Priročnik za nevladne organizacije

Protokol
digitalne varnosti podatkov

Jasna Babić

Ljubljana, 2021

PODPRI: razvoj inovativnih modelov podporništva in komuniciranja za NVO

Koordinator: Mirovni inštitut, Ljubljana
Partnerji: Pod črto, Društvo novinarjev Slovenije, Danes je nov dan

Info: https://www.mirovni-institut.si/projekti/podpri-razvoj-inovativnih-modelov-podpornistva-in-komuniciranja-za-nvo/
Kontakt: jasna.babic@mirovni-institut.si

PROTOKOL DIGITALNE VARNOSTI PODATKOV

Avtorica: **Jasna Babić**

Jezikovni pregled: **UREJANJE BESEDIL Ivan Cepanec s.p.**
Oblikovanje: **Jasna Babić**

Izdajatelj: **Mirovni Inštitut - Inštitut za sodobne družbene in politične študije**

Ljubljana, 2021

Mirovni inštitut
Inštitut za sodobne družbene in politične študije
The Peace Institute
Institute for Contemporary Social and Political Studies

POD ČRTO

DANES JE NOV DAN

DNS ()?!

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Publikacija je nastala s finančno podporo Ministrstva za javno upravo v okviru javnega razpisa za razvoj in profesionalizacijo NVO in prostovoljstva 2019. Za vsebino publikacije odgovarjata izključno izdajatelj in avtorica. Vsebina ne predstavlja uradnega stališča MJU.

PROTOKOL DIGITALNE VARNOSTI PODATKOV

Jasna Babić

KAZALO:

Predgovor

Nevladne organizacije veliko časa preživimo v digitalnem okolju. Dandanes skorajda ni organizacije, ki ne bi poskrbela za vsaj osnovno varno informacijsko okolje ali pa ima v sodelovanju z zunanjim izvajalcem_ko zagotovljeno potrebno informacijsko podporo. Kljub vsemu pa znanje o varni komunikaciji med člani_cami nevladnih organizacij in zunanjimi viri, o varni izmenjavi podatkov in o shranjevanju podatkov, dokumentov in stikov pogosto še vedno ostaja odvisno od zavesti in tehnološke pismenosti posameznika_ce.

Nevladne organizacije in druge civilno-družbene skupine, ki delujemo na področju zagovorništva, človekovih pravic in aktivnega državljanstva, smo občasno tarča organiziranih virusnih napadov na naša spletna mesta in komunikacijske kanale. Digitalna ranljivost (potencialni vdori v komunikacijo, onemogočanje dostopa do spletnih strani ali pridobivanje podatkov in dokumentov) predstavlja resno grožnjo neodvisnemu delu nevladnih organizacij. Zato je nujno, da nevladne organizacije in njihovi zaposleni_e ali člani_ce proaktivno zagotavljamo svojo digitalno varnost, varnost svojih podatkov in vzpostavimo varno komunikacijo s člani _cami svojega kolektiva, projektnimi partnerji in različnimi mediji ali drugimi viri.

Namen priročnika je okrepiti digitalno varnost in varnost komunikacije na organizacijski ravni nevladnih organizacij, opolnomočiti posameznike_ce, ki delajo v/za nevladno organizacijo ter predvsem razviti in izvajati interni digitalni protokol o varnosti in komunikaciji za posameznike, ki delajo v/za nevladne organizacije.

Priročnik je nastal v sklopu projekta *PODPRI: razvoj inovativnih modelov podporništva in komuniciranja za NVO*, s katerim konzorcijski partnerji Pod Črto, Društvo novinarjev Slovenije in Danes je nov dan razvijamo in preizkušamo inovativne modele komuniciranja in podporništva za naslavljanje nižanja demokratičnih standardov v Sloveniji in krčenja prostora za delovanje civilne družbe. Aktivnosti sofinancira Ministrstvo za javno upravo v okviru javnega razpisa za razvoj in profesionalizacijo NVO in prostovoljstva 2019.

Uvod

Bistveni del digitalnih kompetenc je varno vedenje v spletu, tj. odgovorna in varna uporaba spletnih storitev in spletnih aplikacij. Zmotno je mnenje, da zgolj poznavanje dela s spletnimi sistemi pomeni tudi njihovo varno uporabo. Varna uporaba spletnih storitev, z izjemo digitalne usposobljenosti uporabnika, zahteva tudi zavedanje in poznavanje nevarnosti, ki jih prinaša delo na spletu. Protivirusni programi in požarni zidovi predstavljajo minimalno zaščito. Organizacije, ki skrbijo za lastno digitalno varnost, uvajajo posebne varnostne rešitve za zaščito svojih povezav, omrežij, naprav in aplikacij. Digitalno varnost je zato treba v celoti integrirati na dveh ravneh: uvesti prožno zaščito na delovnem mestu pred vsemi grožnjami računalniških virusov, vdorov itd. v delovnih okoljih ter zaposlenim omogočiti znanje o digitalni varnosti, utrditi zavest o nevarnosti spletne zlorabe in vedeti, katero spletno zaščito uporabiti in kako.

Namen priročnika je predstaviti, kako zagotoviti enotno delovanje in sprejemanje odločitev zaposlenih, članov_ic in celotne organizacije o upravljanju s podatki. Upravljanje s podatki je širok pojem, ki vključuje:

- komunikacijska orodja (prek spleta, mobilnih telefonov in brez internetne povezave),
- vzdrževanje komunikacijskih orodij in opreme,
- komunikacijsko infrastrukturo,
- informacijsko infrastrukturo (kdo ima dostop do česa),
- zbiranje podatkov,
- shranjevanje podatkov,
- odstranjevanje in uničenje podatkov,
- fizično varnost (pri delu v pisarni).

Upravljanje s podatki določajo temeljna načela in procesi, s katerimi nevladna organizacija zagotovi, da lahko deluje dosledno, učinkovito in verodostojno. Priročnik obravnava različna področja informacij, ki jih nevladna organizacija pridobiva in z njimi upravlja. Za vsako vrsto informacij in podatkov je določen protokol, ki vsebuje vrsto zavez, ki jih morajo zaposleni_e/člani_ce in nevladna organizacija upoštevati v različnih situacijah, s katerimi se srečujejo, da bi zaščitili integriteto in varnost nevladne organizacije, (zunanjih) sodelavcev_k in članov_ic.

Izvajanje in vzdrževanje protokola

Izvajanje in vzdrževanje protokola temelji na nenehnem učenju in seznanjanju o določenih vrstah ranljivosti in varnostnih tveganjih. Vzdrževanje celovitosti in varnosti informacij ter podatkov obravnavamo kot proces stalne digitalne in fizične pripravljenosti. Pravilnik protokola se zato ves čas posodablja v skladu s pojavom novih varnostnih tveganj in ranljivosti.

Vzpostavitev varnostnega protokola sama po sebi še ni zagotovilo za zagotavljanje varnosti podatkov. Upravljanje s podatki je namreč stalni in nenehno spreminjajoč se proces. Zato se zaposlene in člane_ice spodbuja, da vprašajo za navodila, če naletijo na situacijo, kjer ne vedo, kako ravnati. Pogovor in razprava o vprašanjih ravnanja s podatki sta pomemben del ohranjanja informacijske kulture v nevladni organizaciji.

Doseg protokola

Protokol je namenjen vsem zaposlenim/članom_icam nevladne organizacije. Vsi zaposleni_e/člani_ce se morajo strinjati s protokolom. Ravnanje v skladu s protokolom je pomembno predvsem zaradi varovanja podatkov, službene oz. uradne komunikacije znotraj organizacije in izven nje ter pri uporabi programske in strojne opreme, ki je v lasti organizacije.

Protokolu je treba slediti tudi v primeru, če zaposleni_e uporabljajo osebne naprave za službeno komunikacijo. Enako velja za telekomunikacijo v povezavi s službenim delom. Sem spadajo tudi delo od doma in službene poti.

Vsebina protokola

Protokol digitalne varnosti obsega sedem razdelkov:

- določitev informacijske infrastrukture,
- upravljanje s programsko opremo,
- upravljanje z gesli,
- ravnanje s podatki,
- upravljanje sistemov e-pošte in drugih komunikacij,
- področje telekomunikacije in upravljanje z brezžično povezavo (Wi-Fi) ter
- kakšen je postopek pri zaposlitvi in prenehanju delovnega razmerja.

V nadaljevanju predstavljamo vsak razdelek posebej.

Informacijska infrastruktura

Prvi del protokola vsebuje opis celotne informacijske infrastukture v lasti nevladne organizacije in pravila njene uporabe. V nadaljevanju je opisan niz postopkov, ki opredeljujejo lastništvo različnih sestavnih delov (komponent) informacijskih naprav v pisarni in izven pisarne (doma, na poti) in kako do le-teh dostopajo zaposleni_e ali člani_ce.

Za informacijsko napravo štejejo: lastniški podatki organizacije (v pisarni in doma), računalniki, prenosniki in tablice, strežnik, elektronske mobilne naprave, USB-ključi/odstranljivi mediji/diski, zbirke podatkov, programska oprema.

Nevladna organizacija se v protokolu zavezuje, da bo:

- pripravila *Informacijski dokument*, ki bo služil kot referenca za druge razdelke, ki se nanašajo na uporabo in vzdrževanje informacijskih naprav. Več o dokumentu na str. 21.
- vzdrževala varnost datotečnega strežnika, poštnega strežnika (kjer je odprt e-naslov) in drugih podatkovnih naprav,
- omejila dostop do naprav in določila skrbnike_ce,
- spreminjala gesla v skladu s poglavjem Upravljanje z gesli (str. 12),
- vzpostavila jasna in dosledna dovoljenja za dostop za vse uporabnike_ce,
- fizično zavarovala strežnik v pisarni (npr. zaščita pred neugodnimi vremenskimi vplivi in morebitnimi fizičninimi poškodbami),
- obvestila zaposlene, ko pride do izpadov, zastojev v zvezi s podatkovnimi napravami, sporočila, kdaj bodo naprave ponovno na voljo ter po potrebi omogočila menjavo gesel.

V protokolu se zaposleni_e/člani_ce zavežejo, da bodo:

- na omrežnih strežnikih vzdrževali podatke nevladne organizacije (datoteke in druge dokumente) v skladu s smernicami in želenimi lokacijami,
- upoštevali naslednje smernice glede shranjevanja in upravljanja datotek na strežniku:
    - kam shraniti osebne datoteke in dokumente (npr. v katere dele strežnika/mape),
    - kam shranjevati osnutke datotek in delovnih dokumentov, dokler se te ne delijo z drugimi uporabniki, in kam končni dokument,
    - kam shranjevati velike predstavnostne datoteke (če je to potrebno),
    - obvestili_e tehnično osebje, če uporabnik_ca ne more odpreti datotek na omrežnih pogonih, spremeniti ali shraniti dokumentov,
    - kam shranjevati začasne datoteke, npr. skenirane slike, prenesene datoteke z interneta, dokumenti nezaupne narave (npr. 'desktop' ali 'moji dokumenti', ne na strežnik),
    - da bodo vedno zaprli_e datoteke na omrežnih strežnikih, ko končajo delo,
    - da se bodo vedno odjavili_e iz pisarniškega računalnika ob koncu dneva.

Upravljanje programske opreme

Drugi del protokola pokriva področja, povezana s programsko opremo, vključno s spoštovanjem licenc, namestitvijo programske opreme, posodobitvami programske opreme in protivirusnim programom. Priporočljivo je, da se odgovornost namestitve programske opreme in protivirusnega programa za celotno organizacijo dodeli zunanjemu izvajalcu_ki v skladu s pogodbo o vzdrževanju, zaposleni_e/člani_ce pa skrbijo za redno posodabljanje programske opreme.

Nevladna organizacija se pri tem zavezuje, da:

- ima potrdilo in če je treba, navede licence za potrebno programsko opremo,
- opomni zaposlene, da redno posodabljajo svojo programsko opremo,
- poskrbi za posodobitev operacijskega sistema na datotečnem strežniku in vseh posameznih računalnikih in zažene programske popravke (če je treba, tudi v skladu z zunanjim izvajalcem_ko),
- zagotovi posodobljeno licenčno protivirusno programsko opremo za vse računalnike (če je treba, tudi v skladu z zunanjim izvajalcem_ko),
- omogoči spodbude za posodobitve programske opreme.

Zaposleni_e/člani_ce soglašajo, da bodo:

- preverili_e aplikacije za posodobitve programske opreme in zagnali_e posodobitve najmanj enkrat na mesec oz. takoj, ko so na voljo. Takrat naprave ne ugašajo, dokler ni posodobitev končana;
- opozorili_e tehnično ekipo, če pride do okužbe na njihovem računalniku in sprejeli_e ustrezne ukrepe za reševanje težave,
- kadar je potrebna nova namestitev programske opreme, se obvezno posvetujejo z odgovornimi znotraj nevladne organizacije in z zunanjim izvajalcem_ko.

Upravljanje z gesli

Gesla so ključnega pomena za zaščito elektronskih poštnih računov nevladne organizacije, osebnih elektronskih poštnih računov in podatkov. Zato se v tretjem delu protokola nevladna organizacija in zaposleni_e/člani_ce dogovorijo k zavezi k različnim praksam, navedenim v nadaljevanju.

Nevladna organizacija:

- podpira zaposlene pri uporabi lastnega sistema za shranjevanje/upravljanje gesel (npr. Keepass) in omogoča usposabljanje,
- zagotavlja dostop do organizacijskega sistema za shranjevanje/upravljanje gesel za varni dostop do gesel, povezanih z organizacijo,
- izvaja mehanizme za spreminjanje gesla, ki zagotavljajo, da zaposleni_e enkrat na leto spreminjajo svoje uporabniško geslo (geslo naj bo kompleksno).

Zaposleni_e/člani_ce:

- nikoli ne shranjujejo: a) nešifriranih gesel v računalnike ali jih delijo prek odprtih komunikacijskih kanalov, kot sta e-pošta in Skype; b) gesel v brskalnik (Safari, Chrome, Firefox itd.);
- spremenijo gesla: a) če uporabljajo tuj računalnik, b) po uporabi odprtega brezžičnega dostopa do internet;
- uporabljajo edinstvena, kompleksna gesla in upravljalce gesel za vse e-račune nevladne organizacije,
- shranjujejo svojo bazo gesel v uporabniško mapo,
- na svojih računalnikih nastavijo zaklepanje zaslona, ki se zaklene vsaj po petih minutah neaktivnosti,
- zaklepajo računalniški zaslon, če niso fizično pri računalniku,

- nastavijo PIN-kode ali prstni odtis na telefonih, ki se uporabljajo za delovno komunikacijo,
- enkrat na leto spreminjajo gesla s primerno močnim geslom,
- obvestijo odgovorne v nevladni organizaciji, če sumijo, da je katero od njihovih gesel ogroženo, in kadar ga zamenjajo (če je tako dogovorjeno).

Ravnanje s podatki

Četrti del protokola obravnava zlasti varovanje občutljivih službenih podatkov; da se z njimi ravna na pravilen, namenski in varen način. Poglavje vsebuje prakse pridobivanja podatkov, kako ravnati v primeru občutljivih informacij, kakšno je pravilno (in odvečno) shranjevanje podatkov ter kako ravnati v primeru morebitnega uničenja teh podatkov.

ZBIRANJE OBČUTLJIVIH PODATKOV ZAPOSLENIH ZA NOTRANJO UPORABO

Razdelek se nanaša na primere, ko nevladna organizacija zbira potencialno občutljive podatke zaposlenih/zunanjih sodelavcev_k/sodelujočih na posameznih projektih/članov_ic. Občutljivi podatki vsebujejo osebne podatke, do katerih lahko dostopajo le pooblaščene osebe. Če se občutljivi podatki izgubijo ali uporabijo drugače, kot je bilo predvideno, lahko to povzroči resno škodo ljudem ali organizaciji, ki ji ti podatki pripadajo.

Konkretni primeri občutljivih podatkov so:

- osebni podatki – naslovi zaposlenih in zunanjih sodelavcev_k, njihove telefonske številke, elektronski naslovi, osebne identifikacijske številke;
- finančne informacije – številke bančnih računov, številke kreditnih kartic in podobne informacije;

- administrativne informacije – evidenca zaposlenih; elektronski dokumenti, kot so e-poštna sporočila, poročila, beležke, pisma in druge elektronske datoteke z dokumenti, ki vsebujejo zaupne podatke; pravni dokumenti in pogodbe;
- podatki o računih – ID-ji uporabnikov_ic, gesla in PIN-številke službenih ali zasebnih računov;
- lastniški in/ali avtorsko zaščiteni podatki, kot so raziskovalni podatki in publikacije.

Nevladna organizacija mora poskrbeti, da obstaja jasna in pregledna komunikacija o tem, kateri podatki se zbirajo in kje se podatki uporabljajo. Zbirajo se izključno informacije, ki temeljijo na privolitvi v zbiranje. Organizacija mora uporabljati varen komunikacijski kanal za zbiranje teh informacij (prek varnih/in če je treba – prek šifriranih spletnih obrazcev). Podatki o stikih so shranjeni v varni bazi podatkov, dostop do teh informacij mora biti omejen.

KOMUNICIRANJE OBČUTLJIVIH PODATKOV

Komuniciranje datotek in drugih informacij lahko poteka prek e-pošte, osebno ali prek druge nesočasne komunikacije (npr. SMS, pisma).

Nevladna organizacija se v protokolu zaveže, da:

- omogoči zaposlenim šifriranje e-sporočil za namen njihove notranje komunikacije (kadar je treba),
- namesti in zagotovi zaposlenim storitve takojšnjega sporočanja, glasovnih in video klicev, glasovnih sporočil, skupne rabe namizja, video konference itd.,
- pripravi vse potrebno za varen prenos in deljenje občutljivih informacij/podatkov z drugimi zunanjimi pooblaščenimi osebami.

VARNOSTNE KOPIJE OBČUTLJIVIH IN/ALI SLUŽBENIH PODATKOV

Pomemben vidik upravljanja informacij je zagotavljanje shranjevanja pomembnih podatkov s pomočjo varnostnih kopij. Podatki se lahko shranijo na notranjem, službenem strežniku, prav tako pa jih lahko varnostno kopirate v zaupanja vreden 'oblak' in na zunanje trde diske, nameščene na lokaciji zunaj pisarne.

Nevladna organizacija se zaveže, da poskrbi za:

- vsakodnevno varnostno kopiranje službenih podatkov, vključno z bazami podatkov o upravljanju gesla na posebnem namenskem disku,
- da so strežniki, na katerem se nahajajo varnostne kopije, fizično zaščiteni (pred krajo, ognjem, drugimi elementi), pa tudi elektronsko,
- varno shranjevanje kopij pomembnih fizičnih dokumentov,
- omogoči zaposlenim razpoložljive vire za varnostno kopiranje podatkov na zunanje pogone.

OBNOVITEV IZGUBLJENIH PODATKOV

Nevladna organizacija se zavezuje, da:

- se pravočasno odzove na zahteve zaposlenih za obnovitev podatkov,
- (če je možno) zaposlenim zagotovi sredstva za povrnitev (lastnih) izgubljenih nosilcev podatkov.

UNIČENJE OBČUTLJIVIH PODATKOV

Ta razdelek obravnava pravilno odstranjevanje podatkov na podlagi določitve organizacije, kdaj podatkov ni več treba shranjevati. Na primer, ko se zbira občutljive podatke v okviru raziskovalnega projekta, je treba jasno določiti, kdaj naj se podatki uničijo.

Nevladna organizacija se zavezuje, da:

- uniči trde kopije občutljivih podatkov, preden se jih odvrže stran,
- zagotavlja potrebna sredstva za odstranjevanje fizičnih in elektronskih dokumentov,
- pravilno uniči podatke, shranjene na trdih diskih, preden se jih pošlje v popravilo ali jih odvrže stran,
- opozori zaposlene enkrat letno, da izbrišejo nepotrebne podatke in očistijo prazen prostor na svojih trdih diskih,
- omogoči varno odstranjevanje uničenih fizičnih podatkov.

Zaposleni_e se zavežejo, da:

- počistijo računalniške trde diske enkrat na tri mesece (vključno z brisanjem spletne zgodovine, zgodovine Skypa, dnevnikov klepeta in nepotrebnih informacij),
- ko se ob pričetku projekta prične zbirati podatke in občutljive informacije, se določi datum poteka veljavnosti,
- letno čistijo nepotrebne podatke, čemur sledi čiščenje prostega prostora na trdih diskih.

Upravljanje sistemov e-pošte in drugih komunikacij

V petem poglavju protokola so zajeti različni komunikacijski kanali, ki jih uporablja nevladna organizacija, vključno z e-pošto, e-sporočili in notranjimi komunikacijskimi sistemi zaposlenih.

SPLOŠNA E-POŠTA

Nevladna organizacija se zaveže, da:

- zaposlenim zagotovi službeni račun za e-pošto,
- omogoča shranjevanje e-poštnih sporočil na strežniku, ki je varen in zanesljiv,
- zaposlenim omogoči upravljanje gesel za e-pošto v skladu s protokolom in jim tudi nudi pomoč pri upravljanju z gesli,
- zagotavlja varne kanale za e-pošto (implementacija SSL/TLS in/ali https v spletni pošti).

Zaposleni_e/člani_ce se zavežejo, da:

- nikoli ne odpirajo prilog iz nezaupljivih virov ali v sumljivih okoliščinah,
- nikoli ne posredujejo e-sporočil, ki vključujejo osebne podatke, razen če je to nujno – v tem primeru je zagotovljen varen prenos (šifrirana vsebina po šifriranih kanalih),
- vedno določijo, kdaj se e-sporočilo NE posreduje,
- ne pošiljajo občutljivih informacij po e-pošti, razen če sta vsebina in kanal zaščitena,
- službene e-račune uporabljajo samo za službeno komunikacijo,
- spoštujejo prakse za spreminjanje gesel,
- varujejo šifrirne ključe delovne e-pošte,
- kadar je treba, uporabljajo šifriranje pri komunikaciji z drugim osebjem, kadar poteka: izmenjava finančnih dokumentov, občutljivih informacij in/ali osebnih podatkov.

INTERNA KOMUNIKACIJSKA PLATFORMA (MED ZAPOSLENIMI)

Organizacija uporablja različna interaktivna orodja za medosebno komunikacijo, ki vsebujejo medsebojna sporočanja, zasebne skupine, neposredna sporočila in skupinske klepete, organizirane po temah.

Nevladna organizacija se zaveže, da:

- ustvari uporabniške račune za novo zaposlene in jim omogoči, da se pridružijo ustreznim skupinam,
- ukine uporabniški račun, ko zaposleni zapusti organizacijo.

Zaposleni_e/člani_ce se zavežejo, da:

- upoštevajo poimenovanje pogovornih delovnih skupin, kanalov,
- vedno izberejo nastavitev, ki omogoča dodajanje v pogovorne skupine s povabilom in da imena članov skupine niso vidna javno,
- nikoli ne pošiljajo finančnih, občutljivih ali osebnih podatkov prek interaktivnega orodja za medsebojno komunikacijo.

NOVIČNIK

Novičniki se pošiljajo naročnikom_cam iz spletnega sistema za upravljanje e-pošte. Naročniki_ce so del širše javnosti, ki s prijavo dovolijo, da novičnik prejmejo s spletnega mesta nevladne organizacije. Organizacija se zavezuje, da s podatki naročnikov_ic upravlja v skladu z določili Politike o varstvu podatkov – GDPR.

KAMPANJE

Udeležence_ke kampanj se na spletnem mestu organizacije vpraša (prijavi se), ali želijo biti na posebnem seznamu oglaševalskih akcij, na katerega pošiljamo podatke o kampanji. Nevladna organizacija se zavezuje, da s podatki naročnikov_ic upravlja v skladu z določili Politike o varstvu podatkov – GDPR.

Telekomunikacije in upravljanje z brezžično povezavo (WI-FI)

Šesto poglavje protokola obravnava postopek komunikacije in dostopa do podatkov/informacij v naslednjih primerih:

- delo od doma ali v okviru posebnega delovnega dogovora,
- uporaba osebnih mobilnih naprav, kot so telefoni, prenosni računalniki, tablični računalniki itd. zunaj pisarne,
- na poti in v tujini med službenimi potovanji,
- uporaba brezžične povezave (Wi-Fi), ki jo zagotavlja organizacija v pisarni.

Nevladna organizacija se zaveže, da:

- zaposlenim mogoči zmogljivo navidezno zasebno omrežje (VPN),
- omogoči ločeno uporabo internetne povezave za zaposlene in za goste_je, ki je zaščitena z geslom,
- omogoči ločeno uporabo brezžične povezave za zaposlene in za goste_je, ki je zaščitena z geslom,
- zagotavlja brezžično omrežje v pisarni, ki je zaščiteno z geslom in uporabo zaščitenega dostopa Wi-Fi II (WPA2) ali močnejšega šifriranja, ki ščiti organizacijsko omrežje pred nepooblaščenim dostopom zunanjih uporabnikov_ic,

- enkrat letno spremeni geslo za Wi-Fi račun oz. če je bilo več gostovanj v določenem obdobju.

Zaposleni_e se zavežejo, da:

- pri uporabi nezaščitene odprte dostopne točke Wi-Fi vedno uporabljajo VPN-povezavo in zamenjajo geslo, če pri tem uporabljajo neznan računalnik,
- so seznanjeni z namestitvijo in uporabo programske opreme VPN za oddaljeni dostop na svojih prenosnikih, pametnih telefonih itd.,
- zapirajo vse omrežne datoteke in končane seje VPN takoj, ko za dostop do pisarniških strežnikov ni več potrebe.

Postopek pri zaposlitvi in prenehanju delovnega razmerja

Zadnje, sedmo poglavje protokola obravnava postopke, ko se zaposleni_e, člani_ce, prostovoljci_ke, pripravniki_ce in svetovalci_ke pridružijo organizaciji ali jo zapustijo.

Ko se oseba pridruži nevladni organizaciji, se organizacija zaveže, da:

- zagotovi, da novi zaposleni_a /član_ica razume postopke, smernice in pričakovanja, potrebna za skladnost upravljanja s celovitostjo informacij in varnostno politiko,
- zagotovi vse potrebne ključe, kode za dostop do pisarne in drugo opremo, ki jo zahteva vloga zaposlenega_e,
- zagotovi zaposlenemu_i/članu_ci uporabniški račun, vključno z dostopom do različnih podatkovnih map glede na njegovo/njeno vlogo.

Odhajajoči uslužbenec_ka bo:

- vrnil_a pisarniško opremo, vse ključe ali druga orodja za fizični dostop do stavbe,
- skupaj z vodstvom nevladne organizacije določil_a, katere informacije, vezane na njegovo/njeno preteklo delo, se lahko ali ne smejo posredovati v prihodnje,
- podpisal_a, ali se strinja oz. ne strinja, da se njegov/njen e-naslov uporablja v prehodnem obdobju (npr. preusmeritev pošte).

Ko uslužbenec_ka zapusti nevladno organizacijo, bo organizacija:

- na datum odhoda onemogočila dostop do omrežnih strežnikov/e-poštnih/socialnih spletnih računov,
- spremenila gesla in/ali kode za dostop do te osebe,
- dan po odhodu te osebe spremenila kodo za varnostni alarm pisarne,
- na račun e-pošte bo nastavila samodejen odgovor z napovedjo o odhodu,
- obdržala uporabniške račune (npr. e-pošto) za obdobje enega meseca in jih preposlala ustreznim osebam,
- po enem mesecu odstrani in/ali izbriše račun

DODATEK: Informacijski dokument in priporočila za zaposlene/člane_ice

Za večje nevladne organizacije, ki imajo več zaposlenih, je priporočljivo, da informacijski dokument ne vključijo v začetku protokola, temveč podrobno popišejo stanje ter ga v protokol vključijo kot dodatek. V informacijskem dokumentu naj bo jasno določeno in opisano:

- seznam fizičnih krajev (lokacij), kjer se nahajajo naprave, vključno z zajetjem vseh oblik podatkov in kdo ima dostop do njih,
- če je treba, doda skico pisarniških in drugih prostorov, kjer so označene delovne enote, mrežni disk in strežnik (če ga posedujejo),
- kdo so ponudniki storitev (npr. s katerim zunanjim izvajalcem za IT-storitve imajo podpisano pogodbo in kaj zajema njegovo/njeno delo) in odgovorne osebe za vsako lokacijo, kjer je mogoče najti podatke,
- struktura datotečnih sistemov na datotečnem strežniku (lahko se priloži sliko),
- seznam zunanjih vlog, uporabnikov_ic in dovoljenj, ki se nanašajo na sistem za upravljanje vsebin na spletnem mestu organizacije,
- navedba, ali je prostor nevladne organizacije opremljen z varnostnim alarmnim sistemom (vključno s protipožarnim alarmom) oz. ali ima organizacija pogodbo z zunanjim varnostnim podjetjem,
- programska zaščita.

Nevladna organizacija lahko pripravi za svoje zaposlene ali člane_ice spisek uporabnih programov in aplikacij za digitalno zaščito za:

- večjo kontrolo nad podatki,
- zaščito prenosnikov in varnostne kopije,
- zaščito pametnih telefonov in varnostne kopije,
- upravljalce gesel,
- kriptiranje/šifriranje,
- varno takojšnje sporočanje, glasovne in video klice, glasovna sporočila, video konference ...

Uporabni programi in aplikacije za digitalno zaščito:

Dejavnost	Predlogi
Večja kontrola nad podatki in komu dovolite, da vas opazuje	• Varen brskalnik: Brave Preverjanje, ali je brskalnik zaščiten pred sledenjem: https://panopticlick.eff.org/ • Zaščiten brskalnik s https everywhere: https://www.eff.org/https-everywhere/ • Preprečitev sledenja: Privacy Badger https://www.eff.org/nl/node/99095 • Adblocker (preprečitev reklamnih oglasov): Ublock Origin: Mozilla https://addons.mozilla.org/nl/firefox/addon/ublock-origin/ Chrome: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en • VPN: https://nordvpn.com/nl/
Zaščita prenosnikov in varnostne kopije	• zaklepanje zaslona • ne uporabljajte avtomatskega logiranja (log-in) • kodiran pogon zaščiten z geslom (po potrebi obvesti nadrejene) • nujni protokol ukrepanja • Windows 10 možnost oddaljenega brisanja podatkov: https://www.maketecheasier.com/remote-wipe-windows-pc/ *Za Windows lahko uporabite Bitlocker (Mac uporablja FireVault)
Zaščita pametnih telefonov in varnostne kopije	Aplikacije: • Phone finder: natančno določi lokacijo telefona na zemljevidu • Remote lock: spletna nadzorna plošča, ki uporabnikom omogoča daljinsko zaklepanje telefona • Remote yell: sproži glasen zvok, ki uporabnikom pomaga najti izgubljen telefon ali prestrašiti in prepoznati tatove • Owner prompt: prikaže obvestilo osebi, ki najde telefon, kar olajša stik z lastnikom • Brisanje podatkov: ponastavi na tovarniške nastavitve telefona na daljavo. Programi: Avira: https://www.avira.com/en/free-antivirus-android älska sanningen Avast: https://www.avast.com/free-mobile-security (nekatere opcije so možne samo pri »premium version«, vendar sta brisanje podatkov in iskalec telefona del brezplačne različice) Priporočljivo je, da telefonska gesla zaupajte še nekomu (v primeru nesreče, smrti)

Dejavnost	Predlogi
Upravljalci gesel	• 1password: https://1password.com/ (omogoča popust za neprofitne organizacije) • KeePass: https://keepassxc.org/ > open source & brezplačen, vendar ni preprost za uporabo • LastPass: https://www.lastpass.com/ > uporabljajo mnoge organizacije
Kriptiranje/šifriranje	• Messenger: Signal: https://signal.org/ ali kot aplikacija v Trgovini aplikacij • Mail: Protonmail: https://protonmail.com/ • Tutanota: https://tutanota.com/ • Nujni odziv: https://digitalfirstaid.org/ Seveda lahko še vedno kaj gre narobe. Ta spletni vodič vam pomaga narediti prave korake, da razumete, kaj je narobe, in vas usmeri k pravi podporni organizaciji.
Varno takojšnje sporočanje, glasovni in video klici, glasovna sporočila, skupna raba namizja, video konference ...	• Jitsy: https://www.jitsy.com Večina uporabnikov uporablja aplikacijo Zoom. V preteklosti so se porajala vprašanja o varnosti zasebnosti, vendar so jih odpravili.
Drugo	• Facebook demetricator: dodatek brskalnika, ki skrije metriko na Facebooku: https://bengrosser.com/projects/facebook-demetricator/ • Anti-Surveillance Camouflage for Your Face: https://www.theatlantic.com/technology/archive/2014/07/makeup/374929/

Zaključek

Dandanes skorajda ni nevladne organizacije, ki ne bi poskrbela vsaj za minimalno varnost svojega spletnega mesta in deljenih vsebin. Številni koraki, opisani v priročniku, so že zajeti v vsakodnevnem delu zaposlenih/članov_ic, redko pa nevladna organizacija vpelje ustrezne protokole pri uporabi digitalnih orodij in komunikacij (zlasti pri obravnavi občutljivih vsebin), pa tudi šifriranih kanalov za komunikacijo znotraj organizacije, v komunikaciji s projektnimi partnerji_cami in z različnimi javnostmi. Ravno tako nevladne organizacije pogosto zanemarijo protokole o šifriranju naprav, varnosti gesel ter shranjevanju in izmenjavi občutljivih podatkov. Problem nastane, če se na primer del podatkov izgubi ali uniči. Običajno se takrat na hitro skuša rešiti dano situacijo in šele nato pomisli, kaj bi lahko storili v naprej, da do situacije sploh ne bi prišlo. S pričujočim priročnikom tako zajemamo priporočila, kako razviti enostaven sistem za izvajanje digitalnih varnostnih ukrepov s katerimi zaposlene/člane_ice v nevladnih organizacijah zavežemo k spoštovanju in sledenju dogovorjenega protokola, hkrati pa se znotraj nevladne organizacije vzpostavi pregled nad celotnim stanjem. V korporativnem svetu je posedovanje podatkov ena od najvrednejših dobrin in čas je, da se tega zavemo tudi znotraj nevladnega sektorja.

Prvi osnutek delovnega lista/predloge dokumenta sta pripravila Alix Dunn in Mallory Knodel (Engine Room in APC), naknadno pa je dokument uredil in vnesel določene spremembe Ali Ravi (confabium). Za namen tega priročnika je besedilo priredila in prilagodila vsebino Jasna Babić.