Priručnik o bezbjednosti na internetu:

kiber higijena za javne institucije i mala i srednja preduzeća

Vladan Babić i Aleksandar Bratić

Oktobar 2022

DCAF Geneva Centre for Security Sector Governance

O DCAF-u

DCAF – Ženevski centar za upravljanje sektorom bezbjednosti je posvećen poboljšanju bezbjednosti država i njihovog stanovništva u okviru demokratskog upravlja, vladavine prava, poštovanja ljudskih prava i rodnoj jednakosti. Od svog osnivanja 2000. godine, DCAF je pridoneo kreiranju održivijeg mira i razvoja pomažući države partnere i međunarodne činioce koji podržavaju te države u poboljšanju upravljanja sektorom bezbjednosti kroz inkluzivne i participativne reforme. On kreira inovativne proizvode znanja, promoviše dobre norme i prakse, daje pravne savjete i savjete o politikama i podržava građenje kapaciteta državnih i nedržavnih činioca u sektoru bezbjednosti.

DCAF - Ženevski centar za upravljanje sektorom bezbjednosti
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Ženeva, Švajcarska
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Photo credit: Shutterstock, image contributor: Illus_man
Design & layout: DTP studio

Ova publikacija je razvijena u okviru projekta „Dobro upravljanje sajber bezbjednošću na Zapadnom Balkanu“ koji sprovodi DCAF – Ženevski centar za upravljanje sektorom bezbjednosti, uz podršku Ministarstva spoljnih poslova Velike Britanije (UK FCDO - United Kingdom’s Foreign, Commonwealth and Development Office)

Sadržaj

Uvod

Ovaj dokumenat je pregled minimalnih standarda za uspostavljanje sistema kiber higijene u javnim institucijama i u malim i srednjim preduzećima (MSP). U njemu su predstavljene mjere koje svaka organizacija treba uvesti kako bi obezbijedila odgovarajući nivo informatičke bezbjednosti za svoje informatičke sisteme.

Ovdje je fokus na davanju uvoda u važnost kiber higijene i preporuka o jednostavnim koracima koji će poboljšati kiber bezbjednost u vašoj organizaciji.

Ukratko, higijena u bezbjednosti je ista kao pranje ruku. Kada je mađarski doktor Ignaz Semmelweis rekao tri jednostavne riječi „perite vaše ruke“ u 1850. godini, on je stvorio revoluciju u medicini, čak i ako ga niko nije ozbiljno shvatao ispočetka. On je uočio da je dobra higijena neraskidivo vezana sa dobrim zdravljem, a tokom vremena su podaci dokazali da preventivno pranje ruku stvarno smanjuje infekcije.

Kiber higijena se slično tome odnosi na prakse koje imaju za cilj spriječavanje infekcije zlonamjernim softverom (malware), kao i kiber upade i gubljenje ili korumpiranje podataka i održavanje zdravog kiber okruženja. Time se osigurava zdravlje sistema i poboljšava kiber bezbjednost na isti način na koji rutinsko pranje ruku pomaže u spriječavanju širenja bolesti.

Imajući u vidu da sve organizacije u današnjici koriste informatičke sisteme za poslovanje, sve su pod rizikom od izlaganja različitim kiber napadima koji mogu spriječiti funkcionisanje informatičkih sistema ili blokirati pristup podacima. Prema tome, svaka organizacija mora da zaštiti svoje informatičke sisteme i mora da uspostavi procedure i politike i ponudi redovnu obuku, kako bi uspostavila odgovarajuće prakse kiber higijene.

Definicije

Postoje mnoge različite definicije kiber higijene i sve su tačne.

- Digital Guardian naziva kiber higijenu kao „prakse i koraci koje korisnici računara i drugih uređaja preduzimaju kako bi održali zdravlje sistema i poboljšali bezbjednost na internetu“.
- Kaspersky Lab potencira da se kiber higijena tiče „obučavanja samog sebe za stvaranje dobrih navika u vezi sa kiber bezbjednošću, kako bi bili korak ispred kiber prijetnji i bezbjednosnih problema na internetu“.
- Časopis Security opisuje kiber higijenu u pogledu toga da „trebate biti sigurni da kod vas funkcionišu osnovne kontrole za bezbjednost i da se one konzistentno primjenjuju u cjelom vašem okruženju“.
- CyberSecurity Forum kaže da je kiber higijena „kolokvijalni izraz koji se odnosi na najbolje prakse i druge aktivnosti koje mogu preuzeti administratori i korisnici kompjuterskih sistema kako bi poboljšali svoju kiber bezbjednost dok rade uobičajene aktivnosti na internetu kao pretraživanje interneta, slanje i-mejlova, slanje poruka, itd.“.
- Blog Endpoint objašnjava kiber higijenu kao „zbir uobičajenih praksi za bezbjedno rukovanje kritičnim podacima i obezbijeđivanje mreža. To je kao lična higijena, kada razvijete rutinu malih, posebnih aktivnosti koje spriječavaju ili ublažavaju zdravstvene probleme“.

Drugim rečima, kiber higijena je zbir osnovnih bezbjednosnih praksi koje može preuzeti svaki član osoblja kako bi zaštitili sebe, kao i zdravlje ličnog i organizacijskog hardvera i softvera u kompjuterskim sistemima.

Uobičajene mjere

Dobra kiber higijena zahtijeva sprovođenje određenih uobičajenih mjera, od uspostavljanja standardizovanih procedura i politika do redovnih obuka koje pomažu zaposlenima da razumeju kiber prijetnje koje se stalno mijenjaju. Priroda i karakter nekih od ovih prijetnji su objašnjeni u daljem tekstu (vidite Uobičajene kiber prijetnje). Međutim, prvo su predstavljeni ključni elementi djelotvornog programa za kiber higijenu, kao i dobre prakse.

Analizirajte sisteme i uspostavite procedure i politike

Popis resursa

Održavajte popis hardvera i softvera

Upravljanje IT hardverom i softverom (IT resursi) može biti ogroman zadatak, posebno ako se oprema i osoblje stalno kreću ili mijenjaju, ali je to isto upravljanje i neophodno. Hardver, softver i svi mrežni uređaji i uređaji koji nisu mrežni se smatraju resursima u ovom pogledu.

Održavanje popisa hardvera i softvera će podržati različite procese u vašoj organizaciji, kao:

- Upravljanje incidentima
- Upravljanje problemima
- Upravljanje promenama

Tokom ovih procesa postavljaju se slična pitanja:

- Šta radi određeni IT resurs?
- Kakav operativni sistem koristi?
- Koje se aplikacije čuvaju u/na resursu?
- Kako izgleda topologija mreže?
- Ko ima pristup resursu?
- Ko je odgovoran za njega?

Da odgovorimo na ova pitanja, potrebna je centralizovana baza informacija. Prema tome, prvi korak u uspostavljanju praksi kiber higijene je **standardizacija popisa softvera i hardvera** putem:

1. Dokumentovanja osnovnog bezbjednosnog držanja organizacije
2. Standardizacije istog u cjeloj organizaciji na osnovi politika i procedura
3. Monitoringa i reakcije na odstupanja
4. Smanjenja svih slabih strana uvedenih nepoznatim hardverom i softverom

Prednosti održavanja popisa hardvera i softvera su očite i uključuju:

- Kontrolu nad IT okruženjem
- Kontrolu softverskih resursa (verzija, zakrpa, zavisnost, odgovornost i dokaz koncepta (PoC))
- Kontrolu hardverskih resursa (verzija, kritičnost, dokaz koncepta, zavisnost)
- Efektivno upravljanje
- Bolje srednje vrijeme do ponovnog uspostavljanja usluga (MTTRS)

Popis informacija

Održavajte popis osijetljivih ili kritičnih informacija

Zaštita osijetljivih informacija - koja uključuje odgovarajuće etiketiranje, otkrivanje i rukovođenje njima – je veliki izazov. Može biti teško shvatiti kako korisnici stupaju u interakciju sa ovim informacijama i kako ih razmijenjuju. Prema tome, nije čudno što više od polovine korporativnih podataka su „tamni“, što znači da nijesu klasifikovani, zaštićeni ili rukovođeni.

Važno **je razumjeti vaše okruženje podataka i identifikovati važne podatke u vašoj sredini**. U tu svrhu, važno je kreirati **politiku za klasifikaciju podataka** kao prvi korak. Postoje različite sheme za klasifikaciju koje se mogu koristiti na osnovu potrebe, ali donji primer sadrži tri nivoa:

- *Ograničen nivo* – osijetljivi podaci koji predstavljaju veliki rizik ako budu kompromitovani; njima pristupaju samo oni koji imaju potrebu za to.
- *Povjerljivi nivo* – umjereno osijetljivi podaci kojima se pristupa samo interno.
- *Javni nivo* – podaci koji nisu osijetljivi i predstavljaju mali ili nikakav rizik ako im se pristupi.[1]

Kao drugi korak, podaci trebaju biti šifrirani, posebno svi podaci koji imaju oznaku „ograničeno“.

1 https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data

Na kraju, treba sprovesti **sistem za spriječavanje gubitka podataka** za otkrivanje potencijalnih upada u podacima/transmisijama za izvlačenje podataka i njihovo spriječavanje putem praćenja, otkrivanja i blokiranja osijetljivih podataka tokom upotrebe, u kretanju i u mirovanju.

Ovo treba da uključuje određeno skeniranje i automatizaciju (za šta je Microsoft dobar alatka) i treba da pokriva:

- Spremište na samoj lokaciji
- Office aplikacije
- SharePoint lokacije
- Razmjenu
- Cloud i SaaS (softver kao usluga) aplikacije koje nisu Microsoft aplikacije

Procjena rizika

Identifikacija rizika

Upravljanje rizikom zahtijeva razumjevanje prijetnji sa kojima je suočena vaša organizacija i korake koji se mogu preuzeti kako bi spriječili, smanjili ili spremili se za situaciju koja može, ali i ne mora, da se dogodi.

Postoje tri oblasti rizika po informatičke sisteme:

- **Ljudski rizik**, kao prijevara, krađa ili ljudska greška.
- **Prirodni rizik**, kao poplave, požari ili zemljotresi.
- **Tehnički rizici**, kao defekti u softveru, hardveru ili nedostatak znanja.

Kao početna tačka, procjena rizika uključuje dodeljivanje vrijednosti kritičnim resursima, uključujući i finansijske i reputacijske. Ovo vam pomaže da počnete procjenu kolika je težina svake posebne prijetnje. Jedan djelotvoran način za ovo je da dodijelite ocjenu svakom scenariju – prvo, u pogledu vjerovatnoće da će nešto da se dogodi i drugo, o šteti koja bi nastala ako se to dogodi.

To će vam dati bolju ideju gdje da fokusirate vaše aktivnosti i pomoći će vam da odlučite kako da pristupite utvrđenim rizicima, na primer putem:

- **Izbjegavanja**, kada rizici nijesu neposredna briga vašem poslovanju
- **Smanjenja**, kada rizici zahtijevaju implementaciju novog bezbjednosnog rješenja
- **Prihvatanja**, kada je mala vjerovatnoća da će se rizik dogoditi ili je iznad tekućih kapaciteta
- **Prenošenja**, kada se rizik može osigurati

Procedura za bekap (pravljenje rezervnih kopija)

Uspostavite proceduru za redovni bekap

Isključivo je važno imati bekap proceduru. Cilj je kreirati kopiju podataka koja se može vratiti u slučaju defekta u podacima – koji može biti rezultat softverskih i hardverskih defekata, korumpiranja podataka ili ljudski izazvanih događaja kao što su zlonamjerni napadi ili slučajno brisanje. Dobro osmišljena politika za bekap i povratak podataka je od suštinskog značaja i predstavlja zadnju liniju odbrane za jednu organizaciju.

Skoro sve organizacije imaju postavljene bar neke bekap sisteme. Pitanje je, da li sistem adekvatno zadovoljava potrebe vaše organizacije i usluge koje dajete? Važno je ne raditi bekap samo u ime bekapa, već da radite bekap kako bi mogli da se povrate ključni podaci po potrebi i sa što je moguće manjim uticajem po poslovanje.

Na primjer, rezervne kopije trebaju pokrivati svakodnevni rad, ali isto tako trebaju da omoguće rad i kada sistem nije u funkciji Ili, u slučaju katastrofe, podaci se trebaju čuvati na lokaciji odakle mogu biti povraćeni.

Organizacije trebaju biti realne u kreiranju bekap politika i trebaju pripremiti pisani plan za bekap koji sadrži detalje o tome:

- Šta se stavlja na bekap?
- Gdje se nalazi bekap?

- Koliko često se radi bekap?
- Ko je zadužen da vrši bekap?[2]

Uvijek dajte najviši prioritet ključnim podacima

Utvrdite raspored bekapa na osnovu toga koliko je posla vaša organizacija voljna da rizikuje da izgubi. Ne zaboravite da su baze podataka i vaše računovodstvene datoteke vaši najkritičniji resursi i da se trebaju praviti rezervne kopije prije i nakon svake značajne upotrebe. Za većinu organizacija ovo znači da se bekap ovih datoteka treba raditi svaki dan. Međutim, neprofitne organizacije koje unose velike količine podataka trebaju razmisliti o vršenju bekapa svojih baza podataka nakon svakog značajnog unosa, čak i ako je to nekoliko puta na dan. Bekap osnovnih datoteka kao što je dokumentacija (u direktorijum „Your Documents“, na primer) i datoteke elektronske pošte se trebaju raditi najmanje jednom sedmično ili čak jednom dnevno.[3]

Uvek testirajte vaš bekap

Testiranjem rezervnih kopija možete da utvrdite da li funkcionišu uredno. Ovo vam omogućava da izmjerite koliko će brzo vaše poslovanje biti vraćeno nakon defekta i da utvrdite sva pitanja na koja treba odgovoriti.

Koristite pravilo 3-2-1 za bekap

Profesionalci preporučuju praksu bekap redundantnosti poznatu kao pravilo 3-2-1. Ovo se prevodi u tri kopije vaših podataka, na dva lokalna (ali različita) uređaja i jednu kopiju na uređaju koji se nalazi van lokacije. Ovim se pristupom u velikoj mjeri umanjuje šansa da će podaci biti izgubljeni.

U suštini, kopiranje važnih datoteka na hard disk ili USB ne predstavlja kreiranje dovoljnog bekapa. Hard diskovi se kvare. Dalje, USB diskovi i SD kartice su mali i lako se gube. Dobar bekap sistem zahtijeva redundantnost u obliku nekoliko kopija koje su zaštićene u slučaju nepredviđenog incidenta.

Koristite skladištenje podataka na daljinu

Rješenja za skladištenje podataka van lokacije ili na cloud sistemu su rentabilan i efikasan način da obezbijedite da su vaši podaci dalje od vaše lokacije, ali još uvek vama dostupni.

Radite česti i redoviti bekap

Danas postoje alatke koje vam omogućavaju da automatski radite bekap i oni su i laki za korišćenje i jeftini.

Plan za odgovor u slučaju incidenta

Uspostavite tim za reakciju u slučaju incidenta

Tim za reakciju u slučaju incidenta je grupa IT profesionalaca unutar organizacije koji su zaduženi za pripremanje i reagovanje na svaki hitni IT slučaj koji nastane.

Ovi stručnjaci uobičajeno dolaze iz različitih struka i uloga i imaju komplementarne tehničke vještine, što omogućava timu da bude sposoban da odgovori na široki dijapazon bezbjednosnih incidenata, uključujući i upade ili kiber napade.

Tim za reakciju na incidente je uobičajeno odgovoran za pripremu plana reakcije (pogledajte dole), kako bi se mogao preuzeti metodički pristup u rješavanju bezbjednosnih incidenata i upravljanju sa posledicama. Tim isto tako testira i rješava slabe tačke sistema, održava snažne bezbjednosne prakse i daje podršku mjerama za suočavanje sa incidentom.

Kreirajte plan za reakciju na incidente (PRI)

PRI je alat za upravljanje rizikom koji definiše kontrole za smanjenje upada ili incidenata i koji utvrđuje šta treba raditi, ako se dogodi upad. Njime će se smanjiti rizik od upada, pod uslovom da organizacija ima tim za reakciju u slučaju incidenta.

Važno je ne zaboraviti da će se incidenti redovito događati u svakom poslovnom okruženju. Vaš tim za

2 Your Organization’s Backup Strategy | Articles and How-tos (techsoup.org)
3 Your Organization’s Backup Strategy | Articles and How-tos (techsoup.org)

reakciju na incidente će morati da utvrdi prioritete i na koje incidente se mora reagovati odmah, a na koje se može reagovati kasnije. **Opseg i ciljevi tima za reakciju na incidente se utvrđuju od strane rukovodstva u PRI**.

Dobro definisane procedure kojima se opisuju odgovarajući odgovori na incidente su od suštinskog značaja, posebno što se mogu dogoditi situacije u kojima se incidenti moraju prijaviti lokalnim organima, u zavisnosti od propisa kojima se reguliše vaša industrija. Struktura PRI zavisi od okvira koji se koristi, kao što su ISO 28035 ili NIST (priprema, otkrivanje i analiza, izolacija, iskorijenjivanje i povratak, aktivnosti nakon incidenta).

Kada se dogodi incident kritično je da pratite vaš PRI, koji će sadržati procedure za reakciju na različite vrste incidenata.

Mnogo se incidenata izazivaju od strane korisnika unutra, tako da je važno obučiti zaposlene i druge krajnje korisnike o odgovarajućoj kompjuterskoj bezbjednosti i isto tako pratiti njihovo korišćenje kako bi bili sigurni da oni nijesu uključeni u maliciozne radnje. Kako bi to uradila, organizacija mora:

- Objasniti krajnjim korisnicima kako da prijave incident, sa odgovarajućim informacijama o i-mejl adresama, portalima, telefonskim centralama i centrima za pomoć.
- Pripremiti unutrašnju stranu koja sadrži potrebne informacije za ispravnu prijavu.
- Organizovati godišnje bezbjednosne obuke koje uključuju uputstva o tome šta raditi u slučaju incidenta (malware prijava, prijava o curenju podataka, spam i phish prijava, itd.).
- Obučiti krajnje korisnike da isključe mašine od interneta kada se dogodi incident, ako vaša organizacija nema postavljene tehničke mjere za automatsku izolaciju inficiranog housta.
- Naučiti krajnje korisnike da ne rade nijednu radnju nakon incidenta, osim ako nije odobrena od tima za reakcije na incidente, kako bi se sačuvali neophodni dokazi za moguću forenzičku istragu.
- Obučiti krajnje korisnike da daju što je više moguće informacija o incidentu, uključujući:
    * Šta se dogodilo?
    * Kada se to dogodilo?
    * Gdje se dogodilo?
    * Ko je bio uključen?
    * Koje dopunske informacije mogu da ubrzaju prikupljanje informacija u fazi trijaže?

Kontinuitet i oporavak od katastrofe

Pripremite plan za kontinuitet poslovanja i oporavak od katastrofe

Dok se poslovni kontinuitet odnosi na povratak, oporavak i održavanje cjelokupnog poslovanja jedne organizacije u slučaju velikog neočekivanog problematičnog događaja, oporavak od katastrofe se ovdje odnosi na konkretne aktivnosti koje su povezane sa komunikacijskom i tehnološkom infrastrukturom i podacima.

Kada se dogodi neplanirani incident, suštinsko je da organizacija može nastaviti sa radom što je prije moguće. Plan za kontinuitet poslovanja je u cjelosti usmjeren ka tom cilju, a plan za oporavak od katastrofe utvrđuje kako organizacija može efikasno i efektivno da povrati pristup svojim kritičnim podacima i tehnološkim sistemima.

Prema tome, plan za oporavak od katastrofe u suštini odgovara na dve stvari:

- povratak IT i komunikacijskih sistema i tehnologija; i
- dobijanje punog pristupa čistim podacima, dobrog kvaliteta, na koje se oslanja organizacija.

Vrste neplaniranih problematičnih događaja koji mogu da dovedu do sprovođenja plana za oporavak od katastrofe uključuju:

- Prirodne katastrofe
- Rat ili terorizam
- Javna previranja i metež
- Nesreće ili ljudske greške
- Kiber kriminal

Ti događaji mogu da dovedu do različitih nivoa problema, koji utiču na:

- Jedan centar za podatke ili zgradu
- Cjelu organizaciju
- Lokalne sisteme ili sisteme na nivou grada
- Regionalne ili nacionalne sisteme
- Globalne sisteme

Djelotvoran plan za oporavak od katastrofe koji svodi prekid na minimum treba uzeti u obzir potencijalne komercijalne gubitke i uticaj na reputaciju organizacije i treba pomoći organizaciji da izbegne regulatorne ili zakonske prekršaje.

U planu za oporavak od katastrofe se trebaju detaljno opisati šest elementa:

- Cjeloviti popis resursa (hardver, softver i podaci)
- Minimalni prihvatljivi uticaj (prekid rada i nivo usluge)
- Dokumentacija o procesima i procedurama za oporavak od katastrofe (ugovori na nivou usluge, prioriteti za oporavak, resursi za bekap, ovjera podataka)
- Odgovornosti za oporavak od katastrofe, operativni i ovlašćujući; tj. ko radi aktivnosti za oporavak od katastrofe i ko ih odobrava
- Plan za komunikaciju i odnose sa javnošću (kako bi dali odgovor ključnim činiocima i regulatorima i zaštitili reputaciju organizacije)
- Obuka (plan je beskoristan ako niko ne zna kako da ga upotrebi)

Zaštitite vaš informatički sistem

Zakrpe (patch) i ažuriranje (update)

Zakrpite i ažurirajte vaš operativni sistem i softver aplikacija

Ponekad može biti mučno da se vaši sistemi i aplikacije ažuriraju, ali je vrlo važno da se to uradi, zbog nekoliko razloga:

- **Bezbjednost**: ažuriranje pomaže u **obezbjeđivanju vašeg kompjutera od napada**. Kao što se otkrivaju novi napadi, tako se identifikuju propusti koje kiber kriminalci koriste kako bi kompromitovali vaš operativni sistem i aplikacije. Ti se propusti rješavaju ažuriranim verzijama softvera (update).
- **Nove mogućnosti**: Microsoft, Apple, Android i drugi nude nove mogućnosti kod ažuriranog softvera, a drugi softver drugih kompanija se ponekada ne može koristiti, ako se prvo ne ažuriraju ovi sistemi.
- **Popravke**: Ne dolazi svaki problem od virusa. Ponekad, problemi nastaju u sistemima i softverima i jednostavno se trebaju popraviti. Mnoge greške koje utiču na krajnje korisnike se rješavaju ažuriranim verzijama.

Znači, pametno je **koristiti automatsko ažuriranje za sisteme i aplikacije**. Na taj način se automatski preuzimaju osnovne bezbjednosne popravke koje rješavaju slabe tačke sistema.

Ne zaboravite: kada se pojavi taj mali prozorčić za update, to može biti dobra stvar; ali ipak nije dobro klikati na slepo.

Bezbjedne konfiguracije

Koristite bezbjedne konfiguracije za sve uređaje i softver

Jedan način da zaštitite ljude i organizaciju od zlonamjernih aktivnosti je da koristite bezbjedne konfiguracije za uređaje i softver. Istovremeno, ovo predstavlja veliki izazov jer uvodi skoro stalnu potrebu za nove zakrpe operativnog sistema, nadgrađivanje aplikacija i mijenjanje mreža. Prema tome, primarni cilj je **dokumentovanje svih ažuriranja i promjena**, kako bi se imao uvid u konfiguracije svih sistema.

Kada se vrše izmjene neke aplikacije, to istovremeno zahtijeva mijenjanje i ažuriranje dokumentacije koja je kreirana za taj resurs. Dobra dokumentacija treba da omogući ponovnu izgradnju cijele instance od samog početka i treba da uključuje:

- **Evidenciju (log) promjena** operativnog sistema i aplikacija (update), promjene mreže, nove instance aplikacije, itd. Sve to mora biti adekvatno dokumentovano i praćeno.
- **Spisak svih resursa** u vašoj organizaciji. Sav hardver i softver treba biti identifikovan i dokumentovan.
- **Bezbjednosnu osnovu** za resurse. To je ugovoreni minimalni standard bezbjednosti koji se odnosi na, na primer, isključivanje nepotrebnih usluga, brisanje korisničkih naloga za goste, izloženost javnom internetu, itd.
- **Proces provjere i odobrenja** koji je lako pratiti. Dobra je praksa da vršite proveru vaših konfiguracija i postavki s vremena na vrijeme, jer incidenti u vašem okruženju vam mogu dati ideju o tome šta treba promjeniti. Isto tako, pojedinci ne trebaju mijenjati postavke na osnovu vlastitih potreba, već trebaju da prođu kroz standardni proces odobrenja.
- **Evidencija promjena konfiguracija**.

Dokumentacija treba isto tako da uključuje:

- Dijagrame mreža i uređaja, kao i shemu fizičkih centara podataka
- Parametre za okruženje za rad aplikacija:
    * Uspostavljena osnova koju treba slijediti
    * Firewall postavke, patch verzije, verzije OS
- Standardi i konvencije za imenovanje:
    * Uređaja (naziv i broj resursa na etiketi, naziv kompjutera, lokacija, serijski broj)
    * Mreža (etiketiranje portova)
    * Konfiguracija domena (imena korisničkih naloga, i-mejl adresa)
- IP shema

Za krajnje korisnike, bezbjedna konfiguracija zahtijeva:

- Uklanjanje i isključivanje svih nepotrebnih korisničkih naloga
- Izmjenu fabričkih lozinki ili lozinki koje je lako pogoditi („slabe lozinke“)
- Uklanjanje i isključivanje nepotrebnog softvera
- Isključivanje svih opcija za automatsko izvršenje softvera koje omogućavaju izvršenje datoteka bez odobrenja korisnika

Osijetljivi podaci

Šifrirajte sve osijetljive podatke

Šifriranje (enkripcija) je proces kodiranja podataka kako ne bi mogli biti pročitani bez određenog ključa. Na primjer, vlasnici šifriranih podataka mogu da ih dekodiraju koristeći lozinku, biometrijske informacije ili drugu vrstu ključa.

Šifriranje je kritičan element kiber bezbjednosti i može se koristiti na različite načine kako bi podaci ostali povjerljivi i privatni, kao što su bezbjedni (HTTPS) veb sajtovi, u bezbjednim aplikacijama za slanje poruka i i-mejl usluga i kroz virtuelne privatne mreže (VPN). Šifriranje štiti informacije dok se one aktivno kreću sa jedne lokacije na drugu (tj. u tranzitu), od pošiljaoca do primača, a isto tako štiti i informacije u mirovanju. Ako neko dobije pristup bazi podataka u kojoj postoje šifrirane informacije, šifriranje predstavlja dopunski sloj bezbjednosti.[4]

Drugim rečima, **šifriranje pomaže u zaštiti osijetljivih i privatnih informacija čineći ih nečitljivim za kiber kriminalce**, čak i u slučaju da izvuku te informacije.

Prepoznavanje osijetljivih informacija u vašem posebnom okruženju koje treba šifrirati je od vitalnog značaja i to, između ostalog, uobičajeno uključuje:

- Informacije sa ličnim identifikatorima
- Finansijske podatke

4 Should I Encrypt Sensitive Files on My Computer? - Experian

- Zdravstvene podatke
- Brojeve kreditnih kartica

Suzbijanje zlonamjernog softvera (malware)

Uvođenje anti-malware softvera

Malware ili zlonamjerni softver je svaki program koji je osmišljen da vrši neželjene ili štetne funkcije koje utiču na kompjutere, servere i mreže. Prema tome, anti-malware softver je neophodan deo bezbjednosnih alata.

Pre dosta godina, kompanije za kiber bezbjednost su pokušavale da kreiraju univerzalno anti-virusno rješenje koje može da odgovori na sve naše potrebe u jednom proizvodu. Ipak, to više nije djelotvorno, jer su kiber kriminalci evoluirali. Prijetnja koju predstavljaju stalno postaje sve sofisticiranija, što vodi kompanije da razvijaju posebne anti-malware programe.

Važno je razumjeti da su svi virusi malware, ali nisu svi zlonamjerni softveri virusi. Kompjuterski virus se vlastitom replikacijom širi od korisnika na korisnika, a anti-virus programi identifikuju poznate prijetnje otkrivanjem unikatnih potpisa. Međutim, moderni malware skeneri koriste heurističko otkrivanje koje može proaktivno tražiti zlonamjerni kod.

Anti-malware rješenja će blokirati najveći deo zlonamjernih i potencijalno neželjenih programa i skeniraće ulazne podatke kako bi spriječili da se zlonamjerni softver izvrši na uređaju, promjeni postavke ili izvrši dopunski kompromitovani softver. Oni isto tako blokiraju korisnike od pristupanja veb sajtovima za koje je poznato da distribuiraju zlonamjerni kod (u phishing i ransomware napadima).

Osim toga, anti-malware softver nudi:

- Zaštitu u realnom vremenu
- Skeniranje pri uključivanju uređaja
- Skeniranje spoljašnjih uređaja
- Zaštitu osijetljivih informacija
- Zaštitu od spama i krađe identiteta

Firewall (vatrozid)

Uvedite firewall

Firewall pruža zaštitu od kiber napada pomažući u čuvanju kompjutera i mreža. Firewall može biti i softverski i hardverski, na uređaju ili mreži, ali svi rade na isti način vršeći provjeru saobraćaja i blokirajući neželjene paketiće.

Firewall u velikoj mjeri smanjuje rizik po pojedince i organizacije. Organizacije koje ne koriste firewall samo olakšavaju posao kiber kriminalcima, dajući im potencijalni pristup sistemima i datotekama, kao i mogućnost da šire zlonamjerni sadržaj. Prema tome, adekvatno konfigurisani, održavani i praćeni firewall je ključan u zaštiti vaših podataka, vaše mreže i vaših uređaja.

Između ostalog, firewall vas štiti od:

- Prijavljivanja na daljinu
- Otmice i-mejl sesija
- Slabih tačaka u aplikacijama i OS
- Onemogućavanja usluga (DoS)
- I-mejl bombi
- Malicioznih makroa

WI-FI mreže

Zaštitite vaše WI-FI mreže

WI-FI mreže trebaju biti bezbjedne, šifrirane i sakrivene:

- **Enkripcija bežičnih mreža mora biti uključena**. Ona je suštinska za sigurnost. Zbog toga, vaš ruter mora podržavati WPA2 enkripciju i mora biti zamijenjen ako je ne podržava.
- **Ažurirajte softver sa novim bezbjednosnim verzijama i zakrpama**.
- Razmislite o lokaciji rutera kao o pitanju bezbjednosti. Ljudi često nisu svijesni da ruter koji se nalazi pored vrata ili prozora povećava šansu da će WI-FI signal biti presretnut od osobe sa malicioznim namerama. Kako bi poboljšali vašu WI-FI bezbjednost, **najbolje je da postavite ruter što je moguće bliže sredini vaše kancelarije**, jer time smanjujete šansu da se hakeri povežu na vašu mrežu.
- **Uključite filtriranje MAC adresa** kako bi kontrolisali uređaje koji imaju pristup vašoj mreži.
- **Isključite upravljanje sa daljine**.
- **Kreirajte posebnu WI-FI mrežu za klijente**, kako ne bi koristili vašu internu mrežu.

Postavke internet pretraživača

Konfigurišite bezbjednosne postavke internet pretraživača

Internet pretraživači postoje na skoro svakom uređaju, Zbog toga što njih stalno koristimo u svakodnevnom životu od suštinske važnosti je da ih bezbjedno konfigurišemo, posebno jer se oni uobičajeno koriste sa osnovnim fabričkim postavkama.

Internet pretraživači predstavljaju važnu metu napada za kiber kriminalce, a nebezbjedni pretraživač može da izloži korisnika ili organizaciju na instalaciju malicioznih sadržina bez znanja korisnika. U nekim slučajevima, to može da dovede do gubitka kontrole nad uređajem, korišćenja korisničkih informacija ili čak upotrebe uređaja za napad na druga lica.

Svaki internet pretraživač (Firefox, Chrome, DuckDuckGo, Brave, itd.) treba biti bezbjedan. U tome, uvijek uradite sledeće:

- **Uključite automatsko ažuriranje**. Ovaj ***ključni korak*** će zaštiti vašu organizaciju od mnogih slabih tačaka koje se otkrivaju svakodnevno. To je suštinska komponenta dobre kiber higijene vašeg internet pretraživača koja će vam pomoći da ostanete sigurni i bezbjedni.
- B**lokirajte pop-up obavještenja, plugin softverske dodatke i phishing sajtove**. Većina pop-up obavještenja su reklame, koje mogu biti zaražene zlonamjernim sadržinama, a plugin dodaci su poznati po svojim rizicima po bezbjednost.
- **Nemojte čuvati lozinke u pretraživaču**. Ne preporučuje se ova pogodna navika jer, ako je pretraživač kompromitovan, kompromitovani su i svi akreditivi koji se čuvaju u njemu.
- **Isključite kolačiće (cookies) trećih strana**.
- **Deinstalirajte sve ekstenzije pretraživača koje ne koristite**.
- **Redovno ažurirajte sve ekstenzije koje koristite**.

Lični izbor isto tako utiče na bezbjednost pretraživača, kao što je korisnički pristup **https sajtovima umjesto http sajtovima**.

Mobilni uređaji

Obezbjedite mobilne uređaje

Mobilni uređaji mogu da kreiraju značajne bezbjednosne i upravne izazove, osobito ako sadrže povjerljive informacije ili ako mogu pristupiti poslovnoj mreži.

Za kontrolu upotrebe mobilnih uređaja, organizacije trebaju tražiti od korisnika da:

- štite uređaje lozinkama;
- šifriraju sve podatke; i

- instaliraju bezbjednosne aplikacije koje spriječavaju krađu informacija kada telefon koristi javne mreže.

Organizacije isto tako trebaju da:

- Uspostave procedure za prijavljivanje u slučaju izgubljene ili ukradene opreme.
- Konfigurišu uređaje da se automatski zaključavaju nakon određenog vremena.

IoT uređaji (Internet stvari)

Obezbijedite IoT uređaje

Sve veća važnost tehnologije u našim životima je omogućila „internet stvari“ ili IoT. To znači da je veliki spektar uređajam povezan na internet kroz IoT senzore koji im omogućavaju da prikupljaju i razmijenjuju podatke u realnom vremenu. Zbog toga što prikuplja podatke od fizičkih i virtuelnih sistema, IoT predstavlja ogromnu „površinu za napad“ za kiber napadače, ako nije adekvatno obezbjeđeno.

Obezbjeđivanje IoT mreže znači obezbjeđivanje uređaja pre nego što se priključe na mrežu. Kako bi to uradili:

- Promijenite fabričke lozinke
- Koristite snažne lozinke
- Ažurirajte softver na uređajima (uvijek provjerite dostupne verzije za ažuriranje na veb sajtovima proizvođača pre nego što ih instalirate na uređaje)
- Šifrirajte i provjerite autentičnost uređaja
- Promijenite fabričke postavke za privatnost
- Promijenite fabričke postavke
- Osigurajte bezbjednost vaše mreže i WI-FI
- Kreirajte posebnu mrežu za goste

Fizička bezbjednost

Pobrinite se o fizičkoj bezbjednosti uređaja, osobito mobilnih uređaja

Fizička bezbjednost je isto toliko važna kao i kiber bezbjednost. Ako lopov ukrade laptop ili mobilni uređaj, najdirektnija šteta je gubitak samog uređaja, ali ako je lopov u stanju da pristupi informacijama na uređaju, sve te informacije mogu biti pod rizikom. Isto tako postoji i potencijal da se može pristupiti dodatnim informacijama koristeći podatke koji se nalaze na ovim uređajima, uključujući i osijetljive informacije o poslovnim korisničkim nalozima ili korisničkim nalozima klijenata – kao što su lozinke ili informacije o kreditnim karticama – kojima ne bi trebala pristupati neovlašćena lica.[5]

Kako bi zaštitili sebe i druge u vašoj organizaciji:

- Obezbijedite vaš uređaj lozinkom i uključite dvofaktorsku autentifikaciju (2FA)
- Uvijek čuvajte vrijedne stvari na sebi i nikada ne ostavljajte uređaje bez prismotre, osobito kada putujete

Pristup na daljinu

Ako vaša organizacija koristi pristup na daljinu, isti treba biti bezbjedan, šifriran i sakriven. To zahtijeva:

- Provjeru da li je cjeo softver za pristup na daljinu zakrpljen i ažuriran.
- Ograničavanje pristupa na daljinu od sumnjivih geografskih lokacija ili IP adresa.
- Ograničavanje pristupa na daljinu zaposlenima samo na sisteme i kompjutere koji su im potrebni da rade svoj posao.
- Zahtijevanje snažnih lozinki za dobijanje pristupa na daljinu.
- Uključivanje višefaktorske autentifikacije, ukoliko je moguće.
- Provjeru da li je praćenje i upozoravanje uključeno kako bi ste dobili upozorenje o sumnjivom napadu ili sumnjivoj aktivnosti.

5 https://www.cisa.gov/uscert/ncas/tips/ST04-017

Primjenite dobre prakse

Lozinke

Svaka organizacija treba imati politiku o lozinkama kako bi bila sigurna da se koriste složene i posebne lozinke i da se one redovno mijenjaju. Lozinke su prva linija odbrane protiv neovlašćenog pristupa.

Politika o lozinkama je neophodna kako bi se izbjegle najčešće slabe tačke, kao što su:

- Navika korisnika da čuvaju lozinke u beleškama, tekstualnim datotekama ili drugim nezaštićenim dokumentima kojima kiber kriminalci mogu lako da pristupe.
- Tendencija korisnika da čuvaju lozinke u pretraživačima, što predstavlja još jednu metu za kiber kriminalce.
- Lozinke koje uključuju lične informacije koje je lako naći na internetu.
- Korišćenje samo jedne lozinke za veći broj korisničkih naloga.
- Razmjena lozinki sa kolegama ili putem i-mejla, instant poruka ili drugih platformi (ovo je posebno velika slaba tačka ako se lozinke ne mijenjaju redovno).

Najlakši način da promijenite ili ublažite ponašanje korisnika u vezi lozinki je **korišćenje programa za upravljanje lozinkama**. To omogućava kreiranje složenih lozinki za različite korisničke naloge, koje se sve šifriraju i čuvaju, tako da korisnik treba da upamti samo jednu lozinku kako bi pristupio sefu koji sadrži njihove lozinke. Program za upravljanje lozinkama pomaže korisnicima da generišu lozinke i daje prikaz koliko je snažna lozinka, može da obavijesti korisnike o bezbjednosnim upadima vezanim za njihov i-mejl i mnogo više.

Ako vaša organizacija ne koristi program za upravljanje lozinkama, ovo su neki **saveti za kreiranje politike o lozinkama**:

- **Duže lozinke su bolje** jer je potrebno više vremena za njihovo hakiranje. Prema tome, lozinke trebaju imati najmanje 12 karaktera.
- **Složenost je od ključne važnosti**! Lozinke trebaju sadržati simbole, kombinaciju velikih i malih slova i brojeve. A onda ih treba i promešati.
- **Koristite besmislice** i izbjegavajte predvidljivost. U idealnom slučaju, lozinke ne trebaju sadržati riječi koje se mogu naći u rječniku (bilo kojeg jezika).
- **Lozinke trebaju biti unikatne**. Pravilo u svakoj organizaciji treba biti: jedan korisnički nalog, jedna lozinka.

Isto tako je važno **promijeniti fabričke lozinke** pre nego što date uređaj zaposlenima, kako bi izbegli rizik od mogućnosti izlaganja hakerima ili neki drugi veliki upad.

Višefaktorska autentifikacija

Koristite višefaktorsku autentifikaciju kad god je to moguće

Postoje tri načina na koji kompjuter, ili bilo koji sistem, može da identifikuje korisnika. Može da postavi pitanje o tome što korisnik zna, je ili ima. To su **tri faktora autentifikacije**. Zlatni standard za provjeru identiteta je višefaktorska autentifikacija koja koristi najmanje dva od ovih faktora.

Ideja je da dve različite lozinke nisu mnogo bolje od jedne, ali da dva faktora jesu. To je razlog zašto povlačenje novca iz bankomata zahtijeva dvofaktorsku autentifikaciju: nešto što osoba ima (karticu za bankomat) i nešto što osoba zna (svoj PIN).

Lozinke same po sebi se više ne smatraju bezbjedne, jer su hakeri razvili bezbrojne metode tokom godina za krađu potrebnih akreditiva za neovlašteni pristup privatnim korisničkim nalozima. Tužna istina je da skoro 90% tih incidenata su mogli biti blokirani korišćenjem višefaktorske autentifikacije.

Gdje god je to moguće, organizacije trebaju uvesti dvofaktorsku autentifikaciju za korisnike (2FA), kako bi:

- obezbijedili korisnike od krađe identiteta zbog krađe lozinke.

- zaštitili organizaciju od slabih lozinki zaposlenih.
- umanjili upotrebu nekontrolisanih uređaja, osobito sa povećanom stopom rada od kuće zbog COVID pandemije.
- povećali djelotvornost drugih bezbjednosnih mjera.
- pomogli organizaciji da ispuni zakonske uslove.

Korisnički nalozi (računi)

Koristite ograničene korisničke naloge za redovne i svakodnevne svrhe

Korisničkim nalozima se mora pažljivo rukovati, jer zloupotreba korisničkih naloga može dovesti do gubitka informacija, reputacije organizacije i novca.

Postoje dve vrste korisničkih naloga: Standardni korisnik i Administrator.

Karakteristike standardnog korisničkog naloga su da je on:
- prikladniji za svakodnevne zadatke (korišćenje aplikacija, pretraživanje interneta);
- konfigurisan da zaštiti vaš sistem od očiglednih napada; i
- ne dozvoljava korisnicima da urade promjene koje utiču na sve osobe koje koriste kompjuter.

Korisnički nalozi Standardnih korisnika imaju manju fleksibilnost od korisničkih naloga Administratora. Međutim, sa druge strane, malware instaliran u okviru Standardnog korisničkog naloga može da učini malu štetu sistemskim datotekama. To je zbog toga što napadači koji dobiju pristup Standardnom korisničkog nalogu mogu samo da pristupe datotekama tog korisnika. U tom smislu, restrikcije Standardnog korisničkog naloga idu u prilog organizaciji ako neprijatelj ili zlonamjerni program dobiju pristup.[6]

Pristup zaposlenih

Pristup zaposlenih treba biti ograničen tako da nijedan zaposleni nema pristup svim sistemima

Preporučuje se da se nijednom zaposlenom ne dozvoli pristup svim sistemima sa podacima. Zaposleni trebaju dobiti pristup samo određenim sistemima koji sadrže podatke koji su im potrebni da rade svoj posao.

Ne dozvoljavajte zaposlenima da instaliraju softver bez dozvole

Zaposleni nikada ne bi trebali biti u mogućnosti da instaliraju softver bez dozvole.

Logiranje (evidentiranje)

Sprovođenje logiranja

Iz bezbjednosne perspektive, log (evidencija) funkcioniše kao crvena zastavica kada se nešto loše dogodi. Redovito pregledanje logova može pomoći u otkrivanju zlonamjernih napada na vaš sistem.

Log kome je lako pristupiti i koji uključuje kritične informacije može da spasi informacije ili kompjuterski sistem. Logiranje pomaže sa:
- Otkrivanjem grešaka u programu
- Praćenjem grešaka
- Otklanjanje problema sa performansima
- Računovodstvom
- Revizijom
- Bezbjednošću

Logovi datoteke se isto tako mogu koristiti sa ciljem održavanja usaglašenosti sa zakonima. Mnoge organizacije moraju biti u skladu sa različitim propisima koji zahtijevaju reviziju aktivnosti, uključujući i davanje korisničkih naloga ili pristup finansijskim sistemima.

6 Why You Shouldn't Use an Admin Account as Your Main Account - Make Tech Easier

Najveći problem povezan za logiranje je nedostatak monitoringa. Važno je razumijeti šta treba evidentirati, na osnovu najboljih praksi, i razgledati logove na dnevnoj osnovi tražeći greške, anomalije ili sumnjive aktivnosti. Ipak, pretjerano logiranje nije od pomoći, jer stvara dosta „buke“ i zahtijeva veći kapacitet za čuvanje podataka. Prema tome, neke aktivnosti možda imaju veći prioritet za logiranje od drugih.

Svijest o kiber bezbjednosti

Uobičajene kiber prijetnje

Kiber napad je zlonamjerni i namjerni pokušaj od strane osobe ili organizacije za probijanje informatičkog sistema druge osobe ili organizacije. Uobičajeno, napadač želi da dobije određenu korist od narušavanja mreže mete. Organizacije su suočene sa ogromnim brojem kiber napada, a napadači koriste različite strategije kako bi pokušali ili izvršili napade.

Napadi društvenog inženjeringa

Napadi sa društvenim inženjeringom dovode u zabludu ili manipuliraju mete kako bi dobili informacije ili pristup njihovim kompjuterima. Ove vrste napada se pouzdaju u ljudsku interakciju i uobičajeno uključuju manipulaciju korisnika kako bi prekršili bezbjednosne procedure i najbolje prakse i dobili neovlašćeni pristup sistemima ili dali osijetljive informacije.

U napadima sa društvenim inženjeringom, kiber kriminalci kriju svoje prave identitete i motive, predstavljajući se kao osobe od povjerenja. Napad se potom vrši prijevarom korisnika da kliknu zlonamjerne linkove ili dobijanjem fizičkog pristupa kompjuteru.

Phishing (pecanje)

Većina kiber napada počinje sa phishing i-mejlom. Phishing (pecanje) je vrsta društvenog inženjeringa u kome kiber kriminalce prevare žrtve da im daju osijetljive informacije ili instaliraju malware.

I pored toga što se tehničke mjere bezbjednosti nastavljaju poboljšavati, phishing ostaje jedan od najjeftinijih i najlakših načina da kiber kriminalci dobiju pristup osijetljivim i ličnim informacijama. Korisnici samo trebaju da kliknu link i njihova bezbjednost može biti ugrožena do te mjere da mogu postati žrtve krađe identiteta. Korisnici isto tako mogu da kompromitiraju svoje lične informacije, akreditive za najavu (korisnička imena i lozinke) i finansijske informacije (brojeve kreditnih kartica), ako kliknu na link.

Često napadači ovo postižu kroz zlonamjerne i-mejlove koji deluju kao da su od povjerljivih izvora, ali ponekad koriste i druge metode.

Kako funkcioniše phishing?

Većina phishing kampanja uključuje jedan od dva osnovna metoda:

1. **Maliciozni(Zlonamjerni) prilozi (attachments)** u i-mejlovima, koji uobičajeno imaju alarmantne naslove kao „FAKTURA“. Kada budu otvoreni, ovi prilozi instaliraju malware na mašini korisnika.
2. **Linkovi do malicioznih veb sajtova** koji su često klonovi legitimnih sajtova. Prelazak na sajt može dovesti do preuzimanja malicioznog softvera ili strana za najavu na sajtu može da sadrži skripte koje kradu akreditive.[7]

7 What is phishing? Everything you need to know | IT Governance UK

Vrste phishing napada

Spear Phishing (ciljano pecanje)

Spear phishing je zlonamjerni napad sa lažnim i-mejlom koji cilja na određenu organizaciju ili osobu, pokušavajući da dobije neovlašćeni pristup osijetljivim informacijama. Malo je vjerovatno da će spear phishing pokušaji biti izvršeni od slučajnih napadača, već od kiber kriminalaca koji žele da postignu finansijsku dobit ili prikupe druge vredne informacije.[8]

U spear phishing napadu, i-mejl se šalje od pouzdanog izvora, ali vodi do lažnog veb sajta koji je miniran malicioznim softverom. Ovi i-mejlovi najčešće koriste kreativne metode da privuku pažnju korisnika.

Spear phishing je daleko efektivniji od drugih phishing napada, jer zahtijeva od kiber kriminalaca da provedu vrijeme i resurse na istraživanju pre napada, jer će biti utoliko uspešniji ako nauče o njihovoj meti pre početka napada.

Whale Phishing/Whaling (kitolov)

Whale phishing (lov na kitove) je sličan sa spear phishing (ciljano pecanje), sa nekoliko važnih razlika. Dok je spear phishing uobičajeno usmjeren protiv članova određene grupe, whale phishing je usredsređen na konkretnu osobu – uobičajeno „najveću ribu“ u ciljanoj organizaciji ili pojedinca sa značajnim bogatstvom ili moći.

Vishing

Vishing ili „glasovni phishing“ uključuje manipulaciju ljudi preko telefona. Napadači zavedu metu da otkrije osijetljive informacije u pokušaju da iskoriste te podatke za svoju ličnu korist, uobičajeno finansijsku.

Smishing

Termin smishing se odnosi na SMS phishing i uključuje tekstualnu poruku umjesto i-mejla. Mete uobičajeno dobiju tekstualnu poruku koja sadrži obmanu i koja ih prinuđuje da daju lične ili finansijske informacije kiber kriminalcu koji se pretvara da je organ vlasti, banka ili druga legitimna kompanija.

Smishing napadači često traže lične ili bankovne podatke, kao što su akreditivi korisničkih naloga, brojeve kreditnih kartica i brojeve za identifikaciju. Potom, oni koriste te informacije kako bi sprovodili različite vrste napada, uključujući finansijske prevare, prevare sa poklonima i prevare sa podrškom za klijente.

Kako spriječiti phishing napade

U elektronskoj pošti: naučite da pažljivo gledate i-mejlove, osobito ako sadrže priloge(attachments) ili veb linkove

Obučite zaposlene kako da prepoznaju phishing pokušaje i da prijave sumnjive incidente. Evo nekoliko tipičnih znakova da i-mejl može biti zlonamjeran:

- **Loš pravopis i gramatika**. Profesionalne kompanije ili organizacije uobičajeno imaju lektorsko osoblje kako bi njihovi klijenti dobili visokokvalitetne i profesionalne i-mejl sadržine. Ako je i-mejl poruka puna grešaka, mnogo je veća vjerovatnoća da se radi o prevari.
- **Sumnjivi linkovi.** Korisnici nikada ne trebaju kliknuti linkove u i-mejl poruci za koje sumnjaju da su zlonamjerni. Jedan način za testiranje legitimnosti linka je da odmorite miša na link – bez klikanja – kako bi utvrdili da li adresa odgovara informacijama u poruci.
- **Sumnjivi prilozi**. Ako korisnik dobije i-mejl sa prilogom, ili od osobe koju ne poznaje ili od osobe od koje ne očekuje da će im poslati prilog, on mora da razmisli da li se radi o phishing pokušaju. Preporučuje se da se prilozi nikada ne otvaraju dok se ne potvrdi njihova autentičnost. Zbog toga što postoje više načina da napadači prevare primače da povjeruju da je dodata datoteka legitimna, važno je da korisnici znaju:
    * Ikonici povezanoj sa prilogom se ne može vjerovati bez druge potvrde.
    * Trebaju paziti na kombinovane ekstenzije datoteka kao što su „pdf.exe“, „rar.exe“, ili „txt.hta“.
    * Ako ste u nedoumici, najbolje je stupiti u kontakt sa osobom koja je navodno poslala dotičnu

8 Types of Cyber Threat in 2019 | IT Governance USA

i-mejl poruku i pitati ih da potvrde da su i-mejl i prilog legitimni.

- **Prisilne poruke**. Ovi i-mejlovi imaju za cilj da izazovu osjećaj panike ili pritiska i da dovedu do brzog i nepromišljenog odgovora primača. Na primer, one mogu uključivati izjave kao „Morate odgovoriti do kraja dana!“, ili mogu indicirati da će primač biti suočen sa potencijalnim finansijskim penalima ako ne odgovori.
- **Spoofing (maskiranje)**. Spoofing i-mejlovi koriste **sumnjive linkove** koji deluju kao da se povezuju sa legitimnim veb sajtovima ili kompanijama i mogu da pokazuju pop-up prozore koji deluju legitimno, ali koji vode korisnike na lažne sajtove za prevaru. Jedan spoofing oblik koristi **izmijenjene veb adrese** koje u velikoj mjeri liče na imena veb sajtova dobro poznatih kompanija, kao „www.micorsoft.com“ ili „www.mircosoft.com“.
- **Nepodudarnosti**. Primači trebaju sumnjati ako tekst određenog linka i URL ne odgovaraju ili nema podudarnosti između imena pošiljaoca, potpisa i URL.[9]

Javni WI-FI: Pazite kada koristite javne WI-FI mreže

Opkruženi smo javnim WI-FI mrežama u hotelima, trgovačkim centrima, kafićima, aerodromima itd. Mnogi od nas imaju lošu naviku da se povezuju na ove mreže bez ikakvog razmišljanja o bezbjednosti. Međutim, one predstavljaju prave bezbjednosne rizike i trebaju se pažljivo koristiti.

Najveći bezbjednosni problem sa javnim WI-FI mrežama je što korisnici ne znaju ko operira mrežom ili ko je još drugi prikačen na mrežu.

Prema tome, organizacije trebaju da:

- **Obuče zaposlene o rizicima korišćenja javnih WI-FI mreža**.
- **Zabrane zaposlenima da pristupaju osijetljivim podacima kad koriste javne WI-FI mreže**.
- **Daju upute zaposlenima da se povezuju samo na pouzdane mreže**.
- **Zabrane zaposlenima da se konektiraju na sajtove zaštićene lozinkama koristeći javne WI-FI mreže**.

Trebaju se razgledati druge opcije, umjesto korišćenja javnih WI-FI mreža. Na primjer, telefon može da posluži kao mobilni hotspot, omogućavajući vlasniku uređaja da kontroliše mrežu i ko je koristi. Ako se mora koristiti javna WI-FI mreža, može se upotrebiti VPN kako bi šifrirao sve podatke koji se šalju preko WI-FI mreže, čime se sakrivaju ovi podaci od svih koji „slušaju“ na istoj mreži.

Kompromitovanje poslovnog i-mejla (Business Email Compromise)

Kompromitovanje poslovnog i-mejla (BEC) je vrsta prevare koja cilja na kompanije koje koriste elektronske transfere i imaju dobavljače u inostranstvu. Korporativno ili javno dostupne i-mejl adrese izvršnih osoba ili zaposlenih na visokim pozicijama koji rade sa finansijama ili su uključeni u elektronska plaćanja se ili lažiraju ili kompromituju programima za snimanje otkucaja na tastaturi (key logger) ili phishing napadima kako bi se izvršili lažni transferi. To može da dovede do gubitka stotine hiljada dolara.[10]

Preuzimanje podataka u „prolazu“ (Drive-By Downloads)

U napadima sa preuzimanjem podataka u „prolazu“ preuzimaju se zlonamjerne skripte na kompjutere ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim kiber napadima. To može da se dogodi na svakom uređaju na bilo kojem operativnom sistemu i uobičajeno se događa kada korisnik pređe na i pretražuje kompromitovani veb sajt.

Napadi Čovek-u-sredini (Man in the Middle (MITM))

MITM napad se događa kada se kiber kriminalac tajno ubaci između dva uređaja, ili između uređaja i nebezbjedne WI-FI mreže, kako bi presretao komunikacije koje potom on može da čita i/ili mijenja. U takvom slučaju, korisnik može da nenamjerno pošalje kiber kriminalcu akreditive ili druge informacije.

9 Protecting against coronavirus themed phishing attacks (microsoft.com)

10 https://www.trendmicro.com/vinfo/hk/security/definition/business-email-compromise-(bec)

USB Drop napadi

U USB drop napadu, USB uređaj koji sadrži zlonamjerni kod se uključuje na kompjuter.

Uobičajeno, kiber prijetnja predstavljana ovim napadom je infekcija zlonamjernim softverom ili virusom. Infekcije preko USB diska mogu biti i namjerne i nenamjerne, ovisno o dotičnom malicioznom softveru.

Bilo bi pametno da organizacije prekinu vjerovati zastareloj USB tehnologiji i počnu koristiti moć bezbjednih digitalnih mreža koristeći cloud spremanje podataka.

Malware (zlonamjerni/maliciozni softver)

Malware je opšti termin koji se koristi za definisanje svake datoteke ili programa koji ima za cilj da ošteti ili naruši rad kompjutera. On uključuje:

- **Botnet softver** koji je osmišljen da inficira veliki broj uređaja koji su povezani na internet. Neki botnet (mreže botova) su sačinjene od velikog broja uređaja, od kojih svaki koristi relativno malu procesorsku snagu. Time se otežava otkrivanje ove vrste zlonamjernog softvera, čak i kada je botnet u funkciji.
- **Ransomware napadi (napadi sa softverom za otkupninu)**, koji šifriraju informacije korisnika i zahtijevaju plaćanje za ključ za dešifriranje, kako bi se povratile informacije. Međutim, plaćanje otkupnine ne garantuje uvek da će šifrirani podaci biti vraćeni.
- **Spyware (špijunski softver)** se koristi za nezakonito praćenje aktivnosti korisnika na kompjuteru i prikupljanje ličnih podataka.
- **Trojanski virusi** koji deluju kao legitiman softver, ali izvode zlonamjerne aktivnosti kada budu izvršeni.
- **Virusi i crvi**, koji su zlonamjerni kod instaliran bez znanja korisnika. Virusi se mogu množiti i širiti na druge kompjutere time što se pripijaju na druge kompjuterske datoteke. Crvi se isto tako množe sami, ali ne moraju da se prikače na drugi program kako bi to uradili.[11]

DoS/DDoS napadi

Distribuirani napad za onemogućivanje usluge (DDoS) je kiber napad u kome napadač preplavi server internet saobraćajem kako bi sprečio korisnike da pristupe povezanim internet uslugama i sajtovima.

DDoS napad je potkategorija generalnijeg napada za onemogućivanje usluge (Denial-of-Service (DoS)). U DoS napadu, napadač koristi jednu internet konekciju kako bi zasuo metu sa lažnim zahtijevima ili kako bi pokušao da iskoristi slabu tačku u kiber bezbjednosti. Prema tome, DDoS je većih razmjera i koristi na hiljade (čak i milione) povezanih uređaja kako bi ispunio svoj cilj. Sami broj uključenih uređaja čini borbu protiv DDoS mnogo težom.[12]

Postoje tri opšte vrste DDoS napada:

- **Volumetrijski napad**: u ovom klasičnom DDoS napadu, koriste se metodi za generisanje masovnog obima saobraćaja kako bi se u potpunosti zasitio mrežni protok veb sajta, čime se koči saobraćaj i postaje nemoguće da legitimni saobraćaj pristupi na ili iz ciljanog sajta.
- **Napadi na protokole**: ovi napadi su osmišljeni da pojedu kapacitet obrade mrežnih infrastrukturnih resursa kao što su serveri, firewall i servisi za dodelu mrežnog opterećenja ciljajući na Sloj 3 i Sloj 4 protokolarne komunikacije sa zahtijevima za maliciozne konekcije.
- **Napadi na aplikacije**: između sofisticiranijih DDoS napada, ovi napadi koriste slabe tačke u sloju aplikacija – Sloj 7 – otvaranjem konekcija i iniciranjem procesa i zahtijeva za transakcije koji troše ograničene resurse kao što je disk prostor ili dostupna memorija.[13]

11 Types of Cyber Threat in 2019 | IT Governance USA
12 https://www.fortinet.com/resources/cyberglossary/ddos-attack
13 https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

Redovne obuke

Sa ciljem **podizanje svijesti o kiber prijetnjama i informatičkoj bezbjednosti**, jedan od najvažnijih elemenata kiber higijene koji se može sprovesti u bilo kojoj organizaciji je obuka o bezbjednosnoj svijesti, kako bi naučili zaposlene kako da izbegnu, identifikuju i prijave potencijalne prijetnje.

Uključivanje osoblja u robusni kurs za obuku o bezbjednosti je jedna od proaktivnih mjera koje organizacije mogu da preduzmu kao zaštitu od kiber napada. Ako se ne uzme u obzir ovaj ljudski elemenat, vrata vaše organizacije će biti široko otvorena kiber prijetnjama.

Obuka o podizanju svijesti o bezbjednosti povećava znanje korisnika o potencijalnim prijetnjama, čime se:

- smanjuju rizici;
- spriječava vrijeme neaktivnosti;
- poboljšava samopouzdanost zaposlenih; i
- podstiče povjerenja klijenata.

Prema tome, obuke o podizanju svijesti o bezbjednosti su od vitalnog značaja u efektivnoj kiber bezbjednosti i kiber higijeni. Isto tako, tokom vremena, godišnje obuke za podizanje svijesti mogu da promjene kulturu kiber bezbjednosti u vašoj organizaciji. U najmanjoj ruci, ove obuke trebaju da uključuju informacije o:

- Osijetljivim informacijama: šta su i kako rukovati s njima
- Kako prepoznati phishing i-mejlove
- Kako adekvatno koristiti službene uređaje
- Kako prjaviti incidente
- Šta činiti u hitnom slučaju koji utiče na kompjuterske i informatičke sisteme
- Kako rukovati sa informacijama koje sadrže lične identifikatore (PII)
- Osnovnoj kiber higijeni: šta je i kako je primjeniti

Napredne obuke se trebaju fokusirati na sadržaj, materijale za podršku, phishing testiranje, metriku, izvještavanje i ankete.

Uspješni programi za podizanje svijesti o bezbjednosti:

- Obrazuju i podržavaju zaposlene, a da ih pri tom ne obeshrabre ili osramote.
- Se ne fokusiraju samo na phishing kampanje (cilj je da zaposleni nauče da prepoznaju i prijave prijetnje u realnom vremenu, koje imaju brojne pojavne oblike koji se stalno mijenjaju).
- Izbjegavaju ponavljanje istog sadržaja i žele da obogate zaposlene sa novim informacijama na svakoj obuci.
- Uključuju materijale koji idu van profesionalnog svijeta do privatnih života zaposlenih, jer to vrši personalizaciju sadržaja i zaposleni su voljniji da slušaju.

Preporučuje se da ishodi obuke – pozitivni ili negativni – ostani interni i da se ne dijele sa činiocima.

Sažetak

Skoro svi kiber napadi iskorištavaju uslove koji spadaju pod krovom loše kiber higijene. To uključuje zakrpe softvera koje nedostaju, loše konfiguracije i nisku svijest korisnika. Prema tome, nedostatak konzistentne kiber higijene je jedna od najopasnijih prijetnji koja se može javiti unutar organizacije. Kako bi podstaknuli dobru kiber higijenu u vašoj celoj organizaciji:

- Obezbijedite dovoljno obuke za vaše zaposlene da identifikuju i prijave sumnjive kiber aktivnosti.
- Osigurajte se da se svi serveri, radni kompjuteri, pametni telefoni i drugi uređaji koji koriste zaposleni dobijaju često bezbjednosno ažuriraju.
- Implementirajte strogu politiku za upravljanje pristupom sistemu koja zahtijeva višefaktorsku autentifikaciju gdje god je moguće i stroge standarde za lozinke.
- Uložite u sisteme i rješenja koja omogućavaju jasnu vidljivost i granularnu kontrolu pristupa cjeloj mrežnoj infrastrukturi organizacije.

Iako može izgledati da je složenost/komplesnost neprijatelj kiber kriminalaca, ona je u stvari neprijatelj

vaše vlastite kiber bezbjednosti. U složenom i dinamičnom kiber svijetu, vaša najbolja odbrana je da se vratite na osnove.

Kako bi poboljšali i proširili razmjer kiber higijene, nije dovoljno da organizacija samo ponudi primjere zaposlenima i govori o važnosti kiber bezbjednosti u organizaciji. U svakoj organizaciji, kiber higijena mora biti konkretno definisana, a potom i podržana metrikom i obrazovanjem.

Okvir bezbjednosti je odlična početna tačka, ali on mora biti:

- Prave veličine za potrebe vaše organizacije
- Usaglašen sa vašim jedinstvenim zakonskim uslovima
- Pridružen obukom koja je dostupna i koja vaša organizacija može priuštiti
- Održiv/ponovljiv sa resursima vaše organizacije
- Podržavati vaše poslovne i operativne ciljeve

Zaključak

Na kraju, loše kiber navike – ili niska kiber higijena – su razlog najuspešnijih kiber napada. Zbog toga je toliko važno da organizacija razvije kulturu dobre kiber higijene. Međutim, mjere preporučene u ovom Priručniku, iako uglavnom predstavljene iz perspektive organizacijske bezbjednosti, su primjenjive i na organizacije i na pojedince. Prema tome, organizacije trebaju potencirati zaposlenima da razmisle o primjeni navika kiber higijene i kod kuće. Ipak, dobre navike kiber higijene koje se koriste kod kuće će se vjerovatno i više koristiti na poslu. Isto tako, svi smo mi bezbjedniji u kiber svijetu u kome se kultura kiber higijene odnosi i na lični i na profesionalni prostor.

Reference

ENISA: Review of Cyber Hygiene practices https://www.enisa.europa.eu/publications/cyber-hygiene

Centre for Cyber Security Belgium: Cyber security guide for SME https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf

ANSSI: Guideline for a healthy information system https://www.ssi.gouv.fr/uploads/2013/01/guideline-for-a-healthy-information-system-in-42-measures_v2.pdf

CPME-ANSSI: Guide Des Bonnes Pratiques De L'informatique https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

NIST: Small business information security: the fundamentals https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

CISA: Cyber Essentials Starter Kit https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

CMU SEI: Cyber Hygiene: 11 Essential Practices https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/

Canadian Centre for Cyber Security: Cyber Hygiene https://cyber.gc.ca/en/guidance/cyber-hygiene

Kaspersky: Good cyber hygiene habits to help you stay safe online https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

ANSSI: 40 Essential measures for a healthy network https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf

US House of Representatives: Promoting Good Cyber Hygiene Act of 2017 https://www.congress.gov/115/bills/hr3010/BILLS-115hr3010ih.pdf

NCSC NL: Cyber Hygiene in the Netherlands https://english.ncsc.nl/research/research-results/cyber-hygiene-in-the-netherlands

NIST NCCoE: Critical Cybersecurity Hygiene: Patching the Enterprise https://www.nccoe.nist.gov/projects/critical-cybersecurity-hygiene-patching-enterprise

CISA: Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services

CYBER4Dev: Cyber Security Hygiene/Awareness https://cyber4dev.eu/cyber-security-hygiene-awareness/

eGA: What is Cyber Hygiene? https://ega.ee/blog_post/podcast-what-is-cyber-hygiene/

Aneks: Kontrolna lista dobrih praksi

ANALIZIRAJTE SISTEM I UTVRDITE PROCEDURE I POLITIKE		
Kategorija	**Dobre prakse**	**Relevantni činioci**
Popis hardvera i softvera	- Održavajte popis hardvera i softvera - Standardizirajte vaš popis hardvera i softvera	Javne institucije i MSP
Popis osijetljivih ili kritičnih informacija	- Održavajte popis osijetljivih ili kritičnih informacija - Razumite vaše okruženje podataka i identifikujte važne podatke u vašoj sredini - Kreirajte politiku za klasifikaciju podataka - Šifrirajte podatke, osobito podatke koji su klasifikovani kao „ograničeni“ - Uvedite sistem za spriječavanje gubitka podataka	Javne institucije i MSP
Analiza rizika	- Identifikujte rizike • ljudski rizik (prijevara, krađa, ljudska greška) • prirodni rizik (poplave, požari, zemljotresi, itd.) • tehnički rizici (defekt softvera, hardvera, nedostatak znanja) - Izbijegavajte rizik – ako nije neposredna briga po vaše poslovanje - Smanjite rizik – uvođenjem novih bezbjednosnih rješenja - Prihvatite rizik – kada je mala vjerovatnoća da će se rizik dogoditi ili je iznad tekućih kapaciteta - Prenesite rizik – osiguranjem	Javne institucije i MSP
Procedure za bekap (rezervne kopije)	- Uspostavite proceduru za redovni bekap - Budite realni u pripremi politike za bekap i pripremite napisani bekap plan koji propisuje: • Šta se stavlja na bekap? • Gdje se nalazi bekap? • Koliko često se radi bekap? • Ko je zadužen da vrši bekap? - Uvijek dajte najviši prioritet ključnim podacima - Uvijek testirajte bekap - Koristite pravilo 3-2-1 - Koristite skladištenje podataka na daljinu /cloud - Često i redovno ažurirajte bekap	Javne institucije i MSP
Reakcija na incidente	- Pripremite plan za reakciju na incidente ili PRI - Kada se dogodi incident kritično je da se prati PRI	Javne institucije
Kontinuitet poslovanja i oporavak od katastrofe	- Pripremite plan za kontinuitet poslovanja i oporavak od katastrofe	Javne institucije

ZAŠTITITE VAŠ INFORMATIČKI SISTEM		
Operativni sistem i softver aplikacija	- Zakrpite i ažurirajte vaš operativni sistem i softver aplikacija, zbog: • Bezbjednosti • Novih mogućnosti • Popravki - Uključite automatsko ažuriranje za sisteme i aplikacije	Javne institucije i MSP
Bezbjedne konfiguracije	- Koristite bezbjedne konfiguracije za sve uređaje i softver - Dokumentirajte sva ažuriranja i promjene • Evidentirajte promjene • Utvrdite bezbjednosnu osnovu • Sprovedite proces provjere i odobrenja • Evidentirajte promjene konfiguracija	Javne institucije i MSP
Osijetljivi podaci	- Šifrirajte sve osijetljive podatke - Šifriranje pomaže u zaštiti osijetljivih i privatnih informacija čineći ih nečitljivim za kiber kriminalce, jer se njima samo može pristupiti ključem	Javne institucije i MSP
Anti-malware softver	- Koristite anti-malware softver - Anti-malware rješenja će blokirati najveći deo malicioznih/ zlonamjernih i potencijalno neželjenih programa	Javne institucije i MSP
Firewall (vatrozid)	- Koristite firewall, kako bi: • blokirali najveći deo malicioznih i potencijalno neželjenih programa • spriječili izvršavanje malicioznog softvera na uređaju • spriječili maliciozni softver da promjeni postavke • spriječili maliciozni softver da izvrši dodatni kompromitovani softver	Javne institucije i MSP
WI-FI mreže	- Zaštitite WI-FI mreže - Koristite enkripciju bežičnih mreža - Ažurirajte softver sa novim bezbjednosnim verzijama i zakrpama - Postavite WI-FI ruter što je moguće bliže sredini vaše organizacije - Uključite filtriranje MAC adresa - Isključite upravljanje sa daljine - Postavite posebnu WI-FI mrežu za goste	Javne institucije i MSP
Postavke internet pretraživača	- Uvijek konfigurišite bezbjednosne postavke internet pretraživača - Blokirajte pop-up obaviještenja, plugin softverske dodatke i phishing sajtove - Nemojte dozvoliti da se lozinke čuvaju u pretraživaču - Isključite kolačiće trećih strana - Deinstalirajte sve ekstenzije pretraživača koje ne koristite - Redovno ažurirajte sve ekstenzije koje koristite - Podstaknite korisnike da koriste https sajtove umjesto http sajtove	Javne institucije i MSP
Mobilni uređaji	- Tražite od korisnika da: • Zaštite uređaje lozinkama • Šifriraju podatke • Instaliraju bezbjednosne aplikacije koje spriječavaju kiber kriminalce da kradu informacije kada je telefon povezan na javne mreže • Konfigurišu uređaje da se automatski zaključavaju - Uspostave procedure za prijavljivanje izgubljene ili ukradene opreme	Javne institucije i MSP
IoT uređaji (internet stvari)	- Obezbijedite IoT uređaje: • promjenite fabričke lozinke • koristite snažne lozinke • redovno ažurirajte softver na uređajima • šifrirajte i proverite autentičnost uređaja • promjenite fabričke postavke za privatnost • promjenite fabričke postavke • osigurajte bezbjednost mreže organizacije i WI-FI mreže • kreirajte posebnu mrežu za goste • uvijek proverite dostupne verzije za ažuriranje na veb sajtovima proizvođača pre nego što ih instalirate na uređaje	Javne institucije i MSP
Fizička bezbjednost uređaja	- Pobrinite se o fizičkoj bezbjednosti uređaja, osobito mobilnih uređaja: • Zaštitom uređaja sa snažnim lozinkama • Čuvanja uređaja kod korisnika/vlasnika sve vrijeme	Javne institucije i MSP

Pristup na daljinu	- Proverite da li je sav softver za pristup na daljinu zakrpljen i ažuriran - Ograničite pristup na daljinu od sumnjivih geografskih lokacija ili IP adresa - Ograničite pristup na daljinu zaposlenima samo na sisteme i kompjutere koji su im potrebni da rade svoj posao - Zahtevajte snažne lozinke za pristupa na daljinu - Uključite višefaktorske autentifikacije, ako je moguće - Provjerite da li je praćenje i upozoravanje uključeno kako bi ste dobili upozorenje o sumnjivom napadu ili sumnjivoj aktivnosti	Javne institucije i MSP

PRIMJENITE DOBRE PRAKSE		
Lozinke	- Duže lozinke su bolje - Složenost/Kompleksnost je ključna! Tražite simbole, kombinaciju velikih i malih slova i brojeve - Koristite besmislice i izbijegavajte predvidljivost - Lozinke trebaju biti unikatne - Promjenite sve fabričke lozinke	Javne institucije i MSP
Višefaktorska autentifikacija	- Koristite višefaktorsku autentifikaciju kad god je to moguće - Koristite dva ili tri faktora za provjeru autentičnosti – nešto što korisnik *zna*, *je* ili *ima*	Javne institucije i MSP
Korisnički nalozi	- Koristite ograničene (Standardne korisničke) naloge za redovnu i svakodnevnu upotrebu - Uspostavite Standardne korisničke i Administratorske naloge za različite namene	Javne institucije i MSP
Pristup zaposlenih	- Ne omogućavajte pristup svim sistemima podataka nijednom zaposlenom - Zaposlenima dajte pristup samo onim sistemima koji su im potrebni za njihov posao - Ne dozvoljavajte zaposlenima da instaliraju softver bez dozvole	Javne institucije i MSP
Logiranje (evidentiranje)	- Održavajte konzistentno logiranje - Osigurajte se da ste razumjeli šta treba evidentirati, na osnovu najboljih praksi, i razgledati logove na dnevnoj osnovi tražeći greške, anomalije ili sumnjive aktivnosti	Javne institucije

<table>
<tr><th colspan="4">SVIJEST O KIBER BEZBJEDNOSTI</th></tr>
<tr><td>Uobičajene kiber prijetnje</td><td>VRSTA KIBER PRIJETNJE</td><td>PREPORUKA</td><td rowspan="2">Javne institucije i MSP</td></tr>
<tr><td></td><td>- Društveni inženjering
- Phishing napadi (pecanje)
• Spear Phishing (ciljano pecanje)
• Whale Phishing/Whaling (kitolov)
• Vishing (glasovni phishing)
• Smishing (SMS phishing)
- Kompromitovanje poslovnog i-mejla (BEC)
- Preuzimanje podataka u „prolazu“ (Drive-By Downloads)
- Napadi Čovek-u-sredini (MITM)
- USB Drop napad
- Malware (zlonamjerni softver)
• Botnet softver
• Ransomware napad
• Spyware
• Trojanski virus
• Virusi i crvi
- DoS/DDoS napadi (onemogućavanje usluge)
• Volumetrijski
• Napadi na protokol
• Napadi na aplikacije</td><td>- I-MEJLOVI: pažljivo gledajte i-mejlove, posebno ako sadrže priloge ili veb linkove. Tražite:
• Pravopis i lošu gramatiku
• Sumnjive linkove
• Sumnjive priloge
• Prijetnje u jeziku
• Maskiranje
• Promenjene veb adrese
• Nepodudarnosti
- JAVNE WI-FI MREŽE: budite uvijek oprezni kada se povezujete na javne WI-FI mreže:
• Ne pristupajte osijetljivim podacima
• Povežite se samo na pouzdane mreže
• Odaberite opcije da se ne povezujete automatski</td></tr>
<tr><td>Redovne obuke</td><td colspan="2">- Podignite svijest o kiber prijetnjama i informatičkoj bezbjednosti godišnjim ili češćim obukama
- Robusni kurs za obuku o dizanju svijesti o bezbjednosti treba da pokriva:
• Osijetljive informacije: šta su i kako rukovati s njima
• Kako prepoznati phishing i-mejl
• Kako adekvatno koristiti službene uređaje
• Kako prijaviti incidente
• Šta uraditi u hitnom slučaju koji utiče na kompjuterske i informatičke sisteme
• Kako rukovati sa informacijama koje sadrže lične identifikatore (PII)
• Osnovna kiber higijena: šta je i kako je primjeniti</td><td>Javne institucije i MSP</td></tr>
</table>

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva