Priručnik o sigurnosti na internetu:

sajber 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 sigurnosti je posvećen poboljšanju sigurnosti država i njihovog stanovništva u okviru demokratskog upravljanja, vladavine prava, poštovanja ljudskih prava i rodnoj jednakosti. Od svog osnivanja 2000. godine, DCAF je pridonio kreiranju održivijeg mira i razvoja pomažući države partnere i međunarodne činioce koji podržavaju te države u poboljšanju upravljanja sektorom sigurnosti 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 sigurnosti.

DCAF – Ženevski centar za upravljanje sektorom sigurnosti
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

Sadržaj

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 osigurala odgovarajući nivo informatičke sigurnosti za svoje informatičke sisteme.

Fokus ovde je na davanju uvoda u važnost sajber higijene i preporuka o jednostavnim koracima koji će poboljšati sajber sigurnost u vašoj organizaciji.

Ukratko, higijena u sigurnosti 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 sigurnost 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 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 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 sigurnost na internetu“.
- Kaspersky Lab potencira da se sajber higijena tiče „obučavanja samog sebe za stvaranje dobrih navika u vezi sa sajber sigurnošću, kako bi bili korak ispred sajber prijetnji i sigurnosnih problema na internetu“.
- Časopis Security opisuje sajber higijenu u pogledu toga da „trebate biti sigurni da kod vas funkcionišu osnovne kontrole za sigurnost i da se one konzistentno primjenjuju 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 sigurnost 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 sigurno rukovanje kritičnim podacima i sigurnost 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 sigurnosnih 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 zahtjeva sprovođenje određenih uobičajenih mjera, od uspostavljanja standardiziranih procedura i politika, do redovitih obuka koje pomažu zaposlenima da razumiju sajber prijetnje koje se stalno mijenjaju. Priroda i karakter nekih od ovih prijetnji su objašnjeni u daljem tekstu (vidite Uobičajene sajber prijetnje). Međutim, prvo su predstavljeni ključni elementi efektivnoga 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 mijenjaju, 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 promjenama

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. Dokumentiranja osnovne sigurnosne pozicije organizacije
2. Standardizacija iste u celoj organizaciji na osnovi politika i procedura
3. Monitoring i reagiranje 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 prosječno vreme do ponovnog uspostavljanja usluga (MTTRS)

Popis informacija

Održavajte popis osjetljivih ili kritičnih informacija

Zaštita osjetljivih 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 razmjenjuju. Prema tome, nije čudno što više od polovne korporativnih podataka su „tamni“, što znači da nisu klasifikovani, zaštićeni ili rukovođeni.

Važno je **razumjeti 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 primjer sadrži tri nivoa:

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

Kao drugi korak, podaci trebaju biti šifrirani, osobito 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 provesti **sistem za sprečavanje gubitka podataka** za otkrivanje potencijalnih upada u podacima/transmisija za izvlačenje podataka i njihovo sprečavanje putem praćenja, otkrivanja i blokiranja osjetljivih 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
- Razmjenu
- Cloud i SaaS (softver kao usluga) aplikacije koje nisu Microsoft aplikacije

Procjena rizika

Identifikacija rizika

Upravljanje rizikom zahtjeva razumevanje 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 ne mora da se dogodi.

Postoje tri oblasti rizika po informatičke 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, procjena rizika uključuje dodjeljivanje vrijednosti kritičnim resursima, uključujući i finansijske i reputacijske. Ovo vam pomaže da počnete procjenu kolika je težina svake posebne prijetnje. Jedan efektivan 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 gde da usredsredite vaše aktivnosti i pomoći će vam da odlučite kako da pristupite utvrđenim rizicima, na primjer putem:

- **Izbjegavanja**, kada rizici nisu neposredna briga po vaše poslovanje
- **Smanjenja**, kada rizici zahtijevaju implementaciju novog sigurnosnog rešenja
- **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 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 sa povrate ključni podaci po potrebi i sa što je moguće manjim uticajem po poslovanje.

Na primjer, 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 vraćeni.

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

Utvrdite 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 direktoriju „Your Documents“, na primjer) i datoteke elektronske pošte se treba raditi najmanje jednom nedjeljno ili čak jednom dnevno.[3]

Uvek testirajte vaš bekap

Testiranjem rezervnih kopija možete da utvrdite da li funkcionišu kako treba. 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 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 zahtjeva 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 obezbijedite 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 vještine, što omogućava timu da bude sposoban da odgovori na široki dijapazon sigurnosnih 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 rješavanju sigurnosnih incidenata i upravljanju sa posljedicama. Tim isto tako testira i rješava slabe tačke sistema, održava snažne sigurnosne prakse i daje podršku mjerama za rješavanje incidenta.

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, osobito 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, iskorjenjivanje i povratak, aktivnosti nakon incidenta).

Kada se dogodi incident kritično je da slijedite vaš PRI, koji sadrži procedure za reakciju na različite vrste incidenata.

Mnogu se incidenti izazivaju od strane korisnika unutra, tako da je važno obučiti zaposlene i druge krajnje korisnike o odgovarajućoj kompjuterskoj sigurnosti 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 sigurnosne 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 cjelokupnog 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 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 provođenja plana za oporavak od katastrofe uključuju:

- Prirodne katastrofe
- Rat ili terorizam
- Javne nerede
- 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 izbjegne regulatorne ili zakonske prekršaje.

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

1. Cjeloviti 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, prioriteti za oporavak, resursi za bekap, ovjera 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 informatički sistem

Zakrpe (patch) i ažuriranje (update)

Zakrpite i ažurirajte vaš operativni sistem i softver aplikacija

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

- **Sigurnost**: ažuriranje pomaže u **osiguravanju 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 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 koristi 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.

Prema tome, pametno je **koristiti automatsko ažuriranje za sisteme i aplikacije**. Na taj način se automatski preuzimaju osnovne sigurnosne 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 kliktati na slijepo.

Sigurne konfiguracije

Koristite sigurne konfiguracije za sve uređaje i softver

Jedan način da zaštitite ljude i organizaciju od malicioznih aktivnosti je da koristite sigurne 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 **dokumentiranje svih ažuriranja i promjena**, kako bi se imao uvid u konfiguracije svih sistema.

Kada se vrše izmjene neke aplikacije, to zahtjeva mijenjanje 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) promjena** operativnog sistema i aplikacija (update), promjene 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 dokumentiran.
- **Sigurnu osnovu** za resurse. To je dogovoreni minimalni standard sigurnosti koji se odnosi na, na primjer, isključivanje nepotrebnih usluga, brisanje korisničkih naloga za goste, izloženost javnom internetu, itd.
- **Proces provjere i odobrenja** koji je lako pratiti. Dobra je praksa da provjeravate vaše konfiguracije i postavke s vremena na vreme, jer incidenti u vašem okruženju mogu da vam daju ideju o tome šta treba promijeniti. Isto taka, 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 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, sigurna konfiguracija zahtjeva:

- Uklanjanje i isključivanje svih nepotrebnih korisničkih naloga
- Promjenu 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

Osjetljivi podaci

Šifrirajte sve osjetljive 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 sajber sigurnosti i može se koristiti na različite načine kako bi podaci ostali povjerljivi i privatni, kao što su sigurni (HTTPS) veb sajtovi, u sigurnim aplikacijama za slanje poruka i i-mejl usluga i kroz virtualne privatne mreže (VPN). Šifriranje štiti informacije dok se one aktivno kreću sa jedne lokacije na drugu (tj. u tranzitu), od pošiljaoca do primaoca, a isto tako štiti i informacije u mirovanju. Ako neko dobije pristup bazi podataka u kojoj postoje šifrirane informacije, šifriranje predstavlja dopunski sloj sigurnosti.[4]

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

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

- Informacije sa ličnim identifikatorima
- Finansijske podatke

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

- 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 sigurnosnih alata.

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

Važno je razumjeti 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 prijetnje 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 spriječili 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 osjetljivih 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 provjeru 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 konfigurirani, 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 sigurne, 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 sigurnosnim verzijama i zakrpama**.
- Razmislite o lokaciji rutera kao o pitanju sigurnosti. Ljudi često nisu svjesni da ruter koji se nalazi pored vrata ili prozora povećava šansu da će WI-FI signal biti presretnut od osobe sa malicioznim namjerama. Kako bi poboljšali vašu WI-FI sigurnost, **najbolje je da postavite ruter što je moguće bliže sredini vaše kancelarije**, jer time umanjujete šansu da se hakeri povežu na vašu mrežu.
- **Uključite filtriranje MAC adresa** kako bi kontrolirali 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 sigurnosne 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 konfiguriramo, osobito jer se oni uobičajeno koriste sa osnovnim fabričkim postavkama.

Internet pretraživači predstavljaju važnu metu napada za sajber kriminalce, a nesiguran 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 siguran. U tome, uvek uradite slijedeće:

- **Uključite automatsko ažuriranje**. Ovaj ***ključni korak*** će zaštiti 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 bezbjedni.
- **Blokirajte pop-up obavještenja, plugin softverske dodatke i phishing sajtove**. Većina pop-up obavještenja su reklame, koje mogu biti zaražene malicioznim sadržinama, a plugin dodaci su poznati po svojim rizicima po sigurnost.
- **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 sigurnost pretraživača, kao što je korisnički pristup **https sajtovima umesto http sajtovima**.

Mobilni uređaji

Osigurajte mobilne uređaje

Mobilni uređaji mogu da kreiraju značajne sigurnosne 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 sigurnosne 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.
- Konfigurišu uređaje da se automatski zaključavaju nakon određenog vremena.

IoT uređaji (Internet stvari)

Osigurajte 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 razmjenjuju podatke u realnom vremenu. Zbog toga što prikuplja podatke od fizičkih i virtualnih sistema, IoT predstavlja veliku „površinu za napad“ za sajber napadače, ako nije adekvatno osigurano.

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

- Promijenite fabričke lozinke
- Koristite snažne lozinke
- Ažurirajte softver na uređajima (uvek 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 sigurnost vaše mreže i WI-FI
- Kreirajte posebnu mrežu za goste

Fizička sigurnost

Pobrinite se o fizičkoj sigurnosti uređaja, osobito mobilnih uređaja

Fizička sigurnost je isto toliko važna kao i sajber sigurnost. 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 osjetljive 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:

- Osigurajte vaš uređaj lozinkom i uključite dvofaktorsku autentifikaciju (2FA)
- Uvek 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 siguran, šifriran i sakriven. To zahtjeva:

- Provjeru 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.
- 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

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 redovito mijenjaju. Lozinke su prva linija odbrane protiv neovlaštenog pristupa.

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

- Navika korisnika da čuvaju lozinke u bilješkama, 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.
- Razmjena lozinki sa kolegama ili putem i-mejla, instant poruka ili drugih platformi (ovo je osobito velika slaba tačka ako se lozinke ne mijenjaju redovito).

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 sigurnosnim upadima vezanim za njihov i-mejl i više.

Ako vaša organizacija ne koristi program za upravljanje lozinkama, ovo su neki **savjeti 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 ključna**! Lozinke trebaju imati simbole, kombinaciju velikih i malih slova i brojeve. A onda ih treba i pomiješati.
- **Koristite besmislice** i izbjegavajte predvidljivost. U idealnom slučaju, lozinke ne trebaju imati reči 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 izbjegli 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 zahtjeva dvofaktorsku autentifikaciju: nešto što osoba ima (karticu za bankomat) i nešto što osoba zna (svoj PIN).

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

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

- osigurali korisnike od krađe identiteta zbog krađe lozinke.

- zaštitili organizaciju od slabih lozinki zaposlenih.
- umanjili upotrebu nekontroliranih uređaja, osobito sa povećanom stopom rada od kuće zbog COVID pandemije.
- povećali efektnost drugih sigurnosnih 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 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);
- konfiguriran da zaštiti vaš sistem od očiglednih napada; i
- ne dozvoljava korisnicima da naprave 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 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.

Logiranje (evidentiranje)

Sprovođenje logiranja

Iz sigurnosne 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. Logiranje pomaže sa:
- Otkrivanjem grešaka u programu
- Praćenjem grešaka
- Rješavanje problema sa performansama
- Računovodstvom
- Revizijom
- Sigurnošću

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

Najveći problem povezan za logiranje je nedostatak monitoringa. Važno je razumjeti šta treba evidentirati,

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

na osnovu najboljih praksi, i razgledati logove na dnevnoj osnovi tražeći greške, anomalije ili sumnjive aktivnosti. Ipak, prekomjerno logiranje nije od pomoći, jer stvara dosta „buke“ i zahtjeva veći kapacitet za čuvanje podataka. Prema tome, neke aktivnost možda imaju veći prioritet za logiranje od drugih.

Svijest o sajber sigurnosti

Uobičajene sajber prijetnje

Sajber napad je maliciozni 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 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 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 sigurnosne procedure i najbolje prakse i dobili neovlašteni pristup sistemima ili dali osjetljive informacije.

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

Phishing (pecanje)

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

I pored toga što tehničke mere sigurnosti postaju sve bolje, phishing ostaje jedan od najjeftinijih i najlakših načina da sajber kriminalci dobiju pristup osjetljivim i ličnim informacijama. Korisnici samo trebaju da kliknu link i njihova sigurnost može biti ugrožena do te mere 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 maliciozne i-mejlove koji deluju kao da su od izvora od povjerenja, 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 privitci 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 kradu akreditive.[7]

Vrste phishing napada

Spear Phishing (ciljano pecanje)

Spear phishing je maliciozni napad sa lažnim i-mejlom koji cilja na određenu organizaciju ili osobu,

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

pokušavajući da dobije neovlašteni 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 vrijedne 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 zahtjeva od sajber kriminalaca da potroše vreme i resurse na istraživanju pre napada, jer će biti utoliko uspješniji 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 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 tjera 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 provodili 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 privitke 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 vjerovatnoća da se radi o prevari.
- **Sumnjivi linkovi**. Korisnici nikada ne trebaju kliktati 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 kliktanja – kako bi utvrdili da li adresa odgovara informacijama u poruci.
- **Sumnjivi privitci**. Ako korisnik dobije i-mejl sa privitkom, ili od osobe koju ne poznaju ili od osobe od koje ne očekuju da će im poslati privitak, oni moraju da razmisle da li se radu o phishing pokušaju. Preporučuje se da se privitci nikada ne otvaraju dok se ne potvrdi njihova autentičnost. Zbog toga što postoje različiti načini da napadači prevare primače u vjerovanje da je dodata datoteka legitimna, važno je da korisnici znaju:
    * Ikonici povezanoj sa privitkom se ne može vjerovati 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 privitak legitimni.
- **Prisilne poruke**. Ovi i-mejlovi imaju za cilj da izazovu osjećaj panike ili pritiska i da dovedu do brzog i nepromišljenog odgovora primaoca. Na primjer, one mogu uključivati izjave kao „Morate odgovoriti do kraja dana!“, ili mogu navoditi da će primaoc biti suočen sa potencijalnim finansijskim

8 Types of Cyber Threat in 2019 | IT Governance USA

posljedicama 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 izmjenjene 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 sumnjivi 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 sigurnosti. Međutim, one predstavljaju prave sigurnosne rizike i trebaju se pažljivo koristiti.

Najveći sigurnosni problem sa javnim WI-FI mrežama je što korisnici ne znaju ko operira 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 osjetljivim podacima kad koriste javne WI-FI mreže**.
- **Daju upute zaposlenima da se povezuju samo na mreže od povjerenja**.
- **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 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 upotrijebiti 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.

Kompromitiranje poslovnog i-mejla (Business Email Compromise)

Kompromitiranje poslovnog i-mejla (BEC) je vrsta prevare koja cilja na kompanije koje koriste elektronske transfere i imaju snabdjevače u inostranstvu. Korporativno ili javno dostupne i-mejl adrese izvršnih osoba ili zaposlenika na visokom nivou koji rade sa financijama 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 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 Čovjek-u-sredini (Man in the Middle (MITM))

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

Napadi sa odbačenim USB

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

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

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

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

Bilo bi pametno da organizacije prekinu vjerovati zastariloj USB tehnologiji i počnu koristiti moć sigurnih digitalnih mreža koristeći cloud spremanje 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 zarazi 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 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 vrše maliciozne aktivnosti kada budu izvršeni.
- **Virusi i crvi**, koji su maliciozni 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 zakače za 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 prometom kako bi spriječio korisnike da pristupe povezanim internet uslugama i sajtovima.

DDoS napad je potkategorija opšteg napada za onemogućavanje usluge (Denial-of-Service (DoS)). U DoS napadu, napadač koristi jednu internet konekciju kako bi poslao meti lažne zahtjeve ili kako bi pokušao da iskoristi slabu tačku u sajber sigurnosti. 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 generiranje 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 ciljanoga sajta.
- **Napadi na protokole**: ovi napadi su osmišljeni da pojedu procesorsku moć mrežnih infrastrukturnih resursa kao što su serveri, firewall i servisi za dodjelu mrežnog opterećenja ciljajući na Sloj 3 i Sloj 4 protokolarne komunikacije sa zahtjevima 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 zahtjeva za transakcije koji troše ograničene resurse kao što je disk prostor ili dostupna memorija.[13]

Redovne obuke

Sa ciljem **podizanja svijesti o sajber pretnjama i informatičkoj sigurnosti**, jedan od najvažnijih elemenata sajber higijene koji se može sprovesti u bilo kojoj organizaciji je obuka o sigurnosnoj svijesti, kako bi naučili zaposlene kako da izbjegnu, identifikuju i prijave potencijalne prijetnje.

Uključivanje osoblja u robusni kurs za obuku o sigurnosti je jedna od proaktivnih mjera koje

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

organizacije mogu da preduzmu kao zaštitu od sajber napada. Ako se ne uzme u obzir ovaj ljudski elemenat, vrata vaše organizacije će biti široko otvorena sajber pretnjama.

Obuka o podizanju svijesti o sigurnosti povećava znanje korisnika o potencijalnim pretnjama, čime se:

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

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

- Osjetljivim 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 primjeniti

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

Uspješni programi za podizanje svijesti o sigurnosti:

- 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 sveta do privatnih života zaposlenih, jer to vrši personalizaciju sadržaja i zaposleni su spremniji da slušaju.

Preporučuje se da ishodi obuke – pozitivni ili negativni – ostanu interni i da se ne dijele 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 svijest korisnika. Prema tome, nedostatak konzistentne sajber higijene je jedna od najopasnijih prijetnji koja se može javiti unutar organizacije. Kako bi podstakli dobru sajber higijenu u vašoj celoj organizaciji:

- Osigurajte 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 sigurnosno ažuriraju.
- Implementirajte strogu politiku za upravljanje pristupom sistemu koja zahtjeva 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 djelovati da je složenost neprijatelj sajber kriminalaca, ona je u stvari neprijatelj vaše vlastite sajber sigurnosti. U složenom i dinamičnom sajber svetu, vaša najbolja odbrana je da se vratite na osnove.

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

Okvir sigurnosti 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 koju si vaša organizacija može priuštiti
- Održiv/ponovljiv sa resursima vaše organizacije
- Podržavati vaše poslovne i operativne ciljeve

Zaključak

Na kraju, loše sajber navike – ili niska sajber higijena – su razlog najuspješnijih 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 sigurnosti, su primjenjive i na organizacije i na pojedince. Prema tome, organizacije trebaju potencirati zaposlenima da razmisle o primjeni 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 sigurniji 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: 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 osjetljivih ili kritičnih informacija	- Održavajte popis osjetljivih ili kritičnih informacija - Shvatite vaše okruženje podataka i identifikujte važne podatke u vašoj sredini - Kreirajte politiku za klasifikaciju podataka - Šifrirajte podatke, osobito podatke koji su klasificirani kao „ograničeni“ - Uvedite sistem za sprečavanje gubitka podataka	Javne institucije i MSP
Analiza rizika	- Identifikujte rizike • ljudski rizik (prevara, krađa, ljudska greška) • prirodni rizik (poplave, požari, zemljotresi, itd.) • tehnički rizici (defekt softvera, hardvera, nedostatak znanja) - Izbjegavajte rizik – ako nije neposredna briga po vaše poslovanje - Smanjite rizik – uvođenjem novih sigurnosnih rešenja - 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 pisani bekap plan koji propisuje: • 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	- Pripremite plan za reakciju na incidente ili PRI - Kada se dogodi incident kritično je slijediti 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: • Sigurnosti • Novih mogućnosti • Popravki - Uključite automatsko ažuriranje za sisteme i aplikacije	Javne institucije i MSP
Sigurne konfiguracije	- Koristite sigurne konfiguracije za sve uređaje i softver - Dokumentirajte sva ažuriranja i promjene • Evidentirajte promjene • Utvrdite sigurnosni osnov • Sprovedite proces provjere i odobrenja • Evidentirajte promjene konfiguracija	Javne institucije i MSP
Osjetljivi podaci	- Šifrirajte sve osjetljive podatke - Šifriranje pomaže u zaštiti osjetljivih i privatnih informacija čineći ih nečitljivim za sajber kriminalce, jer se njima samo može pristupiti ključem	Javne institucije i MSP
Anti-malware softver	- Koristite anti-malware softver - Anti-malware rešenja će blokirati najveći deo malicioznih 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 promeni 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 sigurnosnim 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	- Uvek konfigurišite sigurnosne postavke internet pretraživača - Blokirajte pop-up obavještenja, 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	- Tražite od korisnika da: • Zaštite uređaje lozinkama • Šifriraju podatke • Instaliraju sigurnosne aplikacije koje sprečavaju sajber 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)	- Osigurajte IoT uređaje: • promijenite fabričke lozinke • koristite snažne lozinke • redovno ažurirajte softver na uređajima • šifrirajte i provjerite autentičnost uređaja • promijenite fabričke postavke za privatnost • promijenite fabričke postavke • osigurajte mrežu organizacije i WI-FI mreže • kreirajte posebnu mrežu za goste • uvek provjerite dostupne verzije za ažuriranje na veb sajtovima proizvođača pre nego što ih instalirate na uređaje	Javne institucije i MSP
Fizička sigurnost uređaja	- Pobrinite se o fizičkoj sigurnosti uređaja, osobito mobilnih uređaja: • Zaštitom uređaja sa snažnim lozinkama • Stalnog čuvanje uređaja kod korisnika/vlasnika	Javne institucije i MSP

Pristup na daljinu	- Provjerite 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 - Tražite 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

PRIMENITE DOBRE PRAKSE		
Lozinke	- Duže lozinke su bolje - Složenost je ključna! Tražite simbole, kombinaciju velikih i malih slova i brojeve - Koristite besmislice i izbjegavajte predvidljivost - Lozinke trebaju biti unikatne - Promijenite 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 namjene	Javne institucije i MSP
Pristup zaposlenih	- Nemojte dati 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
Logiranje (evidentiranje)	- Održavajte konzistentno logiranje - Shvatite 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">SVEST O SAJBER SIGURNOSTI</th></tr>
<tr><td>Uobičajene sajber prijetnje</td><td>VRSTA SAJBER PRETNJE</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)
- Kompromitiranje poslovnog i-mejla (BEC)
- Preuzimanje podataka u „prolazu“ (Drive-By Downloads)
- Napadi Čovjek-u-sredini (MITM)
- USB Drop napad
- Malware (maliciozni 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, osobito ako sadrže privitke ili veb linkove. Tražite:
• Pravopis i lošu gramatiku
• Sumnjive linkove
• Sumnjive privitke
• Prijetnje u jeziku
• Maskiranje
• Promijenjene veb adrese
• Nepodudarnosti
- JAVNE WI-FI MREŽE: uvek pazite kada se povezujete na javne WI-FI mreže:
• Ne pristupajte osjetljivim podacima
• Povezujte se samo na mreže od povjerenja
• Odaberite opcije da se ne povezujete automatski</td></tr>
<tr><td>Redovne obuke</td><td colspan="2">- Podignite svest o sajber pretnjama i informatičkoj sigurnosti godišnjim ili češćim obukama
- Robusni kurs za obuku o dizanju svesti o sigurnosti treba da pokriva:
• Osjetljive 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 sajber 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