PRIRUČNIK ZA DIGITALNU SIGURNOST

MEDIJSKIH REDAKCIJA I ORGANIZACIJA CIVILNOG DRUŠTVA

USAID FROM THE AMERICAN PEOPLE
Internews
MEDIACENTAR SARAJEVO

Priručnik za digitalnu sigurnost medijskih redakcija i organizacija civilnog društva

Priručnik za digitalnu sigurnost medijskih redakcija i organizacija civilnog društva

Autor: Predrag Puharić

Urednica: Maja Ćalović

Lektura: Azra Hodžić-Čavkić

Dizajn naslovne stranice: Sanja Vrzić

DTP: Hana Kevilj

Izdavač: Mediacentar Sarajevo

Godina izdanja: 2024.

Sadržaj

Uvod 5

- Značaj cyber sigurnosti za civilno društvo i medijske organizacije 5
- Opseg i ciljevi priručnika 5

Pregled uobičajenih prijetnji 8

Procjena rizika i planiranje 11

- Analiza trenutne digitalne infrastrukture 11
- Implementacija preporuka 12
- Kontinuirano praćenje i revizija 12

Kreiranje plana/strategije digitalne sigurnosti za organizaciju 13

- Analiza konteksta 13
- Određivanje modela prijetnje 14
- Planiranje sigurnosnih mjera 15

Preporučeni alati i prakse digitalne sigurnosti 19

- Sigurnost pristupa 19
- Sigurnost uređaja 20
- Sigurnost podataka 22
- Sigurno korištenje interneta 23
- Sigurnost web sajta 25
- Sigurna komunikacija 26

Fizička sigurnost i kontrola okolinskih faktora 31

Zaključak 33

Dodatni resursi 35

Annex 1: Politika digitalne sigurnosti 36

Annex 2: Obrazac za prijavu incidenta iz cyber sigurnosti 39

Annex 3: Osnovni nivo sigurnosti za novinarske redakcije 41

Annex 4: Visok nivo sigurnosti za novinarske redakcije 43

Annex 5: Primjer programa praktične obuke osoblja 45

Uvod

Značaj cyber sigurnosti za civilno društvo i medijske organizacije
Opseg i ciljevi priručnika

U digitalnom dobu sigurnost informacija postaje sve važnija komponenta zaštite kako novinskih redakcija tako i organizacija civilnog društva. S obzirom na to da se veliki dio komunikacije i skladištenje podataka odvija preko interneta, pitanje digitalne sigurnosti postaje ključno za očuvanje integriteta, privatnosti i efikasnosti rada. Ovaj je priručnik osmišljen sa ciljem da pruži osnovne smjernice i savjete za unapređenje digitalne sigurnosti unutar vaših organizacija.

Zašto je digitalna sigurnost važna?

Suočavamo se s brojnim prijetnjama koje mogu ugroziti našu digitalnu sigurnost. Od phishing napada, preko softvera za špijuniranje, do napada ransomwareom, rizici su raznovrsni i sveprisutni. Novinske redakcije često postaju meta napada zbog osjetljivih informacija koje posjeduju, dok organizacije civilnog društva mogu biti na meti zbog svog zagovaračkog rada i uticaja na javne politike. Stoga je od suštinskog značaja razviti strategije i implementirati alate koji će pomoći u zaštiti podataka i komunikacija.

Šta pokriva ovaj priručnik?

Priručnik je podijeljen u nekoliko ključnih poglavlja koja će vam pomoći da razumijete temelje digitalne sigurnosti, identifikujete najčešće prijetnje i primijenite najbolje prakse za njihovo suzbijanje. Svako poglavlje prilagođeno je tako da postepeno gradi znanje i vještine: od osnovnih do naprednih, bez pretpostavke prethodnog tehničkog iskustva.

Kako koristiti ovaj priručnik?

Priručnik je dizajniran tako da bude pristupačan širokom krugu čitatelja – od tehnički osviještenih pojedinaca do onih koji se prvi put susreću s konceptom digitalne sigurnosti. Savjetujemo da priručnik koristite kao vodič kroz sve faze implementacije sigurnosnih mjera u organizaciji. Može se čitati po redu, od početka do kraja, ili skakati na poglavlja koja su trenutno najrelevantnija.

Važno je shvatiti da digitalna sigurnost nije jednokratna akcija, već kontinuirani proces koji zahtijeva stalnu pažnju i prilagođavanje novonastalim situacijama i tehnologijama. Kroz ovaj priručnik stavit ćemo vam na raspolaganje znanja i alate koji će vam pomoći da taj proces učinite što uspješnijim.

Zašto je važno imati strategiju digitalne sigurnosti?

Digitalna strategija predstavlja temelj zaštite organizacija u svijetu koji je sve više digitalno povezan i u kojem informacije predstavljaju moć. Ovo poglavlje detaljnije objašnjava zašto je važno imati jasno definisanu i sveobuhvatnu digitalnu strategiju – kako za novinske redakcije tako i za organizacije civilnog društva, te kako ona može služiti kao prvi korak u osiguravanju digitalnih sredstava. Digitalna strategija obuhvata planiranje i implementaciju tehnologija, alata i praksi koje organizacija koristi za upravljanje digitalnim resursima, komunikacijom i podacima. Uključuje analizu postojećih sigurnosnih mjera, procjenu rizika, odabir odgovarajućih tehnoloških rješenja i edukaciju zaposlenih. Cilj je stvoriti sveobuhvatan sistem koji omogućava

organizaciji efikasno i sigurno upravljanje svojim digitalnim aktivnostima.

Zaštita osjetljivih informacija
Novinske redakcije često rade s povjerljivim informacijama koje mogu uključivati izvore izložene riziku, nedokumentovane tvrdnje ili interne komunikacije. Za organizacije civilnog društva zaštita podataka o donatorima, finansijskih izvještaja i strategija ključna je za očuvanje njihove misije i integriteta.

Prevencija i reakcija na cyber napade
Adekvatna strategija može pomoći u identifikovanju i sprečavanju potencijalnih sigurnosnih prijetnji prije nego što one prouzrokuju štetu. Također, omogućava brzu i organizovanu reakciju u slučaju sigurnosnog incidenta.

Održavanje povjerenja i reputacije
Organizacije koje efikasno upravljaju svojim digitalnim resursima i štite podatke bolje stoje u očima javnosti, partnera i donatora. Odgovorno upravljanje informacijama gradi povjerenje saradnika i publike, a njegovo narušavanje može imati ozbiljne posljedice za kredibilitet organizacije ili medija.

Elementi efikasne strategije digitalne sigurnosti:

Sigurnosna politika
Razvoj jasne i primjenljive sigurnosne politike koja definiše pravila ponašanja, procedura i odgovornosti.

Tehnološki alati
Odabir i implementacija tehnoloških alata koji odgovaraju specifičnim potrebama organizacije, kao što su šifrovani komunikacijski kanali, antivirusni programi i alati za upravljanje lozinkama.

Edukacija zaposlenih
Redovno osposobljavanje zaposlenih o najboljim praksama digitalne sigurnosti i najnovijim prijetnjama može značajno smanjiti rizik od sigurnosnih incidenata.

Redovne revizije i testiranje
Implementacija redovnih revizija sigurnosti i testiranja ranjivosti da se osigura da su sve mjere sigurnosti ažurne i efikasne.

Plan za odgovor na incidente
Razvijanje detaljnih planova za odgovor na incidente koji će osigurati da organizacija može brzo i efikasno reagovati na bilo kakve sigurnosne prijetnje.

Implementacija efikasne strategije digitalne sigurnosti nije samo tehnička obaveza, već strategijska odluka koja može značajno uticati na sposobnost organizacije da funkcioniše u digitalnom okruženju. Pravilno upravljanje digitalnim resursima i strategijama ne samo da štiti organizaciju od vanjskih prijetnji već također pruža osnovu za nesmetano i produktivno poslovanje.

Značaj kibernetičke otpornosti za civilno društvo i medijske redakcije

Kibernetička otpornost predstavlja sposobnost organizacije da se odupre, prilagodi i brzo oporavi od kibernetičkih napada koji mogu ugroziti integritet, dostupnost ili povjerljivost njenih informacionih resursa. Za civilno društvo i medijske redakcije, koje često rade s osjetljivim informacijama i podložne su različitim oblicima digitalnih prijetnji, kibernetička otpornost nije samo tehnička potreba, već ključni aspekt njihovog opstanka i integriteta.

Razumijevanje digitalnog okruženja

Digitalno okruženje obuhvata sve ono što nas okružuje u svijetu tehnologije i interneta, uključujući uređaje, mreže, aplikacije i usluge koje koristimo za svakodnevnu komunikaciju, rad i interakciju. U kontekstu civilnog društva i medijskih redakcija, razumijevanje ovog okruženja ključno je za efikasno upravljanje digitalnim resursima, zaštitu podataka i održavanje kibernetičke otpornosti.

Komponente digitalnog okruženja

Digitalno okruženje sastoji se od nekoliko ključnih komponenti:

Uređaji
Računari, pametni telefoni, tableti i drugi povezani uređaji koji pružaju pristup digitalnim resursima i uslugama.

Mreže
Infrastruktura koja omogućava uređajima da komuniciraju međusobno, uključujući internet, lokalne mreže (LAN) i privatne mreže (VPN).

Aplikacije i softver
Programi koji se koriste za obavljanje specifičnih zadataka kao što su obrada teksta, upravljanje bazama podataka, komunikacija i multimedija.

Servisi i platforme
Online servisi i platforme koje omogućavaju skladištenje podataka, dijeljenje sadržaja, kolaboraciju i komunikaciju kao što su usluge u oblaku, društvene mreže i profesionalni alati.

Razumijevanje kako ove komponente međusobno djeluju i koje sigurnosne rizike mogu predstavljati ključno je za razvoj efikasnih strategija zaštite.

Pregled uobičajenih prijetnji

Trenutni izazovi digitalne sigurnosti s kojima se suočavaju civilno društvo i mediji

Digitalno okruženje donosi brojne sigurnosne izazove koji zahtijevaju pažljivu analizu i proaktivno upravljanje, a spadaju u nekoliko vrsta:

***Cyber* napadi**
Uključuju različite oblike napada kao što su malware, ransomware, spyware, phishing, DDoS (Distributed Denial of Service) i drugi koji ciljaju na kompromitovanje sistema, krađu podataka ili ometanje operacija.

Ranjivosti softvera
Softverske greške i slabosti koje napadači mogu iskoristiti za dobijanje neovlaštenog pristupa ili ometanje normalnog funkcionisanja sistema.

Krađa i gubitak podataka
Nesreće ili napadi koji mogu dovesti do gubitka važnih podataka, što može imati finansijske, pravne ili reputacione posljedice.

Nedostatak kontrole nad podacima
Posebno izazovan u kontekstu usluga zasnovanih na oblaku, gdje organizacije mogu imati ograničenu kontrolu nad sigurnošću i upravljanjem svojih podataka.

U praksi, ovo su neke od najčešćih vrsta sigurnosnih incidenata u digitalnom prostoru sa kojima se susreću svi korisnici i korisnice. Važno je napomenuti da se incidenti s kojima se susreću pojedinci mogu preliti iz ličnog u poslovni prostor organizacije, te je bitno da zaposlenici i zaposlenice imaju svijest o sprovođenju praksi digitalne sigurnosti i u privatnom životu.

PHISHING predstavlja napade putem lažnih e-mejlova ili poruka koje izgledaju kao da su od pouzdanih izvora s ciljem krađe osjetljivih podataka. Phishing je varijanta tzv. socijalnog inžinjeringa gdje se od pojedinca ili organizacije lažnim predstavljanjem i sadržajem pokušavaju dobiti osjetljive informacije poput korisničkog imena, lozinke ili podataka o kreditnoj kartici. *Phishing* e-mejlovi obično (ali ne nužno) sadrže i link koji vodi na internetsku stranicu koja imitira izgled postojeće pouzdane *web* stranice (npr. stranicu banke ili PayPal servisa), gdje se traži upisivanje podataka o nalogu ili kreditnoj kartici. Osim e-mejla, za ovakve kriminalne radnje koriste se i poruke na servisima za direktno komuniciranje (npr. WhatsApp, Viber i slično) i poruke na društvenim mrežama, koje su posebno opasne jer mogu izgledati kao da dolaze od prijatelja.

DDOS (engl. Distributed Denial of Service) napad funkcioniše na način da pokušava učiniti internetski servis ili web stranicu nedostupnom tako što je preplavi ogromnim brojem zahtjeva ili paketa podataka iz različitih izvora. DDoS napadi najčešće se koriste za napad na internetske stranice, a u praksi to znači da se zagušuje određeni servis posebno napravljenim zahtjevima do te mjere da posjetioci više ne mogu otvoriti određenu web stranicu ili drugu vrstu servisa. Ovi napadi su problematični jer se najčešće izvode putem botneta, odnosno mreže računara zaraženim određenim virusom koje je moguće kontrolisati i iskoristiti na način da svi ti računari pošalju veliki broj zahtjeva na određenu IP adresu, zbog čega je otkrivanje napadača veoma kompleksan proces.

CURENJE PODATAKA (engl. *DATA LEAK*) je neovlašteno otkrivanje osjetljivih podataka često zbog sigurnosnog propusta. Naši podaci mogu biti izloženi ili kompromitovani zbog curenja podataka različitih digitalnih servisa, o čemu korisnike obavještavaju stručnjaci za digitalnu sigurnost, mediji ili same kompanije.

FIZIČKI GUBITAK ILI KRAĐA UREĐAJA poput laptopa ili pametnog telefona može dovesti do gubitka podataka ili kompromitovanja naloga na različitim digitalnim servisima, kao i ugroziti druge osobe čije smo podatke ili dokumente skladištili u uređaju.

PREUZIMANJE NALOGA je neovlašten pristup vašim *online* nalozima, obično putem ukradenih lozinki i *phishing* tehnika. Preuzimanje naloga na digitalnim servisima i društvenim mrežama jedan je od najčešćih načina napada na medijske organizacije i organizacije civilnog društva (i njihove zaposlene), a može imati, pored operacionih i sigurnosnih, i ozbiljne reputacione posljedice.

***MALWARE* (ZLONAMJERNI SOFTVER)** je zlonamjerni softver dizajniran za oštećivanje ili neovlašteni pristup računalnim sistemima.

RANSOMWARE je vrsta *malwarea* koja zaključava korisnikove datoteke ili onemogućava korištenje uređaja pojavljivanjem početne poruke koju je nemoguće skloniti s ekrana. Motiv onih koji koriste ransomware je finansijska korist te se od korisnika nakon zaraze zlonamjernim sotverom zahtijeva otkupnina za vraćanje pristupa. Najvažniji korak za odbranu od ransomwarea je redovno kreiranje sigurnosnih kopija podataka (*back up*).

***SPYWARE* (ŠPIJUNSKI SOFTVER)** je široka kategorija štetnog softvera koja presreće ili preuzima djelomično kontrolu rada na korisnikovom uređaju bez znanja ili dozvole korisnika.

***MAN-IN-THE-MIDDLE* (MitM)** je vrsta *cyber* napada u kojem napadač presreće komunikaciju između dvije strane i na taj način može manipulisati ili ukrasti informacije.

DOXXING je otkrivanje i objavljivanje privatnih informacija o osobi bez njenog pristanka, često sa ciljem prijetnje ili ugrožavanja lične sigurnosti. *Doxxing* je vrsta digitalnog nasilja koja je često usmjerena na novinarke i aktivistice.

SOCIAL ENGINEERING je manipulacija ljudi kako bi se otkrile osjetljive informacije putem psiholoških trikova. Napadači koriste psihološke trikove, poput preuzimanja identiteta ili stvaranja lažnog osjećaja hitnosti, kako bi vas natjerali da otkrijete lozinke ili druge važne informacije.

VIRUS je zlonamjerni softver koji se samostalno širi i može oštetiti datoteke ili sisteme.

SPAM je neželjena elektronska poruka poslana s namjerom oglašavanja raznog propagandnog sadržaja u svrhu *phishing* napada ili kao sredstvo distribucije zlonamjernih linkova. Šalje se putem e-mejla, aplikacija za direktnu komunikaciju, foruma, blogova ili društvenih mreža, a najvažnija osobina mu je to što nudi razne vrste usluga bez prethodnog odobrenja korisnika za njihovo primanje. Oni koji šire spam prikupljaju mejl-adrese potencijalnih primatelja putem različitih *web* stranica, *online* servisa, botova i/li zaraženih uređaja. Važno je ne klikati na linkove u ovakvim e-mejlovima i znati da je link koji nudi odjavljivanje sa liste u mejlu koji je spam zapravo način kojim potvrđujete valjanost vaše mejl-adrese. Za sprečavanje širenja mejl-adrese ovim putem savjetuje se izbjegavanje pisanja mejl-adresa na *web* sajtovima ili u elektronskoj komunikaciji u izvornom obliku.

Procjena rizika i planiranje

Sprovođenje procjene rizika digitalne sigurnosti
Identifikacija resursa i ranjivost
Prioritizacija rizika na osnovu uticaja i vjerovatnoće

Analiza trenutne digitalne infrastrukture

Da bi organizacije civilnog društva i medijske redakcije mogle efikasno upravljati rizicima i zaštititi se od kibernetičkih prijetnji, ključno je redovno analizirati trenutnu digitalnu infrastrukturu. Analiza digitalne infrastrukture omogućava organizacijama da identifikuju slabosti u svojim sistemima, procijene rizike i usklade svoje sigurnosne mjere s najboljim praksama i standardima. U ovom poglavlju, istražit ćemo kako izvršiti detaljnu analizu digitalne infrastrukture i korake koje organizacije mogu poduzeti da poboljšaju svoju *cyber* otpornost.

Digitalna infrastruktura obuhvata sve tehnološke resurse koje organizacija koristi za obavljanje svojih operacija, uključujući računarske sisteme, mreže, softver, podatkovne centre i usluge bazirane na oblaku. Analiza ove infrastrukture podrazumijeva detaljno ispitivanje svih aspekata tehnološkog okruženja, od hardvera do aplikacija koje se koriste za poslovne operacije.

Analiza digitalne infrastrukture može se podijeliti u nekoliko ključnih faza:

1. Inventarizacija
Prvi je korak stvoriti sveobuhvatan popis svih IT resursa, uključujući uređaje, softver, mrežne komponente i usluge na oblaku. Ovo uključuje i procjenu verzija softvera, konfiguracija sistema i prava pristupa.

2. Procjena rizika
Nakon što su resursi inventarizirani, slijedi procjena rizika koja uključuje identifikaciju potencijalnih sigurnosnih slabosti i prijetnji koje mogu uticati na digitalnu infrastrukturu. Ovaj korak uključuje analizu kako unutrašnje tako i vanjske prijetnje, od zlonamjernih napada do tehničkih kvarova.

3. Sigurnosno testiranje
Koristeći alate kao što su skeneri ranjivosti i penetracijski testovi, sigurnosni stručnjaci mogu otkriti i dokumentovati slabosti u infrastrukturi. Ovi testovi pomažu u razumijevanju potencijala za neautorizovani pristup ili gubitak podataka

4. Analiza usklađenosti
Provjerava se da li trenutne sigurnosne mjere i politike odgovaraju nacionalnim i međunarodnim standardima i regulativama koje se odnose na zaštitu podataka i informacijsku sigurnost.

5. Izrada izvještaja i preporuka
Na osnovu prikupljenih informacija izrađuje se detaljan izvještaj koji uključuje nalaze o stanju infrastrukture, identifikovanim rizicima i slabostima, te preporuke za poboljšanja.

Implementacija preporuka

Na osnovu izvještaja organizacije bi trebale razviti plan implementacije koji uključuje prioritizaciju zadataka na osnovu njihove hitnosti i potencijalnog uticaja na organizaciju. Preporuke mogu uključivati tehničke nadogradnje, promjene u politikama i procedurama, kao i dodatne edukativne programe za zaposlene.

Kontinuirano praćenje i revizija

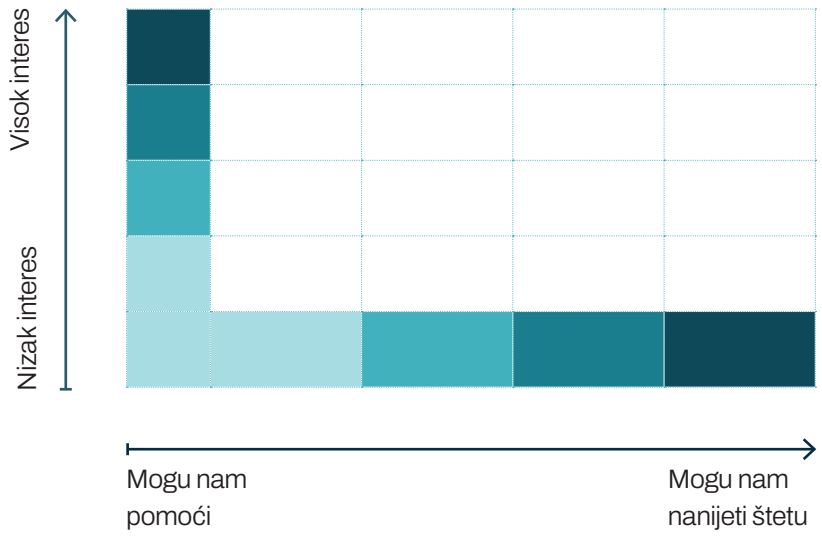
Digitalna infrastruktura nije statična; ona stalno evoluira kako se tehnologija razvija i kako se mijenjaju operativni zahtjevi organizacije. Stoga je ključno uspostaviti procese kontinuiranog praćenja i redovnih revizija kako bi se osiguralo da su sve komponente ažurne i da sigurnosne mjere i dalje odgovaraju trenutnim potrebama i prijetnjama.

Kreiranje plana/strategije digitalne sigurnosti za organizaciju

Kreiranje i implementacija plana digitalne sigurnosti kontinuiran je proces koji se sastoji iz analize konteksta u kojem organizacija djeluje, procjene rizika, osmišljavanja strategija smanjenja rizika, uvođenja propisa i smjernica, kreiranje protokola za slučaj sigurnosnog incidenta, te ponovne analize i prilagođavanja ukoliko do takvog incidenta dođe.

Analiza konteksta

Ko su zainteresovane strane koje bi mogle vašoj organizaciji nauditi ili joj pomoći? Ko su vam protivnici, a ko saveznici? Mapirajte ih i odredite koliko su zainteresirani za vaš rad.



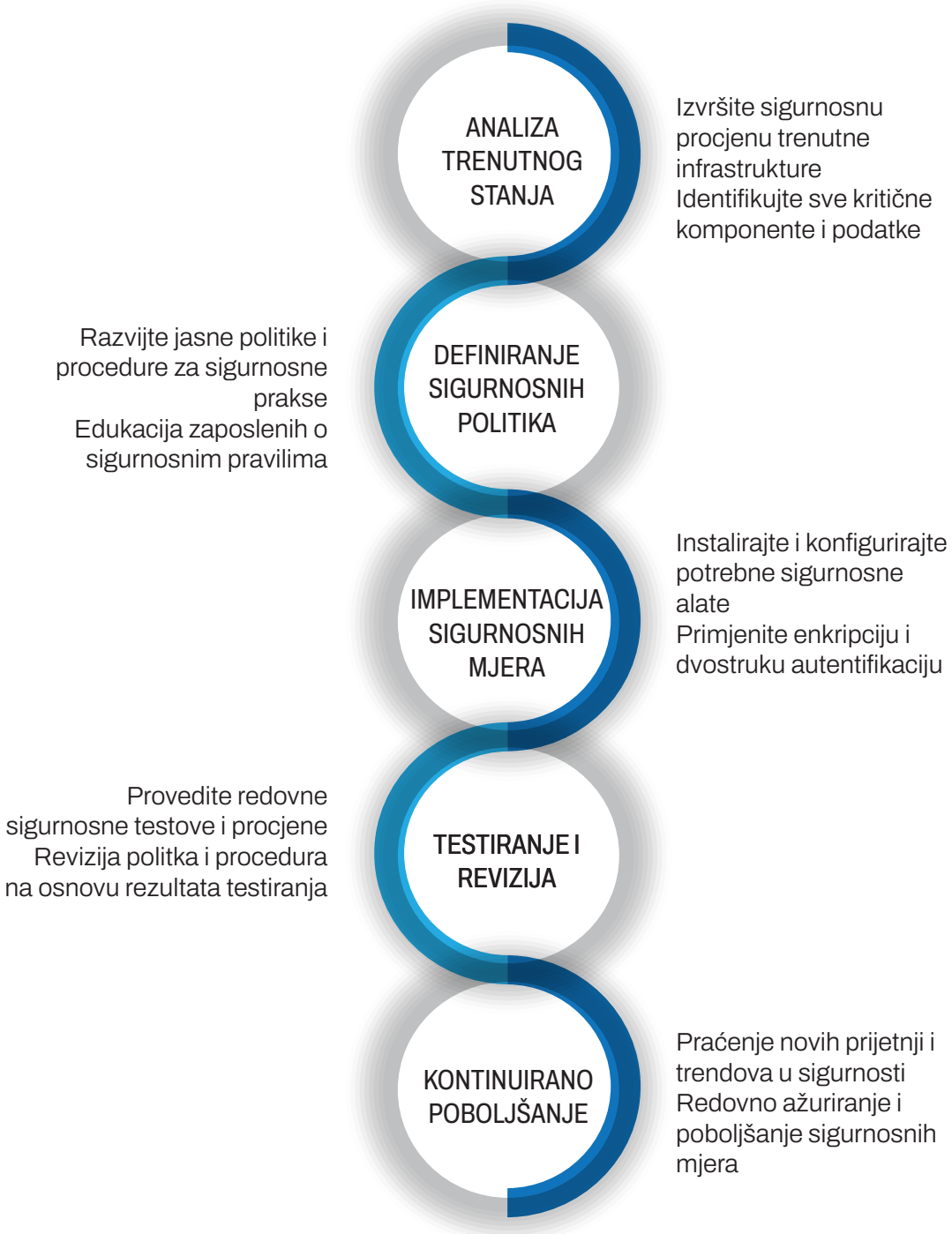
Određivanje modela prijetnje

Da biste procijenili potencijalni rizik u kojem se nalazite, razmislite a) šta želite sačuvati i b) od koga to želite sačuvati. Detaljno odgovorite na pitanja ispod kako biste dobili jasniju sliku o svojim trenutnim praksama digitalne sigurnosti i područjima koja je potrebno unaprijediti.

- Koliko uređaja posjedujete? Koliko ih je priključeno na internetsku mrežu?
- Ko je zadužen za održavanje uređaja?
- Na kojim online servisima imate naloge kao organizacija i/li pojedinci koji ih koriste za poslovne svrhe? Koji su to servisi?
- Ko im ima pristup?
- Kojim podacima ti servisi imaju pristup? Koliko tih servisa ima pristup vašim bankovnim podacima/kreditnoj kartici?
- Koristite li dvofaktorsku autentifikaciju?
- Koje vrste informacija prikupljate tokom svog rada? Da li rukujete ličnim podacima vanjskih lica (saradnika ili izvora)? Na koji način ih primate i skladištite? Koliko ih dugo čuvate? Koristite li enkripciju?
- Da li imate sigurnosne kopije podataka? Gdje ih čuvate?
- Da li imate uspostavljene sigurnosne procedure u slučaju krađe ili gubitka uređaja, naloga i/li podataka?
- Da li imate različite nivoe privilegija pristupa podacima?
- Imate li pravila o brisanju i arhiviranju podataka?

Sjetite se mapiranja aktera koje ste radili: ko bi mogao imati interes za pristup vašim podacima? Provalnici? Gosti? Poslodavci? Države? Korporacije? Razmislite o tome koliko je svaka od gore navedenih prijetnji vjerovatna. Da li poznajete slučajeve sigurnosnih incidenata koji su se desili srodnim organizacijama ili pojedincima? O kojoj vrsti incidenata se radilo? Naposljetku, pokušajte da zamislite posljedice svakog od incidenata i koliko bi oni ozbiljno oštetili funkcionisanje vaše organizacije. Ovo će biti vaša vodilja kroz kreiranje politika i protokola odgovora na incidente.

Planiranje sigurnosnih mjera



Resursi

Kada ste mapirali potencijalne opasnosti za djelovanje vaše organizacije i posljedice koje bi različite vrste sigurnosnih incidenata donijele, sljedeći je korak da razmislite o tome koliko ste resursa spremni i u mogućnosti uložiti da se zaštitite. Koje vještine je potrebno da ima vaše osoblje? Koliko im je treninga potrebno da te vještine i navike steknu? Da li je potrebno da uložite novac u nova softverska i hardverska rješenja? Da li je potrebno da se konsultujete sa stručnjacima za *cyber* sigurnost i/li pravnicima? Odgovori na ova pitanja ključna su komponenta planiranja resursa koje organizacije može prikupiti ili odvojiti za jačane digitalne sigurnosti.

Implementacija politike digitalne sigurnosti organizacije

Nakon analize infrastrukure, potreba, raspoloživih resursa i odabira pristupa zaštiti digitalne infrastrukure i integriteta podataka organizacije, potrebno je kreirati i određene dokumente koji će olakšati implementaciju politika u svakodnevnom radu, a to su smjernice za uposlenike i protokoli za prijavu *cyber* incidenata.

Kreiranje i implementacija smjernica za uposlenike

Smjernice za uposlenike organizacije izvode se iz politike digitalne sigurnosti organizacije i na jednostavan način predstavljaju korake koje uposleni moraju da prate da bi pravila bila poštovana. One izlažu konkretne korake koje zaposleni treba da prate da bi bila očuvana sigurnost podataka i uređaja kojima organizacija upravlja, kao što su prakse sigurnosti pristupa *online* nalozima, fizičke sigurnosti uređaja i slično.

Kreiranje protokola za prijavu cyber incidenta

Vaša strategija digitalne sigurnosti treba jasno odrediti šta se smatra incidentom iz područja digitalne sigurnosti te na koji način i kome se takav incident treba prijaviti. Odredite jasne korake koje je potrebno pratiti u slučaju krađe ili gubitka uređaja, preuzimanja naloga na društvenim mrežama, fizičkog oštećenja podataka itd. Zavisno od veličine organizacije i kompleksnosti infrastrukture, možete kreirati i formular za prijavu incidenta koji sadrži informacije o tome kada i gdje se incident desio, opis incidenta i njegove uzroke. Ovakva evidencija bit će korisna za daljnju analizu vaših praksi digitalne sigurnosti i dati vam šansu da ih u budućnosti revidirate ukoliko je nakon incidenta uočena dodatna slabost. U nastavku možete pogledati nekoliko hodograma za prijavu različitih vrsta incidenata iz područja digitalne sigurnosti, od krađe i nestanka uređaja do gubitka podataka ili preuzimanja naloga na društvenim mrežama, a u aneksu ovog priručnika nalazi se primjer formulara za prijavu *cyber* incidenata.

Predstavnik/ca za digitalnu sigurnost

Specifični scenariji i odgovori

1. Krađa/gubitak uređaja:

- ✔ Onemogućite pristup ukradenom/izgubljenom uređaju putem MDM (Mobile Device Management) sistema
- ✔ Resetujte sve pristupne lozinke
- ✔ Obavijestite nadležne i relevantne korisnike

2. Preuzimanje naloga:

- ✔ Resetujte lozinke i provjerite sigurnosne postavke računa
- ✔ Aktivirajte dvostruku autentifikaciju (2FA)
- ✔ Obavijestite korisnika i nadležne službe o incidentu

3. Napad na web stranicu:

- ✔ Onemogućite pogođeni server
- ✔ Analizirajte i otklonite ranjivost koja je iskorištena
- ✔ Restaurirajte stranicu iz sigurnosne kopije
- ✔ Pratite promet i aktivnosti nakon oporavka

Ukoliko je to moguće, poželjno je odrediti jednu osobu u timu koja će preuzeti obaveze organizacije kontinuirane edukacije zaposlenih iz područja digitalne sigurnosti, podsjećati na redovno zakazana održavanja opreme i ***online*** naloga, te dijeliti informacije o potencijalnim novim opasnostima ili alatima iz područja digitalne sigurnosti, kao i surađivati sa vanjskim ekspertima u redovnom ažuriranju politika organizacije. Za određene digitalne servise moguće je koristiti i automatizirane podsjetnike za promjenu šifri, ažuriranje softvera, kreiranje rezervnih kopija i sl.

Trening uposlenika

Nakon kreiranja politike, smjernica i protokola za prijavu *cyber* incidenata, uposlene je potrebno upoznati s pravilima i postojećim dokumentima putem treninga. Trening je potrebno koncipirati tako da se svi zaposleni upoznaju s potencijalnim opasnostima u digitalnom okruženju i s mjerama koje se mogu poduzeti da se one izbjegnu, kao i s pravilima organizacije. Potrebno je jasno naglasiti pravila i moguće posljedice njihovog kršenja za cijeli tim i vanjske saradnike organizacije. Trening je moguće implementirati u saradnji s nekim od stručnjaka za digitalnu sigurnost iz rostera u aneksu ovog priručnika, gdje možete pronaći i primjer agende programa za trening uposlenih.

Za trening možete koristiti i tzv. ***battle cards***, edukacijski resurs koji je na bosanskom jeziku dostupan na stranicama Centra za izvrsnost u *cyber* sigurnosti i na interaktivan način približava oko 50 mogućih *cyber* incidenata i odgovora na njih.

Važno je napomenuti da je edukacija iz digitalne sigurnosti kontinuiran proces i da je potrebno zakazati periodične radionice za savladavanje novih alata, obavještavati zaposlene o novim i trenutno aktuelnim prijetnjama u *online* prostoru, te od njih prikupljati povratne informacije o implementaciji politike digitalne sigurnosti i integriteta podataka organizacije, kako bi njena sprovedba bila što efikasnija.

Preporučeni alati i prakse digitalne sigurnosti

Sigurnost pristupa

Za organizacije civilnog društva i medijske organizacije, postavljanje pravila o sigurnom pristupu digitalnim servisima, aplikacijama i uređajima od suštinskog je značaja za zaštitu osjetljivih informacija i osiguravanje kontinuiteta rada. Ove organizacije često rukovode povjerljivim podacima, uključujući informacije o članovima, donatorima, i istraživanjima, te su stoga česte mete *cyber* napada. Pravila o sigurnom pristupu pomažu u minimiziranju rizika od neovlaštenog pristupa, krađe podataka, i drugih sigurnosnih prijetnji, čime se štiti integritet i povjerljivost podataka. Pored toga, dosljedna primjena ovih pravila osigurava da svi članovi organizacije razumiju i pridržavaju se najboljih praksi u *cyber* sigurnosti, što dodatno doprinosi kolektivnoj zaštiti i efikasnosti u radu organizacije.

Lozinke

Jaka šifra prvi je stub odbrane vašeg uređaja ili naloga. Jake su šifre kompleksne i sadrže različite vrste znakova, uključujući mala i velika slova, brojeve i specijalne znakove. Pored korištenja slabih šifri, sigurnosni rizik predstavlja i korištenje istih lozinki na različitim uređajima i *online* servisima, čime se incidentom na jednom uređaju ili nalogu dovode u opasnost i svi ostali, te je za svaki uređaj i digitalni alat potrebno osmisliti posebnu šifru. Za čuvanje i upravljanje šiframa, preporučuje se korištenje tzv. menadžera šifri (engl. *password manager).*

Menadžer lozinki

Menadžeri šifri su sigurnosni alati koji generišu i čuvaju vaše šifre i smanjuju rizik od korištenja istih ili nedovoljno jakih šifri na različitim nalozima. Menadžer šifri može biti instaliran lokalno ili u oblaku. Neki od najkorištenijih servisa za menadžment lozinki su Google Password Manager, 1Password i KeePass. Alat koji najbolje odgovara potrebama i mogućnostima vaše organizacije možete odabrati u konsultacijama sa stručnjacima za digitalnu sigurnost.

Dvofaktorska autentifikacija (2FA)

Dvofaktorska autentifikacija je metod zaštite vaših *online* naloga koji kombinuje nešto što znate (vašu šifru) i nešto što imate (dodatni uređaj, aplikaciju ili kanal komunikacije kojim možete primiti kod za autentifikaciju). Uključivanje opcije dvofaktorske autentifikacije značajno otežava pristup vašim ličnim nalozima za neovlaštena lica, čak i ako imaju vašu šifru, a danas je nude skoro svi *online* servisi.

Sigurnost uređaja

Osiguranje pametnih telefona i tableta koji se koriste u radu
Sigurnost mobilnih aplikacija i dozvola
Daljinsko brisanje i praćenje funkcija za izgubljene ili ukradene uređaje

Imati pravila o sigurnosti uređaja koji se koriste u radu od suštinskog je značaja jer osigurava zaštitu osjetljivih podataka i integritet radnih procesa. Uređaji poput računara, pametnih telefona i tablet-uređaja često sadrže povjerljive informacije i pristup ključnim sistemima, što ih čini metama za *cyber* napade i neovlašteni pristup. Pravila o sigurnosti pomažu u sprečavanju gubitka podataka, krađe identiteta i drugih oblika digitalnih prijetnji kroz implementaciju sigurnosnih mjera poput enkripcije, jakih lozinki, redovnih ažuriranja softvera i sigurnosnih kopija podataka. Ova pravila ne samo da štite organizaciju od potencijalnih sigurnosnih incidenata već i podižu svijest zaposlenih o važnosti odgovornog korištenja tehnologije, čime se stvara sigurnije i produktivnije radno okruženje. Ovo su neka od najčešće korištenih i pristupačnih rješenja za digitalnu sigurnost uređaja članova vašeg tima koje organizacija može implementirati sama ili u saradnji sa stručnjacima:

Softverska rješenja za digitalnu sigurnost uređaja

ANTIVIRUS

Softver koji detektira i uklanja zlonamjerni softver (*malware*) s vašeg računara ili uređaja. Postavlja se na sam uređaj i prepoznaje zlonamjerni softver. Kompanije koje proizvode antivirusne programe redovno ih ažuriraju da prepoznaju najnovije prijetnje, a za izbor antivirusnog programa koji najbolje odgovara vašem timu i tehnologiji koju koristite konsultujte se sa stručnjacima.

FIREWALL

Sigurnosni sistem koji prati i kontrolira dolazni i odlazni mrežni promet na osnovu sigurnosnih pravila, štiteći mrežu od neovlaštenog pristupa.

DALJINSKO BRISANJE (engl. *REMOTE WIPE*)

Funkcija koja omogućava daljinsko brisanje podataka s uređaja, korisna u slučaju gubitka ili krađe uređaja. Razgovarajte sa IT stručnjacima o tome da li je ova vrsta funkcije dobro rješenje za vaš tim i na koji ga način zaposleni mogu implementirati.

Hardverska rješenja za digitalnu sigurnost uređaja

YUBIKEY/TITAN SECURITY KEY

Hardverski uređaj koji omogućava dvostruku autentifikaciju i dodatni sloj sigurnosti prilikom prijave na online naloge. Funkcioniše na principu uparenosti s uređajem i online nalogom. Uređaje je moguće kupiti, a Google nudi i program besplatne dostave ovih uređaja za medijske organizacije.

FARADEJEV KAVEZ

Zaštitna konstrukcija koja blokira elektromagnetne signale, sprečavajući presretanje podataka s uređaja.

POKRIVAČI KAMERE I MIKROFONA

Fizički pokrivači koji blokiraju kameru i mikrofon na uređajima, štiteći privatnost od neovlaštenog snimanja.

Sigurnost podataka

Metode šifriranja podataka (u mirovanju i tokom prijenosa)
Sigurnost osjetljivih dokumenata i datoteka
Sigurno i redovno kreiranje rezervnih kopija podataka

Imati pravila o sigurnosti podataka koji se koriste u radu ključno je za zaštitu integriteta, povjerljivosti i dostupnosti informacija unutar organizacije. Ova pravila omogućavaju sistemski pristup upravljanju osjetljivim informacijama, smanjujući rizik od neovlaštenog pristupa, gubitka podataka i *cyber* napada. Sigurnosna pravila obuhvataju mjere kao što su enkripcija, kontrola pristupa, redovne sigurnosne kopije i edukacija zaposlenih o najboljoj praksi u rukovanju podacima. Kroz dosljednu primjenu ovih pravila, organizacija može zaštititi svoje poslovne interese, izgraditi povjerenje među klijentima i partnerima te osigurati usklađenost s relevantnim zakonodavstvom i regulativama. Na taj način, sigurnost podataka postaje temelj stabilnog i efikasnog poslovanja, omogućavajući organizaciji da se fokusira na svoje primarne ciljeve bez ometanja uzrokovanih sigurnosnim incidentima.

Korištenjem ovih prilagođenih digitalnih alata, male organizacije mogu optimizirati svoje operacije, poboljšati komunikaciju i zaštititi svoje vitalne informacije od digitalnih prijetnji. Važno je napomenuti da prilikom izbora alata treba uzeti u obzir specifične potrebe organizacije, kao i budžet i tehničke sposobnosti tima kako bi se osiguralo da odabrana rješenja mogu biti učinkovito implementirana i održavana.

ENKRIPCIJA

Jednostavno rečeno, enkripcija je proces pretvaranja čitljivih podataka u nečitljive, odnosno šifrirane podatke, korištenjem algoritama i ključeva za šifriranje. Cilj korištenja enkripcije je očuvanje sigurnosti komunikacije i/li prijenosa i skladištenja podataka, te se ona može primijeniti na e-mejl i *chat* komunikaciju i podatke skladištene na različitim vrstama diskova: na računaru, na prijenosnom uređaju (USB) ili na oblaku. Preporučuje se da trening iz enkripcije za članove tima organizacija pripremi u saradnji s trenerom iz oblasti digitalne sigurnosti, tako da svi članovi tima, bez obzira na prethodno znanje, mogu primijeniti prakse enkripcije dokumenata i komunikacije.

REZERVNE KOPIJE

Rezervne kopije (engl. *back up*) su kopije važnih podataka smještene odvojeno od primarnog mjesta skladištenja (npr. poslovnog ili personalnog računara). Svrha rezervne kopije je da štiti od gubitka podataka usljed gubitka ili oštećenja uređaja, *cyber* napada ili slučajnog brisanja podataka. Iako veoma jednostavna i bazična praksa digitalne sigurnosti, često je zanemarena u radnom procesu te vrijedi razmisliti o uključivanju podsjetnika za redovno kreiranje rezervnih kopija za zaposlene u politiku digitalne sigurnosti organizacije.

Sigurno korištenje interneta

Smjernice za sigurno korištenje interneta i *online* servisa, uključujući društvene mreže i *online* preglednike, neophodne su za očuvanje integriteta podataka organizacije, ličnu sigurnost zaposlenika, očuvanje produktivnosti i poštivanje zakonskih zahtjeva o zaštiti ličnih podataka. Kontinuirana edukacija zaposlenih o važnosti i metodama sigurnog korištenja *online* servisa ključni je faktor za uspjeh ove strategije, a ona kombinira nekoliko elemenata spomenutih u različtim poglavljima ovog priručnika:

- kreiranje i korištenje jakih i različitih šifri za online naloge,
- korištenje sigurnih načina pristupanja sadržaju putem online preglednika,
- svijest o phishingu i drugim formama socijalnog inženjeringa,
- protokol za sigurno korištenje društvenih mreža.

Kibernetička sigurnost od vitalnog je značaja za sve organizacije. Alati kao što su Bitdefender, Norton Small Business i McAfee Small Business Security pružaju zaštitu od virusa, *malwarea* i drugih *cyber* prijetnji. Ovi su proizvodi dizajnirani tako da budu jednostavni za instalaciju i upotrebu, što je idealno za male organizacije koje nemaju specijalizovane IT timove.

Socijalni inženjering

Šta je *phishing* i kako ga prepoznati?

Phishing je metoda prevare u kojoj napadači šalju lažne e-mejlove ili poruke koje izgledaju kao da su od pouzdanih izvora, s ciljem krađe osjetljivih informacija poput lozinki ili brojeva kreditnih kartica. Prepoznajte *phishing* pokušaje po neslužbenim mejl-adresama, gramatičkim greškama i hitnosti zahtjeva za unos ličnih podataka. Nikada ne otvarajte linkove ili priloge iz sumnjivih poruka i provjerite autentičnost pošiljatelja prije nego što odgovorite.

Kako se zaštititi od socijalnog inženjeringa?

Socijalni inženjering uključuje manipulaciju ljudi kako bi se otkrile osjetljive informacije. Napadači koriste psihološke trikove, poput preuzimanja identiteta ili stvaranja lažnog osjećaja hitnosti kako bi vas natjerali da otkrijete lozinke ili druge važne informacije. Za zaštitu od ovakvih napada, budite oprezni prilikom dijeljenja informacija, provjerite identitet osobe koja traži osjetljive podatke i nikada ne dijelite povjerljive informacije putem telefona ili e-mejla bez prethodne provjere.

Kako reagovati na curenje podataka?

Ukoliko je online servis koji koristite imao sigurnosni incident koji je rezultirao curenjem podataka (engl. data leak), poduzmite sljedeće korake:

- Promjena lozinki i omogućavanje dvofaktorske autentifikacije (2FA) na nalozima.
- Budite oprezni u pogledu sumnjivih e-poruka ili poruka koje pokušavaju iskoristiti informacije koje su procurile.
- Nadgledanje računa za sve neuobičajene aktivnosti i prijavljivanje incidenata podršci online servisa.
- Sprovedite redovne bezbjednosne revizije kako biste identifikovali i adresirali potencijalne ranjivosti.
- Obavijestite sve zaposlene o incidentu i rizicima krađe identiteta i napada socijalnog inženjeringa.

Privacy Badger je inovativno proširenje za *web* preglednike koje su razvile neprofitne organizacije Electronic Frontier Foundation (EFF). Ovaj je alat specijalizovan za blokiranje *trackera* koji prate korisnike tokom surfanja internetom, a posebno je efikasan protiv onih koji prate aktivnosti preko različitih *web* stranica. Iako Privacy Badger uspješno blokira i neke oglase, to čini samo ako ovi oglasi sadrže *trackere*, razlikujući se time od tradicionalnih *ad-blockera* koji ciljaju sve reklamne sadržaje.

Jedinstvenost Privacy Badgera leži u njegovom algoritamskom pristupu detekciji *trackera* umjesto korištenja standardnih lista blokiranja, što mu omogućava da efikasnije štiti korisnikovu privatnost. Također, automatski šalje signale Global Privacy Control (GPC) i Do Not Track (DNT), blokirajući trackere i *web* stranice koje te signale ignorišu.

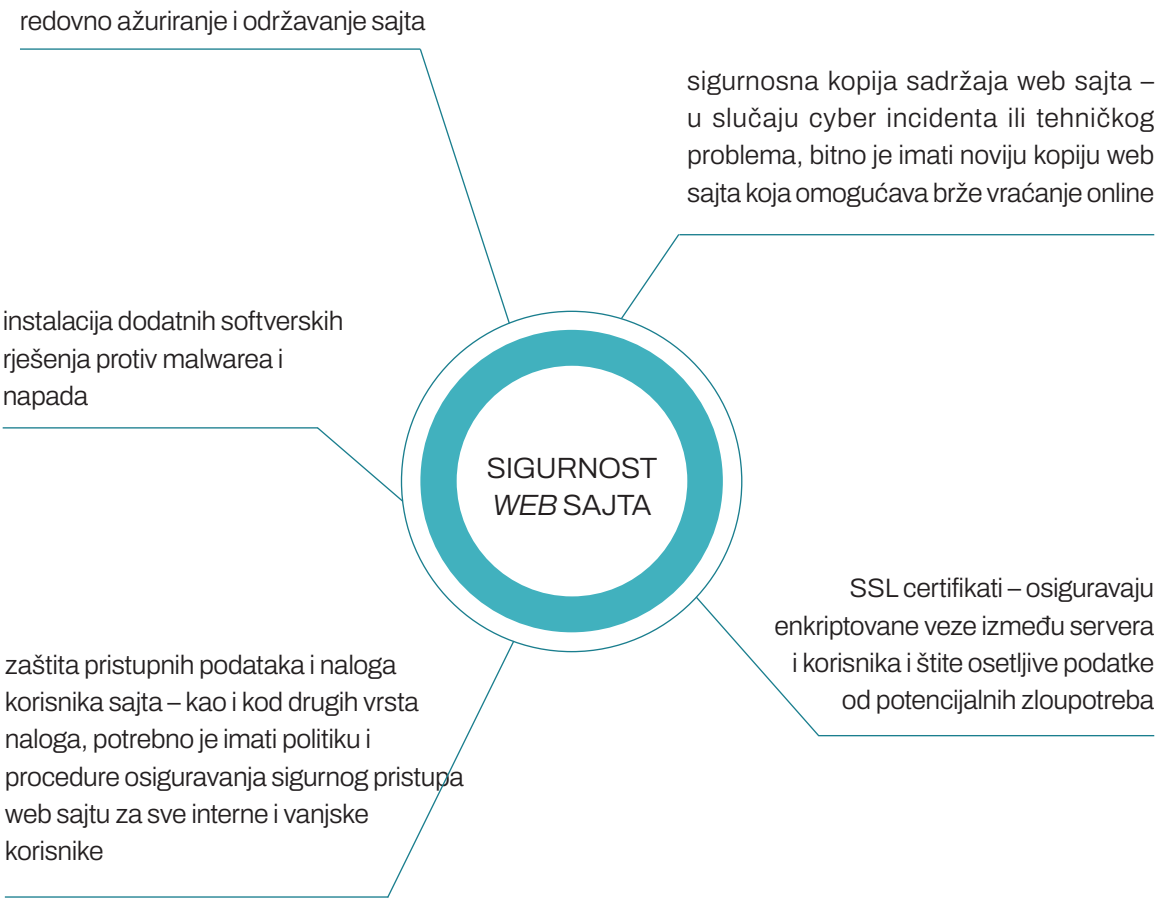
Instalacija Privacy Badgera je jednostavna, s opcijom da korisnik ostavi zadane postavke ili prilagodi parametre po svojim potrebama. Dodatno, korisnici mogu izuzeti određene stranice iz procesa blokiranja ako to žele.

Zajedno s Privacy Badgerom, Ghostery je još jedno korisno proširenje koje upravlja blokiranjem *trackera* i uklanja upozorenja o kolačićima po GDPR-u, omogućavajući korisnicima da automatski odbiju sve kolačiće. Ghostery nudi transparentnost u vidu prikaza broja blokiranih *trackera* i omogućava korisnicima da privremeno pauziraju njegov rad ili da prilagode njegove funkcije kako bi bolje odgovarale njihovim potrebama.

Oba proširenja, Privacy Badger i Ghostery, predstavljaju ključne alate za one koji teže većoj kontroli nad svojom *online* privatnošću i sigurnošću.

Sigurnost *web* sajta

Sigurnost *web* sajta organizacije segment je kojem treba posvetiti posebnu pažnju s obzirom na izloženost ovog dijela prisustva organizacije u internetskom prostoru. Nesigurna *web* stranica izložena je *cyber* napadima, ali i snižava SEO rang vašeg *web* sajta i može ugroziti korisnike i nanijeti reputacionu štetu organizaciji. Ovo su neki od koraka za osiguravanje *web* prezentacije organizacije:



Sigurna komunikacija

Sigurna komunikacija jedna je od osnovnih pretpostavki digitalne sigurnosti tima. Ona obuhvata korištenje principa i alata za siguran prijenos informacija i dokumenata putem e-mejla i aplikacija za direktnu komunikaciju. U nastavku navodimo neke od trenutno dostupnih alata za sigurn(ij)u komunikaciju: kako unutar tima tako i sa vanjskim saradnicima, izvorima informacija i drugim akterima sa kojima organizacije svakodnevno surađuju.

Alati za sigurnu komunikaciju

ProtonMail je siguran mejl-servis koji nudi *end-to-end* enkripciju, čime osigurava da samo pošiljalac i primatelj mogu pročitati poruku. ProtonMail je razvijen u Švicarskoj, zemlji poznatoj po strogim zakonima o privatnosti, i pruža korisnicima potpunu anonimnost. Registracija ne zahtijeva unos ličnih podataka, a svi e-mejlovi i podaci pohranjeni su u šifriranom formatu, čime su zaštićeni čak i od zaposlenika ProtonMaila. ProtonMail omogućava slanje samouništavajućih poruka, postavljanje dvofaktorske autentifikacije za dodatnu sigurnost, te integraciju sa drugim alatima za sigurnu komunikaciju. Ovaj je servis dostupan putem *web* preglednika, kao i putem mobilnih aplikacija za iOS i Android uređaje.

ProtonMail idealan je za novinare, aktiviste i sve one kojima je privatnost prioritet jer pruža visok nivo zaštite podataka i anonimnosti korisnika.

Firefox Send je besplatan i siguran alat za dijeljenje datoteka koji je razvila Mozilla. Omogućava korisnicima da dijele datoteke do 2.5GB uz maksimalnu privatnost. Svi podaci koji se prenose putem Firefox Send-a šifrirani su *end-to-end,* što znači da samo pošiljalac i primatelj mogu pristupiti sadržaju. Firefox Send omogućava postavljanje lozinki za dodatnu zaštitu datoteka, kao i određivanje vremenskog perioda ili broja preuzimanja nakon kojih će datoteke biti automatski obrisane. Ovaj je alat posebno koristan za dijeljenje osjetljivih informacija jer osigurava da podaci ostaju sigurni i privatni tokom prijenosa.

Firefox Send dostupan je putem *web* preglednika i ne zahtijeva kreiranje računa za korištenje osnovnih funkcija, čime pruža jednostavno i sigurno rješenje za dijeljenje datoteka.

Mailvelope je ekstenzija za ***web*** preglednike koja omogućava šifriranje poruka koristeći PGP (Pretty Good Privacy) enkripciju. Ovaj je alat dizajniran da radi s popularnim mejl-servisima poput Gmaila, Yahoo Maila i Outlooka. Mailvelope koristi javne i privatne ključeve za šifriranje i dešifriranje poruka, čime osigurava da samo namjeravani primatelji mogu pročitati sadržaj. Instalacija i konfiguracija Mailvelopea je jednostavna, a korisnici mogu kreirati vlastite ključeve ili koristiti postojeće. Mailvelope je idealan za one koji žele dodati sloj sigurnosti svojim e-komunikacijama, bez potrebe za promjenom e-mejla klijenta. Pruža visoku razinu zaštite podataka i privatnosti, te je kompatibilan s većinom popularnih servisa za e-komunikaciju.

Signal nije samo obična aplikacija zakomunikaciju; on je simbol digitalne privatnosti i sigurnosti, zasnovan na nezavisnom i neprofitnom modelu, čijem je razvoju doprinio i suosnivač WhatsAppa, Brian Acton. Ovaj se alat razlikuje od drugih sličnih servisa svojim *end-to-end* šifriranjem temeljenim na vlastitom otvorenom protokolu,

što ga čini izborom i demostranata i institucija poput Evropske komisije.

Signal nudi dodatne funkcije zaštite privatnosti kao što su autentifikacija PIN-om, inkognito tipkovnica i zaključavanje registracije. Osim standardnih opcija za razmjenu poruka i grupnih razgovora, nudi i mogućnost slanja poruka koje nestaju nakon definiranog vremena, te je na Androidu sposoban za primanje i slanje SMS i MMS poruka. Uz intenzivan fokus na zaštitu podataka i korisničku privatnost, Signal se izdvaja kao jedna od najpouzdanijih aplikacija za one koji cijene sigurnost u digitalnoj komunikaciji.

Session se ističe kao komunikacijski servis sa posebnim naglaskom na sigurnost i privatnost. Implementirajući *end-to-end* šifriranje kroz vlastiti protokol i kriptografsku biblioteku *libsodium*, Session ne štiti samo sadržaj poruka već i identitet svojih korisnika. Poruke prolaze kroz decentralizovanu mrežu nalik na Tor, a sve to bez potrebe za telefonskim brojem ili mejl-adresom – korisnicima se dodjeljuje jedinstveni Session ID, koji osigurava anonimnost.

Sa sjedištem u Australiji, Session ne prikuplja metapodatke, što znači da ni vlasti ne mogu zahtijevati privatne informacije. Lokalno pohranjene poruke na uređaju su šifrirane, kao i *backup* kopije, pružajući dodatni sloj sigurnosti. Iako se visoka sigurnost može odraziti na upotrebljivost, Session uspijeva zadržati jednostavnost korištenja.

Servis omogućuje slanje datoteka i glasovnih poruka, te opciju poruka koje se automatski brišu, ali ne podržava glasovne ili videopozive. Unatoč tome, idealan je za korisnike koji traže maksimalnu privatnost i sigurnost u digitalnoj komunikaciji, prihvaćajući da anonimnost ponekad dolazi sa cijenom u pogledu praktičnosti i brzine.

Telegram, kao aplikacija koja naglasak stavlja na privatnost i sigurnost, izgrađuje svoju reputaciju kroz podršku za *end-to-end* šifriranje u tzv. *Secret chat* modu, dok za standardne razgovore koristi šifriranje između klijenta i servera. Unatoč kritikama da *end-to-end* šifriranje nije univerzalno primijenjeno, transparentnost projekta otvorenog kôda i provjerljivi protokoli nude dodatnu sigurnosnu utjehu, zajedno s izazovima za otkrivanje sigurnosnih propusta sa značajnim novčanim nagradama.

Telegram se oslanja na telefonske brojeve kao osnovni identifikator, ali nudi detaljne postavke privatnosti koje korisnicima omogućuju kontrolu nad tim ko može vidjeti njihov broj. Aplikacija može biti zaštićena PIN-om ili biometrijom, a tu je i opcija autentifikacije u dva koraka. Za razmjenu tekstualnih poruka, glasovnih i videopoziva, Telegram nudi kapacitet datoteka do 2 GB i omogućava stvaranje velikih grupa i kanala za masovnu komunikaciju.

Osim što je aplikacija dostupna na pametnim telefonima, Telegram nudi klijentima opciju i za desktop i *web*, iako s određenim ograničenjima. Integrirani alat za editovanje fotografija, bogata biblioteka animiranih GIF-ova, platforma za virtualne naljepnice i mogućnost izrade botova dodatno obogaćuju korisničko iskustvo. Otvoreni API omogućava korisnicima da prilagode ili kreiraju vlastite aplikacije, čineći Telegram prilagodljivim i moćnim alatom za digitalnu komunikaciju.

Wire, usklađen sa švicarskim zakonima o zaštiti privatnosti, smješta svoje servere unutar EU – u Njemačkoj i Irskoj – čime osigurava da korisnički podaci ostaju pod zaštitom GDPR-a. Otvoren kod Wirea podvrgnut je neovisnim revizijama koje potvrđuju transparentnost u prikupljanju podataka. Wire jamči da podaci prikupljeni za analitičke svrhe nikada neće biti predmet trgovine.

S *end-to-end* šifriranjem Wire štiti komunikaciju, uključujući pozive i dijeljene datoteke, i ne zahtijeva broj telefona za registraciju – korisnici se mogu povezati preko e-mejla. Dostupnost na svim platformama i mogućnost korištenja u *web* pregledniku, uz sinhronizaciju do osam uređaja, čine Wire praktičnim za upotrebu na različitim uređajima bez ograničenja pametnog telefona.

Wire razdvaja personalne i poslovne račune, s različitim setom funkcionalnosti za svaki tip. Registracija se može izvršiti putem telefona ili e-mejla, a komunikacija počinje dodavanjem kontakata putem jedinstvenog korisničkog imena. Osim standardne razmjene poruka, glasovnih i videopoziva, Wire podržava slanje dokumenata i lokacije, grupne razgovore, samouništavajuće poruke i editiranje poslanih poruka. *Interface* je intuitivno i estetski privlačan, nudeći napredne opcije poput dijeljenja zaslona tokom videopoziva.

Za poslovne korisnike, Wire nudi Pro, Enterprise i Red verzije, prilagođene specifičnim potrebama, uključujući komunikaciju u kriznim situacijama. Enterprise izdanje omogućuje korištenje vlastite poslužiteljske infrastrukture, a sve verzije oslanjaju se na end-to-end šifriranje s ključevima koji ostaju isključivo u rukama korisnika. Cijene su prilagođene po modelu po korisniku, čineći Wire sigurnim izborom za one koji traže visoku razinu privatnosti i sigurnosti u digitalnoj komunikaciji.

Bridgefy je inovativna aplikacija iz Meksika koja omogućava komunikaciju bez internetske veze, idealna za situacije gdje je povezivost ograničena, kao što su glazbeni festivali, sportska događanja, velika okupljanja, ili čak u kriznim situacijama poput prirodnih katastrofa. Ova aplikacija koristi Bluetooth Low-Energy (BLE) tehnologiju za stvaranje *mesh* mreže omogućavajući komunikaciju čak i kad standardne mreže nisu dostupne.

Za početak korištenja Bridgefyja potrebna je jednokratna internetska veza za registraciju korisničkog profila, nakon čega internet više nije neophodan, ali je Bluetooth potrebno držati aktivnim. Aplikacija automatski detektira korisnike u blizini, olakšavajući razmjenu poruka unutar radijusa od 100 m.

Bridgefy je intuitivan za korišćenje s osnovnim *intefaceom* sličnim drugim komunikacijskim aplikacijama, iako nije bogat naprednim opcijama. U početku nije podržavao šifriranje poruka, ali je *end-to-end* šifriranje implementirano nakon što je aplikacija stekla popularnost među demostrantima u Hong Kongu i Indiji. Ako je potrebna pouzdana komunikacija bez internetske veze, Bridgefy predstavlja izvrstan izbor.

Threema je komunikacijska aplikacija koja se ne dobiva besplatno, naglašavajući svoju predanost zaštiti privatnosti. Ova platforma, koja zahtijeva jednokratnu kupovinu bez pretplate, omogućava korisnicima da koriste uslugu anonimno, bez potrebe za unošenjem broja telefona. Svaki korisnik dobiva jedinstveni Threema ID koji garantira anonimnost.

Sigurnost u Threemi na visokom je nivou zahvaljujući *end-to-end* šifriranju koje se oslanja na kriptografsku biblioteku NaCl. Svi podaci čuvaju se lokalno na uređaju korisnika i šifrirani su, a poruke se automatski brišu nakon dostave. Dodatno, svi poslužitelji aplikacije locirani su u Švicarskoj, što korisnicima pruža dodatnu sigurnost zbog strogih zakona o privatnosti koji se tamo primjenjuju.

Threema nudi sve standardne funkcije koje se očekuju od moderne komunikacijske aplikacije, uključujući tekstualne poruke, individualne i grupne glasovne i videopozive, kao i razmjenu datoteka. Također, podržava stvaranje grupa, provođenje anketa, i verifikaciju kontakata skeniranjem QR koda. Iako nema klijente za desktop i prijenosna računala, dostupna je upotreba preko *web* preglednika. Threema ne sadrži oglase, ne prati korisnike i redovno je predmetom nezavisnih sigurnosnih revizija.

Za one koji traže aplikaciju koja nudi vrhunsku sigurnost i privatnost i spremni su za to platiti Threema predstavlja izvrsnu opciju.

Tella je aplikacija otvorenog koda dizajnirana za aktiviste, novinare i borce za ljudska prava koji djeluju u područjima visoke državne kontrole. Cilj aplikacije je omogućiti sigurno prikupljanje i pohranjivanje dokaza o kršenju ljudskih prava. Tella pruža posebno šifrirano okruženje za čuvanje osjetljivih podataka, štiteći ih od cenzure, neovlaštenog pristupa, izmjene ili uništenja.

Ključne osobine Telle uključuju automatsko šifriranje svih pohranjenih datoteka koje su dostupne isključivo putem aplikacije. Dodatna sigurnost postiže se zaštitom pristupa pomoću PIN-a, uzorka ili lozinke, a aplikacija se može maskirati kao druga vrsta softvera, poput kalkulatora, čime se dodatno kamuflira njezina prisutnost. Važno je napomenuti da neke od ovih funkcija nisu dostupne na svim platformama.

Tella također omogućava direktne šifrirane snimke video i audio materijala unutar aplikacije, osiguravajući da su podaci odmah zaštićeni. Poseban *offline* način rada omogućava pohranu podataka koji se mogu sigurno sinhronizovati s podržanim platformama čim korisnik pristupi internetu.

Ukratko, Tella je moćan alat za one koji trebaju dokumentirati i zaštititi informacije o kršenju ljudskih prava, a njena besplatna dostupnost i otvoreni kod čine je dostupnom širokom spektru korisnika koji teže visokoj razini sigurnosti i privatnosti u svojim istraživanjima i aktivizmu, a moguće je instalirati i koristiti i na organizacijskom nivou.

VPN

Virtualna privatna mreža (engl. *virtual private network*) je sigurnosni alat koji prikriva lokaciju vašeg uređaja preusmjeravajući vašu *internet* komunikaciju preko servera koji se nalaze na različitim mjestima. Korištenje VPN-a sakriva vašu IP adresu od *web* sajtova koje posjećujete kao i od internetskih provajdera te se preporučuje ukoliko se nalazite u situaciji da koristite otvorenu/javnu *wifi* mrežu.

Mullvad VPN, sa sjedištem u Gothenburgu, Švedska, stekao je reputaciju kao vodeće VPN rješenje za one koji preferiraju privatnost. U Švedskoj nema zakonskih obaveza za VPN usluge da prikupljaju podatke o internetskom prometu, što Mullvad čini idealnim za zaštitu korisničkih informacija. Nezavisne revizije potvrdile su da Mullvad ne pohranjuje nikakve podatke, a otvaranje računa ne zahtijeva otkrivanje ličnih podataka, pa čak ni mejl-adresu.

Korisnici dobivaju nasumično generiran broj koji služi kao jedini potrebni identifikator za korištenje usluge. Mullvad nudi visoku tehničku opremljenost, uključujući prilagođeni *web* preglednik za rad s Tor mrežom, DNS uslugu, te ekstenzije za *web* preglednike koje integriraju VPN funkcionalnost direktno u preglednik. Uz to, Mullvad nije besplatan; usluga se naplaćuje mjesečno bez obavezujuće pretplate, po cijeni od 5 eura, s mogućnošću plaćanja kriptovalutama za dodatnu anonimnost.

Mullvad je izuzetno preporučljiv za korisnike koji traže garantiranu privatnost i sigurnost *online*, naročito kada se koristi u kombinaciji s Mullvad Browserom koji dodatno pojačava zaštitu.

Tor Browser je vodeći *web* preglednik koji integrira Tor mrežu, omogućavajući korisnicima da ostvare visoku razinu anonimnosti na internetu. Iako je potpuna anonimnost u digitalnom svijetu teško ostvariva, Tor pruža jednu od najboljih dostupnih opcija za zaštitu privatnosti korisnika.

Mreža Tor, poznata kao The Onion Router, sastoji se od brojnih računala (čvorova) diljem svijeta koje većinom vode volonteri. Ovi čvorovi štite korisničke podatke preusmjeravajući internetski promet kroz više slojeva šifriranja, što rezultira složenom mrežom koja zamagljuje izvorne podatke. Svaki paket podataka koji putuje kroz Tor mrežu enkriptiran je i proslijeđen kroz tri nasumično odabrana čvora, gdje se na svakom čvoru skida jedan sloj šifriranja.

Ova metoda osigurava da se korisnikova aktivnost na internetu ne može lako pratiti ili identificirati, čineći Tor Browser popularnim alatom među onima koji teže zaštiti svoje *online* aktivnosti od nadzora i cenzure. Namijenjen je svima koji cijene privatnost, od aktivista i novinara do običnih korisnika koji žele očuvati svoju anonimnost na internetu. **Tails** je specijalizirana *live* distribucija GNU/Linuxa koja se vrši izravno iz radne memorije, nudeći izuzetnu razinu anonimnosti putem integracije s Tor mrežom. Ova distribucija dizajnirana je tako da ne ostavlja nikakve tragove korištenja na računalu nakon što se isključi, čime se maksimizira privatnost korisnika.

Iako je Tails osmišljen da ne pohranjuje nikakve podatke nakon gašenja, korisnici imaju mogućnost da prilikom svakog pokretanja odaberu opciju pohrane promjena na USB memoriji s koje se sustav pokreće. Ovo omogućava fleksibilnost u očuvanju određenih informacija bez kompromitiranja osnovnog principa privatnosti i sigurnosti.

Tails se ističe kao izuzetno koristan alat za one koji traže visoku razinu anonimnosti prilikom pristupa internetu. Iako ni Tails, kao ni bilo koje drugo tehničko rješenje, ne može pružiti potpunu anonimnost, ovaj operativni sistem pruža značajnu razinu zaštite i bliži se idealu maksimalne privatnosti u digitalnom svijetu. Savršen je za situacije gdje je neophodna visoka razina diskrecije, poput novinarskog izvještavanja ili aktivizma u osjetljivim političkim uvjetima.

Fizička sigurnost i kontrola okolinskih faktora

Osiguranje fizičkog pristupa osjetljivim područjima i uređajima Faktori okoline koji utiču na digitalnu sigurnost (npr. temperatura, vlažnost)Planiranje za oporavak nakon katastrofe i kontinuitet poslovanja

Digitalna sigurnost u redakciji ili organizaciji ne odnosi se samo na zaštitu podataka u virtualnom prostoru, već i na fizičku zaštitu uređaja i informacija. Implementacija osnovnih principa može značajno smanjiti rizik od gubitka podataka i kompromitovanja sigurnosti. Neki od ključnih elemenata koji se odnose na fizičku zaštitu uključuju:

Redovne sigurnosne kopije (Backups): Sigurnosne kopije od vitalnog su značaja za zaštitu podataka. Osigurajte da se redovno prave sigurnosne kopije svih važnih podataka i pohranjuju na sigurno mjesto izvan primarnog izvora. Idealno, sigurnosne kopije trebaju biti pohranjene na različitim fizičkim lokacijama kako bi bile zaštićene u slučaju prirodnih nepogoda poput poplava, požara ili provala.

Clean Desk Policy: Politika "čistog stola" nalaže da svi zaposlenici na kraju radnog dana uklone sve osjetljive dokumente i uređaje sa svojih radnih površina i pohrane ih na sigurno mjesto. Ova praksa smanjuje rizik od neovlaštenog pristupa informacijama i osigurava da povjerljivi podaci nisu lako dostupni neovlaštenim osobama.

Sigurnosni sefovi i ormari: Osjetljivi uređaji, dokumenti i sigurnosne kopije trebaju biti pohranjeni u zaključanim sefovima ili ormarima kada nisu u upotrebi. Ova mjera dodatno štiti podatke od krađe ili neovlaštenog pristupa.

Pristup kontrolisanim područjima: Ograničite pristup prostorijama gdje se pohranjuju osjetljivi podaci i uređaji samo na ovlaštene osobe. Koristite fizičke barijere poput zaključanih vrata, sigurnosnihkartica ili biometrijskih skenera kako biste osigurali da samo ovlašteni zaposlenici mogu pristupiti tim područjima.

Sigurnosne kamere i alarmni sistemi: Instalacija sigurnosnih kamera i alarmnih sistema može pomoći u prevenciji provala i omogućiti brzu reakciju u slučaju sigurnosnog incidenta. Ovi sistemi djeluju kao odvraćajuće sredstvo za potencijalne napadače i pružaju dodatnu razinu zaštite.

Edukacija zaposlenih: Redovno obučavajte zaposlenike o važnosti fizičke sigurnosti i pravilnim procedurama za zaštitu podataka i uređaja. Osigurajte da su svi svjesni politika i procedura koje se primjenjuju u vašoj redakciji ili kancelariji.

Implementacijom ovih osnovnih principa, redakcija ili kancelarija može značajno unaprijediti svoju digitalnu i fizičku sigurnost, te smanjiti rizik od gubitka podataka i kompromitovanja povjerljivih informacija.

Savjeti za odabir alata i aplikacija za digitalnu sigurnost

1. Lokacija servera:

Pri odabiru alata i aplikacija za digitalnu sigurnost važno je obratiti pažnju na to gdje su bazirani serveri. Serveri smješteni u zemljama s jakim zakonima o zaštiti privatnosti, poput Švicarske ili članica Evropske unije, obično pružaju veću sigurnost i privatnost podataka.

2. Vlasništvo i reputacija kompanije:

Provjerite u čijem su vlasništvu alati i aplikacije koje razmatrate. Kompanije s dugom tradicijom i dobrom reputacijom u oblasti digitalne sigurnosti često nude pouzdanije i sigurnije proizvode. Izbjegavajte alate čiji su vlasnici kompanije poznate po kršenju privatnosti ili koje imaju veze s vladinim nadzorom.

3. Politika privatnosti:

Pročitajte i razumijte politiku privatnosti alata ili aplikacije. Obratite pažnju na to kako kompanija koristi vaše podatke, da li ih dijeli s trećim stranama i u koje svrhe. Idealno, alati i aplikacije trebaju nuditi jasne i transparentne politike koje štite vašu privatnost.

4. End-to-end enkripcija:

Odaberite alate i aplikacije koje nude end-to-end enkripciju. Ova tehnologija osigurava da samo vi i namjeravani primatelj možete pristupiti podacima, čime se značajno smanjuje rizik od presretanja komunikacija ili neželjenog pristupa podacima od strane trećih lica.

5. Open-source kod:

Alati i aplikacije s otvorenim kodom (open-source) omogućavaju zajednici stručnjaka za sigurnost da pregledaju i provjere sigurnost softvera. Ovo doprinosi većoj transparentnosti i sigurnosti jer omogućava brže otkrivanje i ispravljanje eventualnih ranjivosti.

6. Recenzije i preporuke:

Prije nego što odaberete alat ili aplikaciju, provjerite recenzije i preporuke drugih korisnika i stručnjaka za digitalnu sigurnost. Ovo može pružiti vrijedne uvide u stvarne performanse i sigurnost alata.

7. Podrška i ažuriranja:

Odaberite alate i aplikacije koje redovno dobivaju ažuriranja i imaju dobru podršku korisnicima. Redovna ažuriranja ključna su za održavanje sigurnosti jer omogućavaju ispravljanje poznatih sigurnosnih propusta i poboljšanje funkcionalnosti.

Primjenom ovih savjeta možete odabrati alate i aplikacije koje najbolje odgovaraju potrebama vaše organizacije, te osigurati visok nivo zaštite i privatnosti vaših podataka.

Zaključak

Digitalna sigurnost organizacije ključna je za zaštitu njenih podataka, resursa i reputacije u današnjem digitalnom dobu. S obzirom na sve veći broj *cyber* napada i prijetnji, organizacije moraju ozbiljno shvatiti potrebu za efikasnim mjerama digitalne sigurnosti. Pravilno uspostavljeni sigurnosni protokoli i tehnologije pomažu u sprečavanju neovlaštenog pristupa podacima, krađe identiteta, kao i u zaštiti od *ransomwarea* i drugih oblika *malwarea* koji mogu ozbiljno oštetiti poslovanje.

Imati plan za digitalnu sigurnost ključno je za brzo i efikasno reagiranje u slučaju incidenta. Planiranje unaprijed omogućava organizaciji da identificira potencijalne prijetnje, procijeni rizike i postavi jasne procedure za odgovor u slučaju ***cyber*** napada ili kršenja sigurnosti. Ovaj plan također osigurava da su zaposlenici upoznati sa svojim ulogama i odgovornostima, što je ključno za koordinirani i efikasniji odgovor u kriznim situacijama.

Redovno obnavljanje i edukacija zaposlenih ključni su faktori održavanja visokih standarda digitalne sigurnosti organizacije. Digitalna se prijetnja neprestano razvija, stoga je važno da organizacije redovno ažuriraju svoje sigurnosne mjere i tehnologije kako bi ostale korak ispred potencijalnih napadača. Osim toga, kontinuirana edukacija zaposlenika o sigurnosnim praksama i najnovijim prijetnjama osigurava da organizacija ima informirano osoblje koje može prepoznati potencijalne prijetnje i pravilno reagovati u svakodnevnim situacijama koje uključuju digitalnu sigurnost.

U ovom priručniku predstavili smo principe digitalne sigurnosti i trenutno raspoložive alate za njego sprovođenje u kontekstu malih medijskih organizacija i organizacija civilnog društva. Tehnologija se konstantno mijenja i s njom će doći i novi prijetnje i novi alati, ali ono što ostaje aktualno su glavni principi digitalne sigurnosti tima – oprez, zaštita i kontinuirana edukacija cijelog tima.

Lista dodatnih resursa

Dodatni resursi

Cyber Security Excellence Centre (CSEC)

Centar za izvrsnost u cyber sigurnosti nudi sistematski odgovor na cyber incidente u Bosni i Hercegovini – analizu prijetnji, dijeljenje informacija, reagovanje na incidente i savjete i podršku za akademske institucije, medijske organizacije i organizacije civilnog društva.

https://www.csec.ba/?lang=bs

CIRT Playbook Battle Cards

Besplatni resurs koji u obliku kartica vašem timu daje instrukcije o koracima za odbranu u situacijama različitih cyber napada.

https://www.csec.ba/guidelines-1

SHARE Cybersecurity Toolkit

Online alat za infomacije o pitanjima i dilemama iz digitalne sigurnosti koji je kreirala Fondacija Share iz Srbije. Sadržaj platforme je podijeljen u dvije kategorije: rješavanje problema i edukacija i korisnika korak po korak vodi kroz glavne probleme i vrste incidenata.

https://toolkit.sharecert.rs/sr/

CERT.hr

Nacionalno tijelo za prevenciju i zaštitu od prijetnji cyber sigurnosti javnih informacijskih sistema u Republici Hrvatskoj. Nudi bazu znanja u obliku brošura, prezentacija, infografika, dokumenata i drugih resursa iz digitalne sigurnosti.

https://www.cert.hr/

CERT.rs

Nacionalni CERT Republike Srbije redovno objavljuje najnovije informacije o cyber incidentima i novim sigurnosnim ažuriranjima online sevisa.

https://www.cert.rs/rs

Security in-a-box

Online resurs koji su za aktiviste i organizacije civilnog društva kreirali Front Line Defenders i Tactical Technology Collective. Nudi praktične savjete iz digitalne sigurnosti i detaljne vodiče za instalaciju različitih softvera za digitalnu sigurnost. Dostupno na engleskom jeziku.

https://securityinabox.org/en/

Digital Safety Kit

Vodič za digitalnu sigurnost novinara i novinarki koji održava Komitet za zaštitu novinara. Nudi detaljna uputstva za digitalnu sigurnost pri izvještavanju i alat za procjenu rizika.

https://cpj.org/2019/07/digital-safety-kit-journalists/

Annex 1:
Politika digitalne sigurnosti*

**Ovaj predložak pruža osnovne elemente koje treba uključiti u politiku digitalne sigurnosti za organizacije civilnog društva i male medijske organizacije. Prilagodite ga prema specifičnostima i potrebama vaše organizacije.*

1. Uvod

1.1. Svrha

Ova politika uspostavlja okvir za upravljanje digitalnom sigurnošću u našoj nevladinoj organizaciji (NVO). Cilj je zaštititi povjerljive podatke, digitalne resurse i osigurati kontinuitet rada organizacije.

1.2. Opseg

Ova politika se primjenjuje na sve zaposlene, volontere, konsultante i druge osobe koje imaju pristup informacijskim sistemima i podacima organizacije.

2. Odgovornosti

2.1. Menadžment/upravni odbor

Odgovoran za usvajanje politike digitalne sigurnosti i nadzor nad njenom primjenom.

2.2. IT stručnjak/inja ili predstavnik/ca za digitalnu sigurnost

Zadužen za implementaciju, održavanje i redovitu reviziju politike digitalne sigurnosti.

2.3. Zaposleni i suradnici

Svi korisnici informacijskih sustava su odgovorni za pridržavanje ove politike.

3. Upravljanje pristupom

3.1. Korisničke ovlasti

Pristup sustavima i podacima će biti ograničen na osnovu potreba za obavljanjem posla.

3.2. Autentifikacija

Svi korisnici moraju koristiti jake lozinke koje se redovito mijenjaju.

3.3. Pristup logovima

Redovito se prate i analiziraju logovi pristupa radi otkrivanja i sprječavanja neovlaštenih aktivnosti.

4. Zaštita podataka

4.1. Šifriranje

Povjerljivi podaci se moraju šifrirati tokom prenosa i skladištenja.

4.2. Sigurnosne kopije

Redovite sigurnosne kopije podataka se moraju praviti i čuvati na sigurnom mjestu.

4.3. Upravljanje mobilnim uređajima

Mobilni uređaji koji imaju pristup povjerljivim podacima moraju imati odgovarajuće sigurnosne mjere (npr. šifriranje, daljinsko brisanje podataka).

5. Sigurnosni incidenti

5.1. Prijavljivanje incidenta

Svi sigurnosni incidenti se moraju odmah prijaviti IT menadžeru/predstavniku za digitalnu sigurnost.

5.2. Odgovor na incident

IT menadžer i/li predstavnik za digitalnu sigurnost/predstavniku za digitalnu sigurnost će istražiti incident, poduzeti potrebne mjere za sanaciju i izvijestiti upravni odbor.

5.3. Dokumentacija i revizija

Svi incidenti se moraju dokumentovati i redovno analizirati radi poboljšanja sigurnosnih mjera.

6. Obuka i svijest

6.1. Redovita obuka

Svi zaposleni i volonteri će redovito sudjelovati u obuci o digitalnoj sigurnosti.

6.2. Podizanje svijesti

Organizacija će provoditi kampanje za podizanje svijesti o važnosti digitalne sigurnosti.

7. Revizija politike

7.1. Periodična revizija

Politika digitalne sigurnosti će se redovito pregledavati i ažurirati kako bi se osigurala njena usklađenost s promjenama u tehnološkom okruženju.

7.2. Povratne informacije

Zaposleni i volonteri se potiču da daju povratne informacije o politici kako bi se kontinuirano poboljšavala.

8. Pridržavanje i sankcije

8.1. Pridržavanje

Svi korisnici informacijskih sistema i uređaja moraju se pridržavati ove politike.

8.2. Sankcije

Kršenje politike digitalne sigurnosti može rezultirati disciplinskim mjerama, uključujući i raskid radnog odnosa.

Datum usvajanja:

_____

Potpis:

_____

Ime i Prezime, Pozicija

_____

Annex 2:
Interni obrazac za prijavu incidenta iz cyber sigurnosti*

**Ovo je obrazac kakav možete koristiti da uspostavljene interne strukture informišete o cyber incidentu. On treba biti ispunjen i dostavljen zaduženim osobama u organizaciji što je prije moguće nakon otkrivanja incidenta kako bi se omogućilo pravovremeno istraživanje i sprovele odgovarajuće mjere.govarajuće mjere.*

1. Osnovne informacije

Ime i prezime podnositelja prijave:

Datum prijave:

Kontakt (email/telefon):

Odjel/Tim:

2. Detalji incidenta

Datum i vrijeme incidenta:

Lokacija (fizička ili mrežna):

Opis incidenta:

(Detaljno opišite što se dogodilo, uključujući sve relevantne informacije i kontekst)

3. Tip incidenta (označite sve što je primjenjivo)

- ☐ Phishing napad
- ☐ Malware infekcija
- ☐ Ransomware napad
- ☐ Neovlašteni pristup
- ☐ DDoS napad
- ☐ Gubitak uređaja
- ☐ Ostalo (molimo specificirajte):

4. Pogođeni sistemi/podaci

Pogođeni uređaji/sistemi (računala, serveri, mrežna oprema itd.):

Osjetljivi podaci koji su možda kompromitirani (osobni podaci, finansijski podaci, intelektualno vlasništvo itd.):

5. Poduzete akcije

Mjere poduzete odmah nakon otkrivanja incidenta:

(Isključivanje uređaja s mreže, promjena lozinki, kontaktiranje IT tima itd.)

Dodatne akcije (ako ih ima):

6. Prilozi i dokazi

Priloženi dokazi (logovi, snimke zaslona, e-mailovi, poruke itd.):

(Molimo priložite sve relevantne dokaze koji mogu pomoći u istraživanju incidenta)

7. Kontakt za dodatne Informacije

Osoba za kontakt (ako je drugačija od podnositelja prijave):

Kontakt podaci (email/telefon):

8. Dodatne napomene

Dodatni komentari ili informacije koje mogu biti korisne:

Annex 3:
Osnovni nivo sigurnosti za novinarske redakcije

U današnjem digitalnom dobu, novinarske redakcije se suočavaju s brojnim izazovima u vezi sa zaštitom osjetljivih informacija, ali i u vezi s osnovnim integritetom novinara. Osiguravanje osnovnog nivoa sigurnosti ključan je korak za očuvanje integriteta podataka i zaštitu izvora. Ovaj primjer predstavlja set alata i procedura koji mogu pomoći redakcijama i novinarima da unaprijede svoju sigurnost i zaštite prikupljene informacije prije, tokom i poslije rada na terenu.

Prije rada na terenu

Sigurnosne mjere

- **Dvofaktorska autentifikacija (2FA)**:
  Implementacija 2FA na svim važnim računima (e-mejl, društvene mreže, cloud servisi) značajno povećava nivo sigurnosti.
- **Redovno ažuriranje softvera**:
  Softver, uključujući operativne sisteme i aplikacije, treba redovno ažurirati kako bi se zaštitili od poznatih sigurnosnih propusta. Ne krećite na teren ukoliko niste ažurirali operativne sisteme i aplikacije koje koristite na najnovije dostupne verzije.
- Šifriranje **osjetljivih podataka**:
  Prije pohrane, osjetljive podatke treba šifrirati koristeći alate kao što su VeraCrypt ili BitLocker. Ukoliko na teren idete sa uređajima na kojima već postoje neke osjetljive informacije, dobro bi bilo da ih šifrirate.
- **Automatizovane sigurnosne kopije**:
  Postavite automatizovane sigurnosne kopije važnih datoteka na eksternim hard diskovima ili *cloud* servisima kao što su Google Drive ili Dropbox, uz šifriranje podataka.

Planiranje i priprema na nivou redakcije

- **Identifikacija prijetnji:** Identifikujte najvjerovatnije prijetnje i ranjivosti u vašim sistemima.
- **Obuka zaposlenih:** Redovno obučavajte zaposlenike o najboljim praksama digitalne sigurnosti.

Tokom rada na terenu

Alati za sigurnu komunikaciju

Signal: Koristite Signal za enkriptovane tekstualne poruke i pozive.

ProtonMail: Za sigurnu elektronsku poštu koristite ProtonMail, sa ***end-to-end*** enkripcijom.

VPN: Koristite VPN (npr. Mullvad VPN) za zaštitu internetske veze i anonimnost prilikom surfanja.

Napomena: *ovo je samo preporuka, postoje mnoge aplikacije koje se bolje uklapaju u različite kontekste rada, neke od njih smo naveli u tekstu.*

Sigurnosne prakse

Snažne lozinke: Koristite složene lozinke za sve naloge i redovno ih mijenjajte.

***Firewall* zaštita**: Aktivirajte firewall na svim uređajima kako biste blokirali neautorizovane pristupe.

Segmentacija mreže: Odvojte mrežne segmente za osjetljive podatke kako biste smanjili rizik od neovlaštenog pristupa.

Poslije rada na terenu

Izrada sigurnosnih kopija:
Osigurajte da se svi prikupljeni podaci redovno kopiraju i šifriraju.

Zaključak

Osnovni nivo sigurnosti može značajno smanjiti rizik od digitalnih prijetnji za novinarske redakcije. Primjenom ovih alata i procedura, redakcije mogu bolje zaštititi svoje podatke i izvore, te osigurati kontinuitet i integritet svog rada.

Annex 4: Visok nivo sigurnosti za novinarske redakcije

Uvod

Za novinarske redakcije koje se bave osjetljivim informacijama i istraživačkim novinarstvom, visok nivo siguranosti zaštite podataka je neophodan. Ovaj primjer prikazuje napredne alate i procedure koji osiguravaju veoma visok nivo sigurnosti i povjerljivosti informacija prije, tokom i poslije rada na terenu.

Prije rada na terenu

Napredne sigurnosne mjere

- **Fizička sigurnost uređaja**: Koristite fizičke sigurnosne mjere kao što su sigurnosni sefovi za pohranu osjetljivih uređaja.
- **Korištenje Tails OS:** Za rad sa visoko osjetljivim informacijama koristite Tails operativni sistem koji ne ostavlja tragove na korištenim uređajima.
- **Hardware Security Modules (HSM):** Koristite HSM za šifriranje i pohranu kriptografskih ključeva.
- **NAPREDNE KOPIJE (BACKUP):** Koristite RAID tehnologije za redundanciju podataka i redovne offline sigurnosne kopije.

Detaljno planiranje i procjena

- **Izrada plana za hitne slučajeve:** Detaljan plan za postupanje u slučaju sigurnosnog incidenta, uključujući evakuaciju podataka i krizne komunikacije.
- **Obuka za sigurnost:** Napredne obuke za sve zaposlene o prepoznavanju i odgovoru na sofisticirane prijetnje.

Tokom rada na terenu

Visoko sigurnosni alati

- **Session:** Koristite Session za anonimne i enkriptovane komunikacije bez potrebe za telefonskim brojem ili emejlom.
- **Tella:** Koristite Tella za sigurno prikupljanje i pohranjivanje dokaza o kršenju ljudskih prava, uz mogućnost skrivanja aplikacije na uređaju.
- **Qubes OS:** Za rad sa osjetljivim podacima koristite Qubes OS, koji omogućava izolaciju aplikacija u različitim virtualnim mašinama.

Stroge sigurnosne prakse

- **Višefaktorska autentifikacija (MFA):** Implementirajte MFA sa hardverskim tokenima (npr. YubiKey) za sve kritične sisteme.
- **Napredni firewall i IDS/IPS:** Koristite napredne firewall sisteme i IDS/IPS za praćenje i zaštitu mrežnog prometa.
- **Izolacija uređaja:** Koristite uređaje koji su fizički izolovani od mreže (air-gapped) za rad s najosjetljivijim podacima.

Poslije rada na terenu

- **Kontinuirano praćenje:** Implementirati sisteme za kontinuirano praćenje svih mrežnih i sistemskih aktivnosti.
- **Redovno testiranje sigurnosti:** Sprovoditi redovne penetracione testove i sigurnosne revizije kako bi se otkrile i ispravile ranjivosti.

Zaključak

Visok nivo sigurnosti zaštite je ključan za redakcije koje se bave visoko osjetljivim informacijama. Primjenom ovih naprednih alata i procedura, redakcije mogu osigurati maksimalnu sigurnost i povjerljivost svojih podataka i izvora, te zaštititi svoje novinare od potencijalnih prijetnji.

Annex 5:
Primjer programa praktične obuke osoblja iz digitalne sigurnosti organizacije*

**Program se može prilagoditi specifičnim potrebama organizacije i razini tehničkog znanja osoblja. Praktične vježbe su ključne za osiguranje razumijevanja i primjene naučenih praksi u stvarnim situacijama i mogu se razviti u saradnji sa stručnjacima za digitalnu sigurnost.*

Prvi dio

| Uvod

- Uvodna riječ i predstavljanje predavača
- Pregled ciljeva obuke

| Osnove digitalne higijene

- Uvod u koncept digitalne higijene
- Važnost digitalne higijene za nevladine i medijske organizacije
- Primjeri posljedica loših praksi digitalne sigurnosti

| Sigurnosne lozinke

- Kako kreirati jake i jedinstvene lozinke
- Korištenje upravitelja lozinki (Password Manager)
- Praktična vježba: Kreiranje i provjera sigurnosti lozinki

Drugi dio

| Ažuriranja i sigurnosne zakrpe

- Važnost redovnog ažuriranja softvera i operativnih sistema
- Automatizacija ažuriranja
- Praktična vježba: Provjera i instalacija najnovijih ažuriranja

| Sigurno korištenje e-maila

- Prepoznavanje phishing napada
- Sigurnosne prakse pri otvaranju priloga i linkova
- Praktična vježba: Identifikacija lažnih e-mailova

Treći dio

| Sigurno korištenje interneta

- Sigurno pretraživanje interneta i prepoznavanje sumnjivih web stranica
- Korištenje VPN-a za sigurnu vezu
- Praktična vježba: Konfiguracija i korištenje VPN-a

| Upravljanje osjetljivim podacima

- Enkripcija fajlova i uređaja
- Sigurnosne kopije podataka
- Praktična vježba: Enkripcija i sigurnosno kopiranje fajlova

Četvrti dio

| Sigurno korištenje mobilnih uređaja

- Sigurnosne postavke za pametne telefone i tablete
- Korištenje dvofaktorske autentifikacije (2FA)
- Praktična vježba: Postavljanje 2FA na mobilnim uređajima

| Prepoznavanje i prijava incidenta

- Kako prepoznati sigurnosni incident
- Postupak prijave incidenta unutar organizacije
- Praktična vježba: Simulacija prijave incidenta

| Zaključci i Q&A

- Sažetak ključnih tačaka obuke
- Pitanja i odgovori sudionika
- Evaluacija obuke i povratne informacije