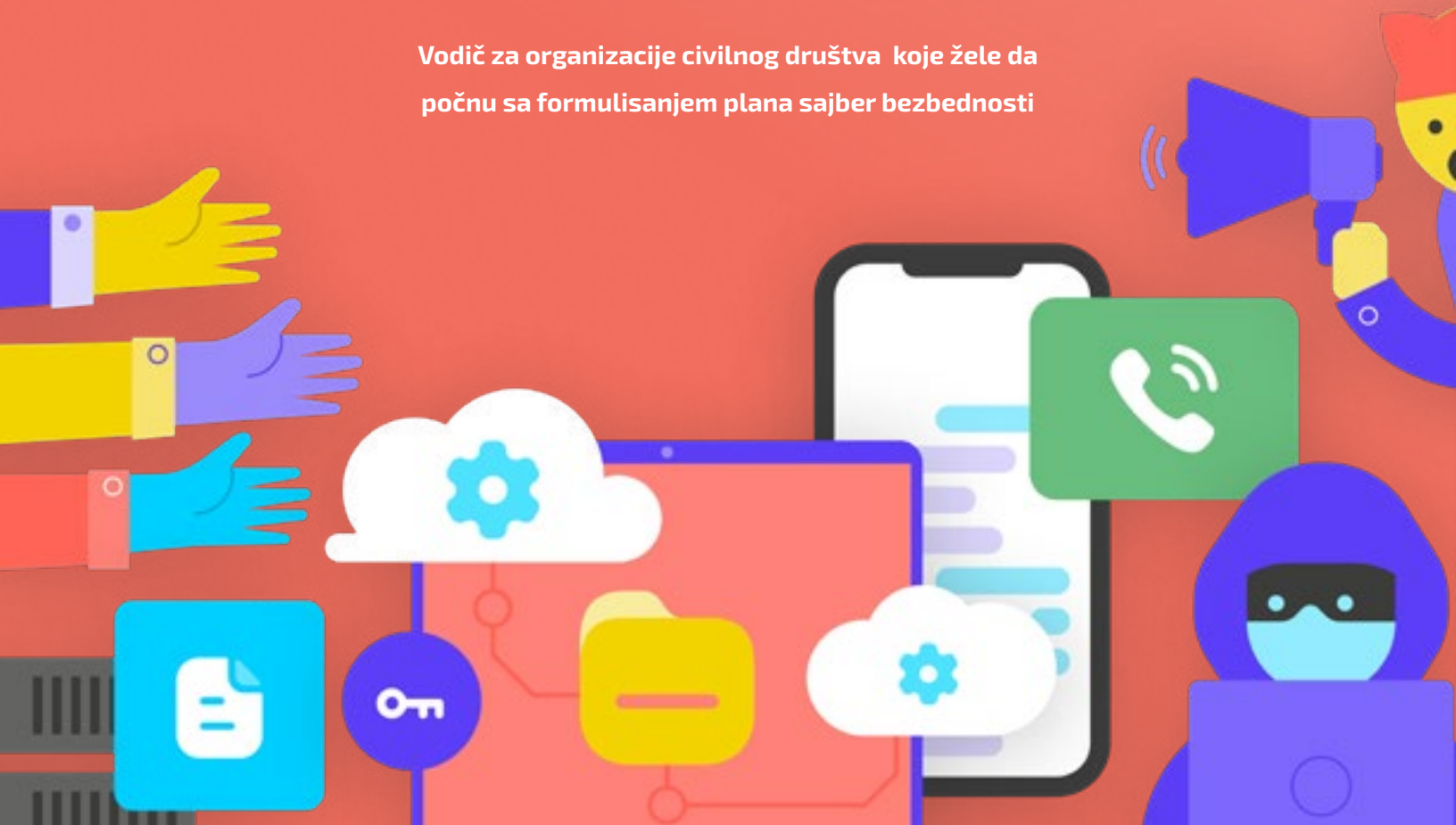
NDI
NATIONAL DEMOCRATIC INSTITUTE

Vodič o sajber bezbednosti

za

Organizacije civilnog društva

Vodič za organizacije civilnog društva koje žele da počnu sa formulisanjem plana sajber bezbednosti



Vodič o sajber bezbednosti

za

Organizacije civilnog društva

Vodič za organizacije civilnog društva koje žele da počnu sa formulisanjem plana sajber bezbednosti

Sadržaj

Vizuelna legenda

Tokom čitanja ovog priručnika primetićete nekoliko različitih naglašenih elemenata koji se ponavljaju pored glavnog teksta. Prilažemo kratku „legendu“ kako bismo vam pomogli da razumete osnovne elemente:

Studija slučaja

Ukazuje na studije slučaja koje naglašavaju realni efekat određene teme na organizacije civilnog društva vna globalnom nivou ili nivou određene države.

Dodatni saveti

Naglašava neke dodatne savete i informacije na koje treba da obratite pažnju tokom čitanja priručnika.

Stvarnost

Ukazuje na uobičajene primere taktičkih instrumenata za sajber bezbednost koje se koriste u „stvarnom svetu“, kako u dobre, tako i u loše svrhe.

Napredno

Ukazuje na naprednu važnu temu - informaciju koju vaša organizacija treba da uzme u obzir, ali koja može biti malo više tehnička ili složenija.

Osnovne Elemente Bezbednosnog Plana

Ukazuje na „osnovne elemente bezbednosnog plana“, to jest ključne informacije koje treba zapamtiti u svakom odeljku priručnika.

1

Izgradnja kulture bezbednosti

2

Jake osnove: Obezbeđivanjenaloga i uređaja

3

Bezvbedno prenošenje i skladištenje podataka

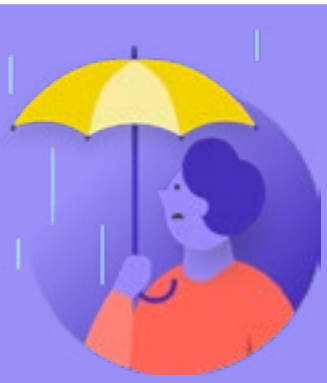
4

Bezbednost na internetu

5

Zaštita fizičke bezbednosti

6



Šta da radite kad stvari krenu po zlu

Deset najbitnijih stavki

1. Sprovodite redovnu obuku iz oblasti bezbednosti u okviru vaše organizacije
2. Budite svesni opasnosti od fišinga „pecanja“ (phishing) i uspostavite sistem izveštavanja
3. Korisite enkripciju za sve vaše komunikacije - obostranu, kad god je to moguće
4. Insistirajte na jakim lozinkama i uvedite program za upravljanje lozinkama (Password Manager) na nivou cele organizacije
5. Zahtevajte dvostruku potvrdu identiteta kad god je to moguće
6. Postarajte se da su svi uređaji i softver koji osoblje koristi ažuriraju
7. Koristite bezbedno skladištenje na klaudu
8. Koristite HTTPS i, ako je to potrebno, VPN za pristup internetu
9. Zaštitite fizičku imovinu svoje organizacije
10. Kreirajte organizacioni plan koraka u slučaju incidenta

Autori i zahvalnice

Glavni autor: **Ivan Samers (NDI)**
Dodatni autori: **Sara Molton (NDI); Kris Doten (NDI)**

Posebnu zahvalnost za pomoć u procesu pisanja ovog priručnika dugujemo našim stručnim eksternim recenzentima koji su nam pružili vredne povratne informacije, redakturu i sugestije dok smo sastavljali ovaj sadržaj, a u njih između ostalih spadaju:

Fiona Krakenburger, Open Technology Fund; Bil Badington i Šajrin Mori, Electronic Frontier Foundation; Džoslin Vulbrajt, Cloudflare; Martin Šelton, Freedom of the Press Foundation; Dej Lajhtman, Microsoft; Stiven Bojs, International Foundation for Electoral Systems; Ejmi Stadart, International Republican Institute; Ema Holingsvort, Global Cyber Alliance; Kerolajn Sajnders, Convocation Design + Research; Dita Katurani; Sandra Pepera, NDI; Eron Azelton, NDI; i Vitni Fajfer, NDI.

Takođe bismo želeli da sa zahvalnošću pomenemo sve fantastične priručnike, vodiče, radne sveske, module obuke i druge materijale koje je kreirala i održava zajednica za organizacionu bezbednost (OrgSec). Ovaj priručnik je zamišljen kao dopuna tih detaljnihmaterijala koja kombinuje ključne pouke u okviru jednostavnog, lako razumljivog resursa za organizacije civilnog društva koje žele da se upuste u kreiranje plana sajber bezbednosti.

Pored toga što smo se indirektno inspirisali brojnim divnim resursima koje je zajednica prikupila, takođe smo direktno prekopirali korisnu terminologiju iz šačice postojećih resursa i koristili je u celom priručniku, naročito iz Vodiča za samodbranu od nadzora (Surveillance Self-Defence Guide) koji je kreirala **Electronic Frontier Foundation,** Holističkog bezbednosnog priručnika (Holistic Security Manual) **Tactical Tech**-a, kao i čitav niz objašenjenja koja su sastavili **Center for Democracy and Technology** i **Freedom of the Press Foundation**. Možete naći pojedinačne reference na te izvore u nastavku teksta, a sve linkove, kao i informacije o autorima i licencama u **Prilogu A**.

Takođe toplo preporučujemo svakom ko čita ovaj Priručnik da iskoristi opsežnu **biblioteku** vodiča i resursa za digitalnu bezbednost koje je prikupio i ažurira Fond za otvorenu tehnologiju.

Ko smo mi?

Nacionalni demokratski institut za međunarodne poslove (NDI) je neprofitna, nestranačka organizacija sa sedištem u Vašingtonu u SAD, koja sklapa partnerstva širom sveta u cilju osnaživanja i zaštite demokratskih institucija, procesa, normi i vrednosti, kako bi se obezbedio bolji život za sve. NDI veruje da svi ljudi imaju pravo da žive u svetu koji poštuje njihovo dostojanstvo, bezbednost i politička prava - a digitalni svet nije izuzetak.

U okviru NDI, Tim za demokratiju i tehnologiju radi na negovanju globalnog digitalnog ekositema u kojem se demokratske vrednosti štite, promovišu i mogu da procvetaju; u kojem su vlade transparentnije i inkluzivnije, a svi građani osnaženi da pozivaju vlade na odgovornost za njihove postupke. Ovo postižemo pružanjem podrške globalnoj mreži aktivista koji su posvećeni digitalnoj otpornosti i kroz saradnju sa partnerima na kreiranju instrumenta i resursa poput ovog Priručnika. Možete saznati nešto više o našem radu na našoj **internet stranici**, tako što ćete nas zapratiti na **Twitter-u**, ili nam pisati direktno na **cyberhandbook@ndi.org**. Uvek nam je zadovoljstvo da vas saslušamo i odgovorimo na pitanja o našem timu i radu iz oblasti sajber bezbednosti, tehnologije i demokratije.

Kome je ovaj priručnik namenjen?

Ovaj priručnik je napisan sa jednostavnim ciljem: da pomogne organizacijama civilnog društva da kreiraju razumljivi i primenjivi plan sajber bezbednosti.

Kako se svet sve više premešta na internet, sajber bezbednost nije samo pomodni termin već i koncept od kritičnog značaja za uspeh neke organizacije i bezbednost nekog tima. Naročito u slučaju organizacija civilnog društva aktivnih na polju demokratije, zastupanja, odgovornosti i ljudskih prava, bezbednost informacija (kako na internetu, tako i van njega) predstavlja izazov koji zahteva fokus, investicije i budnost.

Vaša organizacija će u nekom momentu - ako se to već nije desilo - biti na meti sajber napada. Ne pokušavamo da vas uplašimo, to je realna situacija čak i za organizacije koje sebe ne smatraju atraktivnim metama.

Tokom prosečne godine, Centar za strateška i međunarodna istraživanja, koji vodi ažurirani **spisak** onoga što zovu „Značajni sajber incidenti" beleži stotine ozbiljnih sajber napada, od kojih su mnogi usmereni na desetine ako ne i stotine organizacija odjednom. Pored takvih prijavljenih napada, verovatno postoje stotine manjih koji svake godine prođu nezapaženo ili neprijavljeno, a od kojih su mnogi usmereni protiv organizacija civilnog društva koje rade na promovisanju demokratije, odgovornosti države i ljudskih prava. Organizacije koje zastupaju žene ili druge marginalizovane grupe često su omiljena meta napada.

Sajber napadi poput ovih imaju dalekosežne posledice. Bilo da je njihov cilj da vam uzmu pare, ućutkaju vas, poremete funckionisanje vaše organizacije, ukaljaju vašu reputaciju ili čak ukradu informacije sa ciljem da psihički ili fizički naškode vašim partnerima ili osoblju, takve pretnje morate shvatiti ozbiljno.

Ono što je dobro jeste što ne morate da postanete programer ili tehnološki stručnjak kako biste odbranili sebe i organizaciju od uobičajenih pretnji. Ali morate da budete spremni da uložite malo napora, energije i vremena u formulisanje i sprovođenje izdržljivog organizacionog bezbednosnog plana.

Ako nikad niste razmišljali o sajber bezbednosti u okviru svoje organizacije, niste imali vremena da se time bavite ili znate neke osnovne stvari o toj temi ali mislite da bi vaša organizacija mogla da poboljša svoju sajber bezbednost, onda je ovaj priručnik za vas. Bez obzira na to odakle dolazite, ovaj priručnik za cilj ima da vašoj organizaciji pruži ključne informacije koje su joj potrebne za uspostavljanje izdržljivog plana sajber bezbednosti. Plana koji se neće svesti samo na reči na papiru i koji će vam omogućiti da primenite najbolju praksu.

Šta je bezbednosni plan i zašto bi ga moja organizacija trebalo da ima?

Bezbednosni plan predstavlja niz pisanih politika, postupaka i uputstava koje je vaša organizacija usvojila da bi postigla nivo bezbednosti koji vi i vaš tim smatrate adekvatnim kako bi osigurali bezbednost osoblja, partnera i informacija.

Dobro osmišljen i ažuriran bezbednosni plan vas istovremeno čini bezbednim i delotvornijim pružajući vam osećaj sigurnosti neophodan za fokusiranje na svakodnevne bitne poslove vaše organizacije. Bez promišljanja sveobuhvatnog plana lako je ostati slep na određene vrste pretnji, preterano se skoncentrisati na samo jedan rizik ili ignorisati sajber bezbednost dok ne dođe do krize.

Kad počnete da radite na bezbednosnom planu morate sebi postaviti neka važna pitanja kako biste započeli proces procene rizika. Pružanje odgovora na ova pitanja pomaže vašoj organizaciji da razume jedinstvene pretnje sa kojima se suočavate i dozvoljava vam da napravite odmak i sveobuhvatno promislite o tome šta vam je potrebno kako biste se zaštitili, kao i od koga to tačno treba da se zaštite. Obučeni procenitelji, uz pomoć sistema kao što je Internews **SAFETAG** revizijski okvir, mogu da pruže podršku vašoj organizaciji tokom ovog postupka. Ako možete da dobijete pristup tom nivou ekspertize, to vredi, ali čak i ako ne možete da prođete kroz punu procenu, trebalo bi da organizujete sastanke u okviru organizacije kako biste razmotrili ova ključna pitanja.

1 Kakvu imovinu vaša organizacija poseduje i šta želite da zaštitite?

Možete početi da odgovarate na ovo pitanje tako što ćete **evidentirati svu imovinu vaše organizacije.** Informacije poput poruka, mejlova, kontakata, dokumenata, kalendara i lokacija su sve vrste imovine. Telefoni, kompjuteri i drugi uređaji takođe mogu biti imovina. Kao i ljudi, veze i odnosi. Popišite svu **vašu imovinu** i pokušajte da razvrstate različite stavke na osnovu značaja koji imaju za vašu organizaciju, mesta gde ih držite (možda na više digitalnih i fizičkih lokacija) i onoga što druge sprečava da tim stavkama pristupe, oštete ih ili poremete. Imajte na umu da nije sve podjednako važno. Ukoliko su neki podaci javni, ili ih pak sami objavljujete, to nisu tajne koje morate da štitite.

2 Ko su vaši protivnici i kakve su nihove sposobnosti i motivacija?

„Protivnik" je termin koji se redovno koristi na polju bezbednosti organizacija. Jednostavno rečeno, protivnici su akteri (pojedinci ili grupe) koji su zainteresovani da se okome na vašu organizaciju, poremete vam rad i dobiju pristup vašim informacijama ili ih unište, tačnije -negativci. U potencijalne protivnike mogu da spadaju finansijski prevaranti, konkurenti, lokalni ili nacionalni organi vlasti ili vlade, ili ideološki ili politički motivisani hakeri. Važno je da napravite spisak svojih protivnika i kritički razmislite o tome ko bi potencijalno hteo da negativno utiče na vašu organizaciju i zaposlene. Dok je lako zamišljati eksterne faktore (poput stranih vlada ili određenih političkih grupa) kao protivnike, imajte na umu i da protivnici mogu biti ljudi koje poznajete, poput ozlojeđenih zaposlenih, bivšeg osoblja i članova porodice ili partnera koji ne podržavaju vaše ciljeve. Različiti protivnici predstavljaju različite pretnje i poseduju različite resurse i sposobnosti da poremete vaše aktivnosti i dobiju pristup vašim informacijama ili ih unište. Na primer, vlade često imaju puno novca i sposobnosti koje podrazumevaju mogućnost isključivanja interneta ili upotrebe skupe tehnologije za nadzor, pružaoci mobilnih i internet usluga verovatno imaju pristup istorijatu poziva i sajtova koje ste posetili na internetu, vešti hakeri na javnim wifi mrežama mogu da presretnu loše obezbeđene komunikacije ili finansijske transakcije. Možete čak postati i sami sebi protivnik tako što, na primer, slučajno obrišete važne fajlove ili pošaljete privatnu poruku pogrešnoj osobi.

Motivi protivnika će se verovatno razlikovati u zavisnosti od njihovih kapaciteta, interesa i strategija. Da li žele da diskredituju vašu organizaciju? Možda žele da vas utišaju kako ne biste preneli vašu poruku? Ili vas možda vide kao konkurenciju i žele da steknu prednost? Važno je da razumete motivaciju vašeg protivnika pošto tako možete svojoj organizaciji pomoći da bolje procenite kakvu pretnju može da predstavlja.

3 Sa kakvim pretnjama se vaša organizacija suočava? Koliko su te pretnje izvesne i koliko veliki efekat bi mogle da imaju?

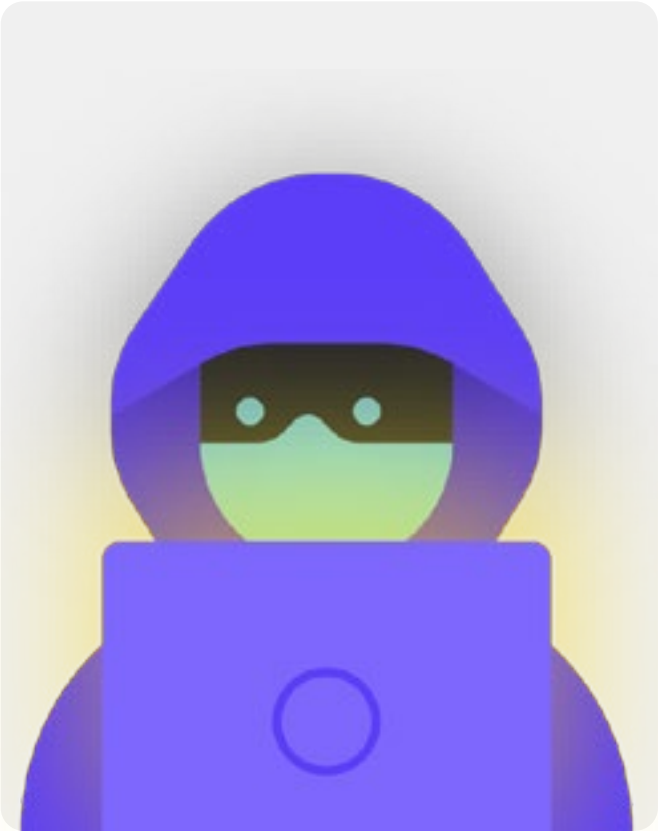
Dok budete identifikovali pretnje, verovatno ćete na kraju imati dugački spisak koji može biti zastrašujući. Može vam se učiniti da će bilo kakvi napori biti besmisleni ili možda nećete znati ni odakle da počnete. Kako biste osnažili vašu organizaciju da preduzme produktivne sledeće korake, korisno je da analizirate svaku pretnju na osnovu dva faktora; verovatnoće da će se pretnja ostvariti i njenog efekta.

Kako biste procenili verovatnoću pretnje (možda na skali „niska, srednja ili visoka“ u zavisnosti od toga da li je malo verovatno da će se nešto desiti, da li bi moglo da se desi ili se često dešava) možete koristiti poznate informacije o kapacitetima i motivaciji vaših protivnika, analizu bezbednosnih incidenata u prošlosti, druga slična iskustva na nivou organizacije i, naravno, postojanje bilo kakvih strategija za ublažavanje efekata ovakvih incidenata koje je vaša organizacija formulisala.

Kako biste izmerili efekat pretnje, razmislite kako bi vaš svet izgledao kad bi se određena pretnja zaista ostvarila. Postavite si pitanja kao što su: „Kako je ova pretnja naškodila organizaciji i nama kao ljudima, fizički i psihički?“, „Koliko je dugotrajan ovaj efekat?“, „Da li ovo dovodi do drugih rizičnih situacija?“ i „Kako ovo podriva našu sposobnost da postignemo organizacione ciljeve sad i u budućnosti?” Dok odgovarate na ova pitanja, razmotrite da li je pretnja niska, srednja ili visoka.

Jednom kad ste pretnje poređali po verovatnoći i efektu možete početi da pravite plan akcije zasnovan na tim informacijama. Fokusiranjem na pretnje koje će se najverovatnije ostvariti KAO I imati najnegativnije efekte, upotrebićete svoje ograničene resurse na najdelotvorniji i najefikasniji mogući način. Vaš cilj je da što je više moguće ublažite rizik, ali niko - čak ni najbolje opremljena vlada ili kompanija na svetu - ne može nikada da u potpunosti eliminiše rizik. I to je u redu - možete učiniti mnogo toga da zaštite sebe, svoje kolege i organizaciju tako što ćete se pobrinuti za najveće pretnje.

Kako biste lakše primenili ovaj postupak procene rizika, razmotrite da koristite tabelarni prikaz, poput ovog koji je kreirala Electronic Frontier Foundation. Imajte na umu da informacije koje generišete tokom ovog procesa (poput spiska svojih protivnika i pretnji koje oni predstavljaju) mogu i same bite poverljive. Tako da je bitno da ih obezbedite.



Kreiranje plana za sajber bezbednost na nivou vaše organizacije

Dok će bezbednosni plan svake organizacije izgledati malo drugačije u zavisnosti od procene rizika i organizacione dinamike, određeni ključni koncepti su skoro univerzalni.

Ovaj priručnik se bavi tim suštinskim konceptima na način koji će vašoj organizaciji pomoći da formuliše konkretni bezbednosni plan zasnovan na praktičnim rešenjima koja su primenjiva u stvarnom svetu.

Ovaj priručnik se trudi da obezbedi opcije ili sugestije koje su besplatne ili veoma ekonomične. Ali imajte na umu da je najveći trošak kod primene delotvornog bezbednosnog plana povezan sa vremenom koje vi i vaša organizacija morate uložiti u diskusiju, učenje i sprovođenje plana. Međutim, ako imamo u vidu rizike sa kojima će se vaša organizacija verovatno suočiti, ova investicija će se višestruko isplatiti.

U svakom odeljku ćete naći objašnjenje ključne teme koje vaša organizacija i njeno osoblje treba da budu svesni i da razumeju šta je i zašto je bitna. Uz svaku temu su priložene ključne strategije, pristupi i preporučeni instrumenti za smanjenje rizika, kao i praktični saveti i linkovi ka dodatnim resursima koji vam mogu pomoći da primenite takve preporuke u okviru vaše organizacije.

Osnovni

Kako bi vaša organizacija lakše usvojila lekcije iz priručnika i prevela ih u pravi plan, možete iskoristiti ovaj osnovni set. Možete ga odštampati ili digitalno popuniti dok čitate priručnik preko interneta. Dok budete hvatali beleške i počeli sa ažuriranjem ili kreiranjem svog bezbednosnog plana, obavezno pogledajte „osnovne elemente bezbednosnog plana“ koje su date u svakom odeljku. Nijedan bezbednosni plan nije potpun ako ne pozabavite bar ovim osnovnim elementima.

TIskoristite i druge resurse koji vam mogu pomoći [illegible]ni vašeg plana. Kao organizaciji civilnog društva besplatna SOAP („obezbeđivanje organizacija uz pomoć automatskog kreiranja politika“) aplikacija vam može pomoći da pojednostavite i automatizujete formulisanje svog bezbednosnog plana.

Iskoristite i besplatne resurse za obuku kao što su Security Planner (Bezbednosni planer) organizacije Consumers Report, Umbrella aplikaciju firme Security First, Totem Project platformu koju su razvili Free Press Unlimited i Greenhost, i Cyber Hygiene for Mission-Based Organizations (Sajber higijena za organizacije zasnovane na misiji) Globalne sajber alijanse koje obuhvataju resurse relevantne za veliki broj najboljih praksi pomenutih u ovom priručniku i linkove ka desetinama instrumenata za obuku koji vam mogu pomoći da sprovedete najosnovnije stvari. links to dozens of training tools to help you implement many core basics.

Izgradnja kulture bezbednosti

Suština bezbednosti je u ljudima i da biste zaštitili svoju organizaciju morate da se postarate da svi ozbiljno shvataju sajber bezbednost. Teško je izmeniti kulturu, ali nekoliko jednostavnih koraka i bitnih razgovora može da značajno potpomogne kreiranje atmosfere koja će izgraditi otpornost vašeg osoblja i organizacije na bezbednosne pretnje. Jedan od najjednostavnijih ali najvažnijih koraka na polju izgradnje bezbednosne kulture neke organizacije je informisanje svih pripadnika te organizacije o ovoj kulturi u sklopu sa liderima koji daju primer svojim ponašanjem.

Integrišite bezbednost u vašu regularnu operativnu strukturu

Kao što je detaljno opisano u Holističkom vodiču za bezbednost kompanije Tactical Tech, od suštinskog je značaja da kreirate redovne, sigurne prostore za razgovor o različitim aspektima bezbednosti.

Tako, ukoliko članovi tima budu zabrinuti u vezi sa pitanjima bezbednosti, manje će se sekirati da li deluju paranoično ili troše tuđe vreme. **Zakazivanje redovnih razgovora o bezbednosti** takođe normalizuje učestalost interakcije i promišljanja pitanja bezbednosti kako se problemi ne bi zanemarivali i povećala verovantoća da će članovi tima biti bar pasivno svesni bezbednosti tokom svojih svakodnenvih aktivnosti. Nije neophodno da sastanke održavate svake sedmice, ali ih sazivajte u redovnim intervalima. Ove diskusije ne bi trebalo da se bave samo temama iz oblasti tehničke bezbednosti, već i pitanjima koja utiču na komfor i bezbednost osoblja kao što su sukobi u zajednici, uznemiravanje na internetu i van njega, ili problemi sa korišćenjem i primenom digitalnih alatki. Razgovori mogu da se dotaknu čak i tema kao što su navike vezane za deljenje informacija van interneta i načini na koji osoblje obezbeđuje ili ne obezbeđuje informacije van posla. Na kraju krajeva, najvažnije je da zapamtite da je bezbednost organizacije jaka samo koliko i njena najslabija karika. Jedan od načina da postignete konstantno angažovanje osoblja u vezi sa ovom temom je da bezbednost stavite na dnevni red redovnih sastanaka. Takođe možete odgovornost za organizovanje i vođenje diskusije o bezbednosti prebacivati sa jednog člana vaše organizaicje na drugog, što može pospešiti usvajanje ideje da su za bezbednost odgovorni svi, a ne samo odabrana šačica. Kako počnete da formalizujete diskusiju o bezbednosti, pripadnicima osoblja će verovatno biti prijatnije da diskutuju o ovim bitnim pitanjima između sebe i u neformalnom okruženju.

Takođe je bitno da elemente bezbednosti uvedete u normalno funkcionisanje organizacije, kao npr. tokom primanja novog osoblja - i da razmislite da uskratite pristup osoblju koje više ne radi za vas. Bezbednost ne bi trebalo da bude neka „dodatna stavka“ na agendi već pre integralni deo vaše ***strategije i rada.***

Zapamtite da sve bezbednosne planove treba da posmatrate kao žive dokumente, i da ih redovno reevaluirate i diskutujete o njima, naročito kad se novi zaposleni ili volonteri pridruže organizaciji ili kad dođe do promena u vašem bezbednosnom kontekstu. Planirajte da jednom godišnje ponovo razmotrite celu strategiju i ažurirate je, kao i da isto to učinite ako dođe do većih promena po pitanju strategije, instrumenata ili pretnji sa kojima se suočavate.

Postignite posvećenost na nivou organizacije

Deo uspešne bezbednosne kulture je i staranje da svi u organizaciji budu posvećeni vašem bezbednosnom planu.

Od kritičnog je značaja da to podrazumeva jaku, glasnu podršku i vođstvo rukovodstva organizacije koje će u brojnim sluačjevima upravo i biti ono koje donosi konačnu odluku o ulaganju vremena, resursa i energije u formulisanje i sprovođenje delotvornog bezbednosnog plana. Ako ga oni ne shvate ozbiljno, niko neće. Kako biste postigli ovakvu posvećenost u celoj organizaciji pažljivo razmislite o tome kada i kako da kolege upoznate sa planom i to učinite jasno, postarajte se da rukovodstvo naglašava poruku i prođite kroz sve elemente i korake plana tako da nema tajne ili konfuzije oko toga šta pokušavate da postignete. Mnogi donatori sada od onih kojima daju sredstva traže da održavaju jaku bezbednost, tako da ako to naglasite osoblju, i to može dovesti do veće posvećenosti. Kad pričate o bezbednosti izbegavajte da plašite ljude. Ponekad pretnje sa kojima se vaša organizacija i osoblje suočavaju mogu biti strašne, ali pokušajte da se fokusirate na predstavljanje činjenica i stvaranje mirnog okruženja za postavljanje pitanja i izražavanje zabrinutosti. Ukoliko opasnosti predstavite kao suviše zastrašujuće, ljudi to mogu otpisati kao senzacionalizam ili se pak prosto predati, verujući da ne mogu ništa da urade - a ništa ne može biti dalje od istine.

Formulišite plan obuke

Jednom kad ste kreirali plan i obezbedili posvećenost, razmislite o tome kako ćete obučiti celo osoblje (i volontere) o ovim novim praksama.

Organizovanje redovne obuke kojoj se mora prisustvovati i gde se pohađanje iste uzima u obzir prilikom ocene učinka osoblje može biti od pomoći. Izbegnite uvođenje strogih negativnih posledica po osoblje koje ima problema da shvati koncepte bezbednosti. Imajte na umu da se određeni članovi osoblja mogu prilagoditi i učiti o tehnologiji na drugačiji način od drugih u zavisnosti od njihovog nivoa upoznatosti sa digitalnim alatkama i internetom. Strah od neuspeha samo dodatno koči osoblje da prijavi probleme i zatraži pomoć. Međutim, podsticanje pozitivne odgovornosti i nagrađivanje uspešnog prolaska obuke i usvajanja politika može da potpomogne unapređenje veština iz oblasti bezbednosti na nivou cele organizacije. Možete naći dragocenu dodatnu podršku u obliku lokalnih ili međunarodnih mreža za obuku iz oblasti digitalne bezbednosti i besplatnih resursa kao što su Umbrella aplikacija firme Security First, Totem Project platforma koju su razvili Free Press Unlimited i Greenhost, i Portal za učenje Globalne sajber alijanse.

Izgradnja kulture bezbednosti

- **Zakažite redovne sastanke i obuke o pitanjima bezbednosti i vašem bezbednosnom planu.**
- **Uključite sve - raspodelite odgovornost za sprovođenje bezbednosnog plana među svim pripadnicima vaše organizacije.**
- **Postarajte se da rukovodstvo daje primer dobrog ponašanja sa aspekta bezbednosti i posvećenosti planu.**
- **Izbegavajte zastrašivanje ili kažnjavanje - nagradite napredak i stvorite okruženje u kojem će osoblje osećati da mogu da prijave probleme i zatraže pomoć.**
- **Ažurirajte svoj bezbednosni plan na godišnjem nivou ili nakon većih organizacionih promena.**

Jake osnove: Obezbeđivanje naloga i uređaja

Zašto stavljamo akcenat na naloge i uređaje? Zato što oni čine osnovu svega što vaša organizacija radi u digitalnom domenu.

Skoro sigurno na njima pristupate osetljivim informacijama, komunicirate kako unutar organizacije tako i sa eksternim akterima i čuvate podatke. Ako oni nisu bezbedni onda će sve to i mnogo čega drugog biti dovedeno u opasnost.

Na primer, ako hakeri beleže koje tastere na tastaturi pritiskate ili vas prisluškuju preko vašeg mikrofona, vaši razgovori će biti snimljeni bez obzira na stepen bezbednosti vaših aplikacija za slanje poruka. Ili ako neki protivnik dobije pristup nalozima vaše organizacije na društvenim mrežama, to bi lako moglo da ima negativan uticaj na vašu reputaciju i kredibilitet i da podrije uspešnost vašeg rada. Zato je od suštinskog značaja za svaku organizaciju da se postara da svi preduzimaju jednostavne ali delotvorne korake za zaštitu svojih uređaja i naloga. Važno je napomenuti da se ove preporuke odnose i na lične naloge i uređaje, pošto su isti često laka meta za protivnike. Hakeri će se rado okomiti na najlakšu metu i uhakovati lični nalog ili kućni računar ukoliko ih vaš tim koristi za komunikaciju i pristup važnim informacijama.

Bezbedni nalozi i civilno društvo

Nadaleko poznati SolarWinds hakerski napad otkriven krajem 2020. godine koji je doveo u opasnost preko 250 organizacija, uključujući većinu ministarstava u SAD, prodavce tehnoloških rešenja poput Microsoft-a i Cisco-a, kao i NVO-e je delimično predstavljao rezultat toga što su hakeri pogodili slabe lozinke koje su korišćene na bitnim administratorskim nalozima. Sve u svemu, do oko 80% svih hakerskih upada dođe zbog loših ili više puta korišćenih lozinki.

Sa sve većim prisustvom ovakog provaljivanja lozniki i lakšim pristupom raznih vrsta protivnika sofisticiranim instrumentima za hakovanje lozinki, dvostruka potvrda ideniteta je obavezna sa tačke bezbednosti civilnih organizacija. Facebook je 2020. prijavio jedan primer napada na naloge organizacija civilnog društva. Po tom izveštaju, hakerske grupe u Bangladešu su napale naloge **lokalnih** aktivista civilnog društva, novinara i pripadnika verskih manjina. Nažalost, hakeri su uspeli da upadnu u neke od Facebook naloga, uključujući i onaj administratora stranice jedne lokalne grupe. Zahvaljujući pristupu administratorskom nalogu, hakeri su uklonili sve druge administratore, preuzeli i ugasili stranicu, te tako grupu sprečili da deli ključne informacije i komunicira sa svojom publikom. Istraga koju je Facebook sproveo je otkrila da su nalozi verovatno bili provaljeni na različite načine, uključujući i pomoću zloupotrebe procesa povraćaja naloga. Da su svi nalozi koristili dvostruku potvrdu identiteta hakerima bi bilo mnogo teže da uspešno izvedu te napade

Bezbedni nalozi: Lozinke i dvostruka potvrda identifikacije

U današnjem svetu vaša organizacija i njeno osoblje verovatno imaju desetine, ako ne i stotine naloga koji bi, ukoliko neko u njih upadne, mogli da otkriju osetljive informacije ili čak dovedu u opasnost neke pojedince.

Pomislite na sve moguće naloge koje pojedinci ili organizacija mogu imati: imejl, aplikacije za četovanje, društvene mreže, elektronsko bankarstvo, skladištenje podataka na klaudu... i prodavnice odeće, lokalne picerije, novine i bilo koji drugi sajt ili aplikacija na koju se prijavite. Solidna bezbednost u današnjem svetu zahteva temeljan pristup kako bi se svi nalozi zaštitili od napada. Za početak je potrebno uspostaviti dobru higijenu lozinki i upotrebu dvostruke potvrde identiteta na nivou cele organizacije.

ŠTA ČINI JEDNU LOZINKU DOBROM?

Postoje tri elementa dobre, jake lozinke: dužina, nasumičnost i jedinstvenost.

DUŽINA

Što je lozinka duža to je teže za protivnika da je pogodi. Danas većinu hakovanja lozinki obavljaju kompjuterski programi i njima ne treba mnogo da provale kratku lozinku. Zbog toga, od suštinskog je značaja da vaše lozinke imaju bar 16 znakova ili bar 5 reči, a po mogućstvu budu i duže.

NASUMIČNOST

Čak i ukoliko je lozinka dugačka, nije dobra ako se odnosi na nešto o vama što protivnik može lako da pogodi. Nemojte za lozinku koristiti informacije poput sopstvenog rođendana, mesta rođenja, omiljenih aktivnosti, ili drugih činjenica koje neko može da sazna o vama ako vas izgugla na pet minuta.

JEDINSTVENOST

Jedan od načina da istovremeno obezbedite dužinu, nasumičnost i jedinstvenost jeste da odaberete tri ili četiri uobičajene ali nasumične reči. Na primer, vaša lozinka bi mogla biti „cvet lampa zeleni medved" što je lako zapamiti, ali teško pogoditi. Možete da pogledate ovu stranicu firme Better Buys da biste videli koliko brzo loše lozinke mogu da budu provaljene.

Jedan od načina da istovremeno obezbedite dužinu, nasumičnost i jedinstvenost jeste da odaberete tri ili četiri uobičajene ali nasumične reči. Na primer, vaša lozinka bi mogla biti „cvet lampa zeleni medved" što je lako zapamiti, ali teško pogoditi. Možete da pogledate ovu stranicu firme Better Buys da biste videli koliko brzo loše lozinke mogu da budu provaljene.

KORISTITE PROGRAM ZA UPRAVLJANJE LOZINKAMA (PASSWORD MANAGER)

Sad znate da je važno da svako u organizaciji koristi duge, nasumične i različite lozinke za svaki od svojih ličnih i profesionalnih naloga, ali kako da to zaista i postignete? Pamćenje dobrih lozinki za desetine (ako ne i stotine) naloga je nemoguće, tako da svi moraju da varaju. Pogrešan način da to odradite je da više puta koristite istu lozinku. Na sreću, možemo se okrenuti programima za upravljanje lozinkama kako bi sebi olakšali život (i učinli prakse po pitanju lozinki mnogo bezbednijim). Ove aplikacije, od kojih mnogima možete pristupiti i na kompjuteru i na mobilnom telefonu , mogu da kreiraju, sačuvaju lozinke i upravljaju istima na nivou cele vaše organizacije. Uvođenje bezbednog programa za upravljanje lozinkama znači da ćete morati da zapamtite samo jednu veoma jaku dugu lozinku koja se naziva primarnom (nekad ranije i glavnom), a da istovremeno možete da imate bezbedne jedinstvene lozinke na svim nalozima. Ovu primarnu lozinku (i verovatno drugi faktor potvrde identiteta, tzv. 2FA koji ćemo predstaviti u sledećem odeljku) ćete koristiti kako biste otvorili svoj program za upravljanje lozinkama i otključali pristup svim drugim lozinkama. Ove programe takođe može deliti više osoba kako bi se olakšalo bezbedno deljenje lozinki na nivou cele organizacije.

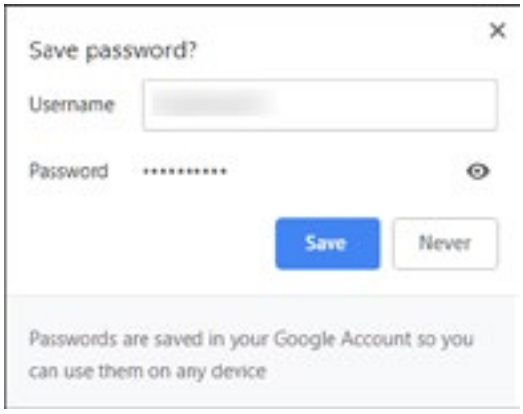
Zašto moramo da koristimo nešto novo? Zar ne možemo samo da ih zapišemo na parčetu papira ili unesemo u tabelu na kompjuteru?

Nažalost, postoji mnogo uobičajenih pristupa upravljanju lozinkama koji nisu bezbedni. Ukoliko lozinke zapisujete na papiru (a taj papir ne zaključavate u sef) izlažete ih fizičkoj krađi, tuđim pogledima i lako ih možete izgubiti ili oštetiti. Ako lozinke čuvate u dokumentu na kompjuteru time samo olakšavate posao hakeru - ili pak nekom ko vam ukrade kompjuter dajete pristup ne samo vašem uređaju već i svim vašim nalozima. Korišćenje dobrog programa za upravljanje lozinkama je podjednako lako kao upisivanje u lozinki u dokument, samo mnogo bezbednije.

Zašto bi trebalo da verujemo programu za upravljanje lozinkama?

Kvalitetni programi za upravljanje lozinkama ulažu velike napore (i zapošljavaju odlične bezbednosne timove) kako bi njihovi sistemi bili bezbedni. Dobre aplikacije za upravljanje lozinkama (nekoliko smo preporučili u nastavku teksta) su takođe tako dizajnirane da ne mogu da „otključaju" vaše naloge. To znači da u većini slučajeva, čak i ukoliko ih hakuju ili zakonski primoraju da predaju informacije, ne bi bili u stanju da izgube ili predaju vaše lozinke. Takođe je važno zapamititi da je beskonačno verovatnije da će protivnik pogoditi jednu od vaših slabih ili ponovljenih lozinki, ili naći neku od njih među procurelim podacimanego da će neko probiti bezbednosni sistem dobrog programa za upravljanje lozinkama. Važno je da budete skeptični i svakako ne bi trebalo da slepo verujete svakom programu ili aplikaciji, ali programima za upravljanje lozinkama sa dobrom reputacijom je u interesu da vas ne prevare.

Umesto da koristite pretraživač (poput Chrome-a prikazanog na levoj strani) za čuvanje lozinki, koristite posebni program za upravljanje lozinkama (kao što je BitWarden, prikazan na desnoj strani). Programi za upravljanje lozinkama imaju funkcionalnosti koje čine život bezbednijim i lakšim za vašu organizaciju.



A šta je sa čuvanjem lozinki u internet pretraživaču?

Čuvanje lozinki u pretraživaču nije isto kao upotreba bezbednog program za upravljanje lozinkama. Ukratko, ne bi trebalo da koristite Chrome, Firefox, Safari ili bilo koji drugi pretraživač za čuvanje lozinki. Iako su oni definitivno bolje rešenje od zapisivanja lozinki na papiru ili unošenja istih u Excel tabelu, bazično tehničko rešenje za čuvanje lozinki koje vaš pretraživač koristi nije baš idealno sa aspekta bezbednosti. Tako takođe gubite mnoge prednosti koje dobar program za upravljanje lozinkama može da pruži vašoj organizaciji. Ako ostanete bez tih prednosti, verovatnije je da će ljudi na svim nivoima organizacije nastaviti da kreiraju slabe lozinke i nebezbedno ih dele sa drugima.

Na primer, za razliku od specijalizovanih programa za upravljanje lozinkama, pretraživačeva ugrađena „sačuvaj ovu lozinku“ ili „zapamti ovu lozinku“ funkcija ne funkcioniše podjednako na mobilnim uređajima ili na različitim pretraživačima, niti poseduje jake alatke za kreiranje i reviziju lozinki. Ove funkcionalnosti predstavljaju veliki deo onoga što program za upravljanje lozinkama čini tako korisnim i dobrim za bezbednost vaše organizacije. Programi za upravljanje lozinkama takođe obuhvataju i specifične funkcionalnosti za potrebe organizacija (kao što je deljenje lozniki) koje se ne odnose samo na bezbednost pojedinaca, već poseduju vrednost sa aspekta bezbednosti organizacije u celini.

Ukoliko ste čuvali lozinke u pretraživaču (namerno ili nenamerno), odvojite momenat da ih uklonite.

Koje programe za upravljanje lozinkama bi trebalo da koristimo?

Postoje mnoge dobre alatke za upravljanje lozinkama koje mogu biti instalirane i pokrenute za manje od pola sata. Ako tražite pouzdanu onlajn opciju za vašu organizaciju kojoj ljudi mogu da u bilo kom momentu pristupe sa više uređaja, 1Password (sa početnom cenom od $2,99 po korisniku mesečno) ili besplatni open-source BitWarden imaju dobru podršku i toplo ih preporučuju.

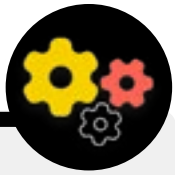
Onlajn opcija kao što je BitWarden može istovremeno biti odlična za bezbednost i laka za korišćenje. BitWarden, na primer,

će vam pomoći da kreirate jedinstvene jake lozinke i pristupite im sa više uređaja preko ekstenzija za pretraživač i mobilne aplikacije. Sa plaćenom verzijom ($10 za celu godinu) BitWarden takođe izveštava o više puta korišćenim, slabim i potencijalno provaljenim lozinkama kako biste bili u toku sa razvojem situacije. Jednom kad upišete svoju primarnu (ili glavnu) lozinku, takođe bi trebalo da uključite dvostruku potvrdu identiteta kako biste maksimalno zaštitili memoriju svog programa za upravljanje lozinkama.

Od suštinskog je značaja da se i prilikom upotrebe programa za upravljanje lozinkama pridržavate pravila bezbednosti. Na primer, ako koristite ekstenziju za pretraživač ili se ulogujete u Bitwarden (ili bilo koji drugi program za upravljanje lozinkama) na vašem uređaju, setite se da se odjavite nakon upotrebe ako delite taj uređaj sa nekim drugim ili verujete da postoji povećani rizik od fizičke krađe uređaja. Ovo podrazumeva i odjavljivanje sa naloga za upravljanje lozinkama i ukoliko ostavite kompjuter ili mobilni telefon bez nadzora. Ukoliko delite lozinke u okviru organizacije, postarajte se da obustavite pristup lozinkama (i promenite ih) kad neko napusti organizaciju. Na primer, ne želite da bivši zaposleni ima lozinku za pristup Facebook stranici vaše organizacije.

Šta ako neko zaboravi svoju primarnu lozinku?

Od suštinskog je značaja da zapamtite svoju primarnu lozinku. Dobri programi za upravljanje lozinkama poput gorenavedenih neće pamtiti primarnu lozinku niti vam dozvoliti da je resetujete direktno putem mejla kao što je moguće na internet sajtovima. Ovo je dobro sa aspekta bezbednosti, ali je zbog toga od ključnog značaja da zapamtite svoju primarnu lozinku kad po prvi put instalirate program. Kako biste to lakše postigli, možda možete da zakažete dnevne podsetnike da biste se setili svoje primarne lozinke kad budete po prvi oput pravili nalog u programu za upravljanje lozinkama.



Korišćenje programa za upravljanje lozinkama u vašoj organizaciji

Možete unaprediti postupanje po pitanju loziniki na nivou cele organizacije i postarati se da svi članovi osoblja imaju pristup programu za upravljanje lozinkama (i koriste ga) tako što ćete jedan takav program uvesti na nivou cele organizacije. Umesto da svaki pojedinačni član osoblja otvara svoj nalog, razmotrite da kupie „timski“ ili „poslovni“ paket. Na primer, BitWarden-ov „timski organizacioni“ paket košta $3 po korisniku mesečno. Sa njim (ili drugim timskim paketima programa za upravljanje lozinkama kao što je 1Password), možete da upravljate svim deljenim lozinkama na nivou organizacije. Funkcionalnosti programa za upravljanje lozinkama na nivou organizacije ne samo da pružaju veću bezbednost već i pogodnosti za osoblje. Možete bezbedno da delite akreditive unutar samog programa sa različitim korisničkim nalozima. A BitWarden, na primer, u okviru svog timskog paketa takođe obezbeđuje zgodnu funkcionalnost za obostrano šifrirano slanje teksta i fajlova koja se zove „BitWarden Send“. Ovakve funkcionalnosti vašoj organizaciji daju veći stepen kontrole nad tim ko može da vidi i deli koje lozinke, i obezbeđuje bezbedniju opciju za deljenje akreditiva za timske ili grupne naloge. Ukoliko instalirate program za upravljanje lozinkama na nivou cele organizacije, postarajte se da neko bude posebno zadužen za to da briše naloge osoblja i menja bilo koje zajedničke lozinke kad neko napusti tim.

ŠTA JE DVOSTRUKA POTVRDA IDENTITETA?

Koliko god da ste oprezni sa lozinkama, hakeri veoma često umeju da ih zaobiđu. Da biste svoje naloge sačuvali od današnjih uobičajenih pretnji potreban vam je još jedna nivo zaštite. Tu u priču ulazi dvostruka potvrda identiteta ili 2FA (akronim engleskih reči „two factor authentication" /prim.prev./).

Postoje brojni odlični vodiči i resursi koji objašanjavaju dvostruku potvrdu identiteta, među kojima i članak Martina Šeltona pod nazivom Two Factor Authentication for Beginners (Dvostruka potvrda identiteta za početnike) i Election Cybersecurity 101 Field Guide (Terenski vodič za osnovnu sajber bezbednost tokom izbora) Centra za demokratiju i tehnologiju. Ovaj odeljak koristi oba ova resursa kako bismo lakše objasnili zašto je tako važno uvesti 2FA na nivou cele organizacije.

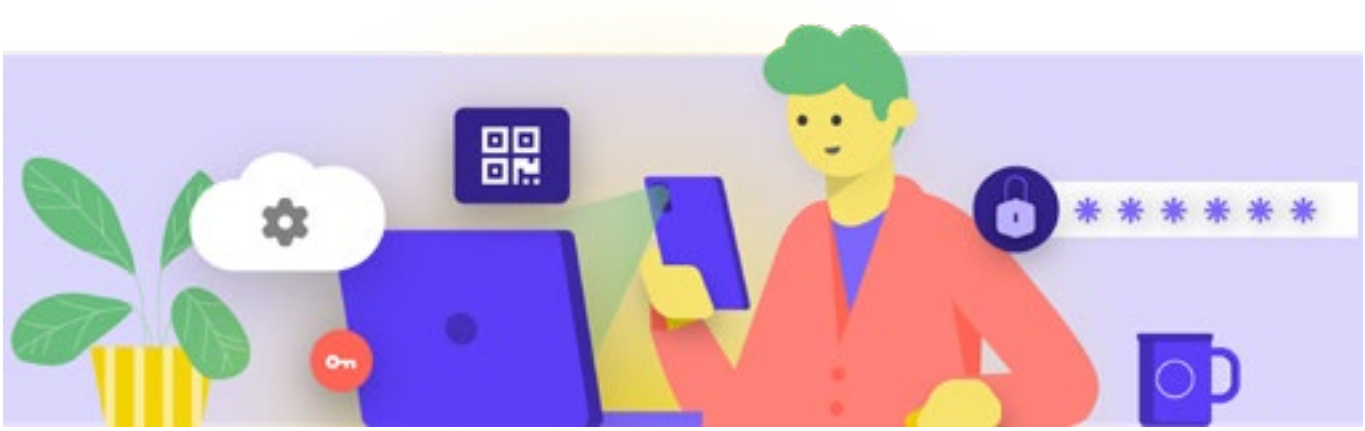
Ukratko, 2FA povećava bezbednost naloga tako što vam je potreban dodatni podatak - ne samo lozinka - da biste dobili pristup. Taj drugi podatak je obično nešto što dobijete, poput broja za autorizaciju sa aplikacije na vašem telefonu ili fizičkog tokena ili ključa. Ovaj drugi podatak predstavlja drugu liniju odbrane. Ako vam haker ukrade lozinku ili je nađe u gomili lozinki koja je provaljena tokom masovne povrede podataka, delotvorna 2FA može da ga spreči da pristupi vašem nalogu (i samim tim privatnim i osetljivim podacima). Od kritične je važnosti da svi u organizaciji uključe dvostruku potvrdu identiteta na svojim nalozima.

KAKO MOŽEMO DA UKLJUČIMO DVOSTRUKU POTVRDU IDENTITETA?

Postoje tri uobičajene metode za 2FA: sigurnosni ključevi, aplikacije za potvrdu identiteta i jendokratni brojevi za autorizaciju koji se šalju preko SMS-a.

sigurnosni ključevi

Sigurnosni ključevi su najbolja opcija, delom i zato što su potpuno neprobojni sa aspekta "fišinga" (phishing). Ovi „ključevi2 su hardverski tokeni (nalik na male USB-e) koje možete prikačiti na privezak za ključeve (ili mogu stalno biti uključeni u kompjuter) kako ih ne biste izgubili. Kad dođe momenat da uz pomoć tog ključa otključate neki nalog, jednostavno ga ubacite u uređaj i fizički ga kucnete kad za to dobijete uputstvo tokom prijavljivanja. Postoji čitav niz modela koje možete kupiti preko interneta (za 20-50 dolara), uključujući Yubikeys ili Google-ove Titan ključeve. Wirecutter, internet stranica Njujork tajmsa za ocenjivanje proizvoda, ima koristan vodič sa preporukama za kupovinu ključeva. Imajte na umu da isti ključ može da se koristi za koliko god želite naloga. Dok su ovi ključevi malo preskupi za mnoge organizacije, inicijative poput Google-ovog Programa za naprednu zaštitu ili Microsoft-ovog AccountGuard ove ključeve besplatno dele ugroženim grupama koje ispunjavaju određene kriterijume. Kontaktirajte one koji su vam dali ovaj priručnik kako biste videli da li mogu da vas povežu sa takvim programima ili nam pišite cyberhandbook@ndi.org.



aplikacije za potvrdu identiteta

Druga najbolja opcija su aplikacije za potvrdu identiteta. One vam dozvoljavaju da primite privremenu šifru za prijavljivanje preko mobilne aplikacije ili push notifikacije na vašem pametnom telefonu. Neke popularne i pouzdane opcije uključuju Google Authenticator, Authy i Duo Mobile. Aplikacije za potvrdu identiteta su sjajne i zato što rade i kad nemate pristup mreži mobilne telefonije i besplatne su za pojedince. Međutim, one su podložnije fišingu od sigurnosnih ključeva jer korisnici mogu biti prevareni da šifru iz aplikacije ukucaju na lažnoj internet stranici. Pazite da šifre za prijavljivanje unosite samo na legitimnim sajtovima. I ne prihvatajte push notifikacije za prijavljivanje osim ako niste sigurni da ste poslali zahtev za prijavu. Takođe je od suštinskog značaja da prilikom upotrebe ovakvih aplikacija da imate rezervnu kopiju šifri (objašnjenje u daljem tekstu) u slučaju da izgubite telefon ili vam ga ukradu.

Kodovi preko SMS

Najnebezbedniji ali nažalost najuobičajeniji oblik 2FA su brojevi za autorizaciju koji se šalju preko SMS poruka. Pošto se SMS može presresti, a brojevi telefona mogu biti lažirani ili hakovani preko vašeg mobilnog operatera, ovakve poruke nisu baš najsrećniji metod za traženje 2FA šifri. To jeste bolje nego da koristite samo lozinku, ali preporučujemo da ako je ikako moguće koristite aplikacije za potvrdu identiteta ili fizičke sigurnosne ključeve. Uporni protivnik može da dobije pristup SMS brojevima za dvostruku potvrdu identiteta, obično samo tako što može pozvati telefoniju i zameniti vašu SIM karticu.

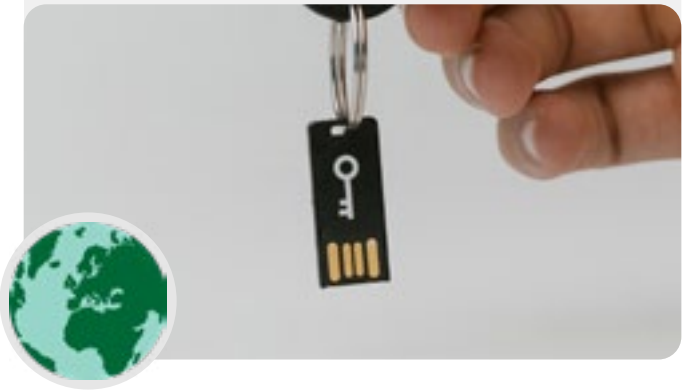
Kad budete spremni da uključite 2FA na svim nalozima svoje organizacije, iskoristite ovu internet stranicu (https://2fa.directory/) da biste videli sažeti pregled informacija i uputstava za različite servise (kao što su Gmail, Office 365, Facebook, Twitter, itd) kao i koji dozvoljavaju koju vrstu 2FA.

2FA i civilno društvo

Po nedavnom izveštaju organizacije Amnesty International, hakeri koji su napadali branitelje ljudskih prava u Uzbekistanu su koristili fišing (phishing) napade kako bi prevarili korisnike da s njima podele svoje lozinke *kao i* šifre za dvostruku potvrdu identiteta na njihovim imejl nalozima preko lažnih stranica za prijavu. Takvi napadi su sve češći način da se zaobiđe dvostruka potvrda identiteta. Važno je - čak i ako ste uključili opciju dvostruke potvrde identiteta - da pazite gde ukucavate šifre. Ili, još bolje, možete u potpunosti da eliminišete taj rizik upotrebom fizičkih ključeva.

Sigurnosni ključevi u stvarnom svetu

Obezbeđivanjem fizičkih ključeva za dvostruku potvrdu identiteta za svih svojih 85 i više hiljada zaposlenih, Google (veoma visoko rizična organizacija koja je stalno meta napada) je zapravo **eliminisao mogućnost uspešnih** fišing napada na organizaciju. Ovaj slučaj pokazuje koliko delotvorni sigurnosni ključevi mogu biti čak i u najugroženijim organizacijama.



ŠTA AKO NEKO IZGUBI 2FA UREĐAJ?

Ako je u pitanju sigurnosni ključ, mislite o njemu kao o svom kućnom ključu, ako ga imate. Ukratko, nemojte ga izgubiti. Međutim, isto kao u slučaju ključeva od kuće, nije loše imati rezervni ključ prijavljen na vaš nalog koji ćete zaključati na nekom bezbednom mestu (kao npr. kućnom ili bankovnom sefu) za slučaj gubitka ili krađe.

Alternativno bi trebalo da (na nalozima na kojima je to moguće) kreirate rezervne šifre. Trebalo bi da ih čuvate na veoma bezbednom mestu, npr. u programu za upravljanje lozinkama ili u fizičkom sefu. Takve rezervne šifre je moguće generisati na većini sajtova koje nude uslugu dvostruke potvrde identiteta (na istom mestu gde ste i uključili opciju 2FA) i mogu funkcionisati kao rezervni ključevi u hitnoj situaciji.

Do najuobičajenijih problema sa 2FA dolazi kad ljudi izgube ili zamene telefone na kojima imaju aplikaciju za potvrdu identiteta. Ukoliko koristite Google Authenticator nemate sreće ako vam ukradu telefon, osim ako niste sačuvali rezervne šifre koje se generišu kad neki nalog povežete sa Google Authenticator-om. Stoga, ako koristite Google Authenticator kao aplikaciju za dvostruku potvrdu identiteta, postarajte se da čuvate rezervne šifre za sve naloge koje ste povezali na sigurnom mestu.

Ako koristite Authy ili Duo, ove ove aplikacije imaju funkcionalnosti za kreiranje bekapa sa jakim bezbednosnim podešavanjima koje možete da uključite. Ako izaberete ijednu od ove dve aplikacije možete konfigurisati ove opcije za bekapovanje u slučaju da vam se telefon pokvari, ukradu ga ili ga izgubite. Vidite uputstva za Authy ovde i Duo ovde.

Postarajte se da su svi u vašoj organizaciji upoznati sa ovim dok budu uključivali 2FA na svojim nalozima.

Primena 2FA na nivou cele organizacije

Ukoliko vaša organizaicja obezbeđuje imejl naloge za celokupno osoblje preko platformi Google Workspace (prethodno poznate kao GSuite) ili Microsoft 365 i koristi svoj domen (na primer, @ndi.org), možete uključiti 2FA i stroge mere bezbednosti za sve naloge. To ne samo da štiti ove naloge, već i upoznaje vaše osoblje sa dvostrukom potvrdom identiteta i čini je normalnim delom svakodnevnog rada, tako da će je lakše usvojiti i za svoje privatne naloge. Kao administrator Google Workspace-a, možete pratiti **sledeća uputstva** kako biste uveli 2FA za svoj domen. Možete nešto slično uraditi i u okviru Microsoft 365 kao admin domena **ako pratite ove korake.**

Bezbedni nalozi

- **Uvedite obavezu jakih lozinki za sve naloge koji pripadaju organizaciji; podstaknite osoblje i volontere da isto urade i na svojim privatnim nalozima.**
- **Uvedite pouzdani program za upravljanje lozinkama na nivou organizacije (i podstaknite osoblje da ga koristi i u privatnom životu).**
  - **Uvedite obavezne jake lozinke i dvostruku potvrdu identiteta za sve naloge programa za upravljanjem lozinkama.**
  - **Podsetite sve da se odjavljuju iz programa za upravljanje lozinkama na zajedničkim uređajima ili kad postoji veći rizik od krađe ili konfiskacije uređaja.**
- **Promenite zajedničke lozinke kad god neko napusti organizaciju.**
- **Delite lozinke samo na bezbedni način, na primer preko programa za upravljanjelozinkama ili aplikacija sa obostranom enkripcijom.**
- **Uvedite obaveznu dvostruku potvrdu identiteta na svim nalozima koji pripadaju organizaciji i podstaknite osoblje da je uključe i za sve privatne naloge.**
  - **Po mogućstvu celokupnom osoblju nabavite fizičke sigurnosne ključeve.**
  - **Ukoliko nemate sredstava za ove ključeve, ohrabrite upotrebu aplikacija za potvrdu identiteta umesto SMS poruka ili telefonskih poziva.**
- **Održavajte redovne sastanke kako biste se postarali da je osoblje upoznato sa najboljim praksama sa aspekta lozinki i dvostruke potvrde identiteta, uključujući i elemente jake lozinke i značaj korišćenja drugačijih lozinki za svaki nalog, prihvatanja samo legitimnih zahteva i kreiranja rezervnih šifara za dvostruku potvrdu identiteta.**

Bezbedni uređaji

Pored naloga, od suštinskog je značaja da dobro zaštitite sve uređaje - kompjutere, telefone, USB-ove, eksterne hard diskove itd.

Ovakva zaštita počinje obraćanjem pažnje na to koje vrste uređaja vaša organizacija i osoblje nabavljaju i koriste. Bilo koji prodavci ili proizvođači koje odaberete bi trebalo da imaju istorijat poštovanja globalnih standarda za bezbedni razvoj hardverskih uređaja (kao što su telefoni i kompjuteri). Bilo koji uređaji koje nabavite bi trebalo da budu proizvedeni u pouzdanim kompanijama koje nemaju motiva da predaju podatke i informacije potencijalnom protivniku. Važno je napomenuti da kineska vlada od kineskih kompanija zahteva da joj prosleđuju podatke. Tako da uprkos svepristunosti jeftinih pametnih telefona kao što su Huawei ili ZTE, iste treba izbegavati. Iako cena jefitnog hardvera može biti jako privlačna nekoj organizaciji, potencijalni bezbednosni rizik za organizacije koje se zalažu za demokratiju, ljudska prava ili odgovornost države bi trebalo da bude dovoljno jak razlog da se opredelite za neke druge uređaje, pošto je pristup ovim podacima pomogao kineskoj i drugim vladama da se okome na određene pojedince i zajednice.

Vaši protivnici mogu ugroziti bezbednost vaših uređaja - i sve što radite sa tih uređaja - tako što će vašim uređajima pristupiti ili direktno (fizički) ili na daljinu.

Bezbednost uređaja i civilno društvo

Neki od najnaprednijih malvera na svetu su kreirani i upotrebljeni kako bi se napale organizacije civilnog društva i branitelji ljudskih prava. U Indiji, na primer, Amnesty International je prijavio da je tokom 2020. bar devet branitelja ljudskih prava bilo meta napada spajverom (vrstom malicioznog softvera) preko kompjutera i mobilnih telefona. Spajver je ubačen preko niza „fišing“ (phishing) mejlova sa linkovima na zaražene fajlove poslate preko Firefox Send-a (programa za slanje linkova koji više ne postoji). Ukoliko bi neko otvorio fajl, uređaji bi im bili zaraženi softverom koji je snimao njihove razgovore, presretao poruke i beležio šta kucaju na tastaturi, te ih tako u principu stavio pod konstantni nadzor napadača. Takvi napadi, koji su često usmereni protiv grupa civilnog društva i pojedinačnih članova njihovog osoblja, nažalost predstavljaju uobičajeni način na koji napadači dobiju pristup uređaju na daljinu.

FIZIČKI PRISTUP UREĐAJIMA USLED KRAĐE ILI GUBLJENJA

Kako biste sprečili da neko fizički pristupi vašim uređajima, od suštinskog je značaja da ih čuvate. Ukratko, nemojte protivniku olakšati da ukrade ili čak privremeno uzme uređaj od vas. Zaključavajte uređaje ako ih ostavite kod kuće ili u kancelariji. Ili, ako mislite da je to bezbednije, stalno ih nosite sa sobom. Ovo naravno znači da je bezbednost uređaja povezana sa fizičkom bezbednošću vašeg radnog prostora (bilo da radite u kancelariji ili od kuće). Možda ćete morati da instalirate jake brave, kamere ili druge sisteme za video nadzor - naročito ako je vaša organizacija izložena velikom riziku. Podsetite osoblje da se prema svojim uređajima ponašaju kao velikom svežnju novčanica – dakle, da ih ne ostavljaju posvuda bez nadzora ili zaštite.

Šta ako vam ukradu uređaj?

Kako biste smanjili štetu ako vam neko ukrade uređaj – ili čak i ako mu samo kratkotrajno pristupi - obavezno **naložite upotrebu jakih lozinki ili šifri na svim kompjuterima i mobilnim telefonima**. U slučaju kompjutera ili laptopa važe isti saveti kao u odeljku koji je obrađivao lozinke. Kad je u pitanju zaključavanje telefona, koristite šifre od bar šest do osam cifara i izbegavajte da otključavate ekran povlačenjem prsta. Za dodatne praktične savete o zaključavanju ekrana, pogledajte Data Detox Kit (Paket za detoksikaciju podataka) koji je kreirao Tactical Tech. Ako koristite jake lozinke na uređajima onda će proitivniku biti mnogo teže da brzo pristupi podacima na njima u slučaju krađe ili konfiskacije. Sa jakom šifrom, aktiviranje prepoznavanja lica ili otključavanja otiskom je u redu, ali obavezno iste deaktivirajte (bez deaktiviranja jake šifre) pre visokorizičnih aktivnosti poput učešća u demonstracijama ili prelaska granice ukoliko se vi ili vaše osoblje brinete da će vam vlasti konfiskovati te uređaje.

Ako bilo koji uređaj u vlasništvu organizacije ima „pronađi moj uređaj“ funkciju, kao npr. na ajfonu ili Find My Device na android telefonima, razmislite da tražite od osoblja da je uključe. Podstaknite osoblje da ove funkcije koristi i na svojim privatnim telefonima. Kad je ova funkcija uključena, vlasnik uređaja (ili osoba iz njegove liste kontakta u koju ima poverenja) mogu da lociraju uređaj ili izbrišu sve na njemu na daljinu ukoliko je ukraden, izgubljen ili konfiskovan. U slučaju ajfona, možete i da podesite uređaj da sam izbriše sav sadržaj na sebi nakon nekoliko neuspešnih pokušaja prijave. Takve funkcionalnosti za upravljanje uređajima postaju od kritičnog značaja za neku organizaciju u slučaju da uređaj sa osetljivim informacijama bude izgubljen ili dospe u pogrešne ruke.

A šta je sa enkripcijom uređaja?

Važno je koristiti enkripciju, šifrovati podatke tako da budu nečitljivi ili neupotrebljivi na svim vašim uzređajima, naročito kompjuterima i pametnim telefonima. Trebalo bi da na svim uređajima u vašoj organizaciji po mogućnosti podesite nešto što se zove **enkripcija celog diska**. Enkripcija celog diska zapravo znači da je ceo uređaj šifriran tako da protivnik, ukoliko ga ukrade, ne bi mogao da izvuče sadržaj sa njega a da ne zna lozinku ili ključ koji je korišten za šifrovanje.

Mnogi moderni pametni telefoni i kompjuteri nude enkripciju celog diska. Apple-ovi uređaji poput ajfona i ajpeda, veoma zgodno uključuju enkripciju celog diska kada kreirate normalnu šifru za pristupanje uređaju. Apple-ovi kompjuteri koji koriste Mac operativni sistem imaju funkcionalnost po imenu FileVault koju možete da uključite kako biste omogućili enkripciju celog diska.

Windows kompjuteri sa pro, poslovnim ili edukacionim licencama nude funkcionalnost koja se zove BitLocker koju možete da uključite kako biste omogućili enkripciju celog diska. BitLocker možete da uključite ako pratite ova uputstva, ali isti možda prvo treba da odobri administrator vaše organizacije. Ako osoblje ima samo Windows licencu za kućnu upotrebu BitLocker im neće biti dostupan. Međutim, i dalje mogu da uključe enkripciju celog diska ako u podešavanjima Windows operativnog sistema odu na komandu ‘Update & Security’ > ‘Device encryption’.

Na android uređajima, od verzije 9,0 nadalje, enkripcija celog diska je uključena u fabričkim podešavanjima. Ako korisite relativno novi android telefon i imate šifru, trebalo bi da vam je uključena i enkripcija celog diska. Međutim, dobra je ideja da proverite podešavanja čisto da budete sigurni, naročito ako su vam telefoni stariji od par godina. Kako biste proverili, idite na Podešavanja > Bezbednost na vašem android uređaju. U okviru bezbednosnih podešavanja bi trebalo da pogledate pododeljak „enkripcija“ ili „enkripcija i akreditivi“ koji će vam ukazati na to da li je vaš telefon pod enkripcijom i ako nije, dozvoliti vam da je uključite.

Kod kompjutera (bilo da imaju Windows ili Mac operativni sistem), naročito je bitno da sve enkripcione ključeve (koje zovu ključevi za povraćaj) držite na sigurnom mestu. Ovi ključevi za povraćaj su u većini slučajeva u principu duge lozinke koje se mogu sastojati i od više reči. U slučaju da zaboravite vašu uobičajenu lozinku ili se desi nešto neočekivano (kao npr. kvar na uređaju), ključevi za povraćaj su jedini način da povratite svoje enkrriptovane podatke i, ukoliko je to potrebno, premestite ih na novi uređaj. Dakle, kad uključite enkripciju celog diska, obavezno te ključeve smestite na sigurno mesto, poput obezbeđenog naloga na klaudu ili u program za upravljanje lozinkama vaše organizacije.

DALJINSKI PRISTUP UREĐAJU

– TAKOĐE POZNAT KAO HAKOVANJE

Pored fizičke bezbednosti uređaja, važno je i zaštiti ih od malvera. Vodič **Security-in-a-Box** (Bezbednost u kutiji) NVO-a Tactical Tech daje koristan opis malvera i važnosti izbegavanja istog, koje u blago adaptiranom obliku prenosimo u ostatku ovog odeljka.

Razumevanje i izbegavanje malvera

Postoje mnogi načini klasifikacije malvera (što je portmanto engleskih reči zlonamerni i softver) Virusi, spajver, crvi, trojanci, rutkitovi, ransomver i kriptodžekeri su sve tipovi malvera. Neki tipovi malvera se internetom šire preko mejlova, SMS-ova, lažnih sajtova i na druge načine. Neki se šire preko uređaja poput USB-a koji se koriste za razmenu i krađu podataka. I dok je u slučaju pojedinih malvera neophodno da nesvesna meta napravi grešku, drugi mogu da iz potaje zaraze ranjive sisteme, a da vi nigde ne pogrešite.

Pored generalnog malvera (koji se široko distribuira i meta mu je opšta javnost), ciljani malver se tipično koristi kako bi se uticalo na određenu osobu, organizaciju ili mrežu ili kako bi se isti špijunirali. Obični kriminalci koriste ove tehnike, ali to čine i vojne i obaveštajne službe, teroristi, lica koja uznemiravaju druge preko interneta, počinitelji nasilja u porodici i sumnjivi političari.

Kako god ih zvali, kako god da se šire, malveri mogu da unište kompjutere, ukradu i izbrišu podatke, dovedu organizacije do bankrota, ugroze privatnost i dovedu korisnike u opasnost. Ukratko, malver je zaista jako opasan. Međutim, postoje jednostavni koraci koje vaša organizacija može da preduzme kako bi se zaštitila od uobičajene pretnje.

Da li će nas antimalveri zaštititi?

Antimalver programi nažalost nisu kompletno rešenje. Ali, jako je dobra ideja da koristite neki osnovni, besplatni program kao osnovu. Malver se menja tako brzo i novi rizici se tako često pojavljuju da ne možete da se oslonite samo na takav program da biste se zaštitili.

Ukoliko koristite Windows bacite pogled na Windows Defender koji dolazi sa tim operativnim sistemom. Mac i Linux kompjuteri nemaju ugrađeni antimalverski softver, kao ni android ili iOS uređaji. Na tim uređajima (kao i na računarima koji koriste Windows) možete instalirati pouzdani, besplatni softver kao što su **Bitdefender** ili **Malwarebytes**. **Ali ne oslanjajte se na njih kao na jedinu liniju odbrane** pošto će sigurno propustiti neki od najciljanijih, najopasnijih novih napada.

Takođe pazite da skidate samo pouzdane antimalvere i antiviruse iz legitimnih izvora (poput gore navedenih internet stranica). Nažalost, postoje mnoge lažne ili kompromitovane verzije antimalverskog softvera koje mogu pre da naškode nego da vas zaštite.

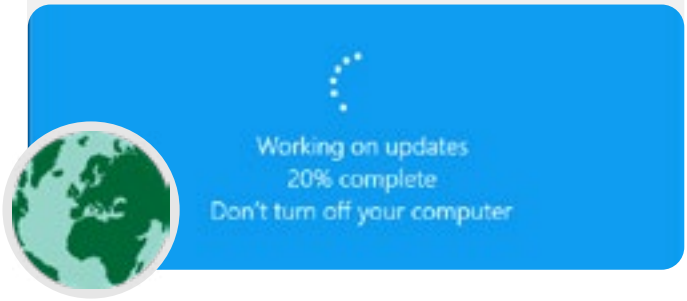
Ukoliko koristite Bitdefender ili još neki antimalver u okviru organizacije, pazite da ih ne aktivirate istovremeno. Mnogi od njih će rad drugog antimalver programa identifikovati kao sumnjivu aktivnost i zaustaviti ga, što će dovesti do toga da nijedan ni drugi program ne funkcioniše kako treba. Bitdefender ili druge pouzdane antimalverske programe možete besplatno ažurirati, a Windows Defender se ažurira zajedno sa vašim kompjuterom. Postarajte se da se vaš antimalverski softver redovno ažurira (neke probne verzije komercijalnog softvera koje dobijete sa računarom prestanu da rade nakon što probni period istekne i tako zapravo predstavljaju pre rizik nego pomoć). Novi malver nastaje i distribuiše se svakodnevno, i vaš kompjuter će brzo postati još ranjiviji ukoliko stalno ne skidate nove definicije malvera i nove antimalverske tehnike. Ukoliko je to moguće, treba da softver podesite tako da se automatski ažurira. Ako vaš antimalverski program ima opcionu „uvek uključen“ funkciju, trebalo bi da je uključite i da razmotrite da povremeno skenirate sve fajlove na kompjuteru.

Ažurirajte uređaje

Ažuriranje je od suštinskog značaja. Instalirajte poslednju verziju operativnog sistema koji vaš uređaj koristi (Windows, Mac, Android, iOS, itd), i redovno ažurirajte taj operativni sistem. Ažurirajte i sav ostali softver, internet pretraživač i bilo koje njegove dodatne komponente. Instalirajte ispravke čim postanu dostupne, idealno tako što ćete **uključiti automatsko ažuriranje**. Što je operativni sistem na vašem uređaju ažuriraniji, to će biti manje ranjiv. Razmišljajte o ažuriranju kao stavljanju flastera na posekotinu. Pokriva ranu i uveliko smanjuje mogućnost infekcije. Takođe dezinstalirajte softver koji više ne koristite. Zastareli softver često predstavlja pretnju po bezbednost i možda ste instalirali alatku koju njen kreator više ne ažurira zbog čega je ranjivija na hakerske napade.

Malver u stvarnom svetu: Ažuriranje je ključno

Napadi WannaCry ransomverom su 2017. godine zarazili milione uređaja širom sveta, zatvorili bolnice, državne institucije, velike i male organizacije i kompanije u desetinama zemalja. Zašto je ovaj napad bio tako uspešan? Zbog zastarelih, neažuriranih Windows operativnih sistema od kojih su mnogi bili piratske verzije. Veliki deo ove štete – kako po ljude tako i finansije – je mogao biti izbegnut da su se koristili legalni operativni sistemi i da je postojala obaveza uključivanja automatskog ažuriranja.



Budite oprezni kad radite sa USB-ima

Budite oprezni prilikom otvaranja fajlova koje vam šalju u prilozima mejlova, preko linkova za skidanje, ili na bilo koji drugi način. Takođe, dobro razmislite pre nego što ubacite uređaje poput USB-a, kartica sa fleš memorijom, DVD-a i CD-a u svoj kompjuter pošto sa njih možete pokupiti malver. USB-i koje duže vreme deli više ljudi vrlo verovatno sadrže viruse. Kako biste videli neke alternativne opcije bezbednog deljenja fajlova u okviru organizacije konsultujte odeljak o deljenju fajlova u ovom priručniku.

Takođe pazite sa kojim uređajima se povezujete preko Bluetooth-a. Sasvim je u redu da povežete svoj telefon ili uređaj sa poznatim i bezbednim Bluetooth zvučnikom kako biste pustili omiljenu pesmu, ali pazite da se ne povezujete sa nepoznatim uređajima niti primate zahteve za povezivanje od njih. Dozvolite povezivanje samo sa pouzdanim uređajima i setite se da isključite Bluetooth kad ga ne koristite.

Budite pametni tokom pretraživanja interneta

Nikad ne prihvatajte niti pokrećite aplikacije sa internet stranica koje ne znate niti im verujete. Na primer, umesto da prosto prihvatite „ažuriranje“ koje vam nudi prozorčić koji iskoči u vašem pretraživaču, proverite da li je nekoj vašoj aplikaciji zapravo uopšte potrebno ažuriranje na njenom zvaničnom sajtu. Kao što je pomenuto u odeljku priručnika koji se bavi fišingom (phishing), od suštinskog je značaja da pazite gde klikćete na interent sajtovima. Proverite destinaciju linka (tako što ćete postaviti strelicu kursora na nju) pre nego što kliknete, pogledajte adresu stranice nakon što kliknete na link i uverite se da izgleda kako treba pre nego što unesete bilo kakve osetljive podatke poput lozinke. Nemojte klikati na poruke ili upozorenja o grešakama i čuvajte se prozorčića koji automatski iskaču u pretraživaču pa ih uvek pažljivo pročitajte umesto da samo kliknete na „da“ ili „OK“.

A šta je sa pametnim telefonima?

Kao i u slučaju kompjutera, redovno ažurirajte operativni sistem i aplikacije na vašem telefonu, i uključite automatsko ažuriranje. Instalirajte aplikacije samo iz zvaničnih ili pouzdanih izvora kao što su Google Play i Apple App Store (ili F-droid, besplatna, open source radnja za android aplikacije). Aplikacije mogu da sadrže malver a i dalje naizgled normalno funkcionišu pa nikad ne znate da li je neka opasna. Postarajte se i da uvek skidate legalne verzije aplikacija. Na android telefonima naročito, postoji puno „lažnih“ verzija popularnih aplikacija. Tako da proverite da li aplikacija ima legitimnog kreatora, dobre recenzije i očekivani broj skidanja (npr. lažna verzija WhatsApp-a će biti skinuta možda nekoliko hiljada puta, ali prava verzija je skinuta 5 milijardi puta). Obratite pažnju na to koje dozvole određena aplikacija traži. Ako ti zahtevi deluju preterani ili nelogični (kao digitron koji traži pristup kameri ili Angry Birds igrica koja traži pristup vašoj lokaciji, na primer) odbijte zahtev ili izbrišite aplikaciju. Brisanje aplikacija koje više ne koristite takođe može da doprinese bezbednosti vašeg telefona ili tableta. Kreatori aplikacija nekad prodaju vlasništvo nad njima drugim ljudima. Ti novi vlasnici mogu pokušati da zarade tako što će u datu aplikaciju ubaciti zlonamerni program.

Malver u stvarnom svetu: zlonamerne mobilne aplikacije

Hakeri u čitavom nizu zemalja su godinama koristili lažne aplikacije u Google Play radnji da šire malver. Jedan specifičan slučaj gde su pod napadom bili korisnici u Vijetnamu je dospeo u vesti u aprilu 2020. Ova špijunska kampanja je koristila lažne aplikacije koje su navodno korisnicima pomagale da pronađu najbližu kafanu ili informacije o lokalnim crkvama. Jednom kad bi je naivni vlasnik android telefona instalirao, ova aplikacija bi evidentirala pozive, podatke o lokaciji i informacije o kontaktima i SMS porukama. Ovo je samo jedan od razloga što treba da pazite kakve aplikacije skidate.

Uštedite novac i poboljšajte bezbednost uz pomoć Tails operativnog sistema

Jedna veoma bezbedna opcija koja doduše zahteva određeni stepen tehničke veštine tokom instaliranja je operativni sistem Tails. Ovaj portabl operativni sistem je besplatan i možete ga pokrenuti direktno sa USB-a, i tako zaobići potrebu oslanjanja na licencirani Windows ili Mac operativni sistem. Tails je takođe dobra opcija za one koji su izloženi visokom riziku jer obuhvata čitav niz funkcionalnosti za zaštitu privatnosti. Ove funkcionalnosti podrazumevaju integraciju Tor-a (koji ćemo predstaviti u nastavku teksta) kako bi se omogućio bezbedan internet saobraćaj, i potpuno brisanje memorije svaki put kad ugasite operativni sistem. Suštinski vam dozvoljavaju da svaki put kad restartujete kompjuter počnete ispočetka. Tails takođe ima i „trajni način rada“ koji vam omogućava da sačuvate važne fajlove i podešavanja tokom više sesija, ako tako želite.

Još jedan besplatni, bezbedni operativni sistem je Qubes OS. Dok nije najednostavnija opcija za korisnike koji nisu tehnički potkovani, Qubes je dizajniran da smanji opasnost od malvera i predstavlja još nešto što napredni korisnici u vašoj organizaciji, kao i oni koji su izloženi visokom riziku treba da razmotre, naročito ako vam cena licenci predstavlja problem.

Šta ako ne možemo da priuštimo legalni softver?

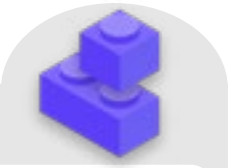
Licence za popularni softver kao što su Microsoft Office (Word, Powerpoint, Excel) za vašu celu organizaciju mogu biti skupe, ali ograničeni budžet nije izgovor za skidanje piratizovanih verzija softvera ili neredovno ažuriranje. Ovo nije pitanje morala, već bezbednosti. Piratizovani softver je često krcat malverom i ne može biti ažuriran kako bi se pokrpile rupe u bezbednosti.

Ako ne možete da priuštite softver koji je vašoj organizaciji potreban, postoji niz odličnih, besplatnih open source softverskih alatki kao što su LibreOffice (zamena za standardne Microsoft Office aplikacije) ili GIMP (zamena za Photoshop) koje mogu da zadovolje vaše potrebe. Takođe razmislite da se registrujete preko TechSoup, što je organizacija koja nudi velike popuste na popularan softver za neprofitne organizacije.

Čak i ako možete da priuštite legalni softver i aplikacije, vaš uređaj je i dalje u opasnosti ukoliko operativni sistem nije legalan. Tako da ako vaša organizacija ne može da priušti licencu za Windows, razmislite o jeftinijim alternativama poput Chromebook-ova, koji predstavljaju odličnu opciju koju je lako obezbediti ako vaša organizacija radi uglavnom u klaudu. Ako koristitite Google Docs ili Microsoft 365, uopšte vam nije potrebno mnogo desktop aplikacija - besplatni editori dokumenata i tabela su sasvim dovoljni za gotovo sve potrebe.

Još jedna opcija, ako imate tehnički potkovano osoblje, je da instalirate besplatni Linux operativni sistem (open source alternativa Windows i Mac operativnim sistemima) na svim kompjuterima. Jedna popularna, laka za upotrebu Linux opcija je Ubuntu. Bez obzira na to koji operativni sistem odaberete, postarajte se da neko u organizaciji bude zadužen za to da redovno sa osobljem proverava da li su ažurirali sve što treba.

Kada odlučujete o novom alatu ili sistemu, razmotrite kako ga vaša organizacija može tehnički i finansijski podržati na duži rok. Postavite sebi pitanja poput: Možete li da priuštite i zadržite osoblje potrebno da ga bezbedno održavate? Možete li da platite obnavljanje pretplate? Da li imate pristup popustima od organizacija kao što je pomenuti TechSoup? Odgovaranje na ova pitanja može vam pomoći da vaše softverske i tehnološke strategije budu uspešnije tokom vremena.



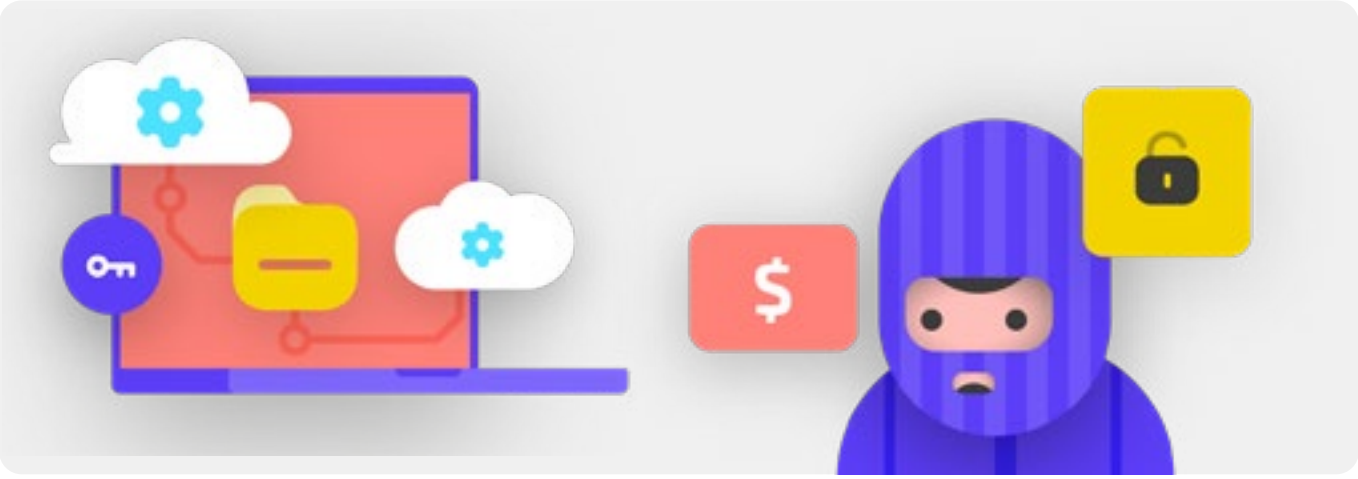
Zaštita uređaja

- **Obučite osoblje o rizicima malvera i najboljim načinima da se isti izbegnu.**
  - Formulišite politike o povezivanju na eksterne uređaje, kliktanju na linkove, skidanju fajlova i aplikacija i proveri dozvola koje softver i aplikacije zahtevaju.
- **Uvedite obavezu redovnog ažuriranja uređaja, softvera i aplikacija.**
  - Kad god je to moguće uključite automatsko ažuriranje.
- **Postarajte se da svi uređaji koriste legalni softver.**
  - Ukoliko je trošak preveliki, prebacite se na besplatnu alternativu.
- **Zahtevajte zaštitu lozinkama na svim uređajima organizacije, uključujući lične mobilne telefone koji se koriste za poslovnu komunikaciju.**
- **Uključite enkripciju celog diska na svim uređajima.**
- **Često podsećajte osoblje da pazi na fizičku bezbednost svojih uređaja - i vodite računa o bezbednosti u poslovnim prostorijama tako što ćete ugraditi brave i zaključavati kompjutere.**
- **Ne delite fajlove preko USB-a ili ne uključujte USB-ove u svoje kompjutere**
  - Umesto toga koristite alternativne bezbedne opcije za deljenje fajlova.

Fišing: Uobičajena pretnja za uređaje i naloge

Fišing (phishing) predstavlja najuobičajeniji i najdelotvorniji napad na organizacije širom sveta. Ovu tehniku koriste i najsofisticiranije državne vojne mašinerije i sitni prevaranti.

Pecanje, jednostavno rečeno, je kad protivnik pokušava da vas prevari da podelite informacije koje se mogu koristiti protiv vas ili vaše organizacije. Mogu vas pecati preko mejlova, SMS-a (to se često naziva i smishing), aplikacija za slanje poruka poput WhatsApp-aporuka ili postova na društvenim mrežama ili telefonskih poziva (to se pak naziva vishing, što je kovanica sastavljena od engleskih reči za glasovni poziv i pecanje). Fišing poruke mogu pokušati da vas navedu da ukucate osetljive informacije (poput lozinki) na lažnoj internet stranici da bi dobili pristup nalogu, da vas pitaju da podelite lične podatke (poput broja kreditne kartice) putem poziva ili poruka, ili vas ubede da skinete malver (zlonamerni softver) koji može da zarazi vaš uređaj. Evo prostog netehničkog primera - svaki dan milioni ljudi dobijaju lažne automatske pozive koji im saopštavaju da je njihov bankovni račun napadnut ili da im je identitet ukraden - sve kako bi ih prevarili da odaju osetljive podatke.



KAKO IDENTIFIKUJEMO FIŠING (PHISHING)?

Može delovati da je nemoguće otkritifišing ,ali postoje neki jednostavni koraci koje svako u vašoj organizaciji može da preuzme kako biste se zaštitili od većine napada. Sledeći konkretni saveti za odbranu od fišinga su prilagođeni i preuzeti iz detaljnog vodiča o fišingu (phishing) koji je napisala Freedom of the Press Foundation (Fondacija za slobodu štampe) i koje treba da podlite sa ostalima u vašoj organizaciji (i drugim kontaktima) i integrišete u svoj bezbednosni plan:

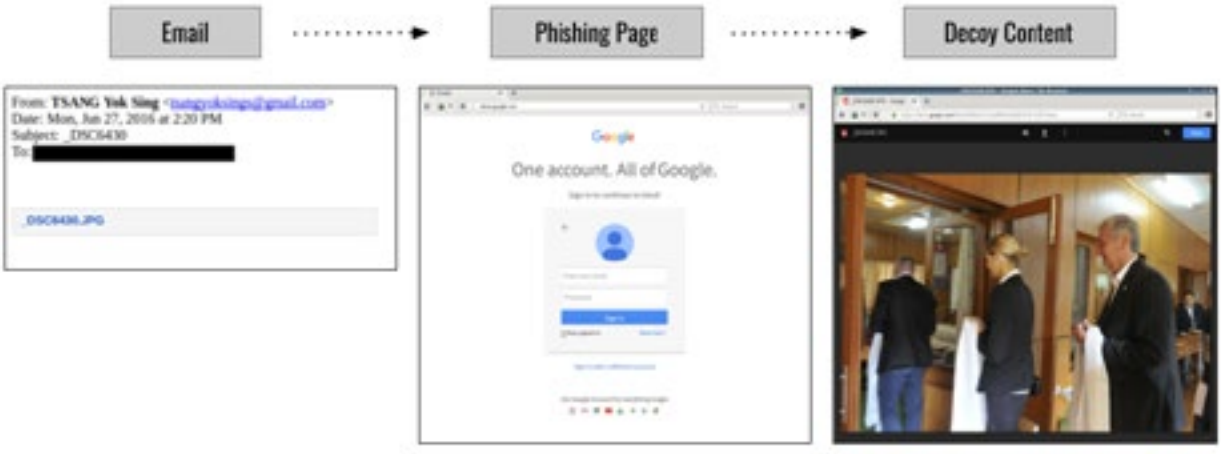
Ponekad vas „od“ polje laže

Budite svesni da „od“ polje u vašim mejlovima može da bude lažirano ili krivotvoreno kako bi vas prevarili. Uobičajena praksa „fišera“ je da naprave imejl adresu koja jako liči na onu legitimnu koju poznajete i od koje se sasvim malo razlikuje kako bi vas prevarili. Na primer, možda primite mejl od nekoga sa adrese „john@goooogle.com“ umesto sa „john@google.com“. Primetite da reč google ima više dodatnih o slova. Možda takođe poznajete nekoga sa adresom „john@gmail.com“, ali primite fišing mejl sa lažne adrese „johm@gmail.com“ - koja se razlikuje samo po jednom slovu. Uvek obavezno dvaput proverite da vam je adresa sa koje je mejl stigao poznata pre nego što ga otvorite. Slično važi i za fišing preko aplikacija za pozive ili poruke. Ako dobijete poruku sa nepoznatog broja, dvaput razmislite pre nego što odgovorite na tu poruku ilil kliknete na nešto u njoj.

Pecanje (phishing) i civilno društvo

Sofisticirani, personalizovani fišing napadi su svakodnevno usmereni protiv grupa civilnog društva u celom svetu.

Jedan primer takvog napada je opisan u izveštaju organizacije Citizen Lab iz 2018. pod nazivom Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community. (Jeftino špijuniranje: Unutar fišing operacije protiv članova tibetanske zajednice). Ovaj veoma jeftin i jednostavan - a opet neverovatno delotvoran fišing napad je bio usmeren protiv tibetanskih branitelja ljudskih prava i drugih aktivista. Napad je počeo sa fišing mejlom (na levoj strani) sa standardne gmail adrese koja je sadržala samo link ka slici. Kad biste kliknuli na taj link, odveo bi vas na lažnu stranicu za prijavljivanje na gmail (u sredini) koja je upotreljena za krađu akreditiva naloga. Ukoliko bi žrtva unela svoje akreditive na lažnoj stranici, njihovi nalozi bi lako bili provaljeni. Nakon što bi žrtva unela svoje korisničko ime i lozinku na lažnom sajtu, bila bi preusmerena na sliku (na desnoj strani) koja pokazuje delegate na jednom tibetanskom sastanku. Slika je ubačena kako bi žrtve zavarala da su se stvarno prijavili na svoj pravi Google nalog i razvejale bilo kakve sumnje o stvarnoj zlonamernoj prirodi mejla.



Čuvajte se priloga u mejlovima

Prilozi mogu da sadrže malvere i viruse, i obično se nalaze u fišing mejlovima. **Najbolji način da izbegnete malver u prilozima jeste da ih nikad ne skidate.** Po pravilu ne otvarajte odmah nijedan prilog, naročito ako je stigao od ljudi koje ne poznajete. Ukoliko je to moguće, pitajte osobu koja vam je poslala dokument da kopi-pejstuje tekst u mejl ili da podeli taj dokument sa vama preko platformi tipa Google Drive ili Microsoft OneDrive, koje imaju ugrađeno skeniranje svih dokumenata koje postavite (upload) na njih. Izgradite organizacionu kulturu gde se slanje priloga obeshrabruje.
Ako apsolutno morate da otvorite prilog, trebalo bi da to uradite u bezbednom okruženju (vidite odeljak sa naprednim lekcijama u nastavku teksta) gde potencijalni malver ne može da zarazi vaš uređaj.
Ako koristite Gmail i primite prilog u mejlu, umesto da ga skinete i otvorite na svom kompjuteru, prosto kliknite na fajl u prilogu i pročitajte ga u pretraživaču (browser) Ovaj korak vam dozvoljava da vidite tekst i sadržaj fajla a da ga ne skinete i samim tim mu ne omogućite da učita potencijalni malver na vaš kompjuter. Ovo je moguće za Word dokumente, pdf-ove pa čak i prezentacije sa slajdovima. Ako morate da uređujete ili menjate dokument, razmislite da fajl otvorite u klaud programu kao što je Google Drive i konvertujete fajl u Google Doc ili Google Slides formate.
Ako koristite Outlook, možete na sličan način da imate uvid u priloge, a da ih ne skinete sa Outlook-ovog mrežnog klijenta. Ako morate da uređujete ili menjate prilog, razmislite da ga otvorite u OneDrive-u ako vam je to dostupno. Ako koristite Yahoo Mail, važi isti koncept. Ne skidajte priloge, već ih pregledajte u svom pretraživaču.

Bez obzira na to kakve alatke imate na raspolaganju, najbolji pristup je da prosto nikad ne skidate priloge od pošiljalaca koje ne poznajete ili kojima ne verujete. I bez obzira nas to koliko važno jedan prilog izgleda, nikad ne otvarajte nešto sa tipom fajla koji vam je nepoznat i koji nikad ne nameravate da koristite.

Odbrana od fišinga (phishing) za vašu organizaciju

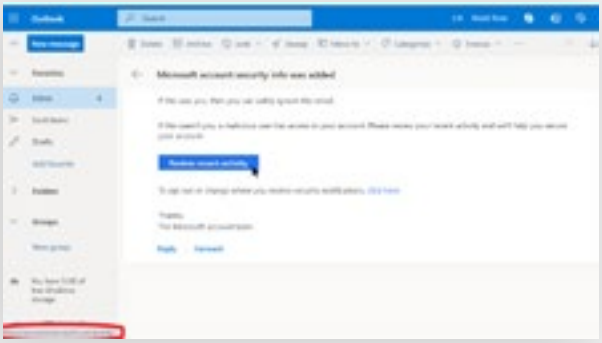
Ako vaša organizacija koristi poslovni Microsoft 365 za imejl i druge aplikacije, vaš administrator domena bi trebalo da oformi politiku bezbednih priloga kako bi ste se zaštitili od opasnih priloga. Ako koristite poslovni Google Workspace (prethodno poznat kao GSuite), postoji slična delotvorna opcija koju bi vaš administrator trebalo da podesi pod nazivom Google Security Sandbox. Napredniji pojedinačni korisnici mogu da razmotre podešavanje sendboks programa kao što su DangerZone ili, za one sa pro ili poslovnom verzijom, Windows Sandbox.

Još jedna napredna opcija čije uvođenje možete razmotriti jeste bezbedna usluga za filtriranje sistema imena domena (DNS). Organizacije mogu koristiti ovu tehnologiju da spreče osoblje da slučajno pristupi zlonamernom sadržaju, obezbeđujući dodatni nivo zaštite od fišinga (phishing). Iako je ranije takva tehnologija zahtevala poseban tim internih IT stručnjaka, novi servisi kao što je Cloudflare Gateway obezbeduju takve funkcije za manje tehnološki sofisticirane organizacije bez potrebe za velikim sumama novca (tako je npr. Gateway, besplatan za do 50 korisnika). Dodatni besplatni instrumenti, uključujući i Quad9 iz paketa alatki Globalne sajber alijanse će vam blokirati pristup internet stranicama za koje se zna da sadrže viruse ili drugi malver i moguće ih je primeniti za manje od pet minuta.

Oprezno klikćite

Budite oprezni kad vidite linkove u mejlovima ili drugim porukama. Linkovi mogu biti zamaskirani tako da ne shvatite da ćete skinuti zlonamerne fajlove ili da će vas odvesti na lažne internet stranice koje vam mogu tražiti lozinke ili druge osetljive informacije. Kada radite na kompjuteru postoji jednostavan trik da se uverite da će vas link zaista odvesti tamo gde treba: stavite strelicu kursora na link pre nego što ga kliknete i u dnu pretraživača ćete videti njegovu stvarnu internet adresu (vidite donju sliku).

Na mobilnim uređajima je teže ovako proveravati linkove a da slučajno ne kliknete na njih, zato budite oprezni. Ali na većini pametnih telefona možete da proverite gde link vodi tako što ćete ga držati dugo pritisnut dok ne iskoči puna adresa.
Kod fišinga (phishing) preko SMS-a i aplikacija za slanje poruka, kao uobičajeni način za maskiranje prave adrese (URL-a) se koriste skraćeni linkovi. Ako vidite skraćeni link (kao što su na primer bit.ly ili tinyurl.com) umesto punog URL-a, nemojte ga kliknuti. Ukoliko je link važan kopirajte ga u program za proširenje URL-a, kao što je https://www.expandurl.net/, kako biste videli pravo odredište skraćenog URL-a. Štaviše, ne klikajte na linkove koji vode na internet sajtove koji su vam nepoznati. Ukoliko niste sigurni šta da radite, unesite u pretraživač ime internet sajta pod navodnicima (npr: „www.badwebsite.com“) da vidite da li je u pitanju legitimna stranica. Potencijalno sumnjive linkove takođe možete proveriti VirusTotal-ovim skenerom internet adresi. On nije 100% tačan, ali je dobra mera predostrožnosti.
Konačno, ako kliknete na bilo koji link u poruci i od vas se traži da se prijavite na neki nalog, nemojte to učiniti osim ako niste 100 posto sigurno da je imejl legitiman i da vas šalje na odgovarajući sajt. Mnogi pecaroški napadi daju linkove koji vas šalju na lažne stranice za prijavljivanje na Gmail, Facebook ili druge popularne sajtove. Nemojte da vas prevare. Uvek možete otvoriti novi prozor u pretraživaču ili sami otići direktno na sajt koji vam je poznat kao npr. Gmail.com, Facebook.com itd. ukoliko želite ili morate da se prijavite. Na taj način ćete takođe bezbedno stići do sadržaja - ako je uopšte bio legitiman.



Šta treba da radimo kad dobijemo fišing poruku?

Ako iko u vašoj organizaciji dobije prilog u mejlu, link ili sliku koje nije tražio, ili uopšte sumnjvu poruku ili poziv, važno je da to odmah prijave osobi koja je zadužena za IT bezbednost. Ako još uvek nemate takvu osobu, trebalo bi da je postavite u toku razvoja svog bezbednosnog plana. Osoblje takođe može da prijavi spem ili pecaroški mejl direktno Gmail-u ili Outlook-u. Od suštinskog značaja je da isplanirate šta osoblje ili pojedinci treba da urade ako/kada prime potencijalnu pecarošku poruku. Pored toga, preporučujemo da usvojite ove dobre prakse po pitanju pecanja - da ne klikate na sumnjive linkove, izbegavate priloge i proveravate „od“ polje - te ove prakse podelite sa kolegama, najbolje preko komunikacionog kanala u širokoj upotrebi. To pokazuje da vam je stalo do ljudi sa kojima komunicirate i podstiče kulturu opreza i upoznatosti sa opasnostima fišinga u svim vašim mrežama. Vaša bezbednost zavisi od organizacija kojima verujete, i obrnuto. Bolje prakse štite sve.
Pored prenošenja gorenavedenih konkretnih saveta svim kolegama i volonterima, možete takođe da vežbate identifikovanje fišing (phishing) uz pomoć Google-ovog pecaroškog kviza. Takođe toplo preporučujemo da organizujete redovne obuke iz oblasti pecanja (phishing) za osoblje kako biste proverili nivo svesti i postarali se da svi budu na oprezu. Takva obuka može biti deo redovnih sastanaka ili se organizovati malo nezvaničnije. Ono što je bitno jeste da nikom u organizaciji ne bude neprijatno da postavlja pitanja o fišingu, prijavi fišing (čak i kad misle da su možda pogrešili tako što su kliknuli link), kao i da svi budu osposobljeni da pomognu u odbrani vaše organizacije protiv ove veoma verovatne pretnje sa ozbiljnim efektima.

Fišing (phishing)

- **Redovno obučavajte osoblje o tome šta je fišing , kako ga primetiti i kako se odbraniti od njega, uključujući fišing preko SMS-ova, aplikacija za slanje poruka, i telefonskih poziva, ne samo mejlova.**
- **Često podsećajte osoblje na najbolje prakse kao što su:**
  - **Nemojte skidati nepoznate i potencijalno sumnjive priloge mejlova.**
  - **Proverite URL linka pre nego što kliknete. Ne klikajte na nepoznate i potencijalno sumnjive linkove.**
  - **Ne delite osetljive ili lične informacije preko mejla, SMS-a ili telefonskog poziva sa nepoznatim ili nepotvrđenim adresama ili ljudima.**
- **Podstaknite prijavljivanje fišinga (phishing).**
  - **Upostavite mehanizam za prijavljivanje i odredite osobu kojoj se osoblje može obratiti u slučaju fišinga u okviru vaše organizacije.**
  - **Nagradite prijavljivanje i nemojte kažnjavati neuspeh.**

Bezbedna komunikacija i skladištenje podataka

Komunikacije i deljenje podataka

Kako biste doneli najbolju moguću odluku o tome kako da komunicirate u ovkiru vaše organizacije, od suštinskog je značaja da razumete različite vrste zaštite koje naša komunikacija može imati i zašto je takva zaštita bitna.

Ono što je jedan od najvažnijih elemnata svake komunikacije je da sadržaj vaših poruka ostane tajan - što u moderno doba uglavnom rešava enkripcija. Bez odgovarajuće enkripcije, raznovrsni protivnici mogu pristupiti privatnim razgovorima. Nebezbedna komunikacija može dovesti do otkrivanja osetljivih informacija i poruka, otkriti lozinke ili druge privatne podatke i potencijalno dovesti vaše osoblje ili organizaciju u opasnost u zavisnosti od prirode vaše komunikacije i sadržaja koji delite.

Bezbedne komunikacije i civilno društvo

Hiljade aktivista i organizacija za odbranu demokratije i ljudskih prava se svakodnevno oslanjaju na bezbedne kanale za komunikaciju kako bi sačuvali tajnost razgovora u problematičnim političkim okruženjima. Bez takvih bezbednosnih praksi, vlasti mogu presresti osetljive poruke i iskoristiti ih da identifikuju aktiviste i razbiju proteste. Jedan prominentan i dobro dokumentovan primer ovakve situacije se desio nakon izbora 2010. godine u Belorusiji. Kao što je detaljno predstavljeno u izveštaju organizacije Amnesty International, vlada je prisluškivala telefonske razgovore i druge nezaštićene komunikacione kanale i koristila ih na sudu protiv prominentnih opozicionih političara i aktivista, od kojih su mnogi proveli više godina u zatvoru. Tokom novog talasa postizbornih protesta u Belorusiji tokom 2020. hiljade demonstranata je instaliralo bezbedne aplikacije za slanje poruka koje su lake za korišćenje, a koje samo pre deset godina nisu bile dostupne svima, kako bi zaštitili svoje osetljive razgovore.

ŠTA JE ENKRIPCIJA I ZAŠTO JE BITNA?

Enkripcija je matematički proces koji se koristi za šifrovanje poruke ili fajla kako bi samo jedna osoba ili telo koje ima ključ moglo da ih dešifruje i pročita. Bez enkripcije, naše poruke su na izvol'te potencijalnim protivnicima, uključujući pružaocima usluga mobilne telefonije ili internetskih usluga (ISP), neoprijateljski raspsoloženim vladama ili hakerima na netu. Surveillance Self-Defense Guide (Vodič za samoodbranu od nadzora) organizacije Electronic Frontier Foundation pruža praktično objašenjenje enkripcije (sa slikama):

Nešifrovane poruke

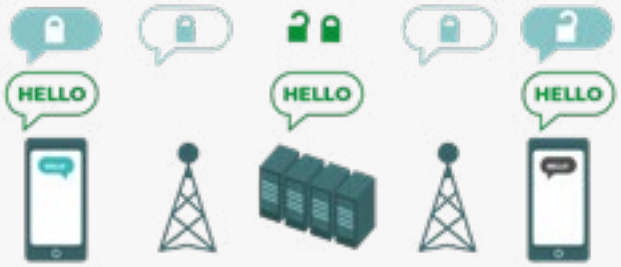
Bez ikakvog šifrovanja, svi koji učestvuju u prenošenju poruke i svako ko može da zaviri dok poruka prolazi, može da pročita njen sadržaj. Ovo možda nije bitno ako je sve što kažete „zdravo", ali može biti velika stvar ako saopštavate nešto privatnije ili osetljivije što ne želite da vaš telekom, ISP, neprijateljska vlada ili bilo koji drugi protivnik vidi. Zbog toga je od suštinskog značaja da izbegavate korišćenje nešifrovanih alata za slanje bilo kakvih osetljivih poruka (i idealno bilo koje poruke uopšte). Imajte na umu da neke od najpopularnijih metoda komunikacije, kao što su SMS i telefonski pozivi, praktično rade bez ikakvog šifrovanja (kao na ovoj slici).

Kao što možete da vidite na gornjoj slici, pametni telefon šalje zelenu, nešifrovanu poruku, („ćao") drugom pametnom telefonu sasvim desno. Usput, bazna stanica mobilne telefonije (ili u slučaju da ste poslali nešto preko interneta vaš pružalac internet usluga) prenosi poruku do firminih servera. Odatle ona skače kroz mrežu do druge bazne stanice, koja može da vidi nešifriranu „ćao" poruku i konačno je preusmerava na odredište. Važno je napomenuti da bez ikakve enkripcije svi koji prenose poruku, i svako ko može da baci pogled dok ona prolazi pored njega, može da pročita njen sadržaj. To možda nije bitno ako kažete samo „ćao", ali moglo bi biti jako bitno ako vaša poruka sadrži neke lične ili osetljive informacije koje ne želite da vide ni telekom, ni pružalac internet usluga, ni neprijateljski nastrojena vlada niti bilo koji drugi protivnik. Zbog toga, od suštinskog je značaja da izbegavate upotrebu nešifriranih alatki za slanje bilo kakvih osetljivih poruka (i idealno, bilo kakvih poruka uopšte), Imajte na umu da neki od najpopularnijih metoda komunikacije - poput SMS-ova i telefonskih poziva - praktično funkcionišu bez bilo kakve enkripcije (kao na gornjoj slici).

Postoje dva načina za enkripciju podataka u pokretu: enkripcija u transportu i obostrana enkripcija. Važno je da znate koju vrstu enkripcije određeni pružalac usluga podržava kad budete morali da ga izaberete u cilju bezbednijih komunikacionih praksi. Takve razlike su dobro opisane u [Surveillance Self-Defense Guide] (Vodiču za samodbranu od nadzora) iz kojeg smo preuzeli i adaptirali neke informacije:

Enkripcija u transportu

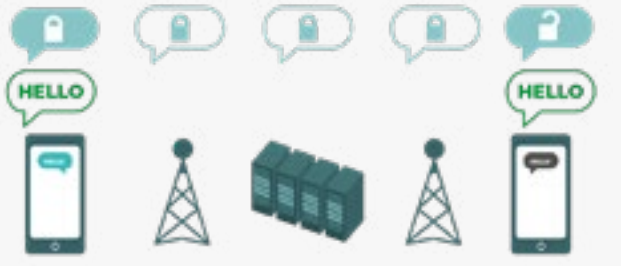
Enkripcija u transportu, poznata i kao i Transport Layer Security (TLS), štiti poruke dok putuju od vašeg uređaja do servera aplikacije/servisa za slanje poruka i odatle do uređaja primaoca. Ovo ih štiti od pogleda hakera koji čuče na vašoj mreži ili kod vaših pružalaca telekomunikacionih/internet usluga. Međutim, na sredini ovog puta, vaš pružalac usluga elektronske pošte/poruka, internet stranica koju gledate, ili aplikacija koju koristie mogu da vide nešifrirane primerke vaše poruke. Pošto vaše poruke mogu da vide firmini serveri (na kojima se često i skladište), one mogu biti predate na zahtev policije ili ukradene ako neko provali u servere te firme.



Gornja slika pokazuje primer enkripcije sloja prenošenja. Na levoj strani vidimo pametni telefon koji šalje zelenu, nešifrovanu poruku: „ćao“. Poruka se šifrira a ond a prenosi do bazne stanice, Na sredini vidimo servere koji mogu da dešifruju poruku, pročitaju sadržaj, odluče gde da je pošalju, ponovo je šifruju i pošalju ka sledećoj baznoj stanici na putu ka njenom odredištu. Na kraju, drugi pametni telefon prima šifrovanu poruku i dešifruje je kako bismo opet dobili: „ćao“.

Obostrana enkripcija

Obostrana enkripcija (end-to-end encryption) štiti poruke u tranzitu celim putem od pošiljaoca do primaoca. Ona se stara da prvobitni pošiljalac pretvori informaciju u tajnu poruku (prva strana) a da je dešifruje samo konačni primalac (druga strana). Niko, uključujući aplikacije ili servise koje koristite, ne može da nadzire i prisluškuje vašu aktivnost.



Gornja slika predsatvlja primr obostrane enkripcije. Na levoj strani, vidimo pametni telefon koji šalje zelenu, nešifrovanu poruku: „ćao“. Ta porukla se onda šifrira i šalje do bazne stanice mobilne telefonije a onda do servera aplikacije/pružalaca usluge koji ne mogu da pročitaju sadržaj, ali će preneti tajnu poruku do njenog odredišta. Na kraju drugi pametni telefon prima šifrovanu poruku i dešifruje je kako bi se dobilo: „ćao“. Za razliku od enkripcije sloja prenošenja, vaš pružalac internet usluga ili usluga slanja poruka nije u stanju da dešifruje poruku. Samo početna i konačna strana (oni uređaji koji šalju i primaju šifrovane poruke) imaju ključ za dešifrovanje i čitanje poruke.

KAKVA VRSTA ENKRIPCIJE NAM JE POTREBNA?

Kada odlučujete da li je vašoj organizaciji potrebna enkripcija sloja prenošenja ili obostrana enkripcija za vaše komunikacije glavno pitanje koje treba da si postavite se tiče poverenja. Na primer, da li imate poverenja u aplikaciju ili pružaoca usluga koje koristite? Da li imate poverenja u njihovu tehničku infrastrukturu? Da li vas brine mogućnost da neprijateljski raspoložena vlada primora ove kompanije da predaju vaše poruke - i ako je tako, da li imate poverenja u politike tih kompanija da je zaštite od zahteva policije i tužilaštva?

Ako je odgovor na bilo koje od ovih pitanja „ne“, onda vam treba obostrana enkripcija. Ako je odgovor „da“ onda vam može biti dovoljna enkripcija u transportu, ali je generalno bolje odmah preći na usluge koje nude obostranu enkripciju.

Prilikom slanja grupnihporuka, imajte na umu da bezbednost vaših poruka zavisi od bezbednosti svih primalaca. Tako da je, pored pažljivog odabira bezbednih aplikacija, podjednako važno da se svako u grupi pridržava najboljih praksi sa aspekta bezbednosti naloga i uređaja. Dovoljno je da samo jedna osoba izneveri vaše poverenje ili da samo jedan uređaj bude zaražen i sadržaj celog grupnog četa ili poziva može biti obelodanjen.

KAKVE ALATKE ZA OBOSTRANU ENKRIPCIJU PORUKA TREBA DA KORISTIMO?

Ako morate da koristite obostranu enkripciju ili samo želite da usvojite najbolje prakse bez obzira na nivo pretnji sa kojima se vaša organizacija suočava, evo nekih primera pouzdanih alatki koje trenutno nude uslugu obostranog šifrovanja poruka i poziva. Ovaj odeljak priručnika će se redovno ažurirati u verziji na internetu, ali imajte na umu da se stvari jako brzo menjaju u svetu bezbednog slanja poruka tako da ove preporuke mogu da zastare do momenta kad vi budete čitali ovaj odeljak. Takođe imajte na umu da bezbednost vaših komunikacija direktno zavisi od bezbednosti fizičkih uređaja. Tako da pored usvajanja praksi bezbednog slanja poruka, treba da primenite i najbolje prakse na polju bezbednosti uređaja date u ovom priručniku.

Preporučene alatke za obostrano šifrovanu komunikaciju

TEKSTUALNE PORUKE (POJEDINAČNE ILI GRUPNE)	• **Signal** • **WhatsApp (samo sa specifičnim podešavanjima koja su opisana u nastavku teksta)**
AUDIO I VIDEO POZIVI	• **Signal (do 40 osoba)** • **WhatsApp (do 32 osoba na zvuku, osam na videu)**
DELJENJE FAJLOVA	• **Signal** • **Keybase / Keybase Teams** • **OnionShare + aplikacija za obostrano šifrovano slanje poruka kao što je Signal**

ŠTA SU METAPODACI I DA LI TREBA DA NAS BRINU?

Sa kim vi i vaše osoblje razgovarate i kad i gde razgovarate sa njima može ponekad biti podjednako osetljivo kao i sama tema razgovora. Važno je zapamtiti da obostrana enkripcija štiti samo sadržaj (ono „šta“) vaše komunikacije. Tu metapodaci ulaze u priču. Već pominjani **Surveillance Self-Defense Guide** (Vodič za samoodbranu od nadzora) daje pregled metapodataka i njihovog značaja za organizacije (uključujući i objašnjenje kako metapodaci izgledaju):

Metapodaci se često opisuju kao sve sem sadržaja vaše komunikacije. Metapodatke možete da zamislite kao digitalni ekvivalent koverte. Kao što koverta sadrži podatke o pošiljaocu, primaocu i odredištu poruke, tako to isto sadrže i metapodaci. Metapodaci su informacije o digitalnim komunikacijama koje šaljete i primate.

Neki od primera metapodataka su:
- sa kime komunicirate
- naslov mejlova
- dužina razgovora
- vreme odigravanja komunikacije
- vaša lokacija tokom komuniciranja

Čak i mali uzorak metapodataka može da pruži dubinski uvid u aktivnosti vaše organizacije. Hajde da vidimo šta sve metapodaci koje prikupe mogu da kažu hakerima, državnim organima i kompanijama:

Znaju da ste zvali određenog novinara i pričali sa njim sat vremena pre nego što je objavio priču u kojoj citira „anonimni izvor“. Ali ne znaju o čemu ste pričali.

Znaju da je više ljudi iz vaše organizacije slalo poruke poznatom lokalnom pružaocu obuke iz oblasti digitalne bezbednosti. Ali tema poruka je ostala tajna.

Znaju da ste dobili mejl od centra za testiranje na COVID, potom zvali vašeg lekara, pa potom posetili sajt SZO i to sve u toku jednog sata. Ali ne znaju šta je pisalo u mejlu niti šta ste rekli preko telefona.

Znaju da ste od lokalne grupe za ljudska prava primili mejl sa naslovom „Recite Vladi: prestanite da zloupotrebljavate svoju moć“. Ali ne vide sam sadržaj mejla.

Metapodaci nisu zaštićeni enkripcijom koju nudi većina aplikacija za slanje poruka. Tako da ako, npr, šaljete poruku preko WhatsApp-a, imajte na umu da iako je sadržaj vaše poruke obostrano šifrovan, drugi i dalje mogu da saznaju koje poruke šaljete, koliko često, a u slučaju telefonskih poziva koliko isti traju. Zbog toga bi možda trebalo da imate na umu potencijalne rizike (ako uopšte postoje) povezane sa time što određeni protivnici mogu da saznaju sa kime vaša organizacija razgovara, kada ste s njima pričali i (u slučaju mejlova) glavne teme vašeg dopisivanja.

Jedan od razloga što svi preporučuju **Signal** je upravo to što je pored obostrane enkripcije **uveo fukcionalnosti koje treba da smanje količinu metapodataka koje evidentira i skladišti.** Na primer, njegova Sealed Sender funkcija šifrira metapodatke o tome ko priča sa kime, tako da Signal zna samo ko prima poruku, ali ne i ko je šalje. Po podrazumevanom podešavanju, ova funkcija radi samo tokom komunikacije sa postojećim kontaktima ili profilima (osobama) sa kojima ste već komunicirali ili koji su u vašoj listi kontakata. Međutim, možete je podesiti na „Dozvoli od bilo koga“ ukoliko vam je bitno da eliminišete ove metapodatke iz svih razgovora u okviru Signala, čak i onih sa nepoznatim ljudima.

ŠTA JE SA IMEJLOM?

Većina provajdera elektronske pošte, na primer Gmail, Microsoft Outlook i Yahoo Mail, koriste šifrovanje transportnog sloja. Dakle, ako morate da komunicirate osetljiv sadržaj koristeći elektronsku poštu i brinete se da bi od vašeg provajdera moglo biti zakonski zahtevano da pruži informacije o vašoj komunikaciji vladi ili drugom licu, možda ćete želeti da razmislite o korišćenju elektronske pošte sa opcijom šifrovanja “end to end”. Imajte na umu, međutim, da čak i opcije šifrovane “end to end” elektronske pošte ostavljaju nešto što se želi iz bezbednosne perspektive, na primer, nešifrovanje naslova elektronske pošte i nemanje zaštite metapodataka. Ako je potrebno da saopštite posebno osetljive informacije, elektronska pošta nije najbolja opcija. Umesto toga, odlučite se za bezbedne opcije za razmenu poruka kao što je Signal.

Ako vaša organizacija nastavi da koristi elektronsku poštu, od ključne je važnosti da usvojite sistem na nivou cele organizacije. Ovo vam pomaže da ograničite uobičajene rizike koji nastaju kada osoblje koristi lične adrese elektronske pošte za svoj rad, kao što su loše bezbednosne prakse naloga. Na primer, pružanjem naloga elektronske pošte koje izdaje organizacija osoblju, možete da primenite najbolje prakse kao što su jake lozinke i 2FA na svim nalozima kojima vaša organizacija upravlja. Ako je, prema vašoj gornjoj analizi, end-to-end enkripcija neophodna za vašu elektronsku poštu, i Protonmail i Tutanota nude planove za organizacije. Ako je šifrovanje na transportnom sloju adekvatno za elekttonsku poštu vaše organizacije, opcije kao što su Google Workspace (Gmail) ili Microsoft 365 (Outlook) mogu biti korisne.

DA LI ZAISTA MOŽEMO DA VERUJEMO WHATSAPP-U?

WhatsApp je popularan izbor za bezbedno slanje poruka i može biti dobra opcija imajući u obziru njegovu sveprisutnost. Neke brine činjenica da je u vlasništvu i pod kontrolom Facebook-a, koji radi na tome da ga integriše sa svojim drugim sistemima. Takođe postoji zabrinutost oko količine metapodataka (tj. podataka o tome sa kim komunicirate i kada) koje WhatsApp prikuplja. Ako se odlučite za WhatsApp kao opciju za bezbedno slanje poruka, obavezno pročitajte gornji odeljak o metapodacima. Takođe je neophodno da pravilno konfigurišete određena podešavanja. Ono što je najbitnije jeste da isključite bekape na klaudu, ili, u najmanju ruku, omogućite WhatsApp-ovu novu end-to-end šifrovanu funkciju rezervnih kopija koristeći ključ za šifrovanje od 64 cifre ili dugu, slučajnu i jedinstvenu lozinku sačuvanu na bezbednom mestu (kao što je vaš menadžer lozinki). Takođe obavezno uključite bezbednosna obaveštenja i proverite bezbednosne kodove Možete naći jednostavne praktične vodiče za ova podešavanja ovde za android telefone, a ovde za ajfon. Ukoliko vaše osoblje *i oni sa kojima komunicirate* ne podese ovo kako treba, onda ne bi trebalo da WhatsApp smatrate dobrom opcijom za slanje osetljivih informacija koje zahtevaju obostranu enkripciju. Signal i dalje ostaje najbolja opcija za slanje poruka sa obostranom enkripcijom uzimajući u obzir njegova bezbedna podrazumevana podešavanja i zaštitu metapodataka.

A ŠTA JE SA SMS-OVIMA?

Bazične tekstualne poruke su jako nebezbedne (standardni SMS-ovi suštinski nemaju enkripciju) i trebalo bi ih izbegavati za bilo šta što ne želite da svi znaju. Dok Apple-ove poruke sa jednog ajfona na drugi (tzv. iMessage) imaju obostranu enkripciju, ako u tom razgovoru učestvuje telefon koji nije ajfon, poruke nisu bezbedne. Najbolje je obezbediti se i **izbegavati slanje SMS-ova za bilo šta što je i izdaleka osetljivo, privatno i poverljivo.**

ZAŠTO SETELEGRAM, FACEBOOK MESSENGER ILI VIBER NE PREPORUČUJU ZA BEZBEDNO ČETOVANJE?

Neke aplikacije, poput Facebook Messenger-a i Telegrama, nude obostranu enkripciju samo ako je namerno uključite (a i to samo za četove između dve osobe), pa nisu dobra opcija za osetljive i privatne poruke, naročito za potrebe organizacije. Nemojte se oslanjati na ove alatke ako vam treba obostrana enkripcija, jer je lako zaboraviti da promenite podrazumevana, manje bezbedna podešavanja. Viber tvrdi da nudi obostranu enkripciju, ali nije svoj kod stavio na uvid nezavisnim revizorima digitalne bezbednosti. Telegramov kod takođe nije dostupan za javnu reviziju. Usled toga, mnogi stručnjaci se pribojavaju da Viberova enkripcija ili Telegramovi „tajni" četovi zapravo ne ispunjavaju postojeće standarde i samim tim nisu adekvatni za komunikaciju koja zahteva pravu obostranu enkripciju.

NAŠI SARADNICI I KOLEGE KORISTE DRUGE APLIKACIJE ZA SLANJE PORUKA - KAKO DA IH UBEDIMO DA SKINU JOŠ JEDNU APLIKACIJU DA BI KOMUNICIRALI SA NAMA?

Ponekad bezbednost zahteva dodatne napore, ali u slučaju osetljivih komunikacija to vredi truda. Dajte dobar primer osobama sa kojima ste u kontaktu. Ako morate da koristite druge, manje bezbedne sisteme, dobro pazite šta na njima govorite. U nekim organizacijama koriste jedan sistem za generalno četovanje i drugi za najpoverljivije razgovore sa rukovodstvom. Naravno, najjednostavnije je ako sve stalno automatski šifruje - onda ne morate ništa da pamtite ili da se razmišljate.

Na sreću, aplikacije sa obostranom enkripcijom poput Signala su sve popularnije i sve lakše za upotrebu, a da ni ne pominjemo da su već lokalizovane na desetinama jezika. Ako vašim partnerima ili drugim kontaktima treba pomoć pri prelasku na opciju sa obostranom enkripcijom poput Signala, odvojte malo vremena da im objasnite zašto je bitno da adekvatno zaštite svoje komunikacije. Jednom kad svi shvate značaj ovakve prakse, neće im smetati da odvoje nekoliko minuta za skidanje nove aplikacije i utroše nekoliko dana da se naviknu na nju.

DA LI POSTOJE DRUGA PODEŠAVANJA APLIKACIJA SA OBOSTRANOM ENKRIPCIJOM ZA KOJA TREBA DA ZNAMO?

U okviru Signala je takođe važno da verifikujete bezbednosne šifre (koje oni zovu bezbednosni brojevi). Kako biste videli bezbednosni broj i verifikovali ga u Signalu, možete otvoriti čet sa nekim kontaktom, kucnuti njihovo ime na vrhu ekrana i na dnu padajućeg menija naći „Prikaži bezbednosni broj". Ukoliko taj broj odgovara broju vašeg kontakta možete ga označiti kao „proverenog" na tom istom ekranu. Naročito je bitno da pazite na te bezbednosne brojeve i proverite svoje kontakte ukoliko u četu dobijete poruku da se bezbednosni broj koji se odnosi na dati kontakt promenio. Ukoliko vama ili ostatku osoblja treba pomoć oko ovih podešavanja, sam Signal je obezbedio korisna uputstva.

Ako koristite Signal koji se univerzalno smatra najboljom opcijom za bezbedno slanje poruka i pojedinačne pozive koja je istovremeno laka za upotrebu, takođe obavezno smislite jak pin. Neka sadrži bar šest cifara i nemojte stavljati nešto što se lako da pogoditi, poput datuma rođenja.

Za više praktičnih saveta o pravilnom podešavanju Signala i WhatsApp-a, možete pogledati vodiče za obe ove aplikacije u okviru Vodiča za samoodbranu od nadzora.

Upotreba aplikacija za četovanje u stvarnom svetu

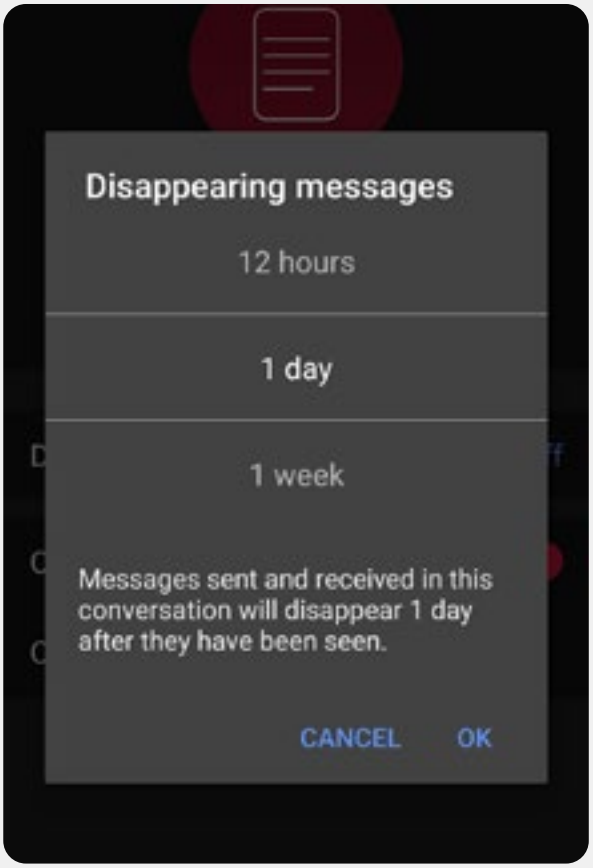
Kako bi se ograničila šteta u slučaju krađe, gubljenja ili konfiskacije telefona, najbolje je da maksimalno smanjite istoriju poruka koje čuvate na telefonu. Lak način da to uradite je da uključite „**samonestajuće poruke**“ za grupne četove vaše organizacije, i da podstaknete osoblje da isto učine i u slučaju svojih privatnih četova.

U Singalu i drugim popularnmi aplikacijama za slanje poruka možete podesiti tajmer gde poruke nestaju u roku od određenog broja minuta ili sati nakon čitanja. Ovo podešavanje se može prilagoditi svakom pojedinačnom ili grupnom četu. U slučaju većine od nas, postavljanje tajmera na nedelju dana nam daje sasvim dovoljno vremena da sve prostudiramo dok istovremeno ne čuvamo poruke koje nam nikad neće trebati - ali koje bi potencijalno mogle da se iskoriste protiv nass u budućnosti. Zapamtite, ono što nemate vam ne mogu ni ukrasti.

Kako biste uključili samonestajuće poruke u Signalu, otvorite čet, kucnite ime osobe/grupe sa kojom četujete, kucnite samonestajuće poruke, izaberite rok i pritisnite ok. Slično podešavanje postoji i u WhatsApp-u.

U ozbiljnijim situacijama gde postoji potreba za momentalnim brisanjem poruke, možda zato što je nečiji telefon ukraden ili ste poslali poruku pogrešnoj osobi, znajte da vam Singal dozvoljava da obrišete poruku pojedincu ili grupi sa telefona svih učesnika u četu u roku od tri sata nakon slanja tako što ćete je prosto izbrisati iz četa. Telegram je upravo i popularan u brojnim zemljama uprkos ograničenoj enkripciji zato što ima sličnu funkcionalnost koja dozvoljava korisnicima da neograničeno brišu poruke sa različitih uređaja.

U svakom slučaju, ako je vaša organizacija zabirnuta za bezbednost osoblja zbog poruka ili razgovora koji se mogu videti na njihovim telefonima, onda je najjednostavnija i najodrživija opcija verovatno da koristite samonestajuće poruke sa kratkim rokom.



A ŠTA JE SA VIDEO POZIVIMA U VEĆIM GRUPAMA? DA LI POSTOJE OPCIJE SA OBOSTRANOM ENKRIPCIJOM?

Sa porastom rada na daljinu, važno je imati bezbednu opciju za video pozive u većim grupama. Nažalost, trenutno ne postoji savršena opcija koja bi odgovorila na sve zahteve: da bude laka za upotrebu, da podržava veliki broj korisnika i u startu obezbeđuje obostranu enkripciju.

Za grupe do 40 ljudi, Signal je veoma preporučljiva opcija za end-to-end šifrovanje. Grupnim video pozivima na Signal-u se možete pridružiti ili sa pametnog telefona ili aplikacije Signal za desktop na računaru, što omogućava deljenje ekrana. Imajte na umu, međutim, da samo vaši kontakti koji već koriste Signal mogu biti dodati u grupu Signal.

Ukoliko ste u potrazi za drugim opcijama, jedna od platformi koje su nedavno dodale opciju obostrane enkripcije je Jitsi Meet. Jitsi Meet softversko rešenje za audio-vizuelne konferencije koje se otvara iz pretraživača, može da podrži velike grupe (do 100 osoba) i ne zahteva skidanje bilo kakvih aplikacija ili programa. Imajte na umu da ako koristite ovu funkciju sa velikim grupama (više od 15-20 ljudi) kvalitet poziva može biti slabiji. Kako biste organizovali sastanak na Jitsi Meet, moćete da odete na **meet.jit.si**, ukucate šifru sastanka i podelite link (preko bezbednog kanala kao što je Singal) sa učesnicima. Kako biste korisitili obostranu enkripciju pogledajte **uputstva** koja je Jitsi pružio. Imajte na umu da svaki pojedinačni korisnik mora sam da podesi obostranu enkripciju kako bi funkcionisala za celu grupu. Dok koristite Jitsi, takođe obavezno dajte nasumična imena zasebnim digitalnim prostorijama i koriste jake lozinke za zaštitu svojih poziva.

Ukoliko ova opcija ne odgovara vašoj organizaciji, možete razmotriti korišćenje popularnih komercijalnih opcija kao što su WebEx ili Zoom, samo uključite obostranu enkripciju. WebEx odavno dozvoljava obostranu enkripciju, ali ova opcija nije uključena od početka i zahteva da učesnici skinu WebEx da bi ušli na sastanak. Da biste omogućili opciju obostrane enkripcije za vaš WebEx nalog, morate da otvorite WebEx-ovu stranicu za podršku i pratite **ova uputstva** kako biste podesili obostranu enkripciju. Samo organizator (host) sastanka mora da uključi obostranu enkripciju. Ukoliko to učini, ceo sastanak će imati obostranu enkripciju. Ako koristite WebEx za bezbedne grupne sastanke i radionice, obavezno svoje pozive zaštite jakim lozinkama.

Nakon više meseci medijske kritike, Zoom je uveo **opciju obostrane enkripcije** za svoje pozive. Međutim ta opcija nije od početka uključena, zahteva da organizator sastanka poveže svoj nalog sa telefonskim brojem i funkcioniše samo ako se svi učesnici pridruže preko Zoom mobilne ili desktop aplikacije umesto preko poziva. Pošto je lako pogrešiti prilikom nameštanja ovih podešavanja, ne preporučujemo da se oslanjate na Zoom kao opciju za obostranu enkripciju. Međutim, ako je obostrana enkripcija neophodna, a nemate drugog izbora sem Zoom-a, možete pratiti njegova uputstva za podešavanje. Samo se postarajte da proverite bilo koji poziv pre početka kako biste se uverili da je zaista obostrano šifrovan tako što ćete kliknuti na zeleni katanac u gornjem levom uglu Zoom-ovog ekrana i videti „end-to-end“ (obostrana) napisano pored podešavanja enkripcije. Takođe bi trebalo da sve Zoom sastanke obezbedite jakom lozinkom.

Pored gorenavednih alatki, možete pogledati **ovaj dijagram** koji je napravila organizacija Frontline Defenders i koji navodi neke opcije za video i grupne pozive koje, u zavisnosti od nivoa rizika sa kojim se suočavate, mogu imati smisla za vašu organizaciju.

Međutim, vredi napomenuti da određene popularne karakteristike gore navedenih alata rade samo sa enkripcijom transportnog sloja. Na primer, uključivanje end-to-end enkripcije u Zoom-u onemogućava odvajanje u sobe (breakout rooms), mogućnosti anketiranja (polling) kao i snimanje sa transkripcijom. U Jitsi Meet-u, odvojene sobe mogu da onemoguće funkciju end-to-end šifrovanja, što dovodi do nesvesnog smanjenja bezbednosti

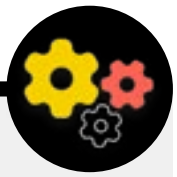
ŠTA AKO VAM STVARNO NE TREBA OBOSTRANA ENKRIPCIJA ZA SVE KOMUNIKACIJE?

Ukoliko na osnovu svoje procene rizika zaključite da vam obostrana enkripcija nije neophodna za sve komunikacije, možete razmotriti korišćenje aplikacija sa zaštitom u obliku enkripcije sloja prenošenja. Imajte na umu da ova vrsta enkripcije zahteva da imate poverenja u svog pružaoca usluga, ako što su Google u slučaju Gmail-a, Microsoft u slučaju Exchange-a, ili Facebook u slučaju Messenger-a, pošto oni (i svako sa kojim mogu biti primorani da podele podatke) mogu da vide/čuju vašu komunikaciju. Da ponovimo, koja će opcija biti najbolja zavisi od vrste pretnje sa kojom se suočavate (na primer, ako ne verujete Google-u ili ako je Vlada SAD vaš protivnik, onda Gmail nije dobra opcija), ali nekoliko popularnih i generalno pouzdanih opcija su sledeće:

ELEKTRONSKA POŠTA	• **Gmail (preko Google Workspace)** • **Outlook (preko Office 365** • Nemojte hostovati sopstveni Microsoft Exchange server za elektronsku poštu vaše organizacije. Ako to trenutno radite, trebalo bi da **pređete** na Office 365.
TEKSTUALNE PORUKE (POJEDINAČNE ILI GRUPNE)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
GRUPNE KONFERENCIJE, AUDIO I VIDEO POZIVI	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **WebEx** • **GotoMeeting** • **Zoom**
DELJENJE FAJLOVA	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

NAPOMENA O DELJENJU FAJLOVA

Pored bezbednog deljenja poruka, bezbedno deljenje fajlova je verovatno važan deo bezbednosnog plana vaše organizacije. Većina opcija za deljenje fajlova su ugrađene u aplikacije ili programe za slanje poruka koje možda već koristite. Na primer, deljenje fajlova preko Signala je odlična opcija ukoliko vam je potrebna obostrana enkripcija. A ako vam je dovoljna enkripcija sloja prenošenja, možete razmotriti korišćenje Google Drive-a ili Microsoft Sharepoint-a. Samo se postarajte da pravilno konfigurišete podešavanja za deljenje tako da samo odgovarajuća lica imaju pristup određenom dokumentu ili folderu i postarajte se da su ove usluge povezane sa poslovnim a ne privatnim mejlovima osoblja. Ako možete, zabranite deljenje osetljivih fajlova preko priloga u mejlovima ili fizički preko USB-a. Upotreba uređaja poput USB-a u okviru vaše organizacije povećava mogućnost malvera ili krađe, a oslanjanje na priloge bilo u mejlovima ili u drugom obliku podriva zaštitu od fišinga (phishing) napada.



Alternative za deljenje fajlova za organizacije

Ako tražite bezbednu opciju za deljenje fajlova za vašu organizaciju koja nije direktno ugrađena u platformu za slanje poruka (ili imate problema sa ograničenjima veličine fajlova kad delite velike dokumente), razmotrite da koristite OnionShare. OnionShare je open source alatka koja vam dozvoljava da bezbedno i anonimno podelite fajl bilo koje veličine. On funkcioniše tako što pošiljalac skine OnionShare aplikaciju (koja je dostupna za kompjutere sa Mac, Windows i Linux operativnim sistemima), otpremi fajl ili fajlove koje želi da podeli i generiše jedinstveni link. Ovaj link, koji radi samo u Tor pretraživaču, se onda može podeliti putem bilo kog bezbednog kanala za slanje poruka (npr. Signala) sa željenim primaocem. Primalac potom može da otvori link u Tor pretraživaču i skine fajl(ove) na svoj kompjuter. Imajte na umu da su linkovi bezbedni samo onoliko koliko i kanal preko kojeg ih delite. Tor ćemo detaljnije objasniti u kasnijem „naprednom“ odeljku ovog priručnika, ali za svrhe deljenja fajlova u okviru vaše organizacije, imajte OnionShare na umu kao bezbedniju alternativu deljenju velikih fajlova preko USB-a u kancelariji ako ne posedujete pouzdanog pružaoca usluga klauda.

Ukoliko je vaša organizacija već investirala u program za upravljanje lozinkama, kao što je opisano u odeljku o lozinkama, i izabere premijum ili timski Bitwarden nalog, imaće pristup još jednoj bezbednoj opciji za deljenje fajlova, tačnije **Bitwarden Send** funkciji. Ona korisnicima omogućava da kreiraju bezbedne linkove za deljenje šifrovanih fajlova preko bilo kog bezbednog kanala za slanje poruka (poput Signala). Veličina fajlova je ograničena na 100MB, ali vam Bitwarden Send dozvoljava da odredite datum isteka linkova, lozinkom zaštitite pristup deljenim fajlovima i odredite koliko puta link može biti otvoren

Bezbedno komuniciranje i deljenje podataka

- **Zahtevajte upotrebu pouzdane usluge slanja poruka sa obostranom enrlkipcijom za osetljive komunikaicje vaše organizacije (i u idealnom slučaju za sve komunikacije).**
  - **Odvojite vremena da osoblju i eksternim partnerima objasnite zašto je bezbedna komunikacija tako važna, jer će to potpomoći uspeh vašeg plana.**
- **Formulišite politiku o tome koliko dugo ćete zadržavati poruke i kada/da li će organizacija koristiti „samonestajuće“ komunikacije.**
- **Postarajte se da namestite odgovarajuća podešavanja kako bi aplikacije za komunikacju bile bezbedne, što podrazumeva i da:**
  - **se postarate da celokupno osoblje obraća pažnju na notifikacije o bezbednosti i, ako koriste WhatsApp, ne bekapuju četove.**
  - **se postarate, ako koristite aplikaciju gde obostrana enkriopcija nije uključena od početka (npr. Zoom ili Webex), da relevantni korisnici uključe odgovarajuće funkcionalnosti na početku bilo kog poziva ili sastanka.**
- **Koristite usluge elektronske pošte bazirane na klaudu kao što su Office 365 li Gmail.**
  - **Ne pokušavajte da hostujete sopstveni server za elektronsku poštu.**
- **Često podsećajte sve u organizaciji o najboljima bezbednosnim praksama u vezi sa grupnim slanjem poruka i metapodacima.**
  - **Budite svesni ko sve učestvuje u grupnim porukama, četovima i mejlovima.**

Bezbedno skladištenje podataka

Za većinu organizacija civilnog društva, jedna od najvažnijih odluka koju treba da donesu jsete gde da skladište podatke.

Da li je „bezbednije" skladištiti podatke na kompjuterima osoblja, na lokalnom serveru, na eksternim diskovima, ili na klaudu? U 99% situacija, najlakša i najbezbednija opcija je da podatke skladištite u pouzdanom klaudu. Neki uobičajeni primeri obuhvataju Microsoft 365, Google Drive ili Dropbox. Bez sveobuhvatnog plana za skladištenje na klaudu verovatno će podaci vaši organizacije biti čuvani na više različitih mesta - uključujući na kompjuterima osoblja, eksternim hard diskovima ili možda čak na lokalnom serveru. Dok je moguće obezbediti podatke na svim tim pojedinačnim uređajima, veoma je teško to uspešno odraditi a da ne potrošite puno novca i zaposlite veći broj IT profesionalaca.

Kada birate alatku ili uslugu za čuvanje vaših podataka, uverite se da verujete kompaniji ili grupi koja stoji iza toga. Brza Google pretraga i provera sa stručnjacima za digitalnu bezbednost mogu vam pomoći da potvrdite pouzdanost potencijalnog dobavljača tehnologije. Neka pitanja koja treba imati na umu uključuju: Da li oni prodaju ili dele vaše privatne podatke? Da li imaju odgovarajuće bezbednosne resurse u osoblju? Da li nude bezbednosne funkcije (kao što je 2FA) koje će vam pomoći da zaštitite svoj nalog?

Skladištenje podataka i civilno društvo

Pojava priuštivih (ponekad besplatnih) sistema za skladištenje podataka na klaudu je olakšala život brojnim organizacijama civilnog društva sa ograničenim resursima (i učinila ih bezbednijim). Nažalost, mnoge i dalje pokušavaju da hostuje sopstvene servere sa ograničenim IT veštinama ili podrškom. U martu 2021. opasnost od takve organizacione infrastrukture je postala stvarnost za hiljade organizacija širom sveta kada je Hafnium, akter povezan sa kineskom vladom, pokrenuo globalnu katastrofu na polju sajber bezbednosti uz pomoć sofisticiranog napada na servere Microsoft Exchange-a koje su organizacije samostalno hostovale. Napad je kompromitovao lokalne servere i hakerima omogućio da dobiju pristup organizacijskim mejl nalozima i instaliraju malver na serverima žrtava i sistemima povezanim sa njima. Dok je Microsoft brzo objavio ažuriranje i uputstvo za identifikaciju i uklanjanje potencijalnih uljeza, mnoge manje organizacije nisu imale IT kapaciteta da brzo ažuriraju svoje servere i stoga su bile duže izložene malveru. Obim i efekat ovog globalnog hakovanja otkriva opasnost situacije gde civilne organizacije, naročito manje sa malim brojem IT profesionalaca, odluče da samostalno hostuju servere elektronske pošte i druge vrste osetljivih podataka.

PREDNOSTI SKLADIŠTENJA U KLAUDU

Čak i ako preduzmete sve potrebne korake da zaštite svoje kompjutere od malvera ili fizičke krađe, uporni protivnik i dalje može da hakuje vaš kompjuter ili lokalne servere. Za njih je mnogo teže da probiju zaštitu, na primer, Google-a ili Microsoft-a. Dobre kompanije za skladištenje u klaudu imaju resurse bez premca i jaku poslovnu motivaciju da obezbede maksimalnu bezbednost za svoje korisnike. Ukratko: strategija sa pouzdanim skladištenjem u klaudu će biti mnogo lakša i jefitinija za sprovođenje i trajno održavanje bezbednosti. Tako da umesto da brinete o zaštiti sopstvenog servera, možete da se skoncentrišete na šačicu jednostavnijih zadataka.

Ako većinu svojih informacija držite na klaudu to vam pomaže i da kontrolišete niz drugih uobičajenih rizika. Da li je neko ostavio kompjuter u restoranu ili telefonu u autobusu? Da li vam je dete oborilo čašu soka na tastaturu i pokvarilo uređaj? Da li je član osoblja zakačio malver i mora da izbriše sve sa kompjutera i formatira ga? Ako je većina dokumenata i podataka u klaudu lako je ponovo ih sinhronizovati i početi ispočetka na formatiranom ili poptuno novom kompjuteru. Takođe, ako malver zarazi kompjuter ili ako lopov skenira hard disk, neće imati šta da ukrade ako se većini dokumenata pristupa preko pretraživača.

KOG PRUŽAOCA USLUGA SKLADIŠTENJA NA KLAUDU TREBA DA IZABEREMO?

Dve najpopularnije opcije za skladištenje na klaudu su Google Workspace (prethodno poznat kao GSuite) i Microsoft 365. Ako vi i vaše osoblje koristite Gmail, ima smisla da registrujete organizaciju za Google Workspace i podatke skladištite u Google Drive-u koji sadrži Google Docs, Sheets i Slides aplikacije za obradu teksta, tabelarne prikaze i prezentacije. Slično, ako ste organizacija koja se oslanja na Excel i Word, najjednostavnije je da se registrujete za Microsoft 365, koji vašoj organizaciji daje pristup Outlook-u za mejlove i licenciranim verzijama Microsoft Word-a, Excel-a, Powerpoint-a i Teams-a.

Bez obzira na to kog pružalaca usluga odaberete, bezbedno skladištenje podataka u klaudu zahteva nameštanje dobrih podešavanja za deljenje, kao i obučavanje osoblja da razumeju kako i kad da dele (ili ne dele) foldere i dokumente. Generalno govoreći, u vašem drajvu za skladištenje na klaudu treba da kreirate foldere kojima može da pristupi samo osoblje kojem trebaju fajlovi iz njih. Rutinski revidirajte svoj sistem kako biste se postarali da ne delite svoje fajlove sa suviše ljudi (kao npr. kreiranjem univerzalnih linkova za deljenje u slučaju fajlova koji treba da budu dostupni samo nekolicini ljudi).

ŠTA AKO NE VERUJEMO GOOGLE-U ILI MICROSOFT-U ILI DRUGIM PRUŽAOCIMA USLUGA SKLADIŠTENJE U KLAUDU?

Ako neko od vaših protivnika (na primer, strana vlada ili lokalna samouprava) može zakonski da primora Google ili Microsoft (ili drugog pružaoca usluga skladištenja u klaudu) da predaju podatke, onda možda nema smisla da ih odaberete za svoje potrebe skladištenja podataka. Ovaj rizik može biti veći ako je vaš protivnik, na primer, vlada Sjedinjenih Američkih Država, ali mnogo manji ako je vaš protivnik neki autoritarni režim. Imajte na umu da i Google i Microsoft imaju politike o predavanju podataka samo ako su zakonski primorani na to, i imajte na umu da bi i vaša organizacija mogla biti podložna istim vrstama zakonskih zahteva sopstvene države ako hostujete podatke na lokalnom nivou.

U situaciji gde skladištenje u klaudu koje Google ili Microsoft obezbeđuju ne odgovara vašoj organizaciji, možete uzeti u obzir sledeću alternativu - Keybase. Timska funkcionalnost u Keybase-u dozvoljava vašoj organizaciji da deli fajlove i poruke uz pomoć obostrane enkripcije i bezbednom klaud okruženju a da ne morate da se oslanjate na trećeg pružaoca. Zbog toga može biti dobra opcija za bezbedno skladištenje dokumenata i fajlova na nivou cele organizacije. Međutim, Keybase je manje poznat većini korisnika, tako da budite svesni da će usvajanje ove alatke zahtevati više napora i bouke od prethodno navedenih rešenja.

Ipak, ako se odlučite da sami rešite svoje skladištenje podataka i uopšte ne koristitite klaud, od ključnog je značaj da uložite vreme i resurse u pojačavanje digitalne zaštite uređaja vaše organizacije i staranje da su lokalni serveri adekvatno konfigurisani, šifrovani i fizički zaštićeni. Možda ćete tako uštedeti na mesečnoj pretplati ali će vas to koštati vremena i resursa i učiniti mnogo ranjivijim na napad.

PRAVLJENJE REZERVNIH KOPIJA PODATAKA

Bez obzira da li vaša organizacija čuva podatke u klaudu ili na fizičkim uređajima, važno je da imate rezervne verzije. Jako je lako izgubiti podatke, naročito ako se oslanjate na skladištenje na fizičkim uređajima. Možda prospete kafu na kompjuter i uništite hard disk. Kompjuteri osoblja mogu biti hakovani i svi lokalni fajlovi zaključani ransomverom. Neko bi mogao da zaboravi uređaj u vozu ili da mu ga ukradu zajedno sa torbom. Kao što je već pomenuto, ovo je još jedan razlog da odaberete skladištenje u klaudu, pošto nije vezano ni za jedan određeni uređaj koji može biti zaražen, izgubljen ili ukraden. Mekovi dolaze sa ugrađenim softverom za pravljenje rezervnih kopija koji se zove Time Machine i koji koristite zajedno sa eksternim uređajem za skladištenje; za uređaje sa Windows operativnim sistemom, File History nudi slične funkcije. Ajfoni i androidi mogu automatski da naprave rezervne kopije većine važnog sadržaja na klaudu ako to uključite u podešavanjima.

Ako vaša organizacija koristi skladištenje u klaudu (npr. Google Drive), postoji jako mali rizik da će neko oboriti Google ili da će vaši podaci biti uništeni u nekoj katastrofi, ali i dalje postoji mogućnost ljudske greške (poput slučajnog brisanja važnih fajlova). Tako da se može isplatiti da razmotrite rešenje koje nudi pravljenje rezervnijih kopija na klaudu, kao što je npr. Backupify ili SpinOne Backup

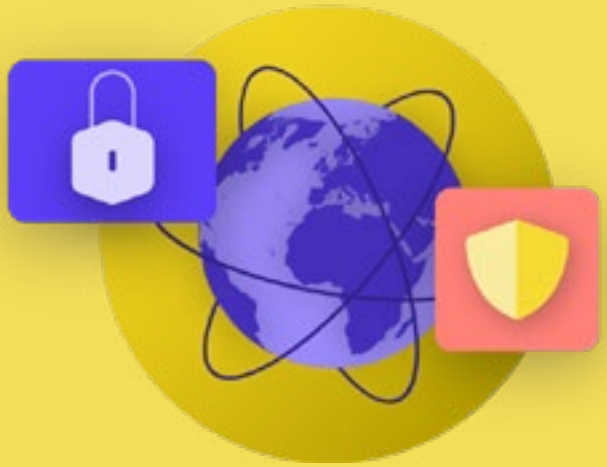
Ako se podaci skladište na lokalnom serveru i/ili lokalnim uređajima, onda je bezbedna rezerva kopija još bitnija. Možete da napravite rezervnu kopiju svojih podataka na eksternom disku, ali onda obavezno taj hard disk zaštitite jakom lozinkom. Time Machine može da šifrira hard diskove za vas ili možete koristiti pouzdane alatke za enkripciju celog hard diska kao što su VeraCrypt ili BitLocker. Obavezno uređaje sa rezervnim kopijama čuvajte na zasebnoj lokaciji. Setite se, ako u požaru istovremeno izgore i vaši kompjuteri i rezervne kopije podataka na njima znači da uopšte nemate rezervne kopije. Razmotrite da te kopije držite na sigurnom mestu, kao npr. sefu u banci. Napomena: ako koristite vašeg cloud provajdera u zemlji sa specifičnim zakonima o lokalizaciji podataka, konsultujte se sa pravnim stručnjacima kako biste bolje razumeli kako rešenje za takvu vrstu skladištenja može da bude u skladu sa svim lokalnim zahtevima. Mnogi cloud provajderi, uključujući Google i Microsoft, sada nude opcije koje omogućavaju nekim klijentima da odaberu geografsku lokaciju svojih podataka u cloudu, na primer.

Poboljšanje bezbednosti podataka organizacije na klaudu

Ako vaša organzacija odluči da uspostavi domen u Google Workspace-i ili Microsoft 365, budite svesni da obe kompanije nude veći nivo bezbednosti (u većini slučajeva besplatno) to organizacijama civilnog društva. Google Advanced Protection Program i Microsoft AccountGuard pružaju još jaču bezbednost za sve klaud naloge vaše organizacije, i pomažu vam da značajno smanjite verovatnoću delotvornog fišinga (phishing) i kompromitovanja naloga. Ako verujete da vaša organizacija može imati prava na ova dva paketa i zainteresovani ste da se prijavite za neki od njih, posetite gornje linkove ili na pišite na cyberhandbook@ndi.org da biste dobili pomoć.

Bezbedno skladištenje podataka

- **Osetljive podatke skladištite isključivo u pouzdanom klaudu.**
  - **Postarajte se da svi nalozi koji imaju pristup tom klaudu imaju jake lozinke i 2FA.**
- **Formulišite i sprovodite politiku koja ograničava broj ososba sa kojima se dele podaci u klaudu.**
  - **Obučite celokupno osoblje kako da adekvatno deli dokumenta i kako da ih ne deli sa prevelikim brojem ljudi.**
- **Ako se vaša organizacija odluči za lokalno skladištenje podataka, investirajte u visokoobučeno IT osoblje.**
- **Zaštitite rezervne kopije svojih podataka - šifrirajte svoje diskove ili uređaje sa rezervnim kopijama podataka.**



Bezbednost na internetu

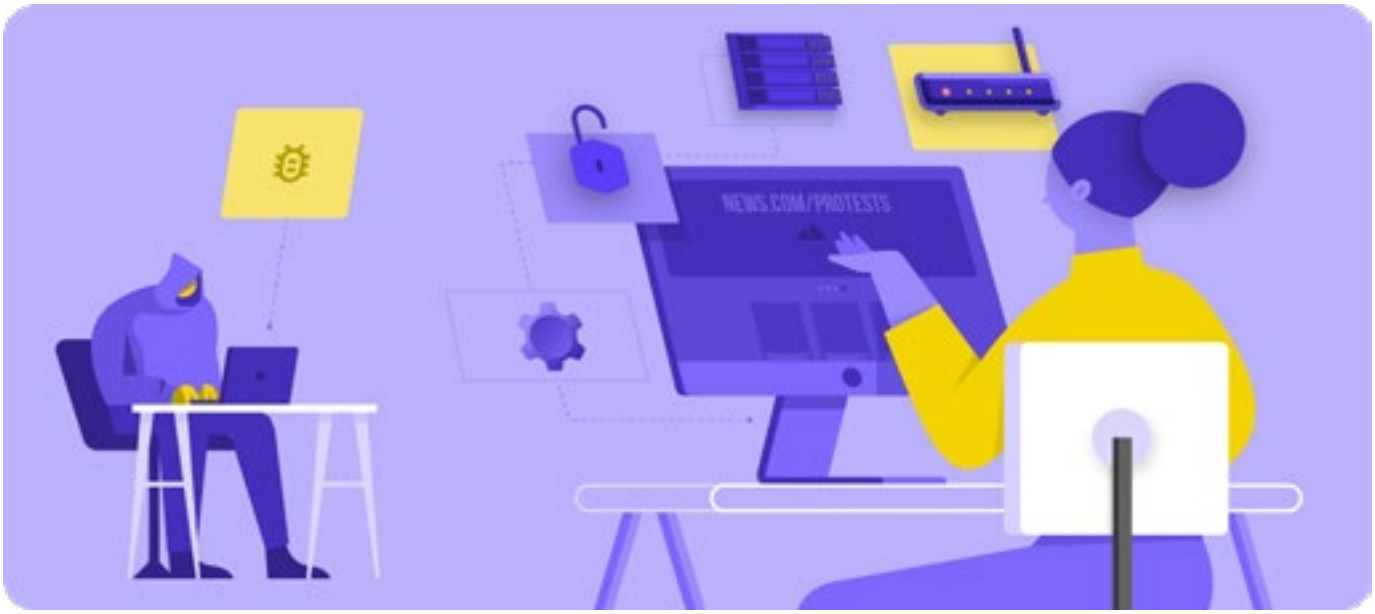
Kada koristite internet na telefonu ili kompjuteru, vaša aktivnost može reći dosta toga o vama.

Važno je da osetljive informacije – poput korisničkih imena i lozinki koje unosite na sajtovima, vaših postova na društvenim mrežama, ili u određenom kontekstu čak i imena sajtova koje posetite - od tuđih pogleda. Takođe je uobičajen problem blokiranje ili ograničavanje pristupa određenim sajtovima ili aplikacijama. Ova dva problema – nadzor i cenzura na internetu – idu ruku pod ruku i samim tim su strategije za smanjivanje njihovog uticaja slične.

Sigurno pretraživanje

UPOTREBA HTTPS-A

Najvažniji korak da ograničite sposobnost svog protivnika da nadzire vašu organizaciju na internetu jeste da maksimlano smanjite količinu dostupnih informacija o tome šta vi i vaše kolege radite na internetu. Postarajte se da se uvek bezbedno kačite na internet: pazite da URL (lokacija) počinje sa „https“ i pokazuje malu ikonu katanca u polju za upisivanje adrese vašeg pretraživača. Kada pretražujete internet bez enkripcije, informacije koje unesete na sajt (poput lozinki, brojeva naloga i poruka), kao i detalji sajtova i internet stranica koje posećujete su svi izloženi. To znači da (1) bilo koji haker na vašoj mreži, (2) vaš administrator mreže, (3) vaš pružalac internet usluga (ISP) i bilo koje telo sa kojim on deli podatke (poput organa vlasti), (4) pružalac internet usluga sajta koji posećujete i bilo koje telo sa kojim on pa deli podatke, i naravno, (5) sam sajt koji posećujete, svi imaju pristup povećoj količini osetljivih informacija.



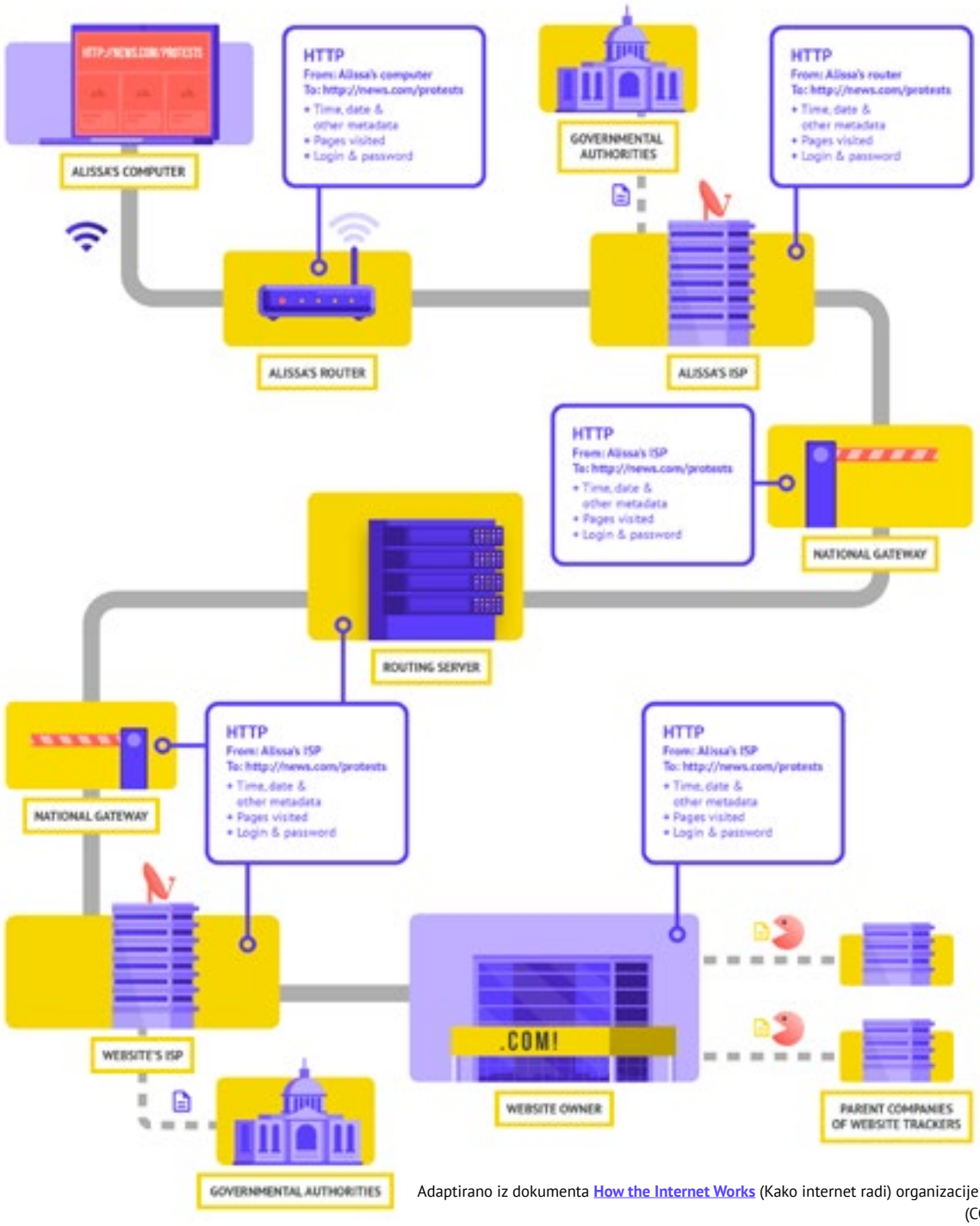
Nadzor, cenzura i civilno društvo

Vlade sve više koriste svoj uticaj i ovlašćenja nad pružaocima internet usluga i drugom lokalnom internetskom infrastrukturom kako bi sprečile pojedince i grupe da pristupe određenom sadržaju na internetu. U nekim slučajevima, takve disrupcije interneta za cilj imaju obaranje glavnih platformi za komunikaciju i deljenje informacija, uključujući i društvene mreže i sajtove sa vestima. Na primer, u odgovoru na proteste protiv vojnog puča, vojska Mijanmara je mobilnim operaterima naložila da privremeno ugase čitav prenos podataka preko mobilne telefonije u celoj zemlji. To je nastupilo ubrzo nakon ciljanog blokiranja Facebook-a, Twitter-a i Instagrama.

Pored blokiranja sajtova i pristupa internetu uopšte, vlade i drugi akteri širom sveta koji predstavljaju pretnju sve više koriste sve pristupačniju tehnologiju za nadzor kako bi pratili aktivnost građana na internetu. Na primer, po izveštaju Freedom House-a pod nazivom Freedom on the Net 2020 (Sloboda na netu 2020.) vlada Ugande je ušla u partnerstvo sa kineskom tehnološkom kompanijom Huawei kako bi **nadzirala opozicione prvake i aktiviste civilnog društva** pre i nakon burnih i osporavanih predsedničkih izbora.

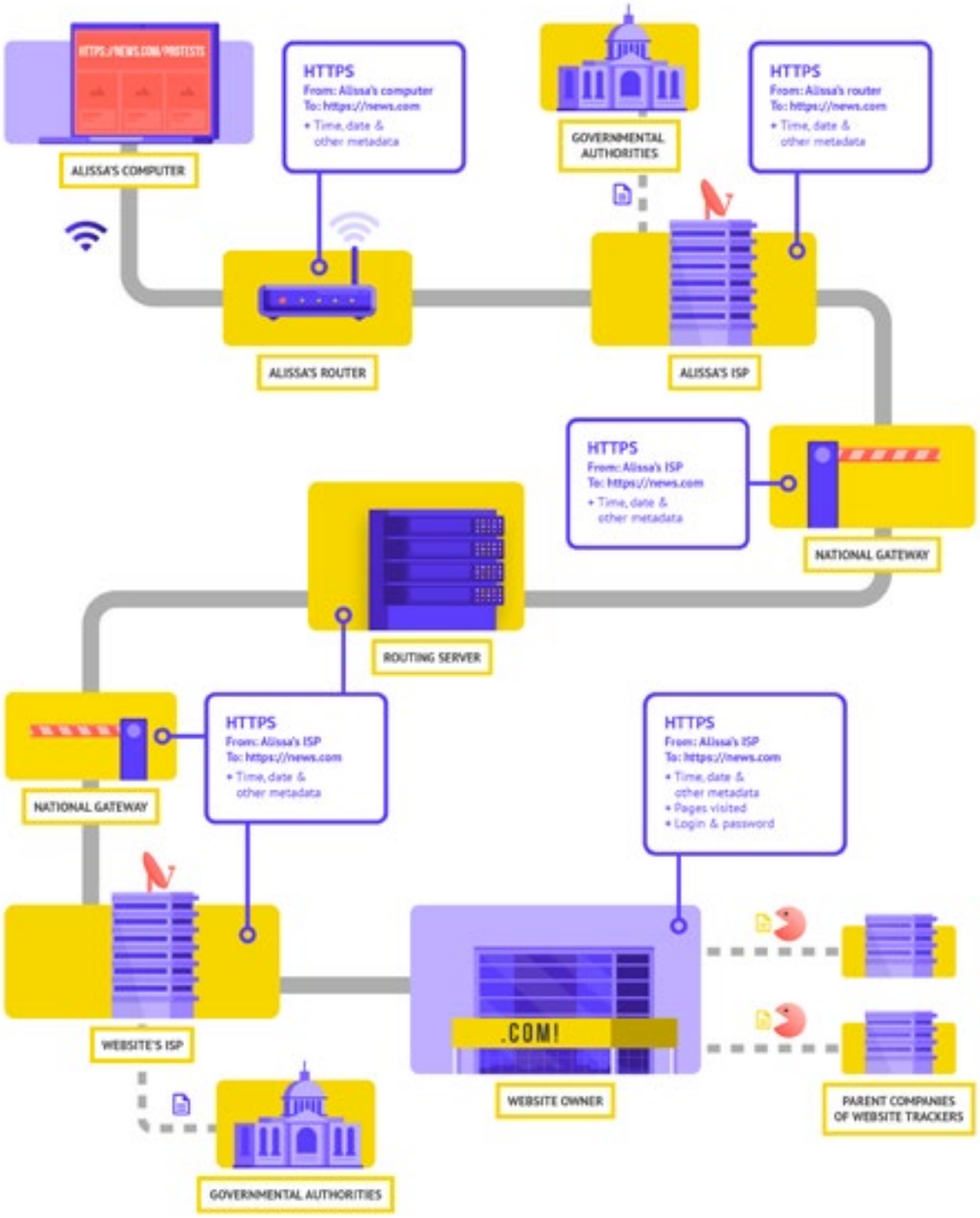
Sve veća učestalost ovakivih napada na slobodu informisanja na internetu potcrtava od kolikog je zapravo značaja za grupe civilnog društva da razumeju rizike rada na internetu i kreiraju planove načina povezivanja na internet kad je to povezivane ograničeno.

Hajde da pogledamo jedan stvaran primer pretraživanja bez enkripcije:



Kada pretražujete bez enkripcije, svi vaši podaci su izloženi. Kao što je gore prikazano, protivnik može da vidi gde se nalazite, da idete na news.com, posebno gledajući stranicu o protestima u vašoj zemlji, i da vidi vašu lozinku koju delite da biste se prijavili na sam sajt. Takve informacije u pogrešnim rukama ne samo da otkrivaju vaš nalog već i potencijalnim protivnicima daju dobru predstavu o tome šta biste mogli da radite ili o čemu razmišljate.

Upotreba HTTPS („s“ označava englesku reč za bezbedan) znači da postoji enkripcija. Tako dobijate veću zaštitu. Hajde da pogledamo kako izgleda pretraživanje sa HTTPS (tj sa enkripcijom):



Adaptirano iz dokumenta [How the Internet Works](#) (Kako internet radi) organizacije Totem Project (CC–BY–NC–SA)

Ako HTTPS postoji, potencijalni protivnik ne može više da vidi vašu lozinku ili druge osetljive informacije koje unosite na dati sajt. Međutim, i dalje mogu da vide koje domene (npr. news.com) posećujete. I iako HTTPS takođe šifruje i podatke o pojedinačnim stranicama na sajtu (na primer, website.com/protests) koje posećujete, sofisticirani protivnici i dalje mogu da dođu do ovih podataka pregledanjem vašeg internet saobraćaja. Tako da ako HTTPS postoji, protivnik može znati da idete na news.com, ali ne bi bio u stanju da vidi vašu lozinku i bilo bi mu teže (mada ne i nemoguće) da vidi da tražite informacije o protestima (da iskoristimo prethodni primer). To je bitna razlika. Uvek proveravajte da postoji HTTPS pre nego što počnete da pregledate sajt ili unosite osetljive informacije. Možete takođe da koristite **HTTPS Everywhere ekstenziju za pretraživač** kako biste se postarali da stalno koristite HTTPS, a ako koristite Firefox, uključite **HTTPS only režim** u pretraživaču.

Ako vam pretraživač izbaci upozorenje da je neki sajt potencijalno opasan, nemojte to ignorisati. Nešto nije u redu. To može biti nešto bezazleno - tipa da je sajtu istekao bezbednosni sertifikat - ili bi to mogao biti lažan ili dupliran sajt. U svakom slučaju, važno je da poslušate upozorenje i ne odete na taj sajt.

HTTPS je neophodan, a šifrovani DNS pruža dodatnu zaštitu od uhođenja i blokiranja sajtova, ali ako se vaša organizacija pribojava usko ciljanog nadzora vaših aktivnosti na internetu i suočava se sa sofisticiranom internetskom cenzurom (npr. blokadom sajtova i aplikacija), možda biste želeli da koristite virtuelnu privatnu mrežu (VPN).

Napredna lekcija: Koristite šifrovani DNS

Ukoliko, u skladu sa nivoom pretnje kojem ste izloženi želite da otežate nekom pružaoca internet usluga da zna detalje sajtova koje posećujete (mada nažalost ne možete i da to potpuno sprečite), možete da koristite šifrovani DNS.

Za slučaj da **ste se pitali**, DNS znači Domain Name System, tj. sistem imena domena. To je u suštini telefonski imenik interneta koji prevodi imena domena koje ljudi razumeju (kao ndi.org) u IP adrese (tj. numeričke indikatore koje mašine razumeju. Ovo ljudima dozvoljava da koriste pretraživače da lako nađu i učitaju internetske resurse i posećuju sajtove. Ali šifrovanje DNS nije podrazumevano.

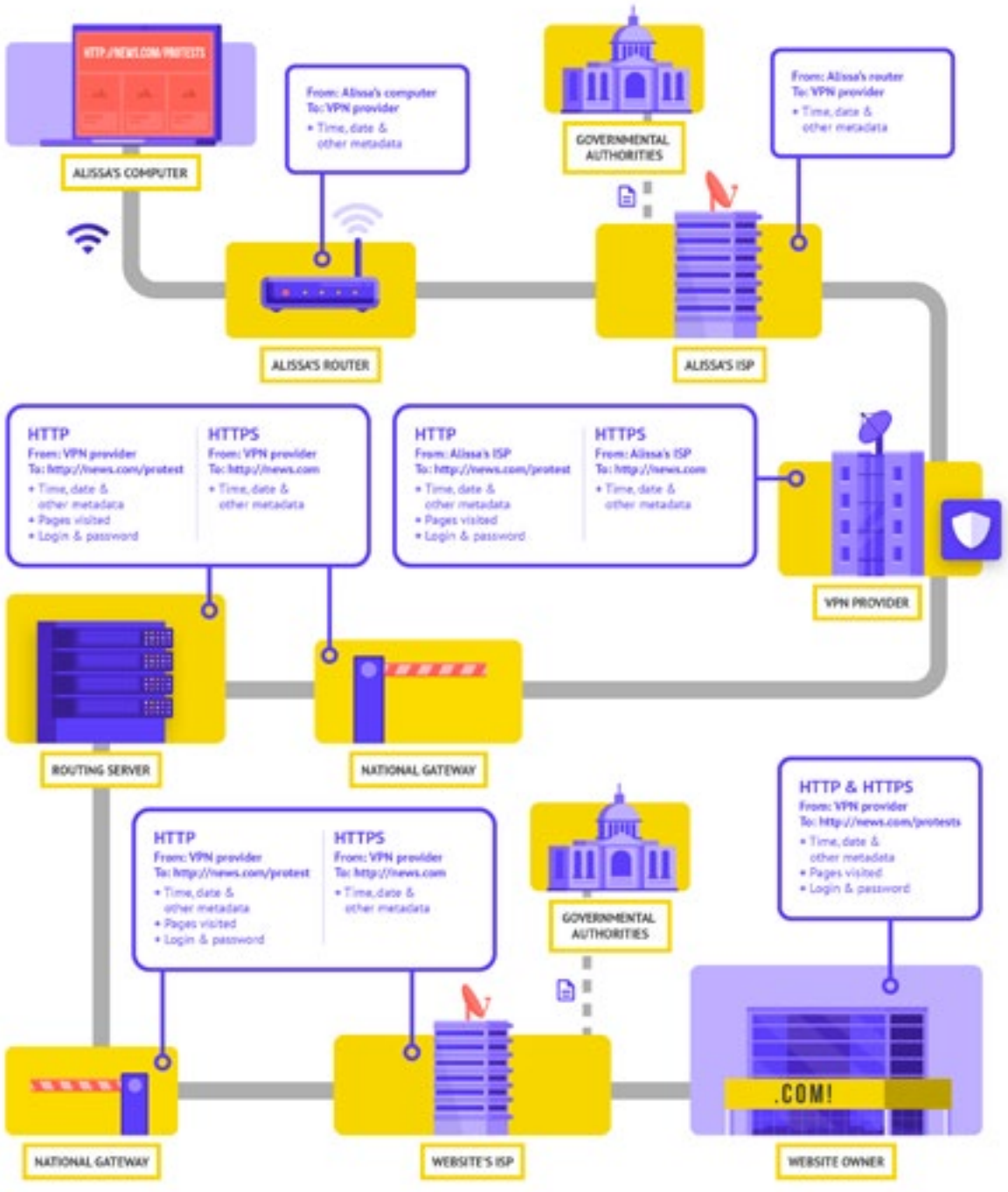
Kako biste koristili šifrovani DNS i istovremeno dodatno zaštitili svoj internet saobraćaj, jedna laka opcija bi bila da skinete i uključite **Cloudflare's 1.1.1.1 aplikaciju** na vašem kompjuteru i moblinom uređaju. Dostupne su i druge opcije za DNS, uključujući Google 8.8.8.8, ali zahtevaju **više tehničkih koraka** kako biste ih podesili.

Ako koristite pretraživač Firefox, šifrovanje DNS je podrazumevano podešavanje. Korisnici Chrome ili Edge pretraživača mogu takođe da **uključe šifrovanje DNS** u naprednim bezbednosnim podešavanjima pretraživača tako što će uključiti „use secure DNS" (koristi bezbedni DNS) i odabrati „With: Cloudflare (1.1.1.1)" ili pružaoca usluga po svom izboru.

Cloudflare 1.1.1.1 sa WARP-om šifruje DNS i podatke o vašem pretraživanju - što je usluga slična tradicionalnom VPN-u. Dok WARP ne sakriva u potpunosti vašu lokaciju od svih sajtova koje posetite, predstavlja jednostavnu funkcionalnost koja može da pomogne osoblju vaše organizacije da iskoristi enkripciju DNS i dodatnu zaštitu od vašeg pružaoca internet usluga u situacijama gde puni VPN ne funkcioniše ili nije potreban, već u skladu sa nivoom pretnje. U naprednim DNS podešavanjima u okviru 1.1.1.1 sa WARP-om, osoblje može da uključi i 1.1.1.1 za porodice kako bi omogućilo dodatnu zaštitu od malvera prilikom pristupanja internetu.

ŠTA JE VPN?

VPN je u suštini tunel koji vas štiti od nadzora i blokiranja internet saobraćaja koje vrše hakeri na vašoj mreži, administrator mreže i pružalac internet usluga, kao i bilo ko sa kime potencijalno dele podatke. Evo primera kako izgleda pretraživanje sa VPN-om:



Adaptirano iz dokumenta How the Internet Works (Kako internet radi) organizacije Totem Project (CC–BY–NC–SA)

Kaako bismo detaljnije opisali VPN u ovom odeljku ćemo se pozvati na [Surveillance Self Defense Guide] (Vodič za samoodbranu od nadzora):

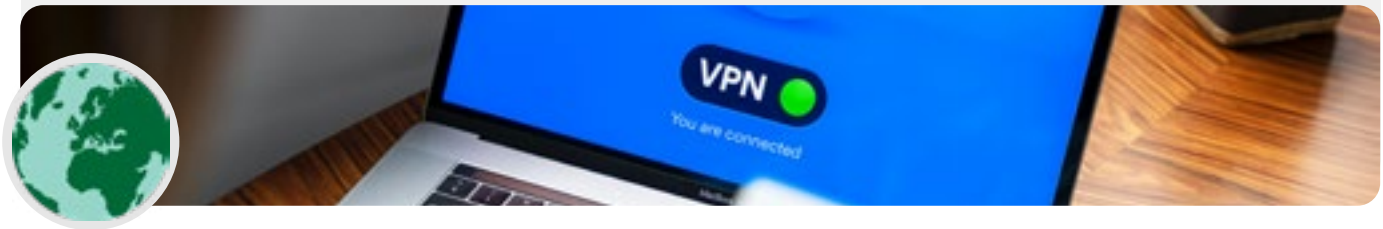
Tradicionalni VPN-ovi maskiraju vašu stvarnu IP adresu i prave šifrovani tunel za internetski saobraćaj između vašeg kompjutera (ili telefona ili bilo kog „pametnog“ uređaja na mreži) i VPN-ovog servera. Pošto se saobraćaj u tunelu šifruje i šalje vašem VPN-u, mnogo je teže za treće strane kao što su pružaoci internet usluga ili hakeri na javnoj wifi mreži da prate, menjaju ili blokiraju vaš saobraćaj. Nako što kroz tunel stigne od vas do VPN-a, vaš saobraćaj onda napušta VPN i ide ka svom konačnom odredištu, maskirajući vašu pravu IP adresu. To sakriva vašu fizičku lokaciju od bilo koga ko proverava saobraćaj nakon što napusti VPN. Samim tim je veći stepen privatnosti i bezbednosti, ali VPN vas neće učiniti potpuno anonimnim jer je vaš saobraćaj i dalje vidljiv operatoru VPN-a. Vaš pružalac internet usluga takođe zna da koristite VPN, što može povećati vaš profil rizika.

To znači da je **od suštinskog značaja da izaberete pouzdanog pružaoca usluga VPN-a**. Na nekim mestima, kao u Iranu, neprijateljski nastrojene vlade zapravo same uspostavljaju VPN-ove kako bi bile u stanju da prate šta građani rade. Kako biste našli VPN koji odgovara vašoj organizaciji i osoblju, možete da procenite VPN-e na osnovu njihovog poslovnog modela i reputacije, podataka koje (ne) skupljaju, i naravno bezbednosti same alatke.

Zašto ne bismo samo koristili besplatni VPN? Kratki odgovor je da većina beplatnih VPN-a , uključujući one koji dobijete sa nekim mobilnim telefonima, dolaze sa velikom začkoljicom. Kao sve kompanije i pružaoci usluga, VPN-i moraju nekako da se izdržavaju. Ako VPN ne prodaje svoju uslugu, kako onda održava svoje poslovanje? Da li traži donacije? Da li naplaćuje premijum usluge? Da li ima podršku finansijera ili humanitarnih organizacija? Nažalost, većina besplatnih VPN-a zarađuje tako što prikuplja i onda prodaje vaše podatke.
Najbolji izbor predstavlja naravno pružalac VPN koji uopšte ne prikuplja podatke. Ako se podaci ne prikupljaju, onda ih niko ne može prodati ili predati vladi na njen zahtev. Kada čitate politiku privatnosti pružaoca VPN usluge, proverite da li taj VPN zapravo prikuplja podatke o korisnicima. Ako ne kaže izričito da se podaci o povezivanju korisnika ne evidentiraju, vrlo su velike šanse da se to zapravo događa, jer čak i ako kompanija tvrdi da zapravo ne evidentira podatke o konekciji to nije uvek garancija poštenog ponašanja.
Vredi istražiti kompaniju koja poseduje VPN. Da li je dobila pzitivne ocene nezavisnih profesionalaca na polju bezbednosti? Da li postoje članci o tom VPN-u? Da li su ikad uhvaćeni u zavaravanju ili direktnom laganju svojih korisnika? Ako su VPN osnovali ljudi koji su poznati u zajednici stručnjaka za informacionu bezbednost, verovatnije je da je pouzdan. Budite skeptični ako vidite VPN koji nudi uslugu za koju niko ne želi da garantuje svojom reputacijom ili neki iza kojeg stoji kompanija za koju niko nije čuo.

Lažni VPN-i u stvarnom svetu

Krajem 2017. godine, nakona talasa protesta u toj zemlji, [Iranci su počeli da otkrivaju „besplatnu“ (ali lažnu) verziju popularnog VPN-a koja se delila preko poruka.] Besplatni VPN (koji zapravo nije radio) je obećavao da će obezbediti pristup Telegramu, koji je u to vreme bio blokiran na lokalnom nivou. Nažalost, lažna aplikacije je bila samo malver koji je dozvolio organima vlasti da prate kretanje i nadziru komunikacije onih koji su je skinuli.



Pa koji onda VPN treba da koristimo?

Ako je vašoj organizaciji potreban VPN, u pouzdane opcije spadaju TunnelBear i ProtonVPN. Još jedna opcija je da konfigurišete sopstveni server uz pomoć programa Outline koji je razvio tehnološki inkubator Jigsaw, gde vašim nalogom ne upravlja nijedna kompanija, ali zauzvrat morate da oformite sopstveni server. Ako je vaša organizacija malo veća, možda treba da razmotrite poslovni VPN koji sadrži i funkcionalnosti za upravljanje nalozima kao što je Teams plan u slučaju TunnelBear-a. TunnelBear takođe obezbeđuje besplatnu upotrebu svog VPN-a (za koji pretplata inače iznosi 3$ mesečno) organizacijama aktivnim u oblasti civilnog društva i ljudskih prava koje ispunjavaju određene uslove. Ako mislite da vaša organizacija možda ispunjava te uslove i zainteresovani ste, kontaktirajte cyberhandbook@ndi.org da biste dobili više informacija.

Iako je većina modernih VPN-a unapredila svoju brzinu i performanse, vredi imati na umu da upotreba VPN-a može da vam smanji brzinu pretraživanja ako ste na mreži sa veoma niskim propusnim opsegom, imate problema sa velikim kašnjenjem signala ili sa čestim pucanjem internet veze. Ako ste na bržoj mreži, trebalo bi da stalno koristite VPN.

Ako osoblju preporučite da koriste VPN, takođe je bitno da se postarate da ga ljudi stalno drže uključenog. To vam možda zvuči očigledno, ali VPN koji je instaliran, ali ne radi ne pruža nikakvu zaštitu.

Napredna lekcija: Anonimnost preko Tor-a

Pored VPN-a, možda ste čuli i za Tor kao još jednu alatku za bezebdnije korišćenje interneta. Važno je da razmete šta su obe ove alatke, zašto bi mogli da koristite jednu ili drugu, i kako obe mogu da utiču na vašu organizaciju.

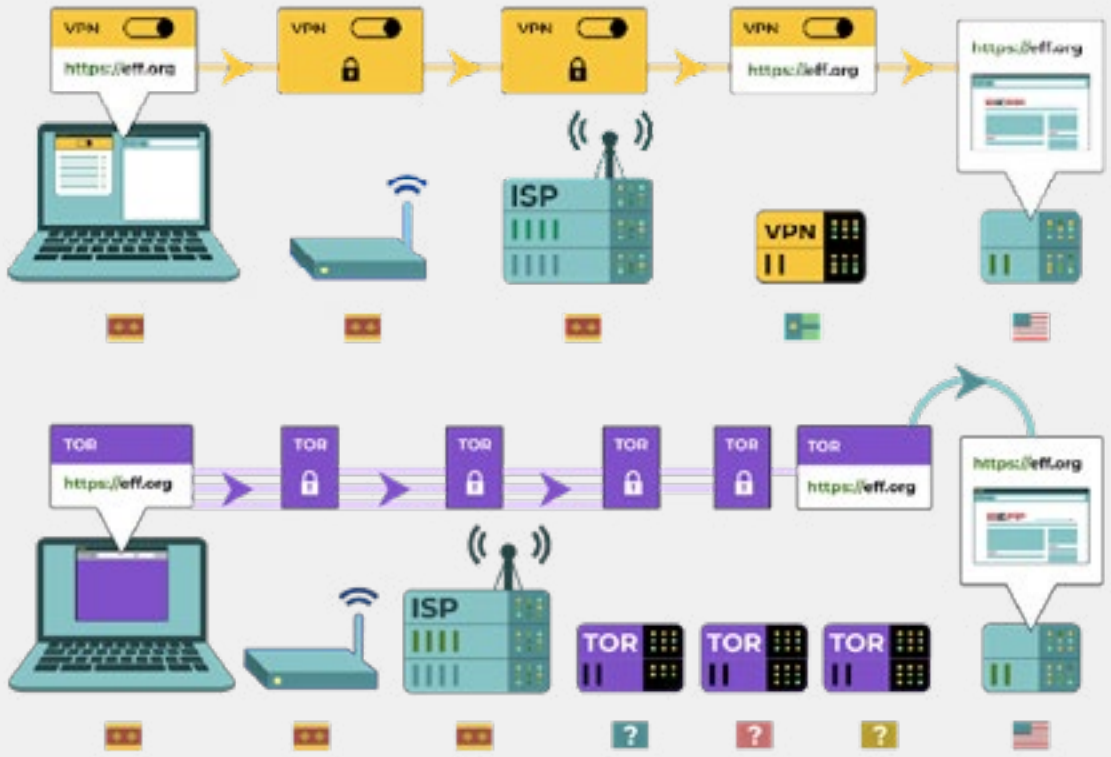
Tor je protokol za anonimno slanje podataka preko interneta usmeravanjem poruka ili podataka kroz decentralizovanu mrežu. Možete da pročitate nešto više o tome kako Tor funkcioniše ovde, ali ukratno, on usmerava vaš saobraćaj kroz više tačaka na putu do njegovog odredišta tako da nijedna pojedinačna tačka nema dovoljno informacija da odjednom otkrije ko ste i šta radite na internetu.

Tor se razlikuje od VPN-a na nekoliko načina. U osnovi, razlika leži u tome što se ne oslanja na bilo koju pojedinačnu tačku (kao pružalac VPN usluga.)

Ova slika, koju je napravila EFF, pokazuje razliku između tradicionalnog VPN-a i Tor-a.

Najlakši način da koristite Tor jeste preko njegovog pretraživača (Tor browser). On funkcioniše kao bilo koji normalni pretraživač osim što vaš saobraćaj preusmrava na Tor mrežu. Ovaj pretraživač možete skinuti za Windows, Mac, Linux ili Android uređaje. Imajte na umu da kad koristite Tor pretraživač, štitite samo informacije kojima pristupate dok ste u pretraživaču. On ne pruža nikakvu zaštitu za druge aplikacije, ili skinute fajlove koje ćete možda zasebno otvoriti na svom uređaju. Takođe imajte na umu da Tor ne šifruje vaš saobraćaj, pa - slično kao kod VPN-a - i dalje je neophodno da koristite HTTPS prilikom pretraživanja.

Ako biste želeli da anonimnost koju Tor obezbeđuje proširite na ceo kompjuter, bolje tehnički potkovani korisnici mogu da instaliraju Tor kao internet konekciju za ceo sistem, ili razmotrite korišćenje Tails operativnog sistema, koji od početka sva saobraćaj preusmerava kroz Tor. Korisnici androida takođe mogu da upotrebe Orbot aplikaciju kako bi pokrenuli Tor za sav internet saobraćaj i aplikacije na svom uređaju. Bez obzira na to kako koristite Tor, važno je da znate da kad ga koristite, vaš pružalac internet usluga ne može da vidi koje sajtove posećujete, ali *može* da vidi da koristite sam Tor. Slično kao kad koristite VPN, to bi moglo da značajno poveća



nivo profila rizika vaše organizacije jer Tor nije baš uobičajena alatka i stoga upada u oči protivnicima koji možda prate vaš internet saobraćaj.

Dakle, da li bi vaša organizacija trebalo da koristi Tor? Zavisi. Za većinu ugroženih organizacija je pouzdani VPN koji celokupno osoblje stalno koristi najlakša i najzgodnija opcija, a u ovo doba sveprisutnosti VPN-a, manje je verovatno da će nekog alarmirati. Međutim, ako ili ne možete da priuštite pouzdani VPN ili radite u sredini gde se VPN-i obično blokiraju, Tor može biti dobra opcija za ograničavanje uticaja nadzora i izbegavanje internetske cenzure.

Da li iz nekog razloga ne treba da koristimo VPN ili Tor?

Osim problema sa nepouzdanim VPN-ovima, najvažnija stvar koju morate da razmotrite jeste da li bi korišćenje VPN-a ili Tor-a moglo da privuče neželjenu pažnju ili, u nekim jurisdikcijama bude protivzakonito. Iako vaš pružalac internet usluga neće znati koje sajtove posećujete koristeći ove usluge, moći će da vidi da se povezujete na VPN ili Tor, tako da ako je to nezakonito u vašoj državi ili će izazvati više pažnje i izložiti vas većem riziku nego prosto pretraživanje interneta uz pomoć standardnog HTTPS protokola i šifrovanog DNS, onda VPN i naročito Tor (koji je mnogo manje uobičajen i stoga mnogo više privlači pažnju) nisu pravi izbor za vašu organizaciju. Međutim, kako upotreba VPN-a postaje sve uobičajenija ovo je sve manje bitan faktor. Najbolji izbor, ako je to legalno i moguće, je da koristite VPN sve vreme.

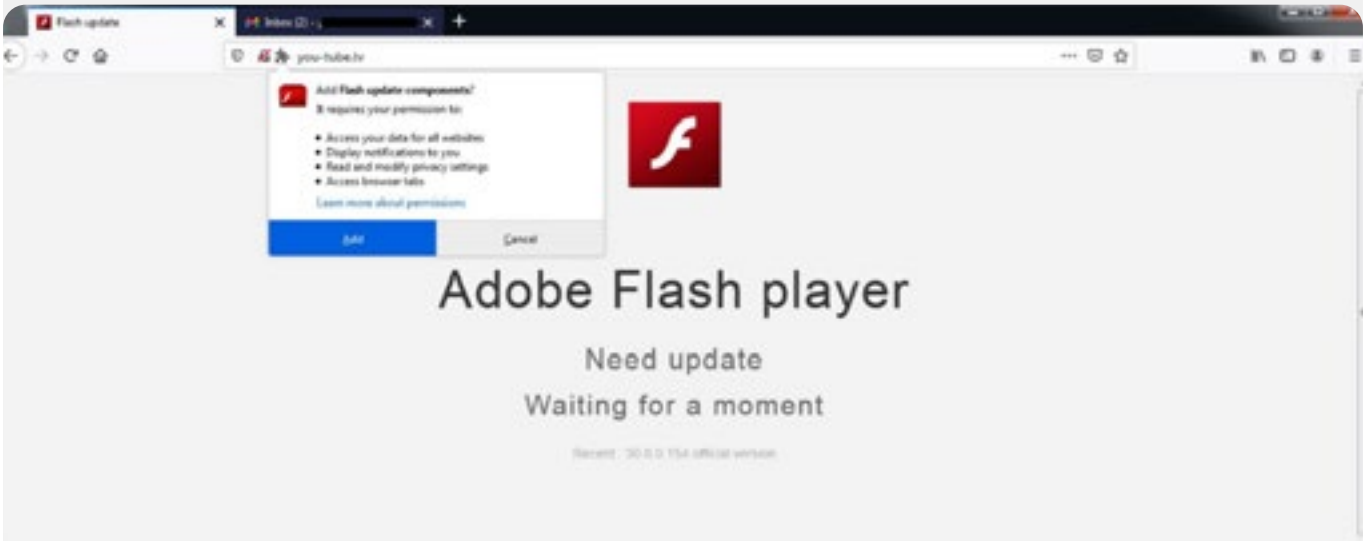
KOJI PREGLEDAČ (BROWSER) BI TREBALO DA KORISTIMO?

Koristite pouzdani pretraživač kao što su Chrome, Firefox, Brave, Safari, Edge ili Tor. I Chrome i Firefox su u širokoj upotrebi i jako su bezbedni. Neki ljudi više vole Firefox pošto ima veći naglasak na privatnosti. U svakom slučaju, važno je da relativno često restartujete i pretraživač i kompjuter kako bi vam pretraživač bio ažuriran. Ako ste zainteresovani da uporedite funkcionalnosti različitih pretraživača, pogledajte ovaj resurs koji je sastavio NVO Freedom of the Press Foundation.

Bez obzira na pretraživač, dobra je ideja da takođe koristite i ekstenziju ili dodatak kao što su Privacy Badger, uBlock Origin, ili DuckDuckGo's Privacy Essentials koji sprečava oglašivače i i ostale lokatore da prate gde idete i koje sajtove posećujete. A dok pretražujete internet, razmislite da termine koje tražite ne ukucavate u Google već DuckDuckGo, Startpage, ili drugi servis za pretraživanje koji štiti privatnost. To će vam pomoći i da ograničite broj oglašivača i trekera (trackers)

Bezbednost pretraživača u realnom svetu

Tibetanski aktivisti iz civilnog društva su bili pod napadom početkom 2021. kad je lukavo osmišljen zlonamerni dodatak za pretraživač krao podatke o njihovim mejlovima i pretraživanjima. Dodatak koji se zvao „Flash update components" (komponente za ažuriranje Flash-a) je nuđen korisnicima koji su posećivali sajtove naveden u fišing (phishing) mejlovima. Takvi napadi preko ekstenzija ili dodataka za pretraživač mogu biti podjednako štetni koliko i malver koji se deli direktno preko skidanja fišing ili drugog softvera.



Bezbednost društvenih mreža

Vaša organizacija može da otkrije mnogo toga, a ponekad i više no što namerava, postovanjem i komentarisanjem na društvenim mrežama.

Bez obzira da li je u pitanju Facebook, Twitter, Instagram, YouTube ili regionalne društvene mreže kao što su VKontakte i Odnoklassniki, uvek treba pažljivo da razmislite šta postujete i adekvatno konfigurišete bilo koja dostupna podešavanja privatnosti. Ovo važi ne samo za zvanične stanice vaše organizacije već u pojedinim slučajevima i za lične naloge osoblja, kao i naloge njihovih prijatelja i porodice.

Bezbednost društvenih mreža i civilno društvo

Čak i organizacije sa niskim nivoom rizika mogu da budu meta napada i uznemiravane na društvenim mrežama ukoliko ne poseduju adekvatne politike bezbednosti. U ovom primeru iz 2018. godine neprofitni azil za životinje je izgubio hilajde dolara i zamerio se onima koji su ga pomagali kad je neovlašćeni administrator naloga lažirao kampanju za skupljanje sredstava, a na platformi su se pojavili i lažni nalozi koji su se predstavljali kao zaposleni u azilu. Ako su hakeri spremni toliko daleko da odu da bi zaradili nekoliko hiljada dolara na račun azila za životinje, možete da zamislite kakvu štetu bi mogli da nanesu sofisticirani protivnici ukoliko dobiju pristup nalozima vaše organizacije ili se uspešno predstave kao vi na internetu.

Pored hakovanja naloga, grupe civilnog društva i pojedinačni korisnici u mnogim zemljama se takođe suočavaju sa represijom zbog postovanja na društvenim mrežama. U jednom primeru iz Zambije iz 2020. godine policija je uhapsila 15-godišnjeg učenika zbog navodnog klevetanja predsednika u postu na Facebook-u. Dečak, koji je postovao pod pseudonimom, je identifikovan na osnovu telefonskog broja korišćenog za registrovanje naloga i svoje IP adrese.

FORMULIŠITE ORGANIZACIONU POLITIKU ZA DRUŠTVENE MREŽE

Pretpostavite da sve što postavljate na društvene mreže može postati javna stvar, i formulišite svoju politiku u skladu sa time. Ona bi trebalo da odgovori na pitanja kao što su: Ko ima pristup vašim nalozima na društvenim mrežama? Ko sme da postuje i ko mora da dobri te postove? Koje informacije treba/ne treba da se dele na društvenim mrežama? Ako postavljate slike, informacije o lokaciji ili druge informacije na osnovu kojih vaše osoblje, partneri ili čak učesnici mogu da budu identifikovani, da li ih pitate za dozvolu, i da li su oni upoznati sa rizicima?

Pored formulisanja politike koju ćete takođe objasniti osoblju, obavezno adekvatno konfigurišite podešavanja za privatnost i bezbednost (koje često nazivaju „sigurnosna podešavanja"). Neka od ključnih pitanja koja morate da sami sebi postavite kako biste odlučili koja podešavanja na polju bezbednosti i privatnosti su najsmislenija za vaše lične i organizacione naloge su:

- Da li želite da svoje postove delite sa javnošću ili samo sa određenom grupom ljudi bilo na internom ili eksternom nivou?
- Da li svako ima pravo da komentariše, odgovara na ili stupa u interakciju sa vašim porukama ili postovima?
- Da li treba da postoji mogućnost da ljudi pronađu vas ili vašu organizaciju preko imejl adrese ili (ličnog ili poslovnog) broja telefona?
- Da li želite da vaša lokacija bude automatski podeljena kad god postujete?
- Da li želite da blokirate ili utišate neprijateljski raspoložene naloge?
- Da li želite da blokirate određene reči ili heštegove?

Svaka društvena mreža ima drugačija podešavanja privatnosti i bezbednosti, ali ovi generalni koncepti važe za sve. Dok razmišljate o ovim pitanjima, iskoristite korisne vodiče koje su kreirale najveće platforme: Facebook, Twitter, Instagram, i YouTube. Kod Facebook-a naročito, budite oprezni oko opcija privatnosti na grupama. Facebook Groups predstavljaju popularno mesto za angažovanje, zagovaranje i deljenje informacija, ali grupama kojima pristup nije ograničen može da se pridruži bilo ko. Neretko se „lažni" nalozi predsatvljaju kao pravi ljudi kako bi se uvukli u privatne stranice ili grupe na društvenim mrežama. Tako da budite oprezni kad je u pitanju prihvatanje zahteva za prijateljstvo i praćenje. Setite se da su nalozi na društvenim mrežama vaše organizacije bezbedni samo koliko i nalozi koji su povezani sa njom. Ovo je naročito važno zapamtiti u slučaju Facebook-a gde stranicu vaše organizacije može da vodi nečiji povezani lični nalog.

UZNEMIRAVANJE PREKO INTERNETA

Nažalost, mnoge organizacije se suočavaju sa velikim nivoom uznemiravanja preko interneta, naročito na društvenim mrežama. Takvo uznemiravanje je često još intezivnije kad je usmereno protiv žena i marginalizovanih populacija. Nasilje protiv žena na internetu naročito može da stvori hostilno okruženje koje vodi ka samocenzuri ili povlačenju iz političkog ili građanskog diskursa. Kao što je identifikovano u izveštaju NDI Tima za rod, žene i demokratiju pod nazivom Tweets that Chill (Tvitovi koji izazivaju jezu) kad se napadi na politički aktivne žene dešavaju na internetu, veliki doseg društvenih mreža može da pojača efekat uznemiravanja i psihološkog maltretiranja i podrije osećaj žena za ličnu bezbednost na način koji se ne dešava muškarcima.

Dok vaša organizacija bude formulisala svoju politiku za društvene mreže, važno je da budete svesni ove dinamike. U svoj bezbednosni plan ugradite podršku za osoblje koje se suočava sa negativnim porukama, uvredama i pretnjama na društvenim mrežama (bilo u svom profesionalnom ili ličnom životu). Uspostavite infrastrukturu za borbu protiv uznenmiravanja u okviru vaše organizacije, što obuhvata i anketiranje osoblja kako biste razumeli kako uznemiravanje preko interneta utiče na njih, i oformite urgentni tim koji će osoblju pomoći da se snađe u izazovnim situacijama. Online Harassment Field Manual (Terenski vodič za uznemiravanje preko interneta) NVO-a PEN America takođe nudi detaljne preporuke o tome kako da podržite osoblje koje se suočava sa takvim uznemiravanjem. Možete takođe razmotriti, ako vaše osoblje to prihvati, da prijavite slučajeve uznemiravanja i/ili problematičnih naloga direktno i platformama.

Kada ulazite u interakciju sa osobljem koje je bilo uznemiravano preko interneta (kao i u fizičkom svetu) važno je biti osetljiv. Kao što se navodi u programu za ženska prava Uduženja za progresivnu komunikaciju pod nazivom Take Back the Tech (Povratite tehnologiju) treba da razumete da je žrtva možda traumatizovana i prepoznate da nasilje (bilo na internetu ili van njega) nikad nije krivica žrtve. Postarajte se da se o takvim pitanjima razgovara (ako osoblje to želi) u poverljivom i bezbednom okruženju, sa opcijom anonimnosti. Takođe u vaš bezbednosni plan uvrstite spisak lokalnih profesionalaca, organizacija, i organa policije i tužilaštva sa kojima možete povezati osoblje kako bi po potrebi dobili pravnu, medicinsku, psihološku i tehničku pomoć. Za još ideja, pogledajte Online Safety Guide (Vodič za bezbednost na internetu) organizacije Feminist Frequency.

Držite svoje sajtove na internetu

Pored toga što ćete se postarati da bezbedno pristupate internetu, takođe je bitno da uradite sve što možete da biste se postarali da drugi mogu da pristupe vašim sajtovima ili vašim drugim lokacijama na internetu.

Kad su u pitanju stranice na društvenim mrežama, to znači da te naloge morate da zaštitite jakim, jedinstvenim nalozima i dvostrukom potvrdom identiteta. U slučaju vašeg sajta, to znači da morate da ga zaštitite od hakera i DDoS napada. DDoS napadi su slučajevi gde velika grupa kompjutera istovremeno zatrpava vaš server zlonamernim saobraćajem. Ako ste organizacija civilnog društva ili druga neprofitna organizacija, onda verovatno možete da dobijete besplatnu DDoS zaštitu - koja značajno otežava pritivniku da vam obori sajt - preko servisa kao što su Cloudflare **Project Galileo**, Google **Project Shield** ili eQualitie **Deflect**.

Bezbedno hostovanje sajta vaše organizacije

Internet sajtovi su hostovani na kompjuterima - a oni su ranjivi na hakovanje kao i vaši lični uređaji. Ukoliko je to moguće, vaša organizacija bi trebalo da iskoristi postojeće usluge hostinga kao što su Wordpress.com, Wix ili drugi koji će upravljati celokupnom bezbednošću sajta u vaše ime. Ako čitate ovaj priručnik, vaša organizacija verovatno ima pravo na besplatni bezbedni hosting Wordpress sajta koji **eQualitie** obezbeđuje preko njihove **eQPress Hosting usluge**. Ovo je odlična opcija za civilne organizacije koje već imaju Wordpress sajtove ili u slučaju da vaša organizacija želi da napravi novi sajt.

Ako morate sami da hostujete svoj sajt, onda se postarajte da se fokusirate na ažuriranje vašeg operativnog sistema i softvera za hosting na internetu, isto kao na vašem ličnom kompjuteru. Razmotrite da koristite poznate pružaoce usluga hostinga u klaudu kao što su Amazon Web Services (AWS), Microsoft Azure ili Greenhost-ov **Eclips.is**, koji obezbeđuje napredne bezbednosne opcije za hostvane sajtove. I naravno, bez obzira na alatke koji koristite da hostujete svoj sajt postarajte se da svi nalozi preko kojih se pristupa podešavanjima i menjanju sadržaja budu zaštićeni jakim lozinkama i dvostrukom potvrdom identiteta.

Ako vaša organizacija ima tehničko znanje za hostovanje sopstvenog sajta trebalo bi takođe da razmotrite da izaberete takozvani statički sajt. Za razliku od dinamičkih sajtova, ovaj tip sajta smanjuje površinu napda za hakere i učiniće vaš sajt otpornijim na napade.

Zaštitite svoju wifi mrežu

Svi ovi koraci za zaštitu internet saobraćaja od nadzora i cenzure su bitni, ali ne predstavljaju zamenu za osnovnu mrežnu bezbednost u kancelariji (i kod kuće).

Nemojte zanemariti osnove poput jake lozinke (ne one koja je došla sa uređajem) na vašem wifi ruteru, starajući se da samo ovlašćeni korisnici imaju pristup vašoj mreži tako što ćete često menjati lozinku i uključiti fajervol ugrađen u ruter. Razmotrite da napravite mrežu za goste i u kancelariji ako imate posetioce koji koriste internet.

Bezbednost na internetu

- **Organizujte redovnu obuku o značaju poštovanja osnovnih mera mrežne bezbednosti za osoblje.**
- **Podestite osoblje da interent uvek pretražuju sa HTTPS i šifrovanim DNS.**
- **Tražite od osoblja da redovno i ponovo pokreće svoje pretraživače kako bi ih ažurirali.**
- **Podstaknite upotrebu pretraživača i ekstenzija za zaštitu bezbednosti.**
- **Ako VPN odgovara kontekstu vaše organizacije, izaberite pouzdani VPN, obučite osoblje da ga koristi, i postarajte se da se dosledno koristi**
- **Kreirajte i distribuirajte jasnu organizacionu politiku o upotrebi društvenih mreža.**
- **Uključite podešavanja za privatnost i bezbednost na svim nalozima na društvenim mrežama.**
- **Steknite razumevanje efekata uznemiravanja preko interneta i budite spremni da podržite osoblje koje ga je doživelo.**
- **Napravite spisak lokalnih prodesionalaca, organizacija i policijskih organa/ organa tužilaštva sa kojima možete da povežete osoblje kako bi im pružili pravnu, psihološku i tehnološku pomoć nakon uznemiravanja preko interneta.**
- **Prijavite se za DDoS zaštitu za vaše sajtove.**
- **Koristite pouzdanog pružaoca usluga hostinga sa dobrom reputacijom.**
- **Koristite jaku lozinku i napravite gostinjsku mrežu za vaš kancelarijski wifi.**

Zaštita fizičke bezbednosti

Od suštinskog je značaja da vaši uređaji budu fizički bezbedni. Ali fizička bezbednost nije ograničena samo na uređaje i trebalo bi da podrazumeva i strategije za zaštitu svega u vašem okruženju, poput opipljivih dokumenata, kancelarijskog ili randog prostora i naravno vas, vašeg osoblja i volontera.

Fizička bezbednost i civilne organizacije

Fizički napadi na organizacije civilnog društva su nažalost uobičajena pojava i često imaju značajne implikacije po kako fizičku, tako i informacionu bezbednost. Jedna od uobičajenih taktika protivnika za gušenje aktivnosti OCD uključuje napade na i zatvaranje poslovnih prostorija - kako bi zaplašili osoblje i u nekim slučajevima ukrali ili konfiskovali informacije i tehničku opremu.Takve pretnje su često usmerene protiv manjinskih grupa i grupa za ljudska prava i OCD koje se bave demokratijom i radom vlade. Na primer, civilna organizacija LGBT+ Rights iz Gane koja je početkom 2021. otvorila prvi centar za lokalnu LGBTQI+ zajednicu je dobijala pretnje da će im zapaliti kancelariju, a na kraju je policija organizovala raciju i zatvorila ih. Takvi napadi ne utiču samo na fizičke aktivnosti neke organizacije, već mogu i da dovedu do toga da se osoblje ne oseća bezbednim.

Zaštita fizičke imovine

Fizička bezbednost vaših uređaja predstavlja osnovnu komponentu bezbednosti informacija.

Pored ublažavanja posledica krađe uređaja uz pomoć zaključavanja ekrana i lozinki, primenom enkripcije celog diska, i uključivanjem funkcionalnosti za brisanje na daljinu, trebalo bi takođe da razmotrite kako da sprečite da neko uopšte ukrade taj uređaj. Kako biste otežali krađu, obavezno ugradite jake brave (i menjajte ih kad god dođe do promene osoblja) u poslovnim prostorijama i/ili kod kuće. Takođe razmotrite da kupite sef za laptop ili ormarić koji se zaključava kako bi uređaji bili bezbedni preko noći. Kamere za nadzor su postale prilično jefitne i široko su dostupni jednostavniji modeli namenjeni za kućnu upotrebu. Takvi sistemi kamera ili senzora koji se aktiviraju na pokret postavljeni oko vaših prostorija mogu da otkriju i nadajmo se ometu fizičke provale i pljačke. Pogledajte koja opcija **koja poštuje vašu privatnost** jer dostupna u vašoj državi i obavezno odaberite kamere pouzdanog proizvođača koji nema razloga da vaše podatke i informacije preda potencijalnom protivniku.

Ukoliko je rizik od provale u ili racije vaših prostorija veliki, čuvajte najosetljivije podatke van kancelarije, bilo tako što ćete ih bezbedno čuvati u klaudu (kao što smo već objasnili) ili tako što ćete ih fizički premestiti na manje opasnu lokaciju. Ako se informacije još uvek nalaze na starim uređajima koje ne koristite, razmislite da ih obrišete - **ovaj vodič** sa internet sajta WireCutter predstavlja odlilčno uputstvo kako da to izvedete na većini modernih uređaja. Ukoliko nije moguće izbrisati uređaje, možete i fizički da ih uništite. Najlakši, mada ne baš i najekološkiji, način je da uređaje i njihove diskove razbijete čekićem. Ponekad su najstarija rešenja i dalje najbolja!

Čak i pre tih tehničkih koraka, odvojite malo vremena da popišete svu opremu organizacije. Ako nemate spisak svih uređaja, teže je pratiti šta nedostaje ako neki ukradu.

Uspostavljanje sopstvenog sistema za obezbeđivanje poslovnog prostora

Ukoliko vaša organizacija nema dovoljno sredstava u budžetu za pun bezbednosni sistem za vaše poslovne prostorije a zabrinuti ste za svoju privatnost, možete probati kreativnu opciju kao što je **Haven App** organizacije Guardian Project koja može da vas obavesti o potencijalnom upadu u prostorije. Haven je aplikacija za pametne telefone koja bilo koji android telefon može da pretvori u detektor pokreta, zvuka, vibracija i svetla. Možete da aplikaciju podesite na nekoliko jeftinih android uređaja koje ćete razmestiti po kancelariji kako bi vas obavestili o bilo kakvim neočekivanim gostima i nepoželjnim uljezima i snimili ih. Haven aplikaciju možete takođe podesiti u hotelskoj sobi ili stanu ako ste izuzetno ugroženi. Pun bezbednosni sistem je uvek najbolje rešenje, ali ako nije moguć, a želeli biste da naučite kako da koristite Haven aplikaciju moežte da posetite **sajt projekta**.

ŠTA DA RADIMO SA OVOLIKIM PAPIRIMA?

Vaša organizacija verovatno ima jako puno informacija koje su odštampane na papiru, zapisane u sveskama ili naškrabane u samolepljivim blokčićima. Neki od ovih podataka mogu biti jako osetljivi: odštampane verzije budžeta, spiskovi učesnika, poverljiva pisma od donatora i beleške sa privatnih sastanaka. Od suštinske je važnosti da mislite na bezbednost i ovih informacija. Ukoliko zaista morate da držite opipljive verzije osetljivih informacija postarajte se da se bezbedno čuvaju u zaključanom ormariću ili na nekom drugom sigurnom mestu. Ne držite osetljive informacije (uključujući lozinke) na stolu ili zapisane na tabli u kancelariji. Ako verujete da postoji velika ospanost da će u vaše prostorije provaliti ili da će biti meta racije, držite veoma osetljive informacije na drugoj, manje opasnoj lokaciji.

Koliko god je moguće se trudite da uništite nepotrebne opipljive informacije. Setite se - ako nešto nemate, ne mogu vam ga ni ukrasti. Formulišite organizacionu politiku o vlasništvu nad fizičkim beleškama, i obavezno prikupite sve papirne beleške od osoblja koje odluči da napusti organizaciju ili koje otpustite (kao što biste pokupili bilo koji kompjuter ili telefon koji ste im obezbedili za rad). Da biste se rešili osetljivog materijala, kupite kvalitetan uništivač dokumenata. Zabavna aktivnost za kraj radne nedelje može biti petnaestominutna pauza tokom koje ćete sa osobljem kroz unuištivač propustiti bilo koje osetljive papire ili beleške od prethodnih pet dana.

KANCELARIJSKA POLITIKA

Iako se za mnoge realnost „kancelarije“ značajno promenila od početka pandemije virusa COVID-19 i dalje je bitno za vašu organizaciju da formulišete jasnu politiku po pitanju pristupa kancelarijama. Ovakva politika bi trebalo da odgovori na ključna pitanja kao što su kome je dozvoljen pristup kancelarijama (i kada), ko može da pristupi kojim kancelarijskim resursima (poput wifi mreže), kao i šta treba raditi sa gostima.
Jednostavno ali bitno pitanje koje treba rešiti je ko ima ključeve od kancelarije. Samo osoblje u koje imate poverenja treba da ih dobije, a potrebno je i da brave menjate na poluredovnoj osnovi i/ili svaki put kad neko napusti organizaciju.Tokom dana, bilo koja otključana vrata bi trebalo da stalno budu u vidokrugu osobe od poverenja. Takođe razmotrite da li imate poverenja u lice koje vam iznajmljuje poslovne prostorije ili čistačko osoblje. Razmislite o tome kojim informacijama ili uređajima takva lica mogu imati pristup i postarajte se da budu zaštićeni, naročito ako nemate poverenja u ove osobe. Ko god da ima pristup, potrebno je da odredite osobu kojoj verujete da zaključava kancelariju i postara se da uređaji budu adekvatno obezbeđeni pre odlaska na kraju radnog dana.
Da li gosti mogu da uđu u kancelariju? Ako je tako, postarajte se da nemaju pristup (ili bar nekotrolisani pristup) uređajima ili osetljivim informacijama na papiru. Ukoliko je potrebno ili očekivano da gosti imaju pristup internetu tokom posete, trebalo bi da uspostavite „gostinsku“ mrežu tako da ti gosti ne mogu da prate vaš redovni saobraćaj. Generalno govoreći, samo osoblje od poverenja bi trebalo da bude u stanju da pristupi mreži i mrežnim uređajima poput štampača. Takođe je obično dobra ideja da tražite gostima da se prijave kako biste imali spisak posetilaca.
Dok kreirate politiku za kancelariju, njen cilj bi trebalo da samo osobe od poverenja imaju pristup osetljivim uređajima, dokumentima, prostorijama i sistemima.

PODRŠKA OSOBLJU I VOLONTERIMA

Pretnje po fizičku bezbednost vašeg kancelarijskog prostora utiču i na vaše osoblje. Slično uznemiravanju na društvenim mrežama, ove pretnje po fizičku bezbednost su često disporporcionalno usmerene protiv žena i marginalizovanih zajednica. Nije stvar samo u slomljenim prozorima i ukradenim laptopovima. Zastrašivanje, pretnje ili slučajevi fizičkog ili seksualnog nasilja, nasilje u porodici i strah od napada mogu imati ozbiljne negativne posledice po živote osoblja. Naročito ako imate organizaciju koja radi sa politički aktivnim ženama ili ih podržava možete iskoristiti **#Think10**, alatku za planiranje bezbednosti koju je NDI kreirao kao korisni resurs za one koji su potencijalno izloženi povećanom ličnom riziku zbog svojih aktivnosti.

Dobrobit osoblja je očigledno važna za njih kao pojedince, ali takođe predstavlja i ključni element zdrave i funkcionalne organizacije. U tu svrhu, razmotrite koje dodatne resurse možete da obezbedite kako biste zaštitili svoje osoblje i, u slučaju fizičkog ili digitalnog napada, pomogli im da se oporave. Kao što je već pomenuto u ovom priručniku, to podrazumeva da u najamnaju ruku sastavite spisak resursa na koje možete uputiti svoje osoblje kako bi dobilo potrebnu pravnu, medicinsku, psihološku i tehničku pomoć ako im bude trebala. I ovde **Online Field Harassment Manual** (Terenski priručnik o zlostavljanju preko interneta) NVO-a PEN America sadrži ideje o tome kako vaša organizacija može da podrži svoje osoblje tokom i nakon krize a Tactical Tech **Holistic Security Manual** (Holistički priručnik za bezbednost) obuhvata relevantni sadržaj o tome kako organizacije često reaguju tokom perioda u kojem trpe intezivne pretnje.

BEZBEDNOST TOKOM PUTOVANJA

Putovanje - bilo u drugu zemlju ili susedni grad - često pogoršava pretnje po fizičku bezbednost informacija. Generalno možete pretpostaviti da vi i vaši uređaji nećete imati nikakvo pravo na privatnost prilikom prelaska granice. S obzirom na to, dobra je ideja da u vaš bezbednosni plan uvrstite i politiku o poslovnim putovanjima koja obuhvata i podestnik o ključnim najboljim praksama na polju bezbednosti.

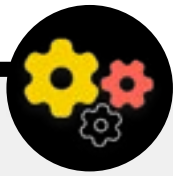
Politika o putovanjima vaše organizacije bi trebalo da pokrije dosta informacija pomenutih u drugim delovima ovog priručnika, uključujući bezbednu upotrebu interneta i fizičku zaštitu uređaja i drugih izvora informacija na putu. Ako je to moguće ostavite sve osetljive informacije kod kuće i koristite novi, poptpuno prazni kompjuter, fajlovima koji su vam neophodni pristupajte iz klauda i onda ih obrišite kad se vratite.

Pored priprema za putovanje i maksimalnog smanjenja podataka koje ćete deliti tokom istog, postoji još nekoliko ključnih praktičnih saveta koje treba da razmotrite i unesete u svoju poliitku o putovanjima.

Razmotrite da koristite posebne putne laptopove ili telefone na kojima se nalazi malo ili nimalo osetljivih podataka. Ukoliko se najveći deo rada vaše organizacije obavlja na klaudu, relativno jeftin Chromebook može biti dobra opcija. Po povratku vratite ove uređaje na fabrička podešavanja ili obrišite sve sa njih pre povezivanja na zajedničke wifi mreže kod kuće ili u kancelariji.

Pripremite osoblje šta treba da rade ukoliko ih državni organi odvedu na ispitivanje ili i zaustave na graničnom prelazu. Razmotrite kako možete da ograničite količinu informacija sa kojima neko putuje ako je to potrebno, i kreirajte posebne protokole za osolje koje putuje u problematične regione. Osoblju recite koga da kontaktiraju i šta treba da urade ukoliko nešto pođe po zlu tokom puta. To podrazumeva i informacije o lokalnim bolnicama, klinikama ili apotekama ako im zatreba medicinska pomoć na putu.

Osoblje takođe treba da drži sve uređaje blizu sebe tokom putovanja. Na primer, držite laptop kod nogu (ne u odeljku za prtljag iznad glave ili u čekiranom prtljagu) kad ste u autobusu, vozu ili avionu. Nemojte unapred pretpostaviti da hotelska soba – ili čak hotelski sef – predstavljaju „sigurno mesto“ za držanje osetljivih uređaja i predmeta. Takođe nemojte imati poverenja u javne portove za punjenje USB-a. Ovi portovi su sve češći prizor na aerodromima, stanicima i u vozilima i predstavljaju vrlo zgodan način da napunite uređaj. Ali iz njih takođe možete vrlo lako pokupiti malver. Tako da se postarajte da ili uređaje punite na tradicionalni način preko utikača u zidu, ili kupite **uređaje za blokiranje prenosa podataka na USB** kako bi osoblje moglo bezbedno da puni USB-ove preko portova dok su na putu.

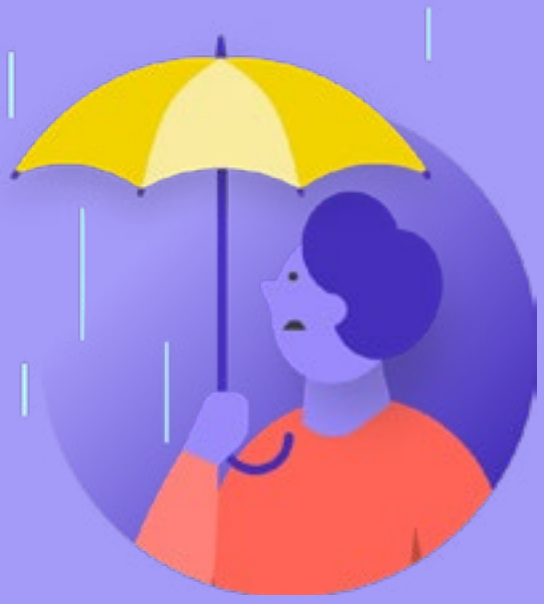


Bezbedno planiranje puta za vašu organizaciju

Prilikom formulisanja politike o putovanju, takođe imajte na umu koje informacije mogu biti izložene prilikom organizovanja puta ili pravljenja rezervacija. To može biti naročito bitno ako organizujete velike događaje, obuke ili konferencije za potrebe kojih rukujete osetljivim informacijama koje dobijate od raznovrsnog osoblja, partnera ili učesnika. Pažljivo razmislite kako ćete bezbedno deliti i skladištiti (ako je to potrebno) lične podatke poput podataka iz pasoša, plana puta i istorija bolesti. Tactical Tech Organizer Activity Book (Radna sveska za organizatore) sadrži odličnu tabelu koja može da vam pomogne da razmotrite ključna pitanja u vezi sa putnom bezbednošću i koju možete naći **na ovom linku**.

Zaštita vaše fizičke bezbednosti

- **Podsetite osoblje da je neophodno da uređaji stalno budu fizički zaštićeni.**
- **Proverite i obezbedite sve ulaze u vaš prostor - vrata i prozore.**
- **Formulišite politiku za goste i pristup kancelariji.**
- **Koristite jake brave, i rotirajte/menjajte ih po potrebi.**
- **Razmotrite da postavite kamere ili drugu vrstu bezbednosnog sistema u kancelariji.**
- **Nabavite i koristite uništivač dokumenata.**
  - **Odredite posebno vreme kad će osoblje uništavati štampane primerke dokumenata koje sadrže osetljive informacije.**
- **Napravite spisak lokalnih profesionalaca, organizacija i policijskih organa/ organa tužilaštva sa kojima možete da povežete osoblje kako bi im pružili pravnu, psihološku i tehnološku pomoć zbog fizičkih napada ili pretnji.**
- **Formulišite politiku za putovanja na nivou organizacije.**
- **Postarajte se da osoblje zna šta treba da radi ako tokom puta dođe do nekog hitnog slučaja, što podrazumeva i da ih pripremite šta treba da rade ako ih zaustave na graničnom prelazu ili kontrolnom punktu.**
- **Podsetite osoblje da pre bilo kakvog putovanja na lokalnom, nacionalnom ili međunarodnom nivou ograniče količinu informacija koje nose na uređajima.**
- **Obratite pažnju na dodatne podatke koji se generišu i dele prilikom organizovanja putovanja ili događaja.**



Šta da radite kad stvari krenu po zlu

Dakle, znate šta treba da radite. Formulisali ste politike i sve u organizaciji obučili o najboljim praksama. Čak i uz sav taj trud, vrlo je verovatno da će nešto u nekom trenutku poći po zlu.

Takav vam je život. Kad se to desi, od suštinske je važnosti da imate plan za slučaj incidenata. Mere za slučaj incidenta predstavljaju ključni, a često zanemareni, deo bezbednosnog plana vaše organizacije pošto one mogu da presude da li će neki napad uništiti reputaciju vaše organizacije ili biti samo manja prepreka na putu.

Imajte na umu da na incident možete da reagujete samo ako znate da je do njega došlo. Vrlo je važno da stvorite robusnu bezbednosnu kulturu na nivou cele organizacije i podstaknete osoblje da prijavljuje probleme. Zato je bolje da nagrađujete dobro ponašanje na polju bezbednosti nego da kažnjavate propuste ili greške. Takođe je važno da pokažete empatiju i proverite kako se član osoblja oseća nakon što prijavi incident. Želite da vaše osoblje odmah prijavi ako su kliknuli na fišing (phishing) poruku, ako su im ukrali telefon ili hakovali nalog na društvenim mrežama, a ne da oklevaju jer se boje kazne ili da im niko neće pružiti podršku. Naposletku, mere za slučaj incidenata, upravo kao strategije ublažavanja posledica pomenute u drugim odeljcima pruručnika, predstavljaju nešto čime treba da se bavi cela organizacija.

Dakle, šta vaši planovi treba da obuhvate? Ukratko, bilo šta što bi verovatno moglo da se desi. Ovo će se razlikovati od organizacije do organizacije, ali neka generalna pitanja na koje bi plan reagovanja u slučaju incidenta trebalo da odgovori su:

- Šta da radimo ako neko hakuje naše naloge ili naš sajt?
- Šta da radimo ako neko klikne na fišinga (phishing) mejl ili se neki uređaj sumnjivo ponaša?
- Šta da uradimo ako neko ukrade i objavi naše mejlove ili osetljive informacije?
- Šta da radimo ako se neko od našeg osoblja nađe u opasnoj situaciji ili bude uhapšen/a? Ili ako se bore sa stresom i anksiopznošću zbog takvih pretnji?
- Šta da radimo ako naša kancelarija nastrada u požaru, poplavi ili elementarnoj nepogodi?
- Šta da radimo ako član osoblja izgubi kompjuter ili telefon ili mu iste ukradu?

Odgovori na ova i druga pitanja će se razlikovati od organizacije do organizacije, ali važno je zajednički ih promisliti, jasno artikulisati i podeliti plan kako bi svi u vašoj organizaciji bili spremni da momentalno preduzmu korake za ograničavanje potencijalne štete.

Kao što je navedeno u Holistic Security Guide (Holističkom bezbednosnom vodiču) organizacije Tactital Tech, jedan od najboljih načina da se započne rad na planu za reagovanje u slučaju incidenta jeste da **definišete incident ili hitnu situaciju** u kontekstu vaše organizacije. Odlučite šta je zapravo "hitna situacija", tj. u kom momentu treba da primenite planirane korake i mere. Ovo je bitno jer je situacija ponekad nejasna. Zamislite slučaj gde izgubite kontakt sa kolegom na terenskom zadatku - koliko ćete čekati pre nego što to proglasite za hitnu situaciju? Ne želite da prenaglite, ali ako predugo čekate u određenim okolnostima posledice mogu biti katastrofalne.

Takođe je bitno da dobro razmislite i o potencijalnim **operativnim** koracima. Svakoj osobi dodelite jasnu ulogu koje su svesni i na koju su unapred pristali – to će smanjiti dezorganizovanost i paniku u slučaju hitne situacije. Razmotrite različite uloge koje ćete morati da preuzmete u pogledu bilo koje pretnje, kao i praktične aspekte reagovanja na hitnu situaciju. Ova bitna strategija za reagovanje u hitnim situacijama treba da obuhvata i kreiranje mreže podrške – široke mreže saveznika u koje mogu spadati porodica i prijatelji, vaša zajednica, lokalni saveznici, državni resursi kao i nacionalni i međunarodni saveznici poput NVO i novinara. Kako vaši saveznici mogu da vas podrže? Da li bi trebalo da ih unapred kontaktirate kako bi vam potvrdili da su voljni da vam pomognu u hitnoj situaciji i kako biste im preneli šta očekujete od njih?

Prilikom reagovanja na neki incident, delotvorna **komunikacija** izuzetno dobija na važnosti. Izaberite najbezbedniji i najdelotvorniji način komunikacije za svaki različiti scenario i identifikujte i rezervne kanale. Budite svesni da bi u hitnim slučajevima moglo biti korisno da posedujete jasne smernice o tome šta treba (i šta ne treba) saopštavati drugima, kada treba da komunicirate, koje kanale da koristite za to i sa kime bi trebalo da komunicirate. Takođe razmislite o uticaju nekog incidenta na reputaciju vaše organizacije i budite spremni da adekvatno reagujete. Postarajte se da glavna osoba zadužena za komunikacije (u nekim slučajevima to može biti prosto osoba koja upravlja vašim Facebook ili Twitter nalogom) bude svesna incidenta i da može da prati društvene mreže ili druge medije zbog potencijalnog efekta. Takođe bi trebalo da je pripremite da po potrebi odgovori na moguća pitanja javnosti ili predstavnika medija o incidentu. Ovo je naročito bitno kako biste predupredili potencijalne negativne pruče ili štetu po vašu reputaciju. Dok su svaki incident i kontekst drugačiji, iskrena i transparentna komunikacja često potpomaže uspostavljanje poverenja nakon nekog incidenta.

Kreiranje sistema za rano upozoravanje i reagovanje

Razmislite da uspostavite sistem za rano upozoravanje i reagovanje. To možda zvuči komplikovano, ali se u suštini svodi prosto na centralizovani dokument (digitalni ili fizički) koji treba konsultovati u hitnim slučajevima. U tom dokumentu bi trebalo da zapišete sve detalje o bezbednosnim pokazateljima i incidentima koji su se desili u određenom vremenskom periodu, date jasan opis planiranih koraka i naznačite šta treba realizovati kako bismo mogli da kažemo da se pretnja opet smanjila.

Trebalo bi takođe da sadrži korake koje treba preduzeti nakon incidenta kako biste zaštitili one umešane u njega i pomogli im da se fizički i emocionalno oporave. Sistem za rano upozoravanje i reagovanje može da obezbedi korisnu dokumentaciju koju (po potrebi) možete podeliti sa policijom ili tužilaštvom, naknadnu analizu onoga što se dogodilo i smernice za unapređenje vaše preventivne taktike i odgovora na pretnje u budućnosti.

Pored ovih važnih generalnih ideja na polju reagovanja na incidente, vaša organizacija bi trebalo da pripremi i specifične **tehničke** korake. U određenim slučajevima ove tehničke mere može da realizuje interno IT osoblje ili pak sistemski administratori. Na primer, ako vam se čini da je neki nalog elektronske pošte hakovan, vaši administratori naloga bi trebalo da budu spremni i u stanu da ugase ili isključe napadnuti nalog. Međutim, pojedini tehnički incidenti mogu zahtevati ekspertizu koju vaša organizacija trenutno ne poseduje. U takvim slučajevima, bitno je da formulišete listu pouzdanih eksternih tehničkih eksperata koji mogu da vam pomognu u slučaju incidenta. U nekim slučajevima, možda ćete hteti da unapred dogovorite uslove sa pružaocima usluga (kao što su host sajta ili konsultant za informacione tehnologije) kako biste se postarali da budu dostupni (i ne naplate vam dodatno) u slučaju da vam je potrebna tehnička pomoć oko incidenta.

Na kraju, ali ne i najmanje važno, trebalo bi da razmotrite **pravne** korake. Važno je da znate koju vrstu pravne zaštite imate, kao i sa kakvim pravnim obavezama ili posledicama se vaša organizacija može suočiti zbog krađe podataka ili drugih bezbednosnih incidenata. Kao prvi korak možete identifikovati pouzdanog pravnog savetnika koji se razume u specifične zakone i propise vaše zemlje ili lokalne oblasti. Odvojite vreme da sa tom osobom razmotrite potencijalne incidente i napravite plan onoga što ćete uraditi ako do istih dođe. Takođe je dobra ideja da sa ovim pouzdanmim pravnikom dogovorite da zastupa vas i vaše interese nakon incidenta ako za to bude bilo potrebe. U okviru ovih pravnih priprema se postarajte i da proučite pravne obaveze svojih dobavljača ili partnera. Da li treba da vas obaveste u slučaju da neko ukrade njihove podatke? Kakvu (ako ikakvu) podršku moraju da vam pruže u slučaju nekog incidenta? Dok budete sklapali ugovore i sporazume sa eksternim dobavljačima imajte na umu potencijalnu krađu podataka ili druge incidente.

Dok ne postoji jedan pristup kreiranju sistema za reagovanje u slučaju incidenata, od suštinskog je značaja da formulišete jasne operativne, komunikacione, tehničke i pravne planove. Toplo preporučujemo da tokom sastavljanja svog plana iskoristite odlične postojeće resurse osmišljene da pomognu organizacijama civilnog društva i drugim visokorizičnim grupama u osmišljavanju koraka za slučaj incidenta. U ove resurse spadaju **Digital First Aid Kit** (Digitalni komplet za prvu pomoć) koji su kreirale RaReNet i CiviCERT, **Online Harassment Field Manual** (Tehnički vodič za uzmeiravanje na internetu) organizacije PEN America, the Cybersecurity Campaign Playbook (Plan igre za kampanje na polju sajber bezbednosti) i **Cyber Incident Communications Plan Template** (Obrazac plana za komunikacije u slučaju sajber incidenta) Belfer Centra i **Digital Security Helpline** (SOS linija za digitalnu bezbednost) organizacije Access Now.

Koraci u slučaju incidenta

- **Kreirajte plan organizacije za reagovanje u slučaju incidenata i primenjujte ga.**
  - **Pokušajte da se setite svih mogućih incidenata i unapred pripremite adekvatne korake.**
- **Postarajte se da svi u organizaciji znaju kako ćete komunicirati i kakve tehničke korake ćete preduzeti u slučaju nekog incidenta.**
- **Postarajte se da razumete kakve oblike pravne zaštite i pravne obaveze imate.**
- **Budite spremni da svom osoblju pružite emocionalnu i socijalnu podršku koja im može biti potrebna nakon nekog incidenta.**

Prilog A: Preporučeni resursi

- Tactical Tech's Holistic Security Manual (Holistički bezbednosni priručnik); Creative Commons Attribution-ShareAlike 4.0 International License (Međunarodna licenca za slobodno deljenje)
  - Poglavlje 2.4 - Kako razumeti i popisati svoje informacije
  - Poglavlje 1.5 - Razgovor o pretnjama u okviru tima ili organizacije
  - Poglavlje 3.4 - Bezbednost u grupama i organizacijama
- The Electronic Frontier Foundation's Security Education Companion (Priručnik za obrazovanje na polju bezbednosti); Creative Commons Attribution 3.0 US License (Američka licenca za slobodno deljenje)
  - Threat Modeling Activity Handout (Uputstva za aktivnost modeliranja pretnji)
- Freedom of the Press Foundation's Phishing Prevention and Email Hygiene Guide ; Creative Commons Attribution 4.0 International License (Međunarodna licenca za slobodno deljenje)
- Freedom of the Press Foundation's Locking Down Signal Guide; Creative Commons Attribution 4.0 International License (Međunarodna licenca za slobodno deljenje)
- Electronic Frontier Foundation's Surveillance Self Defense (SSD) Guide (Vodič za samoodbranu od nadzora); Creative Commons Attribution 3.0 US License (Američka licenca za slobodno deljenje)
  - Šta treba da znam o enrkipciji
  - Komunikacija sa drugima
  - Odabir pravog VPN-a za vas
- Frontline Defenders' Guide to Secure Group Chat and Conferencing Tools (Vodič za bezbedne galatke za grupne četove i koferencije)
- Tactical Tech's Data Detox Kit (Paket za detoksikaciju podataka)
  - Let the Right One In: Make Your Passwords Stronger (Dopustite ulaz samo pravima: Učinite lozinke jačima)
  - Strengthen Your Screen Locks (Unapredite načine za zaključavanje ekrana)
- Center for Democracy and Technology's Elections Security Guide on Passwords (Bezbednosni vodič kroz lozinke); Creative Commons Attribution 4.0 International License (Međunarodna licenca za slobodno deljenje)
- Center for Democracy and Technology's Elections Security Guide on Two Factor Authentication (Bezbednosni vodič kroz dvostruku potvrdu identiteta); Creative Commons Attribution 4.0 International License (Međunarodna licenca za slobodno deljenje)
- Martin Shelton's Two Factor Authentication for Beginners (Dvostruka potvrda identiteta za početnike); Creative Commons Attribution 4.0 International License (Međunarodna licenca za slobodno deljenje)
- Tactical Tech and Frontline Defender's Security in a Box (Bezbednost u kutiji); Creative Commons Attribution-ShareAlike 3.0 Unported License (Licenca za slobodno deljenje)
  - Zaštitite svoje uređaje od malvera i pecanja (phishing)
  - Zaštitite svoje podatke od fizičkih pretnji
- SANS' Ouch! Newsletter: Stop That Malware (Bilten: Zaustavite taj malver)
- Apple's Device and Data Access When Personal Safety is At Risk (Pristup Apple uređajima i podacima kad vam je lična bezbednost ugrožena)
- Global Cyber Alliance Cyber Hygiene for Mission-Based Organizations (Sajber higijena za organizacije zasnovane na misiji)

Prilog B:
Početni set bezbednosnog plana

Iskoristite ovaj početni set kako biste hvatali beleške dok sa svojom organizacijom čitate ovaj priručnik i usvajate njegov sadržaj, te razmotrite data pitanja sa svojim kolegama kako biste pokrenuli produktivnu diskusiju.

Takođe obavezno prokonsultujte „osnovne elemente“ u svakom odeljku priručnika kako biste se postarali da pokrivate važne teme prilikom formulisanja vašeg bezbednosnog plana. Dok stignete do kraja priručnika, osnovni elementi, odgovori na predložena pitanja za diskusiju i vaše beleške bi trebalo da oforme osnovu uspešnog bezbednosnog plana!

Izgradnja kulture bezbednosti

Jake osnove: Obezbeđivanje naloga i uređaja

Bezvbedno prenošenje i skladištenje podataka

Bezbednost na internetu

Zaštita fizičke bezbednosti

Šta činiti kad stvari krenu po zlu

Izgradnja Kulture Bezbednosti

PITANJA KOJA VALJA RAZMOTRITI:

- Kad možete da zakažete razgovor na kome ćeti proći kroz bezbednosni plan sa celom organzacijom?
- Kojim danima ili u koje vreme biste mogli da organizujere redovne diskusije i obuke iz oblasti bezbednosti?
- Koje korake rukovodstvo može da preduzme kako bi bilo uzor dobrog ponašanja sa aspekta bezbednosti i demonstriralo svoju posvećenost bezbednosnom planu? Kako drugi članovi organizacije mogu da imaju ulogu u održavanju bezbednosti?

VAŠE BELEŠKE I IDEJE:

Jake osnove: Obezbeđivanje naloga i uređaja

PITANJA KOJA VALJA RAZMOTRITI:

- Kako ćete primeniti mere za bezbednost naloga – kao što su program za upravljanje lozinkama i 2FA – na nivou cele organizacije? Sa kakvim preprekama se možete susresti prilikom primene tih mera
- Kako će se vaša organizacija postarati da uređaji budu bezbedni i da se ažuriraju? U okviru tih aktivnosti, da li će organizaciji biti potreban plan za rešavanje problema nelicenciranog softvera ili računara?
- Kada je dobar momenat za organizovanje obuke celokupnog osoblja o opasnostima fišinga (phishing), malvera i najboljim praksama sa aspekta bezbednosti uređaja?

VAŠE BELEŠKE I IDEJE:

Bezvbedno prenošenje i skladištenje podataka

PITANJA KOJA VALJA RAZMOTRITI:

- Kako će vaša organizacija uvesti obostranu enkripciju poruka u cilju bezbedne komunikacije? Sa kakvim preprekama se možete susresti tokom tog procesa?
- Kako će vaša organizacija uvesti obavezu korišćenja bezbednih rešenja za deljenje fajlova na internom i eksternom nivou? Sa kakvim preprekama se možete susresti tokom tog procesa?
- Kako će vaša organizacija uvesti bezbedno rešenje za skladištenje podataka i pravljenje rezervnih kopija istih? Sa kakvim preprekama se možete susresti tokom tog procesa?

VAŠE BELEŠKE I IDEJE:

Bezbednost na internetu

PITANJA KOJA VALJA RAZMOTRITI:

- Kako će vaša organizacija uvesti uslove za bezbedno pretraživanje interneta kao što su HTTPS, pouzdani pretraživač i, po potrebi VPN za celokupno osoblje?
- Koji će biti ključni elementi politike vaše organizacije za društvene mreže? Kako ćete sprovesti tu politiku?
- Kako će vaša organizacija zaštiti svoj sajt i druge resurse na internetu?

VAŠE BELEŠKE I IDEJE:

Zaštita fizičke bezbednosti

PITANJA KOJA VALJA RAZMOTRITI:

- Kako će organizacija distribuirati i sprovoditi svoju politiku po pitanju pristupa kancelarijskom prostoru i potencijalnih gostiju u istom?
- Ko je zadužen da pripremi osoblje za izazove na polju fizičke i digitalne bezbednosti sa kojima se mogu suočiti na poslovnom putovanju?
- Koje korake osoblje može da preduzme kako bi se postaralo za sigurnost i bezbednost uređaja kako u kancelariji tako i na putu?

VAŠE BELEŠKE I IDEJE:

Šta činiti kad stvari krenu po zlu

PITANJA KOJA VALJA RAZMOTRITI:

- Kako će organizacija distribuirati i sprovoditi svoju politiku za reagovanje u slučaju incidenata?
- Da li su članovima osoblja kojima je možda potrebna emocionalna ili socijalna podrška nakon incidenta dostupni određeni resursi? Ako nisu, kako bi organizacija mogla da takve resurse obezbedi u slučaju incidenta?

VAŠE BELEŠKE I IDEJE:

Prilog C:
Citati slika

Page 17: CNP Collection, “Security Protection Anti-Virus Software cms”, 2014, digital image, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.
Page 24: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.
Page 26: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
Page 29: "Microsoft Loading Screen," digital image, Kompass, September 23, 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.
Page 30: Mateuz Dach, "Turned-on iPhone and Displaying Icons," 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
Page 33: Crete-Nishihata, "Process For a Phishing Email Sent in 2016," digital image, University of Toronto, January 30, 2017, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/.
Page 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Page 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, January 17, 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
Page 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 50: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Page 55: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.
Page 60: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Page 62: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, April 25, 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
Page 64: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Page 69: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, October 1, 2017, https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE