



Priručnik o bezbednosti na internetu:

sajber higijena za javne institucije
i mala i srednja preduzeća

Vladan Babić i Aleksandar Bratić

Oktobar 2022

O DCAF-u

DCAF – Ženevski centar za upravljanje sektorom bezbednosti je posvećen poboljšanju bezbednosti država i njihovog stanovništva u okviru demokratskog upravljanja, 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 bezbednosti kroz inkluzivne i participativne reforme. On kreira inovativne proizvode znanja, promoviše dobre norme i prakse, daje pravne savete i savete o politikama i podržava građenje kapaciteta državnih i nedržavnih činioca u sektoru bezbednosti.

DCAF – Ženevski centar za upravljanje sektorom bezbednosti

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 bezbednošću na Zapadnom Balkanu“ koji sprovodi DCAF – Ženevski centar za upravljanje sektorom bezbednosti, uz podršku Ministarstva spoljnih poslova Velike Britanije (UK FCDO - United Kingdom's Foreign, Commonwealth and Development Office)

Sadržaj

Uvod	1
Definicije	1
Uobičajene mere	1
Analizirajte sisteme i uspostavite procedure i politike	2
Popis resursa	2
Popis informacija	2
Procena rizika	3
Procedura za bekap (pravljenje rezervnih kopija)	3
Plan za odgovor u slučaju incidenta	4
Kontinuitet i oporavak od katastrofe	5
Zaštitite vaš informacijski sistem	6
Zakrpe (patch) i ažuriranje (update)	6
Bezbedne konfiguracije	6
Osetljivi podaci	7
Suzbijanje malicioznog softvera (malware)	8
Firewall (vatrozid)	8
Wi-Fi mreže	9
Postavke internet pretraživača	9
Mobilni uređaji	9
IoT uređaji (Internet stvari)	10
Fizička bezbednost	10
Pristup na daljinu	10
Primenite dobre prakse	11
Lozinke	11
Višefaktorska autentifikacija	11
Korisnički nalozi (računi)	12
Pristup zaposlenih	12
Logovanje (evidentiranje)	12
Svest o sajber bezbednosti	13
Uobičajene sajber pretnje	13
Napadi sa društvenim inženjeringom	13
Phishing (pecanje)	13
Kompromitovanje poslovnog e-mejla (Business Email Compromise)	15
Preuzimanje podataka u „prolazu“ (Drive-By Downloads)	15
Napadi „Čovek-u-sredini“ (Man in the Middle (MITM))	15
USB Drop napadi	16
Malware (maliciozni softver)	16
DoS/DDoS napadi	16

Redovne obuke	17
Sažetak	17
Zaključak	18
Reference	19
Aneks: Spisak dobrih praksi	20

Uvod

Ovaj dokument je pregled minimalnih standarda za uspostavljanje sistema sajber higijene u javnim institucijama i malim i srednjim preduzećima (MSP). U njemu su predstavljene mere koje svaka organizacija treba da uvede kako bi obezbedila odgovarajući nivo informatičke bezbednosti za svoje informatičke sisteme.

Fokus ovde je na davanju uvoda u važnost sajber higijene i preporuka o jednostavnim koracima koji će poboljšati sajber bezbednost u vašoj organizaciji. Ukratko, higijena u bezbednosti je ista kao pranje ruku. Kada je mađarski doktor Ignaz Semmelweis rekao tri jednostavne reči „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.

Sajber higijena se slično tome odnosi na prakse koje imaju za cilj sprečavanje infekcije malicioznim softverom (malware), kao i sajber upade i gubljenje ili korumpiranje podataka i održavanje zdravog sajber okruženja. Time se osigurava zdravlje sistema i poboljšava sajber bezbednost na isti način na koji rutinsko pranje ruku pomaže u sprečavanju širenja bolesti.

Uzimajući u obzir da sve organizacije u današnjici koriste informatičke sisteme za poslovanje, sve su pod rizikom od izlaganja različitim sajber napadima koji mogu sprečiti funkcionisanje informacionih 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 sajber higijene.

Definicije

Postoje mnoge različite definicije sajber higijene i sve su tačne.

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

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

Uobičajene mere

Dobra sajber higijena zahteva sprovođenje određenih uobičajenih mera, od uspostavljanja standardizovanih procedura i politika, do redovitih obuka koje pomažu zaposlenima da razumeju sajber pretnje koje se stalno menjaju. Priroda i karakter nekih od ovih pretnji su objašnjeni u daljem tekstu (vidite Uobičajene sajber pretnje). Međutim, prvo su predstavljeni ključni elementi efektivnog programa za sajber 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, osobito ako se oprema i osoblje stalno kreću ili menjaju, ali je od ključnog značaja. 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 sajber higijene je **standardizacija popisa softvera i hardvera** putem:

1. Dokumentovanje osnovne bezbednosne pozicije organizacije
2. Standardizacija iste u celoj organizaciji na osnovi politika i procedura
3. Monitoring i reagovanje na odstupanja
4. Smanjenje svih slabosti uvedenih nepoznatim hardverom i softverom

Prednosti održavanja popisa hardvera i softvera su očigledne 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 prosečno vreme do ponovnog uspostavljanja usluga (MTTRS)

Popis informacija

Održavajte popis osetljivih ili kritičnih informacija

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

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

- *Ograničeno* – osetljivi podaci koji predstavljaju veliki rizik ako budu kompromitovani; njima pristupaju samo oni koji imaju potrebu za to.
- *Poverljivo* – umereno osetljivi podaci kojima se pristupa samo interno.
- *Javno* – podaci koji nisu osetljivi 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 sprečavanje gubitka podataka** za otkrivanje potencijalnih upada u podacima/transmisija za izvlačenje podataka i njihovo sprečavanje putem praćenja, otkrivanja i blokiranja osetljivih podataka tokom upotrebe, u kretanju i u mirovanju.

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

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

Procena rizika

Identifikacija rizika

Upravljanje rizikom zahteva razumevanje pretnji sa kojima je suočena vaša organizacija i korake koji se mogu preuzeti kako bi sprečili, smanjili ili spremili se za situaciju koja može, ali ne mora da se dogodi.

Postoje tri oblasti rizika po informacione sisteme:

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

Kao početna tačka, procena rizika uključuje dodeljivanje vrednosti kritičnim resursima, uključujući i finansijske i reputacijske. Ovo vam pomaže da počnete procenu kolika je težina svake posebne pretnje. Jedan efektivan način za ovo je da dodelite ocenu svakom scenariju – prvo, u pogledu verovatnoće da će nešto da se dogodi i drugo, o šteti koja bi nastala ako se to dogodi.

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

- **Izbegavanja**, kada rizici nisu neposredna briga po vaše poslovanje
- **Smanjenja**, kada rizici zahtevaju implementaciju novog bezbednosnog rešenja
- **Prihvatanja**, kada je mala verovatnoća 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 defekta, korumpiranja podataka ili ljudski izazvanih događaja kao što su maliciozni 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 usluga koje dajete? Važno je ne raditi bekap samo u ime bekapa, već da radite bekap kako bi mogli da povratite ključne podatke po potrebi i sa što je moguće manjim uticajem po poslovanje.

Na primer, rezervne kopije trebaju da pokrivaju svakodnevni rad, ali isto tako trebaju da omogućavaju 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?
- Gde se nalazi bekap?

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

Uvek dajte najviši prioritet ključnim podacima

Utvrđite raspored bekapa na osnovu toga koliko je posla vaša organizacija voljna da rizikuje da izgubi. Imajte na umu da su baze podataka i vaše računovodstvene datoteke vaši najkritičniji resursi i da se trebaju praviti rezervne kopije pre i nakon svake značajne upotrebe. Za većinu organizacija ovo znači da se bekap ovih datoteke 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 su dokumenti (u direktorijum „Your Documents“, na primer) i datoteke elektronske pošte se treba raditi najmanje jednom nedeljno ili čak jednom dnevno.³

Uvek testirajte vaš bekap

Testiranjem rezervnih kopija možete da utvrdite da li funkcionišu kako treba. Ovo vam omogućava da izmerite 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 meri 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 zahteva redundantnost u obliku nekoliko kopija koje su zaštićene u slučaju nepredviđenog incidenta.

Koristite skladištenje podataka na daljinu

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

Radite česti i redoviti bekap

Danas postoje alati koji 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 spremanje za i reagovanje na svaki hitni IT slučaj koji nastane.

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

Tim za reakciju na incidente je uobičajeno odgovoran za pripremu plana reakcije (vidite dole), kako bi se mogao preuzeti metodički pristup u rešavanju bezbednosnih incidenata i upravljanju sa posledicama. Tim isto tako testira i rešava slabe tačke sistema, održava snažne bezbednosne prakse i daje podršku merama za spravljanje 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 imati na umu 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 jer 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, iskorenjivanje i povratak, aktivnosti nakon incidenta).

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

Mnogo se incidenti izazivaju od strane korisnika unutra, tako da je važno obučiti zaposlene i druge krajnje korisnike o odgovarajućoj kompjuterskoj bezbednosti i isto tako pratiti njihovo korišćenje kako bi bili sigurni da oni nisu 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 bezbednosne 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 mere za automatsku izolaciju inficiranog hosta.
- Naučiti krajnje korisnike da ne radi nijednu radnju nakon incidenta, osim ako nije odobrena od tima za reakcije na incidente, kako bi se očuvali 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?
 - * Gde 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 celokupnog poslovanja jedne organizacije u slučaju velikog neočekivanog problematičnog događaja, oporavak od katastrofe se ovde odnosi na konkretne aktivnosti koje su povezane sa komunikacijskom i tehnološkom infrastrukturom i podacima.

Kada se dogodi neplanirani incident, suštinsko je da organizacije može nastaviti sa radom što je pre moguće. Plan za kontinuitet poslovanja je u celosti usmeren ka tom cilju, a plan za oporavak od katastrofe utvrđuje kako organizacija može efikasno i efektivno da povрати 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
- Javne neredne
- Nesreće ili ljudske greške
- Sajber kriminal

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

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

Efektivan 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:

1. Celoviti popis resursa (hardver, softver i podaci)
2. Minimalni prihvatljivi uticaj (prekid rada i nivo usluge)
3. Dokumentaciju o procesima i procedurama za oporavak od katastrofe (ugovori na nivou usluge, prioriteta za oporavak, resursi za bekap, overa podataka)
4. Odgovornosti za oporavak od katastrofe, operativne i ovlašćujuće; tj. ko radi aktivnosti za oporavak od katastrofe i ko ih odobrava
5. Plan za komunikaciju i odnose sa javnošću (kako bi dali odgovor ključnim činiocima i regulatorima i zaštitili reputaciju organizacije)
6. Obuku (plan je beskoristan ako niko ne zna kako da ga upotrebi)

Zaštitite vaš informacioni sistem

Zakrpe (patch) i ažuriranje (update)

Zakrpite i ažurirajte vaš operativni sistem i softver aplikacija

Ponekada može biti zamorno ažuriranje vašeg sistema i aplikacija, ali je vrlo važno da se uradi, zbog nekoliko razloga:

- **Bezbednost:** ažuriranje pomaže u **obebeđivanju vašeg kompjutera od napada**. Kao što se otkrivaju novi napadi, tako se identifikuju propusti koje sajber kriminalci koriste kako bi kompromitovali vaš operativni sistem i aplikacije. Ti se propusti rešavaju 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 rešavaju ažuriranim verzijama.

Prema tome, pametno je **koristiti automatsko ažuriranje za sisteme i aplikacije**. Na taj način se automatski preuzimaju osnovne bezbednosne popravke koje rešavaju 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.

Bezbedne konfiguracije

Koristite bezbedne konfiguracije za sve uređaje i softver

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

Kada se vrše izmene neke aplikacije, to zahteva menjanje i ažuriranje dokumentacije koja je kreirana za taj resurs. Dobra dokumentacija treba da omogući ponovnu izgradnju cele instance od samog početka i treba da uključuje:

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

Dokumentacija treba isto tako da uključuje:

- Dijagrame mreža i uređaja, kao i šemu fizičkih centara podataka
- Parametre za okruženje za rad aplikacija:
 - * Uspostavljena osnova koju treba slediti
 - * 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 šema

Za krajnje korisnike, bezbedna konfiguracija zahteva:

Uklanjanje i isključivanje svih nepotrebnih korisničkih naloga

Promenu 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

Osetljivi podaci

Šifrirajte sve osetljive podatke

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

Šifriranje je kritičan element sajber bezbednosti i može se koristiti na različite načine kako bi podaci ostali poverljivi i privatni, kao što su bezbedni (HTTPS) veb sajtovi, u bezbednim 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 bezbednosti.⁴

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

Prepoznavanje osetljivih informacija u vašem posebnom okruženju koje treba šifrirati je od vitalnog značaja i one, između ostalog, uobičajeno uključuju:

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

- Informacije sa ličnim identifikatorima
- Finansijske podatke
- Zdravstvene podatke
- Brojeve kreditnih kartica

Suzbijanje malicioznog softvera (malware)

Uvođenje anti-malware softvera

Malware ili maliciozni 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 bezbednosnih alata.

Pre dosta godina, kompanije za sajber bezbednost su pokušavale da kreiraju univerzalno anti-virusno rešenje koje može da odgovori na sve naše potrebe u jednom proizvodu. Međutim, to više nije efektivno, jer su sajber kriminalci evoluirali. Pretnja koju predstavljaju stalno postaje sve sofisticiranija, što vodi kompanije da razvijaju specifične anti-malware programe.

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

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

Osim toga, anti-malware softver nudi:

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

Firewall (vatrozid)

Uvedite firewall

Firewall pruža zaštitu od sajber 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 proveru saobraćaja i blokirajući neželjene paketiće.

Firewall u velikoj meri smanjuje rizik po pojedince i organizacije. Organizacije koje ne koriste firewall samo olakšavaju posao sajber kriminalcima, dajući im potencijalni pristup sistemima i datotekama, kao i mogućnost da šire maliciozne sadržine. 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:

- Prijavlivanja 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 bezbedne, 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 zamenjen ako je ne podržava.
- **Ažurirajte softver sa novim bezbednosnim verzijama i zakrpama.**
- Razmislite o lokaciji rutera kao o pitanju bezbednosti. Ljudi često nisu svesni 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 bezbednost, **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

Konfigurirate bezbednosne 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 bezbedno konfiguriramo, osobito jer se oni uobičajeno koriste sa osnovnim fabričkim postavkama.

Internet pretraživači predstavljaju važnu metu napada za sajber kriminalce, a nebezbedni 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 bezbedan. U tome, uvek uradite sledeće:

- **Uključite automatsko ažuriranje.** Ovaj **ključni korak** će zaštititi vašu organizaciju od mnogih slabih tačaka koje se otkrivaju svakog dana. To je suštinska komponenta dobre sajber higijene vašeg internet pretraživača koja će vam pomoći da ostanete sigurni i bezbedni.
- **Blokirajte pop-up obaveštenja, plugin softverske dodatke i phishing sajtove.** Većina pop-up obaveštenja su reklame, koje mogu biti zaražene malicioznim sadržinama, a plugin dodaci su poznati po svojim rizicima po bezbednost.
- **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 bezbednost pretraživača, kao što je korisnički pristup **https sajtovima umesto http sajtovima**.

Mobilni uređaji

Obezbedite mobilne uređaje

Mobilni uređaji mogu da kreiraju značajne bezbednosne i upravne izazove, osobito ako sadrže poverljive 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 bezbednosne aplikacije koje sprečavaju krađu informacija kada telefon koristi javne mreže.

Organizacije isto tako trebaju da:

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

IoT uređaji (Internet stvari)

Obezbedite IoT uređaje

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

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

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

Fizička bezbednost

Pobrinite se o fizičkoj bezbednosti uređaja, osobito mobilnih uređaja

Fizička bezbednost je isto toliko važna kao i sajber bezbednost. 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 osetljive informacije o poslovnim korisničkim nalogima ili korisničkim nalogima 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:

- Obezbedite vaš uređaj lozinkom i uključite dvofaktorsku autentifikaciju (2FA)
- Uvek čuvajte vredne stvari na sebi i nikada ne ostavljajte uređaje bez nadzora, osobito kada putujete

Pristup na daljinu

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

- Proveru da li je sav 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.
- Uslov da imate snažnu lozinku za dobijanje pristupa na daljinu.
- Uključivanje višefaktorske autentifikacije, ako je moguće.
- Proveru da li je praćenje i upozoravanje uključeno kako bi ste dobili upozorenje o sumnjivom napadu ili sumnjivoj aktivnosti.

Primenite 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 menjaju. Lozinke su prva linija odbrane protiv neovlašćenog pristupa.

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

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

Najlakši način da promenite ili ublažite ponašanje korisnika u vezi lozinke je **korišćenje programa za upravljanje lozinkama**. To omogućava kreiranje složenih lozinke 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 obavesti korisnike o bezbednosnim upadima vezanim za njihov i-mejl i 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 hakovanje. Prema tome, lozinke trebaju sadržati najmanje 12 karaktera.
- **Složenost je ključna!** Lozinke trebaju sadržati simbole, kombinaciju velikih i malih slova i brojeve. A onda ih treba i pomešati.
- **Koristite besmislene izraze** i izbegavajte predvidljivost. U idealnom slučaju, lozinke ne trebaju sadržati reči koje se mogu naći u rečniku (bilo kojeg jezika).
- **Lozinke trebaju biti unikatne.** Pravilo u svakoj organizaciji treba biti: jedan korisnički nalog, jedna lozinka.

Isto tako je važno **promeniti 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 proveru 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 zahteva dvofaktorsku autentifikaciju: nešto što osoba ima (karticu za bankomat) i nešto što osoba zna (svoj PIN).

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

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

- obezbedili korisnike od krađe identiteta zbog krađe lozinke.
- zaštitili organizaciju od slabih lozinke zaposlenih.
- umanjili upotrebu nekontrolisanih uređaja, posebno sa povećanom stopom rada od kuće zbog COVID pandemije.
- povećali efektivnost drugih bezbednosnih mera.
- pomogli organizaciji da ispuni zakonske uslove.

Korisnički nalozi (računi)

Koristite ograničene korisničke naloge za redovne i svakodnevne svrhe

Korisničkim nalogima se mora pažljivo rukovati, jer zloupotreba korisničkih naloga može da dovede 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 naprave promene 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 korisničkom nalogu mogu samo da pristupe datotekama tog korisnika. U tom smislu, restrikcije Standardnog korisničkog naloga idu u prilog organizaciji ako neprijatelj ili maliciozni 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 da 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.

Logovanje (evidentiranje)

Sprovođenje logiranja

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

Log kojemu je lako pristupiti i koji uključuje kritične informacije može da spasi informacije ili kompjuterski sistem. Logovanje pomaže sa:

- Otkrivanjem grešaka u programu
- Praćenjem grešaka
- Rešavanje problema sa performansama
- Računovodstvom
- Revizijom
- Bezbednošću

Log datoteke se isto tako mogu koristiti kako bi održali usaglašenost sa zakonima. Mnoge organizacije moraju biti u skladu sa različitim propisima koji zahtevaju reviziju aktivnosti, uključujući i davanje korisničkih naloga ili pristup finansijskim sistemima.

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

Svest o sajber bezbednosti

Uobičajene sajber pretnje

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

Napadi sa društvenim inženjeringom

Napadi sa društvenim inženjeringom dovode u zabludu ili manipulišu 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 bezbednosne procedure i najbolje prakse i dobili neovlašćeni pristup sistemima ili dali osetljive informacije.

U napadima sa društvenim inženjeringom, sajber kriminalci kriju svoje prave identitete i motive, predstavljajući se kao osobe od poverenja. Napad se potom vrši varanjem korisnika da kliknu maliciozne linkove ili dobijanjem fizičkog pristupa kompjuteru.

Phishing (pecanje)

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

I pored toga što tehničke mere bezbednosti postaju sve bolje, phishing ostaje jedan od najjeftinijih i najlakših načina da sajber kriminalci dobiju pristup osetljivim i ličnim informacijama. Korisnici samo trebaju da kliknu link i njihova bezbednost može biti ugrožena do te mere da mogu postati žrtve krađe identiteta. Korisnici isto tako mogu da kompromitiraju svoje lične informacije, akreditivne za najavu (korisnička imena i lozinke) i finansijske informacije (brojeve kreditnih kartica), ako kliknu na link.

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

Kako funkcioniše phishing?

Većina phishing kampanja uključuje jedan od dva osnovna metoda:

- **Maliciozni privitci (attachment)** u i-mejlovima, koji uobičajeno imaju alarmantne naslove kao „FAKTURA“. Kada budu otvoreni, ovi prilozi instaliraju malware na mašini korisnika.
- **Linkovi do malicioznih veb sajtova** koji su često klonovi legitimnih sajtova. Prelazak na sajt može da dovede do preuzimanja malicioznog softvera ili strana za najavu na sajtu može da sadrži skripte koje krađu akreditivne.⁷

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

Vrste phishing napada

Spear Phishing (ciljano pecanje)

Spear phishing je maliciozni napad sa lažnim i-mejlom koji cilja na određenu organizaciju ili osobu, pokušavajući da dobije neovlašćeni pristup osjetljivim informacijama. Malo je verovatno da će spear phishing pokušaji biti izvršeni od slučajnih napadača, već od sajber 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 zahteva od sajber kriminalaca da potroše vreme 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 usmeren 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 osjetljive 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 umesto i-mejla. Mete uobičajeno dobiju tekstualnu poruku koja sadrži obmanu i koja ih prinuđuje da daju lične ili finansijske informacije sajber 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 sprečiti phishing napade

U elektronskoj pošti: naučite da pažljivo gledate i-mejlove, posebno ako sadrže priloge ili veb linkove

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

- **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 verovatnoća da se radi o prevari.
- **Sumnjivi linkovi.** Korisnici nikada ne trebaju kliknuti na linkove u i-mejl poruci za koje sumnjaju da su maliciozni. Jedan način za testiranje legitimnosti linka je da zaustavite pokazivač miša na link – bez klikanja – kako bi utvrdili da li adresa odgovara informacijama u poruci.
- **Sumnjivi prilozima.** Ako korisnik dobije i-mejl sa prilogom, ili od osobe koju ne poznaju ili od osobe od koje ne očekuju da će im poslati prilog, oni moraju da razmisle da li se radi o phishing pokušaju. Preporučuje se da se prilozima nikada ne otvaraju dok se ne potvrdi njihova autentičnost. Zbog toga što postoje različiti načini da napadači prevare primaoca u verovanje da je dodata datoteka legitimna, važno je da korisnici znaju:
 - * Ikonici povezanoj sa prilogom se ne može verovati bez druge potvrde.
 - * Trebaju paziti na kombinovane ekstenzije datoteka kako što su „pdf.exe“, „rar.exe“, ili „txt.hta“.
 - * U slučaju sumnje, najbolje je stupiti u kontakt sa osobom koja je navodno poslala dotičnu

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 osećaj panike ili pritiska i da dovedu do brzog i nepromišljenog odgovora primaoca. Na primer, one mogu uključivati izjave kao „Morate odgovoriti do kraja dana!“, ili mogu indicirati da će primalac biti suočen sa potencijalnim finansijskim posledicama 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 izmenjene veb adrese koje u velikoj meri liče na imena veb sajtova dobro poznatih kompanija, kao „www.micorsoft.com“ ili „www.mircosoft.com“.
- **Nepodudarnosti.** Primaoci trebaju biti sumnjičavi 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

Okruženi 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 bezbednosti. Međutim, one predstavljaju prave bezbednosne rizike i trebaju se pažljivo koristiti.

Najveći bezbednosni problem sa javnim WI-FI mrežama je što korisnici ne znaju ko operiše mrežom ili ko je još drugi povezan na mrežu.

Prema tome, organizacije trebaju da:

- **Obuče zaposlene o rizicima korišćenja javnih WI-FI mreža.**
- **Zabrane zaposlenima da pristupaju osetljivim podacima kad koriste javne WI-FI mreže.**
- **Daju uputstva zaposlenima da se povezuju samo na mreže od poverenja.**
- **Zabrane zaposlenima da se povezuju na sajtove zaštićene lozinkama koristeći javne WI-FI mreže.**

Trebaju se razgledati druge opcije, umesto korišćenja javnih WI-FI mreža. Na primer, 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 snabdevače u inostranstvu. Korporativno ili javno dostupne i-mejl adrese izvršnih osoba ili zaposlenih na visokom nivou koji rade sa finansijama ili su uključeni u elektronska plaćanja se ili lažiraju ili kompromituju programima za snimanje otkucanja 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 maliciozne skripte na kompjutere ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim sajber 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 sajber kriminalac tajno ubaci između dva uređaja, ili između uređaja i nebezbedne WI-FI mreže, kako bi presretao komunikacije koje potom on može da čita i/ili menja. U takvom slučaju, korisnik može da nenamerno pošalje sajber 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-\(bec\)](https://www.trendmicro.com/vinfo/hk/security/definition/business-email-compromise-(bec))

Napad sa odbačenim USB

U napadu sa odbačenim USB, USB uređaj koji sadrži maliciozni kod se uključuje na kompjuter.

Uobičajeno, sajber pretnja predstavljena ovim napadom je infekcija malicioznim softverom ili virusom. Infekcije preko USB diska mogu biti i namerne i nenamerne, zavisno od dotičnog malicioznog softvera.

Bilo bi pametno da organizacije prekinu verovati zastareloj USB tehnologiji i počnu koristiti moć bezbednih digitalnih mreža koristeći cloud skladištenje podataka.

Malware (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 malicioznog softvera, čak i kada je botnet u funkciji.
- **Ransomware napadi (napadi sa softverom za otkupninu)**, koji šifriraju informacije korisnika i zahtevaju 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 vrše maliciozne aktivnosti kada budu izvršeni.
- **Virusi i crvi**, koji su maliciozni kod instaliran bez znanja korisnika. Virus 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 onemogućavanje usluge (DDoS) je sajber 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 onemogućavanje usluge (Denial-of-Service (DoS)). U DoS napadu, napadač koristi jednu internet konekciju kako bi zasuo metu sa lažnim zahtevima ili kako bi pokušao da iskoristi slabu tačku u sajber bezbednosti. Prema tome, DDoS je većih razmera 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 pojednu procesorsku moć mrežnih infrastrukturnih resursa kao što su serveri, firewall i servisi za dodelu mrežnog opterećenja ciljajući na Sloj 3 i Sloj 4 protokolarne komunikacije sa zahtevima 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 zahteva 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 **podizanja svesti o sajber pretnjama i informatičkoj bezbednosti**, jedan od najvažnijih elemenata sajber higijene koji se može sprovesti u bilo kojoj organizaciji je obuka o bezbednosnoj svesti, kako bi naučili zaposlene kako da izbegnu, identifikuju i prijave potencijalne pretnje.

Uključivanje osoblja u robusni kurs za obuku o bezbednosti je jedna od proaktivnih mera koje organizacije mogu da preduzmu kao zaštitu od sajber napada. Ako se ne uzme u obzir ovaj ljudski element, vrata vaše organizacije će biti široko otvorena sajber pretnjama.

Obuka o podizanju svesti o bezbednosti povećava znanje korisnika o potencijalnim pretnjama, čime se:

- smanjuju rizici;
- sprečava vreme neaktivnosti;
- poboljšava samopouzdanje zaposlenih; i
- podstiče poverenja klijenata.

Prema tome, obuke o podizanju svesti o bezbednosti su od vitalnog značaja u efektivnoj sajber bezbednosti i sajber higijeni. Isto tako, tokom vremena, godišnje obuke za podizanje svesti mogu da promene kulturu sajber bezbednosti u vašoj organizaciji. U najmanju ruku, ove obuke trebaju da uključuju informacije o:

- Osetljivim informacijama: šta su i kako rukovati s njima
- Kako prepoznati phishing i-mejlove
- 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)
- Osnovnoj sajber higijeni: šta je i kako je primeniti

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

Uspešni programi za podizanje svesti o bezbednosti:

- 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 pretnje u realnom vremenu, koje imaju brojne pojavne oblike koji se stalno menjaju).
- Izbegavaju ponavljanje istog sadržaja i žele da obogate zaposlene sa novim informacijama na svakoj obuci.
- Uključuju materijale koji idu van profesionalnog sveta do privatnih života zaposlenih, jer to vrši personalizaciju sadržaja i zaposleni su voljniji da slušaju.

Preporučuje se da ishodi obuke – pozitivni ili negativni – ostanu interni i da se ne dele sa činiocima.

Sažetak

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

- Obezbedite dovoljno obuke za vaše zaposlene da identifikuju i prijave sumnjive sajber aktivnosti.
- Osigurajte se da se svi serveri, radni kompjuteri, pametni telefoni i drugi uređaji koji koriste zaposleni često bezbednosno ažuriraju.
- Implementirajte strogu politiku za upravljanje pristupom sistemu koja zahteva višefaktorsku autentifikaciju gde god je moguće i stroge standarde za lozinke.
- Uložite u sisteme i rešenja koja omogućavaju jasnu vidljivost i granularnu kontrolu pristupa celoj mrežnoj infrastrukturi organizacije.

Iako može delovati da je složenost neprijatelj sajber kriminalaca, ona je u stvari neprijatelj vaše vlastite

sajber bezbednosti. U složenom i dinamičnom sajber svetu, vaša najbolja odbrana je da se vratite na osnove.

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

Okvir bezbednosti 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 priuštiva vašoj organizaciji
- Održiv/ponovljiv sa resursima vaše organizacije
- Podržavati vaše poslovne i operativne ciljeve

Zaključak

Na kraju, loše sajber navike – ili niska sajber higijena – su razlog najuspešnijih sajber napada. Zbog toga je toliko važno da organizacija razvije kulturu dobre sajber higijene. Međutim, mere preporučene u ovom Priručniku, iako uglavnom predstavljene iz perspektive organizacijske bezbednosti, su primenjive i na organizacije i na pojedince. Prema tome, organizacije trebaju savetovati zaposlene da razmisle o primeni navika sajber higijene i kod kuće. Ipak, dobre navike sajber higijene koje se koriste kod kuće će se verovatno i više koristiti na poslu. Dalje, svi smo mi bezbedniji u sajber svetu u kome se kultura sajber 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: Spisak dobrih praksi

ANALIZIRAJTE SISTEM I UTVRĐITE PROCEDURE I POLITIKE		
Kategorija	Dobre prakse	Relevantni činioci
Popis hardvera i softvera	<ul style="list-style-type: none"> - Održavajte popis hardvera i softvera - Standardizujte vaš popis hardvera i softvera 	Javne institucije i MSP
Popis osetljivih ili kritičnih informacija	<ul style="list-style-type: none"> - Održavajte popis osetljivih ili kritičnih informacija - Shvatite vaše okruženje podataka i identifikujte važne podatke u vašoj sredini - Kreirajte politiku za klasifikaciju podataka - Šifrirajte podatke, naročito podatke koji su klasifikovani kao „ograničeni“ - Uvedite sistem za sprečavanje gubitka podataka 	Javne institucije i MSP
Analiza rizika	<ul style="list-style-type: none"> - Identifikujte rizike <ul style="list-style-type: none"> • ljudski rizik (prevara, krađa, ljudska greška) • prirodni rizik (poplave, požari, zemljotresi, itd.) • tehnički rizici (defekt softvera, hardvera, nedostatak znanja) - Izbegavajte rizik – ako nije neposredna briga po vaše poslovanje - Smanjite rizik – uvođenjem novih bezbednosnih rešenja - Prihvatite rizik – kada je mala verovatnoća da će se rizik dogoditi ili je iznad tekućih kapaciteta - Prenesite rizik – osiguranjem 	Javne institucije i MSP
Procedure za bekap (rezervne kopije)	<ul style="list-style-type: none"> - Uspostavite proceduru za redovni bekap - Budite realni u pripremi politike za bekap i pripremite pisani bekap plan koji propisuje: <ul style="list-style-type: none"> • Šta se stavlja na bekap? • Gde se nalazi bekap? • Koliko često se radi bekap? • Ko je zadužen da vrši bekap? - Uvek dajte najviši prioritet ključnim podacima - Uvek testirajte bekap - Koristite pravilo 3-2-1 - Koristite skladištenje podataka na daljinu/cloud - Često i redovito ažurirajte bekap 	Javne institucije i MSP
Reakcija na incidente	<ul style="list-style-type: none"> - Pripremite plan za reakciju na incidente ili PRI - Kada se dogodi incident kritično je da se sledi PRI 	Javne institucije
Kontinuitet poslovanja i oporavak od katastrofe	<ul style="list-style-type: none"> - Pripremite plan za kontinuitet poslovanja i oporavak od katastrofe 	Javne institucije

ZAŠTITITE VAŠ INFORMACIONI SISTEM		
Operativni sistem i softver aplikacija	<ul style="list-style-type: none"> - Zakrpite i ažurirajte vaš operativni sistem i softver aplikacija, zbog: <ul style="list-style-type: none"> • Bezbednosti • Novih mogućnosti • Popravki - Uključite automatsko ažuriranje za sisteme i aplikacije 	Javne institucije i MSP
Bezbedne konfiguracije	<ul style="list-style-type: none"> - Koristite bezbedne konfiguracije za sve uređaje i softver - Dokumentujte sva ažuriranja i promene <ul style="list-style-type: none"> • Evidentirajte promene • Utvrdite bezbednosni osnov • Sprovedite proces provere i odobrenja • Evidentirajte promene konfiguracija 	Javne institucije i MSP
Osetljivi podaci	<ul style="list-style-type: none"> - Šifrirajte sve osetljive podatke - Šifriranje pomaže u zaštiti osetljivih i privatnih informacija čineći ih nečitljivim za sajber kriminalce, jer se njima samo može pristupiti ključem 	Javne institucije i MSP
Anti-malware softver	<ul style="list-style-type: none"> - Koristite anti-malware softver - Anti-malware rešenja će blokirati najveći deo malicioznih i potencijalno neželjenih programa 	Javne institucije i MSP
Firewall (vatrozid)	<ul style="list-style-type: none"> - Koristite firewall, kako bi: <ul style="list-style-type: none"> • blokirali najveći deo malicioznih i potencijalno neželjenih programa • sprečili izvršavanje malicioznog softvera na uređaju • sprečili maliciozni softver da promeni postavke • sprečili maliciozni softver da izvrši dodatni kompromitovani softver 	Javne institucije i MSP
WI-FI mreže	<ul style="list-style-type: none"> - Zaštite WI-FI mreže - Koristite enkripciju bežičnih mreža - Ažurirajte softver sa novim bezbednosnim 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	<ul style="list-style-type: none"> - Uvek konfigurišite bezbednosne postavke internet pretraživača - Blokirate pop-up obaveštenja, plugin softverske dodatke i phishing sajtove - Nemojte dozvoliti da se lozinke čuvaju u pretraživaču - Isključite kolačiće (cookies) trećih strana - Deinstalirajte sve ekstenzije pretraživača koje ne koristite - Redovno ažurirajte sve ekstenzije koje koristite - Podstaknite korisnike da koriste https sajtove umesto http sajtova 	Javne institucije i MSP
Mobilni uređaji	<ul style="list-style-type: none"> - Tražite od korisnika da: <ul style="list-style-type: none"> • Zaštite uređaje lozinkama • Šifriraju podatke • Instaliraju bezbednosne aplikacije koje sprečavaju sajber kriminalce da krađu informacije kada je telefon povezan na javne mreže • Konfiguriraju uređaje da se automatski zaključavaju - Uspostave procedure za prijavljivanje izgubljene ili ukradene opreme 	Javne institucije i MSP
IoT uređaji (internet stvari)	<ul style="list-style-type: none"> - Obezbedite IoT uređaje: <ul style="list-style-type: none"> • promenite fabričke lozinke • koristite snažne lozinke • redovno ažurirajte softver na uređajima • šifrirajte i proverite autentičnost uređaja • promenite fabričke postavke za privatnost • promenite fabričke postavke • osigurajte bezbednost mreže organizacije i WI-FI mreže • kreirajte posebnu mrežu za goste • uvek proverite dostupne verzije za ažuriranje na veb sajtovima proizvođača pre nego što ih instalirate na uređaje 	Javne institucije i MSP
Fizička bezbednost uređaja	<ul style="list-style-type: none"> - Pobrinite se o fizičkoj bezbednosti uređaja, osobito mobilnih uređaja: <ul style="list-style-type: none"> • Zaštitom uređaja sa snažnim lozinkama • Stalnog čuvanje uređaja kod korisnika/vlasnika 	Javne institucije i MSP

Pristup na daljinu	<ul style="list-style-type: none"> - 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 - Proverite da li je praćenje i upozoravanje uključeno kako bi ste dobili upozorenje o sumnjivom napadu ili sumnjivoj aktivnosti 	Javne institucije i MSP
--------------------	---	-------------------------

PRIMENITE DOBRE PRAKSE		
Lozinke	<ul style="list-style-type: none"> - Duže lozinke su bolje - <i>Složenost je ključna!</i> Tražite simbole, kombinaciju velikih i malih slova i brojeve - Koristite besmislene pojmove i izbegavajte predvidljivost - Lozinke trebaju biti unikatne - Promenite sve fabričke lozinke 	Javne institucije i MSP
Višefaktorska autentifikacija	<ul style="list-style-type: none"> - Koristite višefaktorsku autentifikaciju kad god je to moguće - Koristite dva ili tri faktora za proveru autentičnosti – nešto što korisnik <i>zna, je ili ima</i> 	Javne institucije i MSP
Korisnički nalozi	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Nemojte obezbediti nijednom zaposlenom pristup svim sistemima podataka - 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
Logovanje (evidentiranje)	<ul style="list-style-type: none"> - Održavajte konzistentno logovanje - Shvatite šta treba evidentirati, na osnovu najboljih praksi, i razgledati logove na dnevnoj osnovi tražeći greške, anomalije ili sumnjive aktivnosti 	Javne institucije

SVEST O SAJBER BEZBEDNOSTI

Uobičajene sajber pretnje	VRSTA SAJBER PRETNJE	PREPORUKA	
	<ul style="list-style-type: none"> - Društveni inženjering - Phishing napadi (pecanje) <ul style="list-style-type: none"> • 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 (maliciozni softver) <ul style="list-style-type: none"> • Botnet softver • Ransomware napad • Spyware • Trojanski virus • Virusi i crvi - DoS/DDoS napadi (onemogućavanje usluge) <ul style="list-style-type: none"> • Volumetrijski • Napadi na protokol • Napadi na aplikacije 	<ul style="list-style-type: none"> - I-MEJLOVI: pažljivo gledajte i-mejlove, posebno ako sadrže priloge ili veb linkove. Tražite: <ul style="list-style-type: none"> • Pravopis i lošu gramatiku • Sumnjive linkove • Sumnjive priloge • Pretnje u jeziku • Maskiranje • Promenjene veb adrese • Nepodudarnosti - JAVNE WI-FI MREŽE: uvek pazite kada se povezujete na javne WI-FI mreže: <ul style="list-style-type: none"> • Ne pristupajte osetljivim podacima • Povezujte se samo na mreže od poverenja • Odaberite opcije da se <i>ne</i> povezujete automatski 	Javne institucije i MSP
Redovne obuke	<ul style="list-style-type: none"> - Podignite svest o sajber pretnjama i informatičkoj bezbednosti godišnjim ili češćim obukama - Robusni kurs za obuku o dizanju svesti o bezbednosti treba da pokriva: <ul style="list-style-type: none"> • Osetljive 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 informacione sisteme • Kako rukovati sa informacijama koje sadrže lične identifikatore (PII) • Osnovna sajber higijena: šta je i kako je primeniti 		Javne institucije i MSP

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