon bør følge for å oppnå grunnleggende digital sikkerhet. Disse «første trinnene» er ofte enkle vaner og tiltak som gir betydelige sikkerhetsfordeler. Som ordtaket sier, begynner cybersikkerhet med cyberhygiene – de daglige rutinene og forholdsreglene som holder deg trygg på nettet. Vi skal se på hvordan du oppretter sterke passord, bruker internett med forsiktighet, sikrer kommunikasjonen din og beskytter datamaskinene og smarttelefonene dine. Selv om du i utgangspunktet kun implementerer disse grunnleggende tiltakene, vil du allerede redusere en stor del av vanlige trusler.

Opprette og beskytte sterke passord

En av de raskeste måtene å øke den digitale sikkerheten din på er å styrke passordene dine. Passord er nøklene til kontoene og enhetene dine – hvis de er svake eller kompromitterte, kan angripere låse opp alt fra e-posten din til bankopplysningene dine. Dessverre bruker folk ofte passord som er enkle å huske på nytt, eller velger passord som er enkle for angripere å gjette (som «123456» eller «passord»). Faktisk er svake eller stjålne passord fortsatt en av de viktigste årsakene til sikkerhetsbrudd.

Hva er et sterkt passord?

I henhold til retningslinjene for cybersikkerhet er et sterkt passord langt, unikt og komplekst. Microsofts sikkerhetsveiledning anbefaler minst 14 tegn, inkludert en blanding av store og små bokstaver, tall og symboler. Det bør **ikke** inneholde enkle personopplysninger (som navn eller fødselsdato) eller vanlige ord. En god praksis er å bruke en *passfrase* – en rekke tilfeldige ord eller en setning som er lett for deg å huske, men vanskelig for andre å gjette. For eksempel er «sunbird&glass7rain» langt sterkere enn et kort passord som «blue123», men kan likevel være enklere å huske fordi det er en frase.

Det er avgjørende at passordet er unikt: Hver konto eller tjeneste bør ha sitt eget passord. Hvis du bruker passord på nytt og én konto blir hacket, kommer angripere til å prøve det samme passordet på de andre kontoene dine (en taktikk som kalles «*credential stuffing*»). Bruk av unike passord begrenser skaden fra et enkelt datainnbrudd. Som ENISA (EUs byrå for

nettsikkerhet) anbefaler, *bør du unngå å bruke det samme passordet på flere kontoer*. Vurder også å sjekke om kontoene dine har dukket opp i kjente datainnbrudd (nettsteder som «Have I Been Pwned» lar deg søke etter e-posten din i datainnbruddsdatabaser). Hvis det er tilfelle, må du endre disse passordene umiddelbart.

Passordbehandlere: Det er urealistisk å huske dusinvis av lange og komplekse passord. Det er her passordbehandlingsverktøy kommer inn i bildet. En passordbehandler er en applikasjon (eller en sikker skytjeneste) som kan generere sterke, tilfeldige passord for deg og lagre dem i et kryptert hvelv, slik at du bare trenger å huske ett hovedpassord. Mange sikkerhetseksperter og -byråer anbefaler å bruke passordbehandlere for bedre sikkerhet. For eksempel roste Bitwarden (et passordadministrasjonsselskap) ENISAs råd, som eksplisitt omfatter bruk av en passordadministrator for å holde passord unike og trygge. Populære passordbehandlere omfatter Bitwarden, LastPass, 1Password og KeePass (blant andre). Finn en som passer organisasjonen din (noen har gratisversjoner), og begynn å bruke den til å oppgradere alle de svake eller gjentatte passordene.

Beskyttelse av passordene dine: Selv et sterkt passord må beskyttes. Del aldri passordene dine via e-post eller meldinger, og vær på vakt overfor alle som uoppfordret ber om passordet ditt – legitime supportmedarbeidere (selv i IT-selskaper) trenger ikke det faktiske passordet ditt. Aktiver også tofaktorautentisering (2FA) på kontoene dine når det er mulig. 2FA (også kalt flerfaktorautentisering, MFA) innebærer at du oppgir et ekstra identitetsbevis når du logger på – for eksempel en engangskode sendt til telefonen din eller generert av en autentiseringsapp, eller en fingeravtrykkskanning. På denne måten kan ikke noen få tilgang til kontoen uten denne andre faktoren, selv om de får tak i passordet ditt. ENISAs beste råd omfatter å bruke «et ekstra trinn», for eksempel en telefonkode eller biometri, for pålogging. Mange tjenester (Google, Facebook, Microsoft osv.) tillater 2FA via en app eller SMS. Det er lurt å slå dette på for e-postkontoer, sosiale medier, nettbank, skylagring – i hovedsak enhver konto som ville vært sensitiv dersom den ble hacket.

En annen viktig vane er å endre standardpassord på enheter eller i applikasjoner. Mange maskinvareenheter (som wifi-rutere) eller programvareverktøy leveres med forhåndsinnstilte administratorkpassord (ofte noe generisk som «admin/admin»). Disse standardpassordene er godt kjent for angripere, så angi alltid et nytt, sterkt passord under konfigurasjonen. Hvis for eksempel CSO-en din konfigurerer en ny kontorruter eller en nettbasert database, bør en av de første oppgavene være å tilpasse tilgangsopplysningene.

Til slutt bør du vurdere en tidsplan for å oppdatere passord med jevne mellomrom. Meningene varierer om hvor ofte passord bør endres – noen eksperter sier at hyppige tvungne endringer kan slå feil (brukere kan velge enklere passord eller bare øke et tall). Moderne veiledning antyder at hvis passordene er sterke og unike, trenger du bare å endre dem når det er tegn på at de er kompromittert, eller med jevne mellomrom (for eksempel én gang i året) for å oppdatere dem. Den gamle regelen om å endre passord hver tredje måned er ikke lenger et absolutt krav dersom andre kontroller (som 2FA) er på plass. Hvis du imidlertid mistenker at en konto kan være kompromittert, må du endre det passordet umiddelbart, og alle andre steder du har brukt et lignende passord.

Oppsummert: Sterke passord + 2FA = et kraftig forsvar. Ved å bruke robuste, unike passord og legge til et ekstra innloggingstrinn, stenger du døren for mange innbruddsforsøk. Tenk på det som å låse huset ditt med en lås av høy kvalitet (passord) og en sikkerhetslås (2FA) – en inntrenger må overvinne begge deler for å bryte seg inn. Som team bør dere oppmuntre alle i sivilsamfunnsorganisasjonen til å ta i bruk denne praksisen. Kapittel 3 tar for seg hvordan man kan håndheve gode passordpolicyer i hele organisasjonen, men endringen kan starte med at du går foran med et godt eksempel ved å bruke en passordbehandler og 2FA for kontoene dine.

Trygg internettbruk: Hva du bør passe deg for

Internett er hovedåren for informasjon og kommunikasjon for de fleste organisasjoner, men det kan også være en kilde til trusler dersom det brukes uforsiktig. «Trygg internettbruk» refererer til å utvise forsiktighet og smart atferd når du surfer på nettsteder, bruker nettbaserte tjenester og laster ned innhold. Her er noen viktige prinsipper og tips som CSO-ansatte bør følge:

***Verifiser nettstedets legitimitet*:** Før du oppgir sensitive opplysninger på et nettsted (for eksempel påloggingsinformasjon eller personopplysninger), må du forsikre deg om at nettstedet er autentisk og sikkert. Kontroller at nettadressen er riktig (se etter skrivefeil eller merkelige domener som etterligner ekte domener) og at tilkoblingen er kryptert – indikert med https:// og et hengelåsikon i nettleserens adressefelt. For eksempel er https://secure.CSOportal.org mer pålitelig enn http://CSO-portal.example.com (mangel på HTTPS er et faresignal). Angripere oppretter ofte falske nettsteder som ser legitime ut (for eksempel et nettsted som etterligner en påloggingsside for e-post) for å phishe passord. Dobbeltsjekk alltid adresselinjen når du logger på. Moderne nettlesere fremhever også ofte selskapsnavnet i sertifikatdetaljene for større nettsteder – bruk disse signalene. Hvis du er i tvil om en lenke du har mottatt (for eksempel via e-post eller sosiale medier), må du ikke klikke på den direkte. Naviger i stedet til det offisielle nettstedet via Google eller bokmerker, eller hold musepekeren over lenken for å forhåndsvise nettadressen (uten å klikke). Dersom lenken ser mistenkelig ut eller ikke samsvarer med den påståtte avsenderen (f.eks. en e-post som hevder å være fra banken din, men der nettadressen er et ikke-relatert domene), er den sannsynligvis skadelig.

Tenk deg om før du klikker eller laster ned: Ondsinnede lenker og nedlastinger er en primær kanal for skadevare. Vær forsiktig når du surfer på ukjente nettsteder eller når du blir bedt om å laste ned filer. Popup-vinduer som oppfordrer deg til å laste ned en «kodek» eller «oppdatering» for å se innhold, er ofte feller. Hvis du trenger en bestemt programvare eller et bestemt dokument, må du laste det ned fra en anerkjent kilde (for eksempel programvare fra den offisielle leverandørens nettsted eller en kjent appbutikk). Unngå å laste ned piratkopiert programvare eller media – bortsett fra de juridiske problemene, skjuler slike filer ofte skadevare. Deaktiver også automatiske nedlastinger i nettleserinnstillingene dine – å ha kontroll betyr at du kan avbryte alt som skjer utilsiktet. Hvis nettleseren eller sikkerhetsverktøyet advarer om at et nettsted kan være utrygt, må du følge advarselen og forlate nettstedet. På samme måte bør du være skeptisk til nettleserutvidelser eller programtillegg fra ukjente utgivere. Installer kun tillegg du virkelig trenger og fra offisielle nettbutikker, siden en skadelig utvidelse kan spore aktiviteten din eller injisere annonser/virus.

Bruk sikre tilkoblinger (Wi-Fi og VPN): Når du kobler deg til internett, spesielt utenfor kontoret, må du være oppmerksom på nettverkssikkerheten. Offentlige Wi-Fi-nettverk (som de på kafeer, flyplasser osv.) kan være risikable ettersom angripere på det samme nettverket kan fange opp trafikken din. Hvis du må bruke offentlig Wi-Fi, bør du unngå å gå inn på sensitive kontoer med mindre tilkoblingen er kryptert (se etter HTTPS). Selv da kan en kyndig angriper opprette et falskt wifi-hotspot med et fristende navn («Gratis wifi på flyplassen») for å lokke til seg brukere. En god praksis er å bruke et VPN (virtuelt privat nettverk) når du er på upålitelige nettverk. Et VPN oppretter en kryptert tunnel for all internettrafikken din, noe som reduserer sjansen for avlytting betraktelig. Mange organisasjoner tilbyr VPN-tilgang for hjemmekontor. Hvis organisasjonen din gjør det, må du sørge for at du vet hvordan du bruker den. Hvis ikke, bør du vurdere å bruke en anerkjent kommersiell VPN-tjeneste når du reiser eller jobber fra offentlige steder. I tillegg må du sørge for at Wi-Fi-nettverket hjemme eller på kontoret er sikret med et sterkt passord og bruker WPA2- eller WPA3-kryptering. Endre standard administratorkodeord på ruteren din som nevnt, og deaktiver ekstern administrasjon med mindre det er absolutt nødvendig.

Vær forsiktig med e-postvedlegg og lenker: Selv om e-post vil bli behandlet mer i neste avsnitt, er det verdt å merke seg som en del av trygge internettvaner at det krever forsiktighet å klikke på lenker i e-poster eller på nettsteder. En vanlig svindelforsøk på nettet er falske varsler som «Datamaskinen din er infisert! Klikk her for å skanne» – disse fører ofte til skadevare. På samme måte bør du unngå å klikke på bannerannonser eller popup-vinduer som hevder at du har vunnet noe eller at du trenger en hastende oppdatering. Dette er forsøk på sosial manipulering for å utnytte nysgjerrighet eller frykt. Husk ordtaket: Hvis noe på nettet høres for godt (eller for skummelt) ut til å være sant, er det sannsynligvis svindel. For eksempel bør en nettannonse med teksten «Få et tilskudd på 5 000 USD nå – tidsbegrenset!» bør vekke mistanke. Øv deg på å gjenkjenne disse taktikkene og ikke reagere impulsivt.

Beskytt personlig og organisasjonsrelatert informasjon: Vær oppmerksom på informasjonen du deler offentlig på nettsteder og sosiale medier, ettersom den kan brukes mot deg i cyberangrep. Angripere innhenter ofte opplysninger fra profiler på sosiale medier eller nettsteder for å lage mer overbevisende phishing-e-poster (en praksis som kalles «spear

phishing» når den er svært målrettet). Hvis for eksempel nettstedet til sivilsamfunnsorganisasjonen din oppfører ansattes e-postadresser og interesser, kan noen sende deg en e-post som refererer til denne informasjonen for å vinne tilliten din. Begrens derfor hva du avslører om interne saker i offentlige fora. Når du fyller ut nettskjemaer, bør du vurdere om alle de forespurte opplysningene er nødvendige. Hvis et nettsted ber om din mors pikenavn eller andre personopplysninger uten et klart behov, bør du tenke deg om. Fra et personvernperspektiv bør du bruke personverninnstillinger på sosiale medier for å begrense hvem som kan se innleggene dine. Og for organisasjonens del må du sørge for at kataloger eller sensitive dokumenter ikke utilsiktet blir eksponert på deres egen nettside. Søk jevnlig etter navnet på sivilsamfunnsorganisasjonen din på nettet for å se hvilken informasjon som finnes der ute – på denne måten kan du oppdage et eksponert dokument eller et nettsted som etterligner organisasjonen.

Bruk oppdaterte nettlesere og sikkerhetsverktøy: Trygg internettbruk handler ikke bare om atferd – det handler også om å bruke oppdatert teknologi. Kjør alltid den nyeste versjonen av nettleseren din (Chrome, Firefox, Edge osv.), siden oppdateringer ofte retter opp sikkerhetssvakheter. Aktiver nettleserens innebygde sikkerhetsfunksjoner: De fleste nettlesere har beskyttelse mot nettfisking og skadevare som kan blokkere kjente skadelige nettsteder. Du bør også ha et anerkjent antivirus-/anti-malware-program aktivt på enheten din, som noen ganger kan oppdage om en nedlasting eller et nettsted er skadelig. Moderne antivirusløsninger omfatter ofte nettbeskyttelse som advarer eller blokkerer hvis du prøver å besøke et nettsted som er kjent for phishing eller som er vert for skadevare. For eksempel kan Microsoft Defender eller Avast vise en advarselsside hvis du prøver å få tilgang til et farlig nettsted. Vær oppmerksom på disse advarslene – de er der for å beskytte deg.

Oppsummert handler trygg bruk av internett i stor grad om å være årvåken og skeptisk når du er på nettet. På samme måte som du er smart på gata i en storby – du er oppmerksom på omgivelsene og tenker deg om to ganger før du går inn i en tvilsom smug – bør du på nettet passe på hvor du «reiser» og hvem du samhandler med. Oppmuntre alle i teamet ditt til å ha en forsiktig tankegang: Hold musepekeren over lenker før du klikker, last ned kun fra pålitelige kilder og vær mistenksom overfor uoppfordrede popup-vinduer eller meldinger. I neste avsnitt

skal vi dykke dypere ned i en av de vanligste angrepsveiene, e-post og meldinger, og hvordan man kan sikre denne kommunikasjonen.

E-post- og meldingssikkerhet

E-post er et uunnværlig verktøy for sivilsamfunnsorganisasjoner, og meldingsapper (som WhatsApp, Signal eller Telegram) brukes i stor grad for rask kommunikasjon. Disse kanalene er imidlertid hyppige mål for cyberangrep som phishing, avlytting og kontokapring. Denne delen gir veiledning om hvordan du kan kommunisere på en tryggere måte og unngå vanlige fallgruver.

Bevissthet om phishing: Phishing via e-post ble nevnt tidligere fordi det er så utbredt. For å gjenta og utdype: Undersøk alltid uventede e-poster nøye, spesielt de som oppfordrer til umiddelbar handling eller ber om sensitive opplysninger. En typisk phishing-e-post kan se ut til å komme fra en kollega, en bank eller en nettbasert tjeneste, og inneholde en lenke for å «logge inn» eller et vedlegg som skal åpnes. Før du klikker på en lenke i en e-post, må du verifisere avsenderen og lenkens mål. Kontroller avsenderens adresse nøye – angripere bruker ofte en adresse som avviker med én bokstav (f.eks. john.doe@micros0ft.com i stedet for en legitim Microsoft-e-postadresse) eller en offentlig e-postadresse som ikke samsvarer med den påståtte organisasjonen. Hvis en e-post hevder at du må tilbakestille et passord eller oppgi informasjon, er det tryggere å ikke klikke på lenken i e-posten. Gå i stedet til det offisielle nettstedet selv. Når det gjelder vedlegg, må du ikke åpne filer fra ukjente eller upålitelige e-poster. Selv om den kommer fra en kjent kontakt, bør du bekrefte med avsenderen via en annen kanal dersom den er uventet og merkelig (f.eks. et tilfeldig dokument med tittelen «Faktura» som du ikke forventet). Som regel bør du unngå å aktivere makroer eller aktivere innhold i Office-dokumenter med mindre du er helt sikker på kilden – mange skadevareinfeksjoner skjer via Word-/Excel-makroer i phishing-vedlegg.

Sikkerhetsansvarlige bør opplyse de ansatte om at det er greit (og til og med oppfordret) å være litt paranoide med e-poster – ved tvil bør de verifisere. En rask telefonsamtale eller melding til den angivelige avsenderen kan bekrefte om vedkommende virkelig sendte forespørselen. Det er bedre å dobbeltsjekke enn å klikke og angre. Husk at phishing ikke er begrenset til e-post –

det kan også skje via SMS (tekstmeldinger med skadelige lenker) eller meldingsapper. For eksempel kan en medarbeider motta en WhatsApp-melding som ser ut som et varsel fra en nettbetalingstjeneste med en lenke – behandle disse på samme måte, med forsiktighet.

Sikkerhet for e-postkontoer: Siden e-postkontoer kan være en inngangsport for å tilbakestille andre passord og inneholde sensitiv korrespondanse, er det avgjørende å sikre e-postinnloggingen din. Bruk et sterkt passord og 2FA for e-postkontoen din (som beskrevet i 2.1) – mange e-postleverandører som Gmail, Outlook eller ProtonMail støtter tofaktorautentisering via en app eller SMS. Dette reduserer risikoen for at noen hacker e-posten din drastisk. Vær også oppmerksom når du åpner e-post på delte eller offentlige datamaskiner. Logg alltid ut etterpå og sørg for at nettleseren ikke lagrer påloggingsinformasjonen din. Hvis det er mulig, bør du bruke sikre e-postprotokoller (de fleste moderne tjenester bruker dette som standard): Sørg for at webmailen bruker HTTPS, og hvis du bruker en e-postklientapp (som Outlook, Thunderbird eller på telefonen din), må du sørge for at den er konfigurert til å bruke krypterte tilkoblinger (SSL/TLS) for både mottak (IMAP/POP) og sending (SMTP). IT-støtten din eller leverandørens dokumentasjon kan bekrefte disse innstillingene.

Vurder e-postkryptering for svært sensitiv kommunikasjon. Vanlige e-poster er ikke ende-til-ende-krypterte, noe som i teorien betyr at e-postinnholdet kan leses av utilsiktede parter (for eksempel e-postleverandører eller alle som får tilgang til kontoen). For sensitive data kan du bruke verktøy som PGP/GPG-e-postkryptering eller bytte til sikre meldingsplattformer for den samtalen. PGP kan imidlertid være komplisert for daglig bruk, så en annen strategi er å bruke sikker fildeling for sensitive vedlegg i stedet for å legge inn konfidensiell tekst i e-postens brødtekst. Noen e-posttjenester eller bedriftspakker med fokus på sivilsamfunnsorganisasjoner tilbyr innebygd kryptering eller i det minste muligheten til å passordbeskytte e-poster eller vedlegg. Dersom organisasjonen din håndterer ekstremt sensitive opplysninger (for eksempel menneskerettighetssaker), bør du rådføre deg med en ekspert på digital sikkerhet om å konfigurere en krypteringsarbeidsflyt.

Sikre meldingsapper: Mange sivilsamfunnsorganisasjoner bruker direktemeldinger for raske samtaler og koordinering. Det er viktig å velge meldingsapper som tilbyr ende-til-ende-

kryptering (E2EE), som sikrer at kun de kommuniserende brukerne (og ingen mellom, ikke engang tjenesteleverandøren) kan lese meldingene. WhatsApp har for eksempel E2EE som standard for chatter, i likhet med Signal og Telegrams «hemmelige chatter» (merk: Telegrams skychatter er ikke E2EE som standard). Signal anbefales i stor grad i civilsamfunnets miljø for sensitiv kommunikasjon fordi det er åpen kildekode, E2EE og har sterke personvernpraksiser. En annen er **Wire**, som også er sikker og i samsvar med den europeiske personvernforordningen (GDPR). **Threema** og **Element (Matrix)** er andre sikre meldingsalternativer som noen menneskerettighetsgrupper bruker. Det spesifikke appvalget kan avhenge av konteksten din og hva motpartene dine bruker, men en generell regel er: Unngå ren tekst-kanaler (SMS-er eller ukrypterte e-poster) for sensitive saker og bytt til en kryptert app der det er mulig.

Selv med krypterte apper bør du være oppmerksom på metadata (hvem som snakker med hvem, når). De fleste E2EE-apper avslører fortsatt noen metadata til tjenesten (selv om Signal prøver å minimere dette). For ekstremt sensitive operasjoner kan man bruke mer anonymitetsfokuserte verktøy som *Session* eller bruke meldinger via Tor, men dette er avanserte scenarier. For generell bruk i sivilsamfunnsorganisasjoner vil en vanlig E2EE-app forbedre sikkerheten betraktelig sammenlignet med ukrypterte kanaler.

Lås også meldingsappene dine: Bruk applåsefunksjoner eller PIN-koder for enheten, slik at ingen kan åpne chattene dine dersom telefonen din mistes eller blir stjålet. Aktiver forsvinende meldinger for svært sensitive samtaler – mange apper lar deg angi at meldinger skal slettes automatisk etter en viss tid (Signal, WhatsApp osv.). På den måten kan tidligere meldinger allerede være borte hvis noen kompromitterer kontoen din senere.

Vær på vakt mot meldingssvindel: Phishing-svindel misbruker ikke bare e-post. Du kan motta svindelmeldinger via SMS eller apper som ber deg om å klikke på en lenke (ofte forkortede URL-er) eller videresende noe. Et eksempel er «WhatsApp-kodesvindelen»: Du mottar en SMS med en påloggingskode du ikke har bedt om, og umiddelbart etterpå en WhatsApp-melding fra en venn som sier: «Jeg har problemer, kan du sende meg koden du nettopp mottok?» Vennens konto er sannsynligvis hacket, og angriperen prøver å bruke koden

din til å overta WhatsApp-kontoen din. Lærdom: Gi aldri verifiseringskoder til andre, og vær mistenksom overfor hastende, merkelige forespørsler i chatten, selv om de kommer fra venner.

Vedlegg og skylenker: I stedet for å legge ved dokumenter i e-post, har mange gått over til skylenker (f.eks. lenker til Google Drive, Dropbox og OneDrive). Disse er praktiske, men har sine egne sikkerhetshensyn. Hvis du sender en skydelingslenke, må du sørge for at den kun er tilgjengelig for de tiltenkte personene (bruk private lenker eller legg til e-postadressene deres eksplisitt) og vurdere å angi utløpsdatoer for lenken. Hvis du mottar en skylenke, må du være forsiktig som med enhver lenke – sørg for at den er fra et legitimt skytjenestedomene og at du forventet den. En phishing-taktikk kan innebære å sende en lenke som ser ut som en Google Drive-fil, men som leder til en falsk påloggingsside. Bekreft alltid om nødvendig, og ideelt sett bør du få tilgang til delte stasjoner via det kjente grensesnittet (f.eks. logge deg på Google Drive direkte for å se om en fil ble delt med deg).

E-posthygiene og beste praksis: Noen flere raske tips: Bruk søppelfiltre – moderne e-posttjenester gjør en god jobb med å fange opp det meste av søppelpost/phishing. Du bør likevel sjekke søppelpostmappen din av og til for falske positiver, men ikke samhandle med e-poster i søppelposten med mindre du er sikker på at de er trygge. Ikke avslutt abonnementet på søppelpost-e-poster med mindre de er fra anerkjente kilder. Hvis du klikker på «Avslutt abonnement» på e-poster som virkelig er søppelpost, kan det bekrefte overfor spammere at adressen din er aktiv. Det er bedre å bare slette dem. Når du sender e-poster til store grupper, bør du bruke BCC for å beskytte mottakernes adresser mot å bli sett av alle (for å forhindre utilsiktede lekkasjer av kontaktlister). Og vurder å aktivere varsler om videresending av e-post eller påloggingsvarsler dersom leverandøren tilbyr dem, slik at du vet om det skjer uvanlig aktivitet (Gmail kan for eksempel varsle deg dersom det skjer en ny pålogging fra en ny enhet).
Ved å følge denne praksisen kan organisasjonen din redusere risikoen for å bli offer for e-post- eller meldingsbaserte angrep betydelig. Siden e-post ofte er det første kontaktpunktet for angripere, gir mestring av e-postsikkerhet en stor sikkerhetsgevinst. Tenk på det som sikker kjøring: Som oftest er «veiene» (internett) i orden, men du må bruke sikkerhetsbelte (2FA), følge signaler (advarsler om mistenkelige lenker) og være oppmerksom for å unngå ulykker.

Grunnleggende tips for å sikre datamaskiner og telefoner

Bærbare datamaskiner, stasjonære PC-er og smarttelefoner er arbeidshestene i enhver moderne organisasjon. De lagrer også mange sensitive data og kan være inngangspunkter for angripere hvis de ikke er sikret. Denne delen gir grunnleggende tips for å holde disse enhetene trygge mot vanlige trusler. Mange av disse tipsene faller inn under rutinemessig vedlikehold og fornuftig bruk – den digitale motparten til å låse dørene og skifte olje regelmessig.

Hold programvaren oppdatert: Sørg for at alle enhetenes operativsystemer og programmer holdes oppdatert med de nyeste sikkerhetsoppdateringene. Programvareoppdateringer løser ofte sårbarheter som angripere kan utnytte. Aktiver automatiske oppdateringer der det er mulig – aktiver for eksempel Windows Update eller macOS' automatiske oppdateringer, og gjør det samme på iPhone/Android-telefonen din for system og apper. Oppdater også appene dine (nettlesere, kontorprogrammer osv.) regelmessig. Mange av dem gir beskjed når en oppdatering er tilgjengelig – ikke ignorer disse beskjedene. For programvare som ikke oppdateres automatisk, bør du angi en gjentakende påminnelse om å se etter oppdateringer eller bruke et sentralt administrasjonsverktøy hvis det er tilgjengelig. Husk at dette omfatter nettleserprogramtillegg og rammeverk som Java eller Adobe Reader, som historisk sett har vært inngangsportaler for skadevare dersom de er utdaterte. En oppdatert enhet er en hardfør enhet.

Installer antivirus-/anti-skadevarebeskyttelse: Bruk en anerkjent antivirusløsning på datamaskinene dine (og vurder også en av de anerkjente mobil sikkerhetsappene for Android-enheter). Moderne antivirusprogramvare gir sanntidsbeskyttelse, noe som betyr at den aktivt skanner filer og overvåker systematferden for å blokkere skadevare. Windows 10/11 leveres med innebygd Microsoft Defender, som er ganske bra for grunnleggende bruk hvis det holdes oppdatert. Tredjepartsalternativer (betalte eller gratis) som Avast, Bitdefender, ESET osv. kan også vurderes. Det viktigste er å ha noe og holde virusdefinisjonene oppdatert daglig. Unngå å bruke flere antivirusprogrammer samtidig (de kan komme i konflikt med hverandre). På telefoner trenger iPhoner generelt sett ikke separate antivirus-apper på grunn av måten iOS er utformet på, men Android-telefoner kan ha nytte av en anti-skadevare-app, spesielt hvis du noen ganger installerer apper fra kilder utenfor den offisielle Play Store. Det beste forsvaret for

telefoner er imidlertid å kun installere apper fra pålitelige appbutikker og kontrollere apptillatelser – en lommelyktapp bør for eksempel ikke trenge å se kontaktene eller meldingene dine.

Én ting til: Deaktiver aldri sikkerhetsprogramvaren din av bekvemmelighetshensyn. Hvis den blokkerer en handling, bør du undersøke hvorfor i stedet for bare å slå den av. Ikke installer piratkopiert programvare, som nevnt – bortsett fra lovligheten, leveres piratkopiert programvare ofte med trojanere som antivirusprogramvaren kanskje ikke oppdager.

Bruk enhetslåser og kryptering: Lås alltid enhetene dine med en PIN-kode, et passord eller en biometrisk lås (fingeravtrykk, ansiktsgjenkjenning) når de ikke er i bruk. Angi en kort tidsavbrudd for automatisk låsing (f.eks. at skjermen låses etter fem minutters inaktivitet eller mindre). Dette forhindrer uautorisert tilgang dersom noen fysisk får tak i enheten din. Dersom en CSO-bærbar PC blir stjålet fra en bil eller en telefon går tapt på en konferanse, kan en sterk låseskjerm beskytte dataene mot nysgjerrige blikk – men bare hvis den er på plass. For bærbare datamaskiner bør du vurdere fullstendig diskkryptering. Moderne operativsystemer har ofte dette som standard: Windows har BitLocker (Pro-utgaver) eller enhetskryptering, og macOS har FileVault. Når denne funksjonen er aktivert, forblir dataene krypterte uten dekrypteringsnøkkelen (vanligvis knyttet til påloggingspassordet ditt), selv om harddisken fjernes. På smarttelefoner støtter både iOS og Android enhetskryptering (nyere versjoner krypterer som standard når du bruker en PIN-kode/et passord). Kontroller at kryptering er aktivert, spesielt på eldre Android-versjoner der den kan ha vært valgfri. Kryptering er avgjørende for sensitive data. Hvis for eksempel en bærbar datamaskin som inneholder deltakerdata fra en studie går tapt, men er kryptert, forblir dataene sikre, og hendelsen er et problem med tapt enhet, ikke et datainnbrudd.

Regelmessige sikkerhetskopier: Selv om sikkerhetskopier primært er et tiltak for datagjenoppretting, er de også et sikkerhetstiltak – de gjør det mulig å gjenopprette data etter angrep fra løsepengevirus eller tap av enheter, uten å gi etter for utpressing eller lide totalt tap. Kapittel 3 vil beskrive sikkerhetskopistrategier i detalj, men som et grunnleggende tips: Sikkerhetskopier viktige filer regelmessig og oppbevar sikkerhetskopiene på et sikkert sted atskilt fra datamaskinen din (en ekstern harddisk oppbevart på et trygt sted eller en

sikkerhetskopitjeneste i skyen). Test disse sikkerhetskopiene av og til for å sikre at du kan gjenopprette data. For mobile enheter bør du vurdere å sikkerhetskopiere viktige bilder/dokumenter (telefoner kan konfigureres til å sikkerhetskopiere til skyen eller en datamaskin). Dersom telefonen blir stjålet, er i det minste ikke dataene dine borte for alltid.

Sikker installasjon av apper/programmer: Installer kun programvare fra pålitelige kilder. På datamaskiner betyr dette vanligvis programvarens offisielle nettsted eller en kjent appbutikk (som Microsoft Store eller Mac App Store). På telefoner bør du bruke Google Play Store, Apple App Store eller F-Droid (for Android-apper med åpen kildekode). Vær forsiktig med gratis verktøy fra ukjente nettsteder – hvis du for eksempel trenger en PDF-konverterer eller videospiller, bør du undersøke om det finnes et anerkjent verktøy i stedet for å laste ned det første du finner. Noen skadelige programmer utgir seg for å være nyttige verktøy. Under installasjonen må du også være oppmerksom på meldinger og avslå eventuelle tilbud om å installere ekstra verktøylinjer eller endre søkemotoren (vanlig i gratis installasjonsprogrammer). Dette er ikke akkurat sikkerhetstrusler, men de rotet til systemet ditt og kan føre til sårbarheter eller personvernproblemer.

Sikker konfigurasjon og innstillinger: Ta deg tid til å konfigurere grunnleggende sikkerhetsinnstillinger på enhetene dine. På Windows må du for eksempel sørge for at brannmuren er slått på (den er vanligvis slått på som standard). En brannmur bidrar til å blokkere uønskede innkommende tilkoblinger. De fleste brukere trenger ikke å justere den utover standardinnstillingen, men den bør forbli aktivert. På ruteren din må du sørge for at brannmuren/NAT er på og at ekstern administrasjon er av (som nevnt i «Trygt internett»). På smarttelefoner bør du sjekke personverninnstillingene for hver app – deaktiver unødvendige tillatelser (trenger et spill tilgang til mikrofonen din? Sannsynligvis ikke). Både Android og iOS lar deg se hvilke tillatelser hver app har, og trekke tilbake de som virker overdrevne.

Fysisk sikkerhet for enheter: Digital sikkerhet er ikke bare digital – det er også viktig å sikre enheter fysisk. Ikke la bærbare datamaskiner eller telefoner stå uten tilsyn på offentlige steder. På kontoret bør du ha en policy om å låse skjermene når du forlater skrivebordet ditt (både Windows og Mac har snarveier for dette). Hvis du er på reise, må du være oppmerksom på bærbare datamaskiner ved sikkerhetskontrollen på flyplassen eller i drosjer – mange

datainnbrudd skyldes ganske enkelt tapte enheter med sensitive opplysninger. Vurder også å bruke personvernskjermer til bærbare datamaskiner hvis du ofte jobber på offentlige steder (for å forhindre at andre ser over skulderen din og ser på skjermen din). For stasjonære datamaskiner, spesielt hvis CSO-en din har et kontor som er tilgjengelig for besøkende eller delte områder, kan låsing av serverrom eller bruk av kabellåser for utstyr avskrekke tyveri.

Bruk av administrasjon av mobile enheter (MDM) for organisasjoner: Hvis sivilsamfunnsorganisasjonen din har kapasitet til det (eller etter hvert som den vokser), kan dere implementere en MDM-løsning. MDM-programvare gjør det mulig for en organisasjon å håndheve sikkerhetspolicyer på telefoner og bærbare datamaskiner sentralt – for eksempel ved å kreve en PIN-kode, sende ut automatiske oppdateringer eller slette innholdet på en enhet eksternt hvis den mistes. Selv uten formell MDM bør du i det minste sørge for at du kan slette enheter eksternt: For telefoner kan tjenester som Find My iPhone eller Androids Find My Device eksternt finne og slette en tapt telefon. For bærbare datamaskiner finnes det noen ganger lignende alternativer hvis du bruker Windows koblet til en Microsoft-konto eller bedriftsverktøy. Du bør i det minste vite hvordan du endrer passord og ugyldiggjør økter for kontoer på en tapt enhet (hvis for eksempel en frivillig mister en telefon som hadde tilgang til sivilorganisasjonens e-post, må du umiddelbart endre passordet til den e-posten og logge av alle økter).

Planlegg for feil: Noen ganger svikter maskinvaren eller blir skadet. Selv om det ikke er et «nettangrep», kan disse hendelsene forårsake tap av data eller driftsstans. Grunnleggende tips: Bruk et pålitelig antivirusprogram, men ha også noen gjenopprettingsverktøy tilgjengelig (for eksempel en oppstartbar, ren USB-pinne med antivirusprogram eller systemreparasjonsverktøy). Og sørg for at viktige filer ikke kun lagres på én bærbar datamaskin – hvis maskinvaren svikter, har du sikkerhetskopier eller synkronisering på plass.

Ved å bruke disse grunnleggende tipsene skaper du et grunnleggende beskyttelsesnivå for de personlige enhetene og arbeidsenhetene dine. Tenk på det som å sikre «endepunktene» – hver telefon eller PC er et endepunkt som kan utnyttes hvis det er svakt, men til sammen danner de den digitale miljøet til sivilsamfunnsorganisasjonen din. En angriper går ofte for det enkleste målet. Disse tiltakene (oppdateringer, antivirus, sterke konfigurasjoner) fjerner de

lettest tilgjengelige målene, noe som tvinger motstandere til å jobbe mye hardere eller ideelt sett avskrekker dem helt. Det er analogt med sikkerhet i hjemmet: Du låser dører, installerer røykvarslere og har kanskje en hund – ingenting av dette garanterer sikkerhet, men de reduserer risikoen betraktelig og gir varsler. Innen cybersikkerhet er den oppdaterte, godt konfigurerte enheten din med sikkerhetsprogramvare som et hjem med låser og alarmer – langt mindre attraktivt for inntrengere enn et uoppdatert, ubeskyttet system.

Nå som vi har innført personlige sikkerhetsvaner og sikkerhetsvaner for enheter, går vi videre til organisasjonsnivået: Å utvikle en plan og en kultur i sivilsamfunnsorganisasjonen din som støtter digital sikkerhet. Neste kapittel tar for seg hvordan man vurderer risikoer og utarbeider en enkel, men effektiv **plan for digital sikkerhet** som er tilpasset behovene til sivilsamfunnsorganisasjonen din.

Kapittelsammendrag

Kapittel 2 gir en tilgjengelig introduksjon til grunnleggende cybersikkerhetskonsepter tilpasset civilsamfunnsorganisasjoner, med fokus på CIA-triaden: konfidensialitet, integritet og tilgjengelighet. Konfidensialitet sikrer at data (f.eks. giveroppføringer) forblir private, integritet forhindrer uautoriserte endringer, og tilgjengelighet holder systemene tilgjengelige. Kapitlet bruker enkelt språk og eksempler som er relevante for sivilsamfunnsorganisasjoner, for eksempel å sikre aktivistenes kontaktlister, for å forklare disse prinsippene. Det introduserer trusselsmodellering, en prosess for å identifisere risikoer og prioritere beskyttelsestiltak, noe som gjør den relevant for organisasjoner med begrensede ressurser. Praktisk anbefalt praksis omfatter sterke passord, tofaktorautentisering (2FA) og forsiktig internettbruk. Kapitlet legger vekt på rimelige løsninger, for eksempel gratis passordadministratorer (f.eks. Bitwarden), for å imøtekomme sivilsamfunnsorganisasjoners budsjettbegrensninger. Det fremhever også det menneskelige elementet, og påpeker at 74 % av sikkerhetsbruddene involverer feil som å falle for phishing-svindel. Ved å øke bevisstheten kan sivilsamfunnsorganisasjoner redusere risikoen uten teknisk ekspertise. Kapitlet oppfordrer til å starte med enkle trinn (f.eks. oppdatering av programvare) for å bygge et sikkerhetsgrunnlag. Det kobler digital sikkerhet til sivilsamfunnsorganisasjonenes oppdrag, og forklarer hvordan beskyttelse av data opprettholder tillit og ansvarlighet. For eksempel kan en kompromittert giverdatabase undergrave tilliten i

offentligheten, som vi har sett i tidligere hendelser. Kapitlet gir e-boken en praktisk tone og utstyrer leserne med grunnleggende kunnskap for å iverksette sikkerhetstiltak på en effektiv måte.

Trinnvis veiledning for å utføre en grunnleggende risikovurdering

Denne veiledningen gir en strukturert prosess som sivilsamfunnsorganisasjoner kan bruke til å fylle ut risikovurderingsmalen, med eksempler tilpasset vanlige ressurser for sivilsamfunnsorganisasjoner, som giverdatabaser og frivilligregister. Trinnene er utformet for å være tilgjengelige for organisasjoner med begrenset teknisk ekspertise, i tråd med pensumets vekt på praktiske rammeverk (modul 2) og e-bokens veiledning om risikovurdering (kapittel 5).

Trinn 1: Identifiser kritiske digitale ressurser

- Dette skal du gjøre: Lag en liste over de digitale ressursene (data, systemer, kontoer) som er avgjørende for driften av sivilorganisasjonen din. Fokuser på hva som kan forstyrre oppdraget deres eller skade interessenter dersom det kompromitteres.
- Slik gjør du det: Samle et lite team (f.eks. ledelse, programansvarlige, IT-ansvarlig) for å idémyldre. Vurder data (f.eks. giverlister, informasjon om mottakere), systemer (f.eks. e-post, nettsted) og kontoer (f.eks. sosiale medier, skylagring).

  Eksempel:

  - Giverdatabase: Et regneark eller CRM-system som inneholder givernavn, kontaktopplysninger og donasjonsbeløp.
  - Frivilligregister: Filer med navn på frivillige, kontaktinformasjon og tidsplaner lagret på en delt stasjon eller en skyplattform.
  - E-postkontoer: Ansattes Gmail- eller Outlook-kontoer som brukes til kommunikasjon med interessenter.

Trinn 2: Identifiser trusler mot hver ressurs

- Hva du skal gjøre: For hver ressurs oppfører du potensielle trusler (f.eks. hacking, phishing, skadevare, menneskelige feil) som kan kompromittere den.
- Slik gjør du det: Drøft hvordan angripere kan angripe ressursen eller hva som kan gå galt (f.eks. utilsiktede lekkasjer, tyveri av enheter). Se vanlige trusler fra e-boken (kapittel 1.3), for eksempel phishing, datainnbrudd eller løsepengevirus.

  Eksempel:

  - Giverdatabase:

        - Trussel: Datainnbrudd via phishing (angriperen lurer ansatte til å oppgi påloggingsopplysninger).
        - Trussel: Løsepengevirus krypterer databasen.
    - Frivilliges opptegnelser:
        - Trussel: Uautorisert tilgang på grunn av svake passord eller delte påloggingsopplysninger.
        - Trussel: Tap av data dersom en bærbar datamaskin blir stjålet.

Trinn 3: Vurder sannsynligheten for hver trussel

- Hva du skal gjøre: Vurder sannsynligheten for at hver trussel inntreffer på en skala fra 1 (sjelden) til 5 (nesten sikker).
- Slik gjør du det: Ta hensyn til faktorer som sivilsamfunnsorganisasjonens synlighet, tidligere hendelser eller vanlige angrepstrender (f.eks. at phishing er utbredt). Bruk lokal kontekst hvis tilgjengelig (f.eks. hyppig phishing i regionen din).

  Eksempel:
    - Giverdatabase:
        - Phishing: Sannsynlighet = 3 (Mulig, siden phishing er vanlig, men de ansatte har fått opplæring).
        - Løsepengevirus: Sannsynlighet = 2 (Usannsynlig hvis antivirus er på plass, men ikke umulig).
    - Frivilliges opptegnelser:
        - Uautorisert tilgang: Sannsynlighet = 4 (Sannsynlig, hvis passordene er svake eller tilgangen ikke er begrenset).
        - Tyveri av bærbar PC: Sannsynlighet = 2 (Usannsynlig, men mulig i feltoperasjoner).

Trinn 4: Vurder virkningen av hver trussel

- Hva du skal gjøre: Vurder alvorlighetsgraden av trusselens konsekvenser på en skala fra 1 (lav) til 5 (alvorlig), med tanke på forstyrrelser i oppdraget, tap av data eller skade på omdømmet.

- Slik gjør du det: Tenk på det verst tenkelige scenariet (f.eks. juridiske problemer, tap av tillit, skade på mottakere). Se eksemplene i e-boken, for eksempel datainnbruddet hos Australske Røde Kors (kapittel 1.1).

  Eksempel:

  - Giverdatabase:
    - Phishing/innbrudd: Konsekvens = 5 (alvorlig, på grunn av eksponering av giverdata, GDPR-bøter, tap av tillit).
    - Løsepengevirus: Konsekvens = 4 (høy, ettersom driften kan stoppe uten sikkerhetskopier).
  - Frivilliges opptegnelser:
    - Uautorisert tilgang: Konsekvens = 4 (høy, ettersom brudd på frivilliges personvern kan skade omdømmet).
    - Tyveri av bærbar PC: Konsekvens = 3 (Moderat, hvis dataene er kryptert, men gjenoppretting er kostbart).

Trinn 5: Beregn risikopoengsummer og prioriter

- Dette skal du gjøre: Multipliser sannsynlighet med konsekvens for å oppnå en risikopoengsum (1–25). Høyere poengsummer indikerer risikoer som krever øyeblikkelig oppmerksomhet.
- Slik gjør du det: Bruk malen til å beregne poengsummer og sortere risikoene fra høyest til lavest. Fokuser på å håndtere risikoer med høy poengsum først.

  Eksempel:

  - Giverdatabase:
    - Phishing: 3 × 5 = 15 (høy prioritet).
    - Løsepengevirus: 2 × 4 = 8 (moderat prioritet).
  - Frivilliges opptegnelser:
    - Uautorisert tilgang: 4 × 4 = 16 (høy prioritet).
    - Tyveri av bærbar PC: 2 × 3 = 6 (lav prioritet).

Trinn 6: Utvikle avbøtende tiltak

- Hva du skal gjøre: Lag en liste over spesifikke, gjennomførbare tiltak for å forhindre eller redusere hver trussel, med fokus på praktiske tiltak til lave kostnader.
- Slik gjør du det: Hent ut løsninger som 2FA, kryptering eller opplæring fra læreplanen (modul 1–5) og e-boken (kapittel 2–4). Sørg for at trinnene er gjennomførbare med tanke på ressursene til sivilsamfunnsorganisasjonen din.

  Eksempel:

  - Giverdatabase:
    - Nettfisking: Aktiver 2FA for databaseadgang, krypter filer og lær opp personalet i å oppdage nettfisking.
    - Løsepengevirus: Planlegg ukentlige sikkerhetskopier til en sikker sky, installer oppdatert antivirusprogramvare.
  - Frivilligregister:
    - Uautorisert tilgang: Bruk sterke passord, begrens tilgangen til autorisert personale og revider tillatelser månedlig.
    - Tyveri av bærbar PC: Aktiver enhetskryptering, bruk verktøy for fjernsletting for tapte enheter.

Trinn 7: Gjennomgå og oppdater

- Dette skal du gjøre: Utpek et teammedlem til å gjennomgå risikovurderingen årlig eller etter større endringer (f.eks. ny programvare, endringer i personalet). Oppdater malen etter behov.
- Slik gjør du det: Planlegg et gjennomgangsmøte for å sjekke om ressurser, trusler eller avbøtende tiltak har endret seg. Dokumenter oppdateringer for å sikre at planen fortsatt er relevant.

  Eksempel: Etter implementering av 2FA synker sannsynligheten for uautorisert tilgang til frivilliges opptegnelser til 2, noe som reduserer risikopoengsummen til 8. Oppdater malen deretter.

2.3 KAPITTEL – 3: DIGITALE SIKKERHETSPLANER FOR CIVILSAMFUNNSORGANISASJONER

En digital sikkerhetsplan for sivilsamfunnsorganisasjoner

Etter å ha dekket individuell praksis, vender vi oss mot den bredere organisasjonsmessige tilnærmingen. En digital sikkerhetsplan er et strategisk og operativt veikart for hvordan sivilorganisasjonen din skal beskytte sine digitale ressurser og reagere på trusler. Det trenger ikke å være et komplisert eller omfangsrikt dokument. Faktisk er en kortfattet plan som alle forstår, ofte bedre enn en omfangsrik policy som står på en hylle. Dette kapittelet veileder deg gjennom å opprette en grunnleggende sikkerhetsplan, med fokus på **fire hovedelementer:** – Å identifisere risikoene dine,

– Utarbeide planen med egnede tiltak,

– Øke bevisstheten gjennom opplæring,

– Beskytte dataene dine gjennom sikkerhetskopier og sikker lagring.

Identifisere risikoene: Hvilke trusler står organisasjonen din overfor?

Hver organisasjon har en unik risikoprofil avhengig av aktiviteter, data og motstandere. Det første trinnet i utarbeidelsen av en sikkerhetsplan er å **identifisere og vurdere disse risikoene** – i hovedsak å utføre en enkel digital risikovurdering. Dette krever ikke en høyere utdannelse – det innebærer å tenke systematisk over hva som kan gå galt, og hvor alvorlig det kan skade driften din hvis det skjer.

Identifiser ressursene og dataene dine: Start med å lage en liste over de viktige digitale ressursene og opplysningene som sivilsamfunnsorganisasjonen din innehar. Disse omfatter: maskinvare (datamaskiner, telefoner, servere), programvare og tjenester (e-postkontoer, nettsteder, skydisker, databaser) og data (medlemslister, økonomiske opptegnelser, forskningsdata, kommunikasjon osv.). Still spørsmål som: Hvilke data ville forårsake mest skade dersom de ble offentliggjort? Hvilke systemer er avgjørende for det daglige arbeidet vårt? For eksempel kan en sivilsamfunnsorganisasjon som yter juridisk bistand prioritere klienters saksmapper og kommunikasjon med advokater som kritiske ressurser som må beskyttes (på grunn av taushetsplikt). En utviklings-CSO kan identifisere giverdatabasen og feltforskningsdataene sine som vitale. Å vite hva «kronjuvelene» dine er, bidrar til å fokusere sikkerhetsinnsatsen din.

Identifiser potensielle trusler og trusselaktører: Deretter bør du vurdere hvem eller hva som kanskje ønsker å skade organisasjonens digitale infrastruktur. Noen vanlige trusler er vilkårlige – f.eks. tilfeldige nettkriminelle som sprer løsepengevirus for å tjene penger, og som kan ramme hvem som helst. Andre kan være mer målrettede: Kanskje selskaper eller enkeltpersoner som motarbeider påtalene dine, eller til og med statlig overvåking hvis du arbeider med sensitive saker. Lag en liste over trusselkategorier: Hackere som er ute etter økonomisk gevinst, insidere (ansatte eller frivillige) som utilsiktet eller forsettlig kan kompromittere sikkerheten, og trusler som er spesifikke for din kontekst (for eksempel kan en sivilsamfunnsorganisasjon som driver kampanje mot korrupsjon tiltrekke seg målrettede phishing- eller telefonhackingforsøk fra berørte parter). Vurder også fysiske trusler mot digitale ressurser, for eksempel tyveri av utstyr eller ødeleggelse på grunn av katastrofer (flom, brann – disse kan også forårsake IT-avbrudd, og derfor er det behov for sikkerhetskopier utenfor anlegget).

For hver trussel bør du tenke på mulige scenarier: *Hvordan* kan denne trusselen manifestere seg? For eksempel:

- En nettkriminell kan forsøke å hacke nettstedet ditt for å ødelegge det eller bruke det til å distribuere skadevare.
- En fiendtlig aktør kan sende phishing-e-poster til de ansatte i et forsøk på å stjele passord og lese e-postene deres.
- Skadevare som løsepengevirus kan infisere en av de ansattes datamaskiner, kryptere filer og kreve løsepenger, som omtalt i tidligere kapitler.
- En frivillig kan miste en bærbar PC med ukrypterte sensitive data.
- En misfornøyd tidligere ansatt kan fortsatt ha tilgang til en konto hvis avskjedigelsen ikke ble utført på riktig måte, noe som utgjør en risiko for datatyveri eller sabotasje.

Vurder sannsynlighet og konsekvenser: Ikke alle risikoer er like. Mens noen hendelser kan være svært usannsynlige, men katastrofale hvis de inntreffer, kan andre være sannsynlige, men ha mindre innvirkning. For hvert identifiserte risikoscenario må du vurdere hvor sannsynlig det er at det skjer (lav, middels, høy), og hva virkningen ville bli dersom det skjer (lav, middels, høy

virkning). For eksempel er *phishing-angrep* svært sannsynlige (høy sannsynlighet) og kan ha stor innvirkning (hvis kontodetaljer stjeles) – så det er en høy risiko som krever kraftig risikoreduksjon. På den annen side er *maskinvarefeil* ganske sannsynlig over tid (til slutt svikter en disk), men hvis du har sikkerhetskopier, er konsekvensene lave, så det er en moderat risiko som du håndterer med sikkerhetskopier. Eller *målrettet statssponset hacking* kan ha stor innvirkning (de kan kompromittere dypt), men hvis du er en liten lokal sivilsamfunnsorganisasjon uten høyprofilerte kampanjer, kan sannsynligheten være lav – fortsatt verdt en viss beskyttelse, men ikke ditt hovedfokus.

Denne typen kvalitativ vurdering hjelper deg med å prioritere. Som en veiledning med fokus på sivilsamfunnsorganisasjoner antyder, er forståelse av cyberrisiko og kunnskap om hva som trenger beskyttelse de første trinnene mot effektiv sikkerhet. Du kan til og med formulere dem som spørsmål, slik Liberties' veiledning gjør: «Hva er de viktigste digitale ressursene våre? Hvem kan prøve å angripe dem og hvorfor? Hva ville skjedd dersom ressurs X ble brutt eller ble utilgjengelig?» Involver teamet ditt i denne idémyldringen – ulike medarbeidere kan fremheve ulike bekymringer (f.eks. kan økonomiansvarlig bekymre seg for bankkontoopplysninger, kommunikasjonsansvarlig for at sosiale medier blir hacket osv.).

Vurder juridiske og samsvarsrelaterte risikoer: Civilsamfunnsorganisasjoner må også tenke på forskrifter som personvernlover. I EU krever for eksempel GDPR at organisasjoner beskytter personopplysninger og rapporterer brudd. Et risiko ved dårlig sikkerhet er altså manglende overholdelse av lovgivning og bøter. Hvis sivilsamfunnsorganisasjonen din håndterer personopplysninger om givere eller mottakere, kan et datainnbrudd innebære brudd på personvernlovgivningen. Ta derfor med samsvar i risikotenkningen – f.eks. «Risiko for lekkasje av personopplysninger – konsekvenser omfatter skade på enkeltpersoner + juridiske sanksjoner». Denne risikoen vil tydeligvis ha stor innvirkning, og hvis dere har mange personopplysninger, kanskje middels sannsynlighet, som krever strenge kontroller.

***Dokumenter og ranger risikoer*:** Skriv ned et kort risikoregister – til og med en enkel tabell over risikoscenarier, sannsynlighet, konsekvenser og gjeldende tiltak. Ranger dem etter risikonivå (en kombinasjon av sannsynlighet og konsekvens). Dette vil gi veiledning om hvor ressursene skal fordeles. Du kan for eksempel rangere «Phishing-angrep som fører til

kontokompromittering» som en topprisiko, mens «DDoS-angrep på nettstedet» kan være lavere hvis nettstedet ditt ikke er kontroversielt og har skybeskyttelse. Eller «Insider lekker utilsiktet data via Google Drive-lenke» kan være en middels risiko som kan håndteres via opplæring og tilgangskontroller.

Risikovillighet: Det er også lurt å innse at *ingen organisasjon kan eliminere all risiko*. En del av risikostyringen er å avgjøre hvilket risikonivå som er akseptabelt med tanke på ressursene dine. Dette kalles ofte «risikoappetitt». En liten sivil samfunnsorganisasjon kan akseptere risikoen ved ikke å ha et IT-sikkerhetsteam tilgjengelig døgnet rundt, og i stedet fokusere på grunnleggende forsvar og ekstern støtte ved behov. Målet er å redusere risikoen til et nivå du er komfortabel med. For høye risikoer iverksetter du kraftige avbøtende tiltak; for lavere risikoer kanskje mer grunnleggende tiltak, eller du overvåker dem over tid.

På slutten av denne risikoidentifikasjonsfasen bør du ha et klarere bilde av hvor du står. Du kan for eksempel konkludere med følgende: *De største sårbarhetene våre er phishing og svake passord (høy risiko), pluss utdatert programvare på nettstedet vårt (middels risiko) og lav bevissthet blant de frivillige (bidrar til risiko). Vi har en moderat risiko for tapte enheter (vi deler av og til bærbare datamaskiner), men hvis vi aktiverer kryptering, kan risikoen reduseres. Vi er sannsynligvis ikke et spesifikt mål for nasjonalstater, men vi håndterer sensitive opplysninger om fellesskapet som må holdes konfidensielle.* Denne innsikten legger grunnlaget for utarbeidelsen av sikkerhetsplanen – i hovedsak vil planen håndtere disse identifiserte risikoene med egnede tiltak.

Ved å kjenne organisasjonens digitale svake punkter og truslene som mest sannsynlig vil utnytte dem, kan du planlegge et effektivt forsvar. Denne tilnærmingen er i tråd med konseptet om risikobasert beslutningstaking – et kjerneprinsipp som anbefales i rammeverk for cybersikkerhet. Den sikrer at du fokuserer på det som betyr mest, i stedet for å prøve å gjøre alt overalt. Med dette risikobildet i tankene kan vi nå gå videre med å utarbeide en plan som omfatter retningslinjer og praksis for å redusere disse risikoene.

Utarbeide en enkel digital sikkerhetsplan

Når risikoene er identifisert, er neste trinn å utarbeide en plan for å håndtere og redusere disse risikoene. En digital sikkerhetsplan for en sivilorganisasjon omfatter vanligvis retningslinjer, prosedyrer og kontroller som tar for seg de viktigste risikoområdene, samt oversikter over roller og ansvarsområder. Ikke la deg skremme av begrepet «plan» – den kan være like enkel som en sjekkliste eller et kort dokument. Det viktigste er at den er praktisk og tilpasset organisasjonens størrelse og behov.

Sikkerhetspolicy og styring: Start med å etablere noen veiledende policyer. Dette kan være et kort avsnitt som beskriver organisasjonens forpliktelse til digital sikkerhet og grunnleggende regler som alle bør følge. Ha for eksempel en passordpolicy (f.eks. krev sterke passord av en viss lengde og 2FA på alle kritiske kontoer – du kan se avsnitt 2.1 for nærmere opplysninger), en policy for akseptabel bruk (f.eks. retningslinjer for bruk av arbeidsenheter og internett til hensiktsmessige formål, ikke installere uautorisert programvare osv.) og en personvernpolicy (f.eks. regler for håndtering av personopplysninger, overholdelse av juridiske krav som GDPR og klassifisering av datafølsomhet). ENISA anbefaler at det skrives klare retningslinjer for cybersikkerhet og formidles til de ansatte, der det beskrives hvordan de forventes å oppføre seg med IKT-ressurser og hvilke konsekvenser det får ved manglende overholdelse. Retningslinjene dine kan for eksempel angi at ansatte ikke må dele kontopassord og at de umiddelbart må rapportere mistenkte phishing-forsøk til IT-ansvarlig.

Hvis sivilsamfunnsorganisasjonen din er liten, kan du samle mange ting i ett generelt retningslinjedokument – det er greit. Det viktigste er å tildele ansvar. Bestem hvem i teamet ditt som skal ha ansvaret for sikkerhetstilsynet (det kan være en administrerende direktør eller en teknisk kyndig medarbeider som blir «sikkerhetsansvarlig»). ENISAs veiledning for SMB-er påpeker at tildeling av ledelsesansvar for cybersikkerhet er et sentralt element for å lykkes. Utpek derfor en rolle eksplisitt: f.eks. «Driftslederen skal fungere som informasjonssikkerhetsansvarlig og ha ansvar for å koordinere sikkerhetsarbeidet og sikre at retningslinjene implementeres.» Hvis dere har et styre eller en ledelse, må dere sørge for at de godkjenner denne planen – støtte fra ledelsen er avgjørende for å få med seg alle.

Risikostyringstiltak: For hver identifisert stor risiko (fra 3.1) skal du skissere hva du skal gjøre med den. Dette blir i praksis kjernen i planen din:

- Hvis for eksempel «phishing» er en av de største risikoene, kan planen din omfatte tiltak som å implementere 2FA på e-post (allerede omtalt), gjennomføre opplæring i phishing-bevissthet (se 3.3) og etablere prosedyrer for å verifisere uvanlige forespørsler (f.eks. en bekreftelsesprosess for finansielle transaksjoner).
- Dersom «utdatert programvare» var en risiko, ville planen din omfatte å føre en oversikt over viktig programvare og en tidsplan eller ansvar for oppdateringer (kanskje sikkerhetsansvarlig eller ekstern IT-støtte sørger for oppdateringer månedlig).
- Hvis risikoen «datainnbrudd på personopplysninger» ble identifisert: Planlegg tiltak som å begrense tilgangen til disse opplysningene (bare visse personer kan få tilgang til sensitive mapper), bruke kryptering for spesielt sensitive filer og ha en prosedyre for hendelsesrespons (hvis det skjer et innbrudd, hvordan man begrenser og varsler – mer om dette i kapittel 5).
- Dersom risikoen er «tap av enhet»: Planlegg for fullstendig diskkryptering og fjernsletting som nevnt, pluss kanskje en inn-/utsjekkingslogg for delte enheter.

Hendelsesresponsplan: En god plan, selv en enkel en, forutser at ting kan gå galt. Så ta med en grunnleggende prosedyre for hendelsesrespons: Hvis det oppstår en cybersikkerhetshendelse (f.eks. infisering med skadevare, mistanke om hacking osv.), hvem skal personalet rapportere til, og hvilke tiltak kommer du til å iverksette? Kapittel 5 omhandler dette grundig, men i planen din er det nok å skissere rollene: f.eks. «Alt personell må umiddelbart rapportere enhver mistenkt sikkerhetshendelse til [navn/rolle]. Vi kommer til å isolere berørte datamaskiner fra nettverket, vurdere omfanget og kontakte [IT-støtte eller ekstern ekspert] ved behov. Vi kommer også til å informere ledelsen og, dersom personopplysninger er involvert, forberede oss på å varsle berørte parter og myndigheter i henhold til loven.» Å ha dette på papir betyr at du i krisetilfeller har en referanse å følge, noe som kan spare dyrebar tid og redusere panikken.

Tilgangskontroller og kontoadministrasjon: Planen bør definere hvordan dere administrerer brukerkontoer og tilgang. Dette kan omfatte å føre en liste over hvem som har tilgang til hvilke systemer, bruke prinsippet om minst mulig privilegium (gi folk tilgang kun til

det de trenger), og, viktigst av alt, prosedyrer for onboarding og offboarding av ansatte/frivillige. Når for eksempel noen forlater organisasjonen, må planen sikre at kontoene deres deaktiveres umiddelbart eller at passordene endres. Mange sikkerhetshendelser skjer fordi tidligere ansatte eller partnere fortsatt har aktive påloggingsopplysninger. Inkluder trinn som «Ved personalavgang kommer IT-avdelingen til å tilbakekalle tilgang til e-post, skystasjoner og eventuelle delte passord innen 24 timer.» Hvis dere bruker delte kontoer eller generiske påloggінger (prøv å minimere disse), bør dere ha en plan for å endre disse passordene rutinemessig eller når noen med kunnskap slutter.

Håndtering av tredjeparter: Vær klar over at sikkerheten din også avhenger av eventuelle tredjepartstjenester eller kontraktører du bruker. Hvis du identifiserte «leverandører» som en risiko (f.eks. en outsourcet IT-støtte eller en skyleverandør som er vert for databasen din), må du inkludere tiltak for å håndtere dette. ENISAs veiledning foreslår at man sikrer at alle leverandører med tilgang til sensitive data oppfyller sikkerhetskravene og at man inngår kontraktsavtaler om sikkerhet. I en enkel plan kan dette innebære å verifisere at eventuelle skytjenester du bruker, er anerkjente og overholder databeskyttelsesstandarder, og at du har sikkerhetskopier uavhengig av dem om nødvendig. Hvis du ansetter en webutvikler eller IT-konsulent, må du også sørge for at vedkommende signerer en avtale om å følge sikkerhetspolicyene dine (f.eks. å ikke bruke påloggingsinformasjonen din på andre steder eller holde data konfidensielle).

Implementer grunnleggende kontroller: Oppsummer de konkrete kontrollene du skal implementere (noen overlapper med tipsene i kapittel 2, men her formaliserer du dem):

- **Enhetssikkerhet**: «Alle organisasjonens bærbare datamaskiner skal ha antivirus og brannmur aktivert, og fullstendig diskkryptering (BitLocker/FileVault) slått på. Automatisk skjermlås vil bli satt til 10 minutters inaktivitet.»
- **Passordsikkerhet**: «Håndhev passordpolicy: Minst 12 tegn, ingen vanlige ord, unike for hver konto. Bruk av passordbehandler anbefales og vil bli konfigurert for personalet. 2FA aktiveres på kritiske kontoer (e-post, økonomisystemer osv.).»

- **Datasikkerhetskopiering**: «Kritiske data (f.eks. giverdatabase, programfiler) sikkerhetskopieres ukentlig til [sikker sky/kryptert ekstern stasjon]. Testgjenopprettinger skal utføres kvartalsvis.»
- **Sikker konfigurasjon**: «Sørg for at standardpassord på alt utstyr endres. Deaktiver unødvendige tjenester på nettstedet vårt og hold det oppdatert. Gjennomgå brukerrettigheter med jevne mellomrom for å fjerne overflødige administratorrettigheter.»
- **Kryptering av data under overføring**: «Bruke krypterte kanaler for sensitiv kommunikasjon (f.eks. Signal for konfidensiell meldingstjeneste eller PGP-e-post for visse kontakter der det er mulig). Nettstedet vårt har et SSL-sertifikat (HTTPS), og vi kommer til å håndheve bruken av det slik at brukerinnsendinger krypteres.»

Når du oppfører kontroller, bør du unngå språk som er for generelt eller umulig å måle («Vi kommer til å forhindre alle angrep» – urealistisk). Fokuser i stedet på gjennomførbare kontrolltiltak. Det kan være nyttig å bruke et rammeverk som sjekkliste – for eksempel CIS Controls (en populær liste over grunnleggende cyberpraksis) eller ISO 27001-domener som inspirasjon. Men tilpass den til det du kan iverksette.

Tidsplan og vedlikehold: Oppgi hvor ofte selve planen skal gjennomgås og hvem som skal vedlikeholde den. Teknologi og trusler utvikler seg, så kanskje: «Denne sikkerhetsplanen kommer til å gjennomgås og oppdateres årlig (eller når det skjer en større endring i IT-systemet vårt) av [rolle].» Når du iverksetter planen, er det også mulig at du ikke gjør alt på en gang. Det er greit å prioritere tiltak i faser. Planen din kan ha en del kalt «Handlingsplan» der du skisserer umiddelbare tiltak (f.eks. aktivere 2FA på e-post innen 1 måned, planlegge opplæring neste måned, iverksette sikkerhetskopiering innen 3. kvartal osv.). Dette gjør den fra bare en policy til et prosjekt med tidsfrister.

Kommunikasjon og håndhevelse: En plan fungerer kun hvis folk kjenner til den og den håndheves. Når den er utarbeidet, bør du dele den med alle ansatte og frivillige. Kanskje kan du holde et kort møte for å forklare hovedpunktene («Vi har nå en policy, og dette betyr den for det daglige arbeidet deres»). Få tilbakemelding – kanskje noen ser en mangel eller har et

forslag. Inkluder konsekvensene av manglende overholdelse i planen eller i tilhørende materiale på en vennlig måte – f.eks.: «Dersom retningslinjene ikke følges, kan det føre til disiplinærtiltak, men vi tar sikte på å støtte alle i å oppnå denne beste praksisen gjennom opplæring og ressurser.» Dette sender et signal om at sikkerhet er en del av alles jobb, ikke bare en IT-sak. En god analogi fra CyberPeace Institute: Behandle ikke cybersikkerhet som en isolert IT-utgift, men som en **katalysator** for oppdraget ditt. Ved å integrere sikkerhet i de daglige prosessene sikrer du kontinuitet og tillit til driften.

For å illustrere dette kan du forestille deg et utdrag fra sikkerhetsplanen til en liten miljøorganisasjon:

- **Risiko**: Phishing av personalets e-post – **Avbøtende tiltak**: Obligatorisk 2FA for e-post, opplæring i å gjenkjenne phishing (ledet av en IT-frivillig) og opprettelse av en rapporteringsprotokoll for mistenkelige e-poster.
- **Risiko**: Tap av bærbare datamaskiner i felten – **Avbøtende tiltak**: Aktivering av fullstendig diskkryptering, daglig datasynkronisering til skyen når internett er tilgjengelig, innføring av enhetslåsekoder.
- **Risiko**: Skade på nettsted – **Avbøtende tiltak**: Regelmessige oppdateringer fra webvert, bruk av en sikkerhetsplugin eller -tjeneste, sikkerhetskopiering av nettstedsinnhold, plan for rask gjenoppretting ved hacking.
- **Retningslinjer**: Alle nye frivillige må få grunnleggende sikkerhetsopplæring og signere avtalen om IKT-bruk (som omfatter ikke å dele kontoer osv.).
- **Ansvar**: Utnevnt Jane Doe (programleder) som sikkerhetskoordinator for å overvåke og veilede disse handlingene.

Ved å knytte tiltak til risikoer og tildele hvem som gjør hva, blir planen din gjennomførbar. Den er kanskje bare på noen få sider, men det er greit. Korthet kan være virkningsfullt hvis det er tydelig. Faktisk sammenfatter ENISAs veiledning for SMB-er råd i 12 overordnede trinn som fungerer som en miniplan for bedrifter (ting som «Utvikle en god cybersikkerhetskultur – tildel ansvar», «Planlegg for hendelser» og «Sikre sikkerhetskopier»). Mange av disse gjenspeiles her.

Den siste delen av planleggingen er å iverksette disse tiltakene og fremme bevissthet, noe som fører oss til neste del. Ha utkastet til planen for hånden mens vi diskuterer opplæring og kultur, siden dette ofte er en av planens komponenter.

Bevissthetstrening for ansatte og frivillige

Selv den beste sikkerhetsplanen på papir kan mislykkes hvis personene i organisasjonen ikke er med på bussen eller ikke har kunnskap. Menneskelig atferd er en kritisk faktor for digital sikkerhet – som nevnt tidligere involverer et betydelig flertall av brudd et menneskelig element (feil eller sosial manipulering). Derfor er opplæring av teamet ditt og etablering av en kultur for sikkerhetsbevissthet noe av det mest virkningsfulle du kan gjøre. Tenk på de ansatte og de frivillige som den første forsvarslinjen (eller omvendt, det svakeste leddet hvis de ikke er opplært). Denne delen skisserer hvordan man oppretter og opprettholder effektiv opplæring i sikkerhetsbevissthet i en sivilsamfunnsorganisasjons kontekst.

Start med det grunnleggende: Opplæringen trenger ikke å være altfor teknisk. Faktisk er det ofte bedre å fokusere på grunnleggende ting man bør og ikke bør gjøre, virkelige eksempler og interaktiv diskusjon. Dekk de vanlige truslene på måter folk kan forholde seg til. Vis for eksempel hvordan en phishing-e-post ser ut (kanskje du kan vise en faktisk phishing-e-post som du redigerer for opplæringen), og be deltakerne peke ut faresignalene (dårlig grammatikk, merkelig avsenderadresse, uventet vedlegg osv.). Diskuter et scenario: «Hva bør du gjøre hvis du mottar en e-post fra direktøren som ber om en hastende pengeoverføring?» (Svar: Bekreft alltid via en telefonsamtale eller ansikt til ansikt før du handler, fordi det kan være svindel fra administrerende direktør.) Disse praktiske øvelsene hjelper personalet med å innse hvordan et angrep kan utspille seg og hvordan de kan reagere rolig. ENISA anbefaler at opplæringen fokuserer på **virkelige situasjoner** som SMB-er står overfor, noe som også gjelder for organisasjoner i sivilsamfunnet. Voksne elever forstår ofte begreper bedre gjennom scenarier og historier enn gjennom abstrakte regler.

Viktige emner å ta med: Ta minst opp emnene fra kapittel 2 i opplæringsform:

- Sikker passordpraksis og bruk av passordbehandlere.

- Slik aktiverer og bruker du 2FA (kanskje en livedemo av hvordan du konfigurerer en autentiseringsapp).
- Gjenkjenne phishing-e-poster, mistenkelige lenker og hva du skal gjøre (ikke klikk, rapporter det).
- Riktig håndtering av sensitiv informasjon (f.eks. bruk av krypterte verktøy for konfidensielle data, unngåelse av å bruke personlig e-post til arbeidsinnhold osv.).
- Enhetssikkerhet: Betydningen av oppdateringer, å ikke installere uautoriserte apper, å låse skjermer og å være forsiktig med USB-minnepinner (ukjente USB-minnepinner kan være farlige).
- Forsiktighet på sosiale medier: Ikke dele for mye sensitiv arbeidsinformasjon på Facebook/Twitter, være oppmerksom på sosial manipulering (for eksempel at noen ringer og utgir seg for å være IT-støtte).
- Rapportering av hendelser: Legg vekt på en kultur uten skyldfølelse. Folk bør føle seg trygge på å rapportere hvis de har klikket på noe farlig eller mistet en enhet, i stedet for å skjule det. Gjør det klart at det er avgjørende med rask rapportering, og at de ikke vil bli straffet for en oppriktig feil – prioriteringen er å løse problemet.

Interaktiv og OCSO-opplæring: Bevissthet er ikke en engangshendelse. Planlegg å ha oppfriskningsøkter eller i det minste periodiske påminnelser. Mange organisasjoner gjennomfører en årlig sikkerhetsopplæring. Men i mellom kan du dele tips på personalmøter eller sende en e-post med «Månedens sikkerhetstips». I oktober (Cybersecurity Awareness Month, som ofte fremmes i EU av ENISA) kan du for eksempel avholde en morsom quiz eller dele en kort video om sikkerhet. Opplæringen trenger ikke å være tørr. Noen sivilsamfunnsorganisasjoner inviterer en sikkerhetsekspert eller bruker gratis nettmoduler (det finnes mange gratis kurs og videoer om bevissthet om cybersikkerhet rettet mot ideelle organisasjoner og små bedrifter).

Vurder også å benytte eksterne ressurser: Hvis dere har en IT-partner, eller hvis det finnes et lokalt teknisk universitet, kan de noen ganger hjelpe til med å holde en workshop. Det finnes

også ideelle initiativer som tilbyr gratis cyberbevissthetsworkshopper til sivilsamfunnet (for eksempel kan organisasjoner som TechSoup eller CyberPeace Builders-frivillige hjelpe til med å gjennomføre opplæring).

Spesielt fokus på nøkkelroller: Skreddersy deler av opplæringen etter roller. Økonomiansvarlig kan trenge mer dyptgående opplæring i å oppdage fakturasykling eller sikre bankinnlogginger (fordi sivilsamfunnsorganisasjoner har blitt lurt via falske fakturaer eller e-poster som utgir seg for å være fra administrerende direktør til å sende penger til svindlere). Kommunikasjonsmedarbeiderne dine som håndterer sosiale medier, kan trenge tips om hvordan de kan unngå kontoovertakelser (for eksempel å bruke 2FA og være på vakt mot phishing via direktemeldinger). Ledelsen bør også forstå sin rolle – ledere er ofte mål for spear-phishing («sjef»-e-postsvindelen), så de bør være et forbilde på god atferd (som å aldri be om sensitive opplysninger eller overføringer bare via e-post uten verifisering). Sørg også for at frivillige eller korttidsansatte får minst en mini-innføring i sikkerhet, siden de kanskje ikke deltar på formell opplæring for ansatte. Et jukselark på én side eller en rask orientering om «ting man bør og ikke bør gjøre» når de blir med, kan være til hjelp.

Skap en kultur for å stille spørsmål: Oppmuntre alle til at det er greit å stille spørsmål ved ting som virker mistenkelige. Hvis for eksempel en frivillig får en uvanlig IT-instruksjon som vedkommende er usikker på, bør han/hun spørre. Sørg for at de vet hvem de skal spørre – f.eks.: «Hvis du mottar mistenkelig kommunikasjon eller er usikker på en fil eller lenke, kan du kontakte IT-kontaktpersonen vår (eller sikkerhetskoordinatoren) på [kontakt].» Dette går tilbake til Microsofts råd: Cybersikkerhet er en *lagidrett*, og hvis du ser noe, si ifra til en betrodd rådgiver. Hvis noen tror de kan ha gjort en sikkerhetsfeil, for eksempel ved å klikke på en dårlig lenke, bør de føle seg trygge på å rapportere det umiddelbart i stedet for å frykte å bli klandret. Raske reaksjoner kan ofte avverge eller minimere skade (for eksempel å koble fra en PC ved mistanke om skadevare).

Måling og forsterkning: Det er nyttig å måle hvor godt opplæringen fungerer. En måte er å gjennomføre interne phishing-tester (hvis ressursene tillater det): Send en ufarlig «falsk phishing»-e-post til personalet etter opplæringen for å se hvem som klikker. De som gjør det, kan få en mild oppfølgingsopplæring. Men hvis dere er en svært liten organisasjon, kan

uformelle spørsmål og svar samt diskusjoner være nok til å få en følelse av forståelse. Selv å spørre på et personalmøte: «Hva ville du gjort hvis du fikk et e-postvedlegg fra noen du ikke kjenner?» og høre svarene, kan avdekke forståelsen. Forsterk budskapene ved å legge ut en kort liste med sikkerhetstips på kontorets oppslagstavle eller Slack-kanalen. Noen organisasjoner innlemmer til og med sikkerhet i medarbeidernes resultatvurderinger eller rutiner («Har du fullført den årlige sikkerhetsquizen?»), men i sivilsamfunnsorganisasjoner er en enklere tilnærming ofte tilstrekkelig, med mindre dere håndterer ekstremt sensitive data.

Hold deg informert og del oppdateringer: Trussellandskapet endrer seg. Hvis du blir oppmerksom på en ny relevant trussel, bør du oppdatere teamet ditt. Hvis for eksempel en annen sivilsamfunnsorganisasjon rapporterer om en phishing-kampanje rettet mot organisasjoner i sektoren din, bør du varsle de ansatte: «Obs! Det sirkulerer en phishing-e-post som utgir seg for å være fra en finansierer – ikke klikk på slike e-poster, og gi oss beskjed hvis dere mottar en.» Å være en del av nettverk for sivilsamfunnsorganisasjoner eller grupper for deling av sikkerhetsinformasjon (som vi skal se i kapittel 6) kan gi deg slik informasjon som du kan videreformidle. Dette holder sikkerhetsbevisstheten oppdatert og viser personalet at trusler er virkelige og skjer i miljøet deres, og ikke bare er teoretiske.

Oppsummert gjør bevissthetstrening medarbeiderne dine fra potensielle risikofaktorer til ressurser i sikkerhetsposisjonen din. Som et cybersikkerhetsslagord sier: «De ansatte er den beste brannmuren din.» Ved å fremme kunnskap og en årvåken tankegang reduserer du i stor grad sjansen for en kostbar feil. Husk at teknologi alene ikke er nok – selv den sterkeste brannmuren kan omgås hvis en bruker ubevisst slipper angriperen inn. Men et godt opplært team, støttet av en positiv sikkerhetskultur, kan stoppe mange hendelser før de starter, eller oppdage dem tidlig. Denne styrkingen av den menneskelige faktoren er kjernen i robust digital sikkerhet for sivilsamfunnet.

Beskyttelse av dataene dine: Sikkerhetskopiering og sikker lagring

Data beskrives ofte som organisasjoners «livsnerve». For sivilsamfunnsorganisasjoner kan data omfatte informasjon om mottakere, forskningsresultater, opplysninger om givere, økonomiske opptegnelser, prosjektrapporter, fotografier med mer. Beskyttelse av disse dataene handler ikke bare om å forhindre uautorisert tilgang (konfidensialitet), men også om å

sikre at de ikke går tapt (tilgjengelighet) og ikke endres på feilaktig vis (integritet). I denne delen fokuserer vi på to grunnleggende aspekter ved databeskyttelse: regelmessige sikkerhetskopier og sikker lagring (både fysisk og i skyen).

Betydningen av sikkerhetskopier: Forestill deg de verst tenkelige scenariene – et løsepengevirus angriper og krypterer alle filene dine, en brann/flom ødelegger datamaskinene på kontoret, eller en praktikant sletter ved et uhell en viktig mappe. I hvert av disse tilfellene kan en nylig sikkerhetskopi bokstavelig talt redde organisasjonen din. En sikkerhetskopi er en separat kopi av dataene dine som oppbevares på et annet medium (og helst på et annet sted), som du kan gjenopprette fra om nødvendig. Uten sikkerhetskopier kan alle scenariene ovenfor bety uopprettelig tap. Med sikkerhetskopier har du et sikkerhetsnett.

Her er beste praksis for sikkerhetskopiering, hvorav mange er i tråd med standardråd:

Regelmessig hyppighet: Sikkerhetskopier viktige data regelmessig. «Regelmessig» avhenger av hvor ofte dataene endres og hvor kritiske de er. For ganske statiske data kan ukentlig være tilstrekkelig; for data som endres raskt (som daglige programlogger eller aktive databaser), kan daglig eller til og med flere ganger om dagen være bedre. Fastsett gjenopprettingspunktmålet (RPO – Recovery Point Objective): Hvor mye data har vi råd til å miste? Dersom det er verdt en dag, er daglige sikkerhetskopier i orden. Dersom det å miste bare én times data ville vært katastrofalt, bør du ta sikte på hyppigere øyeblikksbilder.

Automatiser det: Sikkerhetskopieringsprosesser som er avhengige av mennesker, mislykkes ofte på grunn av glemsomhet eller travle timeplaner. Bruk automatiserte sikkerhetskopieringsløsninger når det er mulig. Du kan for eksempel konfigurere filserveren eller NAS-en til å sikkerhetskopiere til en ekstern stasjon hver natt kl. 02.00. Eller du kan bruke sikkerhetskopitjenester i skyen (som Backblaze, Acronis osv.) som kjører kontinuerlig eller etter en tidsplan. Mange skylagringstjenester, som Google Drive eller OneDrive, lagrer også tidligere versjoner av filer, som kan fungere som en form for sikkerhetskopi ved filredigeringer eller -slettinger.

Flere kopier og eksternt: Følg noe sånt som 3-2-1-regelen: 3 kopier av data (primær + to sikkerhetskopier), på 2 forskjellige medier, hvorav 1 er eksternt. Dette kan være overdrevent for en svært liten sivilorganisasjon, men ideen er god. Du kan for eksempel ha én sikkerhetskopi

på en ekstern harddisk på kontoret og en annen kryptert sikkerhetskopi i en skytjeneste. Ekstern lagring betyr at hvis kontoret brenner ned, er den eksterne sikkerhetskopien (eller skybaserte sikkerhetskopien) trygg. Sikkerhetskopier i skyen er i seg selv eksterne. Hvis du bruker fysiske medier, kan du vurdere å oppbevare en harddisk hjemme hos et styremedlem eller i en bankboks, og oppdatere den med jevne mellomrom.

Sikre sikkerhetskopiene dine: En sikkerhetskopi er en kopi av sensitive data, så beskytt den. Hvis du bruker en ekstern harddisk, bør du kryptere den (mange sikkerhetskopiverktøy eller operativsystemer som Windows BitLocker kan kryptere eksterne harddisker). Hvis du bruker sikkerhetskopiering i skyen, må du sørge for at tjenesten krypterer data (de fleste gjør det, men du kan også velge å kryptere filer før du laster dem opp for ekstra sikkerhet). Begrens hvem som kan få tilgang til sikkerhetskopier. Ikke la for eksempel en sikkerhetskopistasjon stå tilkoblet et system som er tilkoblet Internett hele tiden – hvis det oppstår angrep med løsepengevirus, kan den også bli kryptert. Ideelt sett er sikkerhetskopier som ikke er tilkoblet hele tiden (frakoblede sikkerhetskopier) immune mot skadevare i nettverket ditt. Hvis du bruker en nettverksstasjon til sikkerhetskopier, må du sørge for at den har versjonskontroll eller en annen form for beskyttelse som hindrer skadevare i å ødelegge gamle sikkerhetskopier umiddelbart.

Testgjenopprettinger: Sikkerhetskopier betyr lite hvis de ikke fungerer når de trengs. Test gjenopprettingsprosessen minst noen ganger i året. Prøv å gjenopprette en fil fra sikkerhetskopien og se om den åpnes riktig. Gjennomfør en brannøvelse: «Hva om hovedstasjonen vår for felles bruk dør – kan vi enkelt gjenopprette sikkerhetskopien fra i går kveld på en ny enhet?» Testing vil avdekke eventuelle problemer som ødelagt sikkerhetskopi, manglende krypteringsnøkler eller prosedyrer som må forbedres. Mange organisasjoner har oppdaget i krisesituasjoner at sikkerhetskopiene deres var ufullstendige eller hadde sviktet i det stille for lenge siden – ikke la det skje med deg.

Dokumenter sikkerhetskopieringsprosedyrer: Skriv ned hva som sikkerhetskopieres, hvordan og hvor. Noter også hvem som er ansvarlig for å overvåke sikkerhetskopier og hvordan du utfører en gjenoppretting. For eksempel: «Salesforce-donordatabasen vår sikkerhetskopieres av Salesforces egen daglige eksport og i tillegg av en manuell eksport utført

av John den 1. i hver måned til en kryptert USB-stasjon.» Hvis John slutter, kan noen andre lese dette og fortsette praksisen. Dokumenter også påloggingsinformasjonen som trengs for sikkerhetskopier (på en sikker måte, selvfølgelig), slik at du ikke trenger å lete etter et passord under en nødgjenoppretting.

Sikker lagring og tilgangskontroll: I tillegg til sikkerhetskopiering innebærer databeskyttelse også å lagre data på en sikker måte i daglig bruk. Dette omfatter både fysisk lagring (som utskrevne filer, USB-minnepinner og servere) og skylagringsløsninger:

Fysiske filer og enheter: Hvis du har sensitive opplysninger i fysisk form (papirdokumenter, USB-pinner, eksterne harddisker), skal du oppbevare dem i låste skap eller i en safe. Ikke la dokumenter med personopplysninger ligge fremme på skrivebord. For eksempel bør påmeldingsskjemaer for frivillige eller skjemaer for mottakere arkiveres når de ikke er i aktivt bruk. Makuler sensitive dokumenter før avhending. For enheter, som nevnt, bør du bruke fullstendig diskkryptering, slik at dataene ikke er lett tilgjengelige dersom en datamaskin eller en harddisk går tapt. Før en oversikt over enheter – vit hvem som har hvilken bærbar PC eller telefon. Hvis en enhet inneholder sensitive data, bør du vurdere retningslinjer for at den ikke skal etterlates på usikre steder (f.eks. låst i en kontorskuff eller tatt med hjem av ansatte og oppbevart på en sikker måte). Under reiser kan du kanskje bruke personvernfiltre på skjermen og ha enhetene med deg (ikke sjekk inn bærbare datamaskiner i bagasjen om mulig).

Skylagring (Google Drive, Dropbox osv.): Skytjenester er svært praktiske og har innebygd redundans, men du må konfigurere dem riktig for sikkerhet. For det første må du aktivere 2FA på skykontoene for å forhindre uautoriserte påloggинger. For det andre må du administrere delingstillatelser nøye. I stedet for å dele en hel stasjon åpent, bør du kun dele mapper/filer med bestemte personer som trenger tilgang. Gjennomgå med jevne mellomrom hvem som har tilgang til hva i Google Drive eller Dropbox – fjern alle som ikke lenger trenger tilgang (inkludert eksterne samarbeidspartnere hvis prosjekter er avsluttet). Vær forsiktig med «del via lenke»-funksjoner. Dersom du oppretter en offentlig lenke til en fil, kan teoretisk sett alle som finner denne lenken få tilgang til den (noen systemer tilbyr nå passordbeskyttede lenker eller lenker som utløper; bruk disse om nødvendig). For svært sensitive filer bør du vurdere å bruke klientsidekryptering før opplasting (noen verktøy integreres med

Dropbox/Google Drive for å kryptere filer lokalt, slik at selv om noen hacker skykontoen din, ser de bare vrøvl uten nøkkelen din).

ENISAs veiledning om skyen for SMB-er gjentar disse punktene: Forstå de unike risikoene ved skyen og sørg for at du velger anerkjente leverandører. De påpeker spesifikt at man bør sørge for å bruke leverandører som ikke bryter lover om data (for eksempel GDPR-begrensninger på lagring av personopplysninger utenfor EU uten sikkerhetstiltak). Hvis for eksempel sivilorganisasjonen din opererer i EU og lagrer personopplysninger, bør du verifisere hvor skyleverandøren lagrer opplysninger og eventuelt signere databehandleravtaler. Hvis du bruker tjenester som Dropbox eller Google, bør du undersøke samsvaren deres og kanskje velge tjenester med servere i regioner du stoler på, eller bruke et europeisk alternativ om nødvendig.

Kryptering under overføring og i hvile: Sørg for at data krypteres – ikke bare på disker, men også under overføring. De fleste skyleverandører krypterer data i hvile på serverne sine og bruker HTTPS for overføringer, noe som er bra. Hvis du selv er vert for data (for eksempel en NAS på stedet som er tilgjengelig via internett), bør du konfigurere et VPN eller i det minste sørge for at webtilkoblinger skjer via HTTPS. For ekstremt sensitive opplysninger kan du også legge til flere lag med kryptering – for eksempel kryptere et dokument med et passord før du laster det opp til en kryptert sky-mappe (dobbel kryptering). Dette kan for eksempel være relevant for lister over aktivister i en fiendtlig region.

Datasegmentering: Ikke alle i sivilsamfunnsorganisasjonen bør automatisk ha tilgang til alle data. Bruk tilgangskontroller til å segmentere data. For eksempel kan HR-filer eller medisinsk informasjon om ansatte begrenses til kun HR-personell. Økonomiske opptegnelser er kun for økonomiteamet. Prosjektfiler kun for de som er med i det aktuelle prosjektet, osv. Mange skyplattformer tillater tillatelsesnivåer og gruppebasert tilgang. På denne måten får ikke angriperen nødvendigvis tak i alt dersom én brukers konto blir kompromittert, men kun det brukeren hadde tilgang til. Det reduserer også risikoen for internt misbruk – folk kan ikke snoke på data som ikke er relatert til rollen deres.

Plan for oppbevaring og destruering av data: En del av sikker lagring er å ikke oppbevare data lenger enn nødvendig. Gamle harddisker fra utskiftede datamaskiner bør slettes eller ødelegges på en sikker måte (det er ikke nok å bare slette filer; bruk programvare til

å overskrive eller ødelegge disken fysisk). Det samme gjelder for USB-minnepinner som ikke lenger er i bruk. Hvis sivilsamfunnsorganisasjonen din samler inn personopplysninger i flere tiår uten behov for det, bør dere vurdere retningslinjer for arkivering eller sletting av gamle oppføringer. Dette reduserer mengden sensitiv informasjon som kan eksponeres ved et datainnbrudd og er i tråd med prinsippene i personvernlovgivningen (minimere datalagring). Hvis du for eksempel gjennomførte et opplæringskurs for fem år siden og fortsatt har kopier av deltakernes ID-er, bør du vurdere om du virkelig trenger dem nå.

Redundans og forretningskontinuitet: Sikkerhetskopier sikrer datakontinuitet, men tenk også på driftskontinuitet. Hvis kontorserveren krasjer, er sikkerhetskopiering av data første trinn, men andre trinn er å gjenopprette funksjonaliteten. Planen din kan omfatte å ha en ekstra enhet eller en skybasert failover. For mange små sivilsamfunnsorganisasjoner gir det å arbeide fra skytjenester for kritiske funksjoner (e-post, dokumenter osv.) i seg selv kontinuitet – du kan fortsette å arbeide fra hvor som helst på en annen enhet hvis en svikter. Men identifiser eventuelle enkeltfeilpunkter. Hvis bare én person vet hvordan man får tilgang til sikkerhetskopier, utgjør det en risiko – kryssopplær noen andre eller dokumenter det, som nevnt.

Eksempel på implementering: Anta at sivilsamfunnsorganisasjonen din har en delt stasjon på en NAS-enhet på kontoret for alle prosjektfiler. Du iverksetter en nattlig sikkerhetskopiering av denne NAS-en til en kryptert ekstern harddisk som direktøren tar med seg hjem i helgene (eksternt). I tillegg synkroniseres kritiske undermapper til en sikker sky (som Google Drive eller Nextcloud) i sanntid for samarbeid og sikkerhet utenfor arbeidsstedet. Du planlegger sikkerhetskopiering av giverdatabasen fra CRM-systemet og laster ned en kopi månedlig, som du krypterer og lagrer i skyen. Fysiske filer, som signerte samtykkeskjemaer fra mottakere, skanner og laster du opp (slik at de sikkerhetskopieres) og oppbevarer originalene i et låst skap. For alle bærbare datamaskiner sørger du for at BitLocker er aktivert, og at hver av dem har et BIOS-/fastvarepassord, slik at tyver ikke enkelt kan starte opp fra USB for å omgå krypteringen. Én gang i kvartalet simulerer du et datatapsscenario for å sikre at du kan gjenopprette fra sikkerhetskopiene.

Ved å gjøre alt dette oppnår du motstandskraft: Selv om det inntreffer en cyberkatastrofe eller maskinvaren svikter, er dataene dine trygge, og du kan gjenoppta arbeidet med minimale forstyrrelser. CyberPeace Institute har fremhevet at ideelle organisasjoner bør se på cybersikkerhet (og i forlengelsen databeskyttelsestiltak) som noe som gjør dem i stand til å utnytte teknologi på en sikker måte for å oppnå sosial påvirkning. Sikre data og sikkerhetskopier betyr at du kan ta i bruk digitale verktøy uten konstant frykt for å miste kritisk informasjon.

Avslutningsvis kan man si at sikkerhetskopier og sikker lagring er som bilbeltet og kollisjonsputene i den digitale virksomheten – du håper aldri å trenge dem i en nødssituasjon, men hvis du gjør det, kan de redde organisasjonen din fra katastrofale tap. Kombiner dette med de proaktive tiltakene fra tidligere avsnitt (som passordhygiene og tilgangskontroller), så skaper du et sterkt skjold for sivilsamfunnsorganisasjonens informasjonsressurser. I neste omgang skal vi se nærmere på noen av de brukervennlige verktøyene som kan styrke sikkerheten ytterligere i praksis, og som supplerer planen og retningslinjene vi har utarbeidet.

Kapittelsammendrag

Dette kapitlet gir praktisk veiledning til sivilsamfunnsorganisasjoner for å sikre kommunikasjon og sensitive data, som er avgjørende for den daglige driften og tilliten. Det omhandler kryptering av e-post, meldinger og datalagring, og anbefaler verktøy som Signal for sikre chatter og HTTPS for nettrafikk. Det legges vekt på sterke tilgangskontroller, for eksempel robuste passord og 2FA, for å forhindre uautorisert tilgang til kontoer som e-post eller skyplattformer (f.eks. Google Drive). Kapitlet anbefaler regelmessige sikkerhetskopier til sikre steder (f.eks. krypterte stasjoner) for å kunne gjenopprette data etter angrep med løsepengevirus eller datatap, og nevner et tilfelle der sikkerhetskopier reddet en sivilsamfunnsorganisasjon fra et angrep med løsepengevirus. Sikre fildelingsmetoder, som krypterte skytjenester, fremheves for å beskytte mottakerdata. Kapitlet tar for seg overholdelse av GDPR og legger vekt på lovlig datahåndtering og samtykke. Det omfatter praktiske tiltak, for eksempel å aktivere 2FA på Gmail eller bruke gratis krypteringsverktøy, noe som gjør det tilgjengelig for ikke-teknisk personale. Eksempler, som e-posthacking av en veldedig organisasjon via phishing, understreker behovet for årvåkenhet. Kapitlet omhandler også sikre videokonferanser og praksis for sosiale medier, slik at sivilsamfunnsorganisasjoner kan kommunisere på en sikker måte i eksterne eller høyrisikobetonede omgivelser. Ved å iverksette disse tiltakene beskytter sivilsamfunnsorganisasjoner sensitive opplysninger, opprettholder driftskontinuitet og skaper tillit hos givere.

Sjekkliste for årlig gjennomgang og oppdatering av cybersikkerhetsplanen for organisasjoner i sivilsamfunnet

Denne sjekklisten sikrer at sivilsamfunnsorganisasjonens cybersikkerhetsplan forblir oppdatert og effektiv ved å gjennomgå ressurser, trusler, retningslinjer og hendelsesresponsstrategier årlig eller etter vesentlige endringer (f.eks. nye systemer, personalutskiftning). Ved å fullføre disse trinnene opprettholdes en robust digital sikkerhetsposisjon for å beskytte oppdraget og interessentene dine:

1. Gjennomgå og oppdater digitale ressurser

- ⇒ Identifiser nye eller endrede digitale ressurser (f.eks. ny giverdatabase, skylagring, kontoer på sosiale medier) som er lagt til siden forrige gjennomgang.
- ⇒ Fjern utdaterte ressurser (f.eks. programvare som ikke lenger brukes, gamle e-postkontoer) fra planen.
- ⇒ Eksempel: Har dere lagt til et nytt CRM-system for donoradministrasjon? Inkluder det i risikovurderingen. Har du lagt ned en gammel frivilligdatabase? Fjern den fra planen.

2. Vurdere nye eller utviklende trusler

- ⇒ Gjennomgå nylige cybersikkerhetstrender eller -trusler som er relevante for sivilsamfunnsorganisasjoner (f.eks. økt phishing, ransomware eller lokale overvåkingsrisikoer).
- ⇒ Konsulter lokale ressurser (f.eks. nasjonale CERT, CSO-nettverk) eller globale rapporter (f.eks. Microsofts CSO-angrepsstatistikk) for oppdateringer.
- ⇒ Oppdater risikovurderingsmalen for å gjenspeile nye trusler eller endringer i sannsynlighet/konsekvenser.
- ⇒ Eksempel: Har du lagt merke til en økning i phishing-e-poster rettet mot CSO-er i regionen din? Øk sannsynlighetspoengsummen for phishing i risikovurderingen din.

3. Gå gjennom nylige hendelser eller nestenulykker

- ⇒ Dokumenter eventuelle cybersikkerhetshendelser eller nesten-hendelser (f.eks. phishing-forsøk, malware-varsler) siden forrige gjennomgang.
- ⇒ Analyser hva som gikk bra og hva som mislyktes i responsen din (f.eks. fungerte sikkerhetskopiene? Ble hendelsen rapportert umiddelbart?).
- ⇒ Oppdater planen med erfaringer for å forbedre fremtidige respons.
- ⇒ Eksempel: En ansatt klikket på en phishing-lenke, men 2FA forhindret tilgang. Legg til et notat for å forsterke 2FA-opplæringen og oppdatere e-postfiltrene.

4. Oppdatere prosedyrer for hendelsesrespons

- ⇒ Kontroller at hendelsesresponsplanen omfatter gjeldende trinn, roller og ansvarsområder (f.eks. hvem som oppdager, begrenser og kommuniserer).
- ⇒ Oppdater kontaktlister for interne hjelpearbeidere (f.eks. IT-ansatte, ledelse) og ekstern støtte (f.eks. lokalt CERT, juridisk rådgiver).
- ⇒ Test planen med en skrivebordsøvelse (f.eks. simulere et angrep med løsepengevirus) for å identifisere hull.
- ⇒ Eksempel: Ny IT-sjef? Oppdater vedkommendes rolle som hendelsesresponsleder. Er den gamle CERT-kontakten utdatert? Erstatt med gjeldende opplysninger.

5. Kontroller sikkerhetspolicyer og samsvar

- ⇒ Gjennomgå og oppdater sikkerhetspolicyer (f.eks. akseptabel bruk, databeskyttelse, BYOD) for å gjenspeile nye verktøy, forskrifter eller praksiser.
- ⇒ Bekreft overholdelse av personvernlover (f.eks. GDPR, lokale forskrifter) og oppdater prosedyrer om nødvendig (f.eks. samtykkeskjemaer, rapportering av databrudd).
- ⇒ Eksempel: GDPR krever varsling om brudd innen 72 timer. Sørg for at retningslinjene dine omfatter denne tidslinjen og en utpekt rapporteringskontakt.

6. Verifisere tekniske beskyttelsestiltak

- ⇒ Revider sikkerhetstiltak (f.eks. 2FA, antivirus, sikkerhetskopier, kryptering) for å sikre at de er aktive og oppdaterte på alle enheter og kontoer.
- ⇒ Se etter nye sikkerhetsfunksjoner i verktøy (f.eks. skyplattformer, e-postleverandører) og aktiver dem hvis det er aktuelt.
- ⇒ Eksempel: Har Google Workspace lagt til en ny sikkerhetsfunksjon for delte stasjoner? Aktiver den og oppdater tilgangskontrollene.

7. Planlegge opplæring og bevisstgjøring av ansatte

- ⇒ Planlegg opplæring i cybersikkerhet eller oppfriskningskurs (f.eks. bevissthet om phishing, passordadministrasjon) for alle ansatte og frivillige.
- ⇒ Innlem nye emner basert på nylige trusler eller hendelser (f.eks. AI-drevet phishing, skysikkerhet).
- ⇒ Eksempel: Etter en lokal økning i ransomware, legg til en 30-minutters økt om å gjenkjenne advarselstegn på ransomware.

8. Teste sikkerhetskopier og gjenoppretting

- ⇒ Kontroller at sikkerhetskopier utføres som planlagt og lagres på en sikker måte (f.eks. kryptert sky eller ekstern harddisk).
- ⇒ Gjennomfør en test av sikkerhetskopigjenoppretting for å sikre at data kan gjenopprettes raskt og nøyaktig.
- ⇒ Eksempel: Gjenopprett en eksempelfil fra forrige måneds sikkerhetskopi for å bekrefte at den er tilgjengelig og intakt.

9. Engasjer ledelsen og interessenter

- ⇒ Orientere ledelsen om den oppdaterte planen og eventuelle ressursbehov (f.eks. budsjett for nye verktøy, tid til opplæring).
- ⇒ Dele viktige oppdateringer med interessenter (f.eks. givere, partnere) for å styrke tilliten til sikkerhetspraksisen din.
- ⇒ Eksempel: Informer givere om at dere har styrket databeskyttelsen for å overholde GDPR, og dermed økt åpenheten.

10. Dokumenter og planlegg neste gjennomgang

⇒ Registrer alle oppdateringer i cybersikkerhetsplanen og lagre den på et sikkert, tilgjengelig sted (f.eks. kryptert delt stasjon).

⇒ Planlegg neste årlige gjennomgang eller iverksett en gjennomgang etter større endringer (f.eks. ny programvare, kontorflytting).

⇒ Eksempel: Angi en årlig kalenderpåminnelse for å gjenta denne prosessen.

2.4 KAPITTEL 4: BRUKERVENNLIGE SIKKERHETSVERKTØY

Brukervennlige sikkerhetsverktøy

Så langt har vi dekket praksis og planlegging. I dette kapitlet fokuserer vi på verktøy og teknologier som kan gjøre det enklere å iverksette sikkerhet. Den gode nyheten er at du ikke trenger å være en teknologisk troldmann eller investere i svært dyre løsninger for å oppnå et solid beskyttelsesnivå. Det finnes mange **brukervennlige og kostnadseffektive verktøy** tilgjengelig – ofte utformet med tanke på ideelle organisasjoner eller små bedrifter – som kan forbedre den digitale sikkerheten din betydelig. Vi skal gå gjennom kategorier av verktøy: identifisering av sikre applikasjoner, hjelpemidler for sikker nettlesing, sikring av skylagring og verktøy for å beskytte datamaskiner og telefoner. Hvert underavsnitt introduserer viktige verktøy eller metoder, med vekt på praktisk anvendelighet og brukervennlighet.

Gjenkjenne sikre applikasjoner

Hvordan vet du hvilke som er «sikre» når det finnes utallige programmer og apper tilgjengelig? Her skisserer vi noen kriterier og eksempler for å hjelpe deg med å velge applikasjoner som prioriterer sikkerhet og personvern.

Hva gjør en applikasjon sikker? En sikker app har vanligvis følgende egenskaper:

- Den kommer fra en anerkjent utvikler eller kilde og vedlikeholdes aktivt (oppdateres jevnlig for å rette feil).
- Den bruker kryptering for å beskytte data under overføring og i hvile (spesielt viktig for kommunikasjons- og lagringsapper).
- Den har god tilgangskontroll (f.eks. tillater sterk autentisering, kanskje 2FA for kontoer).
- Den har en historikk med å reagere på sårbarheter (utviklere utsteder oppdateringer), og har ideelt sett gjennomgått sikkerhetsrevisjoner.
- Appen respekterer personvernet (samler ikke inn for mye data eller viser tvilsomme annonser som kan injisere skadevare).

For eksempel anses meldingsapper som Signal som sikre fordi de er programvare med åpen kildekode (hvem som helst kan inspisere koden for bakdører), bruker ende-til-ende-kryptering som standard og ikke innhenter metadata unødvendig. På den annen side kan noen

gratisapplikasjoner virke praktiske, men være usikre – for eksempel vil en tilfeldig fildelingsapp som ikke er kryptert, eller en passordbehandler uten 2FA-alternativ, være mindre sikre enn alternativene.

Valg av programvare for viktige oppgaver*:* Her er noen vanlige kategorier av applikasjoner med sikre anbefalinger:

***Passordadministrasjon*:** Bruk en dedikert passordadministratorapp som nevnt. Gode alternativer omfatter Bitwarden (åpen kildekode, skybasert, gratis for grunnleggende bruk), LastPass (populært, har et gratis nivå, men hadde et sikkerhetsbrudd i 2022, noe som understreker behovet for å bruke sterke hovedpassord), 1Password (betalt, brukervennlig) eller KeePass (åpen kildekode, frakoblet). Disse har sterk kryptering for å lagre påloggingsopplysningene dine på en sikker måte, og mange støtter 2FA for å låse opp hvelvet. De kan også generere tilfeldige passord for deg. Å bruke en av disse er langt bedre enn å oppbevare passord i et regneark eller bruke dem på nytt.

Sikker meldingstjeneste og e-post: For meldingstjenester, som nevnt: Signal for de sikreste samtalene; WhatsApp er også ende-til-ende-kryptert (og mye brukt – selv om det eies av Meta, har det sterke krypteringsgrunnlag). Wire eller Threema kan være gode for organisasjonsbruk dersom du ønsker en europeisk vertsløsning. Når det gjelder e-post, bør du vurdere leverandører som ProtonMail eller Tutanota dersom du trenger høyere sikkerhet. Disse tilbyr ende-til-ende-kryptering (spesielt for interne e-poster eller e-poster mellom brukere av samme tjeneste). Dersom du holder deg til Gmail eller Outlook.com, er disse rimelig sikre hvis de brukes med 2FA, men sensitive e-poster kan med fordel sendes via en kryptert kanal eller ved hjelp av verktøy som GnuPG/PGP for kryptering (selv om PGP er komplekst i praksis).

Antivirus/anti-skadevare: Bruk kjente, godt anmeldte antivirusløsninger som nevnt. Windows Defender (innebygd i Windows 10/11) er et solid og problemfritt utgangspunkt. Dersom du ønsker en tredjepartsløsning: Avast, AVG, Bitdefender, Kaspersky (vær oppmerksom på at noen har betenkeligheter med Kaspersky på grunn av opprinnelsen, men teknisk sett er de sterke), ESET osv. Mange av disse har gratisversjoner for grunnleggende beskyttelse. Velg et

program som ikke bremser systemet ditt for mye og som har en god deteksjonsrate (uavhengige AV-testlaboratorier kan veilede deg om dette). Hold det oppdatert.

Brannmur og nettverkssikkerhet: For de fleste er den innebygde brannmuren i operativsystemet grei. Hvis du trenger mer kontroll og visuelle signaler (for avanserte brukere), kan verktøy som ZoneAlarm eller TinyWall på Windows tilby brannmuradministrasjon på programnivå i et mer brukervennlig grensesnitt. Sørg for at brannmuren på ruteren er aktivert. Noen sivilsamfunnsorganisasjoner velger maskinvarebrannmurer eller UTM-enheter hvis de har et kontornettverk, men disse kan være komplekse. Ofte fungerer en god ruter (med oppdatert fastvare) som en grunnleggende brannmur. Hvis du driver et nettsted, kan bruk av en tjeneste som Cloudflare eller vertens sikkerhetstillegg gi en brannmur mot nettangrep.

Sikre nettlesere og utvidelser: Bruk en moderne, sikker nettleser (Chrome, Firefox, Edge, Brave). Alle er ganske sikre; Brave er kjent for personverninnstillinger som standard (blokkering av sporere). Firefox er åpen kildekode og svært konfigurerbar med tanke på personvern. Chrome er svært robust når det gjelder sikkerhet (Google Project Zero oppdager sårbarheter og utfører raske oppdateringer), men sender data til Google (selv om det for det meste er ufarlige brukerstatistikker). Edge er også grei (bygget på Chromes motor med Microsofts sikkerhetsfunksjoner). Du kan forbedre enhver nettleser med utvidelser: f.eks. HTTPS Everywhere (nå i stor grad overflødig siden de fleste nettsteder bruker auto-HTTPS, men den sikrer kryptering når det er mulig), uBlock Origin eller Privacy Badger for å blokkere skadelige annonser og sporere (noe som også reduserer risikoen for malvertising), og nettleserens egen popup-blokkering og antiphishing-filter bør være aktivert. Noen bruker NoScript (blokkerer alle skript som standard), men det er avansert og kan ødelegge nettsteder; det er valgfritt for avanserte brukere som er bekymret for skriptbaserte angrep. Sørg for «click-to-play» for Flash/Java (de fleste nettlesere deaktiverer nå Flash helt, noe som er bra).

VPN-tjenester: Hvis teamet ditt ofte bruker offentlig Wi-Fi eller jobber eksternt, kan bruk av VPN øke sikkerheten. En *god* VPN-tjeneste krypterer internettrafikken din og kan forhindre snoking i det lokale nettverket. Den skjuler også IP-adressen din, noe som kan øke personvernet. Bruk imidlertid kun anerkjente betalte/gratis VPN-er (noen gratis VPN-er har blitt tatt i å gjøre det motsatte av personvern – logge eller injisere annonser). Hvis du har IT-

kompetanse, kan du alternativt konfigurere ditt eget VPN på en skyserver for teamet ditt. Enklere: Mange rutere støtter nå opprettelse av et VPN for hjemmekontor, slik at ansatte trygt kan tunnle tilbake til kontornettverket når de er i utlandet.

Verktøy for diskkryptering: I tillegg til operativsystemets innebygde kryptering finnes det verktøy som VeraCrypt (gratis, åpen kildekode og etterfølger til TrueCrypt) som kan opprette krypterte beholdere eller kryptere hele stasjoner. Dette er nyttig hvis du ønsker å kryptere USB-pinner eller opprette en kryptert mappe (beholderfil) som du kan lagre hvor som helst (til og med i skyen) og vite at den er sikker. VeraCrypt er litt teknisk, men godt dokumentert. Det finnes også enklere hvelv-apper for telefoner og datamaskiner som passordbeskytter og krypterer bestemte filer (f.eks. kan 7-Zip opprette krypterte arkiver for filer).

Trygge alternativer og oppdateringer: Som en del av å gjenkjenne sikre apper, innebærer det noen ganger å erstatte en risikabel app med et tryggere alternativ. Hvis noen for eksempel bruker en utdatert versjon av en app som er kjent for å ha sårbarheter (f.eks. et gammelt CMS for et nettsted eller en gammel Adobe Acrobat), bør de oppdatere den eller bytte til alternativer (f.eks. bruke Chromes PDF-visningsprogram eller SumatraPDF i stedet for en gammel Adobe Reader, som var et vanlig mål for skadevare). Bytt ut programvare som har nådd slutten av levetiden (for eksempel Windows 7, som ikke lenger får oppdateringer – oppgrader til Windows 10/11 eller bruk en lettvekts-Linux hvis budsjettet er begrenset).

Mobilapper: På telefoner skal du kun installere apper fra offisielle appbutikker, som nevnt. For sikker kommunikasjon, igjen Signal og WhatsApp (med forsiktighet når det gjelder sikkerhetskopier, siden WhatsApp-sikkerhetskopier i skyen kan være ukrypterte med mindre du velger den nye krypterte sikkerhetskopifunksjonen). For sikker lagring på telefoner kan du bruke innebygde sikre mappefunksjoner (Samsung Secure Folder) eller apper som **KeePassDX** for Android for å administrere passord offline.

Opplæring i verktøy: Det er bare lurt å introdusere nye apper hvis folk bruker dem riktig. En del av innføringen av ethvert verktøy (f.eks. en passordbehandler eller VPN) er derfor å tilby en kort veiledning eller et jukselark. Mange verktøy er intuitive, men innledende

veiledning sikrer riktig bruk (f.eks. å vise hvordan man deler passord på en sikker måte via passordbehandleren i stedet for via e-post).

Ved å velge og bruke sikre applikasjoner nøye reduserer du sårbarheter. Men hold balansen: «Mest sikker» betyr noen ganger mindre brukervennlig, noe som kan føre til løsninger som medfører risiko (hvis for eksempel en sikker meldingsapp er for tungvint, kan de ansatte gå tilbake til å bruke åpen e-post for enkelhets skyld). Velg verktøy som teamet ditt enkelt kan ta i bruk – ofte gir vanlige verktøy som er godt konfigurert, både sikkerhet og brukervennlighet. For eksempel tilbyr Google Workspace eller Microsoft 365, hvis de er konfigurert med 2FA og riktige administratorkontroller, sterk sikkerhet for e-post/dokumenter og er brukervennlige. De er kanskje ikke like låste som noen nisjeløsninger, men hvis folk faktisk følger sikkerhetspraksisen på dem, kan de være tilstrekkelige og enklere å integrere.

I bunn og grunn handler det å gjenkjenne sikre apper om å gjøre litt forarbeid før du installerer noe nytt og velge de som er kjent for sikkerhet. Mange organisasjoner i sivilsamfunnet deler lister over anbefalte verktøy (for eksempel Front Line Defenders' Security-in-a-Box, som tilbyr verktøyveiledninger). I de neste avsnittene skal vi fokusere på spesifikke områder (nettlesing, sky, enheter) med spesielle tips og verktøy for hvert av dem.

Tryggere nettlesing på internett

Nettsurfing er en såpass vanlig aktivitet at det er lett å glemme potensielle farer. Denne delen bygger på praksis for sikker internettbruk fra kapittel 2, og fokuserer nå på verktøy og nettleserinnstillinger som kan gjøre nettsurfing tryggere og mer privat.

Sikkerhetsinnstillinger for nettleseren: Først må du sørge for at du konfigurerer nettleserens innebygde sikkerhetsfunksjoner:

- Hold nettleseren oppdatert (de fleste oppdateres automatisk som standard – ikke deaktiver dette).
- Aktiver beskyttelse mot nettfisking og skadevare (nettlesere som Chrome, Firefox og Edge har dette aktivert som standard. Det sjekker besøkte URL-er mot kjente lister over skadelige nettsteder og viser en stor rød advarsel hvis et nettsted mistenkes for nettfisking eller inneholder skadevare).

- Slå på «Ikke spor» (selv om dette i stor grad er rådgivende, respekterer noen nettsteder det).
- Vurder å bruke nettleserens sandbox- eller nettstedsisolasjonsfunksjoner hvis de er tilgjengelige (Chrome har nettstedsisolasjon for å redusere visse angrep – vanligvis aktivert som standard for høyrisikodomener).
- I Chrome kan du også bruke modusen «Forbedret sikker nettlesing», som deler mer data med Google for forbedret trusselvurdering (valgfritt hvis du stoler på at Google håndterer disse dataene på en trygg måte).

Annonseblokkering og skriptblokkering: Som nevnt skjer mange skadevareinfeksjoner via skadevareannonsering eller skadelige skript på kompromitterte nettsteder. Bruk av en anerkjent annonseblokkerutvidelse som **uBlock Origin** eller **Adblock Plus** bidrar ikke bare til personvern og estetikk, men også til sikkerhet ved å kutte av vanlige leveringsvektorer for skadevare. Disse utvidelsene blokkerer kjente annonsedomener og kan forhindre at mistenkelige skript lastes inn. Personvernorienterte utvidelser som **Privacy Badger** (fra EFF) lærer seg å blokkere sporere og tar ofte livet av skadelig tredjepartsinnhold i prosessen. Hvis du er svært bekymret eller besøker risikable nettsteder, kan **NoScript** (Firefox) eller **ScriptSafe** (Chrome) blokkere alle skript som standard – svært sikkert, men krever manuell hvitelisting for legitim nettstedsfunksjonalitet, noe som kan være tyngende med mindre du er teknisk kyndig. Du kan bruke en enklere tilnærming: **Firefox** i streng Enhanced Tracking Protection-modus, eller **Brave-nettleseren**, som som standard blokkerer mange skript og annonser.

Sikre tilkoblinger og utvidelser: Prøv alltid å bruke HTTPS-versjoner av nettsteder. Utvidelsen *HTTPS Everywhere* (fra EFF) omdirigerer automatisk til HTTPS når det er mulig, selv om de fleste større nettsteder i dag bruker HTTPS som standard uansett. Nettleserens hengelåsikon er din venn – klikk på det for å inspisere sertifikatdetaljer, eller i det minste for å sikre at det er til stede på alle nettsteder der du oppgir passord eller sensitive opplysninger. Hvis du ofte bruker offentlig Wi-Fi, bør du vurdere en utvidelse som **HTTPS Everywhere** (hvis du ikke bruker et VPN) for □□ sikre kryptering, eller bare være årvåken manuelt. Noen moderne nettlesere (Chrome, Firefox) markerer nå sider som ikke er HTTPS og som har skjemaer, som «Ikke sikre» i adresselinjen – vær oppmerksom på denne advarselen.

Søkemotorer og sporing: Google-søk er kraftfullt, men det sporer søk. Dersom du ønsker å unngå målrettede annonser eller profilering, bør du vurdere å bruke **DuckDuckGo** som standard søkemotor. Den sporer ikke søk og gir gode resultater for generelle søk. Den tilbyr også en utvidelse som vurderer nettsteders personvernpraksis og håndhever kryptering. Alternativt gir **Startpage** Google-resultater, men fjerner identifiserende informasjon. Disse kan forbedre personvernet litt uten å ofre mye av søkekvaliteten.

Unngå forgiftede søkeresultater: Noen ganger dukker skadevarenettsteder eller phishing-sider opp i søkeresultatene (f.eks. falske nettsteder for teknisk støtte). Lær opp personalet til å være forsiktige når de klikker på ukjente søkeresultater, og kanskje holde seg til kjente nettsteder for nedlastinger (f.eks. hente programvare fra en offisiell kilde, ikke fra et tilfeldig aggregerende nettsted). Bruk av en utvidelse som **Web of Trust (WOT)** eller **Bitdefender TrafficLight** kan gi omdømmeikoner ved siden av søkeresultatene, som angir om et nettsted anses som trygt av fellesskapet/algoritmen – selv om slike verktøy i seg selv har vært gjenstand for kontroverser (WOT ble funnet skyldig i å innhente brukerdata, så bruk det med forsiktighet).

Privat nettlesermodus: Bruk «Inkognito»- eller privat modus i nettlesere når det er hensiktsmessig – det gjør deg ikke anonym på internett, men det lagrer ikke informasjonskapsler, historikk eller hurtigbuffer etter at du har lukket den. Dette er nyttig hvis du logger på en tjeneste på en delt datamaskin, eller hvis du bare ønsker å sikre at det ikke blir igjen spor etter en bestemt økt (for eksempel når du tester hvordan nettstedet ditt vises for en ny bruker). Merk: Dette er ikke et sikkerhetsverktøy i seg selv mot eksterne trusler, men det kan hindre andre brukere av samme datamaskin i å snoke på øktene dine.

Tor-nettleser for anonym nettlesing: I situasjoner der du trenger et høyt anonymitetsnivå eller for å omgå lokal internett-sensur, er **Tor-nettleseren** et verktøy du bør vurdere. Den dirigerer trafikken din gjennom Tor-nettverket, skjuler IP-adressen din og krypterer trafikken i nettverket (selv om trafikken går ut til destinasjonen ukryptert med mindre du bruker HTTPS). Sivilsamfunnsorganisasjoner, journalister og aktivister bruker av og til Tor for å få tilgang til blokkerte nettsteder eller unngå overvåking. Ulempen er at den er tregere, og at noen nettsteder blokkerer Tor-utgangsnoder. Men den kan være en del av verktøykassen din i

undertrykkende miljøer eller for sensitiv forskning. Bruk kun den offisielle Tor-nettleseren fra torproject.org og forstå retningslinjene for bruk (f.eks. ikke installer ekstra nettleserprogramtillegg i Tor-nettleseren, ikke åpne dokumenter mens du er tilkoblet, da de kan omgå Tor osv.). Hvis det ikke er nødvendig i din kontekst, kan en godt konfigurert vanlig nettleser med et VPN være tilstrekkelig.

Hensyn ved valg av nettleser: Bruk av flere forskjellige nettlesere kan noen ganger isolere aktiviteter. Du kan for eksempel bruke én nettleser utelukkende til å logge på sensitive kontoer (og med minimale utvidelser, kun sikkerhetsutvidelser), og en annen til vanlig surfing på nettet. På den måten kan den vanlige nettleseren ha alle de eksperimentelle utvidelsene eller av og til besøke mindre sikre nettsteder, mens du behandler den «sikre nettleseren» (f.eks. Firefox) med forsiktighet (ingen unødvendige utvidelser, strenge innstillinger, kun besøk på kjente nettsteder som banken din, e-post osv.). Dette begrenser eksponeringen av kritiske øktinformasjonskapsler eller -data.

E-post-/nettintegrasjon: Mange moderne e-posttjenester åpner lenker eller vedlegg i en form for sandkasse eller sikker visning (Google har «Beskyttet visning» for vedlegg, Outlook Web har sikre lenker hvis dette er aktivert av administratorer). Hvis du har disse funksjonene, bør du la dem være på. De legger til et ekstra lag og åpner innhold i et kontrollert miljø.

Hold plugins og tillegg oppdatert eller fjern dem: Nettleserplugins som Flash eller Java bør, som nevnt, avinstalleres om mulig. De fleste nettsteder trenger dem ikke lenger. Hvis du absolutt trenger Flash eller andre av en eller annen grunn, kan du angi dem til «Be om å aktivere» slik at de ikke kjører automatisk. Fjern alle ubrukte nettleserutvidelser. Behold kun de du stoler på og trenger, siden skadelige eller kompromitterte utvidelser kan kapre nettlesingen.

Bokmerke pålitelige nettsteder: Oppfordre til bruk av bokmerker/favoritter for viktige nettsteder (for eksempel påloggingsinformasjon til donasjonsplattformen din eller offentlige portaler som sivilsamfunnsorganisasjonen din bruker). Dette bidrar til å unngå skrivefeil (at man ved et uhell går til yourbank-secure.com i stedet for yourbank.com). Det gjør det også raskere å gjenkjenne nettstedet – brukerne klikker på det kjente bokmerket i stedet for å skrive inn nettadressen på nytt eller google nettstedet hver gang (noe som kan lede dem på villspor).

Opplæring om popup-vinduer og svindel: Intet verktøy stopper svindel fullstendig, for eksempel popup-vinduer fra «teknisk støtte» som sier: «Du har et virus, ring dette nummeret.» Vær derfor oppmerksom: Hvis et slikt popup-vindu dukker opp, eller en nedlasting plutselig starter, må du lukke nettleseren eller fanen. Moderne nettlesere blokkerer de fleste popup-vinduer, men noen annonser simulerer dem. Bruk av en annonseblokkering eliminerer for det meste disse. Moderne operativsystemer er også smarte: Windows 10s SmartScreen blokkerer ofte kjente skadelige nedlastinger eller advarer deg hvis en app ikke lastes ned ofte.

Ved å kombinere disse verktøyene og innstillingene blir den daglige nettlesingen betydelig tryggere. Målet er et lagdelt forsvar – ett utvidelse kan blokkere en skadelig annonse, nettleseren kan advare om et villedende nettsted, og forsiktigheten din gjør resten. Hvis noe slipper gjennom, kan antivirusprogrammet oppdage det ved nedlasting. Ingen enkeltlag er idiotsikre, men til sammen reduserer de risikoen betraktelig.

Skylagring: Google Drive, Dropbox og sikkerheten deres

Skylagringstjenester som Google Drive, Dropbox, Microsoft OneDrive og andre har revolusjonert måten sivilsamfunnsorganisasjoner samarbeider og lagrer data på. De tilbyr bekvemmelighet og sikkerhetskopiering som standard, men de medfører også sikkerhetshensyn. Denne delen forklarer hvordan du bruker disse tjenestene på en sikker måte.

Tilgangskontroll og delingsinnstillinger: En av de største risikoene med skylagring er utilsiktet overdeling. Dobbeltsjekk alltid hvordan du deler filer eller mapper. Som standard bør du holde dokumenter private for organisasjonen din eller bestemte brukere. Google Drive tillater for eksempel deling med «Alle med koblingen» – bruk dette kun når det er nødvendig, og vurder å legge til et passord eller en utløpsdato (Google tilbyr ikke passord på koblinger, men OneDrive for Business og Dropbox gjør det for betalte kontoer). Velg i stedet å dele med bestemte personers e-postadresser (de må logge på, noe som er sikrere). Både Dropbox og Google viser ikoner som angir om en mappe er delt – gjør deg kjent med disse indikatorene og kontroller dem med jevne mellomrom. Googles **«Delt med meg»** -del og Dropbox' liste over delte mapper kan bidra til å gjennomgå hva som er åpent.

Hvis sivilsamfunnsorganisasjonen din bruker G Suite/Google Workspace eller Microsoft 365, kan du dra nytte av administrative innstillinger: Du kan begrense ekstern deling eller i det minste

overvåke den. Du kan kanskje begrense hvem som kan dele eksternt, eller angi en standardinnstilling der deling av lenker utenfor organisasjonen er deaktivert. På den måten må en ansatt bevisst overstyre innstillingen for å dele offentlig. Hvis du bruker en personlig/kostnadsfri Google-konto, må du være ekstra forsiktig, siden disse mangler administratorovervåking, og man kan utilsiktet eksponere en fil for hele verden.

Aktiver tofaktorautentisering på skytjenestekontoer: Vi har gjentatte ganger lagt vekt på 2FA, og det er avgjørende for skylagring, siden et brudd på kontoen din kan avsløre store mengder data. Google, Dropbox, Microsoft, Box osv. støtter alle 2FA (vanligvis via autentiseringsapper eller SMS). Sørg for at alle brukere i teamet ditt med tilgang gjør dette. Mange datainnbrudd skjer fordi påloggingsopplysninger blir stjålet, men 2FA vil stoppe angriperen.

Enhetsadministrasjon og fjernsletting: Bruk alternativene for å administrere enheter. For eksempel lister Dropbox og OneDrive opp alle tilkoblede enheter (datamaskiner, telefoner). Hvis en enhet går tapt eller noen slutter, kan du fjerne koblingen eksternt og, i Dropbox' tilfelle, til og med slette filer som var angitt som lokale eksternt. Google Drive (Backup and Sync eller den nye Drive for skrivebord) sletter ikke helt lokale filer fordi de vanligvis bare befinner seg i en hurtigbuffer, men det er fortsatt viktig å tilbakekalle tilgangen. Googles administrasjonspanel (for Workspace) kan slette data fra en brukers Drive på en mobilenhet hvis du konfigurerer enhetsadministrasjon. Selv om du ikke kan automatisk slette, bidrar endring av passord og utlogging fra alle økter (vanligvis en kontosikkerhetsinnstilling) til å sikre at en tapt bærbar PC ikke kan synkronisere nye data, eller at kontoen ikke kan åpnes.

Kryptering av sensitive data: Som nevnt tidligere krypterer disse tjenestene data på serverne sine, men de oppbevarer nøklene (bortsett fra visse produkter som MEGA eller SpiderOak, som er ende-til-ende-krypterte, men mindre vanlige). Hvis du har spesielt sensitive data som du legger inn i Google Drive eller Dropbox, kan du legge til ditt eget krypteringslag. Alternativer:

- Bruk verktøy som **VeraCrypt** til å opprette en kryptert beholder og lagre denne filen på Drive/Dropbox. Du trenger da VeraCrypt for å åpne den med passordet.

Ulemper: Hele beholderen må synkroniseres på nytt når den endres, og samtidig samarbeid inne i den er ikke enkelt.

- Bruk **7-Zip** eller **WinZip** til å kryptere bestemte filer før opplasting dersom du planlegger å dele dem eksternt. Bruk et sterkt passord og del dette passordet via en annen kanal.
- Noen skytjenester tilbyr et kryptert «hvelv» eller «skap» som en funksjon (f.eks. har Dropbox Professional et hvelv). Kjenn til verktøyets funksjoner.
- Hvis du bruker Office 365, kan du bruke sensitivitetsetiketter som krypterer filer slik at bare visse kontoer kan åpne dem (dette er imidlertid en mer avansert bedriftsfunksjon).
- Hvis du bruker Google, bør du unngå å legge inn ekstremt sensitivt innhold i Google Docs-tekst med mindre det er nødvendig, siden Google teknisk sett kan få tilgang til det. Du kan kanskje bruke krypterte formater offline og bare lagre dem der, eller bruke noe som **Cryptomator** – et verktøy utformet for å kryptere filer på klientsiden før synkronisering til skyen (det oppretter en virtuell stasjon; filer som plasseres der, krypteres og synkroniseres deretter). Cryptomator fungerer bra med Dropbox, Google Drive osv., og krever ikke spesiell serverprogramvare (skyen ser bare uforståelige filer). For en sivilsamfunnsorganisasjon som håndterer svært konfidensiell informasjon, kan det være verdt å implementere dette for en del av dataene.

Overvåking og varsler: Noen tjenester tillater overvåking av aktivitet. For eksempel viser Dropbox en logg over delingshendelser og påloggінger på kontosiden. Google Workspace-administratoren kan konfigurere varsler for ting som «fil delt eksternt» eller «mistenkelig påloggingsforsøk». Hvis disse er tilgjengelige, bør du konfigurere dem. Selv på personlige kontoer varsler Google Account Security deg om påloggінger fra nye enheter – vær oppmerksom på disse e-postene eller meldingene («Logget du nettopp på fra enheten X?»).

Opplys om sosial manipulering: Angripere hacker kanskje ikke Google direkte, men de kan utøve phishing mot deg. Et eksempel: Du mottar en e-post som ser ut til å være en Google Drive-deling fra en kollega, men det er faktisk en smart forkledd phishing-lenke som fører til en

falsk Google-pålogging. Phishing via Google Drive er en kjent taktikk – fordi folk stoler på e-poster med deling fra Drive/Docs. Verifiser derfor uventede delinger før du logger på via dem. Google har forbedret seg ved å legge til sikkerhetsskanninger i Docs, men det er nødvendig å være forsiktig. På samme måte må du ikke oppgi skypassordet ditt i et uventet popup-vindu – det er bedre å gå til drive.google.com manuelt hvis du blir bedt om det.

Versjonshistorikk og beskyttelse mot løsepengevirus: En fordel med skylagring er versjonshistorikk. Dersom løsepengevirus krypterer de lokale filene dine og de synkroniseres til skyen som uleselig innhold, oppbevarer tjenester som Dropbox og OneDrive eldre versjoner i noen dager. Du kan gjenopprette tidligere versjoner av mange filer (Dropbox Pro har til og med et utvidet versjonshistorikkalternativ). Gjør deg kjent med denne prosessen. OneDrive (bedrifter) har også en «Gjenopprett alle filer til et tidligere tidspunkt»-funksjon for å gjenopprette alle filer etter en løsepengevarehendelse. Vit at den finnes, men forebygging er nøkkelen til å unngå å trenge den.

Bruk av organisasjonskontoer vs. personlige kontoer: Hvis det er mulig, bør du bruke en organisasjonsadministrert konto til skylagring i stedet for en rekke personlige kontoer. Med Google Workspace for ideelle organisasjoner (som ofte er gratis/rabattert for sivilsamfunnsorganisasjoner) får du for eksempel administrerte kontoer (som [navn]@CSO.org) med Drive. På den måten kan dataene eies av organisasjonen, og du kan kontrollere dem hvis noen slutter. Personlige kontoer knytter data til enkeltpersoner, noe som kan bli komplisert hvis personen forlater organisasjonen. Google Workspace og Microsoft 365 for organisasjoner har dessuten bedre sikkerhetskontroller som standard enn gratis kontoer. Se på disse tilbudene for ideelle organisasjoner (Google for ideelle organisasjoner, Microsoft for ideelle organisasjoner), siden de kan øke sikkerheten (og samarbeidet) betydelig til lav eller ingen kostnad.

Regelmessige revisjoner: Sett av tid, kanskje kvartalsvis eller halvårlig, til å revidere skystasjonene dine. Fjern gamle data du ikke lenger trenger (reduserer eksponering). Kontroller delingsinnstillingene for kritiske mapper. Fjern tilgang for brukere som ikke lenger trenger den. Dette vedlikeholdet sikrer at skymiljøet ditt holder seg ryddig og sikkert.

Oppsummert kan tjenester som Google Drive og Dropbox være trygge for sivilsamfunnsorganisasjoner hvis de brukes med omhu: Beskytt kontoer med sterk

autentisering, konfigurer deling med omhu og kanskje legg til ekstra kryptering for svært sensitive filer. Fordelene med hensyn til bekvemmelighet og samarbeid er enorme, så det handler i hovedsak om å utnytte verktøyenes sikkerhetsfunksjoner fullt ut. De fleste hendelsene på disse plattformene skjer på grunn av menneskelige feil (for eksempel å dele en lenke offentlig ved en feiltakelse eller bruke et svakt passord) i stedet for at leverandørene blir hacket. Ved å ta hånd om disse menneskelige faktorene og de tekniske innstillingene, kan du trygt benytte deg av skyen.

Beskyttelse av telefonen og datamaskinen

I tidligere avsnitt diskuterte vi generell sikkerhetspraksis for enheter. Her skal vi se nærmere på noen spesifikke verktøy og innstillinger for å sikre datamaskinene og de mobile enhetene dine ytterligere, siden det er fra disse enhetene du får tilgang til alle de digitale ressursene dine.

f Sørg for at FDE er aktivert på alle bærbare datamaskiner og mobile enheter. På moderne datamaskiner krever dette ofte bare at du slår den på:

- Windows 10/11: Bruk **BitLocker** (på Pro-utgaver) eller enhetskryptering i Home (hvis tilgjengelig). Når den er slått på, krypterer den hele stasjonen og knytter dekrypteringen til passordet/PIN-koden din (og TPM-brikken). BitLocker kan også kryptere USB-minnepinner (du kan bruke BitLocker To Go til det).
- macOS: Slå på **FileVault** i sikkerhetsinnstillingene – det tar bare ett klikk å kryptere Mac-disken.
- Linux: Hvis du bruker Linux, installer med LUKS-kryptering aktivert eller bruk et verktøy som cryptsetup. Mange brukervennlige distribusjoner gjør det mulig å aktivere kryptering under installasjonen.
- Android: De fleste moderne Android-enheter krypterer lagringsplassen som standard (spesielt fra og med Android 7.0 og nyere). Bare sørg for at du angir en sterk PIN-kode / et sterkt passord / et sterkt mønster, fordi krypteringen er bare like sterk som låseskjermen.
- iPhone/iPad: Disse enhetene blir automatisk maskinvarekryptert så lenge du angir en passkode. Bruk derfor alltid en passkode (og Touch/Face ID for enkelhets skyld, men disse er låst til passkoden som sikkerhetskopi).

Sikkerhetsapper for mobilenheter: For Android bør du vurdere å installere en anerkjent sikkerhetsapp. Alternativer: **Google Play Protect** er innebygd og skanner apper (sørg for at dette er aktivert i Play Store-innstillingene). Tredjeparts antivirusprogrammer som **Avast Mobile**, **Bitdefender Mobile** eller **Lookout** kan legge til beskyttelse mot nettfisking og funksjoner for å finne telefonen. De kan også skanne etter skadelige apper utover det Play Protect finner (selv om Googles er ganske bra). For iOS er det mindre behov for separate sikkerhetsapper på grunn av sandboxing (selv om apper som Lookout kan hjelpe deg med å finne telefonen eller sjekke om iOS-enheten din er jailbreaket).

***Finn enheten min*:** Aktiver alltid tjenester for å finne og slette innhold eksternt:

- Android: Bruk **Find My Device** (en Google-tjeneste) – den er vanligvis aktivert hvis du har en Google-konto på telefonen. Test den (Google «find my device» og se om telefonen din blir funnet).
- Samsung-enheter har også **Find My Mobile,** som kan være et alternativ med flere funksjoner.
- iPhone: Sørg for **at «Find My iPhone**» er aktivert (i iCloud-innstillingene). Dette gjør at du kan finne eller slette en tapt telefon.
- Bærbare datamaskiner: Vurder en sporingsprogramvare for bærbare datamaskiner dersom tyveri er et problem. PreyProject (Prey) har et gratis abonnement for opptil tre enheter og kan hjelpe deg med å finne en mistet/stjålet bærbar PC og til og med ta bilder eller sende meldinger. Noen bærbare datamaskiner for bedrifter har innebygd tyverisikring (som Computrace/LoJack). Men selv uten spesialprogramvare bør du, hvis en bærbar PC mistes, umiddelbart endre passordene til kontoene den hadde tilgang til, og hvis den var kryptert, vet du i det minste at dataene er trygge.

Brannmur på datamaskiner: Windows-brannmuren er aktivert som standard – la den være aktivert. Den gjør jobben sin i det stille og blokkerer uønsket innkommende trafikk. Du kan også bruke den til å blokkere utgående trafikk fra bestemte apper om nødvendig (mindre vanlig i CSO-sammenheng). På Mac slår du på brannmuren i Sikkerhetsinnstillinger. Du trenger sannsynligvis ikke brannmurprogramvare fra tredjeparter. De innebygde programmene er gode

nok, og du unngår forvirrende meldinger som mindre teknisk kyndige kanskje bare tillater uansett.

Firmware- og BIOS-sikkerhet: For behov med høyt sikkerhetsnivå bør du vurdere å angi et BIOS/UEFI-passord på bærbare datamaskiner (slik at oppstart fra eksterne medier eller endring av oppstartsinnstillinger krever et passord). Aktiver også sikker oppstart (for å forhindre rootkits). Disse trinnene hindrer en angriper med fysisk tilgang i å for eksempel starte et live-operativsystem for å omgå systemsikkerheten din. Når det er sagt, hvis du har FDE og et sterkt passord, bør de uansett ikke komme seg inn. Men et BIOS-passord legger til et lag mot manipulering eller bruk av maskinen.

Automatisering av enhetsoppdateringer: Vi snakket om operativsystemoppdateringer, men i tillegg:

- Hold apper oppdaterte, f.eks. ved å sørge for at Microsoft Office eller LibreOffice er oppdatert (Office oppdateres vanligvis automatisk via Office 365 hvis du har det, ellers kan du sjekke Windows Update eller Offices oppdatering).
- PDF-leser: Hvis du bruker Acrobat Reader, må du oppdatere den. Eller bruk en tryggere leser som **SumatraPDF** eller nettleserens PDF-visningsprogram, som er enklere og mindre utsatt for angrep.
- Java: Hvis du må ha det, må du konfigurere det til å oppdateres automatisk. Hvis du ikke trenger det, kan du avinstallere det helt.
- På telefoner bør du oppdatere apper via Play Store/App Store når oppdateringer er tilgjengelige (aktiver automatisk oppdatering på Wi-Fi for å gjøre det enkelt).

Deaktiver unødvendige funksjoner: Ubrukte åpne dører kan lukkes:

- Hvis du ikke trenger funksjoner som RDP (Remote Desktop) eller fildeling på Windows, kan du slå dem av for å redusere angrepsflaten.
- På telefoner bør du være oppmerksom på Bluetooth og NFC – hold dem av når de ikke er i bruk (Bluetooth-angrep er mindre vanlige nå med oppdateringer, men det er fortsatt god hygiene, spesielt på offentlige steder).

- Fjern bloatware-apper på telefoner du ikke bruker, spesielt de som kan kjøre i bakgrunnen eller har tillatelser (noen Android-telefoner leveres med forhåndsinstallerte apper som kan utføre datainnsamling).
- På alle systemer skal du ikke logge på som administrator ved daglig bruk. Ha en standard brukerkonto for rutinearbeid og en administratorkonto for installasjon av programvare. På denne måten kan det hende at skadevare ikke har administratorrettigheter til å foreta omfattende endringer hvis den kjører. Riktignok er det mange som ignorerer dette, men det er en anbefalt praksis på Windows og Linux. På Mac er den første brukeren administrator, men Mac ber om passordeskalering, som fungerer på samme måte som å skille privilegier.

Bruk en god sikkerhetsprogramvarepakke: Dersom budsjettet tillater det eller gratis alternativer er tilstrekkelige, bør du bruke en godt utformet sikkerhetspakke. For eksempel inneholder **Microsoft Defender** faktisk ikke bare anti-skadevare, men også kontrollert mappe tilgang (ransomware-beskyttelse som hindrer ukjente apper i å redigere dokumentene dine), og skybasert beskyttelse hvis den er slått på. Tredjepartspakker kan omfatte passordbehandler, VPN-prøveversjon osv. Invester bare hvis du trenger disse tilleggene – ellers fungerer lagdelte individuelle verktøy.

E-postsikkerhet på enheten: Hvis du bruker en e-postklient som Outlook eller Thunderbird, må du sørge for at den er oppdatert. Vær forsiktig med hvilke vedlegg du åpner. Moderne e-postklienter har en viss grad av sandboxing (Outlook laster for eksempel ikke inn bilder eller kjører makroer som standard, og advarer hvis en app prøver å få tilgang til e-postdata). Ikke aktiver «tillat programmatisk tilgang» med mindre det er nødvendig for en integrasjon.

Fysisk beskyttelse: Bærbare datamaskiner – vurder å bruke en Kensington-låsekabel hvis du lar den stå på et delt sted (for å avskrekke fra opportunistisk tyveri). For telefoner bør du bruke beskyttelsesetui og kanskje personvernskjermbeskyttere hvis du håndterer sensitive opplysninger på dem offentlig (forhindrer skuldersurfing).

Sikkerhetskopiering av data for enheter: Vi snakket om sikkerhetskopiering, men ett aspekt: For mobile enheter bør du også sikkerhetskopiere dataene dine (skysikkerhetskopiering eller manuelt). For iPhone-er kan du bruke iCloud eller lokale iTunes-sikkerhetskopier. For Android kan du bruke Googles sikkerhetstjenester eller apper for kritiske data. På den måten betyr ikke en tapt enhet tapte data, og du kan slette innholdet eksternt uten å nøle, vel vitende om at det er lagret.

Tyverisikringsmerking: Noen ganger er de enkleste løsningene de beste: Merk enhetene dine med kontaktinformasjon. En person som finner en tapt enhet, kan returnere den hvis det er enkelt (for eksempel et klistremerke med teksten «Ring [CSO-nummer] hvis du finner denne»). Dette er mer et tips for gjenfinning enn sikkerhet, men det kan redde dagen.

Plan for utskifting av enheter: Ha en enkel plan for tilfeller der en enhet er kompromittert eller utdatert. Hvis for eksempel en datamaskin ikke lenger mottar oppdateringer (Windows 7, gammel Android), bør du fase den ut eller isolere den fra sensitive oppgaver. Kanskje du kan bruke den frakoblet hvis det er nødvendig for noe eldre. Men invester i å holde maskinvaren innenfor den støttede levetiden av sikkerhetshensyn.

Ved å bruke metodene og verktøyene ovenfor på telefonene og datamaskinene dine, skaper du et sterkt forsvarsområde rundt person- og arbeidsdataene dine. Tenk på enheten din som et sikkert hvelv: Du har låst den (sterk pålogging), alarmert den (antivirus og brannmur), forsterket den (oppdateringer og kryptering) og konfigurert en måte å finne eller ødelegge innhold på hvis den blir stjålet (finn enheten min, fjernsletting). Med slike tiltak kan du, selv om det oppstår trusler, enten blokkere dem eller være forberedt på å reagere uten katastrofale tap.

Dette avslutter kapitlet om verktøy. Ved å ta i bruk sikre applikasjoner (4.1), praktisere sikker surfing på nettet (4.2), bruke skylagring på riktig måte (4.3) og styrke enhetene (4.4), vil organisasjonen din ha en mye sterkere digital sikkerhetsposisjon. I neste omgang skal vi se på hva du skal gjøre hvis det til tross for alt dette oppstår et cyberproblem – siden ingen forsvar er 100 % perfekte, er det avgjørende å ha en beredskapsplan.

Kapittelsammendrag

Kapittel 4 fokuserer på å sikre teknologien som sivilsamfunnsorganisasjoner er avhengige av, inkludert datamaskiner, nettverk og nettsteder. Det anbefales å holde programvaren oppdatert

for å rette opp sårbarheter, bruke antivirusverktøy (f.eks. Avast Free) for å bekjempe skadevare og sikre Wi-Fi med WPA2/WPA3-kryptering. For nettsteder anbefales det å aktivere HTTPS, ta regelmessige sikkerhetskopier og oppdatere innholdsstyringssystemer (f.eks. WordPress) for å forhindre skade eller DDoS-angrep. En casestudie av en sivilsamfunnsorganisasjons nettsted som omdirigeres til et tredjepartsnettsted på grunn av utdatert programvare, illustrerer risikoene. Kapitlet fremmer VPN-er (f.eks. ProtonVPN) for sikre tilkoblinger på offentlig Wi-Fi, noe som er avgjørende for feltpersonell. Det legger vekt på rimelige løsninger, som gratis HTTPS via Let's Encrypt, som passer budsjettene til sivilsamfunnsorganisasjoner. Ikke-teknisk personale veiledes til å verifisere innstillinger (f.eks. sjekke om det finnes HTTPS-hengelåser) uten å trenge IT-ekspertise. Kapitlet omhandler også enhetskryptering og sterke passord for å beskytte mot tyveri eller tap. Ved å sikre infrastrukturen forhindrer sivilsamfunnsorganisasjoner forstyrrelser og datainnbrudd, og sikrer dermed kontinuitet i oppdraget. Kapittelets praktiske trinn, som å planlegge automatiske oppdateringer, gjør implementeringen enkel, i tråd med e-bokens mål om tilgjengelig cybersikkerhet.

Sjekkliste for sikkerhet på sosiale medier for organisasjoner i sivilsamfunnet

Denne sjekklisten hjelper organisasjoner med å sikre kontoene sine på sosiale medier (f.eks. Twitter/X, Facebook, Instagram) for å beskytte tilstedeværelsen og omdømmet sitt på nettet mot kapring, feilinformasjon eller uautorisert tilgang. Disse trinnene er utformet for programansatte og frivillige med minimal teknisk ekspertise, og kan fullføres på én eller to timer. Gjennomgå hvert punkt og kryss av for fullførte oppgaver. Hvis du er usikker, kan du be sosiale medier-ansvarlig, IT-kontakten eller plattformstøtten om hjelp. Del funnene med teamet ditt for å opprettholde en sikker tilstedeværelse på nettet.

1. Aktiver tofaktorautentisering (2FA)

⇒ Aktiver 2FA for alle sosiale mediekontoer for å kreve et andre verifiseringstrinn (f.eks. en kode sendt til telefonen eller appen din).

⇒ Plattformtips:

- Twitter/X: Gå til Innstillinger > Personvern og sikkerhet > Tofaktorautentisering. Velg en autentiseringsapp (f.eks. Google Authenticator) eller SMS.
- Facebook: Gå til Innstillinger > Sikkerhet og pålogging > Tofaktorautentisering. Velg en autentiseringsapp eller tekstmelding.
- Instagram: Gå til Innstillinger > Sikkerhet > Tofaktorautentisering. Aktiver appbasert autentisering eller SMS-autentisering.

⇒ Eksempel: En hacket CSO-Twitter-konto la ut falske meldinger. 2FA forhindret ytterligere uautorisert tilgang.

⇒ Logg inn på hver konto, aktiver 2FA og test den med teamets enheter.

2. Bruk sterke, unike passord

⇒ Oppdater passordene til minst 14 tegn, og bland bokstaver, tall og symboler (f.eks. «sunbird&glass7rain»). Bruk et forskjellig passord for hver konto.

⇒ Vurder en gratis passordbehandler (f.eks. Bitwarden) for å lagre passord på en sikker måte.

⇒ Plattformtips:

- Twitter/X: Oppdater under Innstillinger > Endre passord. Unngå å bruke passord fra andre plattformer på nytt.
- Facebook: Gå til Innstillinger > Sikkerhet og pålogging > Endre passord. Sørg for at det er unikt i forhold til e-postkontoen eller andre kontoer.
- Instagram: Gå til Innstillinger > Sikkerhet > Passord. Bruk en passfrase for å gjøre det enklere å huske det.

⇒ Eksempel: En sivilsamfunnsorganisasjons Instagram-konto ble kompromittert på grunn av et gjenbrukt e-postpassord. Et unikt passord løste problemet.

⇒ Endre passord for alle kontoer og lagre dem i en passordbehandler.

3. Fjern ubrukte administratorkontoer

⇒ Sjekk hvem som har administrator- eller redigerer-tilgang til de sosiale mediekontoene dine, og fjern tidligere ansatte, frivillige eller inaktive brukere.

⇒ Plattformtips:

- Twitter/X: Gå til Innstillinger > Kreatørabonnementer > Administrer team for å gjennomgå og fjerne administratorer.
- Facebook: Gå til Sideinnstillinger > Sidroller for å se og slette unødvendige administratorer eller redigerere.
- Instagram: Gå til Innstillinger > Autoriserte apper eller Bedriftsinnstillinger > Brukere for å tilbakekalle tilgang for ubrukte kontoer.

⇒ Eksempel: En tidligere frivilligs administratortilgang ble brukt til å legge ut uautorisert innhold. Fjerning av gamle administratorer forhindret at det skjedde på nytt.

⇒ Spør den sosiale medieansvarlige: «Kan vi gjennomgå og fjerne utdaterte administratorkontoer?»

4. Konfigurer og verifiser e-postadresse/telefonnummer for gjenoppretting

⇒ Sørg for at hver konto har en oppdatert e-postadresse eller et telefonnummer for gjenoppretting som kontrolleres av betrodde medarbeidere, slik at kontoen kan gjenopprettes dersom den blir låst ute eller hacket.

- Plattformtips:
    - Twitter/X: Oppdater under Innstillinger > Kontoen din > Kontoinformasjon. Bekreft at e-postadressen for gjenoppretting er aktiv.
    - Facebook: Gå til Innstillinger > Sikkerhet og pålogging > Kontakt for å legge til eller oppdatere en e-postadresse/et telefonnummer for gjenoppretting.
    - Instagram: Gå til Innstillinger > Sikkerhet > Kontogjenoppretting for å bekrefte en gyldig e-postadresse eller et gyldig telefonnummer.

⇒ Eksempel: En sivilsamfunnsorganisasjon fikk tilbake en hacket Facebook-konto ved hjelp av en e-postadresse for gjenoppretting. Uten den tok gjenopprettingen flere uker.

⇒ Legg til eller oppdater gjenopprettingsopplysninger og test ved å be om en gjenopprettingskode.

5. Overvåk kontoaktivitet

⇒ Kontroller jevnlig om det forekommer uvanlig aktivitet (f.eks. innlegg du ikke har opprettet, påloginger fra ukjente steder).

⇒ Aktiver påloggingsvarsler der det er mulig for å motta varsler om mistenkelig aktivitet.

⇒ Plattformtips:

- Twitter/X: Sjekk Innstillinger > Personvern og sikkerhet > Tilkoblede kontoer for ukjente enheter eller apper.
- Facebook: Gå til Innstillinger > Sikkerhet og pålogging > Hvor du er logget på for å gjennomgå aktive økter. Aktiver påloggingsvarsler.
- Instagram: Gå til Innstillinger > Sikkerhet > Påloggingsaktivitet for å se påloggingssteder og aktivere varslinger.

⇒ Eksempel: En sivilsamfunnsorganisasjon oppdaget en pålogging fra et annet land og låste kontoen før det oppstod skade.

⇒ Gjennomgå aktivitetslogger ukentlig og rapporter mistenkelig atferd til plattformens brukerstøtte.

6. Begrens tilgang for tredjepartsapper

⇒ Fjern tilgang for tredjepartsapper eller -verktøy (f.eks. planleggingsverktøy, analyseapper) som ikke lenger er i bruk eller som ikke er pålitelige.

⇒ Plattformtips:

- Twitter/X: Gå til Innstillinger > Personvern og sikkerhet > Tilkoblede kontoer for å trekke tilbake apptillatelser.
- Facebook: Gå til Innstillinger > Apper og nettsteder for å fjerne ubrukte eller mistenkelige apper.
- Instagram: Gå til Innstillinger > Sikkerhet > Apper og nettsteder for å trekke tilbake tilgang for unødvendige apper.

⇒ Eksempel: En planleggingsapp med utdatert tilgang ble brukt til å legge ut søppelpost på en sivilsamfunnsorganisasjons Twitter-konto. Å tilbakekalle tilgangen løste problemet.

⇒ Gjennomgå og fjern unødvendige app-tilkoblinger i kontoinnstillingene.

7. Opplær personalet i sikker bruk av sosiale medier

⇒ Minn ansatte og frivillige på at de ikke skal dele kontoopplysninger, klikke på mistenkelige lenker eller legge ut sensitive opplysninger (f.eks. giverinformasjon) på sosiale medier.

⇒ Del et tips: «Logg ut av kontoer på delte eller offentlige enheter.»

⇒ Eksempel: En frivillig la ut sensitive kampanjeopplysninger i et offentlig Instagram-innlegg. Opplæring forhindret fremtidige feil.

⇒ Send en e-post til teamet: «Del aldri påloggingsinformasjon for sosiale medier. Logg ut etter bruk på delte enheter.»

8. Plan for feilinformasjon eller kapring

⇒ Utvikle en enkel responsplan for hackete kontoer eller feilinformasjon (f.eks. plattformrapport, publiser en avklaring til følgere).

⇒ Ha et utkast til uttalelse klart: «Kontoen vår ble kompromittert. Vennligst se bort fra de siste innleggene. Vi holder på å løse dette.»

⇒ Plattformtips:

- Twitter/X: Rapporter hacking via help.twitter.com/forms/security.
- Facebook: Bruk facebook.com/hacked til å rapportere kompromitterte kontoer.
- Instagram: Rapporter problemer via Innstillinger > Hjelp > Rapporter en hacket konto.

⇒ Eksempel: En sivilsamfunnsorganisasjon avklarte raskt et hacket innlegg på Facebook, og reduserte dermed spredningen av feilinformasjon.

⇒ Utarbeid en svarerklæring og lagre lenker til plattformstøtte for rask tilgang.

KAPITTEL 5: EKSEMPLER PÅ SITUASJONER MED CYBERSIKKERHETSHENDELSER

Dette skal du gjøre hvis du opplever en cyberhendelse

Til tross for en stor innsats for å forebygge, kan hendelser likevel inntreffe. En rask, rolig og metodisk respons kan redusere skadene forårsaket av en cyberhendelse betydelig. Dette kapitlet veileder deg gjennom å gjenkjenne tegn på en hendelse, umiddelbare tiltak som skal iverksettes, hvem du skal kontakte for å få hjelp og hvordan du kan gjenopprette sikkerheten etterpå. I bunn og grunn er det din beredskapsplan for den digitale verden.

Gjenkjenne tegnene på et cyberangrep

Jo tidligere du innser at noe er galt, jo raskere kan du reagere. Cyberangrep kan manifestere seg på ulike måter – noen åpenbare, andre mer subtile. Her er vanlige faresignaler som kan tyde på et problem:

Løsepengevarsel eller låst skjerm: Et svært tydelig tegn – datamaskinen din viser plutselig en melding om at filene dine er kryptert eller krever løsepenger for å låse opp systemet ditt. Du kan være ute av stand til å åpne filer, og de kan ha merkelige filendelser. Ofte kan bakgrunnen endres til instruksjoner, eller det dukker opp et vindu med filer og betalingsinstruksjoner. Hvis du ser dette, er det nesten helt sikkert et angrep med løsepengevirus.

Antivirusvarsler eller falske antivirus-popup-vinduer: Hvis antivirusprogrammet oppdager noe, bør du ta det på alvor. Omvendt gjelder det motsatte hvis du ser et falskt popup-vindu som hevder «Datamaskinen din er infisert! Klikk her for å skanne», og den ikke er fra antivirusprogrammet ditt, men fra et nettsted, er det en taktikk for å lokke deg til å installere skadevare. Gjenkjenn forskjellen: Det faktiske antivirusprogrammet ditt har et kjent grensesnitt og vil sannsynligvis ikke gi deg beskjed via en tilfeldig annonse i nettleseren.

Uventede verktøylinjer eller nettleseradferd: Plutselig har nettleseren nye verktøylinjer, eller startside/søkemotor har endret seg uten at du har gjort noe, eller søk omdirigeres til merkelige nettsteder. Dette tyder på at det er installert reklameprogrammer eller skadevare. På samme måte kan hyppige popup-annonser når du er frakoblet eller på nettsteder som normalt ikke viser dem, tyde på en infeksjon.

Ukjente programmer eller prosesser: Du legger merke til et program du aldri har installert. Eller datamaskinens vifte går på høyt, og den er treg, og

Oppgavebehandling/Aktivitetsmonitor viser ukjente prosesser som opptar CPU. Noen skadevareprogrammer kan kjøre usynlig, men mange vil forbruke ressurser (for eksempel kryptominere, som gjør systemet tregt). Hvis du ser et program åpnes kort og deretter forsvinne, eller nye ikoner på skrivebordet, bør du undersøke saken.

Vennene dine mottar merkelige meldinger fra deg: Hvis kolleger eller venner sier at de har mottatt en merkelig e-post eller melding på sosiale medier fra deg som du ikke har sendt, kan kontoen din være kompromittert. Eksempler: Spam-e-poster fra adressen din, eller at WhatsApp-kontoen din sender en mistenkelig lenke i gruppechatter. Dette er et tegn på at enten enheten din eller den kontoen ble overtatt.

Passordet fungerer ikke: Et svært alarmerende tegn er hvis du plutselig ikke kan logge inn på en konto fordi passordet ble endret (og du ikke endret det). Hvis det kjente riktige passordet ditt avvises og kontogjenopprettingen indikerer en endring, kan du anta at denne kontoen er utsatt for et brudd.

Uvanlig nettverks- eller systemaktivitet: Dette kan være vanskeligere å legge merke til for en gjennomsnittlig bruker, men hvis du har et nettverksovervåkingsverktøy eller en IT-administrator, er eksempler på dette en økning i utgående trafikk, ukjente enheter på nettverket eller at harddisklampen blinker konstant når du ikke gjør noe (kan bety at data blir eksfiltrert eller at et virus skanner filene dine). Sjekk også brannmurvarsler (hvis det finnes noen) eller Windows Defender-logger for gjentatte blokkerte handlinger.

Filer som mangler eller er endret: Dersom du oppdager at filer er slettet eller innhold er endret uten forklaring, er det bekymringsfullt. Data kan bli slettet eller manipulert av en angriper. Hvis du ser filer med forvrengte navn eller filendelser, f.eks. låste eller krypterte, tyder det også på løsepengevirus.

Merkelig markør eller kontroll: I ekstreme tilfeller, hvis musen beveger seg av seg selv eller vinduer åpnes uten at du gjør det, kan noen ha fjernkontroll (som om et eksternt skrivebord eller RAT-skadevare er i drift). Koble fra internett umiddelbart hvis dette skjer.

Systemadvarsler eller krasjskjermer: Gjentatte krasj eller blåskjermer kan bare være problemer med maskinvare/programvare, men noen ganger forårsaker rootkits eller

dyptgående skadevare ustabilitet. Hvis dette begynte å skje sammen med andre tegn, bør du vurdere skadevare som en mulighet.

Nettleseromdirigeringer: Hvis du konsekvent blir omdirigert til en litt annen URL eller uventet får opp sertifikatadvarsler når du prøver å besøke vanlige nettsteder (for eksempel en bank eller Gmail), kan du ha skadevare eller en DNS-kapring. Hvis du for eksempel prøver å gå til facebook.com, men alltid havner på en side som ikke ser riktig ut, betyr det trøbbel.

I praksis overlapper mange av disse tegnene hverandre. For eksempel vil et angrep med løsepengevirus produsere krypterte filer (som du ikke kan åpne), muligens en tekstfil med løsepenger i hver mappe, og kanskje et endret skrivebordsbakgrunnsbilde som kunngjør det. Kompromittering av kontoer via phishing oppdages ofte når andre informerer deg om rare meldinger, eller når du mottar påloggingsvarsler fra uvanlige steder.

Hvis du mistenker et problem, men ikke er sikker, bør du være på den forsiktige siden:

- Hvis det er et potensielt virus, kjører du en fullstendig antivirusskanning.
- Hvis en konto kan være kompromittert, kan du prøve å logge på fra en annen sikker enhet og endre passordet hvis du fortsatt kan, eller se kontoaktivitetslogger.
- Hold øye med nettverksbruken (på Windows 10 kan du også se nettverksbruken per app i Oppgavebehandling).
- Hvis enheten din har et diagnose- eller sikkerhetsskanningsverktøy (for eksempel Windows Security eller et tredjepartsverktøy), bør du bruke det.

Nøkkelen er å være årvåken. En praksis for sivilsamfunnsorganisasjoner er å oppmuntre de ansatte til å si ifra hvis «datamaskinen oppfører seg rart». Det er bedre å undersøke falske alarmer enn å gå glipp av et reelt brudd. Ikke la potensiell stigmatisering hindre rapportering. I sikkerhetsopplæringen bør du understreke at det er avgjørende med rettidig rapportering, og at de ikke vil bli klandret for å melde fra om en bekymring.

Nå som du vet hva du skal se etter, er neste trinn å handle raskt når noe virker galt. De følgende avsnittene omhandler tiltak for umiddelbar respons, hvem du skal ringe for å få hjelp, og hvordan du kan gjenopprette driften.

Trinnvis respons: Hva du skal gjøre når noe går galt

I det øyeblikket du innser at det kan være snakk om en cyberhendelse, er det avgjørende å iverksette bevisste tiltak for å begrense og undersøke problemet. Å få panikk eller gjøre feil (for eksempel å betale løsepenger umiddelbart eller slette bevis) kan forverre situasjonen. Her er en trinnvis veiledning som er i tråd med standard faser for hendelsesrespons (identifisere, begrense, utrydde, gjenopprette) i forenklede ord for et CSO-miljø:

1. **Ikke få panikk, vurder situasjonen:** Trekk pusten og prøv å forstå hva som skjer. Hva er tegnene og omfanget? For eksempel: Er det én datamaskin som oppfører seg rart, eller er det flere? Er det et konto- eller en enhetsrelatert problem? Identifisering av hendelsens art er veiledende for de neste trinnene. Skriv ned det du observerte (tidspunkt, symptomer). Om nødvendig kan du raskt ta bilder eller skjermbilder av mistenkelige meldinger eller feilskjermer med telefonen (nyttig som bevis og for å spørre eksperter senere).

2. **Koble fra berørte systemer:** Dersom du mistenker aktiv skadevare, spesielt dersom data kan bli stjålet eller dersom flere systemer er infisert, må du umiddelbart isolere maskinen fra nettverket. Koble fra Ethernet-kabelen eller slå av Wi-Fi. Dette forhindrer spredning (f.eks. prøver noen ormer eller ransomware å hoppe til nettverksstasjoner) og stopper angriperens fjernkontroll eller dataeksfiltrering. Du skal imidlertid ikke slå av systemet med mindre du må – bare koble fra nettverket. Det finnes en nyanse: Å slå av strømmen stopper skadevaren, men kan også slette midlertidige bevis. I de fleste CSO-scenarier er det greit å la den stå på og frakoblet, og deretter kjøre skanninger. Men hvis løsepengevirus aktivt krypterer filer foran øynene dine, kan du raskt slå av strømmen for å stoppe det. Bruk skjønn – når du er i tvil, er det å koble fra nettverket et godt første trekk.

3. **Sikre kontoene dine:** Hvis en konto er kompromittert (for eksempel e-post eller sosiale medier), **må du prøve å gjenvinne kontrollen**. Bruk prosedyrer for kontogjenoppretting: Tilbakestill passord umiddelbart. Logg ut av alle aktive økter (mange tjenester har en «logg ut av alle enheter»-funksjon). Aktiver 2FA hvis du ikke allerede har gjort det (selv om hackeren fortsatt har en økt, vil 2FA bidra til å stoppe pålogging på nytt når du har sparket dem ut). Gi kolleger beskjed om at kontoen ble kompromittert, slik at de bør behandle

eventuelle nylige meldinger som potensielt uredelige. Hvis du ikke kan få tilgang på nytt (hackeren har endret passordet og låst deg ute), må du kontakte tjenesteleverandørens brukerstøtte umiddelbart for å rapportere en kontoovertakelse.

4. **Informer den ansvarlige personen (og muligens alle):** I henhold til sikkerhetsplanen din (fra kapittel 3) bør du ha en kontaktperson eller et team for hendelser. Informer dem umiddelbart. Hvis du er den personen, samler du relevante personer. Hvis for eksempel en delt server rammes, må du varsle alle brukere om ikke å bruke den inntil videre. Hvis én ansattes PC er infisert, kan du advare andre om ikke å åpne e-poster fra den PC-en osv. **Ikke hold en hendelse hemmelig** – å skjule den kan forverre skaden. Rask kommunikasjon gjør det mulig for andre å være på vakt eller iverksette beskyttelsestiltak (for eksempel endre passord om nødvendig). Hvis du har IT-støtte (internt eller på kontrakt), bør du også ringe dem tidlig. De kan begynne å hjelpe til med tekniske tiltak eller dypere analyser.
5. **Begrens skaden:** I tillegg til å koble fra nettverket, finner du her tiltak for å begrense skaden:
    - Hvis det er skadevare på en PC, kan du kjøre en antivirusskanning i sikkermodus, hvis det er mulig, eller ved hjelp av en oppstartbar redningsdisk. Dette kan sette skadevaren i karantene og stoppe ytterligere skade. Imidlertid må du først begrense (slå av nettverket) og deretter skanne – ikke kjør skanninger mens du fortsatt er tilkoblet hvis en aktiv angriper kanskje overvåker, eller ytterligere nyttelast kan lastes ned.
    - Hvis det er snakk om løsepengevirus og filene er kryptert, må du finne ut om det har stoppet eller fortsatt kjører. Avslutt mistenkelige prosesser via Oppgavebehandling hvis du ser dem (noen bruker åpenbare navn, andre er tilfeldige). Men på dette stadiet er krypteringen sannsynligvis utført raskt. Inndemming betyr da å sette den PC-en i karantene og ikke røre filene (slik at rettsmedisinske eksperter eller dekrypteringsverktøy kan forsøke å gjenopprette dem).
    - Hvis et nettsted er under angrep (ødelagt eller hacket), bør du koble det fra nettet hvis du kan (f.eks. sette opp en vedlikeholdsside eller be verten om å

suspendere det midlertidig) for å forhindre ytterligere skade på besøkende og gi deg tid til å utbedre problemet.

- Ved e-postbrudd bør du, i tillegg til å endre passordet, vurdere å sende e-post til kontakter for å advare dem om potensiell phishing fra kontoen din.
- Hvis data ble lekket (for eksempel hvis du finner databasen din på et lim inn-nettsted), må du begrense tilgangen til disse systemene til du forstår utnyttelsesveien og kan rette opp den.

6. **Dokumenter alt:** Når du gjør det ovennevnte, bør du ta notater. Skriv ned tidspunkter, tiltak du har iverksatt og hvem som blir varslet. Hvis du finner en mistenkelig fil eller et mistenkelig prosessnavn, må du notere det. Denne dokumentasjonen hjelper deg senere med gjenoppretting, rapportering og forbedring av sikkerhetsplanen din. Det er også nyttig hvis du involverer politiet eller en hendelsesresponsprofesjonell – de vil ønske å kjenne til hendelsesrekkefølgen.

7. **Søk hjelp ved behov:** Ikke nøl med å søke hjelp utenfra. Hvis du har en cybersikkerhetskontakt (kanskje en annen sivilsamfunnsorganisasjons IT-avdeling, en frivillig ekspert eller en hjelpetelefon for cybersikkerhet), bør du ringe dem. Mange land har også CERT-er (Computer Emergency Response Teams) som kan hjelpe eller gi råd til selv små organisasjoner. Det finnes også gratis samfunnsressurser. I et tilfelle med løsepengevirus kan du for eksempel sjekke nettstedet «No More Ransom» for å se om det finnes et dekrypteringsverktøy for varianten din. Men bruk kun anerkjente verktøy – for alle nettbaserte råd må du forsikre deg om at de er legitime. Hvis du er usikker, kan du spørre IT-rådgiverne du stoler på.

8. **Bevar bevis (spesielt ved alvorlige hendelser):** Dersom hendelsen kan innebære en forbrytelse (f.eks. et bevisst hackingangrep, et betydelig tyveri), kan du senere involvere politiet. I slike tilfeller er det avgjørende å bevare logger og bevis. Unngå å slette systemlogger eller slette systemet før problemet er forstått og løst. Hvis du må gjenoppbygge et system, bør du vurdere å lage en avbildning av disken først. I mindre kritiske tilfeller er bevis fremdeles nyttige for å lære – f.eks. kan du beholde phishing-e-posten som lurte noen, for å studere den og opplyse andre.

9. **Utrydde trusselen:** Når den er under kontroll, kan du arbeide med å fjerne den. For skadevare: Bruk antivirusprogramvare til å fjerne den fullstendig, eller i vanskelige tilfeller, formater/installer operativsystemet på nytt (å starte på nytt er den sikreste måten hvis du har sikkerhetskopier og det ikke er for tyngende). For kompromitterte kontoer: Dobbeltsjekk at det ikke finnes bakdører (f.eks. sørg for at angriperen ikke har angitt nye videresendingsregler i e-posten for å videresende e-poster i hemmelighet, et triks som ofte overses). Sjekk andre kontoer, for noen ganger får én påloggingsinformasjon tak i mange – hvis nettleseren for eksempel har lagret passord, kan en angriper få tak i dem, så du må kanskje endre passordene til andre kontoer også.

Hvis hendelsen var en sårbarhet (for eksempel at nettstedet ditt hadde et utdatert programtillegg som ble utnyttet), må du oppdatere eller fjerne det. Hvis problemet var en insider med onde hensikter, må du selvsagt fjerne vedkommendes tilgang.

10. **Gjenopprett og gjenopprett:** Etter å ha eliminert den umiddelbare trusselen, kan du begynne å gå tilbake til normalen:

- Gjenopprett tapte eller ødelagte data fra sikkerhetskopier. Kontroller at sikkerhetskopiene er rene (skann dem med antivirusprogramvare før du gjenoppretter dem, hvis mulig).
- Koble systemene til på nytt med forsiktighet. Etter å ha renset en PC, kan du for eksempel koble den til nettverket igjen og overvåke om mistenkelig utgående trafikk gjenopptas (hvis den gjør det, er kanskje ikke skadevaren helt borte).
- Hvis du har aktivert kontoer på nytt eller endret påloggingsinformasjon, må du sørge for at alle får tilgang til det de trenger igjen, med nye, sikre passord.
- Hvis driften ble stoppet (f.eks. hvis du koblet fra en server), må du koordinere for å få den opp igjen i lavtrafikk for å teste den, og sikre at det ikke foreligger noen gjenværende kompromitteringer.

11. **Kommuniser oppdateringer:** Hold personalet informert om hva som har skjedd og hva som gjøres. Åpenhet skaper tillit og samarbeid. Hvis det er relevant, bør du også informere eksterne interessenter på passende måte (se neste avsnitt om hvem du skal kontakte, f.eks. givere hvis opplysningene deres ble utsatt for datainnbrudd osv.). Generelt kan

imidlertid interne problemer holdes interne, med mindre det er behov for eller plikt til å rapportere eksternt.

Gjennom hele denne prosessen bør du ha en læringsorientert holdning, ikke en skyldorientert holdning. Angrep skjer med de beste av oss. Fokuser på å finne en løsning og forhindre at det skjer igjen, i stedet for å dvele ved hvem som klikket på hva (bortsett fra å bruke denne informasjonen til å forbedre opplæringen).

Denne strukturerte responsen – identifisere, begrense, utrydde, gjenopprette – gjenspeiler veiledning fra eksperter. For små sivilsamfunnsorganisasjoner kan trinnene utføres av én person med mange hatter, men prinsippet gjelder likevel.

La oss deretter se nærmere på hvem du kanskje må ringe eller rapportere til, fordi håndtering av en hendelse kan involvere flere parter enn bare organisasjonen din.

Hvem du kan henvende deg til for å få hjelp: Støtteressurser og få hjelp

Når du håndterer en cyberhendelse, trenger du ikke å håndtere alt alene. Det finnes flere steder og personer du kan henvende deg til for å få hjelp, råd og rapportere. Her er en oversikt over støtteressurser:

Internt team og IT-støtte: Først må du involvere alle i organisasjonen som er ansvarlige for IT eller sikkerhet (det «tekniske» personalet/den frivillige medarbeideren, eller personen som konfigurerte systemene dine). Hvis du har en IT-tjenesteleverandør eller en frivillig IT-rådgiver, må du kontakte dem umiddelbart og beskrive situasjonen. De har sannsynligvis sett lignende problemer og kan veilede deg om tekniske tiltak. Selv et teknisk kyndig styremedlem eller IT-ansvarlig i en partnerorganisasjon kan være en verdifull alliert i en knipe.

Fagfelleskap og andre sivilsamfunnsorganisasjoner: Vurder å ta diskret kontakt med søsterorganisasjoner eller -nettverk. Ofte kan nettverk av sivilsamfunnsorganisasjoner (for eksempel et menneskerettighetsnettverk eller en paraplyorganisasjon for sivilsamfunnsorganisasjoner) ha delte ressurser eller i det minste kollektiv kunnskap. De kanskje kjenner til vanlige trusler i sektoren eller regionen din og har anbefalinger (for eksempel: «Ja, to andre sivilsamfunnsorganisasjoner mottok den samme phishing-e-posten – dette gjorde vi»). Samarbeid kan være virkningsfullt her. Vurder imidlertid hvor mange detaljer du skal dele

eksternt – hold sensitive opplysninger for pålitelige kontakter for å unngå eventuelle omdømmerisikoer frem til det er offisielt.

Hjelpetelefoner for cybersikkerhet for sivilsamfunnet: Det finnes initiativer som er spesielt utformet for å hjelpe sivilsamfunnet med nødssituasjoner knyttet til digital sikkerhet. En av de mest fremtredende er **Access Nows hjelpetelefon for digital sikkerhet**, som tilbyr gratis assistanse døgnet rundt til organisasjoner i sivilsamfunnet, aktivister og journalister over hele verden. De kan hjelpe i tilfeller som nettstedsangrep, kontokompromittering osv., og setter deg ofte i kontakt med frivillige eksperter eller gir skreddersydd veiledning. Hvis du befinner deg i en alvorlig situasjon som overgår evnene dine, må du ikke nøle med å sende en e-post eller ringe en slik hjelpetelefon (Access Nows er ). De ivaretar konfidensialiteten og er vant til å håndtere hastesaker.

Et annet eksempel: **CyberPeace Institutes CyberPeace Builders-program** tilbyr gratis cybersikkerhetshjelp fra frivillige i bedrifter til sivilsamfunnsorganisasjoner. Hvis du allerede er registrert hos dem eller har kontakt med dem, kan du bruke den kanalen. Hvis ikke, er det kanskje noe å vurdere for fremtiden.

Politi: Dette avhenger av hendelsens art:

- Hvis det er snakk om et betydelig datainnbrudd som involverer tyveri av personopplysninger eller et bevisst hack, kan du vurdere å informere lokale politimyndigheter eller en enhet for nettkriminalitet. De kan etterforske, spesielt hvis givernes penger eller sensitive opplysninger ble stjålet, eller hvis det foreligger utpressing (for eksempel krav om løsepenger). Erfaringene varierer imidlertid – noen steder er politiet hjelpsomme, mens de andre steder kanskje ikke prioriterer saken eller mangler ekspertise.
- I land med lover om obligatorisk varsling om databrudd (for eksempel i henhold til GDPR i EU, der alvorlige personopplysningsbrudd må rapporteres til datatilsynet innen 72 timer), bør du følge disse forskriftene. Det innebærer å informere den relevante datatilsynsmyndigheten, hvis det er aktuelt, og eventuelt berørte personer (mer om det i neste avsnitt).

- Hvis du mistenker at angriperen er fra en bestemt region, eller at det finnes et mønster som påvirker flere organisasjoner, kan politiet koble disse sammen.
- Merk: Dersom sivilsamfunnsorganisasjonen din arbeider med sensitive saker i et land der myndighetene kanskje ikke er vennlige eller kan misbruke denne informasjonen (for eksempel dersom angrepet kan være statlig sponset), må du nøye vurdere å involvere politiet. I slike tilfeller kan det i utgangspunktet være å foretrekke å konsultere internasjonale organer (for eksempel kanskje et CERT i et nøytralt land eller bare bruke hjelpetelefoner for sivilsamfunnsorganisasjoner).

Nasjonal CERT/CSIRT: Mange land har et Computer Emergency Response Team (CERT) eller CSIRT, ofte under en statlig eller akademisk paraply. Noen ganger hjelper de organisasjoner (ikke bare kritisk infrastruktur). Noen har spesielle avdelinger for små bedrifter eller ideelle organisasjoner. For eksempel reagerer **CERT-er i EU** ofte på hendelser og kan gi råd eller koordinere med politiet. Hvis du har en kontaktperson eller enkelt kan rapportere via nettstedet deres, kan det være fordelaktig. De kan også advare andre eller spore spredningen av en skadevarekampanje.

Givere eller partnere: Dersom et prosjekt eller giverdata er involvert, eller dersom tjenesteleveransen påvirkes, kan det hende du må informere partnere. Hvis du for eksempel driver et felles prosjekt og hackere ødelegger prosjektets nettsted, sikrer du at partneren fra den andre sivilsamfunnsorganisasjonen er klar over det og kan hjelpe, eller i det minste ikke blir overrasket, ved å informere vedkommende. Givere kan ha rapporteringskrav dersom midler påvirkes (f.eks. økonomisk svindel). På den støttende siden kan noen givere (spesielt større givere eller de som finansierer cybersikkerhetskapasitet) ha ressurser til å hjelpe deg. Men håndter kommunikasjonen nøye – fokuser på hva som gjøres for å løse problemet, ikke bare på problemet, for å opprettholde tilliten.

Forsikring: Hvis du har en cyberforsikring eller en generell ansvarsforsikring som dekker cyberhendelser, må du varsle forsikringsselskapets hendelseshotline så snart som mulig (ofte påkrevd for dekning). De kan sende ut profesjonelle hjelpearbeidere eller veilede om de neste trinnene. Mange forsikringspoliser krever samordning med forsikringsselskapet for ting som beslutninger om å betale løsepenger. Dersom du ikke har forsikring, gjelder dette selvsagt ikke.

Fellesskap og nettbaserte ressurser: Det finnes nettbaserte fora som **Reddit r/cybersecurity eller r/techsupport** eller **StackExchange Security**, der fagfolk noen ganger hjelper til. Men vær forsiktig med å avsløre sensitive opplysninger i offentlige fora. I stedet kan man søke på disse forumene for å se om andre har håndtert den spesifikke skadevaren eller feilen (ofte har noen lagt ut innlegg om akkurat den løsepengennotaten eller virusatferden, noe som kan gi ledetråder om løsninger). Nettsteder som **BleepingComputer** har egne avsnitt for hjelp med fjerning av skadevare og spesifikke tråder for støtte vedrørende løsepengevirus, ofte moderert av eksperter som hjelper ofre gratis. De samarbeider ofte med NoMoreRansom-prosjektet også. Hvis du velger denne veien, bør du følge retningslinjene deres (de ber ofte om å få loggfiler osv., men ikke gjør noe du ikke er komfortabel med; kanskje bør du bruke et pseudonym hvis du diskuterer saken din offentlig).

Når og hvordan du skal informere berørte personer/offentligheten: Dette handler mer om «hvem du skal varsle» også: Dersom personopplysninger om mottakere eller interessenter lekkes, kan etisk og muligens juridisk plikt tvinge deg til å informere disse personene slik at de kan beskytte seg selv (f.eks. endre passordene sine dersom e-postadressen deres ble lekket, passe på identitetstyveri). Det kan være vanskelig å utforme slik kommunikasjon; den bør være ærlig, unnskyldende og gi veiledning (for eksempel: «Vi har opplevd en sikkerhetshendelse der e-postadressen din kan ha blitt eksponert. Vær på vakt for mistenkelige e-poster og vurder å endre passordet ditt hvis du har brukt det på flere steder …»). Hvis du er usikker, bør du rådføre deg med en kommunikasjons- eller juridisk rådgiver – du ønsker å finne riktig tone og ikke utilsiktet innrømme ansvar på feil måte osv.

Psykologisk støtte: Dette kan høres utenom emnet, men en alvorlig hendelse kan være stressende. Folk kan føle seg krenket eller skyldige (personen som klikket på phishingen kan føle seg forferdelig). Det er verdt å ta opp moralen. Sørg for at alle vet at feil skjer, og fokuser på å gå videre. Hvis du er ekstremt stresset, kan du kanskje ta en kort pause eller få noen å snakke med (selv å lufte ut til en kollega i en annen sivilsamfunnsorganisasjon som har vært gjennom en lignende opplevelse, kan være betryggende). Når ting har roet seg, bør du vurdere

en oppsummeringsøkt som er støttende: Drøft hva som skjedde og hvordan dere kan hjelpe hverandre med å takle situasjonen og bli sterkere.

I all kommunikasjon med eksterne enheter skal du føre registrering over hvem du kontaktet og når, samt eventuelle saks-/referansenumre eller råd som er gitt. Dette er en del av dokumentasjonen og hjelper med oppfølging.

Til slutt: Bruk disse støttekanalene ikke bare under en hendelse, men også etterpå for å forbedre dere. For eksempel kan Access Now-hjelpetelefonen gi råd om hvilke tiltak som bør iverksettes i fremtiden for å unngå gjentakelser, eller CERT kan sende deg rapporten og anbefalingene sine.

Gjenopprette sikkerheten: Trinn for gjenoppretting

Etter å ha begrenset hendelsen og fått hjelp, er den siste fasen å bringe systemene tilbake til normal drift og iverksette tiltak for å forhindre at hendelsen gjentar seg. Gjenoppretting handler ikke bare om å gjenopprette data, men også om å gjenopprette tilliten til at miljøet ditt er rent og sikkert igjen.

Rens og gjenoppbygg systemer: Dersom noen maskiner ble infisert, bør du vurdere om en fullstendig ominstallasjon av operativsystemet er nødvendig etter at skadevaren er fjernet. Sikkerhetseksperter antyder ofte at ved alvorlige sikkerhetsbrudd (som rootkits eller ukjent skadevare) er sletting og ombygging den tryggeste måten å sikre at systemet er rent på. Ja, det er tidkrevende å installere apper på nytt og gjenopprette filer, men det gir trygghet for at det ikke gjenstår noen skjult bakdør. Hvis du velger å ikke gjøre det, bør du i det minste kjøre flere skanneverktøy (ett antivirusprogram kan overse noe som et annet oppdager). Verktøy som Malwarebytes, HitmanPro osv. kan kjøres i tillegg til hoved-AV-en din for å få en ekstra vurdering. Sørg for at operativsystemet er fullstendig oppdatert med oppdateringer etter rensing.

For kontoer: Etter at du har fått tilgang på nytt, må du gjennomgå kontoinnstillingene: Har angriperen konfigurert videresendingsregler, lagt til gjenopprettings-e-poster eller egne 2FA-enheter? (Dette er vanlig: En Gmail-hacker kan f.eks. legge til e-postadressen sin som en gjenopprettings-e-postadresse, slik at vedkommende prøver å gjenopprette kontoen selv etter

et passordbytte.) Fjern eventuelle slike uautoriserte endringer. Kontroller e-postfiltre, app-passord og tilkoblede apper – i utgangspunktet alt i kontoinnstillingene som kan gi fortsatt tilgang.

Dersom et nettsted ble hacket, bør du vurdere å flytte det til en sikrere vert eller legge til en brannmur for webapplikasjoner (WAF) etter å ha utbedret sårbarheten og gjenopprettet innholdet. Det kan være lurt å foreta en sikkerhetsrevisjon av koden dersom det er et tilpasset nettsted. Endre også alle database- og FTP-passord i tilfelle de ble kompromittert.

Gjenopprett data fra sikkerhetskopier: Få tilbake eventuelle tapte data. Hvis du for eksempel måtte slette innholdet på en PC, kan du hente brukerfilene fra sikkerhetskopien (men skann dem først, i tilfelle en infisert fil lurte i dokumentene). Hvis en database ble slettet eller kryptert, kan du gjenopprette den nyeste sikkerhetskopien. Test at de gjenopprettede dataene er intakte og at systemene som bruker dem, fungerer som de skal. Noen ganger er ikke sikkerhetskopiene så oppdaterte som vi ønsker, så du kan miste litt arbeid. Etter gjenopprettingen bør du be personalet om raskt å sjekke om noe mangler i mellomrommet, og i så fall se om det kan legges inn på nytt eller innhentes på nytt.

Dersom det er snakk om løsepengevirus og du ikke har sikkerhetskopier, er gjenopprettingen vanskeligere. Rådfør deg med eksperter eller NoMoreRansom for dekrypteringsverktøy – noen ganger finnes det gratis løsninger for visse ransomware-varianter. Det frarådes generelt å betale løsepenger (det finansierer kriminelle og gir ingen garanti), men noen organisasjoner tar det vanskelige valget. Involver politiet før du betaler, siden de noen ganger har nøkler eller kan gi råd. Hvis det til syvende og sist oppstår datatap, må du planlegge hvordan du kan gjenopprette disse dataene (kanskje kontakte partnere for å be dem sende deg kopier av filer de har, osv.).

Forbedre og oppdatere sikkerhetstiltak: Etter et datainnbrudd må man styrke forsvaret. Dette er «erfaringer»-fasen, der du lappe hullene som ble utnyttet:

- Hvis det var phishing, er det tydeligvis behov for mer opplæring og kanskje tekniske kontroller (for eksempel et bedre søppelfilter eller håndheving av MFA). For eksempel kan du kreve at alle e-postkontoer har 2FA aktivert og kanskje innføre en e-postadvarsel for

eksterne avsendere (noen systemer skriver «[Ekstern]» i emnelinjen hvis e-posten kommer utenfra, for å gjøre det enklere å oppdage spoofing).

- Hvis det dreide seg om et svakt passord eller en gjenbrukt påloggingsinformasjon, må du skjerpe passordpolicyene (lengre, unike) og vurdere å bruke en passordbehandler i hele organisasjonen for å bidra til dette. Og absolutt 2FA på alt som er kritisk.
- Hvis skadevare kom via programvare som ikke er oppdatert, må du sørge for at oppdateringer utføres raskere. Du kan kanskje bruke et verktøy for å overvåke manglende oppdateringer eller abonnere på sikkerhetsbulletiner som er relevante for programvaren din.
- Dersom en bestemt tjeneste ble eksponert (for eksempel en åpen RDP-port som ble utsatt for brute force-angrep), må du lukke den eller plassere den bak et VPN.
- Kontroller at brannmurreglene dine er strammet, og at unødvendige tjenester er deaktivert (som vi dekket i 4.4).
- Vurder å segmentere nettverket eller dataene dine: I fremtiden kan du f.eks. oppbevare sikkerhetskopier på en enhet som ikke alltid er tilkoblet, slik at løsepengevirus ikke kan angripe dem, eller plassere sensitive data på en harddisk som ikke alle har tilgang til.
- Implementer bedre overvåking: Kanskje kan du aktivere systemloggføring og konfigurere varsler (det finnes gratis verktøy for loggovervåking, eller du kan til og med bare bruke Windows Event Forwarding til å overvåke visse hendelser, f.eks. flere mislykkede påloggingsforsøk).
- Planlegg en formell prosedyre for hendelsesrespons dersom du ikke hadde en – i bunn og grunn skrive ned hva du gjorde denne gangen og forbedre det til neste gang (en del av oppdateringene av sikkerhetsplanen).

Kommuniser med interessenter: Hvis du måtte varsle folk om hendelsen, må du følge opp når den er løst. Gi for eksempel styret eller giverne beskjed: «Vi opplevde X, vi tok tiltak Y, og nå er driften gjenopprettet. Vi iverksetter Z for å sikre at dette ikke skjer igjen.» Denne forsikringen og ansvarligheten kan styrke tilliten hvis den utføres på en åpen og kompetent måte. På samme måte, hvis frivillige eller mottakere tidligere ble informert om å være forsiktige, bør du senere

informere dem om at problemet er løst: f.eks. «Nettstedet vårt er nå sikkert og tilbake på nettet. Takk for tålmodigheten.»

Psykologisk restitusjon: Etter et sikkerhetsbrudd kan teamets moral bli påvirket. Folk kan føle seg utrygge («Er vi sikre på at hackerne ikke fortsatt er inne?») eller skyldige. Avhold et oppsummeringsmøte for å diskutere åpent hva som skjedde, og behandle det som en læringsmulighet i stedet for en heksejakt. Rost den raske rapporteringen eller tiltakene som begrenset skadene. Kanskje kan du holde en liten workshop om «erfaringer», der du oppdaterer alle om hvilke nye tiltak som er iverksatt, noe som også vil berolige dem og vise at ting er tryggere nå. Tonen bør være: Vi sto overfor en utfordring og overvant den, nå er vi sterkere.

Dokumentasjon og rapportering: Skriv en intern rapport om hendelsen – selv om det bare er én side. Dokumenter tidslinjen, den underliggende årsaken (hvis kjent), iverksatte tiltak og anbefalinger. Dette er nyttig for hukommelsen (seks måneder senere kan du glemme viktige detaljer hvis noe lignende skjer) og for eventuelle eksterne rapporteringsplikter. Dersom det kreves av regelverket (f.eks. GDPR), skal du sende inn den formelle rapporten til myndighetene, inkludert disse opplysningene. Hvis du samarbeider med en overordnet organisasjon eller har en forpliktelse overfor givere (noen tilskudd krever rapportering av alvorlige hendelser som en del av risikostyringen), kan du bruke den interne rapporten til å kommunisere på en hensiktsmessig måte.

Teste og oppdatere planer: Når alt er normalt, er det et perfekt tidspunkt å finpusse sikkerhetsplanen og hendelsesresponsen på. Oppdater kontaktlistene dine (kanskje du innså at du ikke hadde CERT-nummeret tilgjengelig – lagre det nå). Dersom et bestemt verktøy ville ha bidratt til å oppdage eller stoppe hendelsen tidligere, bør du vurdere å ta det i bruk. Vurder til og med å gjennomføre en liten «brannøvelse» i fremtiden – for eksempel å teste gjenoppretting av sikkerhetskopier eller gjennomføre en simulert phishing-test for å se om den nye opplæringen fungerer.

Husk at **fullstendig gjenoppretting omfatter å gjenvinne tillit**. De ansattes tillit til systemene, eksterne partneres tillit til håndteringen din. Åpenhet, handling og oppfølging bidrar til å gjenoppbygge denne tilliten. Det viser at du tok det på alvor og har forbedret deg.

Til slutt er det verdt å dele kunnskap (uten sensitive opplysninger) med fellesskapet, dersom det er hensiktsmessig. Hvis du for eksempel oppdaget en ny svindel rettet mot sivilsamfunnsorganisasjoner, kan det å advare andre via en e-postliste eller et nettverk hindre dem i å bli offer – et positivt resultat av prøvelsen din.

Ved å gå nøye gjennom disse gjenopprettingstrinnene gjenoppretter du ikke bare normalen, men ender ideelt sett opp med en mer robust sikkerhetstilstand. Mange organisasjoner opplever at et sikkerhetsbrudd var en vekkerklokke som til slutt gjorde dem bedre forberedt på fremtiden (selv om det alltid er bedre å forbedre seg uten smerten av en hendelse!).

På dette punktet har vi dekket hvordan man håndterer selve hendelsene. Nå skal vi gå videre til betydningen av samarbeid og fellesskap for å opprettholdelsen av sikkerheten, som er et ofte underutnyttet aspekt av cybersikkerhet for sivilsamfunnet.

Kapittelsammendrag

Dette kapittelet legger vekt på den menneskelige siden av cybersikkerhet og taler for en sikkerhetsbevisst kultur gjennom opplæring og retningslinjer. Det fremheves at 74 % av sikkerhetsbruddene involverer menneskelige feil, for eksempel phishing, noe som gjør opplæring av personalet avgjørende. Civilsamfunnsorganisasjoner veiledes til å gjennomføre grunnleggende opplæring i cybersikkerhet, som omfatter passordhåndtering og å oppdage phishing-e-poster, ved hjelp av øvelser som phishing-quizer. Kapitlet gir råd om utarbeidelse av retningslinjer for akseptabel bruk av enheter og data, og sikrer klare regler for ansatte og frivillige. Det skisserer også protokoller for hendelsesrapportering, og oppfordrer til rask kommunikasjon for å begrense brudd. Eksempler omfatter en CSO som lærer opp personalet til å rapportere mistenkelige e-poster, og dermed forhindre et skadevareangrep. Kapitlet legger vekt på ledelsens rolle i å være et forbilde for sikker praksis (f.eks. ved å bruke 2FA) for å legitimere innsatsen. Det anbefales å belønne årvåkenhet, for eksempel ved å rose ansatte for å rapportere phishing, for å forsterke vaner. Ved å integrere sikkerhet i de daglige arbeidsflytene skaper sivilsamfunnsorganisasjoner en robust kultur. Kapitlet fokuserer på enkle, inkluderende praksiser som sikrer tilgjengelighet for alle ansatte, i tråd med læreplanens opplæringsmodell for instruktører og e-bokens mål om å fremme langsiktige sikkerhetsvaner.

Ikke-teknisk sjekkliste for nettsidessikkerhet for sivilsamfunnsorganisasjoner

Denne sjekklisten gir programansatte og frivillige mulighet til å verifisere og forbedre sikkerheten til sivilsamfunnsorganisasjonens nettsted uten at det kreves teknisk ekspertise. Disse trinnene bidrar til å beskytte nettstedet ditt mot angrep (f.eks. ødeleggelse, DDoS) og sikrer at det fortsatt er en pålitelig plattform for oppdraget ditt:

1. Sjekk om nettstedet ditt bruker HTTPS

⇒ Besøk nettstedet ditt og se etter et hengelåsikon i nettleserens adressefelt (før nettadressen) eller «https://» i begynnelsen av adressen.

⇒ Hvis du ser «http://» eller en «Ikke sikker»-advarsel, må du kontakte webverten din for å aktivere HTTPS (f.eks. be om et gratis Let's Encrypt-sertifikat).

⇒ Eksempel: Nettstedet ditt er «www.CSOexample.org ». Sørg for at adresselinjen viser «https://www.CSOexample.org » med en hengelås.

⇒ Hvis HTTPS mangler, kan du sende en e-post til webhotellet ditt: «Vennligst aktiver HTTPS for nettstedet vårt.»

2. Bekreft regelmessige sikkerhetskopier

⇒ Spør webhotellet eller nettstedsadministratoren om nettstedet ditt sikkerhetskopieres regelmessig (f.eks. daglig eller ukentlig), og hvor sikkerhetskopiene lagres (f.eks. sky eller ekstern server).

⇒ Be om en testgjenoppretting for å sikre at sikkerhetskopiene fungerer (spør f.eks.: «Kan dere gjenopprette nettstedet vårt til forrige ukes versjon?»).

⇒ Eksempel: Nettstedet ditt gikk offline etter et angrep. En nylig sikkerhetskopi lar deg gjenopprette det raskt.

⇒ Kontakt verten din: «Har vi automatiske sikkerhetskopier av nettstedet? Hvor ofte utføres de?»

3. Kontroller programvareoppdateringer for nettstedet

⇒ Sjekk med webhotellet eller nettstedsadministratoren om innholdsstyringssystemet (CMS, f.eks. WordPress, Joomla) og programtillegg/temaer oppdateres regelmessig.

⇒ Spør om oppdateringene skjer automatisk, eller om noen sjekker dem månedlig.

⇒ Eksempel: Et utdatert WordPress-programtillegg førte til at nettstedet til en sivil samfunnsorganisasjon ble hacket. Regelmessige oppdateringer forhindrer dette.

⇒ Send en e-post til verten din: «Holdes innholdsstyringssystemet og programtilleggene våre oppdatert? Hvis ikke, vennligst aktiver automatiske oppdateringer.»

4. Sikker administratortilgang

⇒ Sørg for at kun pålitelige medarbeidere har administratortilgang til nettstedet. Snakk med nettstedsadministratoren din for å fjerne tilgangen til tidligere ansatte eller frivillige.

⇒ Kontroller at administratorkontoer bruker sterke passord (f.eks. over 14 tegn, som «sunbird&glass7rain») og tofaktorautentisering (2FA).

⇒ Eksempel: En tidligere frivilligs gamle påloggingsinformasjon ble brukt til å ødelegge et nettsted. Å fjerne ubrukte kontoer forhindrer dette.

⇒ Spør nettstedsadministratoren din: «Hvem har administratortilgang? Kan vi fjerne gamle kontoer og aktivere 2FA?»

5. Se etter mistenkelige endringer på nettstedet

⇒ Besøk nettstedet ditt og se etter uvanlig innhold (f.eks. merkelig tekst, ukjente bilder eller omdirigeringer til andre nettsteder).

⇒ Rapporter eventuell merkelig atferd til webhotellet eller IT-kontakten din umiddelbart.

⇒ Eksempel: En sivilsamfunnsorganisasjons hjemmeside omdirigeres til et svindelnettsted på grunn av et hack. Tidlig rapportering løste problemet raskt.

⇒ Gjennomgå nettstedet ditt og legg merke til alt som er uvanlig. Kontakt verten din: «Nettstedet vårt har [problem]. Vennligst undersøk saken.»

6. Beskytt mot DDoS-angrep

⇒ Spør webverten din om de tilbyr DDoS-beskyttelse (Distributed Denial of Service) for å holde nettstedet ditt tilkoblet under trafikkbølger.

⇒ Bekreft om grunnleggende beskyttelse (f.eks. Cloudflares gratisabonnement) er aktivert.

⇒ Eksempel: Nettstedet til en menneskerettighetsorganisasjon ble frakoblet under et DDoS-angrep. Gratis DDoS-beskyttelse holdt det i gang.

⇒ Send en e-post til verten din: «Har vi DDoS-beskyttelse? Kan vi aktivere en gratistjeneste som Cloudflare?»

7. Begrens offentlig tilgang til sensitive sider

⇒ Kontroller om sensitive nettsider (f.eks. administratorinnlogging, interne dokumenter) er passordbeskyttet eller skjult for offentligheten.

⇒ Be nettstedsadministratoren om å begrense tilgangen til kun autoriserte brukere.

⇒ Eksempel: En sivilsamfunnsorganisasjons donatorliste ble ved et uhell offentliggjort. Passordbeskyttelse av siden løste problemet.

⇒ Spør: «Er sensitive sider, som administratorinnlogginger, beskyttet? Kan vi legge til passord om nødvendig?»

8. Lær opp personalet i sikker bruk av nettstedet

⇒ Minn ansatte og frivillige på at de ikke skal dele administratortilgangsopplysninger eller legge ut sensitive opplysninger (f.eks. giverdata) på nettstedet.

⇒ Del et raskt tips: «Logg alltid ut av nettstedets administratorpanel etter bruk.»

⇒ Eksempel: En ansatt delte et administratorpassord i en e-post, noe som førte til et hack. Opplæring forhindrer dette.

⇒ Send en e-post til teamet: «Del aldri påloggingsopplysninger til nettstedet. Logg ut etter å ha redigert nettstedet.»

KAPITTEL 6: SAMARBEID OG STØTTE FOR DIGITAL SIKKERHET

Sterkere sammen: Samarbeid og støtte

Digital sikkerhet er ikke utelukkende en individuell eller organisatorisk innsats – det er en kollektiv innsats. Civilsamfunnsorganisasjoner kan dra stor nytte av å samarbeide, dele kunnskap og støtte hverandre i møte med cybertrusler. I dette kapitlet drøfter vi hvordan samarbeid kan øke sikkerheten – fra å dele informasjon med andre sivilsamfunnsorganisasjoner og skape en sikkerhetskultur i fellesskapet, til å opplyse allmennheten og benytte seg av lokale og internasjonale støttenettverk.

Deling av informasjon med andre sivilsamfunnsorganisasjoner

Ingen sivilsamfunnsorganisasjon er en øy, spesielt ikke i den digitale verden. Ofte kan angrep eller risikoer som er rettet mot én organisasjon, også påvirke andre i samme sektor eller region. Ved å dele informasjon om trusler og beste praksis kan sivilsamfunnsorganisasjoner i fellesskap forbedre forsvaret sitt.

Hvorfor dele? Det kan oppstå nøling med å dele sikkerhetshendelser av flauhet eller frykt for at det avslører sårbarhet. Fordelene oppveier imidlertid vanligvis risikoen når det gjøres i riktig setting. Hvis sivilsamfunnsorganisasjonen din ble offer for en phishing-kampanje, kan det å informere andre hjelpe dem med å unngå den fellen. Det ligner på nabovakt: Hvis ett hus blir utsatt for svindel, advarer de naboene. Innen cybersikkerhet er dette konseptet med **informasjonsdeling** formalisert i noen sektorer gjennom ISAC-er (Information Sharing and Analysis Centers). Selv om det finnes formelle ISAC-er for bransjer som finans eller helse, kan sivilsamfunnsorganisasjoner opprette egne uformelle delingskretser eller -grupper.

Hva og hvordan du deler:

- **Trusselvarsler:** Hvis du støter på en bestemt phishing-e-post, en skadevarefil eller en mistenkelig tilnærming (for eksempel at noen utgir seg for å være en giver), kan du dele indikatorer: f.eks. «Vi mottok en e-post fra adressen X med emnet Y som var skadelig. Vær

på vakt.» Oppgi tilstrekkelig informasjon til at andre kan gjenkjenne den. Noen CSO-nettverk oppretter e-postlister eller sikre chat-grupper for slike varsler.

- **Taktikker og lærdom:** Etter å ha opplevd en hendelse eller til og med en øvelse, kan du dele det du har lært, kanskje ved å anonymisere sensitive deler. Du kan for eksempel dele: «Vi implementerte tofaktorautentisering på alle kontoene våre, og det blokkerte flere uautoriserte påloggingsforsøk. Det har vært verdt innsatsen.» Dette motiverer andre til å iverksette lignende tiltak.
- **Retningslinjer og opplæringsmateriell:** Det kan være til gjensidig nytte å utveksle ressurser som eksempler på sikkerhetsretningslinjer eller lysbildefremvisninger for opplæring. En sivilsamfunnsorganisasjon kan ha en flott grunnleggende presentasjon om «Grunnleggende cybersikkerhet for ansatte» som de kan dele ut til andre for å tilpasse, i stedet for at alle må finne opp hjulet på nytt.
- **Kontakter for hjelp:** Dersom du har en god opplevelse med en sikkerhetskonsulent eller IT-frivillig, kan du dele denne kontakten med en annen sivilsamfunnsorganisasjon som trenger det (med tillatelse, selvfølgelig). På samme måte kan et medlem av en sivilsamfunnsorganisasjon som deltar på en cybersikkerhetsworkshop eller et nettinar, videreformidle viktige lærdommer til kolleger som ikke kunne delta.
- **Felles øvelser:** Det er mulig å organisere felles arrangementer, for eksempel en sikkerhetsopplæring for flere organisasjoner eller til og med en simulert phishing-øvelse for noen få organisasjoner i sivilsamfunnet. Dette forbedrer ikke bare ferdighetene, men skaper også tillit blant deltakerne.

Oppbygge tillit for deling: Sikkerhetsinformasjon er sensitiv. For å dele oppriktig («vi ble hacket med X-metoden, mistet Y-data»), trenger du tillit til at kolleger ikke kommer til å misbruke denne informasjonen eller dømme hardt. Etablere en norm for konfidensialitet. Kanskje bør du danne en liten, pålitelig gruppe først (for eksempel innenfor en koalisjon eller en arbeidsgruppe av sivilsamfunnsorganisasjoner som kjenner hverandre) før du utvider. Noen fellesskap etablerer Chatham House-regelen (du kan bruke informasjonen, men ikke avsløre hvem som sa den). Noen kan til og med signere et enkelt memorandum om å håndtere delt informasjon med forsiktighet. Etter hvert som nyttige utvekslinger skjer, vokser tilliten over tid.

Bruk av plattformer: Noen plattformer og verktøy kan legge til rette for sikker deling:

- Krypterte e-postlister (ved hjelp av tjenester eller PGP hvis alle deltakerne kan håndtere det, selv om PGP er vanskelig).
- Meldingsgrupper på Signal eller lignende apper for raske varsler om presserende problemer.
- Eventuelt kan du bruke en plattform som **Rocket. Chat** eller **Matrix/Element** for å opprette et lukket forum for sivilsamfunnsorganisasjoner (selvvert eller på en pålitelig server) der de kan diskutere sikkerhetstemaer utenfor offentlighetens øyne.
- Noen nettverk kan samarbeide med CERT-er for å gi dem anonymisert informasjon og få råd i retur.

Vellykkede eksempler: Det har vært initiativer som **«CyberPeace Cafe»** eller møter for sivilsamfunnsorganisasjoner om sikkerhet. I tillegg jobber **NetHope** (et konsortium av humanitære sivilsamfunnsorganisasjoner) med felles retningslinjer for cybersikkerhet og informasjon om hendelser, og behandler sivilsamfunnets infrastruktur som kritisk. Et annet eksempel er konseptet «Information Sharing and Analysis Organization (ISAO) for CSOs» som noen har lansert. I Europa, innenfor rammer av EU-prosjekter (kanskje i sammenheng med dette læreplanet), kan partner-civilsamfunnsorganisasjoner opprette en delt hendelseslogg eller Slack-kanal spesielt for dette formålet.

Ved å dele informasjon i rett tid kan sivilsamfunnsorganisasjoner **omgjøre et angrep på én organisasjon til en tidlig varsling for alle**. Det utgjør også en effektiv bruk av knapp ekspertise – én IT-medarbeider i en ledende sivilsamfunnsorganisasjon kan effektivt fungere som rådgiver for flere partnere gjennom kunnskapsutveksling.

Oppbygge et fellesskap for sikkerhet

Utover reaktiv informasjonsdeling kan sivilsamfunnsorganisasjoner proaktivt skape en fellesskapskultur som prioriterer digital sikkerhet. Et støttende fellesskap kan samle ressurser, fremme læring og forsterke arbeidet for bedre sikkerhetsverktøy og -retningslinjer.

Nettverk for sikkerhetsforkjempere: Identifiser personer i det lokale civilsamfunnet som har interesse for eller ferdigheter innen cybersikkerhet. Dette kan være teknisk kyndig

personale, frivillige med IT-bakgrunn eller sympatiske akademikere. Dann en lokal «sikkerhetsforkjemper»-gruppe som møtes med jevne mellomrom (selv virtuelt) for å diskutere problemer og løsninger. Disse forkjemperne kan deretter fungere som kontaktpersoner i sine respektive organisasjoner. For eksempel kan IT-ansvarlig i en sivilsamfunnsorganisasjon lære andre hvordan de kan styrke Wi-Fi-nettverkene sine, mens en annen som har lært om GDPR, deler tips om samsvar.

Workshoper og opplæringsarrangementer: Organiser opplæringsøkter i lokalsamfunnet og inviter flere sivilsamfunnsorganisasjoner. Kanskje et kvartalsvis workshop om emner som «Bruk av passordbehandlere», «Sikring av mobilkommunikasjon» eller «Hvordan reagere på en cyberhendelse» – hvorav mye kommer fra innholdet i denne boken. Ved å delta på opplæring sammen får ansatte i sivilsamfunnsorganisasjoner ikke bare kunnskap, men møter også likemenn, noe som kan danne tillitsgrunnlaget for informasjonsdelingen vi snakket om. Du kan ofte få eksperter (fra universiteter, selskaper eller statlige CERT-er) til å holde disse workshopene til lav pris eller gratis for ideelle organisasjoner som en del av samfunnsansvar eller samfunnstjeneste. Det er styrke i antall – en bedriftstrener vil kanskje ikke holde et gratis kurs for én sivilsamfunnsorganisasjon på fem personer, men for et samlet publikum på 50 fra ulike sivilsamfunnsorganisasjoner vil vedkommende kanskje gjøre det.

Støtte og veiledning fra kolleger: Oppmuntre til et kameratsystem: Kanskje kan en mindre sivilsamfunnsorganisasjon som mangler IT-støtte, pares med en større sivilsamfunnsorganisasjon som har en IT-avdeling for å få litt veiledning. For eksempel kan en sivilsamfunnsorganisasjon som har implementert skysikkerhet på en vellykket måte, veilede en annen som nettopp har begynt. Dette kan være uformelt, men gir rask hjelp når det trengs («Hei, hvordan implementerte dere 2FA for alle ansatte? Kan dere vise oss det?»)

Samling av ressurser: Vurder felles innkjøp eller deling av verktøy. En gruppe av sivilsamfunnsorganisasjoner kan få en kvantumsrabatt på sikkerhetsprogramvare eller dele et abonnement (innenfor lisensvilkårene). Alternativt, hvis en sivilsamfunnsorganisasjon har en ekstra server eller sikkerhetsenhet, kan kanskje andre bruke kapasiteten på den. I noen sammenhenger har sivilsamfunnsorganisasjoner opprettet delte IT-tjenester (for eksempel en

felles sikker e-postserver eller en delt IT-brukerstøtte på tvers av tre eller fire organisasjoner) for i fellesskap å ha råd til sikkerhet av høyere kvalitet enn hver for seg.

Samfunnsadvokering: Det er også en rolle for sivilsamfunnsorganisasjoner å samlet arbeide for bedre cybersikkerhetsforhold. For eksempel ved å lobbye et giverfellesskap for å finansiere kapasitetsoppbygging innen cybersikkerhet, eller ved å presse programvareleverandører til å tilby bedre priser eller funksjoner til ideelle organisasjoner (noen ideelle koalisjoner har fått Microsoft eller Google til å inkludere kostnadsfrie sikkerhetstillegg for organisasjoner i sivilsamfunnet). I tillegg kan bevisstgjøring hos internettleverandører eller myndigheter om trusler mot sivilsamfunnet (som sofistikert phishing rettet mot aktivister) føre til mer omfattende beskyttelsestiltak. Tenk på konseptet «sivilsamfunnet som kritisk infrastruktur» som NetHope beskrev – ved å slå seg sammen kan sivilsamfunnsorganisasjoner fremme at de trenger beskyttelse i likhet med myndigheter eller næringen, og dermed tiltrekke seg støtte.

Solidaritet i hendelsesrespons: Når en større hendelse inntreffer (for eksempel at en sivilsamfunnsorganisasjon rammes av et alvorlig angrep eller utsettes for nettbasert trakassering osv.), står et fellesskap sterkere overfor den. Andre sivilsamfunnsorganisasjoner kan hjelpe til med arbeidskraft, dele belastningen ved å sende ut offentlige meldinger eller tilby midlertidige tjenester. Det finnes tilfeller der f.eks. én menneskerettighetsgruppe ble utsatt for DDoS-angrep, og andre speilet innholdet på nettstedet deres for å holde det tilgjengelig (som digital solidaritet). Et slikt samarbeid om forsvar viser motstandere at et angrep på én vil samle mange andre, noe som kan virke avskrekkende.

Deling av suksesshistorier: Når du bygger et positivt fellesskap, bør du også dele suksesshistorier (noe som vil bli fremhevet i kapittel 7). Hvis én sivilsamfunnsorganisasjon lyktes med å avverge et phishing-forsøk takket være opplæring, bør du feire det i fellesskapets nyhetsbrev. Det motiverer alle til at det lønner seg å investere i sikkerhet. Anerkjenn og takk dem som hjelper andre med sikkerhet (kanskje på en årlig konferanse for sivilsamfunnsorganisasjoner kan du nevne den ene IT-frivillige som reiser rundt og installerer antivirusprogrammer gratis hos ulike sivilsamfunnsorganisasjoner – den typen moralboost fremmer fortsatt støtte).

Ved å utvikle et sammensveiset fellesskap rundt sikkerhet, går sivilsamfunnsorganisasjoner fra å være isolerte, sårbare mål til å være et motstandsdyktig nettverk. Angripere (enten det er kriminelle eller undertrykkende regimer) er ofte avhengige av å angripe isolerte organisasjoner. En samlet front betyr at informasjon om taktikken deres sprer seg raskt, og at tiltakene kan koordineres. Som et ordtak sier: «Det finnes sikkerhet i solidaritet.»

Informere offentligheten: Øke bevisstheten om digital sikkerhet

Sivilsamfunnsorganisasjoner fungerer ofte som samfunnsopplysere og -forkjempere. Digital sikkerhet er ikke bare et internt anliggende – mange av personene du jobber med (mottakere, medlemmer av fellesskapet, aktivister osv.) kan også dra nytte av bedre sikkerhetsbevissthet. Ved å spre kunnskap om digital sikkerhet til fellesskapet ditt i bredere forstand, multipliserer du virkningen og bidrar til å skape et tryggere miljø for sivilsamfunnet.

Samfunnsworkshopper og opplæring: Vurder å arrangere offentlige workshopper eller webinarer om grunnleggende digital sikkerhet for målgruppen din. Hvis dere for eksempel er en ungdomsorganisasjon, kan dere avholde en økt om «Holde seg trygg på sosiale medier» for tenåringer og foreldrene deres, som dekker personverninnstillinger, nettmobbing, nettfisking osv. Hvis du jobber med menneskerettighetsforkjempere, kan det kanskje passe med opplæring i sikker kommunikasjon (bruk av Signal, unngåelse av overvåking). Disse øktene kan integreres i den vanlige programplanen din. Mange sivilsamfunnsorganisasjoner tilbyr allerede opplæring i relaterte emner (f.eks. mediekompetanse, personvern på nettet) – du kan innlemme moduler fra dette pensumet. Å tilby slik opplæring hjelper ikke bare fellesskapet, men posisjonerer også sivilsamfunnsorganisasjonen din som ledende i håndteringen av aktuelle problemer, noe som kan styrke omdømmet og tilliten til dere.

Utvikle enkelt opplæringsmateriell: Du kan lage eller tilpasse brosjyrer, infografikker eller blogginnlegg om sikkerhetstips og dele dem offentlig. For eksempel en enkelsidig brosjyre med tittelen «Fem måter å beskytte deg selv på nettet» med enkle trinn (bruk sterke passord, ikke klikk på mistenkelige lenker, oppdater programvare osv.), som du deler ut på arrangementer eller på sosiale medier. Visuelt, ikke-teknisk språk fungerer best for et offentlig publikum. Du kan tilpasse innhold fra nasjonale bevisstgjøringskampanjer om cybersikkerhet (materiale fra cybersikkerhetsmåneden i oktober er ofte fritt tilgjengelig på flere språk via

ENISA eller andre). Sørg for at materialet er på det lokale språket og kontekstmessig relevant (nevn lokale svindelforsøk folk opplever, lokale støttekontakter). Dette kan også knyttes til organisasjonens oppdrag – f.eks. en forbrukerrettighetsorganisasjon som underviser i hvordan man unngår nettsvindel.

***Offentlige bevisstgjøringskampanjer*:** Dersom ressursene tillater det, kan du gjennomføre en kampanje om digital sikkerhet. Dette kan knyttes til for eksempel Safer Internet Day eller en relevant lokal hendelse (for eksempel en økning i SMS-svindel i området ditt). Bruk kommunikasjonskanalene dine til regelmessig å minne følgere om sikkerhet (tweete sikkerhetstips, dele nyheter om aktuelle svindelforsøk å passe seg for osv.). Noen sivilsamfunnsorganisasjoner samarbeider med telekommunikasjonsselskaper eller medier for å kringkaste sikkerhetsrelaterte offentlige servicemeldinger. Selv en kampanje i liten skala, som å legge ut ukentlige «Sikkerhetstips-tirsdager» på Facebook-siden din, kan sakte øke bevisstheten.

Utnytt medier og historiefortelling: Folk forstår gjennom historier. Hvis det er hensiktsmessig, kan du dele anonymiserte historier om digitale hendelser og hvordan de ble overvunnet (kanskje som en del av en blogg eller en foredrag). For eksempel en historie om hvordan e-postkontoen til en fellesskapsleder ble hacket og brukt til å sende falske meldinger, og hva man lærte av det. Det kan gjøre problemet mer menneskelig og varsle andre om å være forsiktige. Mediene kan også være interesserte hvis det finnes en trend (for eksempel økt målretting mot sivilsamfunnsorganisasjoner eller aktivister på nettet). Et intervju med sivilsamfunnsorganisasjonen din om emnet kan fremheve betydningen av digital sikkerhet for et bredere publikum.

Lobbyvirksomhet for bedre retningslinjer og støtte: På et høyere nivå kan du informere allmennheten og beslutningstakere om sivilsamfunnets behov for cybersikkerhet. Sivilsamfunnsorganisasjoner kan samlet fremme offentlige programmer som hjelper sivilsamfunnsorganisasjoner med cybersikkerhet (noen land har tilskuddsprogrammer eller spesielle CERT-tilbud). Arbeid også for brukervennlig sikkerhet i teknologiprodukter – f.eks. ved å presse programvarefirmaer til å gjøre sikre innstillinger til standard, slik at brukerne er tryggere uten å trenge omfattende ekspertise. I EU foregår det for eksempel dialoger om å

beskytte sivilsamfunnet mot cybertrusler. Civilsamfunnsorganisasjoners stemmer i disse foraene sikrer at politiske tiltak inkluderer dem (f.eks. finansiering og opplæring).

Samarbeid med skoler og biblioteker: Kanskje kan du samarbeide med lokale utdanningsinstitusjoner eller biblioteker for å arrangere felles økter om digital kompetanse og sikkerhet. Mange offentlige biblioteker avholder datakurs; å tilby et sikkerhetssegment kan være velkomment. Skoler har i økende grad behov for å undervise i nettsikkerhet; civilsamfunnsorganisasjoner med ekspertise kan støtte denne læreplanen. Ved å bidra til å utdanne ungdom og allmennheten bygger du et mer sikkerhetsbevisst samfunn, som indirekte også beskytter sivilsamfunnsorganisasjonen din (færre kompromitterte personlige kontoer som kan føre til spydphishing av organisasjonen din osv.).

Oppmuntre til rapportering og dialog: Oppfordre publikum du engasjerer deg med til å rapportere nettkriminalitet eller mistenkelige hendelser. Mange lider i stillhet eller skammer seg for mye (som om de har gått på en svindel). Skap et klima der folk kan søke hjelp – kanskje kan sivilsamfunnsorganisasjonen din fungere som megler for å veilede dem til politiet eller hjelpetelefoner hvis de er ofre for nettbasert trakassering eller svindel. Noen sivilsamfunnsorganisasjoner påtar seg en rolle som talsmenn for digitale rettigheter og fremhever temaer som personvern eller overvåking i samfunnet, noe som henger sammen med sikkerhetsbevissthet.

Tilpass deg oppdraget ditt: Skreddersy opplæring i offentlig sikkerhet i tråd med oppdraget ditt for å oppnå sammenheng. Hvis for eksempel sivilsamfunnsorganisasjonen din arbeider med kvinners rettigheter, og du vet at kvinnelige aktivister utsettes for trakassering på nettet, bør du fokusere bevisstgjøringen på dette og hvordan man håndterer det (blokkerings-/rapporteringsfunksjoner, opprettholdelse av personvern). Hvis dere er en miljøorganisasjon, kan dere fremheve hvordan falsk informasjon sprer seg på nettet og grunnleggende verifiseringspraksis – et sikkerhetsrelatert emne (informasjonsintegritet).

Ved å informere allmennheten utfører sivilsamfunnsorganisasjoner en dobbel tjeneste: De beskytter medlemmene sine og styrker sin egen sikkerhet ved å øke den generelle sikkerhets-«hygienen» i miljøet de opererer i. Det skaper en positiv sirkel der et bevisst fellesskap er mindre utsatt for å bli en smittebærer eller et offer for cyberhendelser.

Oppsummert er kunnskap makt, og som betrodde enheter i fellesskapet er sivilsamfunnsorganisasjoner godt plassert for å spre denne makten bredt.

Lokale og internasjonale støtteressurser

I tillegg til samarbeid mellom likemenn og offentlig bevissthet, finnes det formelle støtteressurser tilgjengelige for sivilsamfunnsorganisasjoner på lokalt, regionalt og internasjonalt nivå. Å vite hva disse er og hvordan du får tilgang til dem, kan gi svært tiltrengt hjelp, spesielt når du står overfor sofistikerte trusler eller trenger ressurser som overgår egne kapasiteter.

Lokale ressurser:

- **Nasjonale cybersikkerhetsbyråer/CERT-er:** Som nevnt tidligere har mange land et nasjonalt CERT (Computer Emergency Response Team) eller et cybersikkerhetsbyrå som tilbyr veiledning. Noen har programmer med fokus på sivilsamfunnsorganisasjoner eller små bedrifter. For eksempel tilbyr Storbritannias National Cyber Security Centre (NCSC) gratis veiledning og til og med noen gratis tjenester (som nettkontroll, e-postkontroll) for å forbedre sikkerheten for organisasjoner. Sjekk om ditt lands CERT har en oppsøkende tjeneste eller ressurser på ditt språk (de publiserer ofte varslingsbulletiner som du kan følge).
- **Politiets enheter for nettkriminalitet:** Hvis du opplever problemer som nettsvindel, trakassering eller et målrettet angrep, kan lokale politiets cyberenheter hjelpe deg. Noen land har spesielle enheter som samarbeider med sivilsamfunnet (spesielt i forbindelse med beskyttelse av journalister eller aktivister). Opprett et forhold om mulig – kanskje kan du invitere en tjenestemann til å holde et foredrag på et CSO-forum om rapportering av cyberhendelser, slik at du avmystifiserer prosessen.
- **Akademiske institusjoner:** Lokale universiteter, spesielt de med IT- eller cybersikkerhetsavdelinger, kan være allierte. Professorer eller studenter kan påta seg sikkerhetsoppgaver for sivilsamfunnsorganisasjoner som en del av forsknings- eller frivillighetsprosjekter. For eksempel kan en IT-klubb ved universitetet utføre en sikkerhetsrevisjon for organisasjonen din som et klasseprosjekt (med samtykke fra deg og

under tilsyn). Noen universiteter driver cybersikkerhetsklinikker eller har inkubatorer for løsninger innen sosial teknologi.

- **Teknologiselskapers lokale kontorer:** Store teknologiselskaper har ofte lokal tilstedeværelse og programmer for samfunnsansvar (CSR). De arrangerer av og til workshopper om digital kompetanse eller sikkerhet (Googles opplæring i nettsikkerhet, Metas kampanje for digital kompetanse osv.). Ta kontakt med dem for å inkludere organisasjonens ansatte eller mottakere i disse gratis opplæringene. De kan også donere eller gi rabatt på sikkerhetsprodukter. Cisco har for eksempel donert brannmurmaskinvare til noen ideelle organisasjoner gjennom partnerskap.
- **Støtteorganisasjoner for sivilsamfunnsorganisasjoner:** Enheter som teknologiføderasjoner eller -foreninger (f.eks. TechSoup – en global sivilsamfunnsorganisasjon som tilbyr rabattert programvare, inkludert sikkerhetspakker; i Europa finnes kanskje European Network of Civil Society Security osv.). Spesielt TechSoup tilbyr ikke bare programvare, men også ressurser for kapasitetsbygging og av og til webinarer om sikkerhet. Nasjonale nettverk av sivilsamfunnsorganisasjoner kan også ha arbeidsgrupper for IKT, der du kan få råd.

Internasjonale ressurser:

- **Access Nows hjelpetelefon for digital sikkerhet:** Som allerede nevnt, er dette et globalt tilgjengelig beredskapsteam for sivilsamfunnet som er tilgjengelig døgnet rundt. De opererer på flere språk (døgnet rundt på engelsk, spansk, fransk og andre språk). De kan hjelpe deg med alt fra veiledning om fjerning av skadevare til å dempe DDoS-angrep og gjenopprette kontoer. Det er gratis og konfidensielt.
- **CyberPeace Institute:** Denne organisasjonen analyserer ikke bare cyberangrep mot sivilsamfunnet, men koordinerer også bistand. Organisasjonens CyberPeace Builders-program har frivillige fra teknologiselskaper som tilbyr pro bono-hjelp til sivilsamfunnsorganisasjoner over hele verden. Du kan søke om å bli mottaker av programmet deres, som kan gi deg regelmessig ekspertise, for eksempel hjelp til å etablere sikker infrastruktur eller sikkerhetspolicyer.
- **Internasjonale organisasjoner for ytringsfrihet/digitale rettigheter:** Grupper som Front Line Defenders, The Engine Room, EFF (Electronic Frontier Foundation) og andre

publiserer ofte veiledninger eller kan sette deg i kontakt med eksperter. For eksempel har Front Line Defenders et «Digital Protection»-program og en «Security in a Box»-verktøykasse skreddersydd for menneskerettighetsforkjempere (med verktøy og taktikker).

- **Giverfinansierte programmer:** Noen ganger finnes det giverfinansierte prosjekter som er spesielt utformet for å øke civilsamfunnsorganisasjoners cybermotstandskraft. I EU har det for eksempel vært prosjekter under Erasmus+ eller CEF med fokus på å forbedre digitale ferdigheter, herunder sikkerhet for ideelle organisasjoner (KA220-prosjektet i tittelen din er kanskje et av dem). Hold utkikk etter oppfordringer eller nettverk under slike prosjekter – de produserer ofte verktøysett, arrangerer opplæring eller tilbyr rådgivning til deltakende sivilsamfunnsorganisasjoner.
- **Forum og konferanser:** Internasjonalt har konferanser som RightsCon, Internet Governance Forum (IGF) eller regionale cybersikkerhetskonferanser noen ganger spor for sivilsamfunnet. Deltakelse kan knytte deg til et globalt fellesskap og ressurser. RightsCon handler spesielt om digitale rettigheter og sikkerhet for aktivister. Mange økter gir praktiske råd eller fører til finansiører som kanskje kan støtte sikkerhetsforbedringene dine.
- **Finansieringsmuligheter:** Internasjonale stiftelser har anerkjent cybersikkerhet som en kritisk kapasitet for sivilsamfunnet. For eksempel har Ford Foundation og Open Technology Fund bevilget midler til sivilsamfunnsorganisasjoners cybersikkerhetsinitiativer. EU har finansieringslinjer under programmer som Horizon eller Digital Europe som kan støtte kapasitetsoppbygging hvis du inngår partnerskap eller søker. Hvis du trenger betydelige oppgraderinger (for eksempel å ansette IT-sikkerhetspersonell eller fornye IT-infrastrukturen), bør du vurdere å integrere dette i tilskuddsforslagene for kjernestøtte. Begrunn det som nødvendig risikoreduksjon – mange givere er mer bevisste nå og kan godkjenne budsjettet for dette.

Språklig og kulturell relevans: Når du søker hjelp, bør du prøve å finne den på ditt språk eller i din kontekst, hvis det er mulig. Globale ressurser er flotte, men de kan være på engelsk eller for generelle. Dette er grunnen til at lokale eksperter og oversettelse av internasjonale veiledninger til lokale språk er viktig. Hvis for eksempel sivilsamfunnsorganisasjonen din befinner seg i Tyrkia (jeg ser Istambuls tidssone i ledeteksten), kan det være enklere for de

ansatte å bruke en lokal tyrkisk ressurs (for eksempel en tyrkisk CERT-veiledning eller en opplæring i digital sikkerhet på tyrkisk). Hvis du ikke finner noen ressurser på ditt språk, kan du kanskje melde deg frivillig til å oversette en relevant veiledning – det er i seg selv et bidrag til fellesskapet.

Teknologidonasjoner: Når det gjelder støtte, bør du også merke deg ting som at Google for ideelle organisasjoner tilbyr gratis G Suite, Microsoft for ideelle organisasjoner tilbyr gratis O365-lisenser, Okta tilbyr gratis enkeltpåloggingsløsninger, og at noen sikkerhetsleverandører har donasjonsprogrammer for ideelle organisasjoner (f.eks. tilbyr NortonLifeLock en viss støtte til sivilsamfunnsorganisasjoner). Dette kan redusere kostnadsbarrierene for å bruke sikkerhetsverktøy på toppnivå.

Hold deg oppdatert: Trussellandskapet utvikler seg. Gjør det til en vane å følge noen nyhetsstrømmer om sikkerhet eller melde deg på e-postlister (noen er utvalgt for sivilsamfunnsorganisasjoner). For eksempel CIVICUS' e-postliste for cybersikkerhet (hvis den finnes), eller bare ved å følge troverdige kilder på sosiale medier (f.eks. @enisa_eu på Twitter for EU-nyheter, eller blogger fra lokale cybersikkerhetsselskaper).

Kort sagt: Du er ikke alene. Det finnes et nettverk av støtte, fra lokalt til globalt. Det er verdt å ta proaktivt kontakt med disse ressursene i rolige tider (ikke bare under en krise). Etabler relasjoner med viktige kontakter (vit hvem du ville ringt kl. 22.00 hvis noe gikk galt). Og på samme måte, når du tilegner deg kunnskap eller ressurser, bør du bidra tilbake til disse nettverkene – det er det som holder dem robuste og tilgjengelige for neste sivilsamfunnsorganisasjon i nød.

Ved å utnytte samarbeid (avsnitt 6.1, 6.2), opplyse allmennheten (6.3) og ta kontakt med støttesystemer (6.4), kan sivilsamfunnsorganisasjoner forvandle digital sikkerhet fra en skremmende solokamp til en innsats som støttes av fellesskapet. I neste kapittel skal vi se på konkrete eksempler og vanlige fallgruver for å lære mer av erfaringer fra den virkelige verden.

Kapittelsammendrag

Kapittel 6 gir rammer for at sivilsamfunnsorganisasjoner proaktivt kan identifisere risikoer og forberede seg på cyberhendelser. Det veileder organisasjoner i å vurdere kritiske ressurser (f.eks. donordatabaser) og sårbarheter ved hjelp av enkle risikovurderingsmaler for å prioritere trusler som phishing eller løsepengevirus. Kapitlet skisserer utarbeidelsen av en hendelsesresponsplan og beskriver trinnene for oppdagelse, inndamming, kommunikasjon og gjenoppretting. For eksempel kan en sivilsamfunnsorganisasjon med en beredskapsplan raskt gjenopprette data etter et løsepengevirusangrep og minimere skadene. Det legger vekt på å dokumentere hendelser for å lære av dem og å oppdatere planene årlig. Kapitlet tar for seg GDPRs regel om 72-timers varsling ved databrudd, og sikrer samsvar. Praktiske trinn omfatter tildeling av roller (f.eks. en personvernansvarlig) og testing av planer via simuleringer. Kapitlet fokuserer på forberedelser som hjelper sivilsamfunnsorganisasjoner med å komme seg raskt, og redusere skader på driften og omdømmet. Ved å tilby klare rammeverk til lave kostnader, gir den ikke-teknisk personale mulighet til å bidra til motstandskraft, i tråd med e-bokens mål om å gjøre cybersikkerhet oppnåelig for organisasjoner med begrensede ressurser.

Mal for personvernpolicy for sivilsamfunnsorganisasjoner

Organisasjonsnavn: [Sett inn navnet på sivilsamfunnsorganisasjonen]

Ikrafttredelsesdato: [Sett inn dato]

Sist oppdatert: [Sett inn dato eller «Ikke relevant for første versjon av retningslinjene»]

Denne personvernpolicyen beskriver hvordan [navn på sivilsamfunnsorganisasjon] innhenter, lagrer, får tilgang til og beskytter personopplysninger for å sikre personvern, sikkerhet og overholdelse av gjeldende lovgivning (f.eks. GDPR, [sett inn lokal personvernlovgivning]). Den gjelder for alle ansatte, frivillige og partnere som håndterer personopplysninger, og sikrer tilliten til mottakere, givere og interessenter.

Denne policyen omfatter alle personopplysninger (f.eks. navn, kontaktopplysninger, helseopplysninger eller økonomiske opplysninger) som forvaltes av [CSO-navn], herunder opplysninger knyttet til mottakere, givere, ansatte og frivillige.

1. Datainnsamling

Vi innhenter kun personopplysninger som er nødvendige for oppdraget og programmene våre, og innhenter informert samtykke der det er nødvendig. Opplysninger innhentes på en lovlig og åpen måte og til bestemte formål.

Prosedyrer:

⇒ Forklar tydelig hvorfor opplysninger innhentes og hvordan de kommer til å brukes før innhenting (f.eks. via samtykkeskjemaer eller personvernerklæringer).

⇒ Innhente et minimum av opplysninger for å oppnå formålet (prinsippet om dataminimering).

⇒ Dokumentere formålet med innhentingen og innhente samtykke der det er aktuelt (f.eks. signerte skjemaer, avkrysningsbokser på nettet).

2. Datalagring

Vi lagrer personopplysninger på en sikker måte ved hjelp av kryptering og beskyttede systemer for å forhindre uautorisert tilgang, tap eller tyveri.

Prosedyrer:

⇒ Lagre data på sikre plattformer (f.eks. krypterte skytjenester som Google Drive med 2FA, eller låste fysiske filer).

⇒ Kryptere sensitive data i hvile (f.eks. på bærbare datamaskiner, eksterne stasjoner) og under overføring (f.eks. ved hjelp av HTTPS eller sikker e-post).

⇒ Opprettholde regelmessige sikkerhetskopier (f.eks. ukentlig til en sikker sky eller en ekstern harddisk) for å sikre datagjenoppretting.

⇒ Avhende data på en sikker måte når de ikke lenger er nødvendige (f.eks. makulere papiroppføringer, bruke sikre sletteverktøy for digitale filer).

3. Tilgangskontroll

Tilgang til personopplysninger er begrenset til autorisert personell som trenger dem i forbindelse med sin rolle, i henhold til prinsippet om minst mulig privilegium.

Prosedyrer:

⇒ Tildel tilgang basert på arbeidsroller (f.eks. at kun programledere får tilgang til mottakerdata).

⇒ Bruke sterke passord og tofaktorautentisering (2FA) for alle kontoer med tilgang til personopplysninger.

⇒ Revider tilgangstillatelser regelmessig (f.eks. månedlig) for å fjerne tilgang for tidligere ansatte eller frivillige.

⇒ Opplære ansatte og frivillige i sikker datahåndtering (f.eks. å ikke dele passord, logge av etter bruk).

4. Rapportering av brudd

Vi oppdager, reagerer på og rapporterer personvernbrudd umiddelbart for å minimere skade og overholde juridiske forpliktelser (f.eks. GDPRs regel om varsling innen 72 timer).

Prosedyrer:

⇒ Utpek en databeskyttelsesansvarlig eller kontaktperson (f.eks. [sett inn navn/rolle]) som skal håndtere brudd.

⇒ Rapporter mistenkte brudd umiddelbart til den utpekte personen (f.eks. via e-post til [sett inn e-postadresse]).

⇒ Varsle den relevante databeskyttelsesmyndigheten (f.eks. [sett inn navn på lokal myndighet]) innen 72 timer dersom et brudd risikerer å skade enkeltpersoner.

⇒ Informer berørte personer (f.eks. mottakere, givere) om nødvendig, og gi klar veiledning om de neste trinnene.

⇒ Dokumenter alle brudd og tiltak for å forbedre fremtidig forebygging (f.eks. oppdatere risikovurderingen).

5. Ansvar

Ledelse: Godkjenne og finansiere iverksettingen av policyen (f.eks. budsjett for opplæring, verktøy).
Ansatte og frivillige: Følge denne policyen, rapportere problemer umiddelbart og delta på opplæring i personvern.
Personvernombud/kontaktperson: Overvåke overholdelse av retningslinjene, håndtere brudd og koordinere årlige gjennomganger.

6. Overholdelse og gjennomgang

Overholdelse: Denne policyen er i samsvar med GDPR og [sett inn lokal personvernlovgivning]. Manglende overholdelse kan føre til disiplinærtiltak eller juridiske sanksjoner.
Gjennomgå og oppdater denne policyen årlig eller etter vesentlige endringer (f.eks. nye programmer, forskrifter). Neste gjennomgang: [Sett inn dato, f.eks. november 2026].
Alt personale og alle frivillige mottar opplæring i personvern ved ansettelse og årlig.

7. Kontakt

Dersom du har spørsmål eller ønsker å rapportere et brudd, kan du kontakte: [Sett inn personvernombudets/kontaktpersonens navn, e-postadresse, telefonnummer].
Lokal databeskyttelsesmyndighet: [Sett inn navn og kontaktinformasjon, f.eks. «Tyrkias databeskyttelsesmyndighet (KVKK), [kontaktopplysninger]».

Godkjent av: [Sett inn navn på leder/rolle, f.eks. daglig leder]

Dato: [Sett inn dato]

Merknader om tilpasning: Erstatt plassholdere (f.eks. [navn på sivilsamfunnsorganisasjon], [lokal personvernlovgivning]) med organisasjonens opplysninger. Legg til lokale samsvarskrav eller spesifikke verktøy etter behov.

2.7 KAPITTEL 7: SIKKERHETSSUKSESSER I CIVILSAMFUNNSORGANISASJONER

Virkelige historier: Sikkerhetssuksesser i sivilsamfunnsorganisasjoner

Det er oppmuntrende å finne ut hvordan lignende organisasjoner har overvunnet sikkerhetsutfordringer. Her er noen anonymiserte, men realistiske scenarier som viser positive resultater takket være god sikkerhetspraksis:

Phishing-forsøk forpurret av opplæring: En menneskerettighetsorganisasjon i Øst-Europa mottok en e-post som så ut som en Google Docs-deling fra en kollega. Fordi personalet hadde gjennomgått opplæring i phishing-bevissthet, la et teammedlem merke til at noe var galt (avsenderens e-postadresse var skrevet med et lite feilstavingsfeil), og klikket ikke på lenken. I stedet varslet hun IT-ansvarlig. De bekreftet at det var et phishing-forsøk for å stjele påloggingsinformasjon. Som et resultat ble ingen kontoer kompromittert. Dette understreket verdien av opplæring – på det påfølgende personalmøtet fremhevet direktøren for sivilsamfunnsorganisasjonen hvordan den ansattes forsiktighet beskyttet alle, og gjorde det til et lærerikt øyeblikk. Det var en suksess ved at et angrep ble forhindret uten skade, takket være en årvåken medarbeider.

Overlevde angrep med løsepengevirus takket være sikkerhetskopier: En mellomstor sivil samfunnsorganisasjon innen helse i Afrika ble utsatt for et angrep med løsepengevirus en morgen – de ansatte oppdaget at filene deres var kryptert og at det sto en løsepenningskrav på skjermene deres. I begynnelsen var det kaos. Organisasjonen hadde imidlertid et robust sikkerhetskopisystem: Alle kritiske data ble sikkerhetskopiert til en ekstern server hver kveld. I løpet av få timer isolerte IT-konsulenten de infiserte maskinene, slettet innholdet, installerte programvaren på nytt og gjenopprettet dataene fra sikkerhetskopien fra kvelden før. De tapte maksimalt én dags arbeid med noen få dokumenter. De betalte ikke løsepengene og rapporterte hendelsen. Denne opplevelsen ble til en sikkerhetssuksesshistorie de deler – investeringen i sikkerhetskopiering og gjenopprettingsplanlegging lønnet seg, og beviste hvor viktig det er. Senere presenterte de til og med denne saken i et webinar, og oppfordret andre sivilsamfunnsorganisasjoner til å iverksette sikkerhetskopiering offline.

Sikker kommunikasjon beskyttet sensitive planer: En påvirkningskoalisjon organiserte en kampanje i et land med omfattende overvåking. De mistenkte at kommunikasjonen deres ble overvåket. Under veiledning fra en konsulent innen digital sikkerhet byttet de til å bruke

ende-til-ende-kryptert meldingstjeneste (Signal) og e-post med PGP for de mest sensitive vedleggene. Under kampanjen la de merke til forsøk fra motstandere på å forutse strategien deres, men kritiske detaljer ble aldri lekket. Analyser etter kampanjen tydet på at opposisjonen hadde mistet «innsidekunnskaps»-fordelen etter at de byttet til sikker kommunikasjon. Koalisjonen krediterer de sikre verktøyene for å ha beskyttet planene deres og bidratt til kampanjens suksess. Det befestet forpliktelsen deres til å bruke krypterte kanaler for fremtidige operasjoner og fungerte som et eksempel for andre i nettverket deres.

Tofaktorautentisering forpurret kontokapring: En sivilsamfunnsorganisasjon for kvinners rettigheter i Sør-Asia fikk et av de ansattes Gmail-kontoer utsatt for et målrettet phishing-e-postangrep. Den ansatte oppga ved et uhell passordet sitt på en falsk Google-innloggingsside. Passordet gikk til angriperen. Kort tid etter prøvde angriperen fra et annet land å logge seg på Google-kontoen hennes – men fordi sivilsamfunnsorganisasjonen hadde iverksatt tofaktorautentisering på alle kontoer, krevde påloggingen en verifikasjonskode fra telefonen hennes. Angriperen hadde ikke den, så han ble stoppet. Google varslet brukeren om et blokkert påloggingsforsøk. Hun innså umiddelbart hva som hadde skjedd, rapporterte det og endret passordet sitt. Til slutt gjorde 2FA det som kunne ha blitt et alvorlig innbrudd til en ren skremmeskapsel uten at det oppstod skade. Denne virkelige hendelsen fikk virkelig hele teamet til å innse hvorfor de noe irriterende 2FA-forespørslene var verdt det. Det var en dag med lettelse og en seier for sikkerhetstiltakene deres.

Samarbeid i fellesskapet stoppet DDoS: Et nettverk av miljøorganisasjoner lanserte en kampanje som vakte vrede hos noen motstandere, som deretter satte i gang et DDoS-angrep (Distributed Denial of Service) på nettverkets felles nettsted (ved å oversvømme det med trafikk for å få det til å gå offline). Hver for seg hadde organisasjonene begrensede IT-ressurser til å dempe dette. Gjennom en teknologisk solidaritetskanal tok imidlertid en leder for en sivilsamfunnsorganisasjon raskt kontakt for å be om hjelp. En partnerorganisasjon i et teknologiselskap ordnet med midlertidig bruk av DDoS-beskyttelsestjenesten sin (Cloudflare), og IT-personalet til en annen sivilsamfunnsorganisasjon hjalp til med å omdirigere nettstedet gjennom denne beskyttelsen. Innen få timer var nettstedet oppe igjen til tross for angrepet, og kampanjen fortsatte. Denne samarbeidsbaserte responsen var en suksesshistorie som

illustrerer hvordan støtte fra allierte kan motvirke selv store cybertrusler. Det lærte dem også å konfigurere permanent Cloudflare-beskyttelse etterpå. Senere skrev de om denne saken i en blogg for å takke dem som hjalp, og for å veilede andre i håndteringen av DDoS.

Disse historiene viser at selv når sivilsamfunnsorganisasjoner er mål for cybertrusler, **kan beredskap og raske tiltak føre til et vellykket forsvar eller rask gjenoppretting**. Fellesnevnerne er: forhåndsinvestering i sikkerhetstiltak (opplæring, sikkerhetskopier, 2FA), rask gjenkjenning og respons, og utnyttelse av støttenettverk. Ved å dele og studere slike suksesser kan sivilsamfunnsorganisasjoner lære hva som virkelig fungerer og få tillit til at også de kan håndtere lignende situasjoner.

Vanlige feil og hvordan man kan forhindre dem

Det er avgjørende for å forbedre sikkerheten å lære av andres feil (eller våre egne). Her er noen vanlige fallgruver som organisasjoner i sivilsamfunnet støter på, sammen med strategier for å unngå dem:

Bruk av svake passord eller standardpassord: Den kanskje mest utbredte feilen er å holde seg til enkle passord (som «123456», «password») eller la standardpassord stå uendret på enheter (f.eks. leveres rutere ofte med «admin/admin»). Dette er en gave til angripere. Forebygging: Etabler en passordpolicy som krever sterke, unike passord, og bruk passordbehandlere til å håndtere dem. Under opplæringen bør du vise eksempler på dårlige kontra gode passord. Og når du konfigurerer ny maskinvare/programvare, må du umiddelbart endre standardpåloggingsinformasjon (og dokumentere den på en sikker måte). Gjennomfør sporadiske revisjoner – bruk et verktøy eller et skript for å sjekke om noen kontoer har svake passord (noen organisasjoner bruker databaser over datainnbrudd eller revisjonsverktøy). Legg vekt på 2FA for å kompensere for eventuelle svake passord som slipper gjennom.

Klikke uten å tenke (vellykket phishing): Mange datainnbrudd starter med at noen klikker på en skadelig lenke eller et vedlegg uten å undersøke det nøye. Feilen er å handle på impuls fra en e-post eller melding melding (spesielt de som appellerer til hastverk eller nysgjerrighet), i stedet for å verifisere ektheten. Forebygging: Opplæring, opplæring, opplæring. Kjør simulerte phishing-tester for å identifisere hvem som trenger mer øving. Oppmuntre til en kultur der det er greit å senke farten og verifisere forespørsler – f.eks.: «Hvis en e-post virker

presserende og ber om penger eller tilgangsopplysninger, er det greit (faktisk oppmuntret) å dobbeltsjekke med en telefon eller en separat e-post.» Tilby enkle sjekklister: Kontroller avsenderadressen nøye, se etter stavefeil, ikke last ned uventede vedlegg osv. I tillegg bidrar tekniske forsvarstiltak som gode søppelfiltre og skanning av lenker til å filtrere bort åpenbare svindelforsøk.

***Unnlatelse av å oppdatere programvare i tide*:** Et vanlig scenario: En civilsamfunnsorganisasjons nettsted kjører på WordPress, men har ikke oppdatert programtillegg på ett år, og en angriper utnytter en kjent feil til å ødelegge det. Eller så kjører de ansattes PC-er fortsatt eldre operativsystemversjoner med sårbarheter som ikke er oppdatert. Feilen er å utsette eller ignorere oppdateringer (noen ganger av frykt for at det kan ødelegge noe, noen ganger bare fordi man glemmer det). Forebygging: Aktiver automatiske oppdateringer der det er mulig. På systemer som ikke kan oppdateres automatisk, bør du gi noen i oppdrag å sjekke dette månedlig. Bruk verktøy som samler oppdateringsbehov (selv om det bare er å slå på varsler om «Se etter oppdateringer»). For nettsteder bør du vurdere administrert hosting som tar seg av oppdateringene, eller abonnere på e-postlister for programtilleggssikkerhet. Legg vekt på «oppdateringstirsdag» eller en annen rutine. Hvis ressursene tillater det, bør du føre en oversikt over kritisk programvare og spore oppdateringsstatusen (det finnes gratis skannere som fremhever manglende oppdateringer). Avkref også myter som «oppdateringer gjør datamaskinen tregere» ved å vise sikkerhetsrisikoene ved å ikke oppdatere.

Ikke sikkerhetskopiere (eller teste sikkerhetskopier): Noen organisasjoner innser først viktigheten av sikkerhetskopier etter et tap av data. Feilene inkluderer å ikke sikkerhetskopiere i det hele tatt, eller å ha sikkerhetskopier, men ikke teste dem (og deretter oppdage at de er ufullstendige eller ødelagte når det trengs). Forebygging: Implementer en 3-2-1-sikkerhetskopistrategi (flere kopier, forskjellige medier, én ekstern). Planlegg sikkerhetskopier og automatiser dem. Enda viktigere er det å kjøre testgjenopprettinger regelmessig. En enkel øvelse: Velg en tilfeldig fil og prøv å gjenopprette den fra sikkerhetskopien for å sikre at prosessen fungerer. Sørg også for at selve sikkerhetskopiene er sikret (kryptert og ikke tilgjengelige for det vanlige nettverket, slik at løsepengevirus ikke kan angripe dem). Mange har

lært på den harde måten at en sikkerhetskopi på en nettverksstasjon som er tilgjengelig for alle, ikke er trygg mot krypteringsmalware. Løsninger: Sikkerhetskopier som lagres offline, eller i det minste versjonskontrollerte sikkerhetskopier i skyen, er immune mot kryptering.

Overprivilegium og delte kontoer: Feil: Å gi alle brukere administratorrettigheter «fordi det er enklere», eller dele én pålogging mellom flere personer for enkelhets skyld. Dette kan føre til store problemer – én person kan utilsiktet installere skadevare med administratorrettigheter, eller en ansatt som har sluttet i selskapet vet fortsatt passordet til den delte kontoen. Og ansvarligheten går tapt når kontoer deles (du kan ikke si hvem som gjorde hva). Forebygging: Anvend prinsippet om minst mulig privilegium. Opprett individuelle kontoer for alle, og gi dem kun den tilgangen de trenger. Bruk rollebaserte tillatelser for filer og systemer. Ja, det krever litt mer innledende oppsett, men moderne systemer gjør det ganske enkelt å administrere brukere. Ha også en tydelig sjekkliste for onboarding/offboarding, slik at tilgang tildeles og tilbakekalles systematisk. For administratoroppgaver bør du ha en egen administratorkonto – ikke surf på nettet eller les e-post som administratorbruker. På den måten kan skaden begrenses til brukernivået, selv om en bruker blir lurt.

Ignorere sikkerhetsadvarsler eller beste praksis: Mennesker ignorerer noen ganger nettleservarslene («Dette nettstedets sertifikat er ikke pålitelig») eller deaktiverer sikkerhetsfunksjoner fordi de virker irriterende («La meg slå av brannmuren for å få denne appen til å fungere»). Det kan åpne dører for angrep. Et annet eksempel: Å bruke utdaterte, usikre protokoller (som FTP i stedet for SFTP) av vane. Forebygging: Opplys om hvorfor advarsler finnes. Forklar for eksempel hva en sertifikatadvarsel betyr, og at den kan tyde på et falskt nettsted eller avlytting. Skap et miljø der de ansatte, hvis et sikkerhetstiltak blokkerer noe, ber om riktige løsninger (f.eks. legge til et unntak hvis det er et kjent trygt internt nettsted osv.) i stedet for å deaktivere det. Gi veiledning: Hvis antivirusprogrammet flagger en fil, må du ikke bare hviteliste den av frustrasjon – kontakt IT for å analysere om den virkelig er trygg. Skriv enkle interne vanlige spørsmål: «Hvis du ser en sikkerhetsadvarsel, gjør X.» Når du konfigurerer nye verktøy, bør du også gjøre det på en sikker måte fra starten av, slik at de ansatte ikke fristes til å bruke usikre løsninger.

Mangel på hendelsesresponsplan: Mange CSO-er blir overrasket under en hendelse – de vet ikke hvem de skal ringe eller hvilke tiltak de skal iverksette, noe som kaster bort dyrebar tid. Feil: Ingen forhåndsdefinert hendelsesplan eller øvelser. Forebygging: Utarbeid en grunnleggende hendelsesresponsplan (som beskrevet i kapittel 5), og sørg for at alle kjenner til det grunnleggende i den. Det kan være bare én side: «Hvis det skjer noe rart: Koble fra internett, ring denne personen, osv.» Gjennomfør også minst én bordøvelse: Gjennomgå et hypotetisk «Hva om vi ble utsatt for løsepengevirus, hva ville vi gjort?» for å oppdage hull. Å ha en plan reduserer feil under virkelige kriser, som å slå av feil system eller få panikk.

Ved å være klar over disse vanlige feilene kan en sikkerhetssjef iverksette proaktive tiltak for å unngå å gå i disse fellene. Det er ofte små endringer i atferd eller retningslinjer som utgjør en stor forskjell – for eksempel vanen med å installere oppdateringer eller dobbeltsjekke før man klikker. Oppmuntre til en filosofi om at «**alle er interessenter i sikkerhet»,** slik at feil kan oppdages eller forhindres gjennom kollektiv aktsomhet (f.eks. gjensidig gjennomgang av mistenkelige e-poster – «Hei, kollega, ser dette ut som det er i orden for deg?» kan forhindre en feil).

Oppsummert: Gjør svake passord sterkere, tenk før du klikker, hold alt oppdatert, sikkerhetskopier flittig, begrens privilegier, ta hensyn til advarsler og planlegg for det verste. Ved å unngå disse vanlige feilene kan du forbedre sikkerhetssituasjonen din dramatisk til ganske lave kostnader.

Test din egen sikkerhet: Enkle øvelser

Det er én ting å lese om sikkerhet, og en annen å omsette det i praksis. Her er noen enkle egenvurderinger og øvelser du (og teamet ditt) kan gjøre for å måle og forbedre sikkerhetsberedskapen. Tenk på dem som «sikkerhetsøvelser» eller kontroller:

Phishing-øvelse: Lag en ufarlig «falsk phishing-e-post» for å teste bevisstheten i teamet ditt. Send for eksempel en e-post fra en adresse som ikke tilhører organisasjonen, men bruk organisasjonens navn i visningen, med et emne som «Haster: oppdatering kreves» og en lenke til et Google-skjema (som bare sier «Gratulerer, dette var en test!»). Se hvem som klikker eller sender inn informasjon. Målet er pedagogisk, ikke å fange noen: Etterpå avdekker du det og diskuterer hint om at det var phishing (kanskje en liten adresseforskjell, presserende tone osv.). Hvis få falt for det, er det flott – hvis noen gjorde det, kan du bruke det som en mild opplæringsmulighet. Alternativt kan du bruke gratis verktøy som Googles phishing-quiz eller phishing-simuleringsverktøy (noen AV-pakker har denne funksjonen) på en kontrollert måte.

Kontroll av passordstyrke: Ta en titt på noen passord (uten å be noen om å avsløre sine – du kan simulere vanlige mønstre). Bruk en passordstyrkemåler (mange finnes på nettet, f.eks. Passwordmeter.com) til å teste et utvalg av typiske passord sammenlignet med anbefalte passord. Enda bedre er det å bruke en passordbehandler og se om den rapporterer svake/gjenbrukte passord – mange har en sikkerhetsrevisjonsfunksjon. Som en øvelse kan du be alle om å opprette en sterk passfrase bestående av fire tilfeldige ord (f.eks. «apple caravan tiger dance») og teste styrken mot noe sånt som «Winter2020!» – resultatene viser ofte at passfrasen er sterkere og enklere å huske. Dette forsterker gode vaner for oppretting av passord.

Øvelse i gjenoppretting av sikkerhetskopi: Test sikkerhetskopien din. Simuler et scenario: «Vi mistet fil X, hva gjør vi?» Gå faktisk til sikkerhetskopieringsstedet ditt, hent filen og åpne den for å sikre at den er intakt. Eller velg en dato og lat som om du må tilbakestille alt til hvordan det var den gangen – kan du hente sikkerhetskopien fra den datoen? Mål hvor lang tid det tar å gjenopprette et representativt datasett. Dette verifiserer ikke bare sikkerhetskopier, men forbereder deg også på virkelige hendelser ved å avdekke om instruksjoner/tilgangsopplysninger for sikkerhetskopier er lett tilgjengelige. Kanskje du kan be

noen andre (ikke den vanlige IT-personen) om å prøve å gjenopprette ved hjelp av kun dokumenterte trinn for å se om prosessen er tilstrekkelig tydelig.

Sikkerhetsrevisjon av enheter: Utfør en rask revisjon av kontorets datamaskiner og telefoner (med tillatelse, selvfølgelig). Sjekk: Er alle operativsystemer oppdatert (åpne Windows Update eller tilsvarende, se siste oppdateringsdato)? Kjører antivirusprogrammet, og er det oppdatert? Er brannmurene på? Er det noen enheter som fortsatt bruker standardpassord (f.eks. logg inn på kontorets ruter og se om standardpåloggingsinformasjon fungerer – hvis ja, er det et stort varsel om å endre det)? Sjekk om skjermene låses automatisk når de er inaktive. Du kan lage en enkel sjekkliste og gi hver datamaskin en poengsum. Løs deretter eventuelle problemer som dukker opp, og feir hvis de fleste tingene var sikre som standard (det validerer konfigurasjonspraksisen din).

Test av e-postsvindel: En interessant øvelse: Vis hvor enkelt det kan være å forfalske e-poster, for å øke skepsisen. Ved hjelp av et kontrollert miljø (for eksempel en tjeneste som gjør det mulig å sende e-poster fra en egendefinert adresse du eier, eller til og med bare endre «Fra»-navnet i Gmail), kan du sende deg selv en e-post som ser ut til å være fra f.eks. «» (men som kommer fra et annet domene). Vis personalet hvordan det ved første øyekast ser overbevisende ut, men at e-postoverskriftene eller den faktiske adressen avslører sannheten. Denne øvelsen sjokkerer ofte folk, og deretter sjekker de e-postadresser mer nøye.

Opprydding av tillatelser: Ta én delt mappe eller Google Drive og kontroller hvem som har tilgang. Du kan oppdage at tidligere frivillige fortsatt har tilgang, eller at noen filer utilsiktet er delt med offentlige lenker. Som en «miniøvelse» kan du trekke tilbake all unødvendig tilgang og dokumentere det. Det er som en vårrengjøring av tilgangsrettigheter. Dette fungerer som en påminnelse om å gjøre dette med jevne mellomrom.

Hendelsesrollespill: Velg et scenario (for eksempel «bærbar PC stjålet fra kafé» eller «løsepengevirus på server») og gå muntlig gjennom hvordan du ville reagert (hvem du skulle ringt, hvilke tiltak du skulle iverksatt). Rollespill med personalet: Én spiller den panikkslagne brukeren, en annen IT-beredskapspersonen osv. Denne uformelle øvelsen kan avdekke hull («Å, vi har faktisk ikke bankens nummer tilgjengelig for å ringe og fryse kontoer hvis e-posten ble

kompromittert», eller «Vi innser at vi ikke kan administratorpassordet til nettstedet vårt utenat hvis LastPass er utilgjengelig»). Det er bedre å finne det ut nå enn under en virkelig krise.

Hver øvelse er ment å være enkel og ikke tidkrevende, men svært innsiktsfull. Tenk på det som en brannøvelse for cybertrusler – du øver i omgivelser der det ikke står mye på spill, slik at du i en reell nødssituasjon vet hva du skal gjøre og føler deg mindre engstelig fordi du har gjort noe lignende tidligere.

Etter hver øvelse bør dere diskutere resultatene åpent og uten å legge skylden på noen. Dersom noe gikk galt (f.eks. at halvparten av teamet strøk på phishing-testen), bør dere behandle det som kollektiv læring: Kanskje phishing-e-posten var virkelig snikende – nå vet alle at de må være på vakt mot det trikset neste gang. Hvis en øvelse avslører en alvorlig svakhet, bør du takke prosessen for at den avdekket den og forplikte deg til å rette opp i den.

Regelmessige øvelser av denne typen holder sikkerheten i folks tanker og fremmer en kultur for kontinuerlig forbedring. Det avmystifiserer sikkerhet (fordi du aktivt gjør ting, ikke bare hører om retningslinjer). Det kan til og med være gøy på en måte – noen organisasjoner «gamifiserer» det og tilbyr små belønninger til dem som oppdager phishing eller har færrest problemer i revisjoner.

Integrere digital sikkerhet i den daglige rutinen

Det endelige målet er at god sikkerhetspraksis skal bli en naturlig del av hvordan du og organisasjonen din opererer. Her er tips til hvordan du kan veve digital sikkerhet sømløst inn i hverdagen hos CSO:

Start dagen med sikkerhet i tankene: Oppmuntre til enkle morgenvaner. Når du for eksempel starter datamaskinen, bør du la den installere oppdateringer først før du setter i gang med arbeidet (ta en kaffe mens den oppdaterer i stedet for å trykke på «Utsett»). Eller sjekk eventuelle sikkerhetsvarsler (for eksempel «Windows Defender: ingen problemer funnet» eller en melding om programvareoppdatering) og ta hånd om dem tidlig. Dette sikrer at du begynner å jobbe i en sikker tilstand i stedet for å ignorere de små skjoldene og utropstegnene på oppgavelinjen.

Passordbehandler hver dag: Gjør bruk av passordbehandleren til en rutinemessig del av påloggingsprosessene. Hvis den er riktig konfigurert, kan den fylle ut påloggingsinformasjon

automatisk – slik at de ansatte raskt ser fordelen (raskere pålogging, ingen problemer med å tilbakestille passord), og det blir bare måten de logger på på. Den daglige rutinen endres fra «huske eller skrive ned passord» til «låse opp administrasjonsverktøyet én gang med en sterk passfrase og deretter klikke for å logge på overalt». Over tid kommer de ikke til å kunne forestille seg livet uten den. Noen passordbehandlere ber også om å oppdatere svake passord – kanskje kan du sette av noen minutter hver fredag til å oppdatere ett flagget passord. Smått og smått får alle kontoer sterkere passord.

Team-påminnelser og -kultur: Inkluder sikkerhetstips i vanlige teammøter eller interne nyhetsbrev. På et ukentlig møte kan for eksempel ett punkt på dagsordenen være et sikkerhetstips eller en sikkerhetsnyhet på ett minutt (f.eks.: «Til orientering: Det er for øyeblikket en WhatsApp-svindel i omløp. Husk å ikke dele verifiseringskoder»). Dette normaliserer samtalen. Det trenger ikke å dominere, bare en rutinemessig oppfølging. Noen sivilsamfunnsorganisasjoner henger opp en plakat med «Månedens sikkerhetstips» på veggen eller Slack-kanalen, som passivt holder bevisstheten synlig i hverdagen.

Lås skjermer og ryddede skrivebord: Gjør det til en vane å låse datamaskinen (Win+L på Windows, Ctrl+Cmd+Q på Mac) hver gang du går bort – selv om det bare er for et øyeblikk. Hvis alle gjør det, føles det normalt, ikke paranoidt. Det samme gjelder for å unngå at sensitive papirer eller USB-minnepinner ligger fremme (den gamle «ryddig skrivebord»-policyen). Det er enklere i rutinen hvis du knytter det til noe: F.eks. på slutten av dagen, det siste du gjør: Sikkerhetskopier filer, lås alle skap, sjekk at du er logget av systemene – da vet du at du er klar. Du kan kanskje lage en trykt sjekkliste for sikker avstengning av kontoret (digitalt og fysisk) som de ansatte følger daglig til det blir en vane.

Integrer sikkerhet i arbeidsflyter: Uansett hvilke verktøy du bruker, bør du bruke sikkerhetsfunksjonene som standard. Eksempel: Hvis du deler en fil via skyen, bør du rutinemessig bruke «del med bestemte personer» i stedet for lenken. Det tar kanskje 10 sekunder lenger å skrive inn e-postadressen deres, men hvis det blir den eneste måten folk deler på, er det helt normalt. Eller planlegg periodiske tillatelsesgjennomganger som en del av prosjektavslutningen: Når et prosjekt er ferdig, er f.eks. en del av oppsummeringslisten

«gjennomgå og fjern eventuell ekstern tilgang fra prosjektmapper». På den måten blir sikkerhetsvedlikehold en del av prosjektledelsens livssyklus.

Oppdateringstirsdag (eller en valgt dag): Mange organisasjoner planlegger når de skal utføre vedlikeholdsoppgaver. Kanskje sørger IT-avdelingen/den utpekte personen tirsdag morgen for at operativsystemet og appene er oppdatert på alle enheter, eller kanskje hver bruker sjekker etter telefonoppdateringer ukentlig. Hvis det er forventet og planlagt, vil det ikke bli sett på som et avbrudd, men som en rutine (på samme måte som vi vanner plantene hver mandag, oppdaterer vi systemene). Skytjenester oppdaterer seg selv, men kanskje bør du sjekke administrasjonskonsollen månedlig for eventuelle varsler eller nye sikkerhetsfunksjoner som skal aktiveres (leverandører legger ofte til nye sikkerhetsinnstillinger – det er lurt å sette av tid til å integrere disse regelmessig).

Kontinuerlig læring: Oppmuntre de ansatte til å ta korte nettkurs eller quizer av og til. Kanskje alle gjennomfører én modul av et nettbasert sikkerhetskurs per kvartal (noen er interaktive og korte). Hvis du for eksempel setter av en time av arbeidstiden til dette, viser det organisasjonens engasjement. Dette holder kunnskapen oppdatert og signaliserer at sikkerhet er en del av den profesjonelle utviklingen, og ikke en valgfri oppgave.

Gå foran med et godt eksempel: Ledelsen bør åpent vise eksempler på sikkerhetsatferd. Hvis direktøren alltid bruker en 2FA-token og skryter av at «jeg elsker hvor sikkert og enkelt dette er», følger andre etter. Hvis ledelsen faller for svindel eller bruker svake praksiser, kommer andre ubevisst til å tro at det er greit. Så integrer det på toppnivå – hvis for eksempel en medarbeider sender sensitive data via personlig e-post, bør en leder forsiktig rette på det: «Vennligst bruk den offisielle kontoen vår eller krypter filen – det er slik vi gjør ting her.» Over tid endres gruppens normer.

Utnytt automatisering: En måte å oppnå sikkerhet på uten daglig menneskelig innsats er å automatisere. Du kan for eksempel stille inn alle datamaskiner til å låses automatisk etter fem minutters inaktivitet – da tilpasser de ansatte seg dette mønsteret (og kanskje synes fem minutter er for kort, så de låser proaktivt når de går ut, i stedet for å bli låst ute midt i en setning). Bruk automatiske oppdateringer og automatiske skanninger (planlegg fullstendige antivirusskanninger i lunsjpausen ukentlig). Dette reduserer avhengigheten av hukommelse

eller motivasjon – systemet støtter rutinen. På samme måte kan bruk av en SSO-løsning (Single Sign-On), hvis den er tilgjengelig, integrere sikkerhet (én sterk pålogging låser opp flere apper, slik at brukerne alltid logger på med denne ene robuste metoden i stedet for å sjonglere med svakere metoder).

Belønning og forsterkning: Positiv forsterkning bidrar til vaner. Vurder små belønninger eller anerkjennelse for god sikkerhetsatferd. Eksempel: «Månedens sikkerhetsstjerne» for noen som rapporterte en phishing-e-post eller kom med en idé for å forbedre sikkerheten. Selv bare offentlig ros, «Takk til Alice for at hun la merke til den uvanlige e-posten – flott oppmerksomhet på detaljer!», oppmuntrer alle til å være oppmerksomme. Det viser at sikkerhetsbevissthet verdsettes, og ikke bare forventes.

Ved å integrere denne praksisen i de daglige arbeidsflytene, opphører digital sikkerhet å være et sporadisk prosjekt og blir en del av organisasjonskulturen. Nye medarbeidere vil tilegne seg den fra dag én fordi «det er slik vi jobber her». Det avmystifiserer sikkerhet – det er ikke en spesiell teknisk ting, det er en del av alles rutinemessige arbeidsoppgaver, omtrent som å låse kontordøren eller bruke ID-skilt. Over tid bygger disse små daglige vanene en sterk festning nesten usynlig. Du er kanskje ikke engang klar over hvor trygg du har blitt, fordi det føles rutinemessig og enkelt. Det er målet: Sikkerhet ikke som en byrde, men som et integrert aspekt ved å jobbe smartere og tryggere hver dag.

Kapittelsammendrag

Dette kapitlet utforsker hvordan sivilsamfunnsorganisasjoner kan utnytte samarbeid og eksterne ressurser for å forbedre den digitale sikkerheten. Det understreker at ingen organisasjon står alene overfor cybertrusler, og taler for delt kunnskap og nettverk. Kapitlet fremhever gratis eller fellesskapsdrevne verktøy, som Google Workspace for sivilsamfunnsorganisasjoner eller hjelpetelefoner for digital sikkerhet, for å håndtere budsjettbegrensninger. Det oppfordrer til å delta i sikkerhetsfora og -koalisjoner for å dele trusselinformasjon og suksesshistorier. Eksempler omfatter at sivilsamfunnsorganisasjoner samarbeider med teknologiske frivillige for å sikre servere eller får tilgang til gratis ressurser fra nasjonale CERT-er. Kapitlet fremmer også samarbeid med myndigheter, akademia og teknologibransjen for å arbeide for et tryggere digitalt økosystem. Ved å knytte kontakt med

likemenn forsterker sivilsamfunnsorganisasjoner forsvaret sitt, som vist i et tilfelle der delte varsler stoppet en phishing-kampanje. Kapittelets praktiske veiledning, som å abonnere på sikkerhetsnyhetsbrev, sikrer tilgjengelighet for små sivilsamfunnsorganisasjoner. Det er i tråd med læreplanens modell for opplæring av instruktører, og fremmer en fellesskapsdrevet tilnærming til motstandskraft og kollektivt forsvar.

3. UTDANNINGSMODULER

Innledning og kontekst

I dagens digitale tidsalder er sivilsamfunnsorganisasjoner (CSO-er) og ikke-statlige organisasjoner (frivillige organisasjoner) i økende grad avhengige av digitale verktøy for å oppfylle oppdragene sine. Dessverre gjør dette dem til attraktive mål for cybertrusler. Faktisk ble 50 % av sivilsamfunnsorganisasjonene utsatt for et cyberangrep i 2025, og ideelle organisasjoner er nå den nest mest utsatte sektoren for nasjonalstatslige cyberangrep (31 % av alle tilfeller). Til tross for denne risikoen er mange sivilsamfunnsorganisasjoner dårlig forberedt – fire av fem sivilsamfunnsorganisasjoner mangler en cybersikkerhetsplan, og 70 % føler ikke at de har nødvendig kunnskap eller ferdigheter til å reagere på cyberangrep. Denne statistikken understreker et presserende behov for å styrke kapasiteten innen digital sikkerhet i den ideelle sektoren.

Digital sikkerhet er ikke bare et IT-problem – den påvirker en organisasjons evne til å tjene fellesskapet sitt. Et enkelt datainnbrudd eller angrep med løsepengevirus kan forstyrre kritiske tjenester, kompromittere sensitive mottakerdata og skade tilliten i offentligheten. For sivilsamfunnsorganisasjoner som opererer med begrensede ressurser, kan det å komme seg etter slike hendelser avlede verdifulle midler og tid fra organisasjonens kjerneoppdrag. Det er derfor avgjørende å forbedre infrastrukturen for digital sikkerhet i sivilsamfunnet for å sikre at disse organisasjonene kan operere på en sikker og effektiv måte.

Målet med læreplanen

Et av de viktigste målene med prosjektet vårt er å utvikle en omfattende «læreplan for digital sikkerhet for sivilsamfunnet». Målet er å skape et strukturert opplæringsprogram som gir organisasjoner i sivilsamfunnet og grupper i sivilsamfunnet den kunnskapen og de ferdighetene som trengs for å forbedre den digitale sikkerhetsinfrastrukturen. Med infrastruktur mener vi hele spekteret av en organisasjons digitale sikkerhet – fra sikre teknologier og praksiser til retningslinjer og personalkapasitet. Dette pensumet er tenkt som en praktisk verktøykasse for å hjelpe sivilsamfunnsorganisasjoner med å lære hvordan de kan beskytte egne data, systemer og kommunikasjon, og dermed redusere sårbarheten overfor cybertrusler.

Dette målet er i tråd med prosjektets overordnede mål om å øke den digitale sikkerheten i hele Europa. Ved å bygge opp kapasiteten på nivået for sivilsamfunnet tar vi en

grøntrodstilnærming for å styrke cybersikkerheten på kontinentalt plan. Velopplærte sivilsamfunnsorganisasjoner kommer ikke bare til å beskytte sin egen virksomhet, men også bidra til et tryggere digitalt miljø for lokalsamfunnene de betjener. I bunn og grunn kommer pensumet til å være et strategisk skritt mot å styrke cybersikkerheten gjennom sivilsamfunnet, og sikre at selv mindre organisasjoner kan opprettholde solide digitale forsvarspraksiser.

Etter å ha fullført dette pensumet, vil deltakerne kunne:

- *Identifisere store digitale sikkerhetstrusler mot sivilsamfunnsorganisasjoner og forklare grunnleggende beskyttelsestiltak.*
- *Gjennomføre en grunnleggende risikovurdering av organisasjonens digitale ressurser og utarbeide en enkel cybersikkerhetsplan.*
- *Implementere viktige sikkerhetstiltak på enheter, nettverk og kommunikasjon (f.eks. sterke passord, brannmurer, sikkert Wi-Fi).*
- *Anvende personvernprinsipper og overholde relevante personvernforskrifter (f.eks. GDPR).*
- *Bruke sikre sosiale medier og nettverktøy for å beskytte organisasjonens omdømme og informasjon.*
- *Utvikle og håndheve grunnleggende IT-sikkerhetspolicyer (for eksempel policyer for passord, sikkerhetskopiering og akseptabel bruk) og utføre en grunnleggende prosedyre for hendelsesrespons.*

Oversikt over læreplanen

«Pensum for digital sikkerhet for sivilsamfunnet» er et strukturert læringsprogram utformet som en strategisk verktøykasse som sivilsamfunnsorganisasjoner og frivillige organisasjoner kan følge for å styrke den digitale sikkerhetsinfrastrukturen sin. Pensumet leveres som en modulbasert opplæringspakke som prosjektpartnere tilpasser og implementerer i sine respektive land.

Hovedtrekkene ved læreplanen omfatter:

- **Omfattende innhold:**

  Pensumet dekker emner fra grunnleggende til avanserte nivåer, slik at organisasjoner

med begrenset forkunnskaper gradvis kan bygge opp sin digitale sikkerhetskapasitet trinn for trinn.

- **Praktisk fokus:**

  Pensumet legger vekt på praktiske ferdigheter og virkelige scenarier i stedet for teoretiske tilnærminger. Modulene tar for seg praktiske situasjoner, for eksempel hvordan man reagerer på phishing-forsøk, sikrer nettmøter og beskytter organisasjonsdata. Hver modul gir praktisk veiledning, verktøy og sjekklister som sivilsamfunnsorganisasjoner kan bruke direkte i det daglige arbeidet.

- **Tilpasning og lokal relevans:**

  Pensumet er utformet for å kunne tilpasses nasjonale kontekster. Prosjektpartnerne tilpasser eksempler, casestudier og utvalgt innhold til lokale forskrifter, behov og driftsforhold, mens de sentrale prinsippene og læringsmålene forblir de samme i alle partnerlandene.

- **Format og levering:**

  Opplæringsmateriellet omfatter lysbildeserier, kortfattede forklarende tekster og interaktive komponenter som øvelser og quizer. Pensumet leveres gjennom nettbaserte formater og/eller personlige workshopper for å sikre tilgjengelighet for organisasjoner av ulik størrelse og med ulik teknisk kapasitet. En opplæring-av-instruktøren-tilnærming fremmes, slik at prosjektpartnere og lokale eksperter kan tilby opplæringen på sine nasjonale språk.

- **Resultatorientert struktur:**

  Etter å ha fullført læreplanen, er deltakerne i stand til å vurdere organisasjonens digitale risikoer, iverksette viktige sikkerhetstiltak, utarbeide interne retningslinjer for digital sikkerhet og reagere selvsikkert på vanlige cybertrusler. Pensumet omfatter selvvurderingsverktøy og indikatorer som gjør det mulig for organisasjoner å vurdere eget nivå av digital sikkerhetsberedskap.

Hvorfor trenger sivilsamfunnsorganisasjoner digital sikkerhetskapasitet?

- ***Høy risiko, få ressurser***: Sivilsamfunnsorganisasjoner håndterer ofte sensitive data (f.eks. personopplysninger om mottakere og givere), men opererer med begrensede

budsjetter som begrenser cybersikkerhetstiltakene deres. Angripere vet at mange sivilsamfunnsorganisasjoner er «cyberfattige, men målrike» – rike på data og midler, men dårlige på forsvar.

- ***Et økende trusselslandskap***: Med økt digitalisering (fremskyndet av pandemien) og avhengighet av tredjeparts tjenester på nettet, har angrepsflaten for sivilsamfunnsorganisasjoner vokst. Phishing, skadevare, løsepengevirus og DDoS-angrep mot sivilsamfunnet er på vei opp.
- ***Mangel på bevissthet og opplæring***: Mange ansatte og ledere i sivilsamfunnsorganisasjoner har ikke fått formell opplæring i cybersikkerhet. Omtrent 90 % av ideelle organisasjoner gir ikke regelmessig opplæring til ansatte i cyberhygiene. Dette gapet fører til usikre praksiser (som svake passord eller å falle for phishing-svindel) som motstandere utnytter.
- ***Ingen formelle retningslinjer***: Uten veiledning er det få sivilsamfunnsorganisasjoner som utarbeider sikkerhetsretningslinjer eller planer for hendelsesrespons, noe som gjør at de står uten retning under en hendelse. Nesten 80 % av organisasjonene i sivilsamfunnet har ingen retningslinjer/planer for cybersikkerhet på plass. En læreplan kan hjelpe organisasjoner med å utarbeide disse interne retningslinjene og responsstrategiene.
- ***Press fra regelverk***: Personvernlover som EUs personvernforordning (GDPR) – verdens mest omfattende personvernlov – krever at organisasjoner beskytter personopplysninger. Civilsamfunnsorganisasjoner må overholde disse på samme måte som selskaper, ellers risikerer de juridiske og omdømmesmessige konsekvenser. Å bygge opp kunnskap om slike forskrifter er en avgjørende del av digital sikkerhetskapasitet.
- Disse utfordringene belyser hvorfor det er nødvendig med et egnet pensum. Det kommer til å utbedre kunnskapskløften, fremme en sikkerhetskultur og gi sivilsamfunnsorganisasjoner et veikart for å utvikle egne cybersikkerhetsplaner, -policyer og -beskyttelsestiltak.

Målgruppe og interessenter

Pensumets primære målgruppe består av sivilsamfunnsorganisasjoner (CSO-er) og frivillige organisasjoner, herunder følgende profiler:

- ***Sivilsamfunnsorganisasjoners ledelse og administrasjonspersonell:***
  Personer med ansvar for organisasjonsstrategi, risikostyring og ressursfordeling, som trenger en klar forståelse av digitale sikkerhetsrisikoer og institusjonelle ansvarsområder.
- ***IT-ansatte eller tekniske kontaktpersoner:***
  Personell med ansvar for å iverksette tekniske sikkerhetstiltak og støtte sikker digital praksis i organisasjonen.
- ***Program- og driftsansatte:***
  Ansatte som administrerer daglige datastrømmer, mottakerinformasjon, økonomiske opptegnelser og digital kommunikasjon, og som trenger en solid forståelse av sikker digital praksis.
- ***Frivillige og feltpersonell:***
  Personer som bruker organisasjonens enheter eller håndterer sensitiv informasjon i felten og trenger veiledning om sikker digital atferd.
- ***Partnernettverk og samfunnsorganisasjoner:***
  Organisasjoner som samarbeider eller inngår koalisjoner med sivilsamfunnsorganisasjoner, og som sikrer at praksis for digital sikkerhet strekker seg over institusjonelle nettverk.

Interessenter som er involvert i utarbeidelsen og implementeringen av læreplanen omfatter prosjektpartnerorganisasjoner fra deltakende land og eksperter på cybersikkerhet og digital sikkerhet. Innspill fra spesialiserte eksperter og institusjoner sikrer at læreplanen er i tråd med internasjonalt anerkjent beste praksis innen digital sikkerhet og databeskyttelse.

Sentrale moduler og emner i læreplanen

Pensumet er organisert i flere moduler, som hver fokuserer på et kritisk aspekt ved digital sikkerhet. Nedenfor finner du en oversikt over de viktigste emnene vi planlegger å ta med:

1. Grunnleggende om digital sikkerhet: Forstå trussellandskapet og grunnleggende hygiene – Introduserer hvorfor digital sikkerhet er viktig for sivilsamfunnsorganisasjoner. Dekker typer

trusler (skadevare, nettfisking, hacking, DDoS osv.), trusselaktører (kriminelle, fiendtlige myndigheter som retter seg mot sivilsamfunnet) og grunnleggende beste praksis. Vekt på å skape en sikkerhetsbevisst tankegang og grunnleggende vaner (sterke passord, bruk av tofaktorautentisering, regelmessige programvareoppdateringer, unngåelse av mistenkelige e-poster).

2. Risikovurdering og -planlegging: Vurdere organisasjonsrisiko og utarbeide en sikkerhetsplan – Veileder sivilsamfunnsorganisasjoner i å identifisere egne digitale ressurser og sårbarheter. Slik gjennomfører du en enkel risikovurdering (hva har vi som andre kan angripe? Hvordan kan de gjøre det? Hva er konsekvensene?). Denne modulen vil lede organisasjoner til å utarbeide eller forbedre cybersikkerhetsplanen sin (siden 80 % for øyeblikket mangler en) – inkludert retningslinjer for datahåndtering, tilgangskontroll og en prosedyre for hendelsesrespons.

3. Sikring av enheter og infrastruktur: Beskyttelse av datamaskiner, nettverk og nettsteder – Fokuserer på å sikre teknologien en sivilsamfunnsorganisasjon bruker. Emnene omfatter enhetssikkerhet (antivirus, kryptering av enheter, sikker enhetskonfigurasjon), sikker bruk av Wi-Fi og nettverk, bruk av VPN-er når det er hensiktsmessig, og sikring av nettsteder (grunnleggende om sikkerhet for webhotell, sikkerhetskopier, bruk av HTTPS, beskyttelse mot skade eller DDoS). Eksempler på virkelige angrep (f.eks. et tilfelle av skade på et nettsted som gjorde at en sivilorganisasjons nettsted var nede i månedsvis) vil illustrere viktigheten av disse tiltakene.

4. Sikker kommunikasjon og samarbeid: Sikker e-post, meldinger og hjemmekontor – Lærer ut hvordan man kommuniserer sikkert både internt og med eksterne interessenter. Dekker e-postsikkerhet (gjenkjenne phishing, bruke kryptert e-post eller sikre e-postleverandører), meldingsapper (velge sikre apper som Signal, aktivere ende-til-ende-kryptering) og sikker fildeling. Behandler også utfordringer knyttet til hjemmekontor: Bruk av sikre tilkoblinger, beskyttelse av videokonferanser og administrasjon av kontoer/passord når du jobber hjemmefra eller er på farten.

5. Personvern og overholdelse av personvernregler: Beskyttelse av data og forståelse av juridiske forpliktelser – Legger vekt på å beskytte sensitive data som sivilsamfunnsorganisasjoner innhenter (mottakerdata, giverinformasjon osv.). Introduserer prinsipper for databeskyttelse: dataminimering, kryptering av data i hvile og under overføring, sikker lagring/sikkerhetskopiering og riktig avhending av data. Vi kommer til å fremheve relevante lover som GDPR – et ledende databeskyttelsesrammeverk i Europa – og hva samsvar innebærer for sivilsamfunnsorganisasjoner (f.eks. innhenting av samtykke, sikring av personopplysninger, rapportering av brudd). Denne modulen sikrer at organisasjoner forstår både etiske og juridiske ansvarsområder ved håndtering av data.

6. Sikkerhet på sosiale medier og på nettet: Beskyttelse av organisasjonens omdømme og kontoer – Mange CSO-er er avhengige av sosiale medier for å nå ut. Dette emnet omhandler sikring av kontoer på sosiale medier (sterke passord, tofaktorautentisering, rollebasert tilgang for flere ledere), beskyttelse mot kontokapring og håndtering av nettbasert trakassering eller feilinformasjonskampanjer. Inkluderer også veiledning om innholdsadministrasjon på nettsteder, sikkerhet og trygg atferd på nettet som beskytter sivilorganisasjonens omdømme.

7. Utvikling av en sikkerhetskultur: Opplæring av ansatte, retningslinjer og hendelsesrespons – Fokuserer på menneskelige faktorer og organisatoriske tiltak. Hvordan dyrke en kultur der alle ansatte forstår sin rolle innen cybersikkerhet. Veiledning i å skrive enkle IT-sikkerhetspolicyer (policy for akseptabel bruk, regler for å ta med egne enheter osv.), gjennomføre regelmessige opplæringer for å øke medarbeidernes bevissthet (siden opplæring i å være en «oCSO» er avgjørende for å unngå at 90 % av medarbeiderne blir det svake leddet), og utarbeide en plan for håndtering av hendelser (tiltak som skal iverksettes ved et sikkerhetsbrudd, roller og ansvarsområder, kommunikasjonsstrategi under en cyberkrise). Vi kommer også til å dekke det grunnleggende om å rapportere hendelser til myndighetene og lære av hendelser.

Implementeringsstrategi for læreplanen

Utviklingen og innføringen av dette pensumet ble utført som en samarbeidsbasert og trinnvis prosess.

Gjennomgang og lokalisering av læreplanen:

Etter utarbeidelsen av det første utkastet gjennomgikk prosjektpartnerne pensummaterialet for å sikre at det var relevant for lokale forhold. I denne fasen foreslo partnerne tilpasninger, for eksempel oversettelse av nøkkelterminologi, innlemming av landsspesifikke casestudier og tilpasning av anbefalinger til nasjonal lovgivning og vanlige praksiser. Som et resultat ble læreplanen strukturert med et kjernerammeverk supplert med valgfrie lokaliserte deler for hvert deltakende land.

Pilotopplæring:

Læreplanen ble pilotert med en liten gruppe deltakere fra sivilsamfunnsorganisasjoner i utvalgte partnerland. Pilotimplementeringen ble levert enten som korte modulsegmenter (ca. 15–20 minutter per modul) eller som en heldagsworkshop. Tilbakemeldingene som ble innhentet i denne fasen fokuserte på innholdets klarhet, lengde og praktiske nytte, og læreplanen ble finjustert deretter.

Opplæring av instruktører:

For å sikre skalerbarhet og bærekraft ble det organisert opplæringsøkter for instruktører for prosjektpartnere og utpekte representanter for sivilsamfunnsorganisasjoner i hvert land. Disse øktene dekket ikke bare innholdet i læreplanen, men også veiledede tilretteleggingsteknikker, interaktive øvelser og diskusjonsemner, slik at instruktørene trygt kunne formidle materialet til et bredere publikum.

Lansering for organisasjoner i sivilsamfunnet (kapasitetsoppbygging):

Etter opplæringsfasen for instruktører gjennomførte partnerorganisasjonene opplæring på nasjonalt nivå for lokale civilsamfunnsorganisasjoner og -aktører. Disse opplæringene ble gjennomført via nettmøter, personlige seminarer eller integrert i eksisterende kapasitetsbyggende aktiviteter. Avhengig av lokale behov ble opplæringene strukturert som individuelle moduler på 15–20 minutter eller kombinert til lengre workshopper som dekket flere moduler.

Ressurser og OCSOing-støtte:

Alt pensummateriale og den tilhørende håndboken ble samlet og delt i tilgjengelige formater, primært som nedlastbare PDF-ressurser. I tillegg ble det opprettet en nettbasert

kommunikasjonskanal for å gi deltakere og instruktører mulighet til å stille spørsmål, utveksle erfaringer og dele oppdateringer knyttet til nye trusler eller god sikkerhetspraksis. Dette miljøet for læring mellom likemenn støttet fortsatt engasjement utover de formelle opplæringsøktene.

Overvåking og evaluering:

Gjennom hele implementeringsprosessen ble det gjennomført overvåkings- og evalueringsaktiviteter for å vurdere virkningen av læreplanen. Indikatorene omfatter antall opplærte sivilsamfunnsorganisasjoner, endringer observert mellom vurderinger før og etter opplæringen, og kvalitativ tilbakemelding om organisasjonsmessige forbedringer (for eksempel vedtakelse av cybersikkerhetspolicyer eller nye databeskyttelsesprosedyrer). Disse funnene ble integrert i prosjektets overordnede overvåkingsramme for å sikre at læreplanen effektivt bidro til å styrke praksisen for digital sikkerhet blant deltakende organisasjoner.

Ved å følge denne tilnærmingen var prosessen med å utvikle og implementere læreplanen inkluderende og iterativ, noe som resulterte i et sluttprodukt som var godt tilpasset behovene til sivilsamfunnsorganisasjoner i ulike nasjonale kontekster.

3.1 MODUL 1: GRUNNLEGGENDE DIGITAL SIKKERHET – FORSTÅ TRUSSELSLANDSKAPET OG GRUNNLEGGENDE HYGIENE

På slutten av denne modulen vil deltakeren kunne:

- *Forklare hvorfor digital sikkerhet er avgjørende for sivilsamfunnsorganisasjoner og identifisere grunnleggende cyberhygienepraksis.*
- *Gjenkjenne vanlige cybertrusler (skadevare, phishing, DDoS osv.) rettet mot sivilsamfunnet.*
- *Anvende grunnleggende sikkerhetsvaner (sterke passord, tofaktorautentisering, programvareoppdateringer, årvåkenhet overfor mistenkelige e-poster).*

Læringsmål:

- Øke bevisstheten om hvorfor digital sikkerhet er avgjørende for organisasjoner i sivilsamfunnet, og om de spesifikke cybertruslene som er rettet mot sivilsamfunnet.
- Identifisere vanlige typer cyberangrep (f.eks. skadevare, nettfisking, hacking, DDoS) og trusselaktører (kriminelle grupper, fiendtlige myndigheter) som sivilsamfunnsorganisasjoner kan stå overfor.
- Innføre grunnleggende beste praksis og vaner for cybersikkerhet (f.eks. opprette sterke passord, aktivere tofaktorautentisering, holde programvare oppdatert og gjenkjenne mistenkelig kommunikasjon).

Hovedemner:

- Betydningen av digital sikkerhet for sivilsamfunnsorganisasjoner – hvordan cyberhendelser kan forstyrre driften og kompromittere sensitive data.
- Oversikt over trussellandskapet: Vanlige angrepstyper som skadevare, nettfisking, hacking, DDoS osv., og den økende forekomsten av dem mot sivilsamfunnet.
- Trusselaktører som retter seg mot sivilsamfunnsorganisasjoner: Fra nettkriminelle som søker økonomisk gevinst, til fiendtlige statsstøttede grupper som tar sikte på å overvåke eller forstyrre sivilsamfunnsorganisasjoners aktiviteter.
- Grunnleggende cyberhygienepraksis: Bruke sterke passord og en passordadministrator, aktivere tofaktorautentisering, holde programvare/antivirus oppdatert og være forsiktig med mistenkelige e-poster eller lenker.

- Skaping av en sikkerhetsbevisst holdning blant de ansatte – oppmuntre til årvåkenhet og en kultur der alle tar ansvar for digital sikkerhet.

Eksempler på aktiviteter eller øvelser:

- **Idédugnad om trusler:** Deltakerne lister opp potensielle cybertrusler mot organisasjonen sin og diskuterer hvordan hver trussel kan påvirke arbeidet deres.
- **Passordutfordring:** Deltakerne evaluerer styrken til eksempelpassord og lærer hvordan de oppretter og administrerer sterke passord (f.eks. passfraser, bruk av passordbehandler).
- **Phishing-quiz:** Presenter eksempler på e-poster (noen phishing, noen legitime) og la deltakerne identifisere faresignaler som indikerer et phishing-forsøk.
- **Diskusjon om casestudie:** Beskriv en nylig lokal cyberhendelse som har rammet sivilsamfunnsorganisasjoner – Analyser hva som skjedde i denne hendelsen og diskuter hvilke grunnleggende sikkerhetstiltak som kunne ha forhindret den.

Modul 1 – Eksempel på casestudie: Phishing-angrep mot en lokalsamfunnsbasert sivilsamfunnsorganisasjon

- **Kontekst:** En liten samfunnsbasert sivilsamfunnsorganisasjon som leverer mat og hjelp til sårbare befolkningsgrupper, er avhengig av e-post og nettbaserte donasjonsplattformer. De ansatte har fått minimal opplæring i cybersikkerhet og er kun avhengige av grunnleggende e-postsikkerhet.
- **Problem:** En morgen mottok sivilsamfunnsorganisasjonens økonomiansvarlige en e-post som virket presserende fra noen som utga seg for å være en stor giver. E-posten inneholdt en mistenkelig lenke for å oppdatere betalingsopplysninger. Medarbeideren klikket på lenken og oppga påloggingsopplysningene til civilsamfunnsorganisasjonens bankkonto, uvitende om at det var et phishing-nettsted. I løpet av få timer ble det foretatt uautoriserte uttak fra sivilorganisasjonens konto på til sammen tusenvis av dollar. Sivilorganisasjonen måtte midlertidig stanse driften mens de innhentet midlene og sikret kontoene.
- **Utfall:** Etter hendelsen gjennomgikk sivilsamfunnsorganisasjonen denne sikkerhetssvikten ved hjelp av en teknisk kyndig frivillig. De iverksatte grunnleggende

cyberhygienetiltak umiddelbart: De innførte sterke, unike passord og aktiverte tofaktorautentisering på alle kontoer. De startet også med regelmessig opplæring av personalet i å gjenkjenne phishing-e-poster (se etter skrivefeil, sjekke avsenderadresser osv.). I månedene som fulgte lyktes sivilsamfunnsorganisasjonen med å unngå lignende svindelforsøk og gjenopprette tilliten hos giverne ved å være åpen om forbedringene.

Diskusjonsspørsmål:

- *Hvilken grunnleggende cybersikkerhetspraksis kunne ha forhindret phishing-angrepet i dette tilfellet?*
- *Hvorfor falt medarbeideren for phishing-e-posten, og hvilke tiltak kan hjelpe medarbeiderne med å gjenkjenne slike svindelforsøk i fremtiden?*
- *Hvordan kom sivilsamfunnsorganisasjonen seg etter hendelsen, og hvilke tiltak iverksatte de for å styrke sikkerheten i ettertid?*

Vurdering av modul 1

- Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Modul 1 – Vurdering: Korte spørsmål

1. Hvorfor er digital sikkerhet spesielt viktig for organisasjoner i sivilsamfunnet? (Forklar kort hvordan cyberhendelser kan påvirke organisasjonens virksomhet eller mottakerne.)
2. Nevn to vanlige cybertrusler som ofte retter seg mot sivilsamfunnsorganisasjoner. (Eksempel: phishing, skadevare, DDoS osv.)
3. Hva er phishing, og hvordan prøver det vanligvis å lure brukere? (Forklar den grunnleggende metoden med én eller to setninger.)
4. Nevn to grunnleggende cyberhygienepraksiser som bidrar til å forhindre at kontoer kompromitteres. (Eksempel: sterke passord, tofaktorautentisering, regelmessige oppdateringer.)
5. Nevn ett tydelig varseltegn på at en e-post kan være et phishing-forsøk. (Eksempel: presserende språk, mistenkelig avsenderadresse, uventede lenker eller vedlegg.)

Praktisk oppgave: Identifisering av phishing-risiko

Deltakerne får en kort eksempel-e-post (eller et scenario) knyttet til arbeidet til en sivilsamfunnsorganisasjon (f.eks. en oppdatering om en donasjon, en melding fra en finansierer eller en intern forespørsel).

Deltakerne bes om å:

- Avgjøre om meldingen er legitim eller mistenkelig.
- Identifisere minst to faresignaler (røde flagg) i meldingen.
- Skrive ned én konkret handling de bør utføre i stedet for å klikke på lenken eller svare direkte (f.eks. bekrefte via en annen kanal, rapportere til en veileder).

Vurderingskriterier:

- Identifiserer e-posten riktig som mistenkelig eller risikabel.
- Påpeker riktig minst to røde flagg.
- Foreslår en passende og trygg reaksjon.

3.2 MODUL 2: RISIKOVURDERING OG -PLANLEGGING – VURDERING AV ORGANISASJONSRISIKO OG UTARBEIDELSE AV EN SIKKERHETSPLAN

På slutten av denne modulen kan deltakeren:

- *Identifisere organisasjonens kritiske digitale ressurser og potensielle sårbarheter.*
- *Gjennomføre en grunnleggende risikovurdering ved å anslå sannsynligheten for og virkningen av trusler mot disse ressursene.*
- *Utarbeide en enkel cybersikkerhetsplan eller -policy som dekker datahåndtering, tilgangskontroll og en oversikt over hendelsesrespons.*

Læringsmål:

- Forstå hvordan man identifiserer en organisasjons kritiske digitale ressurser (data, systemer, kontoer) og potensielle sårbarheter.
- Gjennomføre en grunnleggende risikovurdering for å evaluere trusler mot disse ressursene og den potensielle innvirkningen på organisasjonen.
- Utvikle eller forbedre en cybersikkerhetsplan/-policy for sivilsamfunnsorganisasjonen, som dekker sentrale områder som prosedyrer for datahåndtering, tilgangskontroller og beredskap for hendelsesrespons.

Hovedemner:

- Identifisere digitale ressurser og data: Kartlegge hvilken informasjon og hvilke systemer sivilsamfunnsorganisasjonen bruker (f.eks. giverdatabaser, e-postkontoer, nettsteder) og hvorfor de kan bli utsatt for angrep.
- Sårbarheter og trusler: Forstå hvordan man oppdager svakheter (foreldet programvare, mangel på sikkerhetskopier osv.) og forestille seg trusselscenarier (Hva kan angripere angripe? Hvordan kan de gjøre det? Hva er konsekvensene?).
- Risikovurderingsprosess: Vurdere sannsynligheten for og virkningen av ulike trusselscenarier, og prioritere risikoene som skal håndteres først.
- Opprette en cybersikkerhetsplan: Utarbeide en organisatorisk sikkerhetspolicy som dekker databeskyttelsespraksis, kontroll av brukertilgang og en prosedyre for

hendelsesrespons (spesielt viktig siden ca. 80 % av sivilsamfunnsorganisasjonene for øyeblikket mangler en formell sikkerhetsplan).

- Holde planen oppdatert: Tildele ansvar for periodisk gjennomgang og oppdatering av sikkerhetsplanen etter hvert som organisasjonen vokser eller trussellandskapet endres.

Eksempler på aktiviteter eller øvelser:

- **Ressursoversikt:** Deltakerne lister opp viktige digitale ressurser (f.eks. databaser, e-postkontoer, enheter, skytjenester) som sivilorganisasjonen deres er avhengig av, og identifiserer hvilken sensitiv informasjon som er knyttet til hver av dem.
- **Risikokartlegging:** For hver oppført ressurs identifiserer gruppen mulige trusler eller feilscenarier og vurderer sannsynligheten for og virkningen av dem (ved å lage en enkel risikomatrise for å visualisere risikoer med høy prioritet).
- **Planutvikling:** Deltakerne jobber i team og utarbeider et utkast til en grunnleggende cybersikkerhetsplan for en eksempelorganisasjon. Dette bør omfatte avsnitt om retningslinjer for datahåndtering, hvem som har tilgang til dem, og tiltak som skal iverksettes dersom det oppstår en sikkerhetshendelse. Teamene deler deretter planene sine for å få tilbakemelding.
- **Lokalt risikoscenario:** (Eksempler på casescenarier er inkludert i de landsspesifikke lokaliseringsdelene.) Deltakerne diskuterer dette scenariet og brainstormer om hvordan de kan redusere risikoen ved hjelp av elementer fra en sikkerhetsplan (retningslinjer, forebyggende tiltak, responssteg).

Modul 2 – Casestudie: Ignorert sårbarhet fører til tap av data

Kontekst: En mellomstor sivilsamfunnsorganisasjon administrerer en intern server som lagrer giver- og mottakerdata. De vet at serveren er viktig, men har ingen formell dokumentasjon på sikkerhetskopier eller risikoer. De ansatte antok at dataene var trygge fordi «det aldri har skjedd noe dårlig tidligere».

Problem: Et plutselig strømstøt forårsaket av en storm i nærheten skadet sivilorganisasjonens serverhardware og ødela dataene. Fordi serveren ikke hadde blitt sikkerhetskopiert på måneder, gikk alle giveroppføringer, prosjektfiler og økonomiske data tapt. Sivilorganisasjonen

ble tvunget til å stanse programmene sine i flere uker. Givere måtte sende informasjon på nytt, og mange oppføringer kunne ikke gjenopprettes, noe som førte til forvirring og tap av tillit.

Utfall: Etter å ha innsett alvorlighetsgraden av denne feilen, gjennomførte sivilsamfunnsorganisasjonen en grundig risikovurdering med hjelp utenfra. De identifiserte viktige ressurser (databaser, nettsted, e-postkontoer) og trusler (strømbrudd, maskinvarefeil, cyberangrep). De prioriterte å investere i et eksternt sikkerhetskopieringssystem og opprette en regelmessig sikkerhetskopieringsplan. Sivilsamfunnsorganisasjonen utarbeidet en grunnleggende cybersikkerhetsplan, inkludert prosedyrer for sikkerhetskopiering og gjenoppretting av data. Senere, da det oppstod mindre systemproblemer, klarte de å gjenopprette data fra sikkerhetskopier uten avbrudd.

Diskusjonsspørsmål:

- *Hva var advarselstegnene på at organisasjonen var sårbar før katastrofen?*
- *Hvilke elementer bør organisasjonen for sivilsamfunn inkludere i den nye cybersikkerhetsplanen for å forhindre et lignende tap?*
- *Hvordan bidro gjennomføringen av en risikovurdering til at organisasjonen for sivilsamfunn kunne forbedre sikkerheten og driften sin?*

Vurdering av modul 2

Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Modul 2 – Vurdering: Korte spørsmål

- Hva anses som en digital ressurs i en CSO-kontekst? (Nevn to eksempler.)
- Hvorfor er det risikabelt for en organisasjon å stole på antakelsen om at «det ikke har skjedd noe dårlig tidligere»?
- Hvilke to hovedfaktorer evalueres i en grunnleggende risikovurdering? (Forklar kort.)
- Nevn to vanlige sårbarheter som kan øke cybersikkerhetsrisikoen i sivilsamfunnsorganisasjoner.
- Hvorfor er det viktig å regelmessig gjennomgå og oppdatere en cybersikkerhetsplan?

Praktisk oppgave: Øvelse i grunnleggende risikovurdering

Deltakerne bes om å fullføre følgende trinn for en hypotetisk eller virkelig sivilsamfunnsorganisasjon:

- Oppgi én kritisk digital ressurs (f.eks. giverdatabase, e-postsystem, nettsted).
- Identifiser én mulig trussel mot denne ressursen (f.eks. strømbrudd, phishing-angrep, maskinvarefeil).
- Beskriv kort ett forebyggende tiltak som kan redusere risikoen (f.eks. sikkerhetskopier, tilgangskontroller, tofaktorautentisering).

Vurderingskriterier:

- Ressursen er tydelig identifisert,
- Trusselen er realistisk og relevant,
- Det foreslåtte forebyggende tiltaket er hensiktsmessig.

3.3 MODUL 3: SIKRE ENHETER OG INFRASTRUKTUR – BESKYTTE DATAMASKINER, NETTVERK OG NETTSTEDER

På slutten av denne modulen kan deltakeren:

- *Implementere beste praksis for å sikre datamaskiner og mobile enheter (installere oppdateringer, anti-skadevare og kryptering).*
- *Konfigurere og beskytte organisasjonsnettverk (sikre Wi-Fi, bruke VPN-er for ekstern tilgang).*
- *Forbedre nettsteds- og serversikkerheten (aktivere HTTPS, utføre regelmessige sikkerhetskopier og forsvare seg mot vanlige angrep som defacement eller DDoS).*

Læringsmål:

- Implementere beste praksis for å sikre datamaskiner og mobile enheter (f.eks. installere programvare mot skadevare, aktivere enhetskryptering og konfigurere sikkerhetsinnstillinger på riktig måte).
- Beskytt organisasjonens nettverk og internettilgang gjennom sikre Wi-Fi-praksiser og bruk av sikre tilkoblinger (for eksempel VPN-er for ekstern tilgang).
- Styrke sikkerheten til organisasjonens nettsted og nettinfrastruktur ved å bruke moderne beskyttelsestiltak (HTTPS, sikkerhetskopier, DDoS-beskyttelse osv.) og forstå hvordan man reagerer på vanlige angrep.

Hovedemner:

- Grunnleggende om enhetssikkerhet: Installere og oppdatere antivirus-/anti-malware-programvare på alle datamaskiner, aktivere brannmurer og bruke diskkryptering på bærbare datamaskiner og smarttelefoner for å forhindre datatyveri.
- Sikker enhetskonfigurasjon: Håndheve sterke passord/PIN-koder for enhetspålogging, fjerne eller deaktivere unødvendige applikasjoner og tjenester, og regelmessig installere sikkerhetsoppdateringer eller -oppgraderinger.
- Grunnleggende om nettverkssikkerhet: Sikker bruk av Wi-Fi (bruk av pålitelige nettverk, sikring av Wi-Fi på kontoret med sterke passord og kryptering), og når man skal bruke VPN-er for krypterte tilkoblinger (spesielt på offentlige nettverk).

- Nettsteds- og serversikkerhet: Opprettholde oppdatert nettstedsprogramvare (CMS, programtillegg), bruke HTTPS til å kryptere nettrafikk, utføre regelmessige sikkerhetskopier av nettstedsdata og iverksette beskyttelse mot vanlige angrep som defacement eller DDoS.
- Eksempler på infrastrukturangrep fra den virkelige verden: For eksempel et tilfelle av skjemmende inngrep på et nettsted som gjorde en sivilorganisasjons nettsted utilgjengelig i månedsvis, noe som understreker viktigheten av proaktive forsvar.

Eksempler på aktiviteter eller øvelser:

- **Sikkerhetsrevisjon av enheter:** Ved hjelp av en sjekkliste inspiserer deltakerne en eksempel-enhet (eller sin egen, hvis det er hensiktsmessig) for å finne grunnleggende sikkerhetsbeskyttelse – de sjekker om antivirus er installert og oppdatert, statusen til brannmuren, om kryptering er aktivert og om det er utført sikkerhetsoppdateringer nylig.
- **Demonstrasjon av Wi-Fi-sikkerhet:** Instruktøren demonstrerer risikoene ved å bruke usikret offentlig Wi-Fi (f.eks. hvor enkelt det er å snoke på trafikken). Diskuter deretter tiltak for å holde seg trygg: Konfigurere et sikkert Wi-Fi-nettverk hjemme/på kontoret og bruke VPN eller sikre apper når man er på offentlige nettverk.
- **Gjennomgang av nettstedssikkerhet:** Presenter et fiktivt scenario for et sivilsamfunnsorganisasjons nettsted med flere sikkerhetsfeil (utdatert programvare, ingen HTTPS, svakt administratorpassord). Små grupper identifiserer problemene og anbefaler løsninger for å forbedre nettstedets sikkerhet.
- **Lokal casestudie:** Beskriv en lokal sak om skade på en organisasjons nettsted eller et cyberangrep – Diskuter hva som skjedde i denne hendelsen og hvilke forebyggende tiltak (fra modulens nøkkelemner) som kan bidra til å unngå en slik hendelse i fremtiden.

  Modul 3 – casestudie: Skade på nettsted og tjenesteavbrudd

  Kontekst: En sivilorganisasjon driver et offentlig nettsted for programoppdateringer og pengeinnsamling. Nettstedet er bygget på et innholdsstyringssystem (CMS) med åpen kildekode. Det tekniske vedlikeholdet ble håndtert av én enkelt frivillig, som av og til oppdaterte nettstedet.

Problem: Hackere utnyttet en utdatert programtillegg på organisasjonens nettsted, ødela startsiden og erstattet den med et politisk budskap. Sivilorganisasjonen la ikke merke til endringen umiddelbart fordi de ansatte ikke sjekket nettstedet regelmessig. Ødeleggelsen varte i flere dager, noe som skapte forvirring blant støttespillerne og midlertidig avskrekket givere. Besøkende så upassende innhold, og organisasjonens troverdighet ble skadet. I tillegg fikk hackerne tilgang til nettstedets filer, noe som skapte bekymring for sikkerheten til giverdata (selv om ingen brudd ble bekreftet).

Utfall: Etter å ha oppdaget problemet, tok sivilsamfunnsorganisasjonen nettstedet offline for rensing og fjernet det skadelige innholdet. De oppdaterte innholdsstyringssystemet og alle programtilleggene til de nyeste versjonene. Fremover iverksatte sivilsamfunnsorganisasjonen regelmessige sikkerhetskopier av nettstedet og planla ukentlige kontroller av nettstedet. De byttet også til en administrert vertstjenesteleverandør med automatiske oppdateringer og HTTPS-kryptering. I månedene som fulgte forble nettstedet sikkert, og sivilsamfunnsorganisasjonen gjenvant tilliten ved å kommunisere åpent om hendelsen og tiltakene som ble iverksatt for å forhindre den.

Diskusjonsspørsmål:

- *Hvordan kunne oppdatering av programvare og regelmessige sikkerhetskopier ha endret utfallet av dette angrepet?*
- *Hvilke umiddelbare tiltak burde sivilsamfunnsorganisasjonen ha iverksatt da den oppdaget at nettstedet var skadet?*
- *Hvilke langsiktige tiltak iverksatte sivilsamfunnsorganisasjonen for å sikre nettinfrastrukturen sin?*

Vurdering av modul 3

Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Modul 3 – Vurdering

Korte spørsmål

1. Hvorfor er enhetskryptering viktig for bærbare datamaskiner og smarttelefoner som brukes av organisasjoner i sivilsamfunnet? *(Svar med én eller to setninger.)*
2. Nevn to grunnleggende sikkerhetstiltak som bør aktiveres på alle organisasjonens enheter.
3. Hva er de største risikoene ved å bruke usikret offentlig Wi-Fi uten ekstra beskyttelse?
4. Hvorfor utgjør utdaterte CMS-plugins en alvorlig sikkerhetsrisiko for nettsteder til sivilsamfunnsorganisasjoner?
5. Hvordan reduserer regelmessige sikkerhetskopier virkningen av nettsideødeleggelse eller cyberangrep?

Praktisk oppgave: Grunnleggende sikkerhetskontroll av enheter eller nettsteder

Deltakerne velger ett av følgende alternativer:

Alternativ A – Enhetssikkerhet

- Oppgi **tre sikkerhetstiltak** som for øyeblikket er iverksatt på én arbeidsenhet (datamaskin eller smarttelefon)
  (f.eks. antivirus, kryptering, skjermlås, oppdateringer)
- Identifiser **ett manglende eller svakt tiltak** og oppgi kort hvordan det kan forbedres.

Alternativ B – Nettstedsikkerhet

- Identifiser **to grunnleggende sikkerhetskontroller** som bør være på plass for en sivilsamfunnsorganisasjons nettsted.
  (f.eks. HTTPS, regelmessige oppdateringer, sikkerhetskopier, sterke administratorpassord)
- Forklar kort **én risiko** dersom disse kontrollene ikke iverksettes.

Vurderingskriterier:

- De identifiserte tiltakene er relevante for modulen.
- Risikoer eller forbedringer er realistiske og tydelig forklart.

Krav til bestått:

Deltakeren må identifisere minst to gyldige sikkerhetstiltak og én tilknyttet risiko eller forbedring på riktig måte.

3.4 MODUL 4: SIKKER KOMMUNIKASJON OG SAMARBEID – SIKKER E-POST, MELDINGSTJENESTER OG HJEMMEKONTOR

På slutten av denne modulen vil deltakeren kunne:

- *Gjenkjenne og unngå vanlige e-postbaserte trusler (for eksempel phishing) og bruke sikre e-postpraksiser (sterke passord, 2FA).*
- *Bruke sikre meldings- og fildelingsverktøy som tilbyr kryptering.*
- *Implementere sikre fremgangsmåter for hjemmekontor (bruke VPN-er på offentlige nettverk, sikre virtuelle møter med passord).*

Læringsmål:

- Gjenkjenne og unngå vanlige e-postbaserte trusler (for eksempel phishing-svindel) og bruke sikre e-postpraksiser i det daglige arbeidet.
- Velge og bruke sikre kommunikasjonsverktøy for meldinger og fildeling (f.eks. ende-til-ende-krypterte apper, sikre plattformer for dokumentsamarbeid) for å beskytte sensitiv informasjon.
- Implementere sikkerhetstiltak for hjemmekontor og virtuelt samarbeid (ved å bruke sikre nettverk, beskytte nettmøter og administrere kontoer/enheter når du arbeider eksternt).

Hovedemner:

- **E-postsikkerhet:** Hvordan oppdage phishing-forsøk (f.eks. mistenkelige avsendere eller lenker, hastende, uvanlige forespørsler) og viktigheten av å bruke sterke passord og 2FA for e-postkontoer. Dersom sensitive data utveksles, bør man vurdere krypterte e-posttjenester eller tillegg.
- **Sikker meldingstjeneste:** Velge pålitelige meldingstjenesteapplikasjoner som tilbyr ende-til-ende-kryptering (for eksempel Signal eller andre sikre meldingstjenester) og aktivere sikkerhetsfunksjoner som forsvinende meldinger. Veiledning om å verifisere kontakter og ikke dele sensitiv informasjon via usikre kanaler.
- **Fildeling og samarbeid:** Bruk av sikker skylagring eller fildelingstjenester som tilbyr kryptering. Praksis som passordbeskyttelse av sensitive dokumenter eller bruk av plattformer utformet for sikkert samarbeid ved arbeid med eksterne partnere.

- **Sikkerhetstiltak for hjemmekontor:** Beste praksis for å jobbe utenfor kontoret, inkludert bruk av VPN-er på upålitelige nettverk, sikring av Wi-Fi-rutere hjemme, beskyttelse av virtuelle møterom (bruk av venterom, møtepassord, begrensning av skjermdeling) og administrasjon av arbeidsenheter som brukes eksternt.
- **Balansere sikkerhet og tilgjengelighet:** Sikre at sikkerhetstiltak (som kryptering og tilgangskontroller) er brukervennlige nok til at personalet konsekvent bruker dem, og tilby opplæring i eventuelle nye kommunikasjonsverktøy som innføres av sikkerhetsgrunner.

Eksempler på aktiviteter eller øvelser:

- **Øvelse i phishing-e-post:** Veilederen deler eksempel-e-poster med gruppen. Deltakerne må avgjøre for hver e-post om det er en legitim e-post eller et phishing-forsøk, og fremheve ledetrådene som lå til grunn for avgjørelsen.
- **Sammenligning av meldingsapper:** Deles inn i små grupper. Hver gruppe gjennomgår en forskjellig meldingsapp (f.eks. WhatsApp, Signal, Telegram) og rapporterer om sikkerhetsfunksjonene (kryptering, tofaktorautentisering osv.) og eventuelle begrensninger. Diskuter hvilke apper som er mest hensiktsmessige for ulike typer kommunikasjon i sivilsamfunnsorganisasjoner.
- **Sikkert oppsett av videosamtaler:** Direkte demonstrasjon av hvordan man oppretter et nettmøte med riktig sikkerhet: aktivere venterommet, kreve en møtepasskode, begrense deltaking i skjermdeling osv. Etter demonstrasjonen øver deltakerne på å konfigurere disse innstillingene eller diskuterer erfaringer med å sikre egne møter.
- **Diskusjon om lokal kontekst:** [Sett inn et sikkert kommunikasjonsverktøy som er populært i landet ditt, eller en relevant krypteringslov] – Diskuter hvordan denne lokale konteksten påvirker sivilsamfunnsorganisasjonens kommunikasjonssikkerhet. Hvis for eksempel en bestemt kryptert app er mye brukt lokalt, hvordan kan sivilsamfunnsorganisasjonen dra nytte av den? Hvis det finnes lokale forskrifter om kryptering eller datalagring, hvordan påvirker disse kommunikasjonsvalgene?

Modul 4 – Casestudie: E-postbrudd under hjemmekontor

Kontekst: Under en humanitær krise jobber en sivil samfunnsorganisasjons feltmedarbeider eksternt fra en kafé og bruker offentlig Wi-Fi til å sende situasjonsrapporter til hovedkvarteret. Organisasjonen bruker e-post til daglig kommunikasjon, men håndhever ikke krypterte tilkoblinger for eksterne brukere.

Problem: En cyberkriminell på det samme offentlige Wi-Fi-nettverket fanget opp den ansattes ukrypterte e-posttrafikk. Angriperen skaffet seg påloggingsopplysninger da medarbeideren logget seg på sivilorganisasjonens e-postkonto. Dagen etter utga angriperen seg for å være medarbeideren og sendte falske e-poster til givere der han ba om nødfond til et falskt prosjekt. Én giver overførte penger til angriperens konto før svindelen ble oppdaget. Sivilorganisasjonen tapte midler og måtte forklare bedrageriet for giverne.

Utfall: Som svar implementerte sivilsamfunnsorganisasjonen sikre kommunikasjonspraksiser. Alt personale som jobbet eksternt, ble pålagt å bruke VPN eller HTTPS for e-posttilgang, og tofaktorautentisering ble aktivert på e-postkontoer. Organisasjonen innførte også en kryptert meldingsapp for intern kommunikasjon. De kommuniserte med givere om å verifisere eventuelle fremtidige forespørsler og forbedret e-postopplæringen for personalet (oppdage falske e-poster, ikke bruke offentlig Wi-Fi uten beskyttelse). Det oppstod ingen ytterligere hendelser etter disse tiltakene.

Diskusjonsspørsmål:

- *Hvilke sårbarheter hadde sivilorganisasjonens praksis for hjemmekontor i dette tilfellet?*
- *Hvordan kunne VPN-er og tofaktorautentisering ha hindret angriperen i å få tilgang?*
- *Hvilke tiltak iverksatte sivilsamfunnsorganisasjonen etter innbruddet for å beskytte kommunikasjonen og givernes tillit?*

Vurdering av modul 4

Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Modul 4 – Vurdering

Fem korte spørsmål

1. Hva er to vanlige tegn på at en e-post kan være et phishing-forsøk?
   (Svar kort.)
2. Hvorfor er tofaktorautentisering (2FA) spesielt viktig for e-postkontoer som brukes av sivilsamfunnsorganisasjoner?
3. Nevn én sikker meldingsfunksjon som bidrar til å beskytte sensitiv kommunikasjon.
4. Hvilke risikoer står sivilsamfunnsorganisasjoner overfor når ansatte jobber eksternt og bruker offentlig Wi-Fi uten beskyttelse?
5. Hvordan kan sikring av nettmøter (f.eks. passord, venterom) redusere sikkerhetsrisikoen?

Praktisk oppgave: Kontroll av sikker kommunikasjon

Deltakerne fullfører følgende oppgave individuelt eller to og to:

1. **Velg én kommunikasjonskanal** som brukes av sivilsamfunnsorganisasjonen din *(e-post, meldingsapp, fildelingsplattform eller verktøy for videomøter).*
2. Svar kort:
   - **Ett sikkerhetstiltak er for øyeblikket på plass**
     (f.eks. 2FA aktivert, kryptert meldingstjeneste, møtepassord)
   - **Én forbedring** som kan styrke sikkerheten
     (f.eks. aktivere VPN-bruk, bytte til en kryptert app, begrense tilgangsrettigheter)
3. Forklar med **én eller to setninger** hvordan denne forbedringen vil redusere risikoen.

Vurderingskriterier:

- Den valgte kanalen er relevant for kommunikasjon med sivilsamfunnsorganisasjoner,
- Sikkerhetstiltakene og -forbedringene er realistiske.
- Forklaringen viser forståelse for sikker kommunikasjonspraksis.

3.5 MODUL 5: PERSONVERN OG OVERHOLDELSE AV PERSONVERN – BESKYTTE OPPLYSNINGER OG FORSTÅ JURIDISKE FORPLIKTELSER

På slutten av denne modulen kan deltakeren:

- *Identifisere de sensitive opplysningene som sivilsamfunnsorganisasjonen innhenter, og forklare hvorfor de må beskyttes.*
- *Anvende viktige databeskyttelsespraksiser (dataminimering, kryptering, sikker lagring, regelmessige sikkerhetskopier og sikker avhending).*
- *Forstå og skissere civilsamfunnsorganisasjonens juridiske forpliktelser i henhold til personvernlovgivning (for eksempel GDPR) og hvordan man sikrer overholdelse.*

Læringsmål:

- Gjenkjenne typene sensitive data (f.eks. mottakeres personopplysninger, giveroppføringer) som CSO-er innhenter, og hvorfor det er avgjørende å beskytte slike data.
- Anvende viktige databeskyttelsesprinsipper – inkludert dataminimering, kryptering (for data i hvile og under overføring), sikker lagring/sikkerhetskopiering og riktig avhending av data – for å forbedre personvern og sikkerhet.
- Forstå juridiske forpliktelser og rammeverk for personvern, for eksempel EUs personvernforordning (GDPR) og tilsvarende nasjonale personvernlover, og hvordan man sikrer at sivilsamfunnsorganisasjonen overholder disse forskriftene.

Hovedemner:

- **Identifisere sensitive data:** Hva som regnes som personopplysninger eller sensitive data i en CSO-kontekst (navn, adresser, helse- eller rettssaksinformasjon osv.), og risikoen ved lekkasje av slike data.
- **Personvernprinsipper:** Praktiske tiltak for dataminimering (kun innhenting av det som virkelig er nødvendig), kryptering av data som lagres (f.eks. filer på harddisker) og som overføres (ved hjelp av SSL/HTTPS for dataoverføring), sikre

datalagringsløsninger (fysiske og i skyen), opprettholdelse av regelmessige sikkerhetskopier og riktig sletting av data som ikke lenger er nødvendige.

- **Rettslige rammer:** Oversikt over de viktigste personvernlovene – for eksempel GDPR (personvernforordningen) som en ledende ramme i Europa, og [Sett inn personvernforskriften for landet ditt her]. Viktige forpliktelser omfatter å innhente informert samtykke til datainnsamling, sikre personopplysninger gjennom tekniske og organisatoriske tiltak, og krav om varsling ved databrudd.
- **Etisk datahåndtering:** Utover juridiske regler, vekt på det etiske ansvaret for å beskytte enkeltpersoners personvern. Diskusjon om konsekvensene av datainnbrudd for sivilsamfunnsorganisasjoner, herunder skade på mottakere, tap av tillit, juridiske sanksjoner og skade på omdømmet.
- **Innarbeiding av samsvar i praksis:** Hvordan organisasjoner i sivilsamfunnet kan utarbeide enkle personvernpolicyer og retningslinjer for datahåndtering, og lære opp personalet i disse policyene. Introduksjon til begreper som personvernombud (hvis relevant) eller avtaler om databehandling ved samarbeid med partnere.

Eksempler på aktiviteter eller øvelser:

- **Øvelse i datatilsyn:** Deltakerne regner opp hvilke typer personopplysninger deres sivilsamfunnsorganisasjon innhenter eller håndterer, og kartlegger hvor disse opplysningene lagres (databaser, regneark, e-post, skytjenester). Deretter diskuterer de hvert element: Hvem som har tilgang, hvordan det er beskyttet for øyeblikket, og eventuelle hull de legger merke til.
- **Demonstrasjon av kryptering:** Instruktøren demonstrerer kryptering av en eksempelfil eller -mappe (eller bruk av et krypteringsverktøy for e-post/meldinger). Deltakerne lærer hvordan krypterte data ser ut og øver seg på å kryptere og dekryptere testdata, med vekt på viktigheten av nøkkel-/passordadministrasjon.
- **Gjennomgang av retningslinjer:** Del ut en mal eller et eksempel på enkle retningslinjer for personvern eller en personvernerklæring. I små grupper identifiserer deltakerne hvordan dette dokumentet oppfyller GDPR-kravene og vurderer hvilke endringer som vil være nødvendige for å overholde [Sett inn ditt lands personvernforskrift her]. Hver

gruppe kan presentere ett nøkkelpunkt de ville tatt med i sin egen sivilsamfunnsorganisasjons policy.

- **Diskusjon om overholdelse av lovgivning:** Gå gjennom en sjekkliste over tiltak for overholdelse av GDPR (f.eks. utpeking av en ansvarlig person, innhenting av samtykkeskjemaer, plan for datainnbrudd). Deltakerne diskuterer hvilke punkter på listen de allerede har på plass, og hvilke de trenger å iverksette. Legg vekt på eventuelle ytterligere tiltak som kreves av nasjonal lovgivning (f.eks. registrering hos en databeskyttelsesmyndighet dersom det kreves av [Sett inn ditt lands databeskyttelsesforskrift her]).

Modul 5 – casestudie: Brudd på giverdatabase

Kontekst: En sivilsamfunnsorganisasjon for internasjonal bistand fører en database med giverinformasjon (navn, kontaktopplysninger, donasjonshistorikk) og mottakerdata (sensitive helseopplysninger). Opplysningene lagres på en intern nettverksstasjon som er tilgjengelig for programansatte.

Problem: Under en systemoppgradering eksponerte en administrator ved et uhell giverdatabasemappen på en offentlig fildelingslenke i skyen uten kryptering eller tilgangskontroller. En hacker oppdaget lenken og lastet ned hele giverlisten. Personopplysninger om tusenvis av givere (navn, e-postadresser og donasjonsbeløp) ble lekket på nettet. Sivilorganisasjonen ble tvunget til å varsle giverne om bruddet i henhold til loven. Flere givere trakk tilbake støtten og oppga tap av tillit som årsak. Sivilorganisasjonen ble også gransket for ikke å ha sikret opplysningene på riktig måte.

Utfall: Etter datainnbruddet reviderte sivilsamfunnsorganisasjonen sin praksis for datahåndtering. De krypterte alle sensitive data i hvile og under overføring, og begrenset tilgangen til databasen ved å iverksette sterke tilgangskontroller. De anvendte også dataminimering ved å fjerne unødvendige personopplysninger fra offentlige filer. Sivilsamfunnsorganisasjonen utnevnte en personvernansvarlig til å overvåke overholdelse og utarbeidet en tydelig personvernpolicy. Personalet fikk opplæring i riktig datahåndtering, og fremtidig deling ble utført med sikre lenker og passord. Civilsamfunnsorganisasjonen gjenvant

tilliten fra giverne ved raskt å stramme opp sikkerheten og rapportere forbedringene på en åpen måte.

Diskusjonsspørsmål:

- *Hvilke personvernfeil førte til dette bruddet, og hvordan kunne de ha blitt forhindret?*
- *Hvilke databeskyttelsespraksiser (fra emnene i denne modulen) innførte sivilsamfunnsorganisasjonen etter hendelsen?*
- *Hvilke juridiske forpliktelser hadde sivilsamfunnsorganisasjonen for å håndtere dette bruddet, og hvorfor er samsvar viktig for sivilsamfunnsorganisasjoner?*

Vurdering av modul 5

Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Vurdering av modul 5

Korte spørsmål

1. Hvilke typer personopplysninger eller sensitive opplysninger innhenter sivilsamfunnsorganisasjoner vanligvis, og hvorfor må disse opplysningene beskyttes?
2. Forklar prinsippet om dataminimering og gi ett praktisk eksempel på hvordan en sivilsamfunnsorganisasjon kan anvende det.
3. Hva er forskjellen på å kryptere data i hvile og å kryptere data under overføring?
4. Hva er en sivilsamfunnsorganisasjon pålagt å gjøre i henhold til GDPR (eller tilsvarende nasjonale personvernlover) ved et personopplysningsbrudd?
5. Hvorfor er etisk datahåndtering viktig for sivilsamfunnsorganisasjoner utover overholdelse av lovgivningen? Nevn én potensiell konsekvens av å unnlate å beskytte opplysninger på riktig måte.

Praktisk oppgave: Mini-gjennomgang av personvern

Deltakerne bes om å fullføre følgende oppgave:

- Identifiser **én type personopplysninger eller sensitive opplysninger** som samles inn av sivilorganisasjonen deres (f.eks. mottakerjournaler, kontaktopplysninger for givere, personalopplysninger).
- Beskriv kort:
    - Hvor disse opplysningene lagres (f.eks. datamaskin, skytjeneste, e-post, papirfiler),
    - Hvem som har tilgang til dem,
    - Én forbedring som kan gjøres for å beskytte disse opplysningene bedre (f.eks. kryptering, begrenset tilgang, dataminimering).

Deltakerne bør presentere svarene sine **i tre til fem korte punkter** eller diskutere dem kort i små grupper.

3.6 **MODUL 6: SIKKERHET PÅ SOSIALE MEDIER OG PÅ NETTET – BESKYTTELSE AV ORGANISASJONENS OMDØMME OG KONTOER**

På slutten av denne modulen kommer deltakerne til å kunne:

- *Iverksette sikkerhetstiltak for å beskytte sivilsamfunnsorganisasjonens kontoer på sosiale medier (sterke, unike passord, tofaktorautentisering, begrensede administratorroller).*
- *Reagere effektivt på hendelser på sosiale medier (kontokapring eller etterligning) ved å følge rapporterings- og kommunikasjonsprosedyrer.*
- *Implementere beste praksis for å opprettholde en sikker tilstedeværelse på nettet (regelmessige oppdateringer av nettstedet/CMS, retningslinjer for ansatte for publisering og respons på feilinformasjon).*

Læringsmål:

- Implementere sikkerhetstiltak for å beskytte sivilsamfunnsorganisasjonens kontoer på sosiale medier (sterk autentisering, overvåket tilgang, regelmessige revisjoner av kontoinnstillinger).
- Utvikle strategier for å beskytte organisasjonens tilstedeværelse og omdømme på nettet, herunder hvordan man skal reagere på kontokapring, etterligning eller feilinformasjonsangrep.
- Anvende beste praksis for innholdsadministrasjon på nettsteder og medarbeideradferd på nettet for å sikre en konsekvent og sikker organisasjonsrepresentasjon på internett.

Hovedemner:

- **Sikkerhet for kontoer på sosiale medier:** Sikre at alle organisasjonens kontoer på sosiale medier bruker sterke, unike passord og har tofaktorautentisering aktivert. Sikker administrasjon av flere administratorer (ved hjelp av rollebaserte tilgangskontroller eller funksjoner for teamsamarbeid, i stedet for å dele passord).
- **Kontoovervåking og -gjenoppretting:** Holde øye med kontoaktivitet (slik at eventuell uautorisert tilgang oppdages tidlig) og vite hvordan man gjenoppretter kontoer hvis de blir kompromittert (forstå plattformens støtteprosesser for hackete kontoer).

- **Håndtering av kapring og etterligning:** Tiltak som skal iverksettes dersom en sivilsamfunnsorganisasjons konto kapres, eller dersom falske kontoer etterligner sivilsamfunnsorganisasjonen – herunder rapporteringsmekanismer på sosiale plattformer, kommunikasjon med støttespillere for å avklare feilinformasjon og gjenvinnelse av kontrollen over kontoene.
- **Håndtering av nettbasert trakassering og feilinformasjon:** Taktikker for å reagere på nettroll eller koordinerte trakasseringskampanjer (f.eks. dokumentere krenkelser, bruke blokkerings-/rapporteringsfunksjoner, ha retningslinjer for moderering av kommentarer). Hvordan motvirke feilinformasjon eller ærekrenkelse på nettet med saklige budskap uten å forsterke falske påstander.
- **Sikkerhet for nettsteder og innholdsadministrasjon:** Holde sivilsamfunnsorganisasjonens nettsted sikkert og anerkjent – oppdatere nettstedets innholdsstyringssystem/plugins regelmessig, bruke sikre passord for nettstedsadministratorer, begrense hvem som kan publisere innhold, og ha en prosess for raskt å korrigere eller fjerne feilaktig eller uautorisert innhold.
- **Omdømmehåndtering:** Opplæring av ansatte og frivillige i retningslinjer for å representere organisasjonen på nettet (retningslinjer for personlig bruk av sosiale medier, hva man ikke skal legge ut om arbeidet, hvordan man skal reagere hvis man ser feilinformasjon) for å opprettholde en positiv og sikker nettpresens for sivilsamfunnsorganisasjonen.

Eksempler på aktiviteter eller øvelser:

- **Sikkerhetssjekk av konto:** Deltakerne gjennomfører en rask revisjon av en av sivilsamfunnsorganisasjonens kontoer på sosiale medier. De verifiserer om 2FA er aktivert, om passordene er sterke/nylig oppdatert, om kontaktinformasjonen for gjenoppretting er riktig, og om kun autoriserte personer har tilgang. Deretter oppretter de en gjøremålsliste for eventuelle nødvendige forbedringer.
- **Hendelsesrollespill:** Simuler et scenario der en sivilsamfunnsorganisasjons offisielle konto på sosiale medier har blitt kapret, eller der en falsk konto sprer falsk informasjon om organisasjonen. Teamet må bestemme seg for en umiddelbar handlingsplan: Hvem

skal kommunisere med publikum, hvordan skal plattformen og følgerne varsles, og hvilke tiltak som skal iverksettes for å sikre eller gjenopprette kontoen? Etter rollespillet diskuteres hva som gikk bra og hva som kan forbedres i responsen.

- **Responsplan for trakassering:** I grupper utarbeider deltakerne en enkel protokoll for håndtering av nettbasert trakassering eller hatekampanjer. Dette kan omfatte trinn som: Ikke engasjer deg offentlig i sinne, dokumenter de krenkende innleggene, rapporter dem til plattformen, varsle sivilsamfunnsorganisasjonens ledelse og støtt eventuelle ansatte som er målrettet. Gruppene deler planene sine og diskuterer felles elementer.
- **Diskusjon om lokalt eksempel:** [Beskriv en nylig lokal hendelse relatert til sosiale medier som involverer en sivilsamfunnsorganisasjon] – Analyser hva som skjedde og hvordan solide sikkerhetspraksiser for sosiale medier og en plan for hendelsesrespons kan bidra til å håndtere eller forhindre en slik situasjon.

Modul 6 – Casestudie: Kapring av kontoer på sosiale medier

Kontekst: En miljøorganisasjon bruker sosiale medier (Twitter og Facebook) til å engasjere givere og dele kampanjenyheter. Flere ansatte har tilgang til kontoene med delte passord, og ingen overvåker påloggingsaktiviteten nøye.

Problem: En morgen begynte sivilsamfunnsorganisasjonens Twitter-konto å legge ut opphissende politiske meldinger som ikke var relatert til sivilsamfunnsorganisasjonens oppdrag. Følgerne var forvirret, og noen anklaget sivilsamfunnsorganisasjonen for å innta en politisk holdning. Innleggene var et verk av en hacker som hadde fått tilgang etter at en ansatt hadde gjenbrukt et vanlig passord. Innen personalet innså bruddet, hadde meldingene blitt retweetet av støttespillere, noe som forårsaket skade på omdømmet. Det tok timer å få tilgang på nytt gjennom plattformens støtteprosess, og i løpet av denne tiden spredde negative inntrykk seg på nettet.

Utfall: Sivilsamfunnsorganisasjonen gjennomførte en hendelsesrespons ved umiddelbart å legge ut en avklaring på alle kanaler og be om unnskyldning for bruddet. De tilbakestilte alle passord for sosiale medier og aktiverte tofaktorautentisering på alle kontoer. De konfigurerte også rollebasert tilgang (tildeling av spesifikke administratorkontoer i stedet for deling av passord). De ansatte gjennomgikk og oppdaterte innholdet på nettstedet for å sikre at det ikke

var igjen utdatert informasjon. Sivilorganisasjonen innførte en policy for daglig overvåking av kontoaktivitet. Som et resultat klarte de å gjenopprette normal kommunikasjon og fikk senere til og med støtte for å ha vært åpne. De nye sikkerhetstiltakene forhindret ytterligere forsøk på kapring.

Diskusjonsspørsmål:

- *Hva var de viktigste feilene som gjorde at kontoen kunne kapres?*
- *Hvordan reagerte sivilsamfunnsorganisasjonen for å begrense skadene, både teknologisk og kommunikasjonsmessig?*
- *Hvilke sikkerhetsforbedringer iverksatte sivilsamfunnsorganisasjonen for å beskytte sin tilstedeværelse på sosiale medier fremover?*

Vurdering av modul 6

Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Vurdering av modul 6

Korte spørsmål

1. Hvorfor er det viktig for sivilsamfunnsorganisasjoner å bruke sterke, unike passord og tofaktorautentisering på kontoer på sosiale medier?
2. Hvilke risikoer kan oppstå ved å dele passord til kontoer på sosiale medier mellom flere medarbeidere?
3. Hvilke umiddelbare tiltak bør en sivilsamfunnsorganisasjon iverksette dersom den sosiale mediekontoen kapres eller kompromitteres?
4. Hvordan kan feilinformasjon eller etterligning på nettet påvirke en sivilsamfunnsorganisasjons omdømme og tilliten i offentligheten?
5. Hvorfor er det viktig å ha klare retningslinjer for personalet angående atferd på nettet og representasjon av organisasjonen?

Praktisk oppgave: Gjennomgang av sikkerhet på sosiale medier

Deltakerne bes om å fullføre følgende oppgave:

- Velg én offisiell konto på sosiale medier tilhørende deres sivilsamfunnsorganisasjon (eller en hypotetisk sivilsamfunnsorganisasjon).
- Beskriv kort:
    - Om tofaktorautentisering er aktivert,
    - Hvordan tilgangen for øyeblikket administreres (delte passord vs. rollebasert tilgang).
    - Én konkret handling som kan forbedre sikkerheten eller overvåkingen av denne kontoen.

Deltakerne bør oppsummere svarene sine i tre til fem korte punkter eller diskutere dem kort i små grupper.

3.7 MODUL 7: UTVIKLING AV EN SIKKERHETSKULTUR – OPPLÆRING AV PERSONALET, RETNINGSLINJER OG HENDELSESRESPONS

På slutten av denne modulen vil deltakerne kunne:

- *Fremme en sikkerhetsbevisst kultur i organisasjonen ved å engasjere ledelse og ansatte.*
- *Utvikle grunnleggende IT-sikkerhetspolicyer (f.eks. akseptabel bruk, BYOD, passordregler) og planlegge regelmessig sikkerhetsopplæring for alle ansatte.*
- *Opprette og øve på en enkel hendelsesresponsplan (definere roller, trinn og kommunikasjon) for å håndtere cyberhendelser effektivt.*

Læringsmål:

- Fremme en sikkerhetsbevisst kultur i organisasjonen, der alle ansatte forstår sin personlige rolle i opprettholdelsen av cybersikkerhet.
- Utvikle grunnleggende IT-sikkerhetspolicyer (f.eks. akseptabel bruk av teknologi, regler for å ta med egne enheter) og iverksette regelmessige opplæringsprogrammer for personalet for å forsterke god sikkerhetspraksis.
- Opprette og øve på en hendelsesresponsplan slik at organisasjonen kan reagere effektivt på cybersikkerhetshendelser (med tydelig definerte trinn, roller og kommunikasjonskanaler).

Hovedemner:

- **Oppbygge en cybersikkerhetskultur:** Slik får du ledelsens støtte og personalets engasjement for sikkerhetsinitiativer. Skape et miljø der ansatte føler seg ansvarlige for å beskytte data og systemer, i stedet for å se på sikkerhet som utelukkende IT-personens oppgave.
- **Grunnleggende sikkerhetspolicyer:** Utarbeide enkle og tydelige policyer som setter forventninger til sikker bruk av teknologi. Eksempler omfatter retningslinjer for akseptabel bruk (hva som er tillatt/forbudt på arbeidsenheter og -kontoer), BYOD-retningslinjer (bring-your-own-device) dersom ansatte bruker personlige enheter til arbeid, og regler for oppretting og håndtering av passord.

- **Kontinuerlig bevisstgjøring og opplæring av personalet:** Betydningen av kontinuerlig opplæring (workshoper, nyhetsbrev, phishing-simuleringstester) for å holde sikkerhetskunnskapen oppdatert. Det er viktig å merke seg at regelmessig opplæring er avgjørende, siden uopplært personale kan bli det svakeste leddet i sikkerheten.
- **Planlegging av hendelsesrespons:** Nøkkelkomponenter i en hendelsesresponsplan – hvordan man oppdager og rapporterer en hendelse, umiddelbare tiltak for å begrense problemet (f.eks. frakobling av berørte datamaskiner), roller og ansvarsområder (hvem som leder responsen, hvem som kommuniserer med interessenter) og hvordan man holder driften i gang under forstyrrelser.
- **Rapportering og læring av hendelser:** Retningslinjer for når og hvordan man skal rapportere cyberhendelser til myndigheter eller tilsynsorganer (spesielt hvis personopplysninger er involvert), og gjennomføring av en gjennomgang etter hendelsen for å forbedre fremtidig motstandskraft.

Eksempler på aktiviteter eller øvelser:

- **Workshop om utarbeidelse av retningslinjer:** Deltakerne utarbeider et utkast til én kort sikkerhetsretningslinje som er relevant for deres sivilsamfunnsorganisasjon (for eksempel retningslinjer for akseptabel bruk av kontordatamaskiner eller retningslinjer for mobile enheter). Hver gruppe skriver ned noen sentrale regler og deler dem deretter med alle, og ber om tilbakemelding for å sikre at retningslinjene er tydelige og gjennomførbare.
- **Sikkerhetsbevissthetsøvelse:** Organiser en simulert phishing-øvelse eller et overraskende «USB-slipp» (etterlat en USB-minnepinne som om den ble funnet, for å se om noen kobler den til). Etterpå diskuteres resultatene: Hvordan reagerte de ansatte? Hva var røde flagg? Bruk dette som en læringsmulighet til å forsterke opplæringspunkter i et trygt miljø.
- **Simulering av hendelsesrespons:** Presentér en hypotetisk cybersikkerhetshendelse (f.eks. et løsepengevirusangrep som krypterer organisasjonens data). Få teamet til å gå gjennom responsen sin trinn for trinn: Hvordan identifiserer de problemets omfang, hvem ringer de først, hvordan kommuniserer de med personalet og eventuelt

offentligheten, og hvordan gjenoppretter de systemer eller data? Etter øvelsen kan du gjennomgå hva som gikk bra, og hvilke roller eller trinn som trenger avklaring i planen deres.

- **Lokal rapporteringsinformasjon:** [Sett inn landet ditt sin rapporteringsmekanisme for cyberhendelser eller kontaktinformasjon til relevant myndighet her] – Sørg for at deltakerne er klar over hvordan de skal rapportere en alvorlig cybersikkerhetshendelse i sin lokale kontekst (for eksempel ved å varsle et nasjonalt CERT eller politiet), og drøft eventuelle juridiske krav til rapportering av brudd som gjelder for sivilsamfunnsorganisasjoner i landet deres.

Modul 7 – Casestudie: Usikret USB-enhet fører til utbrudd av skadevare

Kontekst: Et CSO-kontor tillot ansatte å bruke personlige USB-minnepinner på arbeidsdatamaskiner. Det fantes ingen skriftlig policy eller opplæring om bruk av flyttbare medier. En ny frivillig brukte ofte sin egen USB-pinne.

Problem: En dag fant en ansatt en USB-minnepinne på kontorets parkeringsplass (sannsynligvis mistet av noen). Nysgjerrig koblet vedkommende den til kontordatamaskinen og åpnet et dokument på den. Den USB-pinnen var infisert med skadevare. Skadevaren spredde seg raskt gjennom sivilsamfunnsorganisasjonens nettverk og krypterte filer på flere datamaskiner. Organisasjonens data var utilgjengelige, og driften ble forstyrret. Mangelen på en hendelsesresponsplan skapte forvirring: Ingen visste hvem som skulle lede responsen eller hvem de skulle varsle.

Resultat: Etter å ha begrenset utbruddet ved å koble fra berørte maskiner, engasjerte sivilsamfunnsorganisasjonen en IT-spesialist for å gjenopprette data fra nylige sikkerhetskopier. De innså at sikkerhetskopier hjalp til med å gjenopprette de fleste data. Sivilsamfunnsorganisasjonen iverksatte deretter strenge retningslinjer: Det ble utarbeidet formelle retningslinjer for akseptabel bruk (som forbød bruk av ikke-godkjente USB-minnepinner og krevde skanning av alle eksterne medier), og alle ansatte gjennomgikk opplæring i å gjenkjenne mistenkelige enheter og vedlegg. De utviklet også en enkel hendelsesresponsplan, utpekte et responsteam og fastsatte klare trinn som skal følges ved en fremtidig hendelse (herunder hvem som skal ringes først og hvordan man skal kommunisere

med interessenter). Senere, under en mindre phishing-hendelse, klarte sikkerhetsansvarlig å begrense den ved hjelp av den nye planen, og minimerte skadene.

Diskusjonsspørsmål:

- *Hvilke retningslinjer eller praksiser manglet som gjorde at denne hendelsen kunne inntreffe?*
- *Hvordan påvirket det å ha nylige sikkerhetskopier og et responsteam utfallet av hendelsen?*
- *Hvilke nye tiltak og planer iverksatte sikkerhetssjefen etter hendelsen, og hvorfor er de viktige for å forhindre fremtidige hendelser?*

Merknad om vurdering i modul 7

Denne modulen vurderes med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Vurdering av modul 7

Korte spørsmål

1. Hva betyr en «sikkerhetskultur» i en sivilsamfunnsorganisasjons kontekst, og hvorfor er personalets engasjement avgjørende for å bygge den opp?
2. Hvorfor er grunnleggende IT-sikkerhetspolicyer (for eksempel policyer for akseptabel bruk eller BYOD) viktige for sivilsamfunnsorganisasjoner?
3. Hvordan kan regelmessig opplæring av personalet og bevisstgjøring redusere cybersikkerhetsrisikoen i en organisasjon?
4. Hva er hovedelementene i en enkel hendelsesresponsplan for en sivilsamfunnsorganisasjon?
5. Hvorfor er det viktig å gjennomgå og lære av cybersikkerhetshendelser etter at de har inntreff?

Praktisk oppgave: Mini-handlingsplan for sikkerhetskultur

Deltakerne bes om å fullføre følgende oppgave:

- Identifiser én konkret handling som sivilorganisasjonen kan iverksette for å styrke sikkerhetskulturen (f.eks. innføre en enkel policy for akseptabel bruk, organisere en årlig sikkerhetsopplæring eller utpeke en kontaktperson for hendelsesrespons).
- Beskriv kort:

- Hvem som skal være ansvarlig for denne handlingen,
- Hvordan vil den bli formidlet til personalet?
- Hvordan det vil bidra til å forhindre eller redusere cybersikkerhetshendelser.

Deltakerne bør presentere svarene sine i tre til fem korte punkter eller diskutere dem kort i små grupper.

3.8 MODUL 8: AVANSERTE EMNER – NYE TRUSLER OG VERKTØY

På slutten av denne modulen vil deltakeren kunne:

- *Gjenkjenne sofistikerte cybertrusler (som målrettet phishing og spoofing) og bruke verifiseringsmetoder (for eksempel å bekrefte forespørsler via alternative kanaler).*
- *Bruke avanserte sikkerhetsverktøy på riktig måte (f.eks. maskinvaresikkerhetsnøkler for kritiske kontoer, nettverksovervåking for avvik, trusselinformasjonsressurser).*
- *Planlegge sikkerhetsforbedringer i organisasjonen (for eksempel innføring av passordbehandlere for bedrifter eller innbruddsdeteksjonssystemer) basert på organisasjonens kapasitet og behov.*

Læringsmål:

- Bli kjent med nye eller sofistikerte cybertrusler (for eksempel avanserte phishing-teknikker eller spoofing-angrep) og lære verifiseringsmetoder for å motvirke dem.
- Utforske avanserte sikkerhetsverktøy og -praksiser som ytterligere kan forbedre beskyttelsen, inkludert maskinvarebasert sikkerhet (f.eks. sikkerhetsnøkler), nettverksovervåking og trusselinformasjon, tilpasset sivilsamfunnsorganisasjoners behov.
- Vurdere hvordan man kan implementere sikkerhetsforbedringer i hele organisasjonen, for eksempel passordbehandlere for bedrifter eller innbruddsdeteksjonssystemer, og forstå når disse avanserte tiltakene er hensiktsmessige for en sivilsamfunnsorganisasjons kapasitet.

Hovedemner:

- **Sofistikert phishing og spoofing:** Forståelse av avanserte sosiale manipulasjonsangrep (svindel-e-poster fra administrerende direktør, klonede nettsteder osv.) og læringsmetoder for å verifisere kommunikasjon (for eksempel verifisering av mistenkelige forespørsler via en sekundær kanal eller ved hjelp av digitale signaturer).

- **Maskinvaresikkerhetsnøkler:** Introduksjon til fysiske autentiseringstokens (som U2F/FIDO2-nøkler) som et alternativ til SMS eller 2FA-app. Hvordan de fungerer for å forhindre kontoovertakelser (phishing-bestandig 2FA), og hensyn ved distribusjon av dem til personalet.
- **Nettverksovervåking og innbruddsdeteksjon:** Grunnleggende konsepter for hvordan en sivilsamfunnsorganisasjon kan overvåke nettverket sitt for uvanlig aktivitet. Enkel forklaring av verktøy som innbruddsdeteksjonssystemer (IDS) eller innbruddsforebyggingssystemer (IPS), og hvordan de varsler administratorer om potensielle brudd.
- **Sikkerhetsverktøy for hele organisasjonen:** Implementering av avanserte verktøy som passordbehandlere for hele organisasjonen (for å sikre at alle ansatte bruker sterke, unike passord), eller bruk av trusselinformasjonsstrømmer/fellesskapsvarsler for å holde seg oppdatert på nye trusler som er relevante for sivilsamfunnet.
- **Tilpasning til din kontekst:** Vektlegging av at disse avanserte tiltakene er valgfrie og bør tilpasses civilsamfunnsorganisasjonens tekniske ekspertise og ressurser. Veiledning om hvordan man avgjør hvilke avanserte verktøy som er verdt å ta i bruk, og sikrer at personalet opplæres i å bruke dem effektivt.

Eksempler på aktiviteter eller øvelser:

- **Spydphishing-scenario:** Veilederen presenterer et eksempel på et svært målrettet phishing-forsøk (for eksempel en e-post som ser ut til å være fra en kjent finansierer som ber om en overføring). Deltakerne øver på et verifiseringstrinn (for eksempel å ringe avsenderens offisielle telefonnummer eller sjekke e-postoverskriften) i stedet for å svare via e-post. Diskuter hvordan denne tilnærmingen kan forhindre sofistikerte svindelforsøk.
- **Demonstrasjon av maskinvarenøkkel:** Deltakerne får se eller prøve en maskinvaresikkerhetsnøkkel. Instruktøren går gjennom registrering av nøkkelen til en konto og deretter innlogging ved hjelp av nøkkelen. Hvis det er mulig, kan du la frivillige prøve prosessen på en demo-konto for å avmystifisere hvordan disse enhetene fungerer og fremheve sikkerhetsfordelene.

- **Minitrusseljakt:** Gi deltakerne en forenklet nettverkslogg eller et eksempel på et varsel fra et hypotetisk innbruddsdeteksjonssystem (IDS). Be deltakerne undersøke oppføringene for å oppdage noe mistenkelig (f.eks. en ukjent IP-adresse som foretar flere påloggingsforsøk på merkelige tidspunkter). Dette gir en forsmak på hvordan nettverksovervåkingsverktøy kan avdekke avvik.
- **Diskusjon om lokal relevans:** [Sett inn et eksempel på en avansert trussel eller et cybersikkerhetsverktøy som har vekt oppmerksomhet i landet ditt] – Diskuter om denne trusselen eller dette verktøyet er noe sivilsamfunnsorganisasjonen bør være opptatt av eller vurdere å bruke. Hvordan kan lokale ressurser (som nasjonale CSIRT-råd eller cybersikkerhetsfellesskap) hjelpe CSO-en med å takle slike avanserte trusler?

Modul 8 – Kasusstudie: Administrerende direktørs svindelforsøk forpurret

Kontekst: En sivilsamfunnsorganisasjon administrerte et stort tilskuddsprosjekt med flere internasjonale givere. De ansatte har erfaring med grunnleggende sikkerhet, men har ikke håndtert svært målrettede angrep. Organisasjonen hadde nylig introdusert maskinvaresikkerhetsnøkler for nøkkelansvarlige og vurdert avanserte sikkerhetsverktøy.

Problem: CSO-ens økonomisjef mottok en hastemelding på e-post som angivelig var fra den administrerende direktøren, med en anmodning om en stor bankoverføring til en ny leverandør for prosjektforsyninger. E-posten så legitim ut, uten tydelige tegn på phishing. Økonomisjefen var i ferd med å gå videre da han/hun husket å verifisere forespørselen. Vedkommende ringte direktøren på kontoret. Direktøren ble overrasket og sa at han ikke hadde sendt noen e-post. De innså umiddelbart at det var et sofistikert forsøk på e-postsvindel (administrerende direktør-svindel). Siden det var installert maskinvaresikkerhetsnøkler for direktørens kontoer, hadde angriperen ikke kompromittert direktørens pålogging; det var en helt falsk e-post.

Resultat: CSO-ansatte blokkerte ytterligere e-poster fra angriperens adresse og rapporterte forsøket på svindel. For å forhindre fremtidige forsøk holdt sivilsamfunnsorganisasjonen en orientering om verifisering av uvanlige forespørsler (ved hjelp av separate kanaler) og oppdaterte sjekklisten for hendelsesrespons til å omfatte trinn for mistanke om phishing. De bestemte seg også for å distribuere sikkerhetsnøkler mer utstrakt til kontoer med høye

privilegier. Takket være disse tiltakene unngikk organisasjonen økonomiske tap og økte de ansattes tillit til at avanserte phishing-angrep kan oppdages og forhindres.

Diskusjonsspørsmål:

- *Hvordan oppdaget og forhindret sivilsamfunnsorganisasjonen svindelforsøket før midlene gikk tapt?*
- *Hvilken rolle spilte maskinvaresikkerhetsnøklene og verifiseringsprosedyren i dette scenariet?*
- *Hvilke avanserte sikkerhetsforbedringer (fra denne modulen) bestemte sikkerhetssjefen seg for å iverksette som følge av denne hendelsen?*

Vurdering av modul 8

Denne modulen vil bli vurdert med fem korte spørsmål og én liten oppgave. Det kreves en poengsum på minst 70 % for å bestå.

Vurdering av modul 8

Korte spørsmål

1. Hva gjør avanserte phishing- eller spoofing-angrep farligere enn grunnleggende phishing-forsøk?
2. Hva er administrerende direktør-svindel, og hvorfor er sikkerhetsledere spesielt utsatt for denne typen angrep?
3. Hvordan skiller maskinvaresikkerhetsnøkler seg fra tradisjonelle tofaktorautentiseringsmetoder, og hvorfor anses de som phishing-bestandige?
4. Hva er formålet med nettverksovervåking eller innbruddsdeteksjonssystemer i en organisasjon?
5. Hvorfor bør CSO-er vurdere kapasiteten og behovene sine nøye før de tar i bruk avanserte sikkerhetsverktøy?

Praktisk oppgave: Sjekk av beredskap mot avanserte trusler

Deltakerne bes om å fullføre følgende oppgave:

- Identifiser **én avansert trussel** som er relevant for deres sivilsamfunnsorganisasjon (f.eks. administrerende direktør-svindel, målrettet phishing, kontospoofing).
- Beskriv kort:
    - Ett verifiseringstrinn personalet bør ta før de handler på mistenkelige forespørsler,

- Ett avansert sikkerhetsverktøy eller en avansert praksis som kan bidra til å redusere risikoen (f.eks. maskinvaresikkerhetsnøkler, passordbehandlere, verifiseringsprosedyrer),
- Om dette tiltaket er gjennomførbart for sivilsamfunnsorganisasjonen deres for øyeblikket, og hvorfor.

Deltakerne bør presentere svarene sine i tre til fem korte punkter eller diskutere dem kort i små grupper.

4. LANDBASERTE RETTSLIGE OG REGULERINGSMESSIGE RAMMEVERK

4.1 Rettslige og regulatoriske rammer i Tyrkia og forslag til organisasjoner i sivilsamfunnet i Tyrkia

Omfanget av personvernloven (KVKK) og dens innvirkning på sivilsamfunnsorganisasjoner

Lov nr. 6698 om beskyttelse av personopplysninger (KVKK) er den primære lovgivningen som regulerer behandlingen av personopplysninger i Tyrkia. Loven gjelder for alle fysiske og juridiske personer som behandler personopplysninger, inkludert offentlige institusjoner, organisasjoner i privat sektor og sivilsamfunnsorganisatorasjoner (CSO-er) (Personal Data Protection Authority [KVKK], 2020).

Civilsamfunnsorganisasjoner innhenter og behandler vanligvis personopplysninger knyttet til medlemmer, frivillige, givere og ansatte. Slike opplysninger kan omfatte navn, kontaktopplysninger, fotografier, donasjonsbeløp og registreringer av deltakelse på arrangementer. Derfor har også sivilsamfunnsorganisasjoner forpliktelser som behandlingsansvarlige i henhold til KVKK.

I henhold til loven kan personopplysninger kun behandles for spesifikke, eksplisitte og legitime formål, og de må slettes eller anonymiseres når formålet med behandlingen opphører. Civilsamfunnsorganisasjoner må handle i samsvar med disse prinsippene i alle datainnsamlingsprosesser, fra medlemskapsskjemaer til digitale kampanjer.

Tiltak som organisasjoner i sivilsamfunnet må iverksette for å overholde KVKK

De viktigste trinnene civilsamfunnsorganisasjoner bør følge for å sikre samsvar med KVKK, omfatter:

1. **Utarbeidelse av en databeholdning:** Civilsamfunnsorganisasjoner bør identifisere og dokumentere hvilke personopplysninger de behandler, til hvilke formål, hvor lenge opplysningene oppbevares og hvem de deles med.
2. **Innhenting av uttrykkelig samtykke:** Det må innhentes uttrykkelig samtykke for behandlingsaktiviteter som ikke er juridisk obligatoriske (f.eks. markedsførings-e-poster). Samtykket må gis frivillig, være informert og kunne tilbakekalles når som helst.
3. **Informasjonsplikt:** Personer hvis personopplysninger innhentes, må informeres skriftlig om hvem som behandler opplysningene deres, til hvilke formål, på hvilket rettsgrunnlag og hvilke rettigheter de har.

4. **Datasikkerhetstiltak:** Fysiske (låste skap), digitale (kryptering, antivirusprogramvare, tilgangsbegrensninger) og organisatoriske (taushetserklæringer, bevissthetstrening) tiltak må iverksettes.
5. **VERBIS-registrering:** Sivilsamfunnsorganisasjoner hvis aktiviteter er begrenset utelukkende til egne medlemmer, frivillige og givere, er unntatt fra VERBIS-registrering. Civilsamfunnsorganisasjoner med en økonomisk virksomhet er imidlertid pålagt å registrere seg i systemet (KVKK, 2020).

KVKK-overtredelser og sanksjoner

KVKK fastsetter administrative bot og, i noen tilfeller, strafferettslige sanksjoner ved overtredelser (KVKK, 2020). Dersom sivilsamfunnsorganisasjoner unnlater å oppfylle datasikkerhetsforpliktelsene sine, kan de bli ilagt betydelige bøter ved databrudd, uautorisert datadeling eller unnlatelse av å varsle om brudd.

Fra og med 2024 varierer administrative botbeløp fra 25 000 TL (569 USD) opptil 1 800 000 TL, avhengig av overtredelsens art. For eksempel utgjør unnlatelse av å registrere seg hos VERBIS for en sivilsamfunnsorganisasjon som er underlagt registreringsplikten, et alvorlig brudd.

KVKK-styret har også iverksatt sanksjoner mot sivilsamfunnsorganisasjoner. I 2020 ble en forening idømt bøter etter en klage angående uautorisert SMS-kommunikasjon, ettersom den ikke hadde innhentet uttrykkelig samtykke og ikke hadde slettet personopplysningene. Dette viser at sivilsamfunnsorganisasjoner er underlagt revisjoner og håndhevelsestiltak i henhold til loven.

Lov om cybersikkerhet og varslingsplikt

Lov nr. 7545 om cybersikkerhet trådte i kraft i 2025 og omfatter alle institusjoner som leverer tjenester i digitale miljøer, uten å skille mellom offentlige og private enheter (Offisiell tidsskrift, 2024). Innenfor dette rammeverket er også sivilsamfunnsorganisasjoner underlagt varslingsplikt ved hendelser.

Dersom det oppstår et datainnbrudd, en infeksjon med skadevare, et cyberangrep eller det identifiseres en kritisk sårbarhet i en sivilsamfunnsorganisasjons systemer, må hendelsen

rapporteres til Cybersikkerhetsdirektoratet, som er tilknyttet det tyrkiske presidentskapet, innen maksimalt 48 timer.

Unnlatelse av å overholde dette kan føre til administrative boter fra 1 000 000 TL og, i visse tilfeller, strafferettslige sanksjoner som fengsel for ansvarlige personer. Denne forskriften fastsetter en grunnleggende forpliktelse til sikkerhet og åpenhet for alle sivilsamfunnsorganisasjoner.

Nasjonal cybersikkerhetsstrategi og rollen til organisasjoner i sivilsamfunnet

Den nasjonale cybersikkerhetsstrategien og handlingsplanen for 2024–2028 er hoveddokumentet som definerer Tyrkias visjon for digital sikkerhet. Dokumentet tildeler spesifikke roller til offentlige institusjoner, privat sektor og civilsamfunnsorganisasjoner (Ministry of Transport and Infrastructure, 2023).

Sentrale forventninger til organisasjoner i sivilsamfunnet omfatter å øke allmenn bevissthet, fremme individuell digital sikkerhetskompetanse og gjennomføre aktiviteter for digital kompetanse for utsatte grupper, som barn og eldre.

Videre understreker strategien viktigheten av sivilsamfunnets deltakelse og oppfordrer organisasjoner i sivilsamfunnet til å gjennomføre kampanjer og opplæringsaktiviteter i samarbeid med offentlige institusjoner.

Rettslig status for digitale verktøy

Som en del av den digitale transformasjonen kan det kreves at sivilsamfunnsorganisasjoner bruker visse digitale verktøy. I henhold til lov nr. 5070 om elektroniske signaturer har elektroniske signaturer samme rettslige gyldighet som håndskrevne signaturer. Styrevedtak, kontrakter og offisiell korrespondanse kan derfor signeres elektronisk (Myndigheten for informasjons- og kommunikasjonsteknologi, 2023).

Civilsamfunnsorganisasjoner med en økonomisk virksomhet eller som overskrider visse omsetningsgrenser, kan være underlagt forpliktelser knyttet til e-faktura (e-Fatura) og e-arkiv

(e-Arşiv). Skatteetaten publiserer årlige meddelelser som spesifiserer de gjeldende tersklene (Skatteetaten, 2024).

Registrert elektronisk post (KEP) er en annen foretrukket metode for offisielle varslinger, spesielt for å sikre juridisk gyldighet. Ved bruk av alle disse verktøyene må sivilsamfunnsorganisasjoner sikre ikke bare teknisk tilstrekkelighet, men også full overholdelse av det relevante rettslige rammeverket.

Digital sikkerhet for små og mellomstore sivilsamfunnsorganisasjoner i Tyrkia

Innledning

Følgende fem originale caser er utarbeidet for opplæringsformål og er basert på realistiske digitale sikkerhetsrisikoer og erfaringer fra små og mellomstore sivilsamfunnsorganisasjoner (CSO-er) som opererer i Tyrkia. Hver sak presenterer tydelig civilsamfunnsorganisasjonens struktur, hendelsen som oppstod, den tekniske eller menneskelige sårbarheten som var involvert, konsekvensene og lærdommene som kan trekkes for andre civilsamfunnsorganisasjoner. Alle sivilsamfunnsorganisasjoner presenteres anonymt i denne studien.

LOKALE CASESTUDIER FRA TYRKIA

Case 1: Hodepine forårsaket av en felle med falsk e-post

Denne sivilsamfunnsorganisasjonen er en liten utdanningsforening som opererer med kun fire ansatte og noen få frivillige, og som har som mål å tilby stipender og utdanningsstøtte til lokale studenter. Den digitale driften er hovedsakelig avhengig av e-postkommunikasjon, kontorprogramvare og WhatsApp-basert koordinering med frivillige. Organisasjonen har ingen egen IT-ansatt, og de ansatte bruker generelt egne bærbare datamaskiner til arbeid.

«En dag kommer det en e-post med emnet «Kunnskapsstipend fra departementet» til foreningens generelle innboks, info@…. I meldingen hevdes det at organisasjonen har fått tildelt et tilskudd den søkte om, og det bes om at den vedlagte PDF-filen åpnes for ytterligere detaljer. Prosjektlederen blir begeistret for nyheten og laster ned og åpner vedlegget uten å

verifisere dets ekthet. Filen åpnes ikke riktig, men en skadelig programvare installeres i det stille på datamaskinen.»

Den største sårbarheten i dette tilfellet er menneskelig feil og manglende bevissthet. Den ansatte hadde ikke mottatt opplæring i cybersikkerhet og unnlot å undersøke avsenderadressen, språkfeilene og det mistenkelige vedlegget nøye. Dette var klare indikatorer på en phishing-e-post utformet for å etterligne en offisiell institusjon.

I løpet av én dag ble delte e-postkontoer som ble brukt av prosjektansvarlig og styret, kompromittert. Angriperne sendte falske meldinger med forespørsler om penger til givere og partnere. Kommunikasjonen ble forstyrret, tilliten ble rystet, og noen støttespillere innstilte engasjementet midlertidig. På mellomlang sikt måtte organisasjonen investere tid og krefter i å gjenopprette troverdigheten og den interne moralen.

Erfaringer og anbefalinger

Phishing-angrep er en av de vanligste cybertruslene for sivilsamfunnsorganisasjoner. Alle ansatte og frivillige bør opplæres i å identifisere mistenkelige e-poster. Avsenderadresser, vedlegg og hastende forespørsler bør alltid verifiseres. Grunnleggende cyberhygienepraksis og tofaktorautentisering for kritiske kontoer bør iverksettes.

Case 1: Hodepine forårsaket av en falsk e-postfelle

Relevant(e) modul(er)

- Modul 4: Vanlige cybertrusler (nettfisking og skadevare)
- Modul 5: Overholdelse av personvern og databeskyttelse
- Modul 7: Utvikle en sikkerhetskultur

Slik kan denne casen brukes i opplæring

- **Eksempel på bevisstgjøring (modul 4):**
  Denne saken kan presenteres i begynnelsen av modulen som et **realistisk phishing-scenario** rettet mot små sivilsamfunnsorganisasjoner. Instruktører kan be deltakerne om å identifisere røde flagg i e-posten (avsenderadresse, vedlegg, hastverk, språkfeil) før de avslører resultatet.
- **Diskusjon om menneskelige feil (modul 7):**
  Bruk denne saken til å understreke at cybersikkerhet ikke bare er et teknisk problem, men også et **problem knyttet til menneskelig atferd**. Den fungerer godt som en diskusjonsstarter om hvorfor opplæring av ansatte og frivillige er avgjørende, spesielt i små sivilsamfunnsorganisasjoner uten IT-ansatte.
- **Refleksjon over kontosikkerhet (modul 5):**
  Saken kan støtte diskusjon om **beskyttelse av e-postkontoer**, herunder tofaktorautentisering og tilgangsadministrasjon, og koble phishing-angrep til mer omfattende databeskyttelsesrisikoer.

Foreslått metode:

Gruppediskusjon + «Hva ville du gjort annerledes?»- -øvelse.

Case 2: Overtakelse av konto på sosiale medier

Denne saken gjelder en mellomstor sivilsamfunnsorganisasjon for kvinners rettigheter med ca. 20 ansatte og frivillige. Organisasjonen bruker aktivt sosiale medieplattformer som Instagram, X (tidligere Twitter) og Facebook til påvirkning og offentlig engasjement. Kontoene administreres hovedsakelig av en kommunikasjonsansvarlig, selv om frivillige av og til bidrar. Ingen tofaktorautentisering er aktivert.

En morgen dukker det opp uvanlige innlegg på organisasjonens offisielle Instagram-konto. Profilbildet og biografien endres, og svindelaktig investeringsrelatert innhold deles med følgere. Medlemmer og følgere varsler organisasjonen om at kontoen er hacket.

Kommunikasjonssjefen brukte det samme passordet på tvers av flere plattformer. Et datainnbrudd på en annen tjeneste avslørte passordet, noe som gjorde det mulig for angriperne å få tilgang til den sosiale mediekontoen. Fraværet av tofaktorautentisering gjorde overtakelsen enda enklere. I tillegg manglet organisasjonen en forhåndsdefinert kriseberedskapsplan.

Kontoen ble midlertidig suspendert mens gjenopprettingsprosedyrene ble iverksatt. Følgerne ble varslet via alternative kanaler. Selv om tilgangen til slutt ble gjenopprettet, oppstod det skade på omdømmet, og noen følgere mistet tilliten. Som svar styrket organisasjonen passordpolicyene og aktiverte tofaktorautentisering.

Erfaringer og anbefalinger

Sosiale mediekontoer er hyppige mål for cyberangrep. Sterke, unike passord og tofaktorautentisering er avgjørende. Gjenbruk av passord bør unngås, og ansatte som administrerer sosiale medier bør få målrettet opplæring i sikkerhetsbevissthet.

Case 2: Overtakelse av konto på sosiale medier

Relevant(e) modul(er)

- **Modul 6: Sikkerhet på sosiale medier og på nettet**
- **Modul 7: Utvikle en sikkerhetskultur**

Slik kan denne casen brukes i opplæring

- **Kjernecasestudie (modul 6):**
  Denne casen er ideell som **primær casestudie** når du underviser i sikkerhet på sosiale medier. Instruktører kan lede deltakerne gjennom hendelsen trinn for trinn og knytte feil til manglende kontroller (gjenbruk av passord, ingen 2FA, ingen beredskapsplan).
- **Øvelse i hendelsesrespons (modul 7):**
  Saken kan omdannes til et rollespillscenarie der deltakerne bestemmer seg for hvordan de skal kommunisere med følgere, rapportere bruddet til plattformen og gjenopprette kontoen.
- **Målrettet opplæringsdiskusjon:**
  Fremhev at ansatte med ansvar for kommunikasjon og påvirkning trenger spesialisert sikkerhetsbevissthet, ikke bare generell opplæring.

Foreslått metode:
Saksanalyse + rollespill om hendelsesrespons.

Casestudie 3: Kostnaden ved tap av data og mangel på sikkerhetskopier

Sivilsamfunnsorganisasjonens type, størrelse og digitale arbeidspraksis

Denne saken gjelder en liten miljøorganisasjon med tre heltidsansatte og flere frivillige. Prosjektdokumenter utarbeides på personlige bærbare datamaskiner og deles via skytjenester. Kritiske data som giverlister og økonomiske opptegnelser lagres imidlertid kun på lederens stasjonære datamaskin, uten regelmessige sikkerhetskopier.

Etter et strømbrudd klarer ikke lederens datamaskin å starte på nytt på grunn av skade på harddisken. Forsøk på å gjenopprette dataene lokalt mislykkes, og profesjonelle datagjenopprettingstjenester anbefales til høye kostnader uten garantert suksess.

Det var ikke noe cyberangrep; hendelsen skyldtes dårlig datahåndtering og mangel på en sikkerhetskopistrategi. Lagring av kritiske data på én enkelt enhet og bruk av utdatert maskinvare økte risikoen for datatap betraktelig.

OCSOing-prosjekter ble avbrutt, og viktige rapporter, finansielle dokumenter og kontaktlister gikk tapt. De ansatte brukte uker på å prøve å rekonstruere manglende data. Tillit fra givere og partnere ble påvirket, og det oppstod økonomiske tap på grunn av gjenopprettingsarbeid og avbrutte prosjekter.

Erfaringer og anbefalinger

Regelmessige sikkerhetskopier av data er avgjørende for organisasjonens kontinuitet. Sikkerhetskopier bør lagres på flere plattformer og testes med jevne mellomrom. Maskinvaren bør holdes oppdatert, og det bør brukes strømbeskyttelsessystemer.

Case 3: Kostnaden ved tap av data og mangel på sikkerhetskopier

Relevant(e) modul(er)

- **Modul 5: Overholdelse av personvern og databeskyttelse**
- **Modul 7: Utvikle en sikkerhetskultur**

Slik kan denne casen brukes i opplæring

- **Eksempel på datahåndtering (modul 5):**
  Denne casen er effektiv for å forklare at ikke alle sikkerhetshendelser involverer hackere. Instruktører kan bruke den til å introdusere sikkerhetskopistrategier, datatilgjengelighet og organisasjonskontinuitet.
- **Øvelse i risikovurdering:**
  Deltakerne kan bes om å liste opp kritiske data i sine egne sivilsamfunnsorganisasjoner og identifisere om det finnes lignende enkeltfeilpunkter.
- **Diskusjon om lederansvar (modul 7):**
  Saken viser hvorfor databeskyttelse og sikkerhetskopiering er ansvar på ledelsesnivå, og ikke bare tekniske oppgaver.

Foreslått metode:
Veiledet refleksjon + miniaktivitet med datarevisjon.

Sak 4: Faren ved svake passord og delte kontoer

Dette scenariet omhandler en mellomstor stiftelse som støtter personer med nedsatt funksjonsevne. Rundt 15 ansatte og frivillige bruker delte e-post- og systemkontoer til den daglige driften, og benytter seg av ett brukernavn og ett passord på tvers av flere plattformer.

Giveren rapporterer at han/hun mottar mistenkelige meldinger med forespørsel om penger. Undersøkelser avdekker at en tidligere frivillig fortsatt hadde tilgang til delte kontoer fordi passordene aldri ble endret etter vedkommendes avreise. Disse påloggingsopplysningene ble senere misbrukt av uautoriserte personer.
Svake og delte passord, gjenbruk av passord og fravær av prosedyrer for inndragning av tilgang skapte et alvorlig sikkerhetshull. Organisasjonen manglet klare retningslinjer for håndtering av digital tilgang når ansatte eller frivillige slutter.

Passordene ble endret umiddelbart, og giverne ble informert. Selv om den umiddelbare skaden var begrenset, oppstod det skade på omdømmet. På mellomlang sikt innførte organisasjonen strengere passordpolicyer, individuelle brukerkontoer og oppmerksomhetsøkter for personalet.

Hver konto bør ha et sterkt, unikt passord. Delte kontoer bør unngås der det er mulig, og tilgangsrettigheter må gjennomgås og tilbakekalles umiddelbart når personell slutter. Tydelige interne retningslinjer er avgjørende.

Case 4: Faren ved svake passord og delte kontoer

Relevant(e) modul(er)

- **Modul 6: Sikkerhet på sosiale medier og på nettet**
- **Modul 7: Utvikle en sikkerhetskultur**
- **Modul 8: Avanserte emner (kontotilgang og -kontroller)**

Slik kan denne casen brukes i opplæring

- **Illustrasjon av policyhull (modul 7):**
  Denne casen demonstrerer tydelig risikoen ved manglende **retningslinjer for tilgangsadministrasjon**, særlig prosedyrer for avmelding, når ansatte eller frivillige slutter.

- **Diskusjon om kontosikkerhet (modul 6):**
  Instruktører kan knytte denne casen til viktigheten av individuelle kontoer, sterke passord og rollebasert tilgang – spesielt for e-post og donorkommunikasjon.
- **Introduksjon til avansert tilgangskontroll (modul 8):**
  Saken kan tjene som en bro til mer avanserte praksiser, for eksempel kontorevisjoner, passordbehandlere og privilegiumsadministrasjon.

Foreslått metode:
Saksbasert øvelse i utarbeidelse av retningslinjer (f.eks. «Hva bør en sjekkliste for avmelding inneholde?»).

Merknad fra instruktør (valgfritt å legge til på slutten av avsnittet)

Disse lokale casestudiene er utformet for å:

- Reflektere over realistiske risikoer som organisasjoner i sivilsamfunnet i Tyrkia står overfor,
- Oppmuntre til læring og diskusjon mellom kolleger,
- Demonstrere at cybersikkerhetshendelser ofte skyldes enkle problemer som kan forebygges,
- Fremheve viktigheten av retningslinjer, opplæring og beredskap, ikke bare teknologi.

Instruktører oppfordres til å tilpasse diskusjonsdybden avhengig av deltakernes organisasjonsstørrelse, digitale modenhet og roller.

Praktiske retningslinjer og maler for digital sikkerhet for sivilsamfunnsorganisasjoner

Innledning

Dette dokumentet presenterer praktiske retningslinjemaler som kan brukes til å styrke den digitale sikkerhetskapasiteten til små og mellomstore sivilsamfunnsorganisasjoner (CSO-er) i Tyrkia. Malene er utformet for å være enkle, praktiske og i samsvar med både nasjonal

lovgivning (personvernloven – KVKK, cybersikkerhetsloven) og internasjonal god praksis (NIST, ENISA, Tactical Tech).

1. Retningslinjer for akseptabel bruk (AUP)

Formål:

Å fremme ansvarlig bruk av organisasjonens digitale verktøy, internettilgang og informasjonssystemer.

Retningslinjebestemmelser:

- Alle ansatte skal utelukkende bruke organisasjonens digitale ressurser til arbeidsrelaterte formål.
- Passord må være individuelle og må ikke deles med andre.
- Ulovlig innhold kan ikke lagres, åpnes eller distribueres via organisasjonens systemer.
- Bruk av sosiale medier må ikke skade organisasjonens omdømme.
- Ingen data kan overføres utenfor organisasjonen uten forhåndsgodkjenning fra ledelsen.

Merknad:

Denne policyen trer i kraft når den signeres av de ansatte under onboarding og må gjennomgås årlig. (ENISA, 2021)

2. Plan for hendelsesrespons (IRP)

Formål:

Å sikre en rask og effektiv respons på potensielle digitale sikkerhetshendelser.

Trinn:

1. Personen som oppdager hendelsen, informerer umiddelbart den utpekte myndigheten i organisasjonen.
2. Myndigheten fastslår hendelsestypen (phishing, skadevare, datainnbrudd).
3. Berørte systemer isoleres (fjernes fra nettverket om nødvendig).

4. Alle digitale logger og registreringer knyttet til hendelsen oppbevares.
5. Hendelsen rapporteres til Cybersikkerhetsdirektoratet innen maksimalt 48 timer (Offisiell tidsskrift, 2024).
6. Det gjennomføres en evaluering etter hendelsen, og prosedyrene oppdateres deretter.

Merknad:

Denne planen er basert på lov nr. 7545 om cybersikkerhet og NIST SP 800-61 Rev. 2.

3. Grunnleggende personvernprosedyre

Formål:

Å sikre at personopplysninger som behandles i CSO, håndteres i samsvar med KVKK.

Implementering:

- Enhver databehandlingsaktivitet må ha et klart formål og overholde prinsippet om dataminimering.
- Personopplysninger kan ikke behandles uten uttrykkelig samtykke, med mindre annet er tillatt ved lov (KVKK, 2020).
- For hver datadelingsaktivitet må årsaken til deling, mottakeren og varigheten dokumenteres.
- Det må etableres retningslinjer for oppbevaring og destruering av data; personopplysninger må slettes eller anonymiseres når de ikke lenger er nødvendige.
- Papirbaserte opptegnelser må oppbevares i låste skap, og digitale data må beskyttes i krypterte mapper.

Merknad:

Det anbefales at organisasjonen utpeker en intern behandlingsansvarlig eller en ansvarlig person.

4. Protokoll for deling av tilgangsopplysninger og enheter

Formål:

Å regulere sikker bruk og deling av passord, brukerkontoer og digitale enheter i organisasjonen.

Regler:

- Passord må tildeles individuelt og må ikke skrives ned.
- På delte enheter må hver bruker logge på med en egen konto og ikke dele passord.
- Det er forbudt å overføre data til eksterne enheter (f.eks. personlige bærbare datamaskiner).
- Bruk av USB-minnepinner eller eksterne lagringsenheter er kun tillatt med godkjenning fra ledelsen.

Merknad:

Organisasjoner kan i tillegg definere en autentiseringspolicy (f.eks. flerfaktorautentisering).

5. Forpliktelse til digital sikkerhet (ansatte/frivillige)

Tekst til forpliktelse (eksempel):

«Med dette dokumentet forplikter jeg meg til å bruke de digitale systemene og verktøyene som [organisasjonsnavn] tilbyr, utelukkende innenfor rammen av mine oppgaver og med nødvendig forsiktighet. Jeg erkjenner mitt ansvar for å oppfylle alle forpliktelser knyttet til sikkerheten til organisasjonsdata.»

«Bu belgeyle, [Kurum Adı] tarafından tahsis edilen dijital sistem ve araçları yalnızca görev kapsamımda ve dikkatli biçimde kullanacağımı taahhüt ederim. Jeg erkjenner mitt ansvar for å oppfylle alle forpliktelser knyttet til sikkerheten til organisasjonsdata.»

Merknad:

Denne forpliktelsen bør signeres av alle ansatte og frivillige og oppbevares i deres personalmapper.

Sjekklister for digital sikkerhet for sivilsamfunnsorganisasjoner

For å styrke den digitale sikkerheten til små og mellomstore sivilsamfunnsorganisasjoner (CSO-er) som opererer i Tyrkia, oppgis det fire separate sjekklister nedenfor. Disse listene består av enkle og praktiske punkter som enkelt kan anvendes, selv av brukere med begrenset teknisk kunnskap. Hver sjekkliste oppsummerer viktige sikkerhetstiltak i tråd med gjeldende lovbestemmelser. Målet er å øke sikkerhetsbevisstheten i den daglige digitale driften og sikre beredskap for potensielle nødssituasjoner.

1. Sjekkliste for grunnleggende digital sikkerhet

☐ Bruker alle brukere sterke og unike passord?

☐ Er automatiske skjermlåser aktivert på datamaskiner og mobiltelefoner?

☐ Er oppdatert antivirusprogramvare installert på alle enheter?

☐ Oppdateres all programvare og alle applikasjoner regelmessig?

☐ Sikkerhetskopieres viktige dokumenter regelmessig (ekstern harddisk eller skylagring)?

☐ Er alle brukere forsiktige når de åpner e-postvedlegg?

☐ Overvåkes bruken av eksterne eller personlige enheter?

2. Sjekkliste for beredskap ved hendelser

☐ Er det utpekt en person som er ansvarlig for digital sikkerhet?

☐ Er det klart definert hvem hendelser skal rapporteres til og hvordan?

☐ Har alle ansatte grunnleggende kunnskap om å identifisere hendelser (nettfisking, skadevare osv.)?

☐ Er det tatt sikkerhetskopi av kritiske dokumenter og systemer?

☐ Finnes det en skriftlig prosedyre for hendelser som har funnet sted?

☐ Er personalet klar over 48-timers varslingsregelen? (Lov nr. 7545)

3. Sjekkliste for sikkerhet på sosiale medier

☐ Har kun autoriserte personer tilgang til kontoer på sosiale medier?

☐ Er tofaktorautentisering (2FA) aktivert på alle kontoer?

☐ Er passordene sterke og brukes de ikke på andre plattformer?

☐ Er det klart hvem som administrerer kontoene og til hvilket formål?

☐ Er innholdet underlagt forhåndsgodkjenning før det deles?

☐ Overvåkes mistenkelige påloginger eller uvanlige økninger i antall følgere?

4. Sjekkliste for informasjonssikkerhet for nye ansatte/frivillige

☐ Får nye medarbeidere eller frivillige opplæring i digital sikkerhet?

☐ Er retningslinjene for akseptabel bruk signert?

☐ Innhentes det forpliktelser angående behandling av personopplysninger?

☐ Er tilgangsrettighetene strengt begrenset til arbeidsoppgaver?

☐ Brukes organisasjonskontoer i stedet for personlige kontoer?

☐ Er det sikret at organisasjonens retningslinjer for passord og enheter overholdes?

4.2 Rettslige og regulatoriske rammer i Bosnia-Hercegovina og forslag til organisasjoner i sivilsamfunnet i Bosnia-Hercegovina

Juridisk og regulatorisk kontekst i Bosnia-Hercegovina (BiH)

Personvern i Bosnia-Hercegovina reguleres av **loven om personvern (Zakon o zaštiti ličnih podataka)**. Den kompetente tilsynsmyndigheten er **Byrået for personvern i Bosnia-Hercegovina (AZLP)**. Selv om EUs personvernforordning (GDPR) ikke er direkte gjeldende i Bosnia-Hercegovina, krever mange EU-finansierte programmer og internasjonale givere standarder som er i tråd med GDPR. Som et resultat av dette gjenspeiler organisatorisk praksis og veiledning i Bosnia-Hercegovina i økende grad de sentrale GDPR-prinsippene, som lovlighet, dataminimering, ansvarlighet og sikkerhet ved behandling.

Bosnia-Hercegovina har ennå ikke én enkelt, omfattende nasjonal lov om cybersikkerhet. I denne sammenhengen forventes det primært at organisasjoner i sivilsamfunnet (OSS-er) sikrer digital sikkerhet gjennom interne styringsmekanismer, herunder klart definerte roller og ansvarsområder, interne retningslinjer for informasjonssikkerhet og dokumenterte prosedyrer som konsekvent anvendes i den daglige driften.

Nasjonale institusjoner og støttemekanismer for cyberhendelser

Flere offentlige institusjoner yter støtte, koordinering eller etterforskningsfunksjoner ved cybersikkerhetshendelser i Bosnia-Hercegovina. Disse omfatter **CERT BiH**, som er ansvarlig for støtte til hendelsesrespons, tidlige varsler og overvåking av trusler, samt **Ministeriet for sikkerhet i BiH – cybersikkerhetssektoren**, som sørger for koordinering og veiledning på politisk nivå. Rapportering og etterforskning av nettkriminalitet håndteres av **Statens etterforsknings- og beskyttelsesbyrå (SIPA)** gjennom spesialiserte enheter, i tillegg til enheters og kantonale politienheter for nettkriminalitet som er ansvarlige for operativ etterforskning på lokalt nivå.

Cybertrussellandskapet for civilsamfunnsorganisasjoner i Bosnia-Hercegovina

Civilsamfunnsorganisasjoner i Bosnia-Hercegovina står oftest overfor cybertrusler knyttet til phishing-angrep rettet mot organisasjonens økonomi, tilskudd og donorkommunikasjon. Ransomware-hendelser og permanent tap av data er også hyppige, ofte på grunn av manglende eller utilstrekkelige sikkerhetskopieringsrutiner. Etterligningsangrep og

angrep basert på sosial manipulering observeres i økende grad via meldingsplattformer som WhatsApp og Viber, mens skade på nettsteder utgjør en spesiell risiko for organisasjoner som arbeider med politisk eller sosialt sensitive temaer. I tillegg er tyveri av tilgangsopplysninger knyttet til bruk av usikrede offentlige Wi-Fi-nettverk fortsatt et tilbakevendende problem.

Operativ realitet for sivilsamfunnsorganisasjoner i Bosnia-Hercegovina og begrunnelse for en forenklet tilnærming

I praksis er mange sivilsamfunnsorganisasjoner i Bosnia-Hercegovina svært avhengige av personlige bærbare datamaskiner og mobiltelefoner for organisasjonsarbeid, og de bruker plattformer som Gmail, Google Workspace og sosiale medier som primære operasjonelle verktøy. Dedikerte IT- eller cybersikkerhetsmedarbeidere er sjeldne, og uformelle praksiser som deling av passord innenfor team er fortsatt vanlige.

Gitt denne realiteten, tar læreplanen bevisst i bruk en forenklet og pragmatisk tilnærming. Den prioriterer rimelige og lett gjennomførbare sikkerhetstiltak, tilbyr praktiske maler og bruksklare dokumenter, og fokuserer på klare, trinnvise sjekklister utformet for ikke-teknisk personale i stedet for komplekse tekniske løsninger.

Tilpasning til europeiske rammeverk for retningslinjer

Selv om Bosnia-Hercegovina ikke er medlem av EU, opererer mange sivilsamfunnsorganisasjoner innenfor rammeverk for EU-finansierte programmer og europeisk politikk. Denne læreplanen er derfor tilpasset de sentrale prinsippene i GDPR, særlig den risikobaserte tilnærmingen, samt bredere europeiske strategier for bevisstgjøring om cybersikkerhet og kapasitetsbygging. Tilpasningen er praktisk snarere enn legalistisk, og fokuserer på daglig implementering og organisasjonsatferd i stedet for formelle samsvarskrav.

Risikobasert tilnærming og policy-logikk

Europeiske politiske rammeverk legger vekt på forholdsmessighet, kontekstbevissthet og konsekvensvurdering. Læreplanen anvender denne logikken ved å prioritere

høyrisikoresurser og -aktiviteter, unngå altfor komplekse eller ressurskrevende kontroller, og fokusere på menneskesentrerte og realistiske sikkerhetspraksiser som kan opprettholdes i organisasjoner for sivilsamfunns organisasjoner.

ISO-inspirert logikk (forenklet)

Selv uten formell sertifisering kan sivilsamfunnsorganisasjoner dra nytte av forenklede prinsipper inspirert av ISO-standarder for informasjonssikkerhet. Disse omfatter identifisering av viktige organisatoriske ressurser, anvendelse av grunnleggende prinsipper for tilgangskontroll, etablering av strukturerte prosesser for hendelseshåndtering og fremming av kontinuerlig forbedring gjennom gjennomgang og læring. Denne tilnærmingen støtter en gradvis styrking av organisasjonens modenhet og motstandskraft over tid.

Lokale casestudier fra Bosnia-Hercegovina

Case 1: Phishing-lenke som fører til fullstendig kontoovertakelse

Denne saken gjelder en ungdomssorganisasjon i det sivile samfunn med base i Sarajevo. Organisasjonen opererer med et lite team og er i stor grad avhengig av delte e-postinnbokser og sosiale medieplattformer som Facebook og Instagram for kommunikasjon, koordinering og informasjon til allmennheten. Passord deles internt, og tofaktorautentisering er ikke aktivert. En medarbeider mottok en Facebook Messenger-melding som så ut til å komme fra en pålitelig prosjektpartner. Meldingen ba om bekreftelse av detaljer for en felles aktivitet og inneholdt en lenke. Medarbeideren klikket på lenken og oppga organisasjonens e-postopplysninger. I løpet av minutter fikk angriperen tilgang til den delte e-postinnboksen og tilkoblede kontoer på sosiale medier. Kontaktopplysninger for gjenoppretting ble endret, og falske betalingsforespørsler ble sendt til givere.

Hendelsen ble muliggjort av flere svakheter, inkludert delte passord, gjenbruk av passord på tvers av plattformer, mangel på tofaktorautentisering og overdrevne administrative rettigheter for alle brukere. Meldingen ble stolt på uten uavhengig verifisering. På kort sikt mistet organisasjonen tilgangen til e-post- og sosiale mediekontoer, noe som forstyrret

kommunikasjons- og pengeinnsamlingsaktiviteter. Svindelmeldinger skadet givernes tillit. På mellomlang sikt måtte sivilsamfunnsorganisasjonen investere betydelig tid i å gjenopprette kontoen og gjenoppbygge troverdigheten.

Erfaringer og anbefalinger

Alle organisasjonskontoer bør bruke unike passord som administreres via en passordbehandler, og tofaktorautentisering bør være aktivert. Administrative rettigheter må begrenses, og sensitive forespørsler bør alltid verifiseres via en sekundær kommunikasjonskanal.

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 1 – Grunnleggende om cybersikkerhet:**
  Brukes som et sentralt eksempel for å illustrere phishing-angrep, tyveri av tilgangsopplysninger og rask kontoovertaking.
- **Modul 4 – Vanlige cybertrusler (phishing og skadevare):**
  Viser hvordan sosial manipulering utnytter tillit og mangel på verifisering.
- **Modul 7 – Utvikling av en sikkerhetskultur:**
  Støtter diskusjon om medarbeidernes bevissthet, passordhygiene og viktigheten av tofaktorautentisering.

Foreslått bruk:
Saksanalyse etterfulgt av identifisering av røde flagg og kartlegging av forebyggende kontrolltiltak.

Case 2: WhatsApp-/Viber-etterligning som fører til økonomisk tap

Denne saken gjelder en mellomstor sivilorganisasjon som ofte bruker WhatsApp og Viber til intern koordinering og økonomisk kommunikasjon. Sensitive beslutninger håndteres ofte uformelt via meldingsapplikasjoner.

En angriper opprettet en WhatsApp- eller Viber-konto ved hjelp av navnet og profilbildet til en ekte prosjektkoordinator. Angriperen kontaktet økonomiavdelingen med en hastemelding om at bankopplysningene var endret, og ba om umiddelbar bruk av en ny IBAN. Forespørselen ble behandlet uten verifisering.

Organisasjonen stolte på uformelle meldingsplattformer for sensitive økonomiske beslutninger og manglet sekundære verifiseringsmekanismer. Det var ikke krav om godkjenning fra flere personer for finansielle transaksjoner.

Midlene ble overført til angriperen og kunne ikke gjenvinnes. Hendelsen resulterte i økonomisk tap og intern uro, samt omdømmeproblemer overfor givere og partnere.

Finansielle transaksjoner bør aldri godkjennes via meldingsplattformer. Alle betalingsrelaterte forespørsler må verifiseres gjennom offisielle kanaler, for eksempel signerte e-poster fra organisasjonens domene eller telefonsamtaler til kjente numre. Det bør innføres en regel om godkjenning av to personer for betydelige finansielle transaksjoner.

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 2 – Kommunikasjon og sosial manipulering:**
  Hovedsakelig sak som illustrerer etterligning og hastighetsbasert manipulering via meldingsplattformer.
- **Modul 7 – Utvikle en sikkerhetskultur:**
  Fremhever behovet for interne regler, verifiseringsprosedyrer og delt ansvar for økonomiske beslutninger.

Foreslått bruk:
Rollespilløvelse om verifisering av hastende økonomiske forespørsler og anvendelse av regelen om godkjenning av to personer.

Sak 3: Tyveri av tilgangsopplysninger via offentlig Wi-Fi

Denne saken gjelder en sivilorganisasjon som lar frivillige jobbe eksternt ved hjelp av personlige enheter. Skytjenester som Gmail og Google Drive er sentrale for den daglige driften, og det finnes ingen formell policy som regulerer ekstern tilgang eller enhetssikkerhet.

En frivillig jobbet fra en kafé ved hjelp av gratis offentlig Wi-Fi og logget seg på organisasjonens e-post og skylagring. Enheten manglet nylige sikkerhetsoppdateringer, og passord var lagret i nettleseren. Kort tid etterpå ble det oppdaget ukjente påloggінger, og kontaktlister over givere ble lastet ned. Responsen ble forsinket på grunn av uklare rapporteringsprosedyrer.

Organisasjonen tillot tilgang til sensitive kontoer via usikret offentlig Wi-Fi, brukte utdaterte enheter og tillot passord lagret i nettleseren. Det fantes heller ingen tydelig intern hendelsesrapporteringsmekanisme.

Sensitive data ble eksponert, og givernes tillit ble satt i fare. Forsinket respons økte den potensielle virkningen av datainnbruddet.

Sensitive kontoer bør ikke åpnes via offentlig Wi-Fi uten VPN. Enheter må holdes oppdatert, funksjoner for automatisk tilkobling må deaktiveres, og prosedyrer for hendelsesrapportering må formidles tydelig til alle ansatte og frivillige.

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 3 – Enhets- og infrastruktursikkerhet:**
  Kjerneeksempel på risiko knyttet til offentlig Wi-Fi, enheter uten oppdateringer og usikker lagring av tilgangsopplysninger.
- **Modul 7 – Utvikling av en sikkerhetskultur:**
  Understreker viktigheten av tydelige prosedyrer for hendelsesrapportering og medarbeidernes bevissthet.

Foreslått bruk:

Gruppediskusjon etterfulgt av en sjekklisteøvelse om sikker hjemmekontorpraksis.

Sak 4: Løsepengevirus via e-postvedlegg

Denne saken gjelder en regional sivilsamfunnsorganisasjon som bruker delte kontorbærbare datamaskiner og e-postbasert dokumentutveksling. Sikkerhetskopieringspraksisen var uformell, og det ble ikke opprettholdt noen frakoblede sikkerhetskopier. Det ble mottatt en e-post som lignet på en giverrapport, og en ansatt åpnet vedlegget på en delt bærbar PC. Kort tid etter ble filene utilgjengelige, og en løsepengsnotat dukket opp på skjermen. Organisasjonen stolte på avsenderens utseende, manglet regler for filtrering av vedlegg og opprettholdt ikke frakoblede eller isolerte sikkerhetskopier. Økonomiske opptegnelser og prosjektdokumentasjon gikk tapt for alltid. Pågående prosjekter ble avbrutt, og det påløp gjenopprettingskostnader. Civilsamfunnsorganisasjoner bør opprettholde minst én frakoblet sikkerhetskopi og bruke skytjenester med versjonshistorikk aktivert. Makroaktiverte og kjørbare vedlegg bør begrenses, og personalet bør opplæres i ikke å åpne uoppfordrede filer.

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 4 – Vanlige cybertrusler (skadevare og løsepengevirus):**
  Viser hvordan løsepengevirus sprer seg via e-postvedlegg og virkningen av manglende sikkerhetskopier.
- **Modul 5 – Overholdelse av databeskyttelse og personvern:**
  Fremhever datatilgjengelighet, sikkerhetskopieringsforpliktelser og risikoer knyttet til organisasjonens kontinuitet.

Foreslått bruk:

Scenariebasert diskusjon om sikkerhetskopistrategier og «Hva ville du gjort først?»-responstrinn.

Sak 5: Kapret Facebook-side på grunn av delte påloggingar

Flere ungdomsorganisasjoner delte én og samme Facebook-pålogging mellom ansatte og frivillige for å administrere offentlige sider. Tilgangen ble ikke gjennomgått da frivillige forlot organisasjonen. En tidligere frivillig beholdt tilgangen til den delte kontoen og misbrukte den senere. Facebook-siden ble kapret og brukt til å publisere svindelmeldinger og politisk innhold. Delte påloggingsopplysninger, mangel på rollebasert tilgang og unnlatelse av å tilbakekalle tilgang da personell sluttet, skapte et stort sikkerhetshull. Organisasjonens omdømme ble skadet, og givere kontaktet sivilsamfunnsorganisasjonen for å verifisere legitimiteten til det publiserte innholdet. Gjenoppretting krevde tid og offentlig avklaring.

Erfaringer og anbefalinger

Delte påloggingar bør unngås. Tilgang må tildeles gjennom plattformens rollefunksjoner, tofaktorautentisering bør være obligatorisk for administratorer, og tilgangsrettigheter må gjennomgås regelmessig.

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 6 – Sikkerhet på sosiale medier og på nettet:**
  Primært eksempel på delte påloggingsopplysninger, rollebasert tilgang og prosedyrer for kontogjenoppretting.
- **Modul 7 – Utvikling av en sikkerhetskultur:**
  Støtter policy-diskusjoner om tilbakekalling av tilgang og prosedyrer for avmelding.
- **Modul 8 – Avanserte emner (praksis for tilgangskontroll):**
  Kan refereres til ved innføring av sterkere kontoadministrasjon og administrative kontroller.

Foreslått bruk:
Saksbasert øvelse i utarbeidelse av retningslinjer med fokus på administrasjon av tilgang til sosiale medier.

PRAKTISKE MALER OG SJEKKLISTER For organisasjoner i sivilsamfunnet (OSS-er) i Bosnia-Hercegovina

VEDLEGG 1 – RETNINGSLINJER FOR AKSEPTABEL BRUK (AUP)

Mal for små og mellomstore CSO-er i Bosnia-Hercegovina

Dokumenttittel: Retningslinjer for akseptabel bruk (AUP)

Gjelder for: Alt personale, frivillige, praktikanter, eksterne konsulenter

1. Formål

   Denne policyen definerer reglene for sikker og ansvarlig bruk av OS-ens enheter, brukerkontoer og data.
2. Kontoer og passord

- Bruk unike passord for hver konto.
- Ikke del passord via chatgrupper, meldingsapper eller e-post.
- Aktiver tofaktorautentisering (2FA) for e-post-, skylagrings- og administratorkontoer på sosiale medier.
- Bruk en passordbehandler der det er mulig.

3. Enheter (bærbare datamaskiner og mobiltelefoner)

- Lås alle enheter med PIN-kode, passord eller biometrisk beskyttelse.
- Aktiver automatiske system- og sikkerhetsoppdateringer.
- Rapporter tapte eller stjålne enheter til hendelseslederen innen 1 time.

4. E-post og lenker

- Ikke åpne uventede vedlegg eller lenker.
- Bekreft alltid bank- eller betalingsendringer via en telefonsamtale til et kjent nummer.
- Behandle hastemeldinger eller meldinger som inneholder press som høyrisiko.

5. Wi-Fi og hjemmekontor

- Unngå å bruke offentlig Wi-Fi til administratorkontoer eller sensitive kontoer.
- Bruk en mobil hotspot eller VPN hvis tilgjengelig.

- Deaktiver automatisk tilkobling til wifi-nettverk.

6. Sosiale medier

- Bruk sideroller i stedet for delte pålogginger.
- Behold minimum antall administratorer.
- Fjern tilgangen umiddelbart når en medarbeider eller frivillig slutter.

7. Datahåndtering

- Innhent kun nødvendige personopplysninger.
- Lagre personopplysninger kun på godkjente steder (f.eks. CSOs skystasjon).
- Ikke lagre mottakerdata på personlige enheter uten kryptering.

8. Hendelsesrapportering

   Enhver mistanke om sikkerhets- eller datahendelser må rapporteres umiddelbart ved hjelp av CSO-organisationens hendelsesresponsplan.

Godkjent av: _____

Dato: _____

Neste gjennomgangsdato: _____

VEDLEGG 2 – HENDELSESRESPONSPLAN (IRP)

Forenklet – for små sivilsamfunnsorganisasjoner

Dokumenttittel: Plan for hendelsesrespons (forenklet)

1. Hva er en hendelse?

   En hendelse er enhver hendelse som truer sivilsamfunnsorganisasjoners kontoer, enheter, data eller omdømme, inkludert nettfisking, kontoovertakelse, skadevare, løsepengevirus eller datalekkasje.
2. Roller og ansvarsområder (fyll inn navn)

   Hendelsesansvarlig: _____

   Kommunikasjonsansvarlig: _____

   IT-støtte (intern/ekstern): _____

   Godkjenning fra ledelsen: _____
3. Første 15 minutter – umiddelbare tiltak

- Koble den berørte enheten fra Wi-Fi eller internett.
- Ta skjermbilder og noter tidspunktet og de berørte kontoene.
- Informer det interne teamet: «Ikke klikk på lenker. Hendelsen er under gjennomgang.»
- Sikre e-postkontoen først (endre passord og aktiver 2FA).

4. Første 60 minutter – inndamming

- Tilbakestill passord i denne rekkefølgen: e-post, skylagring, sosiale medier, bank- eller finansverktøy.
- Logg ut alle ukjente eller mistenkelige økter.
- Fjern ukjente administratorer, apper og integrasjoner.
- Kontroller regler for videresending av e-post.

5. Vurdering (samme dag)

- Hva skjedde?

- Hvilke opplysninger kan bli berørt (givere, mottakere, mindreårige)?
- Hvilke systemer og kontoer er berørt?

6. Ekstern rapportering (når det er nødvendig)

- CERT BiH for hendelsesstøtte og varsler.
- SIPA eller politiets enheter for nettkriminalitet ved mistanke om nettkriminalitet.
- Se gjennom AZLP-kravene dersom et personopplysningsbrudd er sannsynlig, og dokumenter iverksatte tiltak.

7. Kommunikasjonsregler

- Kun kommunikasjonsansvarlig utsteder eksterne uttalelser.
- Del kun fakta.
- Informer givere eller partnere om nødvendig.

8. Gjenoppretting

- Gjenopprett systemer fra sikkerhetskopier.
- Oppdater alle enheter.
- Gi personalet opplæring på nytt om hendelsestypen.

9. Gjennomgang etter hendelsen (innen 7 dager)

- Hvilken kontroll sviktet?
- Hva må endres (2FA, tilgangsroller, sikkerhetskopier, opplæring)?
- Oppdater retningslinjer og sjekklister.

VEDLEGG 3 – REGELBOK FOR PERSONVERN (INTERN)

Enkel intern regelbok for sivilsamfunnsorganisasjoner

Dokumenttittel: Regelbok for personvern (intern)

1. Omfang

   Dette regelverket gjelder for alle personopplysninger som behandles av CSO-en.

2. Grunnleggende personvernregler

- Behandle opplysninger på en lovlig og rettferdig måte.
- Innhent kun det som er nødvendig (dataminimering).
- Oppbevar opplysninger kun så lenge det er nødvendig.
- Iverksett beskyttelsestiltak som tilgangskontroll, sikkerhetskopier og 2FA.

3. Godkjente datalagringssteder

   CSO-skystasjon: _____

   CSO-e-postsystem: _____

   Lokal kryptert mappe (om nødvendig): _____

4. Tilgangskontroll

- Kun ansatte som trenger opplysningene, kan få tilgang til dem.
- Fjern tilgangen innen 24 timer når noen slutter.

5. Sensitive opplysninger og mindreårige

   Når du behandler opplysninger om mindreårige, må du iverksette strengere kontroller og begrense tilgangen.

6. Datadeling

- Del kun opplysninger via godkjente kanaler.
- Ikke del lister over mottakere via WhatsApp eller Viber.
- Bruk passordbeskyttede filer for sensitive data.

7. Håndtering av hendelser

   Enhver mistanke om datainnbrudd utløser umiddelbart hendelsesresponsplanen.

Godkjent av: _____

Dato: _____

Neste gjennomgangsdato: _____

VEDLEGG 4 – PRAKTISKE SJEKKLISTER

For sivilsamfellssorganisasjoner i Bosnia-Hercegovina med lav IT-kapasitet

Sjekkliste A – Grunnleggende sjekkliste for digital sikkerhet (startpakke)

Kontoer

- 2FA aktivert for e-post-, sky- og sosiale medieadministratorer.
- Unike passord i bruk.
- Passord deles ikke i chatgrupper.

Enheter

- Skjermlås aktivert.
- Automatiske oppdateringer er slått på.
- Antivirusprogram eller systembeskyttelse er aktivt.

Wi-Fi og hjemmekontor

- Gjeste-Wi-Fi er atskilt fra personalets Wi-Fi.
- Ingen administratorpåloggінger på offentlig Wi-Fi uten hotspot eller VPN.

Data og sikkerhetskopier

- Skyversjonshistorikk aktivert.
- Ukentlig sikkerhetskopiering tilgjengelig (én frakoblet kopi om mulig).
- Tilgangen fjernes umiddelbart når noen slutter.

Sosiale medier

- Sideroller i bruk.
- Kun 1–2 administratorer.
- Gjenopprettings-e-post og -telefon tilhører CSO-en.

Sjekkliste B – Sjekkliste for hendelsesrapportering (intern)

Når du mistenker en hendelse

- Koble den berørte enheten fra internett.
- Ta skjermbilder og noter klokkeslettet.
- Informer hendelseslederen umiddelbart.
- Endre e-postpassord og aktiver 2FA.
- Se etter ukjente påloggінger og regler for videresending av e-post.
- Identifisere berørte data (givere, mottakere, mindreårige).
- Avgjør om ekstern rapportering er nødvendig (CERT BiH, SIPA, politi, AZLP).

Minimumsregistrering av hendelser

Dato og klokkeslett for oppdagelse: _____

Oppdaget av: _____

Hva skjedde (kort beskrivelse): _____

Berørte kontoer eller systemer: _____

Iverksette tiltak: _____

Bevis lagret i: _____

Ekstern rapportering fullført (ja/nei): _____

4 .3 Juridiske, regulatoriske og operasjonelle rammer for sivilsamfunnsorganisasjoner i Nord-Makedonia

Rettslig og regulatorisk rammeverk i Nord-Makedonia

27. april 2016 vedtok Europaparlamentet og Rådet for Den europeiske union forordning (EU) 2016/679 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, og opphevet direktiv 95/46/EF. Dette markerte begynnelsen på en omfattende reformer på området personvern. Etter en toårig overgangsperiode trådte forordningen i kraft i hele EU 25. mai 2018.

Denne forordningen, ofte omtalt som GDPR, er fullt ut innført i Republikken Nord-Makedonia gjennom vedtakelsen av loven om personvern, som trådte i kraft 24. februar 2020.

Personvernloven regulerer syv grunnleggende prinsipper for behandling av personopplysninger:

- Lovlighet, rettferdighet og åpenhet,
- Formålsbegrensning,
- Dataminimering,
- Nøyaktighet,
- Lagringsbegrensning,
- Integritet og konfidensialitet,
- Ansvarlighet.

Ikke-statlige organisasjoner er som behandlingsansvarlige forpliktet til å anvende alle prinsippene kumulativt i alle tilfeller av behandling av personopplysninger og gjennom hele opplysningenes livssyklus. Unnlatelse av å anvende noen av disse prinsippene utgjør et brudd på personvernloven. Hovedmyndigheten med ansvar for implementering av og tilsyn med personvernloven er Byrået for personvern.

I tillegg, på området cybersikkerhet, representerer loven om sikkerhet for nettverks- og informasjonssystemer, vedtatt i juli 2025, det første omfattende rettslige rammeverket som regulerer cybersikkerhet i Nord-Makedonia. Loven er tilpasset det europeiske NIS2-direktivet og tar sikte på å etablere et høyt og felles beskyttelsesnivå for nettverks- og informasjonssystemer i både offentlig og privat sektor.

Ministeriet for digital transformasjon og det nasjonale teamet for håndtering av datainnsatser (MKD-CIRT), som opererer innenfor Byrået for elektronisk kommunikasjon, er ansvarlige for å overvåke, koordinere og reagere på cybersikkerhetshendelser. Av relevans for privat sektor, herunder ikke-statlige organisasjoner, er overgangsperioden for implementering som varer til 2027, og i løpet av denne perioden forventes alle enheter gradvis å overholde forpliktelsene som innføres ved loven.

Vanlige trusler og nylige hendelser som påvirker sivilsamfunnsorganisasjoner

I likhet med andre sektorer er ikke-statlige organisasjoner i Nord-Makedonia svært sårbare for cybersikkerhetstrusler. En sentral utfordring er at mange cyberhendelser fortsatt ikke oppdages eller rapporteres, noe som resulterer i mangel på omfattende og pålitelige hendelsesdata. Selv om et betydelig antall sivilsamfunnsorganisasjoner rapporterer at de er informert om endringer i lovgivningen og tilpasser sin operasjonelle praksis deretter, indikerer tilgjengelige data at mange organisasjoner ikke har vedtatt interne lover om beskyttelse av personopplysninger og ikke har utnevnt en personvernansvarlig.

Videre er andelen ansatte i sivilsamfunnsorganisasjoner som har mottatt formell opplæring i personvern fortsatt svært lav. Gitt at organisasjoner i sivilsamfunnet ofte opererer med begrensede økonomiske ressurser og står overfor vanskeligheter med å tildele midler til opplæring av ansatte, anbefales det at det etableres strukturerte samarbeidsmekanismer mellom Byrået for personvern og den ikke-statlige sektoren for å lette tilgangen til opplæringsmuligheter.

En stor risikofaktor for sivilsamfunnsorganisasjoner er det begrensede budsjettet de har til å investere i databeskyttelse og cybersikkerhet. Mange mindre organisasjoner fortsetter å bruke ulisensiert eller utdatert programvare, noe som øker eksponeringen for cybertrusler betydelig. Samtidig er det tilgjengelig flere håndbøker og veiledningsdokumenter på makedonsk som kan hjelpe sivilsamfunnsorganisasjoner med å styrke den digitale sikkerheten sin.

De mest identifiserte truslene omfatter:

• unnlatelse av å verifisere avsendere før man klikker på lenker eller åpner meldinger,
• begrenset bruk av passordadministratorer og hyppig gjenbruk av lignende passord,
• uregelmessig eller manglende sikkerhetskopiering av data,
• bruk av ulisensiert og utdatert programvare,
• utilstrekkelige sikkerhetstiltak for mobile enheter,
• svært lav bruk av tofaktorautentisering.

Nasjonal støtte og ressurser

Flere nasjonale institusjoner, deriblant Byrået for beskyttelse av personopplysninger, Departementet for digital transformasjon og Byrået for elektronisk kommunikasjon, yter støtte og veiledning til sivilsamfunnsorganisasjoner med sikte på å forbedre digital sikkerhet og databeskyttelse. Likevel er det behov for ytterligere institusjonelle tiltak, herunder systematisk planlegging og statlig finansierte initiativer.

Støtte ytes også gjennom prosjekter i sivilsamfunnet som primært finansieres av utenlandske givere for å øke den digitale kompetansen blant sivilsamfunnsorganisasjoner og befolkningen generelt. Et bemerkelsesverdig eksempel er prosjektet «CyberShield: Empowered Citizens for Cyber Resilience», som i 2025 omfattet tre opplæringsøkter i cybersikkerhet for organisasjoner som arbeider med marginaliserte grupper. Som oppfølging ble det utarbeidet digitale sikkerhetsplaner for seks organisasjoner i sivilsamfunnet. Disse skreddersydde planene tar sikte på å sikre systematisk implementering av cybersikkerhetspraksis, øke organisasjonens motstandskraft og indirekte forbedre tjenesteleveransen til sluttbrukerne.

Til tross for disse positive eksemplene betyr begrenset finansiering at bare et lite antall sivilsamfunnsorganisasjoner kan dra nytte av slike initiativer. Selv om flere håndbøker og opplysningsmateriell er tilgjengelig på makedonsk, er det nødvendig med et bredere og mer bærekraftig samarbeid mellom offentlige myndigheter og sivilsamfunnsorganisasjoner for å utvide tilgangen til opplærings- og kapasitetsbyggende aktiviteter. Økt finansiering og

målrettede programmer er spesielt nødvendig for å støtte direkte utdanning og opplæring av ansatte i sivilsamfunnsorganisasjoner.

Kulturell og operativ kontekst for organisasjoner i det sivile samfunn i Nord-Makedonia

De fleste sivilsamfunnsorganisasjoner i Nord-Makedonia opererer etter en donor- og prosjektbasert modell og har vanligvis små administrative og operasjonelle team, eller er i stor grad avhengige av frivillige. Organisasjonsarbeid utføres ofte ved hjelp av personlige enheter og allment tilgjengelige digitale tjenester som Google Workspace, Dropbox eller Microsoft 365, ofte uten riktig lisensiering.

Opplærings- og kapasitetsbyggende initiativer bør derfor fokusere på praktiske og realistiske tiltak, inkludert:

- Fordelene ved å bruke lisensierte produkter og tjenester.
- Bevisstgjøringkampanjer av typen «Tenk før du klikker».
- Regelmessige sikkerhetskopier av data og informasjon.
- Aktiv og konsekvent bruk av tofaktorautentisering.
- Sikring av mobile enheter og styring av bruken av dem.
- Ansvarlig passordpraksis.
- Effektiv bruk av skybaserte løsninger.
- Økt bevissthet om datadelingspraksis.

Nivået av digital kompetanse i Nord-Makedonia er fortsatt utilstrekkelig, også innenfor civilsamfunnsorganisasjonssektoren. Det kreves ytterligere finansiering, ressurser og koordinerte innsatser for å oppnå et høyere nivå av digital sikkerhet. Denne innsatsen bør omsettes i konkrete programmer og praktiske handlingsplaner som er tilpasset sivilsamfunnsorganisasjonenes faktiske behov og kapasitet.

Vedlegg og bruksklare maler (Nord-Makedonia)

VEDLEGG 1 – Landskapet for digital sikkerhet for sivilsamfunnsorganisasjoner i Nord-Makedonia

Dette vedlegget gjenspeiler de juridiske, institusjonelle og operasjonelle realitetene som påvirker sivilsamfunnsorganisasjoner i Nord-Makedonia, og støtter lokaliseringen av læreplanen.

Trussellandskap

- Phishing-angrep via e-post og falske institusjonelle meldinger.
- Ransomware-hendelser og tap av data på grunn av manglende sikkerhetskopier.
- Misbruk av usikrede personopplysninger.
- Risiko knyttet til bruk av personlige bærbare datamaskiner og mobile enheter.

Driftsutfordringer

- Lav bruk av passordbehandlere og hyppig gjenbruk av passord.
- Uregelmessige eller manglende rutiner for sikkerhetskopiering av data.
- Bruk av ulisensiert eller utdatert programvare.
- Utilstrekkelig sikkerhet på mobile enheter.
- Begrenset bruk av tofaktorautentisering.
- Mangel på øremerket finansiering til digitale sikkerhetstiltak.

Mal: 10 grunnleggende trinn for å øke den digitale beskyttelsen

Følgende grunnleggende trinn anbefales for sivilsamfunnsorganisasjoner i Nord-Makedonia:

- Installere og regelmessig oppdatere antivirus- og anti-malware-programvare.
- Utføre system- og programvareoppdateringer umiddelbart.
- Bruke sterke og unike passord for hver konto.
- Unngå å åpne vedlegg fra ukjente eller mistenkelige kilder.
- Kun oppgi sensitive opplysninger på krypterte nettsteder.
- Utføre regelmessige sikkerhetskopier av organisasjonsdata.
- Bruke separate e-postadresser til ulike formål.

• Forhindre phishing ved å skrive inn nettstedsadresser manuelt.
• Fjerne utdaterte eller ikke-støttede programmer.
• Behandle personopplysninger og organisasjonsdata med forsiktighet.

Mal – Interne driftsregler for digital sikkerhet

Hver sivilsamfunnsorganisasjon bør vedta et enkelt internt dokument som definerer regler for digital sikkerhet for ansatte, frivillige og besøkende. Dokumentet bør omfatte:

• Bruk unike passord for hver konto.
• Ikke del passord via chat-applikasjoner eller e-post.
• Aktiver tofaktorautentisering for e-post, skylagring og administratorkontoer på sosiale medier.
• Bruk en passordbehandler der det er mulig.
• Lås alle enheter med PIN-koder eller passord.
• Aktiver automatiske oppdateringer.
• Rapporter tapte eller stjålne enheter umiddelbart.
• Verifiser alle forespørsler om endring av bank- og betalingsopplysninger.
• Bruk mobile hotspots når du arbeider utenfor sivilsamfunnsorganisasjonens lokaler.
• Tildel tilgang til sosiale medier utelukkende via plattformroller.
• Hold antallet administratorer på et minimum.
• Innhent og lagre kun nødvendige personopplysninger.
• Rapporter eventuelle sikkerhetshendelser umiddelbart til den utpekte ansvarlige personen.

Mal – Plan for hendelsesrespons (forenklet)

Når en digital sikkerhetshendelse inntreffer eller mistenkes, må følgende tiltak iverksettes:

- Koble den berørte enheten fra nettverket,
- Bevare bevis knyttet til hendelsen,
- Informer det interne teamet,

- Sikre e-postkontoen først ved å endre passord og aktivere 2FA,
- Tilbakestill passordene for alle berørte kontoer,
- Logg ut ukjente eller mistenkelige økter,
- Fjerne ukjente administratorer og tilkoblede applikasjoner, rapportere hendelser til MKD-CIRT,
- Rapporter mistanke om nettkriminalitet til politiets nettkriminalitetsenheter,
- Rådføre seg med Datatilsynet ved mistanke om datainnbrudd,
- Vurdere hendelsens innvirkning og gjenopprette systemer fra sikkerhetskopier,
- Oppdatere enheter og programvare,
- Gi personalet opplæring på nytt,
- Oppdatere interne retningslinjer og sjekklister ved behov.

Praktiske sjekklister for sivilsamfunnsorganisasjoner i Nord-Makedonia

VEDLEGG 1 – Digitalt sikkerhetslandskap for sivilsamfunnsorganisasjoner i Nord-Makedonia

Dette vedlegget skisserer den juridiske, institusjonelle og operasjonelle konteksten som påvirker sivilsamfunnsorganisasjoner (CSO-er) i Nord-Makedonia. Det støtter lokaliseringen av læreplanen for digital sikkerhet ved å reflektere over vanlige risikoer, kapasiteter og praktiske behov hos sivilsamfunnsorganisasjoner som opererer i landet.

Trussellandskap

Sivilsamfunnsorganisasjoner i Nord-Makedonia står ofte overfor følgende digitale sikkerhetstrusler:

- Phishing-angrep via e-post og falske meldinger fra institusjoner
- Ransomware-hendelser og tap av data på grunn av manglende eller utilstrekkelige sikkerhetskopier
- misbruk eller eksponering av usikrede personopplysninger
- Risiko knyttet til bruk av personlige bærbare datamaskiner og mobile enheter til organisasjonsarbeid

Driftsutfordringer

I praksis opplever mange sivilsamfunnsorganisasjoner i Nord-Makedonia følgende utfordringer:

- Lav bruk av passordbehandlere og hyppig gjenbruk av passord,
- Uregelmessige eller manglende rutiner for sikkerhetskopiering av data,
- Bruk av ulisensiert eller utdatert programvare,
- Utilstrekkelig sikkerhet på mobile enheter,
- Begrenset bruk av tofaktorautentisering,
- Mangel på øremerket finansiering til digitale sikkerhetstiltak.

Ti grunnleggende trinn for å øke den digitale beskyttelsen

Følgende grunnleggende trinn anbefales for sivilsamfunnsorganisasjoner i Nord-Makedonia for å forbedre den digitale sikkerhetssituasjonen:

1. Installer og oppdater antivirus- og anti-malware-programvare regelmessig.
2. Installer system- og programvareoppdateringer umiddelbart når de er tilgjengelige.
3. Bruke sterke og unike passord for hver konto.
4. Unngå å åpne vedlegg fra ukjente eller mistenkelige kilder.
5. Oppgi sensitive opplysninger kun på krypterte nettsteder (HTTPS).
6. Utfør regelmessige sikkerhetskopier av organisasjonsdata.
7. Bruke separate e-postadresser til ulike formål (f.eks. administrasjon, prosjekter, offentlig kommunikasjon).
8. Forhindre phishing ved å skrive inn nettstedsadresser manuelt i stedet for å klikke på lenker.
9. Fjern utdaterte eller ikke-støttede programmer fra enheter.
10. Håndter personopplysninger og organisasjonsdata med forsiktighet til enhver tid.

Interne driftsregler for digital sikkerhet

Hver sivilsamfunnsorganisasjon bør vedta et enkelt internt dokument som definerer regler for digital sikkerhet for ansatte, frivillige og besøkende. Dette dokumentet bør som et minimum inneholde følgende regler:

- ☐ Bruk unike passord for hver konto.
- ☐ Ikke dele passord via chat-applikasjoner eller e-post.
- ☐ Aktiver tofaktorautentisering for e-post-, skylagrings- og administratorkontoer på sosiale medier.
- ☐ Bruk en passordbehandler der det er mulig.
- ☐ Lås alle enheter med PIN-koder, passord eller biometrisk beskyttelse.
- ☐ Aktiver automatiske system- og programoppdateringer.

- ☐ Rapporter tapte eller stjålne enheter umiddelbart.
- ☐ Verifisere alle forespørsler om endring av bank og betaling via en sekundær kanal.
- ☐ Bruke mobile hotspot-er når du arbeider utenfor CSO-lokaler.
- ☐ Tildele tilgang til sosiale medier kun via plattformrollfunksjoner.
- ☐ Begrense antallet administratorer til et minimum.
- ☐ Bare innhent og lagre nødvendige personopplysninger.
- ☐ Rapporter eventuelle sikkerhetshendelser umiddelbart til den utpekte ansvarlige personen.

Plan for håndtering av hendelser for sivilsamfunnsorganisasjoner i Nord-Makedonia

Når en digital sikkerhetshendelse inntreffer eller mistenkes, bør følgende tiltak iverksettes i rekkefølge:

1. Koble den berørte enheten fra nettverket.
2. Bevar bevis knyttet til hendelsen (skjermbilder, logger, meldinger).
3. Informer det interne teamet og den utpekte ansvarlige personen.
4. Sikre e-postkontoen først ved å endre passord og aktivere tofaktorautentisering.
5. Tilbakestill passordene for alle berørte kontoer.
6. Logg ut ukjente eller mistenkelige aktive økter.
7. Fjern ukjente administratorer og tilkoblede applikasjoner.
8. Rapporter hendelser til **MKD-CIRT**.
9. Rapporter mistanke om nettkriminalitet til politiets nettkriminalitetsenheter.
10. Rådføre seg med **Datatilsynet** ved mistanke om personopplysningsbrudd.
11. Vurdere hendelsens innvirkning.
12. Gjenopprett systemer og data fra sikkerhetskopier der det er mulig.
13. Oppdater enheter og programvare.
14. Gi personalet og de frivillige opplæring på nytt om nødvendig.
15. Oppdatere interne retningslinjer og sjekklister basert på erfaringer.

VEDLEGG 2: Sjekkliste for grunnleggende digital sikkerhet

Aktivitet/tiltak	Avkrysset (J/N)
2FA aktivert for alle nettbaserte kanaler	
Unike passord brukes til ulike kontoer	
Passord deles ikke i digital form	
Skjermlås er aktivert på alle enheter	
Automatiske oppdateringer er slått på	
Antivirus aktivert og oppdatert	
Personalets Wi-Fi er atskilt fra gjestenes	
Sikkerhetskopiering av data aktivert	
Ulike sideroller på sosiale medier	
Gjenopprettings-e-post/-telefon tilhører CSO-en	
Bruk av hotspot for Wi-Fi på administratorenheter på offentlige steder	
Alle enheter lukkes og kobles fra etter arbeidstid	

VEDLEGG 3: Sjekkliste for hendelsesrapportering

Aktivitet/tiltak	**Avkrysset (Ja/Nei)**
Berørte enheter koblet fra internett	
Bevis fra angrepet er innhentet	
Passord til e-post og andre sosiale medier endret	
Berørte data identifisert	
Ukjente administratorer/apper fjernet	
2FA aktivert	
Det interne teamet ble informert om hva som skjedde	
Bank- og betalingsopplysninger er deaktivert på enheten	
Den ansvarlige myndigheten/institusjonen ble informert om angrepet	

Rettslige og regulatoriske rammer i Norge og forslag til organisasjoner i sivilsamfunnet i Norge

Rettslige og regulatoriske rammer i Norge

Civilsamfunnsorganisasjoner (CSO-er) som opererer i Norge, er underlagt EUs personvernforordning (GDPR) og den norske personopplysningsloven, som inkorporerer og supplerer GDPR i norsk lovgivning. Disse rettslige rammeverkene gjelder for alle organisasjoner som behandler personopplysninger, inkludert ideelle og frivillighetsbaserte organisasjoner, uavhengig av størrelse. Vedkommende tilsynsmyndighet er Datatilsynet.

Norske sivilsamfunnsorganisasjoner behandler ofte personopplysninger knyttet til mottakere, medlemmer, frivillige, givere, ansatte og i mange tilfeller sårbare grupper. Slike opplysninger kan omfatte navn, kontaktopplysninger, økonomisk informasjon, helserelaterte opplysninger, saksdokumentasjon eller sensitive bakgrunnsopplysninger. Som behandlingsansvarlige er sivilsamfunnsorganisasjoner pålagt å overholde de grunnleggende prinsippene i personvernlovgivningen.

Viktige juridiske forpliktelser omfatter:

Rettslig grunnlag for behandling: Alle personopplysninger må behandles på et gyldig rettslig grunnlag, for eksempel samtykke, legitim interesse, kontraktsmessig nødvendighet eller juridisk forpliktelse.

Informert samtykke (der det er aktuelt): Samtykket må gis frivillig, være spesifikt, informert og kunne tilbakekalles.

Åpenhet: Enkeltpersoner må informeres om hvordan personopplysningene deres innhentes, brukes, lagres, deles og oppbevares gjennom tydelige personvernserklæringer.

Dataminimering og formålsbegrensning: Kun data som er strengt nødvendige for definerte formål, kan innhentes og oppbevares.

Sikkerhet ved behandling: Sivilsamfunnsorganisasjoner må iverksette egnede tekniske og organisatoriske tiltak for å beskytte personopplysninger mot uautorisert tilgang, tap eller misbruk.

Oppbevaring og sletting av opplysninger: Personopplysninger må ikke oppbevares lenger enn nødvendig; oppbevaringsperioder og sletterutiner må defineres.

Behandlingsadministrasjon: Det må opprettholdes skriftlige databehandlingsavtaler med alle eksterne tjenesteleverandører som håndterer personopplysninger.

Internasjonale dataoverføringer: Personopplysninger bør fortrinnsvis lagres innenfor EU/EØS. Overføringer til tredjeland krever gyldige sikkerhetstiltak, som standard kontraktsklausuler (SCC-er) og supplerende tiltak.

Melding om databrudd: Personopplysningsbrudd må vurderes umiddelbart og, der det er påkrevd, rapporteres til Datatilsynet innen 72 timer.

Datatilsynet har gjentatte ganger identifisert vanlige utfordringer blant norske sivilsamfunnsorganisasjoner, herunder uklare samtykkerutiner, usikker skylagring utenfor EU/EØS, mangel på dokumenterte interne prosedyrer og overdreven datalagring.

Etisk ansvar ved personvern

Utover juridiske forpliktelser har norske sivilsamfunnsorganisasjoner en etisk plikt til å beskytte personvernet, verdigheten og sikkerheten til personene de behandler opplysninger om. Mange sivilsamfunnsorganisasjoner jobber med personer i sårbare situasjoner – for eksempel flyktninger, barn, voldsofre eller politisk utsatte personer – der dataeksponering kan føre til alvorlig personlig skade.

Personvernbrudd kan føre til:

- Skade på mottakere og frivillige,
- Tap av tillit fra givere, partnere og allmennheten,
- Juridiske konsekvenser og økonomiske sanksjoner,
- Omdømmeskade og driftsforstyrrelser.

Etisk datahåndtering krever derfor en forsiktig tilnærming: Innhenting av minst mulig nødvendige data, effektiv beskyttelse av dem og deling av dem kun når det er strengt nødvendig.

Innarbeiding av samsvar i den daglige praksisen

For mange norske sivilsamfunnsorganisasjoner, særlig de som er avhengige av frivillige og har begrenset IT-kapasitet, må samsvar være praktisk og bærekraftig.

Effektiv implementering omfatter:

- Utpeke en person som er ansvarlig for personvern og digital sikkerhet, selv om det er på deltid eller kombinert med en annen rolle.
- Utvikle korte og tilgjengelige interne dokumenter, for eksempel en personvernpolicy og retningslinjer for datahåndtering.
- Implementere rutiner for tilgangskontroll, inkludert individuelle brukerkontoer, rollebasert tilgang og rettidig fjerning av inaktive brukere.
- Valg av sikre lagringsløsninger, helst EU/EØS-baserte skytjenester for personopplysninger.
- Sikre at det er inngått databehandlingsavtaler med alle eksterne leverandører.
- Tilby regelmessig bevissthetsopplæring for ansatte og frivillige om phishing, passord og sikker datahåndtering.
- Opprettholde en enkel hendelsesresponsrutine som omfatter identifikasjon, inndemming, dokumentasjon og eskalering.
- Innlemmelse av disse rutinene i den daglige driften bidrar til å sikre at samsvar er kontinuerlig og ikke reaktivt.

Casestudier fra Norge

Casestudie 1: Målrettet phishing under en innsamlingskampanje (Oslo, 2023)

I 2023 opplevde en liten humanitær sivilsamfunnsorganisasjon med base i Oslo en målrettet phishing-kampanje under den årlige innsamlingsaksjonen. Angriperne opprettet en falsk versjon av sivilsamfunnsorganisasjonens donasjonsside og sendte e-poster til støttespillere der de hevdet at organisasjonen hadde «oppdatert betalingssystemet sitt». Flere givere oppga kortopplysningene sine før sivilsamfunnsorganisasjonen ble klar over svindelen. Hendelsen skadet givernes tillit, og det krevdes betydelig tid og innsats for å løse problemer med banker og berørte støttespillere.

En grunnleggende kombinasjon av sikkerhetstiltak – for eksempel tofaktorautentisering på e-postkontoer, domenetilsyn og opplæring av personalet i phishing-røde flagg – kunne ha redusert virkningen av hendelsen eller forhindret angrepet helt.

Diskusjonsspørsmål:

- Hva var de viktigste sårbarhetene som ble utnyttet i denne hendelsen?
- Hvilke faresignaler kunne ha indikert at e-postene og donasjonssiden var falske?
- Hvilke grunnleggende digitale sikkerhetstiltak kunne ha forhindret eller begrenset skaden?

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 1 – Grunnleggende om cybersikkerhet:**
  Brukes som et grunnleggende eksempel på phishing og utnyttelse av tillit rettet mot givere og støttespillere.
- **Modul 4 – Vanlige cybertrusler (phishing og sosial manipulering):**
  Demonstrerer avanserte phishing-teknikker, inkludert falske nettsteder og etterligning.
- **Modul 6 – Sikkerhet på sosiale medier og på nettet:**
  Kan refereres til når man drøfter organisasjonens omdømme, tillit i offentligheten og sikre praksiser for pengeinnsamling på nettet.

- **Modul 7 – Utvikling av en sikkerhetskultur:**
  Støtter diskusjon om medarbeidernes bevissthet, kommunikasjonsprotokoller for givere og forebyggende opplæring.

Foreslått bruk:

Saksanalyse etterfulgt av en gruppeøvelse i å identifisere phishing-røde flagg i innsamlingskommunikasjon og utforme en sjekkliste for sikker giverkommunikasjon.

Casestudie 2: Skade på nettsted på grunn av en utdatert programtillegg (Bergen, 2022)

I 2022 fikk en liten menneskerettighetsorganisasjon med base i Bergen WordPress-nettstedet sitt ødelagt etter at angripere utnyttet et utdatert programtillegg. Startsiden ble erstattet med politisk propaganda, og organisasjonen mistet tilgangen til administratorpanelet. Ettersom sivilsamfunnsorganisasjonen ikke hadde noen nylige sikkerhetskopier av nettstedet, tok det mer enn to uker å gjenopprette nettstedet, og det krevde ekstern teknisk assistanse. Hendelsen forstyrret kommunikasjonen med frivillige og givere og forårsaket bekymringer for omdømmet.

Rutinemessige programvareoppdateringer, sterke administratorpassord, tofaktorautentisering og automatiske sikkerhetskopier ville ha redusert virkningen av angrepet betydelig**.**

Diskusjonsspørsmål:

- Hvilke tekniske og organisatoriske svakheter bidro til denne hendelsen?
- Hvordan påvirket mangelen på sikkerhetskopier organisasjonens evne til å gjenopprette seg?
  - Hvilke forebyggende tiltak som er omtalt i modulens hovedemner, kan bidra til å unngå lignende hendelser i fremtiden?

Praktiske sjekklister for digital sikkerhet og databeskyttelse for organisasjoner i det sivile samfunn i Norge

Relevant(e) modul(er) og bruk i læreplanen

- **Modul 3 – Enhets- og infrastruktursikkerhet:**
  Hovedsak illustrerer risikoer knyttet til utdatert programvare og usikker nettstedsinfrastruktur.
- **Modul 5 – Overholdelse av databeskyttelse og personvern:**
  Fremhever viktigheten av datatilgjengelighet, -integritet og -sikkerhetskopier for organisasjonens kontinuitet.
- **Modul 6 – Sikkerhet på sosiale medier og på nettet:**
  Relevant for diskusjoner om nettstedsintegritet, omdømmehåndtering og innholdskontroll.
- **Modul 7 – Utvikling av en sikkerhetskultur:**
  Støtter bevissthet om felles ansvar for oppdateringer og vedlikehold, ikke bare «IT-oppgaver».

Foreslått bruk:

Scenariebasert diskusjon etterfulgt av en praktisk sjekklisteøvelse om nettstedsvedlikehold, oppdateringsrutiner og sikkerhetskopiplanlegging.

VEDLEGG 1: Sjekkliste for overholdelse av lovgivning og GDPR for organisasjoner i sivilsamfunnet i Norge

☐ Alle personopplysninger som behandles av organisasjonen, er identifisert og dokumentert.

☐ Et lovlig grunnlag for hver behandlingsaktivitet er definert og registrert.

☐ En personvernerklæring/personvernpolicy er tilgjengelig og formidles.

☐ Samtykkemekanismene er tydelige og kan tilbakekalles ved behov.

☐ Oppbevaringsperioder for personopplysninger er definert og anvendt.

☐ Det foreligger databehandlingsavtaler med alle eksterne tjenesteleverandører.

☐ Personopplysninger lagres innenfor EU/EØS eller beskyttes av gyldige sikkerhetstiltak.

☐ Det finnes en rutine for varsling om datainnbrudd, og 72-timersregelen er kjent.

VEDLEGG 2. Grunnleggende sjekkliste for digital sikkerhet

☐ Det brukes sterke, unike passord til alle organisasjonskontoer.

☐ En passordbehandler er i bruk.

☐ Tofaktorautentisering er aktivert på e-post-, sky- og sosiale mediekontoer.

☐ Enheter er beskyttet med skjermlåser og sterke PIN-koder/passord.

☐ Operativsystemer og programmer oppdateres automatisk.

☐ Antivirus-/anti-skadevareprogramvare er installert og oppdatert.

☐ Det tas sikkerhetskopi av kritiske data regelmessig og på en sikker måte.

VEDLEGG – 3. Sjekkliste for sky- og kontoadministrasjon

☐ Individuelle brukerkontoer brukes; delte påloginger unngås.

☐ Tilgangsrettigheter er rollebaserte og begrenset til det som er nødvendig.

☐ Inaktive kontoer fjernes umiddelbart.

☐ Tilgangstillatelser til skyen gjennomgås med jevne mellomrom.

☐ Sensitive filer deles med restriksjoner og utløpsfrister.

☐ Aktivitetslogger er aktivert der de er tilgjengelige.

VEDLEGG 4. Sjekkliste for sosiale medier og tilstedeværelse på nettet

☐ Tofaktorautentisering er aktivert på alle sosiale mediekontoer.

☐ Administratorroller tildeles individuelt.

☐ E-postadresser og telefonnumre for gjenoppretting er oppdaterte.

☐ Administratorlister gjennomgås regelmessig.

☐ Det finnes en beredskapsplan for kontokapring eller etterligning.

☐ Nettstedets innholdsstyringssystem og programtillegg oppdateres regelmessig.

VEDLEGG 5. Sjekkliste for hendelsesrespons og -rapportering

☐ Det er utpekt en sikkerhetsansvarlig person.

☐ Personalet vet hvordan de skal rapportere mistenkte hendelser internt.

☐ Det finnes en skriftlig prosedyre for hendelsesrespons.

☐ Bevis og logger oppbevares etter hendelser.

☐ Alvorlige cyberhendelser rapporteres til NorCERT når det er hensiktsmessig.

☐ Personopplysningsbrudd rapporteres til Datatilsynet når det er nødvendig.

☐ Erfaringer dokumenteres, og prosedyrer oppdateres.

VEDLEGG 6. Sjekkliste for bevissthet hos ansatte og frivillige

☐ Nye ansatte og frivillige får opplæring i sikkerhet og personvern.

☐ Retningslinjer for akseptabel bruk og databeskyttelse erkjennes.

☐ Det tilbys jevnlig oppfriskningsopplæring.

☐ Det finnes klare regler for bruk av personlige enheter til sivilsamfunnsorganisasjonens arbeid.

☐ Sensitive data deles ikke via usikre kanaler.

Forslag og praktiske anbefalinger

Norske sivilsamfunnsorganisasjoner bør prioritere enkle, veldokumenterte rutiner fremfor komplekse tekniske løsninger. Ved å kombinere tydelige interne retningslinjer, grunnleggende tekniske sikkerhetstiltak, jevnlig opplæring og etisk bevissthet, kan organisasjoner redusere de digitale risikoene sine betydelig, samtidig som de overholder GDPR og norsk lovgivning.

Ytterligere Norge-spesifikke punkter civilsamfunnsorganisasjoner bør være oppmerksomme på

1. Frivilligomsättning og håndtering av tilgangslivssyklus

Norske sivilsamfunnsorganisasjoner er i stor grad avhengige på korttidsfrivillige, praktikanter og deltidsansatte. En av de vanligste risikoene Datatilsynet og NSM rapporterer om, er unnlatelse av å inndra tilgang når personer forlater organisasjonen.

Dette bør organisasjoner i sivilsamfunnet vite:

- Hver onboarding må ha en tilhørende sjekkliste for offboarding.
- Kontoer, e-posttilgang, skymapper og roller på sosiale medier må fjernes umiddelbart.
- Delte kontoer øker risikoen dramatisk i frivillighetsbaserte organisasjoner,
- Dette punktet forsterker modul 7 (Sikkerhetskultur og -policyer).

2. Personnummer og sensitive identifikatorer

Noen norske sivilsamfunnsorganisasjoner behandler fødselsnummer, helsedata, asylrelatert informasjon eller opplysninger om rettssaker.

Hvorfor dette er viktig:

- Disse datatypene krever høyere beskyttelsesstandarder i henhold til GDPR.
- Lagring i usikrede regneark eller generelle skymapper er en praksis med høy risiko.
- Kryptering og streng tilgangskontroll er avgjørende.
- Dette passer naturlig inn under modul 5 (Databeskyttelse og personvern), men kan kryssrefereres til opplæringen i modul 7.

3. Bevissthet om skytjenester og Schrems II

Mange norske sivilsamfunnsorganisasjoner bruker globale skytjenester (Google, Microsoft, Dropbox) uten å forstå konsekvensene av dataoverføring.

Norsk spesifikk virkelighet:

- Datatilsynet forventer at organisasjoner i sivilsamfunnet er klar over at personopplysninger må oppbevares i EU/EØS.
- Overføringer utenfor EU/EØS krever sikkerhetstiltak (standard kontraktsklausuler + risikovurdering).
- «Vi bruker en stor leverandør» er ikke en tilstrekkelig begrunnelse.
- Dette styrker modul 8 (Avanserte emner) med et juridisk-teknisk perspektiv.

4. Koordinering mellom NorCERT og Datatilsynet

Civilsamfunnsorganisasjoner er ofte usikre på hvem de skal rapportere hva til.

Tydelig skille CSO-er bør kjenne til:

- NorCERT (NSM): Alvorlige cybersikkerhetshendelser (ransomware, kontoovertakelse, tjenesteavbrudd).
- Datatilsynet: Personopplysningsbrudd (GDPR – innen 72 timer),
- Noen hendelser krever varsling til begge,
- Dette er et viktig tillegg til modul 7 (Hendelsesrespons og -rapportering).

5. Psykologisk trygghet og «ingen skyld»-rapporteringskultur

Norsk organisasjonskultur verdsetter sterkt tillit og flate hierarkier – men dette kan slå tilbake hvis personalet frykter å bli satt i forlegenhet.

Beste praksis:

- Ansatte bør oppfordres til å rapportere feil (klikket på phishing-lenke, mistet enhet) umiddelbart.
- En kultur uten skyldfølelse reduserer skader og forbedrer responstiden.
- Dette er et viktig kulturelt lag for modul 7 som går utover tekniske kontroller.

6. Styrets ansvar og tilsyn med ledelse

I Norge forventes det i økende grad at styret i sivilsamfunnsorganisasjoner forstår digital risiko som en del av god ledelse.

Dette bør styret vite:

- Cybersikkerhet og databeskyttelse er ledelsesspørsmål, ikke bare IT-spørsmål
- Styret bør godkjenne grunnleggende sikkerhetspolicyer og planer for hendelsesrespons

- Alvorlige hendelser kan få juridiske og omdømmemessige konsekvenser for ledelsen
- Dette kan legges til som et styringsnotat under modul 7 eller modul 8.

7. Sivilsamfunnet som strategisk mål

Norske organisasjoner i sivilsamfunnet som arbeider med demokrati, menneskerettigheter, utenrikspolitikk eller internasjonal bistand, anses som strategiske mål, ikke tilfeldige ofre.

Konsekvenser:

- Angrepene kan være vedvarende, subtile og etterretningsdrevne
- Ikke alle trusler er rettet mot penger – noen er rettet mot overvåking eller forstyrrelser
- Kunnskap om NSM-trusselorienteringer er avgjørende
- Dette forsterker modul 1 og modul 8 med en Norge-spesifikk trusselsmodell.

VEDLEGG

Vedlegg 1: Ordliste over nøkkelbegreper

- ***Antivirus (AV):*** *Programvare som oppdager og fjerner skadevare (virus, trojanere osv.) fra datamaskiner. Eksempel: Windows Defender eller Avast.*
- ***Sikkerhetskopi:*** *En ekstra kopi av data som lagres separat for gjenopprettingsformål, f.eks. lagring av filer på en ekstern harddisk eller en skytjeneste, slik at de kan gjenopprettes dersom originalene går tapt.*
- ***Brute-force-angrep:*** *En metode der angripere prøver mange passord eller nøkler til de finner det riktige. Sterke passord og utlåsingspolicyer bidrar til å beskytte mot dette.*
- ***Datainnbrudd:*** *En hendelse der sensitive opplysninger gjøres tilgjengelige eller utleveres uten tillatelse. Kan oppstå via hacking, tapte enheter osv.*
- ***Kryptering:*** *Prosessen med å konvertere data til et kodet format som er uleselig uten en nøkkel. Beskytter informasjonens konfidensialitet (f.eks. krypterer HTTPS nettrafikk).*
- ***Brannmur:*** *En nettverkssikkerhetsenhet eller programvare som overvåker og filtrerer innkommende og utgående nettverkstrafikk basert på sikkerhetsregler. Den kan blokkere uautorisert tilgang, samtidig som den tillater legitim kommunikasjon.*
- ***Skadevare:*** *Skadelig programvare utformet for å skade eller utnytte systemer. Omfatter virus, løsepengevirus, spionprogrammer osv. Leveres ofte via e-postvedlegg eller skadelige nettsteder.*
- ***Flerfaktorautentisering (MFA/2FA):*** *Bruk av mer enn én verifiseringsmetode for å logge på (f.eks. passord + engangskode på telefonen). Forbedrer kontosikkerheten dramatisk.*
- ***Phishing:*** *Et svindelforsøk (vanligvis via e-post) for å lure personer til å avsløre sensitive opplysninger eller installere skadevare ved å utgi seg for å være en pålitelig enhet. Spydphishing refererer til målrettede forsøk mot bestemte personer eller organisasjoner.*

- ***Løsepengevirus:*** *Skadevare som krypterer et offers data og krever betaling for dekrypteringsnøkkelen. Hvis det ikke finnes sikkerhetskopier, utsettes ofrene for press om å betale hackere for å få tilgang igjen.*
- ***Sosial manipulering:*** *Taktikker som manipulerer folk til å avsløre konfidensiell informasjon eller utføre handlinger som kompromitterer sikkerheten. Phishing er én form; andre former omfatter pretexting eller baiting. Det utnytter menneskelig tillit og nysgjerrighet.*
- ***VPN (virtuelt privat nettverk):*** *Et verktøy som oppretter en kryptert tunnel over internett fra enheten din til en server, og som beskytter data under overføring og skjuler IP-adressen din. Nyttig på offentlige Wi-Fi-nettverk for en sikker tilkobling.*
- ***Sårbarhet:*** *En svakhet i programvare, maskinvare eller prosedyrer som angripere kan utnytte for å få uautorisert tilgang eller utføre uautoriserte handlinger. Oppdateringer utbedrer kjente sårbarheter.*
- ***Wifi-kryptering (WPA2/WPA3):*** *Sikkerhetsprotokoller for trådløse nettverk som krypterer trafikk mellom enheter og ruteren. Sørg for at Wi-Fi-nettverket ditt bruker minst WPA2 med en sterk passfrase for å forhindre avlytting.*

Vedlegg II: Mal for passordpolicy (eksempel)

Formål: Å fastsette krav til opprettelse, bruk og håndtering av passord for å beskytte organisasjonens informasjonssystemer.

Omfang: Denne policyen gjelder for alle ansatte, frivillige og kontraktører i [organisasjonsnavn] som bruker IT-systemer (inkludert datamaskiner, e-post, applikasjoner og nettsteder) til organisasjonsarbeid.

Retningslinjeerklæringer:

- *Alle brukerpassord må bestå av minst 12 tegn og kombinere store og små bokstaver, tall og spesialsymboler.*
- *Standardpassord må endres umiddelbart ved første bruk.*

- *Passord må ikke deles mellom personer eller skrives ned på usikre steder.*
- *Tofaktorautentisering (2FA) er påkrevd for all ekstern tilgang til organisasjonens systemer og for e-postkontoer.*
- *Passord for kritiske systemer (økonomi, giverdatabaser) må endres hver 90. dag.*
- *Brukere må ikke gjenbruke passord som har blitt brukt på andre (offentlige) kontoer eller lekket i datainnbrudd.*
- *Dersom det er mistanke om at et passord er kompromittert, må det endres umiddelbart, og IT-/sikkerhetsansvarlig må varsles.*

Roller og ansvarsområder:

- *Brukere må følge disse reglene og rapportere enhver mistanke om kompromittering.*
- *IT-ansatte skal håndheve passordreglene gjennom tekniske kontroller (f.eks. passordbehandlere, kontolåsing etter mislykkede forsøk).*
- *Sikkerhetsansvarlig skal gjennomgå overholdelsen og oppdatere policyen årlig.*

Håndhevelse: Brudd på denne policyen kan føre til tilbakekalling av tilgangsrettigheter eller andre disiplinærtiltak.

Vedlegg III: Mal for sikkerhetskopieringspolicy (eksempel)

Formål: Å sikre at det regelmessig tas sikkerhetskopi av kritiske data og at de kan gjenopprettes i tilfelle tap, skade eller katastrofe.

Omfang: Gjelder for alle data som er lagret på organisasjonens servere, arbeidsstasjoner og nettverkslagringsenheter hos [organisasjonsnavn].

Retningslinjeerklæringer:

- *Kritiske data (giveroppføringer, økonomifiler, prosjektdatabaser osv.) må sikkerhetskopieres minst én gang daglig.*
- *Sikkerhetskopier bør omfatte systemkonfigurasjoner og programmer som er nødvendige for å gjenopprette driften.*
- *Sikkerhetskopier må lagres sikkert eksternt eller i en separat skylagring for å forhindre tap som følge av lokale hendelser.*
- *Fullstendige sikkerhetskopier utføres ukentlig, med inkrementelle sikkerhetskopier daglig (eller oftere for svært sensitive data).*
- *Kontroller av sikkerhetskopienes integritet og testgjenopprettinger må utføres månedlig for å sikre at data kan gjenopprettes.*
- *Oppbevaring: Oppbevar minst én hel uke med daglige sikkerhetskopier på stedet, og en månedlig fullstendig sikkerhetskopi arkivert eksternt i minst ett år.*
- *Tilgang til sikkerhetskopierte data er begrenset til autorisert IT- eller ledelsespersonell.*

Roller og ansvarsområder:

- *IT-personalet må konfigurere og overvåke automatiserte sikkerhetskopier i henhold til denne tidsplanen.*
- *Den utpekte sikkerhetskopiadministratoren skal dokumentere sikkerhetskopieringsprosedyrer og verifisere at sikkerhetskopieringen er fullført og at den er intakt.*
- *Alt personale er ansvarlig for å lagre kritiske arbeidsfiler på de angitte stedene som er inkludert i sikkerhetskopieringsplanen.*

Håndhevelse: Unnlatelse av å overholde dette kan føre til tap av data og vil bli håndtert av ledelsen i [Organisasjonsnavn] deretter.

Vedlegg IV: Mal for ressursinventar (eksempel)

Ressurs-ID	Ressursnavn	Kategori	Eier/avdeling	Sted	Sensitivitetsnivå	Beskyttelse påkrevd	Merknader
A001	Giverdatabase	Programvare/data	Programdirektør	På stedet	Høy	Kryptert, passordbeskyttet	Inneholder givernes PII
A002	Økonomiserver	Maskinvare/server	IT-avdeling	Datasenter	Høy	Regelmessige sikkerhetskopier, 2FA for tilgang	Støtter regnskapsprogramvare
A003	Bærbare datamaskiner	Maskinvare/enhet	Diverse ansatte	Kontor/felt	Middels	Påtvunget diskkryptering, passord	Hver enhet har en ID-tagg
A004	Nettsted	Programvare	Kommunikasjon	Skybasert	Medium	HTTPS-aktivert, oppdatert CMS	Offentlig nettsted
A005	CRM-programvare	Programvare	Databehandler	Sky	Høy	Rollebasert tilgang, daglige sikkerhetskopier	Sporer mottakerinformasjon

(Merk: «Sensitivitetsnivå» kan være lavt/middels/høyt. «Beskyttelse påkrevd» skisserer sikkerhetstiltak for hver ressurs.)

Vedlegg V: Enkel risikomatrisemal (eksempel)

	Konsekvens: Lav (1)	**Konsekvens: Middels (2)**	**Konsekvens: Høy (3)**
Sannsynlighet: Høy (3)	Høy risiko (3×1)	Kritisk risiko (3 × 2)	Kritisk risiko (3 × 3)
Sannsynlighet: Middels (2)	Middels risiko (2 × 1)	Høy risiko (2 × 2)	Kritisk risiko (2 × 3)
Sannsynlighet: Lav (1)	Lav risiko (1×1)	Middels risiko (1×2)	Høy risiko (1×3)

- **Risikonivåer:** Beregn risikoen ved å multiplisere sannsynlighets- og konsekvenspoengsummene. For eksempel gir et scenario med sannsynlighet = 3 (høy) og innvirkning = 2 (middels) en risikoscore på 6 (kritisk risiko).
- Bruk denne matrisen til å prioritere håndtering av scenarier med høyere risiko først (kritisk > høy > middels > lav).

KONKLUSJON

Digital sikkerhet er ikke et engangsprosjekt eller en boks som skal krysses av – det er en vedvarende forpliktelse for organisasjoner i det sivile samfunnet. Når vi avslutter denne e-boken, ønsker vi å bekrefte en sentral lærdom som har gjentatt seg gjennom hvert kapittel: Å holde sivilsamfunnsorganisasjonene våre trygge på nettet krever kontinuerlig oppmerksomhet, tilpasning og omsorg. Cybertrussellandskapet vi omtalte i begynnelsen, er i stadig utvikling, og angripere søker daglig etter nye måter å bryte gjennom forsvaret på. Det vi sikrer i dag, kan bli utfordret av nye taktikker i morgen.

Denne realiteten innebærer at digital sikkerhet må forbli på radaren vår på lang sikt, like integrert i planleggingen og driften vår som budsjettering eller programadministrasjon. Vi har ikke råd til å behandle cybersikkerhet som en ettertanke – den bør heller bli en naturlig del av måten vi jobber på. Innsatsen er ganske enkelt for høy – når ett enkelt vellykket hack kan avsløre sensitive mottakerdata eller spolere en påvirkningskampanje, er årvåkenhet innen digital sikkerhet en integrert del av å oppfylle oppdragene våre. Kunnskapen og strategiene du har tilegnet deg fra denne e-boken, er et grunnlag å bygge videre på. Fremover vil det å holde seg trygg innebære å regelmessig gjennomgå disse emnene på nytt, oppdatere praksisen din etter hvert som nye trusler (og løsninger) dukker opp, og fremme et miljø der læring om sikkerhet er en kontinuerlig prosess. Kort sagt er arbeidet med digital sikkerhet aldri «ferdig», men det er heller ikke uoverkommelig. For hvert skritt du tar for å styrke organisasjonens cyberforsvar, bidrar du til et mer motstandsdyktig sivilsamfunn.

Enkelt å opprettholde sikkerheten: En viktig lærdom er at sikkerhet ikke trenger å være altfor komplisert. Ofte handler det om å gjøre de enkle tingene konsekvent. Bruk sterke, unike passord (og en passordadministrator). Hold programvaren oppdatert. Tenk deg om to ganger før du klikker på uventede lenker. Sikkerhetskopier dataene dine regelmessig. Når disse grunnleggende praksisene er forankret, håndterer de en stor andel av truslene. Som vi så, lykkes mange angrep på grunn av oversette grunnleggende ting – så ved å ta vare på disse, stenger du de vanlige dørene som angripere utnytter.

Tilpasning til nye utfordringer: Den digitale verdenen kommer til å fortsette å endre seg. For fem år siden var ikke løsepengevirus like dominerende – i dag er det en av de største

truslene. I fremtiden kan vi komme til å stå overfor angrep på verktøy for kunstig intelligens eller mer sofistikert deepfake-phishing. Sikkerhetssjefen din bør fortsette å tilpasse seg og lære. Abonner på en relevant sikkerhetsfeed eller bli med i et fellesskap der nye trusler diskuteres – på den måten får du tidlig varsel om nye problemer. Vurder periodisk oppfriskningsopplæring eller nye moduler for personalet når noe vesentlig endrer seg (hvis for eksempel skadevare for mobilenheter øker, bør du holde en spesiell økt om det). Ha en tankegang basert på kontinuerlig forbedring, og betrakt hver nestenulykke eller hendelse som en læringsmulighet for å styrke forsvaret ytterligere.

Fordel ressurser klokt: Sikkerhet er en investering i organisasjonens bærekraft. Det kan kreve et visst budsjett (for bedre utstyr, programvare eller opplæringstid) og oppmerksomhet fra ledelsen. Men som vist er kostnaden ved å ikke sikre seg (inndring, driftsstans, tapt tillit) langt høyere. Planlegg sikkerhet i den langsiktige strategien din – f.eks. ved å inkludere en post i tilskudd for teknologioppdateringer eller opplæring. Dra nytte av gratis tjenester eller tjenester til nedsatt pris for sivilsamfunnsorganisasjoner (det finnes mange, fra gratis Google Workspace til donerte brannmurer), som beskrevet i kapittel 6. Vurder også å utpeke en sikkerhetsansvarlig (selv om det ikke er på heltid) som holder oversikt over sikkerhetsoppgaver og -utviklinger – å ha noen ansvarlige sikrer at ingenting faller mellom stolene.

Støtte fra ledelsen: Bærekraftig sikkerhet krever støtte fra ledelsen. Når ledere prioriterer sikkerhet – ved å være et godt eksempel og tildele ressurser – sender det et klart budskap om at dette er viktig for alle. Det motvirker også eventuell motstand (som «Trenger vi virkelig å bry oss med dette?»): Hvis direktøren logger på med 2FA og deltar på de samme opplæringene, legitimerer det innsatsen. Sørg derfor for at ledergruppen din er helt med på bølgelengde og til og med kjemper for sikkerhetsinitiativer.

Engasjer hele teamet**:** En trygg fremtid avhenger av at alle spiller en rolle. Fra den nyeste praktikanten til styremedlemmene – hver person spiller en rolle i kjeden. Hold sikkerheten inkluderende: Oppmuntre til spørsmål, ikke skam ut feil, belønn årvåkenhet. Noen organisasjoner inkluderer en sikkerhetskompetanse i medarbeidervurderinger eller stillingsbeskrivelser, og understreker at dette er en forventning for alle roller. Ved å styrke de ansatte – gi dem kunnskap og verktøy – har du i hovedsak skapt en menneskelig brannmur

rundt sivilsamfunnsorganisasjonen din. Som et ordtak sier: «Brukernes sikkerhetsbevissthet er den billigste og mest effektive brannmuren du kan ha.»

Se fremover med optimisme: Det kan være lett å føle seg skremt av cybertrusler, men husk at kunnskap og forberedelse vipper vekten sterkt i din favør. Mange sivilsamfunnsorganisasjoner over hele verden, selv de med begrensede ressurser, har lykkes med å forsvare seg ved å være proaktive og samlede. Ved å lese denne e-boken og implementere veiledningen i den, har du tatt et viktig skritt mot å sikre organisasjonens digitale fremtid. Det er en reise – det kommer til å oppstå hindringer og muligens hendelser – men hvert skritt du tar nå reduserer virkningen av disse og fremskynder gjenopprettingen.

I en verden der sivilsamfunnet av og til er et spesifikt mål for cyberangrep, er engasjementet ditt for digital sikkerhet også et engasjement for saken din og menneskene du hjelper. Det betyr at det viktige arbeidet ditt kan fortsette uten å bli avsporet av forstyrrelser som kan forebygges. Det betyr at tilliten folk setter til deg – for å håndtere opplysningene deres eller forsterke stemmene deres – er velbegrunnet.

For å konkludere, la oss oppsummere noen langsiktige sikkerhetsvaner det er lurt å dyrke:

- *Gjennomgå risikovurderingen din regelmessig og oppdater sikkerhetsplanen din (minst én gang i året eller når det skjer store endringer).*
- *Fortsett å lære – delta på det nettmøtet, les den veiledningen, del innsikt med kolleger.*
- *Hold kontakten – ikke isoler sikkerhetsinnsatsen din. Vær en del av fellesskapet som lærer og forsvarer seg sammen.*
- *Vær forberedt – opprettholde hendelsesresponsplanen din og test den av og til, slik at den er klar ved behov.*
- *Vær årvåken – men ikke redd. Med god praksis på plass kan du være trygg og rolig, ikke engstelig, når det gjelder digitale trusler.*

Mot en trygg fremtid: Ved å gjøre digital sikkerhet til en integrert del av den daglige driften og kulturen i sivilsamfunnsorganisasjonen din, er du godt posisjonert til å møte fremtiden. Det vil utvilsomt dukke opp utfordringer, men du har verktøyene, kunnskapen og støtten som trengs

for å overvinne dem. Ved å gjøre dette beskytter du ikke bare organisasjonen din, men bidrar også til et tryggere digitalt miljø for det bredere sivilsamfunnet.
Fremover må du forplikte deg til kontinuerlig forbedring. Feir sikkerhetsseirene dine (selv de små, som «Ingen falt for phishing dette kvartalet!» eller «Vi gjenopprettet data fra sikkerhetskopien etter en mindre serverkrasj»). Lær av eventuelle tilbakeslag. Og husk alltid hvorfor: En sikker sivilsamfunnsorganisasjon kan bedre oppfylle oppdraget sitt og gjøre en positiv innsats uten avbrudd.

Å bygge motstandskraft er et annet tema vi har lagt vekt på, og det fortjener å bli understreket igjen her i konklusjonen. Motstandskraft betyr ikke bare å prøve å forhindre angrep, men også å sikre at organisasjonen din kan komme seg på beina igjen hvis noe går galt. Det handler om å ha sikkerhetskopier slik at et angrep med løsepengevirus ikke lammer driften, om å ha beredskapsplaner slik at en phishing-hendelse kan begrenses og man kan lære av den, og om å dyrke en organisasjonskultur som ser på tilbakeslag som muligheter til forbedring. Når du fortsetter med arbeidet ditt, må du huske at enhver utfordring kan gjøre deg sterkere hvis du møter den med forberedelse og refleksjon. Hvis det oppstår en sikkerhetshendelse, kan du bruke den som en læringsopplevelse til å finpusse retningslinjene og opplæringen. Feir fremgangen du har gjort – for eksempel ved å snu statistikken om at «80 % av organisasjonene ikke har en sikkerhetsplan» på hodet i din egen kontekst ved å iverksette en robust plan. Og fortsett å utdanne deg selv og teamet ditt. Området for digital sikkerhet utvikler seg raskt, men det finnes flere ressurser enn noensinne (mange av dem har vi oppført i kapittel 7 og vedleggene) for å holde deg oppdatert. Vurder periodiske oppfriskningsworkshoper, abonner på varsler eller nyhetsbrev om cybersikkerhet for ideelle organisasjoner, og oppmuntre yngre ansatte eller frivillige med IT-interesser til å påta seg roller som «digitale sikkerhetsforkjempere» i organisasjonen din. Fortsettende læring er hjørnesteinen i motstandskraft. Det holder deg smidig og klar til å møte alt den digitale verden sender din vei.

Når vi ser fremover, er vi fortsatt optimistiske og fremtidsrettede når det gjelder sivilsamfunnets fremtid i den digitale tidsalderen. Ja, utfordringene er betydelige – cyberangrep blir stadig mer sofistikerte, og vi må holde oss på tå hev. Men fremgangen som er gjort de siste årene, er oppmuntrende. Flere organisasjoner blir oppmerksomme på viktigheten av digital

sikkerhet, og støttestrukturene styrkes sakte, men sikkert. Vi ser en utvikling av verktøy og tjenester skreddersydd for ideelle organisasjoner, økt bevissthet blant givere og institusjoner om å finansiere cybersikkerhetsbehov, og større global oppmerksomhet rundt begrepet «digital motstandskraft» for lokalsamfunn. Hvert kapittel i denne e-boken har ikke bare gitt advarsler, men også fremhevet muligheter – muligheten til å utnytte teknologien til vår fordel, til å innovere måten vi beskytter oss selv på og til å forme et digitalt miljø som opprettholder verdiene våre. Som vi har påpekt, kommer cybertrusler til å fortsette å utvikle seg, men det kan også forsvaret vårt. Ved å bygge bro over gjenværende hull i kunnskap og kapasitet, ved å styrke partnerskap og ved å holde cybersikkerhet som en prioritet for dem som trenger det mest, kan vi skape et tryggere digitalt økosystem der sivilsamfunnet kan fortsette sitt kritiske arbeid uten frykt.

Avslutningsvis ønsker vi å gi deg en oppmuntrende tanke: Hver eneste innsats du investerer i digital sikkerhet er en investering i friheten og integriteten til arbeidet ditt og menneskene du hjelper. Hver nye passordpolicy, hver krypterte database, hver opplæringsøkt for ansatte – alt sammen bidrar til et sterkere skjold som beskytter menneskerettigheter, sosial rettferdighet og initiativer for samfunnsvelferd over hele verden. Det faktum at du har lest denne e-boken og engasjert deg i disse temaene, er et positivt skritt mot en tryggere fremtid. Vi oppfordrer deg til å videreføre denne forpliktelsen. Del det du har lært med kolleger og partnerorganisasjoner. Hold samtalen om digital sikkerhet i live på strategimøter og planleggingsøkter. Kjemp for ressursene og støtten dere trenger – enten det er finansiering av bedre infrastruktur eller ganske enkelt tid avsatt til at ansatte kan lære om og iverksette sikkerhetstiltak – fordi digital sikkerhet er verdt det. Det fremtidsrettede synspunktet er at ved å integrere sikkerhet i det daglige arbeidet vårt, gjør vi mer enn bare å beskytte organisasjonene våre – vi gjør dem i stand til å blomstre. En sikker sivilsamfunnsorganisasjon kan tale høyere, handle dristigere og nå lenger, vel vitende om at stemmen ikke lett kan bringes til taushet av digitale trusler.

En av de mest oppmuntrende innsiktene fra KA220-prosjektet og denne e-boken er at vi ikke er alene om å møte disse utfordringene. Faktisk er samarbeid en av våre sterkeste ressurser. Hvis det er ett budskap vi skal videreføre, er det at vi er tryggere sammen.

Cybertrusler kan ofte føles isolerende – en liten ideell organisasjon kan føle seg underlegen overfor en sofistikert hacker – men sivilsamfunnets kollektive kraft, når det arbeider sammen, kan snu balansen. Gjennom hele dette prosjektet har vi blitt inspirert av eksempler på organisasjoner som slår seg sammen for å dele ekspertise, av nettverk av digitale frivillige som gir en hjelpende hånd, og av partnerskap som har dannet seg på tvers av landegrenser for å takle felles sikkerhetsproblemer. Veien til digital sikkerhet er ikke en ensom vei – det er en felles reise. Ved å kommunisere åpent om trusler og hendelser, ved å dele verktøy og suksesshistorier, og ved å støtte hverandre i nødssituasjoner, forsterker organisasjoner i sivilsamfunnet sin forsvarskapasitet. Videre er et bredt samarbeid utover den ideelle sektoren avgjørende. Vi må fortsette å knytte partnerskap med allierte i myndigheter, akademia og teknologibransjen som er opptatt av å beskytte det åpne og trygge internettet som sivilsamfunnet er avhengig av. Som eksperter og globale cyberledere har påpekt, krever effektivt forsvar av risikogrupper «investeringer i cybersikkerhetsløsninger, samarbeid mellom interessenter og innovative finansieringsmodeller for langsiktig motstandskraft». Ingen enkelt organisasjon – uansett hvor godt utstyrt den er – kan håndtere alle aspekter av digital sikkerhet alene. Det kreves et fellesskap av fagfolk fra ulike sektorer og med ulike kompetanser for å sikre at beskyttelsestiltak er tilgjengelige, effektive og bærekraftige på lang sikt. Jeg oppfordrer dere til å oppsøke slike samarbeid: Bli med i sikkerhetsfora og -koalisjoner, engasjer dere i initiativer som tilbyr cybersikkerhetshjelp til sivilsamfunnsorganisasjoner, og nøl ikke med å ta kontakt med kolleger for å be om hjelp eller tilby deres egen. Ved å styrke disse båndene skaper vi en samlet front som kan reagere raskt på trusler og forhindre at små problemer blir til store kriser. Takk for at du er en del av denne reisen for å utvikle infrastruktur for digital sikkerhet gjennom sivilsamfunnet. Konklusjonen i denne læreboken er ikke en slutt, men snarere en begynnelse – utgangspunktet for nye initiativer, samtaler og samarbeid som kommer til å fortsette utover disse sidene. Vær nysgjerrige, vær årvåkne og hold sammen. Sammen kommer vi til å skape et digitalt miljø der sivilsamfunnet ikke bare er trygt, men også i stand til å utnytte teknologi til å forsvare sakene vi bryr oss om. Med motstandskraft, samarbeid og kontinuerlig læring som veiledning beveger vi oss fremover mot en fremtid der organisasjoner som din trygt kan omfavne innovasjon og drive sosial endring, støttet av et solid fundament av digital sikkerhet.

La oss fortsette dette viktige arbeidet – fellesskapene våre stoler på det, og verktøyene og de allierte vi trenger er innen rekkevidde. Skål for et tryggere, sterkere og mer selvstendig sivilsamfunn i den digitale tidsalderen.

Practical Digital Transformation Guide and Curriculum on Strengthening Digital Security in Civil Society ble utarbeidet med ett klart formål: Å gjøre digital sikkerhet oppnåelig, forståelig og gjennomførbar for enhver organisasjon, uavhengig av størrelse eller teknisk kapasitet. Etter hvert som dere beveger dere fremover, håper vi at denne veiledningen ikke bare skal fungere som en ressurs, men også som en ledsager på reisen mot sterkere og tryggere digital praksis.

Digital motstandskraft vokser trinn for trinn, gjennom bevissthet, samarbeid og konsekvens. Ved å integrere disse praksisene i det daglige arbeidet ditt beskytter du ikke bare data og kommunikasjon, men forsvarer også menneskerettigheter, tillit og demokratiske verdier i den digitale tidsalderen.

Vær oppmerksom. Vær motstandsdyktig. Hold deg trygg.


SETA
BRUSSEL
SETA
TÜGVA
BRAVO
TtB
ANKA
Gelecek ve Yenilik Derneği
MACEDONIAN
HUMAN
RESOURCES
ASSOCIATION