VODIČ ZA DIGITALNU BEZBEDNOST BRANITELJA I BRANITELJKI LJUDSKIH PRAVA I ORGANIZACIJA CIVILNOG DRUŠTVA

Шведска
Sverige

Centar za podršku ženama
Center for Support of Women

OEBS Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

SADRŽAJ

PROCENA RANJIVOSTI I TEHNIČKA OTPORNOST

RIZICI, JAVNI NAPADI I REAGOVANJE

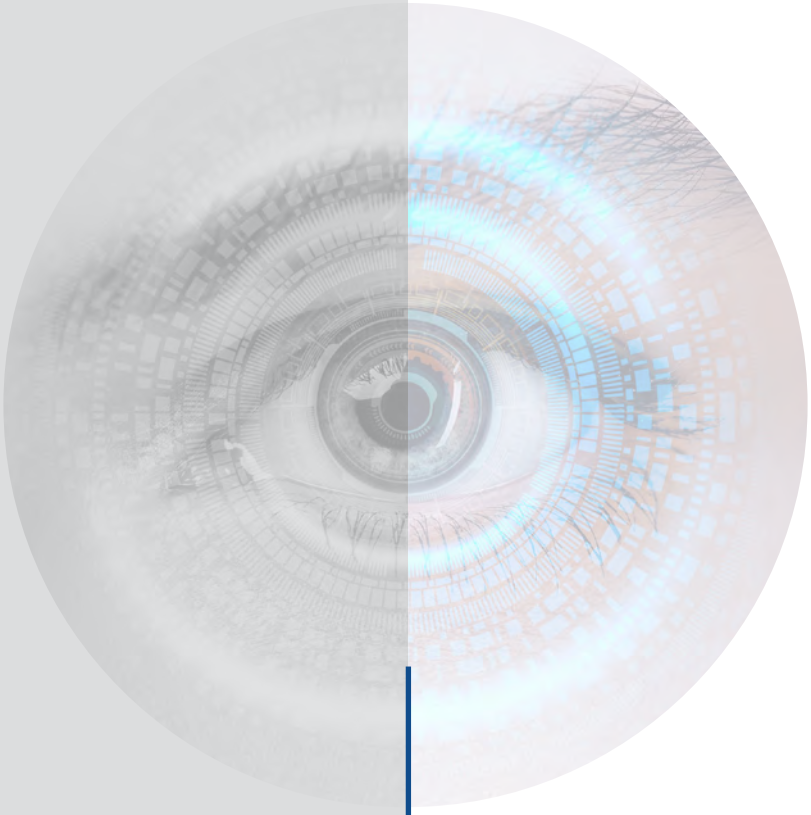
Izradu ove publikacije omogućila je Misija OEBS-a u Srbiji u okviru projekta „Konsolidovanje procesa demokratizacije u sektoru bezbednosti u Republici Srbiji" koji je finansijski podržala Vlada Švedske.

Svi pojmovi koji su u publikaciji upotrebljeni u muškom gramatičkom rodu obuhvataju muški i ženski rod lica na koja se odnose.

Шведска
Sverige

Centar za podršku ženama
Center for Support of Women

oebs Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji



VODIČ ZA DIGITALNU BEZBEDNOST BRANITELJA I BRANITELJKI LJUDSKIH PRAVA I ORGANIZACIJA CIVILNOG DRUŠTVA

2025.

Autorka: Danijela Maljević
Urednice: Biljana Stepanov i Dragica Reljanović
Izdavač: Centar za podršku ženama
Za izdavača: Biljana Stepanov

Dizajn: Aleksandra Milaković Radinović

ISBN 978-86-87681-17-0

Predgovor

Prisutnost u digitalnom prostoru danas je neizostavni deo savremenog života- kako u privatnoj, tako i u profesionalnoj sferi. Informaciono-komunikacione tehnologije i digitalni alati omogućavaju nam da učimo, povezujemo se, gradimo mreže solidarnosti, širimo poruke i povećavamo domet svog delovanja. Za branitelje i braniteljke ljudskih prava, kao i za organizacije civilnog društva, digitalni prostor predstavlja ključni kanal za zagovaranje, informisanje i mobilizaciju zajednica.

Istovremeno, vidljivost u digitalnom prostoru nosi i ozbiljne rizike. Organizacije i pojedinci/ke koji se bave rodnom ravnopravnošću, borbom protiv nasilja, mirovnim i bezbednosnim pitanjima, sve su češće izložene/i ciljanim napadima, uznemiravanju, nadzoru i pokušajima diskreditacije u online okruženju. Digitalni napadi nisu izolovani incidenti- oni su deo šireg konteksta pritisaka na civilno društvo i pokušaja sužavanja prostora za kritičko delovanje. U tom smislu, koliko je važno biti prisutan u digitalnom prostoru, jednako je važno znati kako se u njemu zaštititi.

Ova publikacija ima za cilj da doprinese unapređenju praksi digitalne bezbednosti i jačanju lične i organizacijske otpornosti branitelja/ki ljudskih prava i organizacija civilnog društva. Vodič polazi od razumevanja digitalne bezbednosti kao svakodnevne prakse, a ne isključivo kao tehničkog pitanja. On podstiče

promišljanje ličnih i organizacionih rizika, ali i nudi konkretne alate, preporuke i procedure koje mogu pomoći u prevenciji napada, kao i u adekvatnom reagovanju kada do njih dođe.

Poseban fokus stavljen je na zaštitu identiteta u online prostoru, bezbedno korišćenje društvenih mreža, upravljanje osetljivim podacima i planiranje reagovanja u situacijama digitalnih napada- kako u *online*, tako i u *offline* kontekstu. Vodič prepoznaje i rodnu dimenziju digitalnog nasilja, imajući u vidu da su žene, a naročito aktivistkinje i braniteljke ljudskih prava, nesrazmerno često mete seksualizovanih pretnji, kampanja mržnje i pokušaja javne diskreditacije.

Vodič za digitalnu bezbednost branitelja/ki ljudskih prava i organizacija civilnog društva doprinosi ostvarivanju ciljeva Nacionalnog akcionog plana za primenu Rezolucije SB UN 1325 „Žene, mir i bezbednost", kroz stvaranje podsticajnog i bezbednog okruženja za smisleno učešće žena u mirovnim, bezbednosnim i društvenim procesima.

Verujemo da digitalna bezbednost nije individualna odgovornost, već zajednička praksa zasnovana na znanju, solidarnosti i međusobnoj podršci. Nadamo se da će ovaj vodič poslužiti kao praktičan alat, ali i kao podsticaj za dalje učenje, razmenu iskustava i jačanje kolektivne otpornosti u digitalnom prostoru

Uvod

Digitalna bezbednost kao svakodnevna praksa

Svako jutro budimo se u digitalnom svetu koji je već značajno drugačiji od prethodnog. Algoritmi su se (ne)primetno ažurirali, pojavile su se nove aplikacije, a pretnje koje juče nismo mogli ni da zamislimo danas su već deo naše svakodnevice. Tehnologija se menja brzo, pa ujedno raste i naša potreba za sigurnošću, poverenjem i otpornošću.

Ovaj vodič je nastao kao odgovor na te ubrzane promene, koje često nisu praćene odgovarajućim mehanizmima zaštite. Infrastruktura je moćna, a oni koji je koriste u borbi za ljudska prava često se suočavaju sa najvećim bezbednosnim izazovima.

Kako se tehnologija menja, menjaju se i načini na koje se sprovode nadzor, kontrola i digitalni napadi. Prvi korak nije tek neki novi alat, već dogovorene navike i spremnost da učimo. Tehnika jeste važna, ali su kontekst, odnosi moći i rizici podjednako presudni. Ako stojimo u mestu u digitalnom svetu, to ne znači samo da zaostajemo već i da postajemo sve izloženiji i ranjiviji.

Digitalni napadi na branitelje/ke ljudskih prava i organizacije civilnog društva predstavljaju pokušaje da se oslabi kritičko delovanje i ućutka politički otpor. U svemu ovome žene su posebno ranjive i rodna dimenzija digitalnog nasilja se vrlo brzo prepoznaje. Žene su u digitalnom svetu meta seksualizovanih pretnji iz najrazličitijih povoda. Protiv njih se vode kampanje mržnje i pokušaji diskreditacije koji često ne ostaju samo na internetu, već prelaze u stvarni život i nose realne posledice.

Digitalne platforme daju civilnom društvu vidljivost i domet, ali u Srbiji ta ista vidljivost često znači i da ste pod reflektorom nadzora. Najnoviji izveštaji o forenzičkim alatima i špijunskim softverima pokazuju da zloupotreba tehnologije ugrožava rad civilnog društva u kome mnoge organizacije još uvek nemaju uspostavljene protokole zaštite.

Moćni akteri na globalnom nivou koriste digitalne alate za nadzor, manipulaciju i cenzuru. Zato su zajednički protokoli, savezništva i razmena iskustava ključni deo zaštite. Ne traži se savršeno tehničko znanje, već doslednost i solidarnost.

Ako vodič pomogne **bar jednoj organizaciji** da uvede redovan *backup* (rezervna kopija podataka), **bar jednoj osobi** da uključi dvofaktorsku zaštitu i **bar jednom timu** da uspostavi rutinu prijavljivanja incidenata, postigao je cilj.

Kako koristiti ovaj Vodič

Ovaj vodič je zamišljen kao brz i jasan alat i da u pravom trenutku ponudi ono što je najpotrebnije. Ne morate da ga čitate od početka do kraja, bolje je da ga koristite selektivno, u skladu sa vremenom koje imate, trenutnom potrebom ili svojom ulogom u organizaciji.

Ako vam treba brzi uvid za potrebe lične digitalne bezbednosti, fokusirajte se na delove koji donose najvažnije korake i alate koji mogu da podignu bezbednost već u kratkom roku:

- Lični minimum digitalne bezbednosti (lozinke, 2FA, osnovna higijena uređaja)
- Prepoznavanje neposrednih rizika (fišing - mrežna krađa identiteta, doksing - objavljivanje privatnih podataka), nadzor, nasilje na mreži)
- Šta raditi kada se pojavi sumnja na digitalni napad (mini-protokol za incident)

Ako tek počinjete rad u organizaciji civilnog društva i treba vam da se upoznate sa procedurama i politikama, krenite od sledećeg, pre nego se upoznate sa protokolima koji su već usvojeni u vašoj organizaciji:

Osnovna pravila i politike organizacije, na primer:

- kako se čuva pristup zajedničkim nalozima
- kako se radi *backup*
- šta se smatra osetljivim podacima

Bezbedna komunikacija i rad sa osetljivim informacijama

- Kome se prijavljuje problem (kontakt osobe, interni protokoli)

Cilj je da što pre postane jasno šta je redovna aktivnost, a šta može da bude rizik.

Ako ste osoba zadužena za digitalnu bezbednost u organizaciji, ne morate da znate svaki tehnički detalj, važnije je da znate kako se bezbednost organizuje i održava. To obično uključuje:

- Organizacijske nivoe bezbednosti (politike, kontrole pristupa, klasifikacija podataka)
- Protokole za upravljanje incidentima
- Podršku timu tokom napada (psihološka bezbednost, komunikacija, raspodela/redistribucija uloga)

Ovaj set pomaže da vodite tim kroz krizne situacije i da sprečite većinu problema pre nego što se uopšte pojave.

Za one koji rade direktno sa žrtvama nasilja ili sa osetljivim zajednicama, prioriteti su jasni:

- Bezbedno skladištenje osetljivih podataka i evidencija
- Zaštita identiteta žrtava i poverljivost komunikacije
- Bezbedna razmena dokaza i materijala
- Reagovanje na digitalno nasilje i reputacione napade

Cilj je jednostavan: da se nijednim korakom ne ugrozi osoba kojoj se pruža podrška.

DIGITALNA BEZBEDNOST I OSNOVE SAMOZAŠTITE

1. Digitalna bezbednost i samozaštita
2. Osnove digitalne bezbednosti

1. Digitalna bezbednost i samozaštita

Digitalna bezbednost nije zbir tehničkih trikova, nego svakodnevna praksa kojom štitimo sebe, svoje kontakte i svoj rad. Za branitelje/ke ljudskih prava i organizacije civilnog društva digitalni prostor je infrastruktura rada bez koje nema stabilnog i sigurnog delovanja.

Samozaštita se ne zasniva na ideji da budemo nevidljivi na internetu, već na tome da razumemo gde su naši rizici, kako najčešći napadi izgledaju i šta svako od nas može da uradi da ostane dovoljno zaštićen da bi mogao da nastavi svoj rad.

U ovom vodiču se lični i organizacijski nivo bezbednosti stalno prepliću. Znanja i veštine o pretnjama i načinima reagovanja su univerzalni, a kada se neka mera ili preporuka odnosi posebno na jedan od tih nivoa, to će biti jasno naznačeno sledećim ikonicama:

LIČNI NIVO

TIMSKI NIVO

ORGANIZACIJSKI NIVO

MINUM BEZBEDNOSNIH MERA

NAPREDNE PRAKSE

1.1. Oblici digitalnog nasilja

Digitalno nasilje obuhvata namerne radnje u digitalnom prostoru kojima se pojedinac ili organizacija zastrašuje, kompromituje, ometa u radu ili izlaže riziku. U praksi se najčešće ispoljava kroz tri vrste napada: **(1)** napade na osobe i reputaciju, **(2)** napade na privatnost i fizičku bezbednost i **(3)** napade na naloge, podatke i komunikaciju.

Ovi oblici se često prepliću. Ista kampanja može istovremeno uključiti uznemiravanje, lažne naloge i manipulaciju sadržajem. Takođe, lični podaci do kojih se dođe jednim napadom (na primer fišingom) mogu postati okidač za doksing, pretnje i druge oblike nasilja koji se potom preliju i van interneta.

Da bi se brže prepoznalo „šta se dešava", korisno je razlikovati **metod** i **cilj** napada:

- **Metod**: da li je napad komunikacioni (uvrede/pretnje), informativni (objava privatnih podataka), tehnički (krađa naloga), ili medijski/manipulativni (montaže, izvlačenje iz konteksta).
- **Cilj**: da li je primarni cilj zastrašivanje i utišavanje, diskreditacija pred publikom, preusmeravanje narativa, ili onemogućavanje rada (gubitak naloga/podataka, prekid komunikacije).

U nastavku sledi pregled **najčešćih oblika digitalnog nasilja** sa kojima se branitelji/ke ljudskih prava i organizacije civilnog društva susreću. Tabela služi kao brza orijentacija: pomaže da prepoznamo šta se dešava, zašto se dešava i koji su prvi koraci koje možemo da preduzmemo.[1]

OBLIK NASILJA	KAKO IZGLEDA U PRAKSI	TIPIČNE POSLEDICE	PRVA BEZBEDNA REAKCIJA
Ciljano uznemiravanje	Talasi uvreda, pretnji, spam poruka, koordinisano prijavljivanje naloga	Strah, iscrpljivanje, povlačenje iz javnosti, autocenzura	Ne ulaziti u raspravu; dokumentovati; prijaviti platformi; aktivirati mrežu podrške
Doksing	Objavljivanje adrese, broja, privatnih fotografija, podataka o porodici	Fizička ugroženost, napadi offline, osećaj izloženosti	Hitno uklanjanje tragova; prijava platformi/policiji; bezbednosni plan za *offline*

1 SHARE Fondacija dokumentuje oblike digitalnog nasilja u Srbiji (doksing, uznemiravanje, pretnje, zloupotreba privatnih sadržaja) i naglašava rodnu dimenziju napada https://sharefoundation.info

Fišing	Lažne poruke „partnera”, „banke”, „platforme” koje traže lozinku ili klik	Gubitak naloga, curenje podataka, reputacijska šteta	Ne kliktati; proveriti identitet drugim kanalom; promeniti lozinke; uključiti 2FA
Manipulacija sadržajem	Montaže, lažne izjave, izvlačenje iz konteksta, deepfake	Diskreditacija, gubitak poverenja, medijski linč	Sačuvati originalne dokaze; javno kratko demantovati; prijaviti i pravno konsultovati
Lažni nalozi/ imitacija identiteta	Profil koji se predstavlja kao aktivistkinja/ organizacija i širi laži	Zbunjenost publike, rušenje kredibiliteta, preusmeravanje narativa	Dokumentovati; prijaviti platformi; obavestiti publiku sa proverenih kanala
Bot kampanje	Automatizovani nalozi koji napadaju, šire laži ili pumpaju mržnju	Percepcija „masovne osude”, pritisak na tim, širenje dezinformacija	Mapirati obrasce; ne hraniti kampanju; aktivirati saveznike; moderacija

2. Osnove digitalne bezbednosti

Ovo poglavlje je pre svega namenjeno organizacijskom nivou rada. Ipak, principi bezbednosti koje ovde predstavljamo nisu samo za organizacije i najbolje funkcionišu kada ih svako od nas prevede u svakodnevne lične digitalne navike i postepeno ih unapređuje.

Ako želimo organizaciju koja je zaista otporna, moramo da usvojimo osnovne principe digitalne bezbednosti. Ti principi ne zavise od ličnih preferenci članova i članica, veličine organizacije, fokusa rada ili nivoa tehničke pismenosti. Oni su temelj bezbednog radnog okruženja. Mnogi vodiči za branitelje/ke ljudskih prava i organizacije civilnog društva naglašavaju isto: digitalna bezbednost počinje jasnim praksama i zajedničkim dogovorima, a ne savršenim alatom.[2]

Ignorisanje ovih osnova nije samo tehnički propust. To znači izlaganje ljudi, podataka i same misije organizacije riziku koji može imati dugoročne posledice, od gubitka poverenja korisnika/ca i zajednice, preko prekida rada, do fizičke ugroženosti u situacijama kada digitalni napad eskalira u realni svet.[3]

Svako u organizaciji treba da zna kako da prepozna sumnjivu aktivnost, zaštiti svoje naloge, koristi bezbedne kanale komunikacije i reaguje kada nešto pođe po zlu, jer tako doprinosi bezbednosti cele organizacije.

2 Tactical Tech https://tacticaltech.org/projects/security-in-a-box
3 United Nations https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework

Tehnička infrastruktura može biti odlično podešena, ali je dovoljan jedan klik na zlonamerni link ili ista lozinka na više naloga da cela organizacija postane ranjiva.

Zato je važno i da svako u timu razume svoj nivo rizika: koje podatke čuva, sa kim komunicira, šta bi napadač dobio ako preuzme njihov nalog i kakve bi posledice to moglo da ima, ne samo po tu osobu, već i po druge. To je procena rizika, standardan korak u bezbednosnom planiranju.

2.1. Jasna pravila, edukacija i kultura prakse

Organizacije često funkcionišu na osnovu neformalnih dogovora, što može biti praktično, ali u kontekstu bezbednosti je opasno. Potrebno je definisati:

- Ko ima pristup kojim podacima (princip najmanjeg potrebnog pristupa);
- Kako se lozinke kreiraju i dele (nikad *e-mail*-om ili u *chat*-ovima bez enkripcije);
- Koje platforme se koriste za internu komunikaciju;
- Kako se čuvaju osetljivi dokumenti i *backup*-ovi;
- Šta se radi kada se sumnja na kompromitaciju.

Ove procedure ne moraju biti komplikovane, ali moraju biti jasne, dosledne i dostupne svima.

Edukacija je drugi stub. Alati se menjaju iz dana u dan, ali osnovne veštine ostaju iste: prepoznati fišing poruku, razumeti dozvole koje aplikacije traže, pažljivo rukovati linkovima i prilozima, i proceniti rizik pre nego što nešto kliknemo, podelimo ili preuzmemo. *Access Now helpline*, servis koji pruža direktnu tehničku podršku i savete u realnom vremenu organizacijama i aktivistima civilnog društva, medijima, novinarima i braniteljima/kama ljudskih prava širom sveta, fišing navodi kao jedan od najčešćih ulaznih vektora napada što dodatno potvrđuje koliko je stalna obuka važna.

Edukacija tima mora biti kontinuirana, prilagođena kontekstu, praćena praktičnim vežbama, i u nju moraju biti uključene praktične vežbe. Nije dovoljno poslati PDF sa uputstvima. Potrebno je razgovarati, prolaziti kroz različite scenarije i graditi poverenje u to da tim može da reaguje kada se nešto desi. Bezbednost je veština i najbolje se održava vežbom.

2.2. Dokumentovanje i solidarnost kao odgovor na incidente

Incidenti se dešavaju, to je realnost. Ono što otpornu organizaciju razlikuje od ranjive nije odsustvo problema, već način na koji na njih reaguje: da li ume da ih zabeleži, razume i iz njih izvuče pouku. Zato svaku sumnjivu aktivnost, pokušaj napada ili čak „običnu" grešku vredi dokumentovati. Ne da bismo tražili krivca, već da bi se gradila institucionalna memorija: šta se desilo, kako je izgledalo, šta je pomoglo, a šta nije. Upravo tu počinje otpornost. Ovakav pristup je standard u *incident-response* (odgovoru na incident) praksi u civilnom društvu.[4]

Dokumentovanje znači i jednu jednostavnu, ali ključnu rutinu: ko prijavljuje incident, kome se prijavljuje, gde se čuvaju logovi i skrinšotovi, kako se beleži tačno vreme događaja i koje naloge ili uređaje incident obuhvata. Bez tih osnova, organizacije lako upadaju u začarani krug, ponavljaju iste greške i ne primećuju za sopstvene ranjivosti.

A pošto digitalna bezbednost nije individualna borba, ona traži i mrežu podrške: razmenu znanja, kolektivnu zaštitu i spremnost da reagujemo kada neko iz zajednice bude napadnut. *Access Now helpline*[5] postoji upravo iz tog razloga, kao praktičan bezbednosni resurs zasnovan na solidarnosti, gde se u trenutku incidenta može dobiti stručna i hitna podrška.

Organizacije treba da grade savezništva, dele resurse, konsultuju stručnjake i ne ostavljaju pojedince same sa posledicama digitalnog nasilja.

2.3. Bezbedno skladištenje podataka ★★

U digitalnom radu organizacija civilnog društva, podaci su srž svega. U njima je sačuvana istorija borbe, identiteti članova i članica, strategije, kontakti, dokumentacija, fotografije, izveštaji i prepiske. U ženskim organizacijama civilnog društva, posebno onima koje pružaju podršku žrtvama rodno zasnovanog nasilja, tu su često i baze korisnica. A u zavisnosti od fokusa rada, te korisnice mogu biti i osobe koje su preživele različite oblike eksploatacije i nasilja. Zato gubitak ili kompromitacija ovih podataka nije „samo" tehnički problem: to može direktno ugroziti bezbednost ljudi, narušiti reputaciju organizacije i prekinuti kontinuitet rada.

4 Amnesty International https://securitylab.amnesty.org/digital-resources
5 Access Now https://www.accessnow.org/about-us/

Zbog toga je bezbedno skladištenje podataka jedno od najvažnijih pitanja digitalne bezbednosti.

Važno je razumeti razliku između lokalnog i udaljenog (*Cloud*) online skladištenja podataka. Lokalno skladištenje, na laptopu, eksternom disku ili USB-u, daje direktnu kontrolu, ali nosi i očigledne rizike: fizički gubitak, krađu, kvar ili oštećenje uređaja. Cloud rešenja poput *Google Drive*-a, *Dropbox*-a ili *OneDrive*-a olakšavaju pristup sa više uređaja i nude automatsku sinhronizaciju. Ipak, ona traže pažljivo upravljanje pristupima, dodatne mere zaštite (poput enkripcije) i promišljanje o tome kome i koliko verujemo kao pružaocu usluge. Bezbednost u velikoj meri zavisi od toga kako koristimo opcije koje su nam na raspolaganju.

Mapiranje podataka znači da jasno znamo koje podatke imamo, gde se nalaze, ko im može pristupiti i kako su zaštićeni. Prvi korak je klasifikacija po osetljivosti. Na primer: **javni, interni, poverljivi i kritični**. Promotivni materijali mogu biti javni. Ali baze kontakata, finansijski izveštaji, interne strategije i komunikacija sa partnerima traže ozbiljniju zaštitu i višeslojni pristup. U praksi to znači da ne čuvamo sve na jednom mestu, pristup ograničavamo prema ulozi i potrebi (ko šta radi), a enkripciju koristimo i kada podaci miruju i kada se prenose.

Enkripcija (šifrovanje) znači da se podaci pretvaraju u nečitljiv format koji se može otključati samo odgovarajućim ključem. Postoje alati za šifrovanje pojedinačnih fajlova, ali i celih diskova u zavisnosti od toga šta želite da zaštitite. U *Cloud* okruženju dodatna enkripcija pre slanja podataka često je posebno važna, jer većina servisa ne nudi *end-to-end* (od kraja do kraja) zaštitu. Takođe, vredi izbegavati automatsku sinhronizaciju osetljivih fajlova na lične uređaje, naročito ako se ti uređaji koriste za više različitih namena.

Pristupne dozvole su još jedan kritičan deo digitalne bezbednosti. Organizacije često prave greške kada koriste zajedničke naloge ili kada zaborave da uklone pristup bivšim članovima tima. Zato svaki nalog treba da bude vezan za konkretnu osobu i zaštićen jakom lozinkom i dvofaktorskom autentifikacijom. Kada neko napusti organizaciju, pristup mora biti odmah ukinut. Važno je i da postoji jasna evidencija: ko ima pristup kojim folderima i dokumentima i da se te dozvole redovno proveravaju, kako bi ostale opravdane i svedene na minimum koji je potreban za rad.

Rezervne kopije su neizostavan deo bezbednog skladištenja - One se prave lokalno (na eksternim diskovima) i udaljeno (na sigurnim serverima), u redovnim intervalima, i moraju biti zaštićene od neovlašćenog pristupa. Idealno je imati najmanje

dve kopije (tri je još bolja opcija) jednu fizičku i jednu digitalnu koje se čuvaju na različitim lokacijama. Rezervne kopije ne smeju biti dostupne preko istih naloga kao originalni podaci, jer u slučaju kompromitacije, napadač može da uništi i *backup*.

Kultura odgovornosti prema podacima - Osetljivi dokumenti se ne šalju putem nesigurnih kanala, fajlovi se ne čuvaju na desktopu bez zaštite, ne koristi se javni *Wi-Fi* za pristup poverljivim informacijama, i redovno se ažurira softver koji upravlja skladištenjem. Bezbedno skladištenje nije samo tehnička praksa već izraz poštovanja prema ljudima čiji su podaci povereni organizaciji.

ORGANIZACIJA, PRAKSA I ALATI

3. Bezbednosna politika i upravljanje rizikom u organizaciji
4. Upravljanje lozinkama
5. Alati za bezbednu komunikaciju
6. Bezbedan rad na terenu i u pokretu

3. Bezbednosna politika i upravljanje rizikom u organizaciji

U ovom poglavlju ćemo bliže razmatrati šta jedna organizacija treba da uradi kako bi strateški pristupila digitalnoj bezbednosti.

Digitalna bezbednost se najlakše raspadne tamo gde nema jasnih dogovora. Alati mogu biti vrhunski, lozinke jake, tim motivisan, ali bez bezbednosne politike sve ostaje na dobroj volji i improvizaciji. Improvizacija je baš ono na šta napadači najviše računaju.

Bezbednosna politika/ strategija jedne organizacije ne mora da bude formalan ili predugačak dokument. U malim organizacijama ona može biti i dogovor od dve strane teksta: ko pristupa čemu, kojim kanalima komuniciramo, kako čuvamo podatke, šta radimo kad dođe do incidenta i kako se međusobno podržavamo. Bitno je da taj dogovor postoji, da ga svi razumeju, i da važi jednako za sve.

3.1. Šta ulazi u minimalnu bezbednosnu politiku

- **Mapiranje podataka i klasifikacija**
  Ovo se pominje i u poglavljima o skladištenju i šifrovanju, ali ovde to dobija organizacijski okvir. Politika treba da kaže:

- Koje vrste podataka imamo (kontakti, svedočenja, finansije, medijski materijal, interne strategije);
- Šta smatramo poverljivim ili kritičnim;
- Gde se ti podaci smeju čuvati;
- Koliko dugo ih čuvamo i kada se brišu.

Data minimization je princip koji podrazumeva da prikupljanje ličnih podataka treba da se ograniči na ono što je direktno relevantno i neophodno za postizanje određene svrhe/posla/zadatka. Podatke takođe treba čuvati samo onoliko dugo koliko nam je potrebno za ispunjenje te svrhe. Ovaj princip je često potcenjena taktika zaštite: ako neki podatak nije potrebno imati, to je podatak koji ne može ni da procuri.

➢ **Pristupi, uloge i odgovornosti**
Umesto „svi imaju sve", politika uvodi pravilo „potrebe da se zna".

Primer: osoba koja radi logistiku ne mora da ima pristup bazama osetljivih kontakata, baš kao što osoba koja radi na osetljivim svedočenjima ne mora da ima pristup svim finansijskim dokumentima.

Dobro je napraviti tri nivoa:

- Osnovni pristup (svakodnevni rad);
- Poverljivi pristup (ograničen na mali broj ljudi);
- Administrativni pristup (najviši nivo, što manje osoba).

➢ **Standardi za naloge i uređaje**
Podrazumeva da se u okviru politike formalizuju pravila iz poglavlja o lozinkama i uređajima:

- 2FA obavezan za *e-mail*, *Cloud*, društvene mreže;
- Menadžer lozinki kao standard;
- Uređaji zaključani i ažurirani;
- Instaliranje softvera samo preko dogovorenih izvora.

➢ **Komunikacioni protokoli**
Politika treba da kaže:

- Koje kanale koristimo za osetljive teme;
- Šta nikad ne šaljemo preko nešifrovanih kanala;
- Kako verifikujemo identitet kontakata kod važnih razgovora;
- Šta radimo kad posumnjamo da došlo do kompromitacije kanala.

- ***Incident response* u jednoj strani**
  Deo o odgovorima na incidente biće u nastavku detaljno obrađen. U politici je dovoljan sažetak:
  - Ko odlučuje u kriznoj situaciji;
  - Gde se incident dokumentuje;
  - Kako se obaveštava tim o tome šta se desilo;
  - Kada se zovu spoljne mreže da podrže;
  - Ko je portparol.

- **Briga o ljudima kao bezbednosna stavka**
  U digitalnoj bezbednosti ljudi nisu resursi, oni su prva linija. Politika treba da ima makar jednu stavku o:
  - Pravu na pauzu i povlačenje kad je pretnja jaka;
  - Timskoj podršci posle napada;
  - Nultoj toleranciji na nalaženje krivca za incident u organizaciji.

3.2. Kako se uvodi politika bez otpora

Ljudi ne vole da im se bezbednost predstavi kao skup zabrana. Zato je pri uvođenju politika važno najpre baviti se pitanjima zašto se politika uvodi, i zašto je ona korisna i važna, a zatim se baviti pitanjima kako na koji način se uvodi i primenjuje.

Najbolji put je:

1. Kratka zajednička radionica o rizicima koji su realni u vašem radu;
2. Dogovor o pravilima koja su iz toga proizašla;
3. Test period od tri meseca;
4. Dorada na osnovu iskustva.

Bezbednosna politika je dogovor koji raste s timom. U idealnom slučaju ona prati promene u digitalnim tehnologijama i usklađuje se prema njima u realnom vremenu.

4. Upravljanje lozinkama

Lozinke su najčešće korišćeni, ali mehanizam zaštite koji je i najčešće meta kompromitacije u digitalnom prostoru. I dalje su osnovna barijera između napadača i vaših podataka, ali se u praksi često zanemaruju, pojednostavljuju ili dele usput. Upravo zato savremeni bezbednosni standardi stalno naglašavaju higijenu lozinki i višefaktorsku zaštitu kao minimum.[6]

Organizacije civilnog društva, posebno one koje rade sa malim timovima i ograničenim tehničkim resursima, često biraju lozinke koje su lake za pamćenje, a samim tim i lake za probijanje. Upravljanje lozinkama zato mora da postane sistemska praksa, a ne individualna improvizacija.

4.1. Šta čini jaku lozinku

Dugačka lozinka (najmanje 12 karaktera) je danas važnija od komplikovanih pravila, jer dužina najviše otežava automatizovane napade. Dobro je kombinovati slova, brojeve i simbole, ali još bolje je koristiti duge fraze koje se lako pamte, a teško pogađaju. Snaga lozinke ne vredi mnogo ako se koristi ista lozinka za više naloga. U slučaju kompromitacije jednog naloga, svi ostali postaju ranjivi. Zato je ključno da svaka platforma, servis ili uređaj ima jedinstvenu lozinku.

6 Verizon https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf

4.2 Korišćenje menadžera lozinki

Ovi alati omogućavaju bezbedno čuvanje, generisanje i automatsko unošenje lozinki, pa tim ne mora da pamti desetine kompleksnih kombinacija. To je trenutno praksa koja se najviše preporučuje za organizacije.[7]

Najpoznatiji menadžeri lozinki su:

- **Bitwarden**[8] - otvorenog koda, uz mogućnost lokalnog hostovanja.
- **1Password** - intuitivan interfejs, dobar za timove i deljenje pristupa.
- **KeePassXC**[9] - lokalni menadžer bez obavezne sinhronizacije u oblaku.
- **NordPass** - jednostavan za upotrebu, sa dodatnim bezbednosnim slojevima.

Važno je da se menadžer lozinki zaštiti **glavnom lozinkom** koja je izuzetno jaka i da se uključi dvofaktorska autentifikacija (2FA) gde god je moguće. 2FA dodaje dodatni sloj zaštite, najčešće kroz kod u aplikaciji na telefonu, i značajno otežava neovlašćen pristup čak i kad je lozinka procurela.

4.3 Uspostavljanje pravila za deljenje lozinki unutar organizacije

Lozinke se ne smeju slati *e-mail*-om, čuvati u dokumentima bez enkripcije, niti deliti usmeno bez traga. Ako više osoba mora da koristi isti nalog, koristite menadžere lozinki koji omogućavaju deljenje pristupa **bez otkrivanja same lozinke**. Takođe, kada neko napusti organizaciju, mora se odmah promeniti lozinka svih naloga kojima je ta osoba imala pristup.

4.4. Redovna revizija

Umesto rutinskog menjanja lozinki na svakih nekoliko, savremene smernice preporučuju:

- Redovan pregled naloga i pristupa;
- Uklanjanje neaktivnih naloga;
- Promenu lozinke **odmah** ako postoji sumnja na kompromitaciju ili curenje podataka.

7 Drata https://drata.com/blog/nist-password-guidelines
8 Bitwarden https://bitwarden.com/open-source
9 Techrepublic https://www.techrepublic.com/article/bitwarden-vs-keepass

Revizija ne mora da bude komplikovana. Dovoljno je da se kvartalno napravi pregled svih naloga, pristupa i lozinki, i da se izvrše neophodne promene.

4.5. Edukacija

Članovi tima moraju da razumeju zašto se lozinke ne smeju zapisivati na papiru ili u beleškama na telefonu bez zaštite, zašto se ne koriste očigledne kombinacije tipa “123456” ili “password”, i kako da prepoznaju pokušaje krađe lozinki kroz fišing poruke. Bez razumevanja, pravila ostaju mrtvo slovo na papiru.

U svetu u kom se identiteti kradu, nalozi preuzimaju, a podaci zloupotrebljavaju, lozinka je često prva i najvažnija barijera. Zato mora biti duga, jedinstvena, zaštićena i deo jasne organizacione prakse.

5. Alati za bezbednu komunikaciju

U kontekstu digitalne bezbednosti komunikacija nam je važna i iz lične i organizacijske perspektive. Način na koji komuniciramo privatno uvek se reflektuje na naš rad u organizaciji. Zato organizacijski protokoli čuvaju i naše razmene sa drugima koji nisu u direktnoj vezi sa našim radom.

Najpouzdaniji alati za bezbednu komunikaciju su:

- **Signal**[10]- aplikacija za poruke i pozive sa snažnom *end-to-end* enkripcijom i minimalnim zadržavanjem metapodataka; dobra je za timsku komunikaciju.
- **Proton Mail**[11]- šifrovani *e-mail* servis sa serverima u Švajcarskoj/Nemačkoj; sadržaj *e-mail*-ova između Proton korisnika je E2EE, ali kao i kod svakog *e-mail*-a postoje metapodaci koje servis mora tehnički da vidi (npr. Adrese pošiljaoca/primaoca), a IP logovanje zavisi od podešavanja i pravnih obaveza.
- **Tutanota**[12]- privatno orijentisan *e-mail* servis otvorenog koda, sa *end-to-end* enkripcijom sadržaja.
- **Element (Matrix)**[13]- decentralizovana platforma za poruke; E2EE je podrazumevan za direktne razgovore i može se uključiti za sobe/grupe; pogodna je za veće mreže, uz napomenu da *homeserver* i dalje vidi deo metapodataka.
- **Session**[14]- aplikacija koja ne traži telefonski broj i dizajnirana je da maksimalno minimizuje metapodatke.

Korišćenje ovih alata traži i promenu navika. Navikli smo na brzinu i komfor, ali bezbedna komunikacija traži strpljenje, dosle-

10 Signal https://signal.org/blog/sealed-sender
11 Proton Mail https://proton.me/mail/privacy-policy
12 Open Source Security Atlas https://www.opensecatlas.com/tool/3836
13 Element https://element.io/en/features/end-to-end-encryption
14 Session https://getsession.org

dnost i malo više pažnje. Na primer, šifrovani *e-mail*-ovi ne mogu uvek da se šalju ka običnim adresama bez gubitka dela zaštite (to je ograničenje e-mail protokola, ne mana servisa). Signal ne radi bez interneta, što može biti izazov na terenu. Ali poenta je da kompromis između udobnosti i bezbednosti pravimo svesno, u skladu sa procenom rizika.

5.1. Upravljanje kontaktima

Komunikacija nije bezbedna ako nije jasno s kim se komunicira. Lažni nalozi, kompromitacija kontakata i neprovereni brojevi mogu biti ulazna tačka za napad. Zato je važno razviti praksu verifikacije identiteta: kroz direktan poziv, dogovorene fraze, proveru preko drugog kanala ili jednostavno ključnu rečenicu koju samo vi znate. Takođe, treba izbegavati automatsku sinhronizaciju kontakata sa aplikacijama koje nemaju jasnu politiku privatnosti.

5.2. Zaštita metapodataka

Čak i kad je sadržaj poruke šifrovan, metapodaci, ko je s kim komunicirao, kada i koliko često, mogu otkriti mrežu odnosa. U represivnim uslovima, takva analiza se koristi za mapiranje grupa, prepoznavanje ključnih osoba i planiranje pritisaka ili napada. Zato je važno birati alate koji metapodatke svode na minimum i izbegavati platforme koje rutinski prate i beleže korisničke aktivnosti.

5.3. Edukacija tima

Bezbedna komunikacija ne funkcioniše ako je koristi samo jedna osoba. Ceo tim mora da zna kako se instaliraju aplikacije, kako se verifikuju kontakti, kako se šalju šifrovane poruke i kako se izbegavaju greške koje ruše zaštitu. To uključuje: ne slati lozinke porukama, ne otvarati sumnjive linkove i razumeti da se osetljive informacije dele samo kad su stvarno potrebne.

5.4. Planiranje komunikacije u kriznim situacijama

Kad se dogodi napad, pojavi se sumnja na kompromitaciju ili treba brzo reagovati, komunikacija mora biti unapred dogovorena. To znači da treba definisati bezbedne kanale za hitne poruke, znati ko donosi odluke, imati plan prebacivanja na rezervni kanal i izbeći paniku koja obično vodi u greške. Krizna komunikacija treba da bude jasna, kratka i fokusirana na zaštitu ljudi i podataka.

Zašto metapodaci znače moć:

ČAK I KAD JE SADRŽAJ ŠIFROVAN (*END-TO-END*)[15] ...	METAPODACI I DALJE MOGU DA OTKRIJU...
Sadržaj poruke je zaštićen (čitljiv samo pošiljaocu i primaocu).	Ko sa kim komunicira.
Platforma ne može da vidi tekst poruka.	Kada je komunikacija ostvarena i koliko često.
Treće strane ne mogu da pročitaju sadržaj bez ključeva.	Obim komunikacije (npr. Koliko poruka / veličina fajlova).
Odakle se komunicira (npr. IP adresa, mreža/ bazna stanica, približna lokacija).	
Obrazac mreže kontakata (struktura odnosa, centralne tačke/hijerarhija).	

15 Surveilance Self-defence https://ssd.eff.org/

6. Bezbedan rad na terenu i u pokretu

Ovaj deo vodiča odnosi se na bezbednost u radu na terenu i važan je na sva tri nivoa: **ličnom, timskom i organizacijskom.** Lične navike i oprez su prva linija zaštite, timski dogovori pomažu da se rizici uoče i podeli odgovornost, a organizacijske procedure obezbeđuju da se u nepredvidivim situacijama zna ko šta radi i kako se reaguje.

Veliki deo aktivističkog posla odvija se van kancelarije: na javnim skupovima, u zajednici, u kafiću, na putu. U takvim uslovima rizik raste, jer je okruženje promenljivo i često nepredvidivo.

U nastavku su navedeni ključni elementi koje je važno proveriti kada se radi na terenu.

Pre terena:

- Očistiti telefon od osetljivih podataka koje ne moraš da nosiš;
- Proveriti da su uređaji ažurirani i zaključani;
- Dogovori *safe check-in* sa timom;
- Poneti rezervni način autentifikacije.

Na terenu:

- Ne koristiti javni *Wi- Fi* za osetljive stvari;
- Ne ostavljati uređaj bez nadzora;
- Izbegavati otključavanje telefona pred nepoznatima;
- Koristiti nestajuće poruke ako je rizik visok.

Posle terena:

- Prebaciti materijale u organizacijski prostor, ne ostavljati ih u telefonu;
- Uraditi mini pregled: ima li čudnih poruka, notifikacija, pristupa;
- Ako je nešto bilo sumnjivo, dokumentovati odmah.

6.1. Bezbednost telefona

Telefon je danas praktično kancelarija u malom. U njemu su kontakti, *e-mail*, *chat*-ovi, fotografije, lokacije, često i lozinke. Zato je telefon najčešća meta i najlakša ulazna tačka.

Osnovna zaštita uređaja podrazumeva:

- Uključiti jak PIN ili lozinku (ne otisak prsta kao jedini faktor);
- Uključiti automatsko zaključavanje posle kratkog vremena;
- Držati uključen *Find my device* / opciju daljinskog brisanja podataka;
- Šifrovanje je po *default*-u uključeno u modernim Android i iOS uređajima, ali je važno proveriti da li je ova opcija aktivna.

Ažuriranja možda deluju zamorno, ali su važna zbog zaštite

- Redovno ažurirati Operativni sistem (OS) i aplikacije;
- Ne odlagati *update* nedeljama, jer napadi često koriste ulaz kroz neažurirane aplikacije.

Dozvole aplikacija

- Potrebno je proveriti dozvole u aplikacijama za korišćenje kamere, mikrofona, kontakata, lokacije;
- Isključiti dozvole aplikacijama kojima to nije potrebno;
- Ostaviti opcije uključene samo dok se koristi aplikacija;
- Izbrisati aplikacije koje se ne koriste.

Mreže i povezivanje

- Izbegavati javni *Wi-Fi* za osetljive razgovore;
- Isključiti automatsko spajanje na otvorene mreže i *Bluetooth* kad se ne koristi.
- Ako je neophodni koristiti javnu mrežu obavezno koristiti *VPN* - Virtual Private Network (virtuelna privatna mreža).

Poruke i linkovi

- Ne otvarati linkove iz sumnjivih poruka, čak i kad deluju kao da su od poznate osobe;
- Ako nešto zvuči hitno i „samo brzo klikni", važno je zastati i proveriti o čemu se radi.

Kada postoji rizik od nadzora ili oduzimanja telefona

- Držati minimalan broj osetljivih podataka na telefonu;
- Koristiti aplikacije koje imaju opciju nestajućih poruka;
- U kriznim situacijama, bolja je zaštita PIN lozinkom nego biometrija, jer je biometriju lakše prisilno iskoristiti.

Mini Čeklista za tim

Pre nego što tim pređe na alate, podešavanja i tehničke korake, važno je da postoji brz zajednički dogovor o tome kako se međusobno komunicira i ko za šta odgovara. Ova mini check list-a služi kao početna orijentacija, da se usklade navike, razjasne očekivanja i spreče najčešće greške koje se u praksi ne dešavaju zbog tehnologije, već zbog neusklađenog rada. Ovo je najkraći mogući skup koraka koji timu daje stabilnu osnovu.

1) Pre nego što se pređe na alat

- Napraviti kratak spisak: ko s kim komunicira, o čemu, koliko često i koliko je to osetljivo.
- Dogovoriti koji kanal je za šta (npr. *Signal* za interno/urgentno, *Proton/Tutanota* za formalno, *Element* za šire mreže).
- Odrediti jednu osobu / mali tim za podršku i podešavanja (umesto „svi po malo").

2) Podešavanja za Signal / slične E2EE aplikacije

- Uključiti registracioni PIN i zaključavanje aplikacije.
- Uključiti nestajuće poruke za osetljive *chat-ove*.
- Isključiti automatski preview linkova ako vas to izlaže.
- Proverite *Safety Number / verification* sa ključnim kontaktima (uživo ili drugim kanalom).
- Ne šaljite lozinke ni 2FA kodove kroz *chat*.

3) Podešavanja za šifrovani *e-mail* (*Proton/Tutanota*)

- Uključiti 2FA na nalogu.
- Koristiti šifrovanje/lozinku kada se šalje *e-mail* na „obične" adrese.
- Ne prosleđivati osetljive priloge bez dodatne enkripcije (npr. *Zip* sa lozinkom ili *VeraCrypt/Cryptomator*).
- Razdvojiti privatni i organizacioni nalog.

4) Kontakti i verifikacija identiteta

- Za novi kontakt: proveriti identitet preko drugog kanala (poziv, *e-mail*, zajednički kontakt).
- Uvesti dogovorenu frazu ili ključnu rečenicu za hitne situacije.
- Ne sinhronizovati kontakte sa aplikacijama koje ne koristite ili kojima ne verujete.
- Ako mislite da je došlo do kompromitacije kontakta, tretirajte ga kao kompromitaciju dok se ne proveri.

5) Metapodaci i navike

- Za najosetljivije teme koristiti alate koji minimizuju metapodatke (*Signal*/*Session*).
- Ne mešati javne i osetljive razgovore u istim grupama.
- Razmisliti pre dodavanja ljudi u grupe.

6) Krizni plan (mini-incident protokol)

- Imati rezervni kanal za hitnu komunikaciju (unapred dogovoren).
  Znate ko donosi odluke prilikom incidenta (1–2 osobe).
- Imati poruku „za uzbunu" (kratka, jasna) i spisak koga prvo obaveštavate.
- Ako postoji sumnja na kompromitaciju:
  - prestati sa korišćenjem sumnjivog kanala,
  - prebaciti se na rezervni,
  - dokumentovati šta se desilo (vreme, nalog, uređaj),
  - menjati lozinke/2FA tek sa bezbednog uređaja.

PROCENA RANJIVOSTI I TEHNIČKA OTPORNOST

7. Prepoznavanje i reagovanje na online pretnje
8. Dijagnostičke kontrolne liste za procenu ranjivosti
9. Šifrovanje podataka
10. Rezervne kopije podataka
11. CDN u praksi

7. Prepoznavanje i reagovanje na *online* pretnje

Ovaj deo vodiča važi za sva tri nivoa bezbednosti, **lični, timski i organizacijski**. Na ličnom nivou pomaže da prepoznamo šta nam se dešava na nalozima i uređajima. Na timskom nivou olakšava da delimo sumnje na vreme i proverimo jedni druge. A na organizacijskom nivou gradi rutinu: kako se incident beleži, kome se javlja i kako se reaguje bez panike.

U digitalnom prostoru pretnje retko dolaze kao očigledan napad. Mnogo češće izgledaju kao sitni, čudni signali: neobične aktivnosti na nalozima, poruke u kojima nešto ne štima, promene u ponašanju platformi ili neočekivani zahtevi za pristup. Ključna veština u savremenom aktivizmu je da te signale primetimo na vreme, da ih ne normalizujemo i ne guramo pod tepih, već da reagujemo mirno, sistematski i bez odlaganja. Upravo takav pristup preporučuju i globalni vodiči za zaštitu civilnog društva.[16]

Prepoznavanje pretnji traži usmeravanje pažnje na detalje. Promene u ponašanju naloga, poruke koje iznenada stižu od poznatih kontakata, insistiranje na hitnoj akciji, neočekivane greške u sistemu ili čudne notifikacije o prijavama, sve to mogu biti signali da je bezbednost ugrožena. Važno je da se članovi tima ohrabre da prijave sumnjive situacije i kad nisu potpuno sigurni da je u pitanju napad. Bolje je reagovati preventivno nego čekati dokaz koji obično dođe prekasno.

16 Field Guide to incident response for civil society and media https://internews.org/wp-content/uploads/2023/11/Field-Guide-to-Threat-Labs.pdf

U kriznim situacijama, najvažnije je sačuvati kontrolu nad informacijama. Ne treba odmah iznositi sve detalje napada, jer to može pomoći napadaču da prilagodi taktiku ili pobegne od posledica. Umesto toga, prioritet je stabilizacija sistema, procena štete, zaštita ugroženih osoba i priprema javne komunikacije koja je promišljena, kratka i usmerena na očuvanje poverenja. Ovo posebno važi kod kampanja uznemiravanja i doksinga, gde previše informacija može dodatno ugroziti metu.

Takođe, važno je da se incidenti ne zaboravljaju čim prođe kriza. Svaka pretnja mora biti analizirana: kako je do nje došlo, šta je omogućilo napad, koje su bile slabe tačke, i šta menjamo da se ne ponovi. Ta analiza treba da bude deo kolektivnog učenja, ne samo tehničkog, nego i emocionalnog. Napadi ostavljaju posledice: strah, nesigurnost, osećaj izloženosti ili krivice. Potrebno je da organizacija pruži podršku članicama i članovima tima koji su bili meta napada, da normalizuju razgovor o digitalnom nasilju i da grade kulturu u kojoj se o pretnjama govori na vreme, a ne tek kad eskaliraju.[17]

Ako pretnja preraste u incident koji tim ne može sam da reši, postoje međunarodne mreže podrške za organizacije civilnog društva koje pružaju hitnu pomoć, procenu rizika i vođene korake oporavka.

17 United Nations https://www.ohchr.org/en/get-involved/stories/women-activists-fighting-safe-digital-space

8. Dijagnostičke kontrolne liste za procenu ranjivosti

Procena ranjivosti možda zvuči formalno, ali u praksi je vrlo konkretna stvar: pomaže da na vreme uočite gde može da „pukne”, pre nego što se to zaista desi.

Na primer, da li bivši član tima i dalje ima pristup *Drive* folderima, da li se isti admin nalog deli na više ljudi, da li su 2FA i *backup* zaista uključeni, ili se osetljivi fajlovi i dalje sinhronizuju na privatne telefone i laptope. Kada znate gde su slabe tačke, lakše je postaviti prioritete, uložiti energiju tamo gde najviše znači i reagovati brže kad se pojavi pretnja.

Zato kontrolne liste nisu birokratija radi birokratije. One su jednostavan način da izmerite stanje: šta već radite dobro, šta nedostaje i šta je sledeći realan korak koji možete da uvedete.

U ovom poglavlju nalaze se dijagnostičke liste koje možete koristiti za samoprocenu, internu reviziju ili kao osnovu za bezbednosnu politiku. Ne morate sve odjednom, često je mnogo korisnije da ih prolazite periodično (na primer jednom u 3–6 meseci), beležite šta ste promenili i pratite napredak kroz vreme.

Kako koristiti ove liste

Ove kontrolne liste mogu biti odličan povod za refleksiju, razgovor i konkretno planiranje. Koristite ih na radionicama, internim sastancima, tokom uvođenja novih članova i članica ili kao polaznu tačku za izradu bezbednosne politike. Najvažnije je da

ih ne popunjava jedna osoba, već da se kroz njih prolazi kolektivno i da se na kraju izvuče nekoliko jasnih, malih koraka koje možete odmah da sprovedete.

Organizacije koje ovakve procene rade redovno vremenom grade kulturu u kojoj se bezbednost doživljava kao briga, solidarnost i profesionalni standard. Sledeća poglavlja ulaze u alate i tehnike, ali sve to ima smisla tek kada znamo gde smo sada i šta nam, realno, najviše treba.

8.1. Kontrolna lista za ličnu digitalnu bezbednost

Ova lista je namenjena osobama čiji je rad javan, koje koriste digitalne alate za organizovanje i zagovaranje i žele da procene sopstvenu izloženost riziku. Logika je ta da je lična bezbednost prvi sloj kolektivne zaštite.

IDENTITET I PRISUSTVO

- Da li koristimo isto korisničko ime na više platformi?
- Da li su lične informacije (adresa, broj telefona, fotografije) javno dostupne?
  Da li imamo kontrolu nad svojim digitalnim identitetom (nalozima, biografijama, slikama)?

LOZINKE I PRISTUP

- Da li koristimo jedinstvene lozinke za svaki nalog?
- Da li koristimo menadžer lozinki?
- Da li smo uključili dvofaktorsku autentifikaciju gde god je moguće?

UREĐAJI

- Da li su naši uređaji zaštićeni lozinkom ili biometrijom?
- Da li redovno ažurirmo operativni sistem i aplikacije?
- Da li imamo aktivan antivirus ili *antimalware* zaštitu?

KOMUNIKACIJA

- Da li koristimo šifrovane aplikacije za razmenu poruka kada je tema osetljiva?
- Da li proveravamo identitet osoba pre nego što podelimo osetljive informacije?
- Da li izbegavamo korišćenje javnog *Wi-Fi* za poverljive razgovore?

PSIHOLOŠKA OTPORNOST I PODRŠKA

- Da li imamo plan kako da reagovanja u slučaju da postanemo meta uznemiravanja ili doksinga?
- Da li imamo mrežu podrške kojoj možemo brzo da se obratimo?
- Da li znamo gde možemo da dobijemo pravnu ili tehničku pomoć?

8.2. Kontrolna lista za organizacije

Ova lista je za organizacije koje žele da procene koliko su sistemi, podaci i timovi zaštićeni od digitalnih pretnji.[18]

PRISTUP PODACIMA

- Da li postoji mapa svih podataka koje organizacija poseduje?
- Da li su podaci klasifikovani po osetljivosti?
- Da li je pristup podacima ograničen po funkciji i potrebi?

SKLADIŠTENJE I REZERVNE KOPIJE

- Da li se podaci čuvaju na bezbednim lokacijama, lokalno i u oblaku?
- Da li se redovno prave rezervne kopije?
- Da li su rezervne kopije zaštićene od neovlašćenog pristupa i odvojene od glavnih naloga?

NALOZI I PRISTUPI

- Da li svaki član tima ima svoj nalog (bez deljenih naloga)?
- Da li se pristupi bivšim članovima tima odmah ukidaju?
- Da li postoji pregled ko ima koji nivo pristupa i kada je poslednji put revidiran?

KOMUNIKACIJA I KOORDINACIJA

- Da li se za interne dogovore koriste šifrovani kanali kada je potrebno?
- Da li postoji unapred dogovoren kanal za hitne situacije?
- Da li platforme koje koristite omogućavaju kontrolu pristupa i evidenciju aktivnosti?

18 Squarespace https://static1.squarespace.com/static/54dbcb77e4b011d9d8fd69f1/t/60250a4db0e7682485c5822b/1613040205449/lifeline%2Btoolkit%2Bdigital%2Bsecurity%2Bfinal%2B%28feb%2B2021%29.pdf

REAGOVANJE NA INCIDENTE

- Da li postoji protokol za reagovanje na digitalne napade?
- Da li je jasna odgovornost za procenu rizika i koordinaciju?
- Da li se incidenti dokumentuju, analiziraju i koriste za učenje?

EDUKACIJA I KULTURA

- Da li se tim redovno edukuje o digitalnoj bezbednosti?
- Da li postoji prostor da se o greškama priča bez straha od sankcija?
- Da li se bezbednost razume kao kolektivna odgovornost, a ne kao posao jedne osobe?

8.3. Kontrolna lista, partnerstva i eksterni odnosi

Pošto organizacije ne funkcionišu izolovano njihova bezbednost je jaka onoliko koliko je jak najslabiji kanal u mreži partnera, donatora, medija i zajednice.

DELJENJE INFORMACIJA

- Da li se osetljive informacije dele samo preko bezbednih kanala?
- Da li se jasno zna koje informacije smeju da idu javno, a koje ne?
- Da li se koristi šifrovanje prilikom slanja važnih dokumenata?

ZAJEDNIČKI ALATI I RESURSI

- Da li se koriste zajednički softveri ili folderi sa partnerima?
- Da li su pristupi jasno definisani i vremenski ograničeni kada treba?
- Da li je poznato ko je odgovoran za bezbednost zajedničkih resursa?

REAKCIJA NA INCIDENTE

- Da li postoji dogovor šta se radi ako dođe do kompromitacije kod partnera ili u vašoj organizaciji?
- Da li se incidenti dele sa partnerima radi zajedničke zaštite?
- Da li postoji zajednička praksa dokumentovanja i analize?

9. Šifrovanje podataka

U Srbiji i regionu šifrovanje nije napredna opcija, nego realna potreba. To se jasno vidi iz javno dokumentovanih slučajeva poslednjih godina. Ovakvi incidenti nisu izuzetak ni u regionu šire gledano.

Zapadni Balkan ima rastući trend *spyware* (bilo koji zlonamerni softver koji ima za cilj prikupljanje informacija o osobi ili organizaciji i slanje istih drugom entitetu) i *ransomware* (vrsta zlonamernog softvera koji šifruje lične podatke žrtve dok se ne plati otkupnina) napada, a mete su sve češće i organizacije civilnog društva i mediji.[19] U takvom kontekstu, šifrovanje je najjednostavniji način da ukradeni ili presretnuti podaci ostanu neupotrebljivi.

Šifrovanje se, međutim, često doživljava kao tehnička komplikacija, a ne kao deo svakodnevnog rada i upravo ta percepcija pravi rupu u zaštiti. Šifrovanje nije luksuz.[20]

9.1. Šta treba da znamo o šifrovanju

- Šifrovanje pretvara podatke u nečitljiv format koji se može dešifrovati samo uz ključ.
- Postoje dve osnovne vrste: simetrično (isti ključ) i asimetrično (par ključeva).
- Šifrovati treba sve što može da nanese štetu ako se kompromituje: baze kontakata, interne dokumente, komunikaciju, fotografije i *backup* fajlove.

19 Atlantic Council https://www.atlanticcouncil.org/content-series/balkans-debrief/how-do-cyber-attacks-threaten-the-balkans-a-debrief-with-dan-ilazi-and-filip-stojanovski

20 Digital Threat Landscape: Serbia https://internews.org/wp-content/uploads/2023/11/Serbia-Digital-Threat-Landscape-Report.pdf

- Najčešći alati: *VeraCrypt*, *Cryptomator*, *PGP* - sistem za zaštitu privatnosti (OpenPGP), kao i E2EE komunikacioni alati poput *Signala* i *Elementa*.
- Kultura šifrovanja podrazumeva razumevanje, doslednost i kolektivnu odgovornost.

9.2. Kako šifrovanje funkcioniše

Šifrovanje se zasniva na matematičkim algoritmima koji podatke pretvaraju u nizove znakova koje niko ne može smisleno da pročita bez ključa. Kada se fajl šifruje, on postaje nečitljiv za sve osim za osobu koja ima odgovarajući ključ ili lozinku. Ako se fajl ukrade, presretne ili izgubi, on ostaje zaključan i praktično bezvredan napadaču.

Simetrično šifrovanje koristi isti ključ za šifrovanje i dešifrovanje. Ovo je idealno za lokalne fajlove, diskove i rezervne kopije. *VeraCrypt* je jedan od najpoznatijih alata u toj kategoriji: može da šifruje ceo disk ili da napravi šifrovane kontejnere koji se ponašaju kao virtuelni diskovi.

Asimetrično šifrovanje koristi dva ključa, javni i privatni. Standard *OpenPGP* (često nazvan *PGP*) radi tako što pošiljalac šifruje poruku javnim ključem primaoca, a primalac je otključava privatnim ključem. Time možete slati osetljive informacije čak i preko kanala koji nisu sami po sebi bezbedni.

9.3. Kako šifrovanje izgleda u svakodnevnom radu

U organizaciji koja šifrovanje koristi dosledno, neke stvari postaju rutina:

- Osetljivi fajlovi se ne čuvaju nezaštićeni na desktopu ili u nepreglednim folderima.
- Dokumenti koji sadrže lične podatke ili interne strategije šifruju se pre deljenja.
- *Backup* kopije se čuvaju na eksternim diskovima koji su šifrovani i fizički odvojeni od glavnog sistema.
- Timska i partnerska komunikacija ide kroz *end-to-end* šifrovane kanale.
- Ljudi u timu znaju kako se koriste ključevi, kako se proverava sagovornik i šta je prvi korak čim se pojavi sumnja na kompromitaciju.

9.4. Elementi kulture šifrovanja

- Razumevanje svrhe: svi znaju zašto šifruju, ne samo kako;
- Doslednost: šifrovanje je pravilo u radu, ne samo reakcija u krizi;
- Kolektivna odgovornost: svi učestvuju, niko nije izostavljen;
- Otvorenost za učenje: greške se koriste za unapređenje prakse;
- Solidarnost sa drugima: znanje se deli i širi kroz mreže podrške.

10. Rezervne kopije podataka

U Srbiji već imamo jasan, javno dokumentovan primer šta se desi kad rezervne kopije nisu dobro postavljene, i koliko mogu da znače kad jesu. Na početku pandemije COVID-19, javno komunalno preduzeće u Novom Sadu bilo je pogođeno *ransomware* napadom koji je enkriptovao oko 50 TB podataka.

Preduzeće je izbeglo katastrofu samo zato što je uspelo da povrati podatke zahvaljujući oporavku iz kopija, što je u izveštaju *Internews* i SHARE fondacije navedeno kao lekcija o važnosti *backup*-a (rezervnih kopija podataka) u Srbiji.[21] Poenta je jednostavna, napad može biti finansijski motivisan, politički ili samo oportunistički, ali posledica je ista ako ne postoji kopija, nestaje rad, dokazi, istorija i kapacitet da se nastavi dalje.

Backup je praktičan alat otpora protiv brisanja, sabotaže i zaborava. *NIST* (*National Institute of Standards and Technology* https://www.nist.gov/ - Agencija Ministarstva trgovine Sjedinjenih Američkih Država koja promoviše inovacije unapređenjem nauke o merenju, standarda i tehnologije) i drugi standardi tretiraju *backup* kao deo osnovne otpornosti organizacije, ne kao dodatak ako nam ostane vremena.

21 https://internews.org/wp-content/uploads/2023/11/Serbia-Digital-Threat-Landscape-Report.pdf

Osnovne istine o rezervnim kopijama

- *Backup* mora biti redovan, automatizovan i višestruko distribuiran.
- Idealno je imati najmanje dve kopije, jednu lokalnu i jednu udaljenu, a moderna 3 2 1 logika kaže tri kopije, na dva različita medija, uz jednu van lokacije ili *offline*.
- Backup mora biti šifrovan i fizički odvojen od originalnih podataka.
- Ne sme se oslanjati na iste naloge, uređaje ili lozinke kao primarni sistem, jer *ransomware* i nalozi koji su kompromitujući često brišu i kopije.

Backup nije arhiva. Mora biti ažuran, testiran i dostupan u kriznim situacijama.

10.1. Šta se zapravo čuva

Prvi korak u izgradnji sistema rezervnih kopija je mapiranje podataka. Organizacija mora znati šta poseduje, gde se nalazi, koliko je osetljivo i koliko često se menja. *Backup* ne mora obuhvatiti sve, ali mora obuhvatiti ono što je ključno za kontinuitet rada i zaštitu ljudi.

PODACI KOJI MORAJU BITI OBUHVAĆENI:

- Interna dokumentacija (strategije, planovi, izveštaji);
- Baze kontakata i komunikacija sa partnerima;
- Fotografije i video materijali sa događaja;
- Finansijski dokumenti i ugovori;
- Pravni dokumenti i svedočenja;
- Konfiguracije sistema, lozinke i pristupni ključevi.

U nekim timovima ima smisla napraviti i minimalni set za oporavak, dakle šta vam je potrebno da nastavite rad i za 24 sata i za 30 dana, jer ta dva nivoa oporavka nisu isto.

10.2. Gde se čuva

Backup mora biti fizički i digitalno odvojen od primarnog sistema. Ako se sve čuva na istom uređaju, u slučaju krađe, kvara ili napada sve odlazi zajedno. Najbezbedniji pristup je kombinacija lokalnog i udaljenog čuvanja.

Lokalne kopije (na lokaciji):

- **Eksterni SSD diskovi** (*Solid-State Drive*, brzi disk bez pokretnih delova) sa šifrovanjem
- USB uređaji sa hardverskom zaštitom (npr. enkriptovani USB)
- **NAS sistemi** (*Network Attached Storage*, mrežni uređaj za centralno čuvanje fajlova) za veće organizacije

Udaljene kopije (van lokacije):

- Cloud servisi sa enkripcijom i kontrolom pristupa
- **SFTP serveri** (*SSH File Transfer Protocol*, bezbedan prenos fajlova preko šifrovanog kanala) sa ograničenim pristupom
- ***Self-hosted* rešenja** (servisi koje organizacija sama instalira i administrira) poput **Nextcloud** instalacija (platforma za deljenje i sinhronizaciju fajlova na sopstvenom serveru)

Ključna napomena: *backup* ne treba da se sinhronizuje nekritički sa sistemom kod koga postoji kompromitacija. Automatika je dobra, ali bez *offline* ili izolovane kopije rizikuje se da napad prepiše i rezervu. Ovo je posebno važno u *ransomware* scenarijima.

MODEL	PREDNOSTI	RIZICI	MINIMALNE MERE ZAŠTITE	KADA JE NAJBOLJI
Lokalno (laptop, eksterni disk)	Potpuna kontrola; radi *offiine*	Krađa/šteta; gubitak bez backupa	Šifrovanje diska (*VeraCrypt*), jaka lozinka, fizičko odvajanje	Kad je internet slab ili podaci ekstremno osetljivi
Cloud (Drive, Dropbox...)	Deljenje i saradnja; automatski backup	Nadzor servisa; kompromitacija naloga; pravna nesigurnost	2FA, ograničeni pristupi, dodatno šifrovanje pre slanja (*Cryptomator*)	Za timski rad i simulaciju *single source of truth*
Hibridno	Najbolje od oba sveta	Kompleksnost ako nema protokola	Jasna klasifikacija podataka + dvostruki backup	Za većinu OCD koje rade osetljiv i javni rad paralelno

10.3. Kako se pravi *backup*

Backup treba da bude automatizovan, ali i proverljiv. Postoje alati koji olakšavaju redovno pravljenje kopija bez ručnog rada, ali organizacija mora imati uvid šta se kopira, kada, gde i kako, i ko može da vrati podatke.

Preporučeni alati:

- Duplicati[22], *open source* alat koji podržava šifrovane *backup*-ove u *Cloud*.
- *BorgBackup*, efikasan alat za komandnu liniju, pogodan za tehnički pismene timove.
- *Arq*, jednostavan alat za *backup* na više destinacija.
- *Restic*, brz i bezbedan, radi na više platformi i podržava razne *backend* opcije.

Backup mora biti testiran. Nije dovoljno da postoji, mora se proveriti da li se može vratiti. *NIST* eksplicitno preporučuje redovno testiranje oporavka, makar kvartalno, jer je to jedini način da se proveri da li kopije stvarno funkcionišu.

U praksi to znači da je potrebno povremeno simulirati oporavak: obrisati fajl, vratiti ga iz kopije i proveriti integritet.

10.4. Greške koje se ponavljaju

Najčešće greške u vezi sa rezervnim kopijama su:

- čuvanje *backup* kopije na istom nalogu kao originalni podaci;
- zaboravljanje pristupnih lozinki i ključeva za *backup*;
- nešifrovanje rezervnih kopija;
- pravljenje kopija po osećaju umesto redovno;
- oslanjanje na besplatne servise bez kontrole nad podacima.

Backup mora biti tretiran kao sistem, ne kao jednokratna radnja. Treba da ima svoj protokol, odgovornu osobu i mesto u budžetu, isto kao i svaka druga važna infrastruktura. Kad se to postavi kako treba, ne štite se samo fajlovi, štiti se mogućnost da vaš rad preživi napad, grešku ili nesreću.

22 Sourceforge https://sourceforge.net/software/product/Duplicati

11. CDN (Content Delivery Network) u praksi

CDN - Content Delivery Network (mreža za isporuku sadržaja) je mreža servera raspoređenih na više lokacija. Umesto da se sve na sajtu učitava sa jednog glavnog servera, CDN korisniku šalje sadržaj poput slika, videa, fajlova i skripti sa servera koji mu je najbliži.

Zbog toga se stranice brže otvaraju, a sajt lakše podnosi nagli porast poseta (npr. Kada mnogo ljudi u isto vreme pokušava da pristupi sadržaju). **To je važno jer nam pomaže da informacije ostanu dostupne i kada je interesovanje veliko ili kada sajt trpi napade i opterećenje.**

11.1. Zašto je CDN relevantan za branitelje/ke ljudskih prava

Za sajtove, kampanje i platforme koje mogu biti meta napada ili talasa poseta (npr. nakon objave istraživanja), *CDN* može:

- **Poboljšati dostupnost**: sadržaj se servira sa više lokacija, pa je sistem manje osetljiv na lokalne prekide.
- **Ublažiti *DdoS***: mnogi CDN provajderi imaju zaštitu za upijanje i filtriranje velikog saobraćaja pre nego što stigne do glavnog servera.
- **Smanjiti opterećenje origin servera**: keširani sadržaj se preuzima sa *CDN*-a umesto direktno sa vašeg servera.

CDN uvodi sloj između korisnika i vašeg servera. To može povećati sigurnost, ali znači i da:

- **Deo saobraćaja i metapodataka** (IP adrese, obrasci pristupa, *user-agent*) vidi treća strana,
- Pogrešne postavke mogu dovesti do **curenja podataka** ili **pogrešnog keširanja** (npr. Privatni sadržaj postane javno dostupan),
- U incidentu zavisite od **procesa podrške** i pravila provajdera.

11.2. Kada *CDN* nije dovoljan

CDN pomaže kod dostupnosti i *DdoS*-a, ali ne rešava sve rizike. Ne štiti automatski od kompromitacije *CMS*-a, curenja podataka sa matičnog servera, niti od socijalnog inženjeringa (fišing). *CDN* je jedna komponenta u širem planu: ažuriranja, *backup*, pristupne kontrole i incident protokoli ostaju ključni.

RIZICI, JAVNI NAPADI I REAGOVANJE

12. Ublažavanje rizika na društvenim mrežama

Društvene mreže su danas neizostavan deo rada branitelja/ki ljudskih prava i organizacija civilnog društva. One omogućavaju brzo širenje informacija, mobilizaciju zajednice, povezivanje sa međunarodnim mrežama i veću vidljivost tema koje se često prećutkuju u tradicionalnim medijima. Ali ta vidljivost ima svoju cenu.

U digitalnom prostoru žene koje rade na ljudskim pravima suočavaju se sa specifičnim oblicima nasilja, nadzora i manipulacije koji direktno utiču na njihov rad, bezbednost i psihološko zdravlje. SHARE Fondacija[23] u svojim monitoring izveštajima pokazuje da je rodno zasnovano onlajn nasilje u Srbiji rašireno i da često cilja žene u javnom životu, uključujući aktivistkinje i novinarke.

U praksi, aktivistkinje koje se bave pravima žena, pravima osoba diskriminisanih po različitim osnovama, migranata i političkih disidenata sve češće postaju mete koordinisanih kampanja uznemiravanja na mrežama. Zabeležen je porast pretnji, manipulacija i kampanja mržnje na društvenim platformama, uz posebno prisutne obrasce poput seksualizovanih uvreda (specifična vrsta verbalnog nasilja gde se osoba napada, ponižava ili diskredituje korišćenjem rečnika koji ima seksualnu konotaciju), objavljivanja intimnih sadržaja bez saglasnosti, *deepfake* napada i drugih rodno obojenih pritisaka.

Primer iz Srbije, javno dokumentovan. U avgustu 2022. Sofija Todorović, programska direktorka Inicijative mladih za ljudska prava, bila je meta ozbiljnih pretnji i targetiranja u onlajn prostoru nakon javnog angažmana.[24] Slučaj je izazvao široku reakci-

23 Share fondacija, Monitoring digitalnih prava 2023 https://sharefoundation.info/monitoring-digitalnih-prava-2023-srbija-u-spirali-digitalnog-nasilja

24 https://www.slobodnaevropa.org/a/srbija-pretnje-grafit-inicijativa-mladih-ambasada-ukrajine/32550703.html

ju, uključujući i međunarodnu podršku, i jasno je prepoznat kao pokušaj zastrašivanja žene koja javno deluje protiv dominantnih narativa. Ovakvi napadi funkcionišu kao poruka i njoj i svima koji je prate: cena vidljivosti može biti visoka, a cilj je da se javni prostor suzi.

Sličan obrazac vidimo i kroz doksing kampanje u Srbiji[25], gde se privatni podaci aktivistkinja i građanki objavljuju u političke svrhe, a zatim se preko mreža uvreda i pretnji pravi atmosfera linča. Takve prakse su detaljno opisane u regionalnim analizama i domaćim medijskim izveštajima, uz upozorenje da doksing postaje normalizovan alat političkog pritiska (SHARE Fondacija, »Rodno zasnovano digitalno nasilje u Srbiji«, 2024).

12.1. Strategije za ublažavanje rizika

Ublažavanje rizika ne znači povlačenje sa mreža. Znači promišljeno prisustvo. Ideja je da se štiti identitet, komunikacija i reputacija bez gubitka političke vidljivosti.

Privatnost naloga i sadržaja. Redovno proveravati podešavanja privatnosti. Ograničiti ko može da komentariše, deli ili označava sadržaj. Ako je potrebno, koristiti pseudonime ili odvojene naloge za lične i profesionalne aktivnosti. Izbegavati objavljivanje lokacije u realnom vremenu, posebno tokom akcija, protesta ili terenskog rada. Ovakve mere direktno smanjuju rizik od doksinga i praćenja.

Upravljanje digitalnim identitetom. Verifikovati (proveriti) naloge gde god je moguće. Pratiti pojavu lažnih naloga i prijavljivati ih odmah. Koristiti prepoznatljiv vizuelni identitet i dosledan jezik da bi publika lako razlikovala vaše naloge od imitatora. Arhivirati objave koje lako mogu biti izvučene iz konteksta, jer se manipulacija sadržajem često oslanja na stare ili isečene citate.

Reagovanje na uznemiravanje. Ne ulaziti u direktne rasprave sa nalozima koji prete ili koordinisano napadaju. To uglavnom hrani kampanju. Dokumentovati incident odmah: skrinšot, link, datum, opis. Prijaviti sadržaj platformi i zatražiti uklanjanje. Uključiti mreže podrške i, kada postoji osnov, pravne savetnike. Ključ je da se reaguje brzo, ali hladne glave.

Vidljivost na mrežama mora biti strateška. Ne mora svaka aktivistkinja ili svaki aktivista da bude javno lice, ali mora postojati plan kako se štite oni koji jesu. Ne mora svaki nalog da bude potpuno otvoren, ali mora postojati siguran kanal za komunikaciju sa zajednicom. Ne mora svaki komentar da se briše, ali mora postojati prostor u timu da se o nasilju razgovara, da se ono dokumentuje i da se na njega odgovori zajednički.

25 https://zoomer.rs/ucinimo-ih-poznatim-doksing-kao-sredstvo-politicke-borbe-u-srbiji

13. Napadi na reputaciju, *deepfake* i krizna javna komunikacija

Digitalni napadi danas sve manje liče na klasično hakovanje, a sve više na borbu za narativ. Cilj napadača nije samo da dođe do podataka, nego da proizvede sumnju, sramotu, strah ili umor. Reputacijski napadi su zbog toga jedan od najopasnijih oblika digitalnog nasilja prema braniteljima/kama ljudskih prava i organizacijama civilnog društva.

KAKO IZGLEDAJU REPUTACIJSKI NAPADI

- lažne ili montirane izjave koje se pripisuju aktivistkinjama;
- isečeni snimci i izvučeni citati;
- koordinisano širenje priča kroz bot mreže;
- targetiranje porodice, partnera, zajednice;
- *deepfake* fotografije i video materijali.

Deepfake (tehnologija koja koristi veštačku inteligenciju za kreiranje izuzetno uverljivih, ali potpuno lažnih video, audio ili foto materijala) se posebno koristi jer pravi dokaz tamo gde ga nema. Nije ni važno da ljudi u potpunosti poveruju, dovoljno je da se javi mala sumnja, a to napadaču otvara prostor.

ŠTA ORGANIZACIJA MOŽE DA URADI PRE NAPADA

Ojačati osnovni kredibilitet. Redovno arhivirati javne objave, izveštaje i snimke. Napadač teže manipuliše narativom kad postoji jasan trag realnog rada.

Dogovoriti liniju istine. Ko proverava činjenice, ko piše odgovor, ko javno istupa. To je deo kriznog paketa.

NAPRAVITI FOLDER „HITNI MATERIJALI"

- zvanični logoi, fotografije članova tima koje želite u javnosti;
- prethodna saopštenja;
- kontakt osobe za medije;

Tako u krizi nije potrebno da trošite vreme na traženje bitnih podataka.

KAKO REAGOVATI KAD *DEEPFAKE* ILI LAŽNA PRIČA KRENE

Ne ulaziti odmah u raspravu. Prva reakcija treba da ide na stabilizaciju: šta se tačno širi, gde, ko plasira priču, procena koliki je domet.

Dokumentovati. Sačuvati skrinšot, link, vreme, nalozi. Ovo je važno za platforme i za eventualnu pravnu reakciju.

Odgovori kratko i jasno. U reputacijskim napadima preopširan odgovor ponekad daje dodatni podstrek priči. Dobro pravilo je:

- jasno reći da je sadržaj lažan/manipulisan;
- uputiti na jedan verifikovani izvor istine;
- reći šta će se dalje uraditi (prijava, pravni koraci).

Aktivirati mreže solidarnosti. Napad se gasi brže kad više glasova istovremeno kaže isto.

LEKCIJE:

Reputacijski napadi nisu PR problem, nego bezbednosni incident. U trenutku kad neko pokušava da uništi poverenje u vaš rad, on pokušava da uništi vaš aktivistički kapacitet. Zato nema neutralnog odgovora.

14. Veštačka inteligencija i digitalna bezbednost

Veštačka inteligencija (*AI*) nije tema za jedan dan. Ona je već ovde, u telefonima, platformama, kamerama, pretragama, kao i u alatima za pisanje, prevođenje i analizu.

U aktivističkom radu AI može biti korisna saveznica: pomaže da brže obradimo informacije, mapiramo probleme, uočimo obrasce nasilja ili urednije dokumentujemo kršenja prava.

AI istovremeno menja i pejzaž pretnji. Omogućava napade koji su brži, jeftiniji i masovniji, a posebno pogađaju žene i braniteljke ljudskih prava. UN i evropske institucije već upozoravaju da se AI sve češće koristi kao alat digitalne represije i da bez jasnih garancija i nadzora može ozbiljno ugroziti pravo na privatnost, slobodu izražavanja i udruživanja.

AI KAO POJAČIVAČ NADZORA

U mnogim zemljama *AI* se već koristi za masovni nadzor: prepoznavanje lica na kamerama, praćenje kretanja preko podataka sa telefona, automatsko "prepoznavanje" sumnjivog ponašanja, pa čak i predviđanje ponašanja branitelja/braniteljki ljudskih prava. Te tehnologije ne moraju biti savršene da bi bile opasne. Dovoljno je da naprave listu potencijalnih meta, da izgrade mapu odnosa ili da povežu ljude koje ranije nije bilo lako povezati. Evropski i UN izveštaji ovakve prakse sve češće opisuju kao oblik „algoritamskog autoritarizma", koji širi moć države i privatnih aktera u digitalnom prostoru (OHCHR, A/HRC/48/31, 2021. I EU AI Act, 2024/1689).

Za branitelje/ke ljudskih prava to znači da se rizik ne završava na javnom okupljanju ili sastanku. Danas se on lako premešta i u digitalni trag: fotografiju, *check-in*, metapodatke poruka, pa čak i pojavljivanje u videu koji je objavio neko drugi. *AI* omogućava da se ti tragovi automatski prikupljaju, ukrštaju i koriste za nadzor mreža solidarnosti.

GENERATIVNA *AI* KAO ORUŽJE ZA NAPADE NA ŽENE

Generativna *AI*, alati koji prave tekst, sliku, zvuk ili video, otvorila je novu fazu rodno zasnovanog digitalnog nasilja. Danas je za par minuta moguće napraviti lažnu fotografiju, kompromitujući video ili audio snimak sa tuđim glasom. Najčešći i najbrutalniji primer su seksualizovani *deepfake* sadržaji bez saglasnosti, koji služe da zastraše, posrame i oteraju žene iz javnog prostora. Sve više istraživanja i međunarodnih tela upozorava da se ovo nasilje širi brzo upravo zato što je jeftino, lako za proizvodnju i teško zaustavljivo dok se već deli (UN Women, 2024 / UNESCO, 2023).

Takvi napadi ne ciljaju „samo" reputaciju, oni ciljaju to da žena prestane da govori javno. *Deepfake* ne mora ni da bude uverljiv. Dovoljno je da napravi konfuziju, da pokrene talas komentara, da potroši vreme i živce i da fokus prebaci sa onoga što se zagovara na beskrajno objašnjavanje i odbranu od laži.

AI-FIŠING I AUTOMATIZOVANE KAMPANJE UZNEMIRAVANJA

Fišing danas više nije onaj loše napisan *e-mail* sa smešnom adresom. Uz *AI*, napadači mogu da sastave poruke koje zvuče potpuno uverljivo: na lokalnom jeziku, u pravom tonu, čak i sa stilom koji liči na konkretnu osobu. A kada se to spoji sa alatima za *voice cloning*, lažnim pozivom glasom kolege ili partnera, dobijaš pretnju koja ne cilja tehničku rupu, nego **poverenje.**

I bot mreže su, uz *AI*, postale „pametnije". Mogu da vode razgovore, da se prilagođavaju reakcijama, da masovno prijavljuju naloge ili da zatrpaju komentare i poruke. Ono što je ranije zahtevalo desetine ljudi, danas može da odradi mali broj aktera uz dobru automatizaciju. Globalni izveštaji o stanju branitelja/ki ljudskih prava već beleže da je digitalno uznemiravanje sve sofisticiranije i da posebno pogađa žene i marginalizovane grupe.

ALGORITAMSKA NEPRAVDA I „NEVIDLJIVO UĆUTKIVANJE"

Još jedan sloj rizika je manje vidljiv, ali podjednako politički: **algoritmi platformi**. To su AI sistemi koji odlučuju šta je „problematičan" sadržaj, šta se briše, a šta se gura u stranu. Problem

je što često ne razumeju kontekst. Objave o nasilju, ratu, pravima osoba diskriminisanih po različitim osnovama, lako mogu da budu označene kao neprimerene, dok govor mržnje prođe jer je upakovan drugačije. UN i EU dokumenti već upozoravaju da ovakve algoritamske odluke mogu da dovedu do diskriminacije i selektivnog gušenja slobode izražavanja. [26]

Za organizacije civilnog društva to znači da vidljivost nije samo pitanje dobrog sadržaja. Često je i borba sa neprozirnim sistemima koji imaju ugrađene pristrasnosti.

Ovo poglavlje nije tu da uplaši, nego da proširi mapu rizika. Ne morate da postanete AI eksperti da biste se zaštitili, dovoljno je uvesti nekoliko jasnih navika i pravila.

PRAVILO VERIFIKACIJE IDENTITETA

- Za sve hitne zahteve koji dolaze *e-mail*-om/porukom: proveriti drugim kanalom.
- Ako stigne poziv glasom „kolege" koji zvuči čudno ili traži nešto osetljivo, prekinuti i nazvati nazad na poznati broj.
- Dogovoriti u timu jednostavnu verifikacionu frazu za krizne situacije.

POSTUPATI PREMA MEDIJIMA KAO PREMA DOKAZIMA

- Arhivirati originalne fotografije i snimke (sa metapodacima) u šifrovanom prostoru.
- Ne objavljivatij lokaciju u realnom vremenu kad je rizik visok.
- Razmisliti pre objave: „Da li ovo može biti izvučeno iz konteksta ili montirano?"

PRIPREMITI ODGOVOR NA *DEEPFAKE* UNAPRED

- U kriznom paketu imati kratak šablon saopštenja: *„Sadržaj je lažan/manipulisan. Naši verifikovani kanali su X i Y. Prijavili smo platformi i pravnim kanalima."*
- Ne ulaziti u rasprave sa napadačima. Fokusirati se na dokumentovanje i mreže solidarnosti.
- Ako je sadržaj seksualizovan ili posebno traumatičan, prioritet je zaštita osobe, ne pobeda u komentarima.

26 https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA%282024%29754450%28SUM01%29_EN.pdf

MINIMIZIRATI DIGITALNI TRAG GDE GOD JE MOGUĆE

- Ne čuvati osetljive liste kontakata na telefonu ako nije neophodno.
- Koristiti nestajuće poruke za teme visokog rizika.
- Periodično očistiti aplikacije i dozvole (telefon je najčešća meta).

UČITI TIM KAKO AI MENJA PRETNJE

Nije dovoljno da jedna osoba zna o *AI* rizicima. Na internim sastancima uvesti kratke primere:

- Kako izgleda *AI*-fišing;
- Šta je *deepfake* i kako se prepoznaje;
- Zašto je glasovna poruka danas isto što i link u *e-mail*-u.

Kratko, praktično, bez dramatizacije.

Veštačka inteligencija nije neutralan alat. Ona pojačava moć onih koji već imaju resurse: države, platforme, bogate privatne aktere, organizovane napadačke mreže. Zato je važno da je organizacije civilnog društva i branitelji/ke ljudskih prava ne posmatraju samo kao tehnološku novinu, nego kao novo polje borbe za slobodu, privatnost i sigurnost.

DIGITALNA BEZBEDNOST U DOBA AI ZNAČI DVE STVARI ISTOVREMENO:

- Da koristimo tehnologiju pametno, za našu misiju i zajednice,
- Da odbijemo da nam ista tehnologija postane alat ućutkivanja.

15. Reagovanje na digitalne incidente

U digitalnom prostoru napadi nisu rezervisani za velike organizacije. Na meti mogu biti i male lokalne inicijative, neformalne grupe, pojedinci/ke koje vode kampanje pa čak i timovi od dve ili tri osobe. Iskustvo rada sa civilnim društvom u Srbiji i regionu pokazuje da su napadi često oportunistički ili politički motivisani. Ali gotovo uvek idu istim putem: traže najslabiju tačku sistema, nalog ili uređaj koji nije dovoljno zaštićen.

Kada se dogodi incident, panika je najgora reakcija. Odmah za njom dolazi ignorisanje, a zatim i prebacivanje odgovornosti. Zato je unapred definisan plan reagovanja na digitalne incidente, prilagođen vašim kapacitetima, kontekstu i vrsti rada, presudan. Svi glavni modeli *incident response* ciklusa stalno ponavljaju istu stvar: plan mora da postoji pre nego što se incident desi, jer pod pritiskom nije vreme za improvizaciju.[27]

Pojam *incident response* je najbliže rečeno organizovano reagovanje na digitalne bezbednosne incidente. To podrazumeva skup koraka koje organizacija preduzima kada se suoči sa napadom, kompromitacijom podataka, uznemiravanjem na mrežama, hakovanjem naloga ili bilo kojom vrstom digitalne pretnje. Ti koraci ne moraju biti tehnički sofisticirani, ali moraju biti jasni, dostupni i primenljivi, baš kao u standardnom *incident response* životnom ciklusu: priprema, identifikacija, obuzdavanje, uklanjanje, oporavak i učenje.

27 Acronis https://www.acronis.com/en/blog/posts/what-is-incident-response

FAZA[28]	CILJ	KO VODI	PRVI KONKRETNI KORACI
1. Identifikacija	Potvrditi šta se dešava	Osoba zadužena za digitalnu bezbednost	Proveriti naloge, uređaje, poruke; ne širiti paniku
2. Obuzdavanje i zaštita	Zaustaviti širenje štete	IT podrška ili digitalno najpismenija osoba u timu	Promena lozinki, odjava sa svih sesija, privremena deaktivacija naloga
3. Dokumentovanje	Sačuvati dokaze	Osoba za dokumentovanje	Screenshot-ovi, linkovi, vreme, opisi, lista pogođenih naloga
4. Oporavak i učenje	Vratiti sistem i izvući lekcije	Tim zajedno	Povrat iz *backup*-a, zakrpe, analiza "šta je omogućilo napad"

28 Digital Firts Aid Kit https://digitalfirstaid.org

15.1. Osnovni elementi reagovanja na incidente

PRVI KORAK: **PREPOZNATI DA SE NEŠTO DEŠAVA**[29]

Mnoge organizacije ne reaguju jer ne prepoznaju da je incident u toku. Promene u ponašanju naloga, neautorizovani pristupi, čudne poruke od poznatih kontakata, iznenadne greške u sistemu ili neočekivane notifikacije o prijavama, sve to mogu biti rani signali. Potrebno je da postoji osoba ili mali tim zadužen za praćenje digitalne infrastrukture, čak i ako je ta infrastruktura „samo" *e-mail* i društvene mreže. U manjim organizacijama to može biti rotirajuća uloga, ali mora biti jasno definisana da se ne bi dogodilo da svi misle da je to nečiji tuđi posao.

DRUGI KORAK: **ZAŠTITITI ONO ŠTO JE NAJVAŽNIJE**

Kada se incident potvrdi, prioritet je zaštita ljudi i podataka. To znači:

- odmah promeniti lozinke naloga kod kojij je došlo do kompromitacije i uključiti ili resetovati 2FA sa bezbednog uređaja;
- isključiti pristup osobama koje nisu deo tima ili za koje sumnjate da su kompromitujuće;

29 UK National Cyber Security Center https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes

- privremeno deaktivirati naloge ako napad traje i ne može se brzo obuzdati;
- obavestiti tim da ne koristi određene kanale dok se bezbednost ne proveri.

U slučaju uznemiravanja, važno je pružiti psihološku podršku osobama koje su meta, smanjiti javnu izloženost ako je to bezbednije i, kada postoji osnov, uključiti pravnu pomoć. *Incident response* okviri posebno naglašavaju da je „*containment*" (obuzdavanje) često prvo pitanje bezbednosti ljudi, pa tek onda tehnologije.

TREĆI KORAK: **DOKUMENTOVATI SVE**

Bez dokumentacije incident ostaje nevidljiv, a učenje nemoguće. Potrebno je zapisati:

- datum i vreme kada je incident primećen;
- ko je pogođen;
- koji nalozi, podaci ili sistemi su bili uključeni;
- šta je konkretno primećeno (skrinšot, link, poruka, log);
- koje korake je organizacija preduzela i kada;

Ova evidencija pomaže i za internu analizu i za eventualnu pravnu zaštitu, ali i za komunikaciju sa partnerima ili javnošću ako organizacija odluči da o napadu govori.

ČETVRTI KORAK: **KOMUNICIRATI INTERNO I EKSTERNO**[30]

Interna komunikacija mora biti jasna, smirena i fokusirana na zaštitu tima. Svi treba da znaju šta se dešava, šta se od njih očekuje i koje kanale trenutno koriste ili ne koriste. Eksterna komunikacija zavisi od konteksta. Nekad je pametno ne izlaziti odmah sa detaljima dok se situacija ne stabilizuje, a nekad je bitno brzo obavestiti partnere, donatore, medije ili zajednicu, posebno ako postoji rizik da će se napad preliti na njih.

U oba slučaja komunikacija mora biti promišljena. Ne deliti sve operativne detalje, ali pokazati da organizacija reaguje odgovorno, da štiti ljude i da napad ne tretira kao normalan deo posla.

30 Acronis https://www.acronis.com/en/blog/posts/what-is-incident-response

PETI KORAK: **OBNOVA SISTEMA**

Nakon što se incident obuzda, proverava se integritet sistema:

- Skeniranje na *malware;*
- Provera pristupa i dozvola;
- Ažuriranje softvera i uređaja;
- Reset lozinki i 2FA gde je potrebno;
- Vraćanje podataka iz rezervnih kopija ako je došlo do gubitka.

Ako organizacija nema tehnički tim, može se obratiti mrežama podrške. U Srbiji SHARE Fondacija ima specijalizovani SHARE CERT koji pruža tehničku i pravnu pomoć medijima i organizacijama civilnog društva u incidentima.

ŠESTI KORAK: **ANALIZA I UČENJE**

Svaki incident mora da se iskoristi kao prilika za učenje. Šta je omogućilo napad? Koje slabosti su isplivale? Kako sprečiti ponavljanje? Analiza treba da bude kolektivna i bez lova na krivce, a rezultat mora biti konkretna promena u pravilima, praksi i kulturi organizacije. Upravo *lessons learned* faza (naučene lekcije) je ono što *incident response* okviri stavljaju kao završni, ali najvažniji korak, jer bez njega svaki sledeći napad počinje sa istih slabih tačaka.[31]

Organizovano reagovanje ne traži savršene uslove. Traži dogovor, raspodelu uloga, osnovnu dokumentaciju i volju da se iz incidenta izađe pametnije i solidarnije. To je razlika između organizacije koja se stalno gasi pod pritiskom i one koja uči da se brani.

15.2. Minimalni krizni paket

Minimalni krizni paket obuhvata sve što je potrebno da bude spremno pre incidenta. Planiranje pre incidenta omogućava da se u trenutku napada sačuva prisebnost. Ovo je minimum koji svaka organizacija može da pripremi bez mnogo resursa.

31 Web Asha Technologies https://www.webasha.com/blog/what-are-the-six-phases-of-incident-response-in-cybersecurity-step-by-step-guide

KONTAKT LISTA ZA HITNE SITUACIJE:

- Osoba u timu zadužena za digitalnu bezbednost;
- IT podrška (interno ili eksterno);
- Pravna podrška;
- Psihološka podrška ili bar kontakt osobe za brigu;
- Partnerske mreže solidarnosti;

Ova lista treba da postoji *offline (*papir ili šifrovani fajl van glavnog sistema).

Bezbedni kanal za hitne poruke. Dogovoriti unapred gde se tim okuplja kad postoji sumnja na kompromitaciju. Primer: *Signal* grupa ili *Element* soba. Važno: taj kanal se ne koristi za svakodnevno ćaskanje da bi ostao jasan za krizne situacije.

OFFLINE **KOPIJE NAJVAŽNIJIH PODATAKA**

- Ključni dokumenti organizacije (ugovori, strategije, baze kontakata);
- *Backup* ključevi / *recovery codes* za naloge;
- Uputstva za oporavak (koraci za vraćanje pristupa).

Šablon za evidenciju incidenta. Jedan dokument u koji se odmah upisuje: šta se desilo, kad, ko je pogođen, koji su dokazi i šta je urađeno.

Dogovor o javnoj komunikaciji. Ko govori u ime organizacije, kada se izlazi u javnost, šta se nikad ne objavljuje u prvoj fazi (operativni detalji, identiteti ugroženih osoba, lokacije).

15.3. Briga o timu posle incidenta

Digitalni incidenti retko ostaju samo digitalni. U telu i glavi ostavljaju trag: anksioznost, bes, nemoć, paranoične misli, povlačenje iz javnosti, narušeno poverenje u ljude i tehnologiju. Ako organizacija to ignoriše, napad uspeva i nakon što je tehnički završen.

Pristup zasnovan na informisanosti o traumi znači da uz tehničke korake pravimo i ljudske.

Normalizujte reakcije. Osoba koja je meta napada nije preosetljiva ako reaguje. Reakcije su normalne. Podeliti to naglas u timu je prvi korak podrške.

Ne tražiti krivca. U trenutku kad krene lov na grešku, tim se zatvara i sledeći put ćuti. Fokus je na tome „šta se desilo" i „šta menjamo", ne na „ko je kriv".

Dati pravo na pauzu i rotaciju. Nekad je digitalna bezbednost i pravo na povlačenje:

- privremeno gašenje naloga;
- rotiranje javnog lica;
- raspodela medijskih istupa.

Organizovati *debrief.* *Debrief* je kratki sastanak posle incidenta, strukturirana sesija ili razgovor nakon završenog događaja, čiji je cilj da se analizira šta je prošlo dobro, šta nije i kako se može poboljšati u budućnosti, učenje iz grešaka i postizanje kolektivnog rasta i transparentnosti. *Debrief* obuhvata razgovor o tome:

- Šta se desilo (faktički);
- Kako je to uticalo na ljude (emocionalno);
- Šta menjamo (organizacijski);
- Šta nam treba (podrška, resursi).

Uključiti eksternu podršku kada je potrebno. Neke situacije prevazilaze mogućnosti tima:

- Dugotrajne kampanje uznemiravanja;
- Doksing porodice;
- Pretnje fizičkim nasiljem.

U ovim situacijama je se preporučuje potražiti psihološku ili pravnu pomoć.

Zašto je ovo deo digitalne bezbednosti?

Zato što napadači računaju na iscrpljivanje. Zato što ako tim izgori, napad je uspeo čak i bez tehničke štete. Zato što je briga o ljudima strateški deo odbrane.

15.4. Kako se zaštititi na ličnom nivou

Digitalni napadi ne dolaze uvek u prepoznatljivim, dramatičnim oblicima. Često počinju sitno: čudnom porukom, nalogom koji se ponaša neobično, komentarima koji postaju neprijatni ili iznenadnim interesovanjem za naš rad i privatni život. Razumevanje ovih obrazaca prvi je korak lične zaštite jer tek kada prepoznamo šta zapravo treba da gledamo, možemo da reagujemo pravovremeno i smireno.

Pre upoznavanja sa alatima i tehnikama, najvažnije je razumevanje sebe, svojih navika u digitalnom prostoru, svojih granica i svojih rizika, jer digitalna bezbednost počinje od ličnog uvida, a ne od tehnologije.

1) Identifikovati svoje najosetljivije podatke, odnosno šta je najugroženije ukoliko procure: kontakti, lokacije, priznanja, fotografije, planovi, komunikacija sa žrtvama. Ovo je crvena zona.

2) Nije potrebno svuda biti pod istim imenom. Može se odvojiti lični i javni identitet. Ovo smanjuje doksing rizik i targetiranje porodice.

3) Rizik nastaje kroz rutinu. Najviše grešaka se desi iz navike: brz klik, deljenje lozinke iz žurbe, slanje fajla na pogrešnu adresu. Zato je važno stati na 10 sekundi pre slanja osetljivih podataka.

4) Psihološka sigurnost je deo digitalne bezbednosti. Kada se desi napad, telo i um reaguju: može se pojaviti stres, nesanica, povlačenje, osećaj srama. To nije slabost, nego reakcija na nasilje. Važno je potražiti podršku. Korisno je dogovoriti *buddy* osobu (osobu od poverenja) u timu koja može biti podrška. Ne prolaziti kroz napad samostalno.

5) Uvek postoji mogućnost da se napravi pauza od digitalne izloženosti i prisustva u dugitalnom svetu, ili mogućnost da se privremeno povučete. Digitalni prostor nije neutralan. Ponekad je taktički bezbednije napraviti pauzu, promeniti kanal, prebaciti javno lice na drugu osobu ili preći na anonimizovani način rada. U pitanju je strategija opstanka, a ne poraz.

16. Studije slučaja iz Srbije

Digitalna bezbednost nije teorija iz priručnika. Ona se uči i gradi u stvarnim situacijama: kroz napade, pogrešne procene, dobre (i loše) reakcije i kroz posledice koje često traju i dugo nakon što se incident zatvori.

Zato su studije slučaja dragocene: omogućavaju nam da učimo brže i pametnije, bez toga da svaka organizacija mora sve da prođe na sopstvenoj koži. Kroz primere vidimo obrasce, razumemo taktike napadača, prepoznajemo šta je funkcionisalo, a šta nije i na osnovu toga jačamo sopstvenu otpornost.[32]

Zašto su studije slučaja važne?[33]

Zato što pokazuju kako izgledaju stvarni napadi, ne idealni scenariji. Zato što oslikavaju kontekst i ranjivosti koje napadači najčešće koriste. Zato što nude primere uspešnog i neuspešnog reagovanja. Zato što pomažu u izgradnji preventivnih strategija i protokola. Zato što povezuju lokalne borbe sa globalnim obrascima represije i nasilja.

32 Share fondacija https://www.sharefoundation.info/wp-content/uploads/Gender-Based-Digital-Violence-in-Serbia.pdf

33 https://lac.unwomen.org/sites/default/files/2023-12/report_onlineviolence_21dec23.pdf

PRIMER: ŽENE ZA MIR LESKOVAC, SRBIJA

U julu 2022. Članice udruženja Žene za mir iz Leskovca prijavile su niz pretnji i sajber napada. *Front Line Defenders* dokumentuje da su napadi trajali danima, uz pokušaje zastrašivanja zbog njihovog rada i javnog istupanja.[34]

Odgovor: Organizacija je slučaj prijavila policiji i javno ga dokumentovala. Front Line Defenders je zatim objavio hitan apel, čime je slučaj dobio međunarodnu vidljivost. To je lokalnu pretnju prebacilo u širi okvir zaštite branitelja/ki ljudskih prava i smanjilo rizik da napad ostane nevidljiv i da se ponavlja bez posledica.

Lekcije: Ovaj primer jasno pokazuje nekoliko stvari. Prvo, u manjim sredinama digitalne pretnje se često prepliću sa fizičkim i društvenim pritiscima, pa reakcija mora biti i digitalna i organizaciona. Drugo, internacionalizacija slučaja može da bude važan zaštitni mehanizam kada lokalne institucije ne reaguju dovoljno brzo ili ozbiljno. Treće, lokalnim grupama su potrebni unapred dogovoreni incident protokoli i saveznici van neposrednog okruženja, jer napad često ima cilj da ih izoluje i iscrpi. U ovom slučaju bila bi dragocena i solidarna podrška srodnih organizacija iz Srbije koja je izostala.

PRIMER: DRŽAVNI NADZOR I ŠPIJUNSKI SOFTVER *NOVISPY*, SRBIJA

Jedan od najozbiljnijih primera digitalne represije u Srbiji poslednjih godina jeste kampanja nadzora o kojoj je *Amnesty International* izvestio u decembru 2024. Prema njihovim nalazima, novinari i aktivisti bili su meta nezakonitog otključavanja telefona uz pomoć forenzičkih alata (*Cellebrite*), nakon čega je na uređaje instaliran špijunski softver *NoviSpy*. Takav *spyware* (špijunski softver) omogućava izvlačenje podataka i pristup porukama, kontaktima i drugim osetljivim informacijama, praktično, kompletan uvid u digitalni život mete.[35]

Odgovor: Mete napada su, uz podršku *Amnesty Security Lab* i domaćih organizacija, uradile forenzičku proveru uređaja i javno objavile nalaze (Amnesty International, 2024; SHARE Fondacija, 2024). Slučaj je brzo dobio međunarodnu pažnju: uključili su se mediji i organizacije, a upućeni su i pozivi na nezavisnu istragu i političku odgovornost. Javna dokumentacija i uključivanje međunarodnih aktera bili su ključni, jer se kod ovako sofisticiranog nadzora ne možete osloniti samo na „unutrašnju" proveru naloga ili osnovne tehničke korake.

34 Frontline Defenders https://www.frontlinedefenders.org/en/case/threats-members-citizens-association-women-peace-1

35 Amnesty International https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists

Lekcije: Ovaj slučaj nosi nekoliko važnih poruka. Prvo, pretnje u Srbiji ne dolaze samo od anonimnih napadača, već i od aktera sa institucionalnim resursima zato bezbednosno planiranje mora da uključuje i scenarije nadzora, a ne samo klasično hakovanje. Drugo, šifrovanje uređaja, minimizacija osetljivih podataka na telefonu i jasne procedure za situacije oduzimanja uređaja postaju obavezan deo bezbednosne kulture. Treće, u ovakvim situacijama saradnja sa nezavisnim laboratorijama i javno objavljivanje nalaza često su najefikasnija odbrana jer menjaju odnos moći i otvaraju prostor za pravni i politički pritisak.

PRIMER: BIRN NOVINARI META *PEGASUSA*, SOFISTICIRANI NADZOR KAO PORUKA, SRBIJA

U februaru 2025. Najmanje dvoje novinara Balkanske istraživačke mreže (BIRN) u Srbiji bili su meta pokušaja instalacije špijunskog softvera Pegasus. *Amnesty International Security Lab* je forenzičkom analizom potvrdio da su novinari dobili sumnjive poruke preko *Vibera*, sa linkom koji je bio deo Pegasus napada. *Pegasus*, jednom kada uđe na uređaj, može da obezbedi gotovo potpun pristup telefonu, porukama, kontaktima, fajlovima, pa čak i mikrofonu i kameri često bez jasnih tragova za korisnika.[36]

Odgovor: BIRN je javno objavio nalaze i sarađivao sa *Amnesty Security Lab*, čime je incident odmah internacionalizovan i dokumentovan (BIRN, 2025; Amnesty International Security Lab, 2025). Javna objava je sprečila da napad ostane „tiha mera", a organizacije za slobodu medija su slučaj dodatno pojačale kroz kampanje i pritisak na institucije.

Lekcije: Ovaj slučaj pokazuje da pretnje u Srbiji 2025. Nisu ograničene na trolovanje ili fišing, već uključuju i visoko sofisticiran nadzor. To znači da zaštita mora da ide dalje od jakih lozinki: važni su šifrovanje uređaja, minimizacija osetljivih podataka na telefonu, redovne bezbednosne provere i jasan plan za situacije nadzora. U ovakvim slučajevima, saradnja sa nezavisnim laboratorijama i javno dokumentovanje često postaju ključan deo odbrane.

36 https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware

17. Prilozi

17.1. Čeklista za ORGANIZACIJE 

1. Politike i pristupi

- Postoji kratka, jasna bezbednosna politika (2–3 strane).
- Dodeljeni pristupi prate princip „najmanjeg potrebnog pristupa".
- Svi zajednički nalozi se čuvaju u menadžeru lozinki.

2. Tehnički minimum

- 2FA uključena na svim važnim nalozima (*e-mail*, društvene mreže, *Cloud*).
- Redovna ažuriranja svih uređaja i platformi.
- Backup važnih podataka postoji i testiran je.

3. Rad sa osetljivim podacima

- Osetljivi dokumenti čuvaju se u šifrovanim skladištima.
- Komunikacija o poverljivim temama ide samo E2EE kanalima.

4. *Incident-response* spremnost

- Postoji jasan protokol za prijavu i rukovanje incidentima.
- Tim zna ko je kontakt osoba za hitne slučajeve.
- Postoji formular za prijavu incidenta i koristi se.

5. Ljudi i podrška

- Novi članovi/članice prolaze *onboarding* o bezbednosti.
- Tim ima kontakt za psihološku podršku tokom napada.

17.2. Čeklista za LIČNU DIGITALNU BEZBEDNOST

1. Nalozi i lozinke

- Sve lozinke su duge, jake i jedinstvene.
- Menadžer lozinki se koristi svakodnevno.
- 2FA uključena na svim ključnim nalozima.

2. Uređaji

- Telefon i laptop zaključavaju se PIN-om/lozinkom (ne *Pattern*).
- Ažuriranja uključena i redovna.
- *Backup* važnih podataka postoji (*Cloud* ili eksterni disk).

3. Privatnost i identitet

- Privatnost na društvenim mrežama podešena (ko vidi šta).
- Odvojen lični i javni identitet, ako je potrebno.
- Svest o digitalnom tragu (šta gde ostavljam).

4. Komunikacija

- Osetljive poruke šalju se samo E2EE kanalima (*Signal, Proton Mail*).
- Opasni linkovi i poruke se proveravaju- "stop 10 sekundi".

5. Psihološka bezbednost

- Postoji *buddy* osoba za podršku tokom napada.
- Znam da je povlačenje iz konflikta legitimna strategija, ne poraz.

18. Resursi, alati i mreže podrške

Digitalna bezbednost ne može se graditi u izolaciji. Ona zahteva pristup znanju, alatima, podršci i zajednicama koje razumeju specifične izazove s kojima se suočavaju aktivistkinje i organizacije civilnog društva. U ovom poglavlju predstavljeni su najvažniji resursi – od softverskih alata do mreža solidarnosti – koji mogu pomoći u jačanju digitalne otpornosti.

Ovaj deo sadrži;

- Preporučene aplikacije i softveri za bezbednost;
- Platforme za edukaciju i samopomoć;
- Organizacije koje pružaju tehničku i pravnu podršku;
- Mreže za hitne intervencije i solidarnost;
- Lokalne i međunarodne inicijative;

18.1. Alati za digitalnu bezbednost

ZA ŠIFROVANJE I ZAŠTITU FAJLOVA:

- *VeraCrypt* - šifrovanje diskova i kontejnera: veracrypt.fr
- *Cryptomator* - šifrovanje fajlova u oblaku: cryptomator.org
- *KeePassXC* - lokalni menadžer lozinki: keepassxc.org

ZA BEZBEDNU KOMUNIKACIJU:

- *Signal* - šifrovana razmena poruka i poziva: signal.org
- *ProtonMail* - šifrovani *email* servis: proton.me
- *Element (Matrix)* - decentralizovana komunikacija: element.io

ZA *BACKUP* I OPORAVAK:

- *Duplicati* - automatski *backup* sa enkripcijom: duplicati.com
- *Restic* - efikasan alat za komandnu liniju: restic.net

EDUKATIVNE PLATFORME I VODIČI

- *Security in-a-Box* - vodič za digitalnu bezbednost aktivista: securityinabox.org
- *Surveillance Self-Defense* (EFF) - praktični saveti za zaštitu privatnosti: ssd.eff.org
- *Digital First Aid Kit* - koraci u slučaju digitalnog napada: digitalfirstaid.org

18.2. Organizacije koje pružaju podršku

U SRBIJI:

- SHARE Fondacija- pravna i tehnička podrška u oblasti digitalnih prava: sharefoundation.info
- Beogradski centar za bezbednosnu politiku- istraživanja i analize: bezbednost.org

REGIONALNO I GLOBALNO:

- *Access Now- Digital Security Helpline*: accessnow.org/help
- *Digital Defenders Partnership* - podrška braniteljima/kama ljudskih prava: digitaldefenders.org
- *Front Line Defenders* - hitna pomoć i zaštita aktivistima: frontlinedefenders.org

MREŽE SOLIDARNOSTI I HITNE INTERVENCIJE

- *Women's Rights Online (Web Foundation)* - zagovaranje digitalne jednakosti: webfoundation.org
- *Digital Rights Watch*- monitoring i edukacija: digitalrightswatch.org.au

Rečnik ključnih pojmova

TEHNIČKI POJMOVI	
Enkripcija (šifrovanje):	Proces pretvaranja podataka u nečitljiv format koji se može dešifrovati samo uz odgovarajući ključ, radi zaštite fajlova, komunikacije i sistema.
Simetrično šifrovanje:	Tip šifrovanja u kome se isti ključ koristi i za šifrovanje i za dešifrovanje podataka; praktično za lokalne fajlove, diskove i rezervne kopije.
Asimetrično šifrovanje:	Tip šifrovanja koji koristi par ključeva: javni ključ za šifrovanje i privatni ključ za dešifrovanje; osnova za *PGP* i srodne protokole bezbedne razmene.
PGP - Pretty Good Privacy / OpenPGP (sistem za zaštitu privatnosti):	Standard za šifrovanje *email*-ova i fajlova zasnovan na asimetričnom šifrovanju, omogućava bezbednu razmenu informacija preko inače nesigurnih kanala.
End to end (od kraja do kraja) enkripcija (E2EE):	Sistem u kome samo pošiljalac i primalac mogu da čitaju poruke; ni platforma koja prenosi poruku nema pristup njenom sadržaju.
Metapodaci:	Podaci o komunikaciji, a ne o njenom sadržaju, na primer ko je s kim komunicirao, kada i koliko često; mogu se koristiti za praćenje i mapiranje mreža.
Podaci u mirovanju / podaci u prenosu:	Podaci „u mirovanju" su fajlovi dok stoje na uređaju ili u *Cloud*-u; "u prenosu" su podaci dok se šalju (*email*, *chat, upload*). Obe faze traže zaštitu.
Zero click **napad** (napad bez klika):	Napad koji ne zahteva interakciju korisnika; kompromitacija se dešava automatski, bez klika na link ili otvaranja fajla.
Zero day **ranjivost** (ranjivost nultog dana):	Bezbednosna rupa u softveru koja je nepoznata proizvođaču ili još nije zakrpljena, pa može biti iskorišćena pre nego što postoji odbrana.
Patch (zakrpa) **i** ***patching***:	Ažuriranje softvera koje ispravlja ranjivosti ili greške; redovno *patch*-ovanje je ključna preventivna mera.
Malver (zlonamerni softver):	Zlonamerni softver dizajniran za krađu podataka, špijuniranje, sabotiranje ili preuzimanje kontrole nad uređajem.
Spyware (špijunski softver):	Vrsta malvera koja tajno prati korisnika i prikuplja podatke (poruke, lokacije, fajlove), često bez vidljivih simptoma.
Ransomware (ucenjivački softver):	Malver koji šifruje ili zaključava podatke i traži otkup za njihovo otključavanje; često se širi fišingom ili eksploatacijom ranjivosti.

Firewall (zaštitni zid):	Softverski ili hardverski mehanizam koji kontroliše dolazni i odlazni mrežni saobraćaj i blokira neovlašćen pristup.
VPN - Virtual Private Network (virtuelna privatna mreža):	Tehnologija koja šifruje internet saobraćaj i maskira IP adresu, čime smanjuje mogućnost nadzora i praćenja.
Backup (rezervna kopija):	Duplikat podataka koji se čuva odvojeno od originala radi zaštite od gubitka, sabotaže ili kvara.
***Cloud* skladištenje** (onlajn skladištenje):	Čuvanje podataka na udaljenim serverima kojima se pristupa putem interneta (npr. *Google Drive, Dropbox, Proton Drive*).
Menadžer lozinki:	Softver koji bezbedno čuva, generiše i automatski unosi lozinke, olakšava korišćenje jedinstvenih jakih lozinki.
***Passphrase* (lozinka fraza):**	Duga lozinka sastavljena od više reči ili smislenih delova; dužina i raznolikost je čine otpornijom na provale.
MFA / 2FA (višefaktorska autentifikacija):	Dodatni korak prijave pored lozinke (kod iz aplikacije, SMS, hardverski ključ) koji značajno otežava preuzimanje naloga.
CDN - *Content Delivery Network* (mreža za isporuku sadržaja):	Ukoliko dodje do napada na organizaciju, ova aplikcija pomaže da se brojni *email*-ovi koji su usmereni ka sajtu, podele na više servera, tako da omogući lakši protok.

BEZBEDNOSNI INCIDENTI I TAKTIKE

Fišing (mrežna krađa identiteta)	Prevara kroz lažne poruke koje navode korisnika da otkrije lozinku, klikne zlonamerni link ili preuzme malver.
***Spear* fišing** (targetirano “pecanje” ili precizni fišing)	Ciljani fišing usmeren na konkretnu osobu ili organizaciju, često personalizovan tako da deluje kao legitimna poruka iz poznatog kruga.
Socijalni inženjering	Manipulacija ljudima da urade nešto u korist napadača (otkriju podatke, kliknu link, promene pristup), umesto napada na tehnologiju.
***Brute force* napad** (napad „sirovom silom”):	Automatizovano isprobavanje velikog broja lozinki ili ključeva dok se ne pogodi tačan.
Credential stuffing (napad ukradenim akreditivima):	Napad u kome se procurele lozinke sa jedne platforme koriste za pokušaje prijave na drugim nalozima; zato su jedinstvene lozinke ključne.
Doksing (objavljivanje privatnih podataka)	Objavljivanje privatnih informacija (adresa, broj telefona, fotografije) bez dozvole sa ciljem zastrašivanja ili diskreditacije
Ciljano uznemiravanje	Koordinisani napadi putem komentara, poruka ili prijavljivanja naloga, sa ciljem da proizvedu strah, stres ili reputacijsku štetu.

Lažni nalozi	Nalozi koji imitiraju identitet aktivistkinja ili organizacija, koriste se za dezinformacije, prevare ili diskreditaciju.
Diskreditacija	Taktika širenja lažnih, manipulisnih ili izvučenih sadržaja radi narušavanja ugleda osobe ili organizacije.
Bot mreža	Automatizovani ili poluautomatizovani nalozi koji služe za širenje sadržaja, uznemiravanje, manipulaciju algoritmima i lažno stvaranje utiska javnog mnjenja.
Incident response (odgovor na incidente)**:**	Organizovani skup koraka koje organizacija preduzima kada se suoči sa digitalnim napadom, od identifikacije i obuzdavanja do oporavka i učenja.

Lista korišćenih izvora:

- Access Now. (n.d.). *Digital Security Helpline*. https://www.accessnow.org/help
- Amnesty International. (2024, December 16). *Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists*. https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities--using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists
- Amnesty International Security Lab. (2024, December). *A digital prison: Surveillance and the suppression of civil society in Serbia*. https://securitylab.amnesty.org/latest/2024/12/a-digital-prison-surveillance-and-the--suppression-of-civil-society-in-serbia
- Amnesty International Security Lab. (2025, March 27). *Serbia: Journalists targeted with Pegasus spyware*. https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware
- Atlantic Council. (n.d.). *How do cyber attacks threaten the Balkans? A Debrief with Dan Ilazi and Filip Stojanovski* (Balkans Debrief). https://www.atlanticcouncil.org/content-series/balkans-debrief/how-do-cyber-attacks-threaten-the-balkans-a-debrief-with-dan-ilazi-and-filip-stojanovski
- Balkan Insight. (2025, March 27). *Two BIRN journalists in Serbia targeted with Pegasus spyware*. https://balkaninsight.com/2025/03/27/two-birn-journalists-in-serbia-targeted-with-pegasus-spyware
- Cybersecurity and Infrastructure Security Agency (CISA). (2024). *Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society* (PDF). https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating--cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf
- Digital Defenders Partnership. (n.d.). *Digital Defenders Partnership* (Incident Response Fund and partnerships). https://www.digitaldefenders.org
- Digital First Aid Kit. (n.d.). *Digital First Aid Kit*. https://digitalfirstaid.org/
- Drata. (n.d.). *NIST password guidelines* (blog). https://drata.com/blog/nist-password-guidelines
- Electronic Frontier Foundation. (n.d.). *Surveillance Self-Defense* (home). https://ssd.eff.org/
- Front Line Defenders. (2022, July 22). *Threats to members of Citizens' Association of Women for Peace (Žene za mir), Serbia*. https://www.frontlinedefenders.org/en/case/threats-members-citizens-association-women-peace-2
- Internews. (2023). *Field Guide to incident response for civil society and media* (PDF). https://internews.org/wp-content/uploads/2023/11/Field-Guide-to-Threat-Labs.pdf
- Internews. (2023). *Digital Threat Landscape: Serbia* (PDF). https://internews.org/wp-content/uploads/2023/11/Serbia-Digital-Threat-Landscape-Report.pdf
- Lifeline (Digital Defenders Partnership). (n.d.). *Lifeline Toolkit: Digital Security* (PDF). https://static1.squarespace.com/static/54dbcb77e4b011d-9d8fd69f1/t/60250a4db0e7682485c5822b/1613040205449/lifeline%2Btoolkit%2Bdigital%2Bsecurity%2Bfinal%2B%28feb%2B2021%29.pdf
- Mimecast. (n.d.). *Google Drive security guide* (blog). https://www.mimecast.com/blog/google-drive-security-guide
- Open Source Security Atlas. (n.d.). *Tool entry (ID 3836)*. https://www.opensecatlas.com/tool/3836

- Radio Slobodna Evropa. (n.d.). *[Članak o pretnjama/grafitima – inicijativa mladih / ambasada Ukrajine]*. https://www.slobodnaevropa.org/a/srbija-pretnje-grafit-inicijativa-mladih-ambasada-ukrajine/32550703.html
- Session. (n.d.). *Session* (website). https://getsession.org
- SHARE Foundation. (2023). *Monitoring digitalnih prava 2023: Srbija u spirali digitalnog nasilja*. https://sharefoundation.info/monitoring-digitalnih-prava-2023-srbija-u-spirali-digitalnog-nasilja
- SHARE Foundation. (n.d.). *Gender-Based Digital Violence in Serbia* (PDF). https://www.sharefoundation.info/wp-content/uploads/Gender-Based-Digital-Violence-in-Serbia.pdf
- SHARE Fondacija. (2024). MUP and BIA illegally hacking phones of activists and journalists. SHARE Foundation. https://sharefoundation.info/en/mup-and-bia-illegally-hacking-phones-of-activists-and-journalists/
- Signal. (n.d.). *Sealed Sender* (blog). https://signal.org/blog/sealed-sender
- SourceForge. (n.d.). *Duplicati* (software page). https://sourceforge.net/software/product/Duplicati/
- Tactical Tech & Front Line Defenders. (2020, May 20). *Security in-a--Box*. Front Line Defenders. https://www.frontlinedefenders.org/en/resource-publication/security-box
- Tactical Tech. (n.d.). *Security in-a-Box* (website). https://securityinabox.org/en
- TechRepublic. (n.d.). *Bitwarden vs. KeePass* (članak). https://www.techrepublic.com/article/bitwarden-vs-keepass
- UK National Cyber Security Centre (NCSC). (n.d.). *Cyber incident response processes* (Incident management collection). https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes
- UN Women (Regional Office for the Americas and the Caribbean). (2023, December 21). *[Report on online violence]* (PDF). https://lac.unwomen.org/sites/default/files/2023-12/report_onlineviolence_21dec23.pdf
- United Nations Office of the High Commissioner for Human Rights. (n.d.). *A/HRC/29/32: Report on encryption and anonymity and the human rights framework* (tematski izveštaj). https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework
- United Nations Office of the High Commissioner for Human Rights. (n.d.). *Women activists fighting for safe digital space* (story). https://www.ohchr.org/en/get-involved/stories/women-activists-fighting-safe-digital-space
- Verizon. (2024). *Data Breach Investigations Report (DBIR) 2024* (PDF). https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf
- WebAsha Technologies. (n.d.). *What are the six phases of incident response in cybersecurity? Step-by-step guide* (blog). https://www.webasha.com/blog/what-are-the-six-phases-of-incident-response-in-cybersecurity-step--by-step-guide
- Zoomer.rs. (n.d.). *Učinimo ih poznatim: Doksing kao sredstvo političke borbe u Srbiji*. https://zoomer.rs/ucinimo-ih-poznatim-doksing-kao-sredstvo-politicke-borbe-u-srbiji

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад

364.63:004.738.5]:343.988(036)

МАЉЕВИЋ, Данијела, 1975-
Vodič za digitalnu bezbednost branitelja i braniteljki ljudskih prava i organizacija civilnog društva [Elektronski izvor] / Danijela Maljević. - Kikinda : Centar za podršku ženama, 2025

Начин приступа (URL): Način pristupa (URL): https://www.cpz.rs/publikacije-cpz/. - Opis zasnovan na stanju na dan 28.1.2026. - Nasl. sa naslovnog ekrana. - Bibliografija.

ISBN 978-86-87681-17-0

а) Дигитални простор - Насиље - Заштита - Водичи

COBISS.SR-ID 185722121

VODIČ ZA DIGITALNU BEZBEDNOST BRANITELJA I BRANITELJKI LJUDSKIH PRAVA I ORGANIZACIJA CIVILNOG DRUŠTVA