NDN

SADRŽAJ

Poglavlje 1: Uvod u digitalnu bezbednost 4

1.1. Zašto je digitalna bezbednost važna 4
1.2. Pregled čestih digitalnih pretnji u novinarstvu (DDoS, fišing, malver) 4

Poglavlje 2: Osnove digitalne bezbednosti 6

2.1. Upravljanje lozinkama 6
Kreiranje snažnih lozinki 6
Prednosti dvostruke autentifikacije (2FA) 7

2.2. Bezbedno pretraživanje interneta 7
Identifikacija bezbednijih veb brauzera (Firefox, Brave, Tor) 7
Dodaci za brauzere 8
Incognito mode - prednosti i mane 8
VPN 8

Poglavlje 3: Bezbednost komunikacije 10

3.1. Aplikacije za enkriptovane poruke 10
End-to-end enkripcija 10
Aplikacije za četovanje sa E2EE po difoltu 10
Šta još treba uzeti u obzir 11

3.2. Bezbedna mejl komunikacija 11
End-to-end enkripcija (E2EE) za mejlove 12
Pretty Good Privacy (PGP) 12
Mejl provajderi sa E2EE po difoltu 13

3.3. Kako prepoznati fišing mejlove 14
Vrste fišing mejlova 14
Analiza mejlova 15
Korisni alati 17

Poglavlje 4: Zaštita vaših uređaja i naloga 18

4.1. Bezbednost uređaja 18
Bezbednost računara 18
Bezbednost mobilnih telefona 20

4.2. Tails operativni sistem 23
Ključne karakteristike Tails-a 23
Kako koristiti Tails? 23
Dodatne napomene kako Tails funkcioniše 24

„Ова публикација објављена је уз финансијску помоћ Европске уније. За садржину ове публикације искључиво је одговорно Независно друштво новинара Војводине и та садржина нипошто не изражава званичне ставове Европске уније”.

SADRŽAJ

4.3. Bezbednost na društvenim mrežama 24
Pregled pretnji 24
Ključne smernice za bezbednost na društvenim mrežama 25

Poglavlje 5: Pravljenje rezervnih kopija 27
Opcije za bekap 27
Pravilo za bezbedan bekap 28
Dodatne smernice za bezbednost bekapa 28

Poglavlje 6: Bezbednost vebsajtova 29

6.1. Odabir hostinga 29
Hostovanje veb sajta 29
Šta tražiti kod pružaoca hostinga 29

6.2. Zaštita od DDoS napada 29
Hosting za aktere od javnog interesa 30
Dobre prakse održavanja sajtova 30

Poglavlje 7: Bezbednosne politike i procedure 32
Primer Politike lozinki 33
Primer Politike e-pošte i naloga 33
Primer Bezbednosnog plana 34

Poglavlje 8: Zaključak 37

8.1. Pregled brzih preporuka za digitalnu bezbednost 37
8.2. Pomoć u reagovanju na incidente 39

Dodatni resursi 40

POGLAVLJE 1: UVOD U DIGITALNU BEZBEDNOST

1.1. Zašto je digitalna bezbednost važna

Sve više informacija i procesa kojima smo okruženi se digitalizuje i u takvim okolnostima sajber kriminal je u porastu, a pored toga su znatno povećane sposobnosti državnih i korporativnih aktera da sprovode špijunažu i druge sajber operacije. Sve ovo dovodi do toga da su novinari, aktivisti i uzbunjivači kao akteri od javnog interesa pod ogromnim pritiskom kada je u pitanju ne samo fizička već i sajber bezbednost. “Obaranje” sajtova medija u Srbiji i regionu je česta pojava, a krajem 2023. su otkriveni pokušaji da se telefoni predstavnika civilnog društva zaraze naprednim špijunskim softverom.

Bilo koji sigurnosni rizik može izazvati velike probleme za organizaciju, kao što su kompromitacija, krađa ili gubitak podataka, prekid rada, finansijska šteta, reputaciona šteta itd. U tom pogledu, postoji nekoliko opštih faktora rizika kada je reč o digitalnoj bezbednosti:

- Pojedinačni: zaposleni koji na primer koriste slabe lozinke i istu lozinku za više naloga;
- Organizacijski: nepostojanje organizacione koordinacije ili zajedničke politike digitalne bezbednosti;
- Tehnički: korišćenje zastarelog ili ranjivog softvera i hardvera;
- Politički: zemlja ili region gde vladajuće strukture vrše pritisak na civilno društvo, novinare ili opoziciju i napadaju ih;
- Socio-kulturološki: društvo u kome postoji uopšteno nizak nivo bezbednosne kulture, što se prenosi i na digitalno okruženje.

Uzimajući u obzir značaj digitalne bezbednosti, da bi se pripremila i efikasnije upravljala rizicima u digitalnom okruženju, organizacija može da preduzme nekoliko važnih koraka:

- Tehničke mere: korišćenje alata za enkripciju, upravljanje lozinkama, itd;
- Organizacione mere: usvajanje i implementacija internih politika i procedura;
- Podizanje svesti i edukacija: pružanje obuke, uključivanje u kampanje, izgradnja organizacione bezbednosne kulture.

U narednim poglavljima ćemo predstaviti ključne savete, alate i prakse kada je reč o digitalnoj bezbednosti, posebno u kontekstu novinarskog rada.

1.2. Pregled čestih digitalnih pretnji u novinarstvu (DDoS, fišing, malver)

Pretnje po sajber bezbednost odnose se na mogućnost sajber napada koji će rezultirati krađom podataka, finansijskim ili operativnim gubicima, reputacionom štetom i tome slično. Sajber napadi se izvode različitim metodama, najčešće kombinacijom tehnika socijalnog inženjeringa i tehničkog znanja i veština napadača.

Kao česte digitalne pretnje po novinarski rad, za potrebe ovog priručnika razmotrićemo DDoS, fišing i ransomver kao primer napada malverom.

DDoS (Distributed Denial of Service) је најчешће коришћен начин за "рушење" servera. Napad se vrši tako što se na server šalje veliki broj zahteva na koje ne može da odgovori i jednostavno prestaje da radi, te samim tim sajt koji je hostovani na njemu postaje nedostupan. Nakon što napad prestane, u većini slučajeva server i sajt rade normalno. Sajtovi medija se često susreću sa DDoS-om: u Srbiji su tokom 2023. godine sajtovi Južnih vesti, agencije JugPress, Demostata i RTS-a bili pod ovom vrstom napada.

Najbolje prakse zaštite uključuju pokretanje analize internet saobraćaja i identifikaciju zlonamernog saobraćaja ili znakova upozorenja, plan odgovora u slučaju DDoS napada, korišćenje klaud usluga, kao i servisa za zaštitu od DDoS kao što je Cloudflare.

Fišing (phishing) je vrsta napada putem lažnih mejlova koje izgledaju zaista autentično i navodno dolaze iz pouzdanog izvora ili od nekoga ko je na poziciji autoriteta. Od primaoca se zatim traži da otvori fajl u prilogu ili klikne na link u mejlu kako bi uradio nešto veoma važno. Međutim, kada se preuzme i otvori fajl ili klikne na link, najčešće se pokreće maliciozni program (malver) koji ugrožava bezbednost vašeg uređaja i informacija. Fišing poruke postaju sve sofisticiranije i zbog toga je ključno obučiti zaposlene kako da ih prepoznaju, označe kao neželjenu poštu (spam/junk) i obrišu. U nastavku priručnika ćemo u posebnom odeljku pružiti više detalja kako se mogu prepoznati fišing poruke.

"Spearing" ili "spear phishing" je vrsta fišinga gde napadač cilja određenog pojedinca ili grupu ljudi unutar organizacije i prilagođava poruke prema imenu, poziciji, kompaniji, službenom broju telefona i drugim informacijama kako bi prevario primaoca da poveruje da postoji povezanost sa njim. "Spear phishing" je uobičajena pojava na sajtovima društvenih mreža kao što je LinkedIn gde napadači mogu da koriste više izvora podataka da bi napravili mejlove za ciljani napad. Mete ove vrste fišinga su obično zaposleni u HR, pravnoj službi ili finansijama, kao i ljudi na rukovodećim pozicijama.

Malver (malware) je opšti termin za softver koji se koristi za ometanje rada računara, prikupljanje osetljivih informacija ili dobijanje pristupa zaštićenom informacionom sistemu. Ovu vrstu softvera kreiraju i koriste sajber kriminalci i drugi zlonamerni akteri, u nekim slučajevima čak i države, kako bi naškodili informacionom sistemu i/ili ukrali informacije iz njega. Malver može da zarazi sistem na brojne načine: preuzimanjem priloga poslatih mejlom ili sa malicioznih sajtova, instalacijom naizgled legitimnih programa ili dodataka, itd. Zato je važno koristiti pouzdan antimalver softver i redovno vršiti skeniranje uređaja, ali i obučiti zaposlene da budu obazrivi sa preuzimanjem i otvaranjem fajlova iz sumnjivih ili nepoznatih izvora.

Ransomver je naročito opasan oblik malvera koji šifruje (enkriptuje) datoteke na uređajima tako da se datotekama ne može pristupiti bez ključa za dešifrovanje. Napadači zatim traže isplatu "otkupa" u kriptovaluti kako bi pogođenim metama dali ključ za dešifrovanje, obično u kratkom vremenskom okviru da bi izvršili veći pritisak. Opšti savet je da se otkup ne plaća jer se na taj način podstiče dalje vršenje ovih krivičnih dela i finansiraju sajber kriminalci. U slučaju incidenta, najbolja zaštita od ransomvera je redovno pravljenje rezervnih kopija podataka iz kojih se mogu povratiti podaci.

POGLAVLJE 2: OSNOVE DIGITALNE BEZBEDNOSTI

2.1. Upravljanje lozinkama

Lozinke su ključ našeg digitalnog identiteta i zbog toga je važno da budu dovoljno jake da se ne mogu lako pogoditi ili "probiti" tehničkim metodama. Takođe, lozinke predstavljaju prvu liniju odbrane od pretnji i malicioznih aktera u digitalnom prostoru. Ciljevi napada na lozinke, kao i kod svakog sajber napada, mogu biti raznovrsni, npr. krađa ličnih ili organizacionih podataka, šteta po ugled, prodaja pristupnih kredencijala trećim licima, ucena itd. U nastavku ćemo predstaviti ključne savete kada je reč o kreiranju i rukovanju lozinkama.

Kreiranje snažnih lozinki

Tri elementa koja se ističu kod pouzdanih ili snažnih lozinki su:

- **Dužina:** što je lozinka duža, protivniku je teže da je pogodi ili probije. Preporučuje se da imate lozinku sa više od 10 ili čak više od 20 karaktera, što duža to bolje;
- **Jedinstvenost:** možda je najčešća nebezbedna praksa kada je reč o loznikama korišćenje iste lozinke za više naloga. Ponavljanje lozinki je veliki problem jer to znači da kada je kompromitovan samo jedan nalog, ranjiv je i svaki drugi nalog koji koristi istu lozinku, što može u velikoj meri povećati uticaj jedne greške ili povrede podataka;
- **Nasumičnost:** čak i ako je lozinka duga, nije dobro ako je to nešto što napadač može lako da pogodi ili sazna o vama. Izbegavajte informacije kao što su datum i mesto rođenja, devojačko prezime ili bilo koje druge činjenice koje bi neko mogao da sazna o vama brzom internet pretragom. Umesto toga, prilikom kreiranja lozinke savetuje se kombinacija različitih tipova karaktera, kao što su cifre, mala i velika slova i specijalni znakovi (interpunkcija, zvezdica, procenat, valute i sl).

Sa toliko naloga koji prosečan korisnik interneta ima danas, postalo je nemoguće zapamtiti sve lozinke i da one budu jedinstvene, dugačke i složene u isto vreme. Zbog toga bi trebalo da koristite posebne aplikacije poznate kao menadžeri lozinki (password managers), koje bezbedno čuvaju vaše kredencijale i štite ih glavnom lozinkom (master password). Na taj način, neophodno je samo da zapamtite svoju glavnu lozinku i možete da kopirate/nalepite svoje kredencijale direktno iz aplikacije. Menadžeri lozinki vam takođe omogućavaju da bezbedno generišete kvalitetne lozinke za nove naloge.

Aplikacije koje se obično preporučuju za upravljanje lozinkama su KeePass, KeePassXC i Bitwarden - svi su besplatna rešenja otvorenog koda. Dok su prva oflajn, tj. rade sa bazama lozinki samo na lokalnom uređaju, Bitwarden ima prednost jer je klaud aplikacija, što znači da se vašem trezoru lozinki može pristupiti sa drugog računara ili mobilnog uređaja. Više o menadžerima lozinki možete pročitati na sajtu SHARE Fondacije.

Prednosti dvostruke autentifikacije (2FA)

Koliko god da je vaša higijena lozinki dobra, dešava se da napadači uspeju da dođu do lozinke. Zaštita vaših naloga od današnjih pretnji zahteva još jedan sloj zaštite. Ovde dolazi na red dvostruka autentifikacija (2FA).

Dvostruka autentifikacija znači da je potrebna kombinacija dva metoda potvrde identiteta pre nego što se odobri pristup nalogu. Njena implementacija se svodi na potvrdu uspešnog pokušaja prijavljivanja lozinkom pomoću dodatne informacije ili sredstva identifikacije.

Postoje tri raširena tipa 2FA:

- **Bezbednosni ključevi:** korisnik je dodatno autentifikovan pomoću fizičkog USB fleš uređaja. To je najbezbedniji metod jer da biste pristupili nalogu potrebna vam je i lozinka i pristup fizičkom uređaju;
- **Aplikacije za autentifikaciju:** mobilne aplikacije za autentifikaciju, kao što je Google Authenticator ili Aegis Authenticator, automatski generišu jednokratne kodove;
- **Jednokratni SMS kodovi:** najčešći tip 2FA, ali najmanje bezbedan jer se SMS može lako presresti zbog nepostojanja enkripcije, a postoji i mogućnost tzv. napada zamenom SIM kartice (“SIM swapping”) kada napadač tehnikama socijalnog inženjeringa prevari osoblje vašeg mobilnog operatora da mu izda novu karticu sa vašim brojem telefona na koji stižu bezbednosni kodovi.

Jedan od najvećih nedostataka 2FA jeste činjenica da uglavnom na servisima i platformama nije podešena po difoltu, a iako je veliki provajderi onlajn usluga poput Mete, Gugla ili X podržavaju, i dalje postoje brojni sajtovi na kojima ne postoji ta mogućnost. Takođe, neiskusnim korisnicima je nezgodno da pronađu ovo podešavanje, pošto se uglavnom nalazi u odeljku bezbednosti naloga koji uglavnom nisu jednostavno dostupni. Instrukcije kako da podesite 2FA na raznim platformama možete pronaći u ovom tekstu.

2.2. Bezbedno pretraživanje interneta

Identifikacija bezbednijih veb brauzera (Firefox, Brave, Tor)

Internet oglasi, osim što su veoma dosadni i predstavljaju pretnju našoj privatnosti, takođe mogu uticati na našu onlajn bezbednost. Sajber kriminalci targetiraju korisnike skrivanjem zlonamernog koda ili malvera u reklamama i pop-ap prozorima koje inače deluju legitimno. Napadači pronalaze sofisticirane načine da vas navedu da kliknete na zlonamerni oglas kako bi zarazili vaš uređaj malverom. U tom pogledu, dobra praksa je blokirati što više oglasa je moguće.

Neželjene oglase i pop-ap prozore možete jednostavno blokirati korišćenjem nekih od bezbednijih veb brauzera:

- Firefox: brauzer neprofitne organizacije Mozila, ima dobre inicijalne postavke kada je reč o zaštiti privatnosti, koje se mogu proširiti brojnim dodacima (add-ons) iz kolekcije;

- Brave: pogodan za one koji su navikli na Chrome interfejs (razvijen na njegovoj osnovi) a ne žele da ih Gugl konstantno prati, ima ugrađen bloker oglasa, kompatibilan sa dodacima iz Chrome Web Store;
- Tor Browser: prilagođena verzija Firefox brazera, omogućava vam da se povežete na Tor mrežu i pristupite .onion sajtovima, obezbeđuje anonimnost dodelom nasumične IP adrese i čuva internet saobraćaj enkripcijom, nezaobilazan alat u uslovima internet cenzure i nadzora.

Dodaci za brauzere

Kompanije koje razvijaju internet brauzere, drugi pružaoci internet usluga ili zajednice entuzijasta kreiraju tzv. dodatke (add-ons) kojima se mogu proširiti funkcionalnosti brauzera, a koje je moguće instalirati kroz specijalizovane onlajn prodavnice.

Dodaci koji se preporučuju za poboljšanje privatnosti i bezbednosti su sledeći:

- **uBlock Origin:** Besplatan bloker oglasa otvorenog koda. Takođe štiti od malvera tako što ima listu poznatih izvora, tako da ih takođe automatski blokira.
- **Privacy Badger:** blokira trekere koji su ugrađeni u veb sajtove (Meta Pixel, Google Analytics) a koji su nevidljivi redovnom korisniku.
- **MinerBlock:** blokira potencijalne kriptomajnere na sajtovima koji koriste resurse vašeg računara radi rudarenja kriptovaluta.

Sa instalacijom dodataka za brauzer treba biti veoma oprezan, imajući u vidu da mogu biti maliciozne prirode, npr. kreirani da iz brauzera pokupe korisničke kredencijale za pristup sajtovima.

Incognito mode - prednosti i mane

Jedan od mitova o inkognito režimu (tj. “incognito mode”, “private window”) brauzera je da vas čini zaista anonimnim na internetu i da vaše aktivnosti čuvaju u tajnosti. Međutim, realnost je da inkognito režim samo briše vašu istoriju lokalno i uklanja kolačiće kada završite sesiju, odnosno zatvorite inkognito prozor. Sve druge mogućnosti za praćenje vašeg onlajn ponašanja ostaju na stolu, naročito kada se uzme u obzir raširenost već spomenutih trekera koje kompanije koriste da bi prikupile što više podataka o posetiocima sajtova, kao što su Google Analytics ili Meta Pixel. Takođe, ukoliko koristite brauzer u inkognito modu ali bez dodatnih mera anonimnosti, identifikatori poput vaše IP adrese ne ostaju sakriveni već se potencijalno mogu dovesti u vezi sa vama.

Prednost inkognito prozora je da na jednostavan način možete pristupiti sajtovima za koje ne želite da ostanu u istoriji poseta ili ukoliko koristite uređaj ili nalog koji nije vaš. Ukoliko se radi o osetljivim aktivnostima ili informacijama, recimo u vezi sa novinarsko-istraživačkim radom, neophodno je da se koriste alati poput Tor Browser-a ili VPN konekcije.

VPN

Često spominjan kao važan alat za očuvanje privatnosti i anonimnosti na internetu, korišćenjem usluga virtuelne privatne mreže (VPN) vaš internet saobraćaj je enkriptovan i usmeravan kroz infrastrukturu vašeg VPN provajdera pre nego što se povežete na vebsajt ili drugu onlajn uslugu,

што значи да su vaš saobraćaj i IP adresa zaštićeni. VPN vam pomaže da zaobiđete geoblokiranje sadržaja i mere državne cenzure i nadzora interneta, kao i da ostvarite barem nešto onlajn anonimnosti promenom vaše IP adrese, jer povezivanjem na VPN, slično kao kod Tor Browser-a, dobijate “maskirnu” IP adresu koja krije pravi identifikator vaše internet konekcije.

Prilikom odabira VPN provajdera treba da obratite pažnju na nekoliko stvari:

- Vodite računa u kojoj državi je sedište kompanija i da li u toj jurisdikciji važe visoki standardi zaštite podataka o ličnosti poput GDPR-a;
- Da li postoje eksplicitne “no logs” politike, što znači da VPN provajder ne evidentira vaš internet saobraćaj;
- Da li provajder redovno vrši nezavisne bezbednosne revizije i da li se o tome mogu pronaći informacije na sajtu kompanije;
- Izbegavajte “besplatne” VPN usluge, jer se njihov biznis model zasniva na prikupljanju vaših podataka.

Neki od preporučenih komercijalnih VPN servisa su Proton VPN i Mullvad VPN. Njihove kompanije se nalaze u Švajcarskoj, odnosno Švedskoj, zemljama sa strogim zakonima o zaštiti podataka, i pružaju brojne korisne opcije. Proton VPN ima besplatan nivo usluge sa ograničenim opcijama, dok Mullvad zahteva plaćanje. Više detalja o funkcionisanju VPN-a možete pronaći na sajtu SHARE Fondacije.

Pitanje koje se često postavlja tiče se razlika između Tora i VPN-a. Ukratko, Tor Browser je besplatan softver otvorenog koda, razvijen od strane neprofitne organizacije, koji vas čini anonimnim zbog nasumičnog rutiranja saobraćaja kroz Tor mrežu. Međutim, samo saobraćaj preko Tor Browser-a je anonimizovan, s tim da postoji izuzetak ako koristite specijalizovani operativni sistem kao što je Tails, o kome ćemo više reći u posebnom poglavlju. Korišćenje interneta Tora je veoma sporo zbog karakteristika Tor mreže i nije predviđeno za zahtevne radnje poput video-striminga.

Kada je reč o VPN-u, korišćenje pouzdanih provajdera zahteva novčanu pretplatu, a postoji i rizik zbog poverenja u pružaoca usluga, npr. da li oni zaista ne vode logove vašeg saobraćaja ili šta bi uradili da im državni organi zatraže podatke. Za razliku od Tor Browser-a, sav saobraćaj na uređaju ide preko VPN-a i manji je uticaj na performanse mreže.

POGLAVLJE 3: BEZBEDNOST KOMUNIKACIJE

3.1. Aplikacije za enkriptovane poruke

U eri u kojoj se digitalna povezanost sve više širi, bezbednost komunikacije postaje ključna tačka fokusa. Ovo poglavlje nudi uvid u enkriptovane čet aplikacije, razotkrivajući njihovu suštinu, funkcionalnosti i niz benefita koje pružaju korisnicima širom sveta. Prvi korak na našem putovanju kroz bezbednost komunikacije je razmatranje koncepta end-to-end enkripcije (E2EE). Ovaj tehnološki stub postavlja temelje za bezbedno deljenje informacija, čime se osigurava da samo pošiljalac i primalac mogu pristupiti sadržaju komunikacije. Pružićemo pregled popularnih čet aplikacija poput Signala, WhatsApp-a i Element-a, kao i pregled važnih elemenata aplikacija koje treba uzeti u obzir.

End-to-end enkripcija

Najpouzdaniju vrstu komunikacije putem čet poruka u pogledu očuvanja integriteta i poverljivosti sadržaja predstavljaju aplikacije koje omogućavaju end-to-end enkripciju (end-to-end encryption, E2EE) bez dodatnih podešavanja, dakle kao podrazumevan način funkcionisanja aplikacije. E2EE čuva poruke u enkriptovanoj formi zaštićene od svih kojima nisu namenjene, uključujući provajdera servisa za razmenu poruka. Pošiljalac je jedan “kraj” komunikacije, a primalac drugi, što će reći da je sadržaj zaštićen enkripcijom u okviru celog procesa komunikacije - na oba kraja, kao i u tranzitu.

Međutim, jedan od problema sa onlajn komunikacijom jeste lažno predstavljanje. Da bi se potvrdio identitet učesnika u E2EE čet komunikaciji, moguće je izvršiti validaciju “otiska prsta”, odnosno kriptografskog potpisa. U enkriptovanim čet aplikacijama se to obično može uraditi kroz verifikaciju uživo tako što skenirate QR kod na telefonu druge osobe i potvrdite njen potpis. Ukoliko nije moguće da uživo potvrdite potpis skeniranjem QR koda, možete poslati niz nasumično generisanih karaktera iz aplikacije drugim sigurnim kanalom komunikacije.

Aplikacije za četovanje sa E2EE po difoltu

Sledi pregled najkorišćenijih E2EE aplikacija za četovanje koje podrazumevano koriste end-to-end enkripciju. Postoje i aplikacije za čet koje imaju E2EE enkripciju, ali nepodrazumevano, poput Telegrama, gde je morate omogućiti korišćenjem funkcije “tajnih razgovora” (secret chat).

Signal

Signal je besplatna i open source aplikacija razvijena od strane nezavisne neprofitne organizacije, što znači da ne sadrži oglase niti trekere unutar aplikacije.

Korisne funkcije aplikacije su samobrišuće poruke, dostupnost i za mobilne uređaje i za desktop, kao i pristup preko proksija (ako je Signal blokiran u određenoj zemlji).

WhatsApp

Kao što verovatno znate, WhatsApp je besplatan za korišćenje, ali je reč o aplikaciji zatvorenog koda čiji je vlasnik Meta. Poseduje korisne funkcije poput samobrišućih poruka, dostupna i za mobilne uređaje i za desktop i pristup preko proksija.

Ipak, bilo šta što je u vlasništvu Meta, matične kompanije Facebook-a, ne pruža zaista osećaj privatnosti, jer je njihov poslovni model zasnovan na monetizaciji podataka korisnika.

Element

Element je besplatno rešenje otvorenog koda za četovanje, izgrađeno na Matrix-u, otvorenoj mreži za bezbednu, decentralizovanu komunikaciju.

Neke prednosti Element-a su:

- Može se samostalno hostovati;
- Jednostavan je za organizacionu implementaciju;
- Postoje besplatne i plaćene verzije.

Šta još treba uzeti u obzir

Prilikom izbora čet aplikacije, treba imati na umu sledeće:

- Pod kojom jurisdikcijom platforma posluje, jer se zakoni o zaštiti podataka o ličnosti i razlikuju od zemlje do zemlje.
- Ko poseduje servere, da li kompanija ima dobar istorijat zaštite privatnosti i bezbednosti korisnika?
- Da li vam je potreban broj telefona ili neki drugi identifikator za registraciju?
- Da li prikupljaju metapodatke, i ako da, u kojoj meri?
- I na kraju, da li redovno sprovode bezbednosne revizije sistema?

Da zaključimo, E2EE aplikacije za čet pružaju siguran i brz način komunikacije, posebno za pozive, ali svaka aplikacija ima svoje prednosti i mane. Naravno, najvažnije je kombinovati i druge sigurnosne mere, posebno u vezi sa mobilnim uređajima.

3.2. Bezbedna mejl komunikacija

U okviru ovog poglavlja objasniće se osnove enkripcije elektronske pošte, istražiti popularne implementacije kao što su Thunderbird mejl klijent i Mailvelope dodatak za webmail interfejs, te otkriti kako ovi alati pružaju korisnicima kontrolu nad bezbednošću njihovih elektronskih prepiski. Proučićemo i dva renomirana pružatelja elektronske pošte, ProtonMail i Tuta, čiji integrisani pristup end-to-end enkripciji automatski podiže nivo bezbednosti i privatnosti.

End-to-end enkripcija (E2EE) za mejlove

Cilj end-to-end enkripcije (E2EE) je zaštita sadržaja elektronske pošte kako pružalac usluga elektronske pošte ili bilo koja druga strana koja bi mogla presresti poruku ne može da otkrije sadržaj, jer ne poseduje enkripcione ključeve. Sadržaj elektronske pošte je vidljiv samo pošiljaocu i primaocu ako poseduju odgovarajuće ključeve, međutim, metapodaci poput vremena i datuma ili mejl adrese pošiljaoca i primaoca se ne enkriptuju.

Da bi E2EE bila primenjena u mejl komunikaciji, potrebno je generisati par ključeva koji zajednički funkcionišu. Jedan ključ je javan i potrebno ga je podeliti javno ili direktno sa osobama s kojima se komunicira, dok je drugi ključ privatni i potrebno ga je čuvati samo za sebe. U slučaju da privatni ključ dospe u ruke nekog zlonamernog aktera, posledica bi mogla da bude dešifrovanje prepiske.

Kao softver za generisanje ključeva i korišćenje enkriptovane elektronske pošte izdvaja se PGP.

Pretty Good Privacy (PGP)

PGP predstavlja skraćenicu za Pretty Good Privacy, što je enkripcioni softver koji postoji od ranih devedesetih godina. Ima mnogo implementacija, a jedna od njenih glavnih prednosti je visoka interoperabilnost, što znači da se E2EE e-pošta može razmenjivati između različitih pružalaca usluga, npr. između Gmail-a i Yahoo-a i obrnuto. PGP je alat koji se često koristi u programima za mejl enkripciju poput Thunderbird-a i Mailvelope-a.

Funkcioniše tako što se prvo potrebno generisati javni i privatni ključ, a potom razmeniti javne ključeve pre slanja enkriptovanih mejlova. Korišćenje ekriptovanih mejlova u suštini nije komplikovano, ali zahteva malo prakse.

Thunderbird

Thunderbird je besplatan mejl klijent otvorenog koda, sa mnogo korisnih opcija. Kada je reč o šifrovanju, ovaj klijent nudi ugrađene mogućnosti za OpenPGP, koji je proistekao iz originalnog PGP-a.

U Thunderbird-u, OpenPGP Key Manager služi za generisanje para ključeva i povezivanja sa vašim mejl nalogom, kao i za čuvanje javnih ključeva osoba sa kojima ste ih razmenili. Proces šifrovanja mejlova je jednostavan: Thunderbird automatski prepoznaje da li imate javne ključeve svih primalaca u poruci, tako da nakon što se jednom razmene javni ključevi enkripcija mejlova funkcioniše automatski.

Mailvelope

Neki ljudi radije koriste webmail intefejs za razmenu e-pošte, jer je to bila glavna platforma za mnoge popularne pružaoce usluga kao što je Gmail. Ukoliko korišćenje posebnog mejl klijenta poput Thunderbird-a malo komplikuje proces, Mailvelope se može instalirati kao dodatak za brauzer. Namijenjen je radu u veb interfejsu i podržava više popularnih pretraživača, kao što su Firefox, Chrome i Edge.

Proces nije previše komplikovan - nakon instalacije Mailvelope dodatka, potrebno je generisati par ključeva ili dodati postojeći. Mailvelope je dostupan besplatno, dok se neke napredne opcije naplaćuju, poput integracije sa Google Workspace i vašim organizacionim mejlom, i dostupne su u Business i Enterprise paketima.

Mejl provajderi sa E2EE po difoltu

Sledi prikaz mejl klijenata koji podrazumevano koriste end-to-end enkripciju za mejlove, što znači da nije potrebno vršiti nikakva dodatna podešavanja - mejl nalog je šifrovan odmah po otvaranju. Međutim, glavna mana je što je enkripcija omogućeno samo za komunikaciju između korisnika istog mejl provajder. Imajući to u vidu, neki od ovih pružalaca nude opcije za slanje enkriptovanog mejla osobi koja koristi drugog pružaoca usluge.

Ovi pružaoci su takođe dobro rešenje za implementaciju na nivou organizacije, budući da pružaju visok nivo poverljivosti za internu mejl komunikaciju i nude širok spektar korisnih opcija, poput postavljanja mejl adresa sa domenom vaše organizacije.

ProtonMail

Verovatno najpoznatiji pružalac usluga za enkriptovane mejlove je ProtonMail, koji je deo paketa usluga koji uključuje enkriptovan kalendar, VPN, cloud skladištenje itd. Kompanija iza ProtonMail-a ima sedište u Švajcarskoj, što znači da je obavezna da se pridržava rigoroznih zakona o zaštiti podataka. Takođe je važno napomenuti da je ProtonMail otvorenog koda, što znači da svako može pregledati kod kako bi pronašao moguće ranjivosti. Postoji opcija za kreiranje besplatnog naloga, koji ima ograničene opcije, ali za napredne korisnike ili one sa dodatnim potrebama postoje opcije koje se naplaćuju i postoje poslovni planovi za organizacije.

Još jedna veoma korisna opcija je mogućnost slanja enkriptovanog mejla osobi koja koristi bilo koji drugi mejl klijent, putem opcije da se mejl zaštiti lozinkom. Pre slanja mejla potrebno je postaviti lozinku, kako bi se mejl enkriptovao i potom je potrebno podeliti tu lozinku sa primaocem mejla putem drugog bezbednog kanala komunikacije (na primer, Signal). Primalac će primiti poruku sa posebnim prozorom gde je potrebno uneti lozinku koju ste podelili s njima kako bi dešifrovali poruku.

Tuta

Tuta (nekada Tutanota) je nemački mejl klijent otvorenog koda za enkriptovanu mejl uslugu, koji takođe pruža enkriptovani kalendar uz vaš nalog. Takođe ima besplatne i plaćene opcije, kao i opciju slanja enkriptovane poruke spoljašnjem primaocu. Ovo funkcioniše vrlo slično kao i ProtonMail-ove poruke zaštićene lozinkom.
Primena end-to-end enkripcije mejlova je veoma pouzdan način zaštite poverljivosti i integriteta mejl prepiske. Postoji mnogo opcija, alči bitno je odrediti šta najviše ogdovara potrebama orgnaizacije i jednostavnom funkcionisanju, zavisno od toga da li biste želeli da pređete na novog pružaoca mejl usluga ili koristite PGP sa trenutnim mejl nalogom. Međutim, ono što je najbitnije jeste da enkripcija mejla nije dovoljna za bezbednost komunikacije, potrebno je da nalozi budu zaštićeni snažnim lozinkama i multifaktorskom autentifikacijom.

3.3. Kako prepoznati fišing napade

Kao dominantno sredstvo komunikacije i razmene dokumenata i informacija, u poslovnom i svakom drugom kontekstu, mejlovi su poslednjih godina sve popularnija metoda za prevare i napade u digitalnom okruženju. Najčešći način zlonamerne upotrebe elektronske pošte je slanje takozvanih fišing mejlova. Uspešni su jer ih je na prvi pogled teško razlikovati od autentičnih mejlova - ime pošiljaoca je isto kao ime kolege s kojim svakodnevno razmenjujete elektronsku poštu, u naslovu se nalazi sadržaj koji vam je poznat. Međutim, otvaranje takvog mejla može biti korak u ozbiljan rizik po vas ili vašu organizaciju.

Zato je važno upoznati se sa nekim osnovnim forenzičkim metodama radi utvrđivanja autentičnosti mejla i identifikacije pošiljaoca. Tehnike za pronalaženje, analizu i interpretaciju informacija koje se nalaze u mejlu pomoći će vam da lakše otkrijete fišing mejl i bezbedno utvrdite da li sadrži maliciozne priloge ili lažan link.

Vrste fišing mejlova

Fišing napadi predstavljaju sajber pretnju koja može da se realizuje ne samo preko e-pošte, već i telefonskim pozivom ili tekstualnom porukom. Napadač se predstavlja kao legitimna institucija ili osoba od poverenja da bi na prevaru izvukao osetljive podatke od svoje potencijalne mete. To mogu biti informacije o identitetu, podaci o bankarskim i kreditnim karticama ili lozinke za pristup zaštićenim resursima preko kojih napadač može da kompromituje uređaje i čitave informacione sisteme. Često se fišing koristi i kao uvod u razne vrste drugih napada u sajber svetu, na primer za ransomver napad ili za instaliranje spajvera (malicioznih programa za špijuniranje uređaja).

Postoje različite vrste zlonamernih e-poruka. Najpre, mogu se klasifikovati u dve velike grupe: targetirani fišing mejlovi i fišing kampanje. U targetirani fišing spadaju namenski sastavljeni mejlovi za ciljane zaposlene određene organizacije da bi se došlo do željenih informacija. Fišing kampanje igraju na masovnost, a mejlovi se sastavljaju tako da mogu da se šalju nasumično, što većem broju ljudi. Targetirane fišing poruke je mnogo teže otkriti, jer su pažljivo sačinjene da deluju autentično, dok je mejlove za masovno slanje lakše prepoznati, jer obično sadrže neke od tipičnih karakteristika. Međutim, u oba slučaja forenzika mejlova je korisna veština.

Tipične karakteristike fišing mejlova:

1. obično se zahteva neka hitna akcija;
2. sadrže ili link ili neki prilog;
3. nedoslednost u imejl adresi pošiljaoca sa imejl adresom osobe ili organizacije koje napadač oponaša;
4. nedoslednost u URL adresama sajtova i domenima;
5. nedoslednost u ekstenzijama dokumenata u prilogu;
6. zahteva se slanje kredencijala, osetljivih podataka, ličnih podataka, podataka o platnim karticama itd.

Analiza mejlova

U forenzici je najbitnije sakupiti sve relevantne i korisne informacije o mejlu koji se istražuje. Ovo uključuje informacije koje su vidljive u pregledu samog mejla: mejl adresa pošiljaoca, datum slanja, naziv i tekst mejla, očekivanost takve poruke. Potom sledi detaljnija analiza i provera svih informacija sadržanih u mejlu - da li su autentične, da li odgovaraju onome što se navodi u mejlu, da li je pošiljalac autentičan, legitiman, odnosno osoba ili institucija za koju se predstavlja. Da bi se utvrdila autentičnost, pregledaju se zaglavlje (header) i sadržaj mejla. Kod zaglavlja se traže nepravilnosti analizom metapodataka, dok se kod sadržaja analizira sam tekst, prilozi, linkovi i drugo.

Analiza zaglavlja (headers)

Važan korak u procesu forenzičke analize e-pošte jeste pregled zaglavlja mejla. Ono sadrži informacije o poruci koje se ne prikazuju direktno u samom telu poruke, kao što su informacije o pošiljaocu, primaocu, vremenu slanja i prijema poruke i putu kojim je poruka prošla pre nego što je stigla do svog krajnjeg odredišta.

U Gmail-u, uključujući e-poštu za bilo koji Google Workspace nalog, celom mejlu se može pristupiti klikom na tri vertikalne tačke u gornjem desnom uglu poruke, a zatim odabirom opcije “Show original”. To će otvoriti novi tab gde se vide zaglavlje i tekst - mada ne uvek ceo tekst (prilozi su ponekad isključeni). U novom tabu možete preuzeti ceo mejl klikom na dugme “Download Original”.

Tipični podaci koji se mogu pronaći u zaglavlju e-pošte:

1. From: Polje u kom se navodi ime i adresa pošiljaoca. U nekim slučajevima, adresa može biti lažna ili promenjena kako bi se prikrio identitet pošiljaoca. Ovo polje se obavezno analizira.
2. To: Ovde se navodi ime i adresa primaoca što može biti značajno za forenzičku analizu jer može ukazati na to koja osoba ili organizacija je potencijalna meta poruke.
3. CC i BCC: Ova polja navode druge osobe koje su dobile kopije poruke. CC (Carbon Copy) se odnosi na javno polje, dok se BCC (Blind Carbon Copy) odnosi na skriveno polje koje primaoci ne vide.
4. Datum i vreme: Ovo polje sadrži trenutak kada poruka poslata ili primljena, što može biti značajno u slučajevima u kojima se vremenski žigovi koriste kao dokazi u istrazi.
5. X-Mailer: Ovde saznajemo koji su programi ili platforme korišćeni za slanje poruke. Takođe nam može pružiti informacije o tipu uređaja koji je korišćen za slanje poruke.
6. Received: Ovo polje navodi sve servere kroz koje je poruka prošla dok je putovala od pošiljaoca do primaoca. Takva informacija može biti značajna za forenzičku analizu, jer može pomoći u identifikaciji lokacija pošiljaoca i primaoca, kao i u identifikaciji servera koji su bili umešani u slanje ili prijem poruke. Ovo polje se obavezno analizira.
7. DKIM-Signature header: DKIM (Domain Keys Identified Mail) je značajno polje,

označava bezbednosni standard koji koristi enkripciju da bi se osiguralo da je mejl stigao od pravog pošiljaoca.

8. Message-ID: Ovo polje sadrži jedinstveni identifikator poruke. Ta informacija može biti korisna u identifikaciji poruke u bilo kojoj fazi istrage.

Kako proveriti domen u mejlu

Pre analize domena, da pogledamo prvo šta čini mejl adresu. Sastoji se iz dva dela: korisničko ime i domen. Napadači često prave korisničko ime i domen tako da liče na proverene izvore. Među načinima manipulacije domenom, najčešća su tri:

1. mogu se koristiti domeni koji su istekli,
2. može da se zameni domen najvišeg nivoa (top level); na primer, umesto .org može da stoji .com,
3. može se drugačije ili pogrešno napisati:
    - pogrešno napisani: goggle.com umesto google.com,
    - dodata tačka ili neki drugi karakter: go.ogle.com umesto google.com,
    - slova se mogu zameniti brojevima : g00gle.com umesto google.com,
    - množina umesto jednine ili obrnuto: googles.com umesto google.com,
    - može se dodati još neka reč: googleresults.com umesto google.com,
    - slova se mogu zameniti sličnim ili istim slovima iz drugih pisama što ljudsko oko ne razlikuje, ali ih kompjuter drugačije čita; na primer, slovo “a” iz latinične u slovo “a” iz ćirilične tastature.

Liste blokiranih IP adresa i domena

Kada se u “Received” polju u zaglavlju mejla pronađe IP adresa servera sa kog je poslat mejl i u mejl adresi domen, njihova autentičnost može se analizirati na nekom od sajtova koji ažuriraju liste blokiranih IP adresa i domena:

- MultiRBL - alat za proveru da li se IP adresa domen nalazi na spam blok listama;
- Autonomous System Lookup - podaci o internet provajderu kom pripadaju IP adrese;
- Spamhaus - kombinuje spam liste i sadrži verovatno najbolji spisak blokiranih IP adresa.

Analiza tela (sadržaja) mejla

Pored analize zaglavlja mejla, veoma je važno ispitati i tekst e-pošte. Ključno je utvrditi da li je mejl legitiman i da li zaista dolazi od osobe ili organizacije za koju se pošiljalac izdaje. Cilj jeste da se utvrdi verodostojnost mejla.

Pregled tela mejla predstavlja analizu samog sadržaja poruke. To uključuje tekst poruke, bilo koje priloge, slike, linkove, kako bi se utvrdilo da li sadrže fišing elemente. Tipični elementi fišinga uključuju lažne linkove, zahtev za prijavu na lažnu stranicu, zahtev za slanje novca i slično. Analiza linkova je ključna kako bi se utvrdilo da li vode na lažne stranice.

Analiza teksta

Ispitivanje sadržaja može da obuhvata i analizu izražavanja, što može biti korisno u identifikaciji

tonova poruke, kao i u utvrđivanju emocionalne reakcije pošiljaoca i primaoca. Ova analiza se može koristiti za utvrđivanje namera i motiva iza slanja poruke.

Analiza linkova

Prilikom analiziranja URL adresa u mejlu, najvažnije je paziti da se greškom ne klikne na link, već u internet brauzeru treba potražiti originalnu stranicu i uporediti njenu URL adresu sa linkom ispisanim u mejlu. Za analizu linkova može se naći puno korisnih alata.

Analiza priloga

Prvi korak u ovoj fazi biće analiza formata fajla, odnosno njegove ekstenzije. Neki maliciozni fajlovi mogu imati dodatne ekstenzije, na primer .pdf.zip, a mogu da budu i bez ekstenzije. Neke ekstenzije se često koriste za maliciozne fajlove. Međutim, prisustvo takve ekstenzije govori da fajl može biti, a ne da sigurno jeste opasan. Evo samo nekih primera:

.zip - Format koji se često koristi za kompresiju i arhiviranje fajlova, što je funkcionalnost koja može da posluži za maskiranje malicioznog softvera unutar fajla;
.exe - Ova ekstenzija ukazuje na izvršni program, a može biti korišćena za instaliranje malvera;
.bat - Koristi se za “batch” skripte i može sadržati naredbe koje će pokrenuti malver;
.vbs - Ova ekstenzija se koristi za Visual Basic skripte, koje mogu biti maliciozne;
.js - Poznata ekstenzija za JavaScript fajlove, koji mogu sadržati maliciozni kod;
.msi - Ekstenzija Microsoft Installer fajlova, koji se mogu koristiti za instaliranje malvera;
.scr - Koristi se za screensaver fajlove, koji mogu biti maskirani kao nešto drugo, ali u stvari sadrže maliciozni kod;
.dll - Ekstenzija za dinamičke biblioteke, koje se često koriste za napade na softverske ranjivosti.

Prilikom analiziranja linkova i priloga, treba biti oprezan da se slučajno ne klikne na njih, a obavezno treba koristiti softver za antivirusnu zaštitu koji otkriva i sprečava maliciozne fajlove.

Korisni alati

VirusTotal

VirusTotal omogućava analiziranje sumnjivih priloga, linkova, IP adresa i domena kako bi se otkrilo da li je nešto zaraženo malicioznim softverom. Ono što se kopira u ovaj alat, automatski se deli sa bezbednosnom zajednicom, pa treba paziti da se ne kopiraju fajlovi koji sadrže poverljive informacije. Alat omogućava korišćenje premijum opcije.

PhishTool

Alat koji može automatizovano da analizira potencijalne zlonamerne mejlove je PhishTool. Umesto pojedinačnog analiziranja i prelaženja svih navedenih koraka, potencijalno zlonamerni mejl se može prebaciti u PhishTool i analizirati. Postoji opcija da se nalog na ovom servisu poveže sa VirusTotal nalogom. Takođe postoji besplatna verzija PhishTool alata.

POGLAVLJE 4: ZAŠTITA VAŠIH UREĐAJA I NALOGA

4.1. Bezbednost uređaja

Bezbednost računara

U ovoj poglavlju obradićemo najvažnije mere kada je reč o obezbeđivanju laptop i desktop računara. To uključuje fizičku sigurnost računara i svest o rizicima prilikom rada u terenskim uslovima. Takođe ćemo istaći značaj “čišćenja” uređaja, odnosno redovnog ažuriranja softvera, provere na prisustvo malvera, vođenja dijagnostike i slično.

Pristup uređaju

Rad se promenio za mnoge profesije tokom poslednjih nekoliko godina, posebno kada je reč o veličini i prenosivosti računara. Ljudi kuckaju na svojim laptopovima u kafićima, na aerodromima, u vozovima i mnogim drugim mestima gde biraju da rade. To naravno dovodi do povećanog rizika kada je reč o uređajima, jer mogu biti ukradeni ili im neovlašćene osobe mogu pristupiti.

Prvi korak kako biste osigurali da samo vi imate pristup vašem uređaju i korisničkom nalogu je zaštita lozinkom ili PIN-om, kao i za bilo koji drugi nalog. Mnogi novi laptopovi sada nude opcije biometrijskog otključavanja, na primer putem čitača otisaka prstiju. Iako zaštita lozinkom ne garantuje savršenu sigurnost, može poremetiti ili odvratiti zlonamernog aktera da pokuša pristup vašim datotekama.

Deljenje računara na poslu nije toliko uobičajeno kao nekada, ali u nekim slučajevima, na primer, kada ljudi rade u smenama, to može biti slučaj. Stoga je važno postaviti odvojene korisničke naloge za svaku osobu koja koristi računar i obezbediti ovlašćenom osoblju samo administratorski nalog na uređaju. Administrator nalog koji je probijen od strane zlonamernog aktera može biti veoma problematičan ne samo za uređaj na kojem se nalazi, već i za druge uređaje u mreži ako napadač uspe da dobije dovoljan pristup.

Fizička bezbednost

Rad i izveštavanje sa terena mogu biti veoma stresni, posebno kada su u pitanju događaji visokog rizika, poput protesta ili demonstracija, ili okruženja zahvaćena ratom ili prirodnim katastrofama. Kada se nalazite na javnom mestu, pobrinite se da ne ostavljate svoj računar otključanim ili bez nadzora, jer će biti lak plen za svaku lošu nameru. Ukoliko često putujete ili obavljate terenski rad koji zahteva nošenje radnog laptopa sa sobom, ozbiljno razmotrite enkripciju njegovog hard diska. Kada je disk enkriptovan, operativni sistem instaliran na njemu ne može se pokrenuti bez lozinke koju vi određujete.

MacOS ima FileVault, Windows operativni sistem ima Bitlocker, a VeraCrypt kao aplikacija takođe nudi opciju sistemskog enkriptovanja. Na kraju, budite veoma oprezni sa svojim uređajima tokom događaja koji mogu postati nasilni, kao što su protesti, jer mogu biti ukradeni, oštećeni ili na meti zlonamernih aktera.

Ажуриранја

Ажурирање вашег softvera od kritičnog je značaja kako biste osigurali da vaš uređaj bude zaštićen od potencijalnih napadača i da što bolje funkcioniše. Čak i kritične ranjivosti mogu proći neprimećene i nezakrpljene tokom dužeg vremenskog perioda, što uređaje čini poželjnim ciljem hakera, posebno ako uređaji sadrže poverljive informacije i mogu se koristiti za dalje napade i druge zlonamerne aktivnosti.

Vrste ažuriranja

Postoje tri vrste ažuriranja na koje treba obratiti pažnju:

1. **Ažuriranja operativnog sistema (OS):** mogu biti bilo šta, od male zakrpe do potpuno nove verzije OS-a. Proizvođači obično pružaju sigurnosna ažuriranja OS-a tokom mnogo godina, ali u mnogim slučajevima zastarele verzije OS-a ne bivaju zamenjene;
2. **Ažuriranja instaliranih aplikacija:** sve aplikacije koje instalirate, a posebno antivirusni/antimalver proizvodi, takođe treba redovno ažurirati. U slučaju da se aplikacija dugo ne ažurira ili se više ne održava, preporučuje se potraga za alternativom.
3. **Ažuriranja drajvera za hardverske komponente:** drajveri su mali programi dizajnirani da omoguće rad hardvera, poput grafičke kartice, na određenom uređaju. Često zanemareni, zastareli drajveri takođe mogu biti ključni za hakera da otkrije ranjivost koju može iskoristiti.

Stoga, redovna ažuriranja su ključna za sigurnost i performanse vašeg uređaja. To je već spomenuto, ali još jednom napominjemo:

- Omogućite automatska ažuriranja gde god možete;
- Instalirajte ažuriranja označena kao kritična od strane dobavljača softvera i hardvera (na primer zero-day zakrpe) što je pre moguće;
- Zamenite zastarele i neodržavane operativne sisteme i aplikacije.

Instaliranje pouzdanog softvera

Tokom rada često se nalazimo u situaciji da obavimo zadatke koji zahtevaju instaliranje dodatnog softvera, kao što su konvertori različitih vrsta fajlova, alati za preuzimanje video sadržaja ili editori multimedijalnog sadržaja. Ovi programi mogu doći i u obliku dodataka za brauzere, koji takođe mogu doneti ranjivosti ili sami biti zlonamerni. U ovim situacijama trebalo bi da se odlučite za softver kome verujete, odnosno koji je visoko ocenjen u zajednici i nije javno poznat po sigurnosnim kompromisima.

Pouzdane aplikacije

Čest vektor napada je korišćenje fišing mejlova ili poruka i traženje od cilja da instalira određenu aplikaciju, navodno radi obezbeđenja komunikacije, vršenja ključnog ažuriranja ili iz bilo kog

drugog razloga koji bi potencijalno ubedio metu da instalira malver koji je maskiran kao obična aplikacija. Stoga je vrlo važno:

- **Preuzimati instalacione pakete sa zvaničnih sajtova proizvođača ili prodavnica aplikacija za operativni sistem:** međutim, trebalo bi da budemo svesni da čak i zvanične prodavnice mogu biti pune malvera - nedavni slučaj Google Play prodavnice je dobar primer;
- **Izbegavati instaliranje softvera koji nije ažuriran dugo vremena:** moguće je da su zlonamerni akteri pronašli načine da iskoriste njegove ranjivosti koje nisu zakrpljene na vreme ili uopšte.
- **Ne koristiti "krekovan" softver, jer može sadržavati malver ili špijunski softver:** umesto toga, potražite besplatnu i otvorenu alternativu. Danas čak i složeni zadaci, poput dizajna i manipulacije slikama, mogu se obaviti pomoću pouzdanih besplatnih aplikacija kao što su GIMP ili Inkscape.

Ako primetite bilo šta neobično na svom uređaju, kao što je spor rad ili neočekivano ponašanje određenih aplikacija, odmah pokrenite antivirus/antimalver skeniranje.

Tehnologija za neprofitne organizacije

Plaćanje licenci obično nije jeftino i može značajno uticati na budžet neprofitne organizacije. Srećom, postoje opcije za dobijanje licenci softvera sa popustom ili čak besplatan pristup plaćenim uslugama:

- TechSoup: organizacija koja pruža širok katalog licenciranog softvera, od kancelarijskih paketa do antivirusnih proizvoda, dostupnih organizacijama civilnog društva po sniženoj ceni. Potrebna je registracija kod regionalnog predstavnika TechSoup-a, ali nije teško dobiti je;
- Google for Nonprofits: omogućava osnovni plan Google Workspace (paketa za produktivnost sa mejlovima, video pozivima, skladištenjem fajlova, kolaborativnim softverom, itd) besplatno.
- Project Galileo: inicijativa kompanije Cloudflare namenjena subjektima od javnog interesa (civilno društvo, novinari, aktivisti za ljudska prava...) koja im pruža besplatnu DDoS zaštitu sajta i druge plaćene opcije.

Budite svesni koliko vam je računar dostupan i pobrinite se da ga zaštitite, posebno u javnosti ili van kancelarijskog prostora. Takođe, važno je redovno ažurirati računar, bez obzira koliko to vremena oduzimalo i bilo dosadno. Na kraju, izbegavajte instaliranje nepoznatih ili nepouzdanih aplikacija - koristite samo zvanične izvore za preuzimanje softvera.

Bezbednost mobilnih telefona

Bezbednost mobilnih uređaja postaje ključna s porastom sajber pretnji uperenih ka pametnim telefonima i tabletima. Rizici uključuju neovlašćen pristup osetljivim podacima, finansijske gubitke i druge potencijalne štete. Mobilni uređaji, sada izloženi brojnim pretnjama, često služe za čuvanje važnih informacija poput e-pošte, bankovnih podataka i privatnih fotografija. Kako bi se minimalizovale potencijalne štete, ključno je prepoznati ranjivosti i upravljati uređajima odgovorno.

Potencijalne digitalne pretnje

Potencijalne digitalne pretnje od kojih treba zaštititi mobilne uređaje uključuju zlonamerne aplikacije i sajtove, često maskirane kao legitimne. Preširoke dozvole aplikacija koje skidamo na telefon mogu ugroziti privatnost naših podataka. Fišing napadi su takođe veoma česti preko SMS poruka i čet aplikacija, jer korisnici često u realnom vremenu prate poruke, otvarajući i čitajući ih odmah po prijemu, pa oprez u nekim trenucima može izostati. Curenje podataka često proizlazi iz besplatnih aplikacija čiji je poslovni model da prodaju podatke o svojim korisnicima drugim kompanijama. Mobilni uređaju nisu izuzeti ni od napada malicioznim programima. Česti su i poznati napadi špijunskim softverima na pripadnike civilnog sektora. Takođe treba biti oprezan i kada se pristupa nekoj Wi-Fi mreži, jer može biti lažna i prisluškivana od strane zlonamernog aktera.

Kako prepoznati lažnu (zlonamernu) mobilnu aplikaciju

Čak i ako se primeti da neka aplikacija ima malo recenzija ili veoma malo preuzimanja, moglo bi se pretpostaviti da je relativno nova. S druge strane, to može biti lažna aplikacija koja je tu da nanese štetu svakome ko je instalira.

1. Pretražiti aplikaciju i kompaniju na internetu: većina legitimnih developera će imati sajt na kojem se prikazuju detaljno sve funkcije koje aplikacija ima i sve druge njihove aplikacije koje su razvili;
2. Pročitati dostupne recenzije aplikacije: ako izgledaju kratke i bezopisne, niej bezbedno skidati tu aplikaciju. Dodatno, mogu postojati recenzije korisnika koji su prethodno bili prevareni od strane te aplikacije.
3. Obratite pažnju na detalje: da li aplikacija izgleda profesionalno? Dobar dizajn ukazuje na dobru aplikaciju. Obratiti pažnju na neslaganja u fontovima, greške u kucanju i nesimetrično postavljanje logotipa i slika.
4. Mnoge lažne aplikacije su kopije popularnih, već postojećih i popularnih aplikacija: tada je korisno pogledati ko stoji iza aplikacije, da li se podudara sa aplikacijom. Obratite pažnju na broj recenzija - izuzetno popularne aplikacije imaće stotine, ako ne i hiljade recenzija korisnika.

Kako prepoznati smišing

Smišing (SMS phishing) je oblik fišing prevara gde se umesto mejlova, veliki broj poruka šalje preko SMS poruka ili čet aplikacija. Ima iste karakteristike kao bilo koja druga vrsta fišing napada, slične se tehnike koriste u tim napadima i isti su ciljevi ovih vrsta napada.

Karakteristike smišinga su sledeće:

- Nepoznati brojevi: smišing poruke često dolaze od nepoznatih brojeva ili brojeva koji izgledaju neobično. Ako poruka dolazi od broja koji vam nije poznat, budite oprezni;
- Zastrašujuće ili hitne poruke: smišing često koristi taktiku zastrašivanja ili hitnosti kako bi naterao korisnike da brzo reaguju. Poruke koje tvrde da imate hitan problem ili da će biti neke negativne posledice ukoliko nešto ne uradite odmah mogu biti znak smišinga;
- Linkovi u porukama: smišing poruke često sadrže linkove na koje korisnici treba da

kliknu. Ovi linkovi mogu voditi do lažnih sajtova ili aplikacija koje pokušavaju prikupiti vaše informacije. Nikada ne klikćite na linkove iz sumnjivih poruka;
- Zahtevaju se lične informacije: smišing poruke mogu sadržavati zahteve za lične informacije poput lozinki, brojeva kreditnih kartica ili druge osetljive informacije. Legitimne organizacije neće vas tražiti da delite takve informacije putem SMS poruka;
- Gramatičke greške: smišing poruke često sadrže gramatičke ili pravopisne greške. To može biti znak da poruka nije autentična.

U trenucima kada se sumnja na autentičnost poruke, najbolje je direktno kontaktirati organizaciju od koje je navodno stigla poruka i tako utvrditi legitimnost poruke.

Dobre bezbednosne prakse za mobilne uređaje

Za kraj ćemo se osvrnuti na neke od opštih saveta kada je reč o dobrim praksama zaštite mobilnih uređaja.

1. Zaštita lozinkom: postavite lozinke radi zaštite uređaja;
2. Enkripcija mobilnog uređaja - ovaj proces štiti osetljive informacije od neovlašćenog pristupa, posebno ako uređaj bude izgubljen ili ukraden;
3. Radite redovan bekap podataka;
4. Oprez sa aplikacijama - preuzimati aplikacije samo sa pouzdanih izvora i pre instalacije pregledati čemu sve aplikacija traži pristup;
5. Redovna ažuriranja aplikacija i operativnih sistema;
6. Aktivirati opciju “Pronađi moj uređaj” na Android i iPhone uređajima;
7. Odjavite se iz organizacionih naloga nakon što obavite šta je neophodno na telefonu;
8. Koristite menadžer lozinki: mnoge aplikacije koje bezbedno skladište lozinke dostupne su i za mobilne uređaje, i ove aplikacije znatno olakšavaju pristup lozinkama i bezbedno čuvanje istih;
9. Odredite važne fajlove/foldere i podesiti opciju “skrivanja” (hide) radi dodatne privatnosti i bezbednosti;
10. Korišćenje VPN-a: razmislite o korišćenju virtuelne privatne mreže (VPN) radi poboljšane sigurnosti na mreži;
11. Odjaviti se nakon izvršenog onlajn plaćanja: uvek se treba odjaviti sa sajtova nakon obavljanja plaćanja;
12. Isključiti Wi-Fi i Bluetooth kada nisu u upotrebi kako bi se smanjile potencijalne ranjivosti;
13. Instalirati pouzdan antivirus - koristiti pouzdanu antivirusnu zaštitu (npr. Bitdefender) radi detekcije i sprečavanja potencijalnih pretnji;
14. Potencijalno napraviti različite profile/korisnike na svom telefonu ako je potrebno radi dodatne bezbednosti.
15. Apple je omogućio stavljanje uređaja u tzv. “Lockdown Mode”, koji onemogućava brojne funkcionalnosti ali pokazao kao efikasan u sprečavanju napada naprednim špijunskim softverom.

4.2. Tails operativni sistem

Tails, što znači “The Amnesic Incognito Live System” (Operativni sistem sa amnezijom i inkognito režimom), predstavlja operativni sistem fokusiran na privatnost, osmišljen da ne ostavlja nikakav trag korisničke aktivnosti. To je operativni sistem koji možete pokrenuti na gotovo svakom računaru putem USB stika ili DVD-a. Tails ima za cilj pružanje anonimnosti, privatnosti i sigurnosti korisnicima, posebno onima koji su zabrinuti zbog onlajn nadzora ili cenzure.

Ključne karakteristike Tails-a

- Anonimno pretraživanje interneta: Tails usmerava sav internet saobraćaj kroz Tor mrežu, što pomaže u anonimizaciji onlajn aktivnosti korisnika putem niza servera koji su operisani od strane volontera.
- Amnezički dizajn: Tails je dizajniran da ne ostavlja digitalni otisak, kada isključite sistem, briše sve tragove vaših aktivnosti, kao što su istorija pregledanja ili fajlovi sačuvani tokom sesije.
- Unapred instalirani alati za pivatnost i bezbednost: Tails dolazi sa unapred instaliranim alatima za privatnost i enkripciju, uključujući Tor Browser, PGP enkripciju mejlova i alate za sigurno slanje poruka.
- Bezbedna komunikacija: naglašava bezbedne metode komunikacije kako bi zaštitio korisnike od prisluškivanja i neovlašćenog pristupa.
- Open Source: Tails je softver otvorenog koda, što znači da je izvorni kôd dostupan za pregled i doprinos svima, promovišući transparentnost i saradnju zajednice.

Tails se često koristi za osetljive aktivnosti, kao što su pristup informacijama u restriktivnim okruženjima, sprovođenje privatnih istraživanja ili sigurno komuniciranje. Važno je napomenuti da, iako Tails pruža visok nivo privatnosti i sigurnosti, korisnici treba da budu svesni najboljih praksi i potencijalnih rizika povezanih sa njihovim specifičnim potrebama.

Kako koristiti Tails?

Korišćenje Tails-a uključuje sledeće opšte korake:

1. Preuzimanje Tails-a:
    - Posetite zvanični sajt (tails.net).
    - Preuzmite Tails ISO fajl.
2. Insatlirajte Tails na USB-u ili na DVD-u:
    - Koristite USB stik (po mogućstvu 8GB ili veći) ili DVD kako biste napravili instalacioni Tails medij.
    - Pratite uputstva data na Tails sajtu za kreiranje instalacionog USB-a ili DVD-a.
3. Podignite Tails:
    - Ubacite Tails USB ili DVD u računar.
    - Ponovo pokrenite računar i podesite ga da se sistem podiže sa USB-a ili DVD-a.
    - Pokrenite Tails kad budete upitani.

4. Konfigurišite Tails:
    - Tails će vas voditi kroz početni proces podešavanja, gde možete konfigurisati neke opcije, kao što su jezik i postavke tastature.
5. Povežite se sa Tor mrežom:
    - Tails automatski rutira sav internet saobraćaj kroz Tor mrežu. Proverite da li ste povezani sa internetom.
6. Koristite Tails:
    - Kada je Tails pokrenut, možete ga koristiti kao običan operativni sistem. Sadrži radnu okolinu i razne preinstalirane aplikacije za pregledanje interneta, mejl i sigurnu komunikaciju.
7. Isključite i uklonite medijum:
    - Kada završite sa korišćenjem Tails-a, isključite računar.
    - Uklonite Tails USB ili DVD. Tails je dizajniran da ne ostavlja tragove na računaru.

Dodatne napomene kako Tails funkcioniše

Ako su vam za rad u Tails-u često potrebni određeni fajlovi, Tails omogućava korisnicima da postave persistenciju na posebnom USB uređaju, gde se odabrani podaci i postavke mogu sačuvati između sesija. Ovo pruža siguran način za čuvanje određenih informacija uz očuvanje amnezične prirode Tails sistema.

Zapamtite da je Tails dizajniran za specifične slučajeve upotrebe, kao što su privatnost i anonimnost, i možda nije pogodan za sve računarske potrebe. Korisnici takođe treba da budu svesni ograničenja i potencijalnih rizika povezanih sa korišćenjem ovakvih alata.

4.3. Bezbednost na društvenim mrežama

Bezbednost na društvenim mrežama je ključna u uslovima kada smo konstantno onlajn. Zato je važno imati osnovno znanje o zaštiti ličnih i profesionalnih informacija u digitalnom okruženju, prepoznavanju rizika i pretnji, upravljanju postavkama privatnosti i usvajanju dobrih bezbednih praksi. Bilo da se radi o ličnim povezivanjima ili profesionalnom umrežavanju, razumevanje kako bezbedno koristiti ove platforme ključno je u današnjem digitalnom dobu.

Pregled pretnji

Bezbednost na društvenim mrežama odnosi se na zaštitu vaših ličnih i profesionalnih informacija na ovim platformama. Sa milijardama korisnika širom sveta, društvene mreže postale su jedna od glavnih meta sajber pretnji, uključujući fišing, socijalni inženjering i infekcije malverom. Ljudske greške, zloupotrebe naloga i lažni profili predstavljaju dodatne izazove.

Najčešće digitalne pretnje na društvenim mrežama uključuju:

- **Fišing i socijalni inženjering:** fišing i socijalni inženjering su dva tipa prevare koja imaju za cilj da prevare žrtve i navedu ih da pruže privatne informacije – uglavnom lične podatke

ili kredencijale za prijavljivanje na nalog. Te informacije se mogu zatim prikupiti i prodati, ili koristiti za pristup mreži gde bi mogli pokrenuti malver, što dovodi do gubitka podataka, a možda čak i enkripcije podataka za upotrebu u napadu ransomverom;

- **Malver na društvenim mrežama:** širenje malvera kroz zlonamerni sadržaj, linkove ili priloge na društvenim platformama. Čest način infekcije malverom je otvaranje priloga ili kliktanje na link u zlonamernom mejl, što je mnogima poznato - ali ono što se ne razmatra uvek je koliko je lako kliknuti na nesiguran link na društvenoj mreži, što potencijalno omogućava pristup uređajima i nalozima na mreži vaše organizacije;
- **Zloupotreba naloga:** neovlašćen pristup i zloupotreba korisničkih naloga, uključujući tehničke napade na lozinke i krađu naloga. Neaktivne naloge treba redovno pratiti kako bi se osiguralo da nisu bili meta napadača. Ako se nalog više ne koristi, moglo bi proći neko vreme pre nego što se primeti da je narušena njegova bezbednost;
- **Lažni profili i zloupotreba identiteta:** stvaranje lažnih profila radi obmane ili krađe identiteta korisnika. Slično kao kod napada na nekorišćene profile, napadači mogu pokušati da prevare korisnike stvaranjem lažnih naloga i stranica kako bi imitirali neku organizaciju i tako joj naneli štetu;
- **Zloupotreba privatnosti:** neovlašćeno prikupljanje i korišćenje podataka o ličnosti pojedinaca bez njihovog pristanka i znanja.

Posledice sajber napada na društvenim mrežama mogu biti brojne, a najuočljivije su gubitak reputacije, gubitak naloga i curenje podataka.

Ključne smernice za bezbednost na društvenim mrežama

Da zaključimo ovaj odeljak, osvrnućemo se na nekoliko ključnih smernica kada je reč o bezbednosti na društvenim mrežama:

1. Zaštitite nalog snažnom lozinkom i podesiti dvostruku autentifikaciju;
2. Podesiti rezervni mejl u slučaju da se nešto desi sa glavnim mejl nalogom ili sa profilom na društvenoj mreži
3. Jedinstveno prijavljivanje (“single-sign on”, SSO) omogućava korisnicima pristup više aplikacija i uređaja putem jednog, sigurnijeg korisničkog ID-a. Jedinstvena prijava (SSO) omogućava korisniku da se prijavi jednim identitetom i ostvari pristup na više aplikacija i usluga;
4. Redovno ažuriranje aplikacije: ovo otklanja ranjivosti u samoj aplikaciji koje bi napadač mogao da iskoristi;
5. Upravljanje dozvolama aplikacija trećih strana: sve aplikacije trećih strana koje imaju dozvolu da se povežu, pristupaju ili prikupe podatke sa vaših naloga na društvenim mrežama predstavlju određeni rizik;
6. Izbegavanje prekomernog deljenje ličnih informacija: preterano deljenje ličnih informacija, poput adrese ili finansijskih detalja, može izložiti korisnike sajber pretnjama. Zlonamerni akteri mogu iskoristiti ove informacije za krađu identiteta, fišing ili druge zlonamerne aktivnosti;
7. Oprez pri prihvatanju zahteva za prijateljstvo ili praćenje je ključan, s obzirom na lažne profile koje mogu koristiti sajber kriminalci;

8. Oprez prilikom otvaranja sajtova ili skidanja fajlova: linkovi i fajlovi deljeni na društvenim mrežama mogu nositi skrivene opasnosti. Pre otvaranja linka ili fajla, treba razmisliti o njegovom izvoru i legitimnosti;
9. Praćenje aktivnosti na svim društvenim kanalima (logovanje pristupa i uređaja, praćenje objava itd) i pravovremeno reagovanje kada se primete bilo kakve nepravilnosti takođe predstavlja važnu bezbednosnu meru.

POGLAVLJE 5: PRAVLJENJE REZERVNIH KOPIJA

U ovom poglavlju prikazane su dobre prakse po pitanju pravljenja rezervne kopije podataka. Rezervna kopija ili bekap je jedna od bezbednosnih mera koja neće sprečiti incident, ali će omogućiti brži oporavak nakon bilo kog sajber napada ili nepoželjnog incidenta, kvara računara, kao i sprečiti gubitak važnih podataka. Rezervna kopija se odnosi na kopiranje fizičkih ili virtuelnih informacija na sekundarnu lokaciju radi čuvanja u slučaju kvara opreme ili sajber napada. Bekapovanje ne utiče na nivo bezbednosti samog sistema, ali ima suštinski značaj posle bezbednosne krize kada treba povratiti izgubljene podatke. Ponekad, na osnovu bekapa moguće je odrediti uzrok pada sistema rekonstrukcijom bezbednosnih propusta ili grešaka u sistemu.

Bez obzira na veličinu organizacije, redovno pravljenje rezervnih kopija podataka je od velikog značaja.

Opcije za bekap

Decentralizacija sistema, kao mera fizičke zaštite, postavlja se kao ključan uslov za njegovu bezbednost. Preporučuje se da se podaci ne čuvaju na istom uređaju sa koga se šalju u mrežu ili na kome se obrađuju. Ima nekoliko načina za skladištenje velikih količina podataka: eksterni hard diskovi, iznajmljivanje prostora za skladištenje na klaud serveru, formiranje vlastitog mini data centra.

Eksterni hard diskovi

Najjednostavniji način za čuvanje podataka je na eksternom hard disku. Eksterni hard diskovi sa relativno dobrim performansama su pristupačni, ali ovaj tip računarske opreme nema ugrađeni mehanizam dupliciranja. To znači da bi u slučaju kvara većina podataka na tom disku bila izgubljena zauvek. Zato je rezervno kopiranje podataka sa eksternog hard diska na drugi eksterni hard disk veoma značajno. Eksterni diskovi nemaju direktni pristup internetu i aktivni su samo kada su povezani sa računarom, pa se može reći da su relativno sigurni. Čuvanje podataka na eksternom hard disku znači da podaci uglavnom ostaju u fizičkom prostoru organizacije.

Klaud rešenja

Iz perspektive gubitka podataka, iznajmljivanje prostora za skladištenje na klaud serveru mnogo je pouzdaniji način za čuvanje važnih podataka. Klaud je internet tehnologija zasnovana na korišćenju resursa na daljinu (protok podataka, prostor za čuvanje, radna memorija, itd) i njihove razmene između više aplikacija i korisnika. Neki od klaud rešenja su Google Drive, Dropbox, OneDrive, Proton Drive, Tresorit, itd. Međutim, ako je reč o osetljivim podacima, ne preporučuje se skladištenje na tuđim uređajima, uprkos činjenici da sve klaud usluge uključuju enkripciju.

Formiranje vlastitog mini data centra

Treći način za skladištenje podataka jeste formiranje vlastitog mini data centra na kome će svi organizaciji važni podaci biti čuvani. Oprema za te namene zavisi od potreba. Postoji više gotovih

rešenja koja su pristupačna i relativno trajno rešavaju ovo pitanje. Pri izboru, treba voditi računa da bekap sistem pruža mogućnost za brz i pouzdan povraćaj podataka, kao i da je optimalan, tj. da ne preopterećuje resurse skladištenja.

Preporučuje se da se koristi bekap sistem otvorenog koda, kao što je UrBackup. Jedno od već gotovih rešenja za data centre manjeg obima je QNAP.

Pravilo za bezbedan bekap

3-2-1 pravilo je jedno od osnovnih načela za efikasno upravljanje rezervnim kopijama podataka. Ovo pravilo pruža smernice o tome kako organizovati i čuvati rezervne kopije kako biste osigurali otpornost na gubitak podataka. Evo šta svaki od brojeva označava:

- **3 kopije podataka:** ovaj deo pravila preporučuje održavanje najmanje tri nezavisne kopije vaših podataka. To znači da pored originalnih podataka imate još najmanje dve dodatne kopije;
- **2 različita medija:** ovaj deo pravila naglašava važnost čuvanja kopija podataka na barem dva različita medija ili uređaja. Na primer, možete čuvati jednu kopiju na eksternom hard disku i drugu na klaud servisu. Ova redundancija pomaže u zaštiti od gubitka podataka uzrokovanog problemima s određenim medijem;
- **1 kopija van radnog okruženja:** treći deo pravila ukazuje na potrebu čuvanja bar jedne kopije van radnog okruženja. To znači da bi jedna od kopija trebala biti smeštena na lokaciji koja je fizički razdvojena od mesta gde se čuvaju originalni podaci i prva rezervna kopija. Ovo pomaže u slučaju katastrofalnih događaja kao što su poplave, požari ili krađe.

Dodatne smernice za bezbednost bekapa

Za kraj ovog odeljka navešćemo još nekoliko važnih smernica za očuvanje bezbednosti i integriteta rezervnih kopija.

1. Enkripcija - bilo bi poželjno da svi digitalni fajlovi koji sadrže osetljive i poverljive informacije budu enkriptovani.
2. Redovno ažuriranje rezervnih kopija: postaviti redovan raspored ažuriranja rezervnih kopija kako bi se redovno čuvale najnovije promene;
3. Automatizacija procesa: koristiti automatizaciju gde je to moguće kako bi se smanjile ljudske greške i kako bi se osiguralo da se rezervne kopije redovno prave prema postavljenom rasporedu;
4. Različiti tipovi rezervnih medija: razmislite o korišćenju različitih tipova rezervnih medija (npr. lokalni uređaji, oblak, eksterni hard diskovi) kako biste povećali otpornost na gubitak podataka zbog oštećenja jednog tipa medija;
5. Sigurnost pristupa: obezbediti siguran pristup rezervnim kopijama kako bi se sprečio neovlašćeni pristup korišćenjem mera kao što su snažne lozinke i dvofaktorska autentifikaciju.

POGLAVLJE 6: BEZBEDNOST VEB SAJTOVA

6.1. Odabir hosting provajdera

Briga o bezbednosti podataka, bilo da se radi o veb sajtovima, bazama podataka ili rezervnim kopijama, jedan je od najkritičnijih aspekata upravljanja digitalnom infrastrukturom organizacije. U ovoj poglavlju proći će se kroz značaj odabira dobrog pružaoca hostinga, uobičajene vrste hosting usluga sa fokusom na hosting provajdere prilagođene organizacijama civilnog društva i medijskim organizacijama.

Hostovanje veb sajta

Iako postoji mnogo opcija za hostovanje veb sajta, pojedinci i organizacije uglavnom biraju da iznajme server od spoljnog entiteta, poput hosting provajdera ili eksterne IT kompanije koja upravlja veb sajtom. Oni sa veštinama i resursima mogu, naravno, odabrati da postave, administriraju i održavaju sopstveni server. Pružaoci hostinga upravljaju serverima, koji su suštinski računari korišćeni za skladištenje podataka i pružanje različitih usluga po zahtevu.

Iako postoji mnogo faktora koji utiču na izbor vaših pružalaca hostinga, pouzdano hostovanje ključno je kada je reč o reagovanju na incidente i oporavak sistema. Jeftin hosting provajder može biti primamljivo rešenje, ali svaki incident može imati ogromne posledice za vaš veb sajt ako njihove bezbednosne politike nisu na visokom nivou.

Šta tražiti kod pružaoca hostinga

Ovo su važni faktori koje treba uzeti u obzir prilikom izbora vašeg pružaoca hosting usluga:

- **Lokacija:** izbor između domaćeg i stranog hostinga zavisi od nivoa usluga koje nude. Strana kompanija može pružiti generalno bolje usluge za manje novca u poređenju sa domaćom, ali mogu biti spori u reagovanju u slučaju da su udaljeni, na primer, u SAD. Kompanije sa sedištem u EU moraju da poštuju stroge nacionalne zakone o zaštiti podataka o ličnosti i GDPR, pa je to takođe važan faktor koji treba uzeti u obzir.
- **Tehnička podrška:** dostupnost podrške 24/7 ključan je faktor za svakog pružaoca hostinga, jer nikada ne znate kada će incident pogoditi vaš veb sajt. U ovim okolnostima, brza reakcija od strane tima za podršku provajdera je ključna za rešavanje incidenta i oporavak sistema;
- **Recenzije:** proverite onlajn ocene i recenzije za pružaoce sa sličnim ponudama, iskustva drugih ljudi mogu biti vrlo vredna;
- **Cena:** generalno treba izbegavati najjeftiniju opciju, dok s druge strane najskuplji paket hostinga može biti nepotreban, posebno ako je vaš veb sajt jednostavan i ne privlači mnogo poseta.

6.2. Zaštita od DDoS napada

Kao što smo već napomenuli, DDoS napadi su česti kada je reč o sajtovima medija i to ne samo

u Srbiji, već i u mnogim drugim zemljama širom sveta. Da bi sajt bio otporan na ovakvu vrstu napada, neophodno je koristiti usluge DDoS zaštite.

Kao najčešći provajder DDoS zaštite uglavnom se posmatra Cloudflare, koji nudi besplatne usluge, ali sa ograničenim opcijama, ali postoje i drugi kao što je Deflect, čije usluge koriste mnogi mediji, organizacije za zaštitu životne sredine i ljudska prava. Gugl takođe nudi besplatnu DDoS zaštitu preko Project Shield, koji je namenjen sajtovima za vesti, ljudska prava i izbore. Nezavisni mediji, istraživački novinari i aktivisti za ljudska prava u represivnim režimima takođe mogu da se prijave za program brze podrške organizacije Qurium, koja između ostalog uključuje DDoS zaštitu. Cloudflare pruža svoje plaćene usluga besplatno preko projekta Galileo, za koji se mogu prijaviti akteri koji deluju u javnom interesu.

Hosting za aktere od javnog interesa

Iako su komercijalni akteri (Hetzner, DigitalOcean, itd) uobičajeni izbor za mnoge organizacije, uključujući medije i civilno društvo, treba napomenuti da postoje pružaoci čije su usluge posebno prilagođene potrebama novinara, aktivista, zaštitnika ljudskih prava i drugih aktera od javnog interesa. Primeri su Greenhost i Qurium, oba su članovi CiviCERT-a, prominentne zajednice aktera civilnog društva koji se bave sajber bezbednošću:

- Greenhost je kompanija sa sedištem u Holandiji, posvećena zelenoj i održivoj tehnologiji. Pružaju podršku 24/7 i potpuno poseduju i kontrolišu hardver, infrastrukturu i veze. Sloboda interneta je jedno od načela kompanije, a generalno je usluga orijentisana ka privatnosti i zaštiti podataka.
- Qurium je neprofitna organizacija sa sedištem u Švedskoj koja nudi Virtualroad.org kao bezbedno hosting rešenje, potpuno poseduje fizičku infrastrukturu i održava sav hardver i softver. Njihova podrška je dostupna na više jezika 365 dana godišnje. Uključuju usluge poput mitigacije DDoS napada i nude programe podrške za brzo reagovanje nezavisnim medijima, istraživačkim novinarima i aktivistima za ljudska prava.

Da sumiramo, odabir pružaoca hostinga trebalo bi da se obavi u skladu sa vašim potrebama, budžetom i organizacionim kontekstom. Dobra podrška tehničke podrške za hosting ključna je pri upravljanju i reagovanju na incidente i može napraviti veliku razliku. Na kraju, razmotrite korišćenje usluge hostinga koja ima iskustvo sa civilnim društvom, novinarima i medijskim organizacijama.

Dobre prakse održavanja sajtova

Kako biste na bezbedan način održavali sajt, navodimo najvažnije prakse:

- **Redovno ažuriranje softvera:** ažuriranje softvera na veb sajtu, uključujući sisteme za upravljanje sadržajem kao što je WordPress, ali i dodatke i teme, ključno je za održavanje sajta bezbednim. Redovna ažuriranja takođe poboljšavaju funkcionalnost i performanse veb sajta;
- **Zaštita od DDoS napada:** usluge poput Project Galileo, Project Shield ili Deflect nude kvalitetne bezbednosne opcije i infrastrukturu koja štiti vaš veb sajt od različitih pretnji, uključujući DDoS napade;

- **Jaka autentikacija:** korišćenje jakih lozinki i implementacija dvostruke autentikacije (2FA) na svim nalozima kojima se pristupa sajtu je od velike važnosti;
- **Siguran prenos podataka:** osigurajte siguran prenos podataka korišćenjem HTTPS protokola i podešavanjem SSL/TLS sertifikata. HTTPS enkriptuje podatke koji se razmenjuju između veb sajta i korisnika, sprečavajući prisluškivanje i presretanje podataka, dok SSL/TLS sertifikati potvrđuju autentičnost sajta. Organizacija Let's Encrypt deli besplatne sertifikate u cilju što većeg broja bezbednih sajtova;
- **Firewall i prevencija upada:** implementiranje zaštitnog zida za aplikacije (web application firewall, WAF) doprinosi zaštiti veb sajta od različitih onlajn pretnji. WAF filtrira ulazni saobraćaj i blokira zlonamerne zahteve, čineći sajt otpornijim na pretnje. Mnogi hosting provajderi to nude kao uslugu;
- **Redovni bekapi:** planirajte redovne automatizovane bekape veb sajta i čuvajte ih na lokacijama van sajta. Ovi bekapi su ključni za oporavak u slučaju incidenta jer omogućavaju vraćanje veb sajta na prethodno stanje i pored ostalog sprečavaju gubitak podataka.

POGLAVLJE 7: BEZBEDNOSNE POLITIKE I PROCEDURE

Ovo poglavlje analizira suštinske aspekte digitalnih bezbednosnih politika i procedura, pružajući primere za tri najvažnije bezbednosne politike: Politiku lozinki, Politiku e-pošte i naloga i Bezbednosni plan. Postavljanje jasnih smernica u vidu politika značajno je za olakšavanje implementacije preventivnih mera u bilo kojoj organizaciji.

Politika lozinki: ovaj dokument pruža organizacijama uputstva o tome kako lozinke treba da se koriste, generišu, modifikuju i bezbedno čuvaju (tj. korišćenjem menadžera lozinki) za sve organizacione resurse, uključujući uređaje i naloge.

Politika e-pošte i naloga: ovaj dokument pruža organizacijama uputstva o tome kako treba kreirati i ukloniti e-poštu i povezane naloge za deljene kalendare, klaud ili deljene dokumente (u slučaju da organizacija koristi rešenje za produktivnost kao što je Google Workspace ili Microsoft 365) zaposlenima koji se pridružuju i napuštaju organizaciju.

Bezbednosni plan: ovaj dokument opisuje potencijalne bezbednosne rizike za organizaciju, preventivne mere i korake koje treba preduzeti u slučaju incidenta u digitalnoj bezbednosti. Takođe je data lista preporučene opreme (npr. različiti softverski alati za poboljšanje bezbednosti i privatnosti) i primeri kako primeniti mere u slučaju incidenta.

Primer Politike lozinki

_____ (Naziv organizacije)

Politika lozinki

1. Ova politika se primenjuje na lozinke (passwords) u upotrebi za zaštitu naloga, uređaja, dokumenata, baza podataka i drugih resursa kojima upravlja _____ (Naziv organizacije).
2. Jedna lozinka se ne sme koristiti za zaštitu više različitih resursa. Lozinke se ne smeju javno prikazivati i deliti sa neautorizovanim osobama.
3. Ukoliko postoji tehnička mogućnost, neophodno je uvesti dvostruku verifikaciju prijave (2-step verification) na svaki resurs kojim upravlja _____ (Naziv organizacije).
4. Promena svih lozinki za resurse kojima upravlja _____ (Naziv organizacije) vrši se na period od _____ meseci.
5. Lozinke moraju biti duge najmanje 15 karaktera, moraju sadržati posebne karaktere (npr. znaci interpunkcije), velika slova, mala slova i cifre. Lozinke ne smeju sadržati podatke o ličnosti zaposlenih (npr. imena, prezimena, datume rođenja, brojeve telefona, adrese stanovanja) niti njima bliskih lica (npr. članova uže porodice).
6. Za naročito osetljive resurse (npr. baze koje sadrže podatke naročito osetljive prirode: žrtve nasilja, zdravstveno stanje, seksualno opredeljenje itd) neophodno je uvesti zaštitne fraze (passphrases) koje čine nizovi nasumično odabranih reči u kombinaciji

sa drugim obaveznim elementima za lozinke iz tačke 5. ove politike. Zaštitne fraze moraju da budu dužine najmanje 20 karaktera.

7. Lice u organizaciji zaduženo za administriranje lozinkama je _____ (ime i prezime, radno mesto).
8. Po dodeli lozinke za naloge koji se koriste za poslove i aktivnosti _____ (Naziv organizacije), kao što su recimo službeni mejl nalozi, zaposleni su dužni da datu lozinku promene u skladu sa ovom politikom odmah pošto je dobiju od nadležnog lica koje je kreiralo nalog (npr. tehnički administrator) i dodelilo ga zaposlenom. Nove lozinke moraju biti generisane i skladištene u menadžeru lozinki.
9. Lozinke i zaštitne fraze se čuvaju u posebnim aplikacijama namenjenim isključivo za upravljanje lozinkama (npr. KeePass, KeePassXC, Bitwarden) koje čuvaju bazu lozinki u zaštićenom obliku. Čuvanje lozinki u internet pregledačima (internet browsers) i na sajtovima za onlajn čuvanje lozinki nije dozvoljeno.
10. Pravljenje rezervne kopije baze lozinki koja se čuva na eksternoj memoriji (npr. eksterni hard disk, USB fleš memorija) se vrši prilikom svake izmene lozinki i zaštitnih fraza (dodavanje novih ili menjanje starih) i obavezno se u nazivu fajla označava datum kada je napravljena.
11. U slučaju da zaposleni primeti ili posumnja da je bilo koji resurs kojim upravlja _____ (Naziv organizacije) kompromitovan, odmah će o tome obavestiti nadređenog i promeniti lozinku ili zaštitnu frazu za taj resurs, a ukoliko je reč o resursu koji se zajednički koristi obavestiće lice u organizaciji zaduženo za administriranje lozinkama.
12. Ova politika stupa na snagu ____ dana od dana donošenja.

Datum: _____ Ovlašćeno lice organizacije: _____
Mesto: _____

Primer Politike e-pošte i naloga

Naziv i adresa organizacije

Politika korišćenja email i pratećih naloga _____ (naziv organizacije)

U ovoj politici su sadržani uslovi korišćenja email i pratećih naloga na internet domenima u vlasništvu _____, i to: _____ **(upisati domene, npr. organizacija.rs)** (u daljem tekstu: domeni _____).

1. Email i prateći nalozi kreirani za potrebe rada, obavljanja prakse i volontiranja u _____ su u vlasništvu _____.
2. _____ upravlja nalozima i izdaje ih na korišćenje licima koja su u radnom odnosu u _____, licima koja su na praksi i licima koja volontiraju.
3. Lice kome je izdat email nalog koristi nalog i _____ nema uvid

u sadržaj tog naloga niti u njegove prateće delove (cloud storage, kolaborativni dokumenti i sl).

4. Nalozi na domenima _____ se koriste isključivo u svrhe koje odredi _____.
5. U slučaju prestanka odnosa između _____ i lica kome je izdat nalog, vlasništvo naloga ostaje kod _____.
6. _____ će ostaviti rok od 30 dana od dana prestanka odnosa da lice kome je izdat nalog prikupi iz naloga sav sadržaj koji smatra da će mu biti potreban.
7. Posle isteka roka od 30 dana od prestanka odnosa nalog će biti izbrisan, a kopija sadržaja arhivirana za potrebe _____.
8. Politika stupa na snagu danom donošenja.
9. Lica kojima su dodeljeni nalozi će biti obaveštena o svakoj budućoj izmeni ove politike.

Mesto i datum,

Odgovorno lice

_____

Primer Bezbednosnog plana

CILJ	**Unaprediti digitalnu bezbednost organizacije kao celine i njenih pojedinačnih članova**
PRETNJE I RIZICI	• Kompromitacija podataka o ličnosti i poverljivih informacija (dokumenti, prepiske...) • Kompromitacija tehničke infrastrukture i resursa organizacije • Gubitak kontrole nad infrastrukturom i podacima kao rezultat
PREVENTIVNI KORACI	• Pristup infrastrukturi i resursima organizacije (serveri, mrežna oprema, nalozi na društvenim mrežama, admin paneli sajtova...) omogućen samo određenim licima i zaštićen jakim lozinkama koje se čuvaju u posebnim aplikacijama za tu namenu (password managers, npr. KeePass) • Usvojena politika lozinki organizacije • Dvostruka autentifikacija (2-step authentication) uključena na svim korisničkim nalozima koji je podržavaju. • Naročito osetljive podatke (npr. informacije o žrtvama seksualnog nasilja) čuvati enkriptovane, na posebnim uređajima koji se ne koriste za svakodnevni rad. • Uređaji zaposlenih zaštićeni lozinkama/pin kodovima • Redovno pravljenje rezervnih kopija podataka (backup) na lokalnim uređajima (npr. eksterni hard diskovi) i/ili onlajn (na serveru organizacije ili na cloud uslugama, npr. Dropbox, Google Drive, OneDrive...). **Međutim, naročito osetljive podatke o ličnosti i druge poverljive informacije ne treba čuvati na cloud servisima.** • Za razmenu poverljivih informacija koristiti enkriptovane mejlove (PGP) i čet aplikacije (Signal).

KORACI U SLUČAJU INCIDENTA	• Što pre obavestiti nadležne kolege (administratore zadužene za tehničku infrastrukturu u organizaciji) i tehničku podršku (npr. hosting kompaniju) i pratiti njihove instrukcije • Prikupiti sve dostupne informacije o incidentu (vreme, mesto, aktivnosti u toku incidenta, IP adrese, logovi, skrinšotovi, poslednje ispravne konfiguracije...) kako bi se utvrdila šteta i posledice • Obavestiti posebne/sektorske timove za reakciju u slučajevima sajber incidenata: **SHARE CERT**, čiji je osnivač SHARE Fondacija, prvi je poseban centar za zaštitu informacionih sistema onlajn i građanskih medija i prevenciju od rizika u sajber okruženju: Adresa: Kapetan Mišina 6a, kancelarija 31, Beograd Email: info@sharecert.rs, emergency@sharecert.rs Sajt: sharecert.rs Telefon: 064 089 7067 • Prijaviti incident nadležnim državnim organima: **MUP Republike Srbije, Odeljenje za borbu protiv visokotehnološkog kriminala** (pri Službi za borbu protiv organizovanog kriminala Uprave kriminalističke policije): Adresa: Bulevar Mihaila Pupina 2, Beograd Email: ukp@mup.gov.rs Sajt: mup.gov.rs **Posebno tužilaštvo za borbu protiv visoko-tehnološkog kriminala:** Adresa: Savska 17a, Beograd Email: vtk@vtk.jt.rs Sajt: beograd.vtk.jt.rs Telefon: 011 745 1233 **Ako su kompromitovani podaci o ličnosti, neophodno je obavestiti Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti:** Adresa: Bulevar kralja Aleksandra 15, Beograd Email: office@poverenik.rs Sajt: poverenik.rs Telefon: 011 3408 900 • Proveriti poslednju dostupnu verziju podataka/konfiguracije sistema radi pokušaja vraćanja u pređašnje stanje i rekonstrukcije napada

PREPORUČENI UREĐAJI I OPREMA	• Mobilni telefoni sa instaliranim enkriptovanim čet aplikacijama (Signal) • Računari: instaliran i redovno ažurirani anti-virus softver, kao i svi ostali softveri koji se koriste • Računari: instaliran menadžer lozinki (npr. KeePass, KeePassXC, Bitwarden) • Računari: instaliran softver za enkripciju hard diska (VeraCrypt) • Kreirani PGP ključevi za mejlove zaposlenih i instaliran odgovarajući softver (npr. Thunderbird, Mailvelope) • Browsers: Mozilla Firefox, instalirani dodaci (Privacy Badger, uBlock Origin, minerBlock) ili Brave na kome se mogu instalirati verzije dodataka za Google Chrome • Na uređajima instaliran pouzdan VPN (npr. Mullvad, ProtonVPN) i Tor Browser
PRIMENA INTERNIH PROCEDURA (PRIMER)	Među zaposlenima je primećeno je da je sajt organizacije nedostupan ili da se stranica teško učitava 1. Proveriti dostupnost stranice na servisu “Down For Everyone Or Just Me” (https://downforeveryoneorjustme.com/) i internet konekciju 2. Izvršiti skeniranje svih računara i uređaja anti-virus softverom 3. Ukoliko se utvrdi da nije reč o tehničkom problemu, zaposleni obaveštava tehničkog administratora organizacije lično ili putem sigurnog kanala komunikacije (Signal čet, enkriptovana mejl poruka) 4. Administrator, u saradnji sa tehničkom podrškom, izvršava proveru infrastrukture i ukoliko se utvrdi da je došlo do neuobičajenog saobraćaja, neovlašćenog pristupa ili druge povrede integriteta informacionog sistema, vrši prikupljanje digitalnih dokaza 5. Sledi pokušaj povraćaja podataka/povraćaj funkcionalnosti pomoću rezervnih kopija i/ili poslednjih dobrih konfiguracija 6. Sledi utvrđivanje vrste napada i pravne kvalifikacije, obaveštavanje nadležnih organa i pripremanje podnesaka (npr. krivične prijave) u saradnji sa posebnim/sektorskim timovima (npr. SHARE CERT)

POGLAVLJE 8: ZAKLJUČAK

Opšti zaključak o digitalnoj bezbednosti obuhvata svest o stalnom rastu broja sajber pretnji i neophodnost razvoja efikasnih mera zaštite. Sa porastom digitalne povezanosti, postaje ključno razumeti prirodu pretnji i preduzimati odgovarajuće korake kako biste sačuvali svoje digitalne resurse.

Ukratko, digitalna bezbednost zahteva sveobuhvatni pristup koji obuhvata tehničke, organizacione i edukativne mere. Svest o sajber pretnjama i dosledno sprovođenje bezbednosnih praksi ključni su faktori u očuvanju integriteta digitalnih resursa.

8.1. Pregled brzih preporuka za digitalnu bezbednost

Lozinke:

- Primena politike lozinki organizacije kroz upotrebu jedinstvenih, dugačkih i nasumičnih lozinki za zaštitu svih naloga i uređaja koji se koriste;
- Podešavanje dvostruke autentifikacije (2FA) na nalozima gde postoji tehnička mogućnost. Umesto SMS-a ili ako ne posedujete bezbednosni USB ključ, preporučeni oblik za 2FA je mobilna aplikacija (npr. Google Authenticator) na servisima koji podržavaju upotrebu aplikacija za generisanje pristupnih kodova;
- Imajući u vidu način rada i kontekst obavljanja posla organizacije, preporuka je da se koristi menadžer lozinki Bitwarden koji je dostupan za računare, mobilne uređaje i kao dodatak za internet brauzere, a poseduje i veb verziju. Takođe, poslovni Bitwarden paket daje mogućnost centralizovanog upravljanja svim lozinkama, što je često predočeno kao jedan od problema sa organizacionom zaštitom lozinki.

Bezbedno čuvanje podataka i rezervne kopije (bekap):

- Radi pojednostavljenja rukovanja podacima, organizacija može da pređe na Google Workspace i u okviru nje koristi Google Drive platformu, koja omogućava bezbedno deljenje i čuvanje podataka i dokumenata;
- Jedna od predloženih mera je i enkriptovanje hard diskova računara uz pomoć alata VeraCrypt i FileVault i enkriptovanje klaud rešenja uz pomoć alata Cryptomator. Ukoliko organizacija želi da čuva i bekapuje podatke u klaudu sa end-to-end enkripcijom, postoje rešenja kao što su Proton Drive i Tresorit;
- Još jedna mogućnost jeste da se koristi bekap sistem otvorenog koda, kao što je UrBackup.

Zaštita Wi-Fi mreže:

- Potrebno je podesiti lozinku za Wi-Fi mrežu u podešavanjima rutera, većina proizvođača podržava WPA2-PSK (AES) verziju zaštite bezične mreže koju treba odabrati kao bezbedniju. Podešenu lozinku za pristup mreži ne treba deliti javno, već samo sa autorizovanim osobama;
- Ukoliko postoji sumnja da su nepoznati uređaji povezani na bežičnu mrežu, može se izvršiti provera svih povezanih uređaja koji se mogu identifikovati preko njihove MAC adrese;
- Većina modernih rutera poseduje mogućnost da se podesi odvojena mreža za posetioce,

tzv. “guest network”, odnosno mreža kojoj mogu da pristupaju lica koja dolaze u prostorije organizacije ali nisu ovlašćena da pristupe glavnoj mreži.

Zaštita interne i eksterne komunikacije:

- Mejl komunikacija može da se enkriptuje koristeći Thunderbird program ili dodajući ekstenziju za brauzer Mailvelope, koja radi na popularnim vebmejl servisima;
- Postoje mejl provajderi, kao što su ProtonMail ili Tuta, koji automatski enkriptuju poruke koje razmenjuju njihovi korisnici, a takođe omogućavaju slanje enkriptovanih mejlova nekome ko koristi druge provajdere;
- Da bi se obezbedilo komuniciranje preko poruka, preporučljivo je koristiti aplikacije koje takođe imaju omogućenu enkripciju. Signal je široko rasprostranjena besplatna čet aplikacija otvorenog koda koja pruža end-to-end enkripciju.

Antivirus/antimalver:

- Na sve računare i mobilne telefone instalirati antivirus/antimalver softver pouzdanog proizvođača i vršiti redovna skeniranja, a naročito u slučaju da su primećene smetnje u radu koje mogu ukazivati na incident, odnosno zaražavanje uređaja malverom;
- Prilikom priključivanja prenosivih uređaja (USB fleš memorije, eksterni hard diskovi) u računare potrebno ih je skenirati antivirus/antimalver softverom;
- Bitdefender antivirus je preporučeno rešenje imajući u vidu da je dobro rangiran u ekspertskoj zajednici, da se licence mogu povoljno nabaviti putem Techsoup programa za neprofitne organizacije, te da poseduje verzije za računare i mobilne telefone.

Računari:

- Potrebno je da svi računari budu redovno ažurirani, odnosno da se operativni sistem i sav instaliani softver redovno ažuriraju;
- Instalacija krekovanog softvera predstavlja značajan rizik te je potrebno pronaći alternative koje su besplatne i otvorenog koda (free and open source software) ili pribaviti licence za komercijalna rešenja po povoljnijim uslovima ukoliko su dostupna preko Techsoup ili sličnih programa za neprofitne organizacije.

Mobilni uređaji:

- Potrebno je da svi mobilni uređaji, i privatni i službeni, budu redovno ažurirani, odnosno da se operativni sistem i sve aplikacije redovno ažuriraju;
- Ukoliko najnovije verzije operativnog sistema, a naročito bezbednosna ažuriranja koja obezbeđuju proizvođači, više nisu dostupna za korišćene modele uređaja, neophodno je izvršiti njihovu zamenu.

Fišing:

- Zaposleni treba da budu obučeni da sprovode osnovnu analizu mejlova i provere autentičnost sumnjivog mejla, kao i sumnjivih priloga i linkova u mejlu;
- Za analizu sumnjivih informacija i artefakata se preporučuju dva alata - VirusTotal i PhishTool - s tim da je važno biti pažljiv u pogledu toga koje informacije se analiziraju pomoću ovih alata i da se kada su u pitanju osetljivi, lični podaci ne koriste ovi alati;
- Preporučeno je da organizacije sve nove saradnike i zaposlene obuče načinima za proveru

verodostojnosti poruke u skladu sa znanjima stečenim kroz priručnik. Dobra praksa je da zaposleni povremeno urade fišing test i provere njihovo znanje - jedan primer testa se može pronaći ovde.

8.2. Pomoć u reagovanju na incidente

SHARE Fondacija je osnovala SHARE CERT, prvi CERT (Computer Emergency Response Team) u Srbiji specijalno namenjen za online medije i organizacije civilnog društva. Aktivnosti SHARE CERT-a takođe uključuju pružanje pro bono pravne i tehničke podrške kod incidenata, posebno organizacijama koje prolaze kroz proces mentorstva u oblasti digitalne bezbednosti.

Tok procesa pomoći pri incidentu je sledeći:

- Obaveštavanje našeg tima putem mejla (ako je moguće korišćenjem PGP enkripcije) o incidentu;
- Naš tim se javlja tražeći dodatne informacije u zavisnosti od vrste incidenta i daje dalja uputstva u cilju istrage incidenta;
- Ukoliko je potrebno, naš tim kontaktira internacionalne partnere i mreže za pomoć. Kao članovi CiviCERT-a, udruženja CERT-ova civilnog društva, naš tim sarađuje sa linijom za pomoć Access Now kada je potrebno eskalirati određeno bezbednosno pitanje višim instancama, npr. kada korisnik izgubi pristup nalogu za društvene mreže a ne može da ga vrati pomoću regularnog procesa povratka;
- Nakon incidenta, naš tim daje preporuke i savete o tome kako zaštititi informaciona sredstva i tehničku infrastrukturu.

U slučajevima gde postoji visok stepen sumnje da su mobilni telefoni novinara i aktivista zaražen ili targetiran naprednim špijunskim softverom kao što su Pegasus ili Predator, tim SHARE CERT-a može uz saradnju sa stručnim organizacijama Access Now, Citizen Lab i Amnesty Tech pomoći da se izvrši analiza uređaja.