Priručnik o kiber prijetnjama: identifikacija i borba protiv rizika za korisnike u javnom i privatnom sektoru i građane

Aleksandar Bratić

Oktobar 2022. godina

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 upravlja, vladavine prava, poštovanja ljudskih prava i rodnoj jednakosti. Od svog osnivanja 2000. godine, DCAF je pridoneo kreiranju održivijeg mira i razvoja pomažući države partnere i međunarodne činioce koji podržavaju te države u poboljšanju upravljanja sektorom 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
Design & layout: DTP studio

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

DCAF Geneva Centre for Security Sector Governance

Sadržaj

Sažetak

Svijet zavisi od povezanih digitalnih sistema i tehnologija u svakoj sferi svakodnevnog života kao što su trgovanje, finansije, komunikacije, itd.

Mi živimo u digitalnom svijetu gdje su lični podaci najvažniji. Važno je razumijeti da su lični podaci ranjiviji od bilo kada prije. Često čujemo o povredama podataka i kiber prijetnjama koje utiču na milione korisnika. Većina kompanija i institucija se bori da zaštiti svoje podatke od hakera i kiber kriminalaca, a i vi biste trebali isto tako da igrate ulogu u tome. Kiber bezbjednost se ne odnosi samo na organizacije, već i na lične kompjutere, mobilne telefone i tablet uređaje.

Kiber prijetnja ili prijetnja po kiber bezbjednost je maliciozna aktivnost osmišljena za krađu ili oštećivanje podataka ili narušavanje sistema jednog pojedinca ili cele organizacije.

U ovom Priručniku biće vam predstavljene različite kiber prijetnje. Kiber prijetnje uključuju široki spektar različitih napada, a najčešće su:

- Društveni inženjering
- Phishing napadi (pecanje – fišing)
- Preuzimanje podatka u prolazu (Drive by downloads)
- Napadi Čovjek-u-sredini (MITM napadi)
- Napadi sa odbačenim USB uređajem
- Malware – maliciozni softver

Kako bi zaštitili sebe i svoje sisteme, vi morate naučiti o ovim različitim vrstama kiber prijetnji i različitim načinima kako da ostanete bezbjedni na internetu.

Uobičajeni kiber napadi

Društveni inženjering

Društveni inženjering se koristi da se dovedu 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 prekršile bezbjednosne procedure i najbolje prakse i dobili neovlašćeni pristup sistemima ili dali osjetljive informacije.

Kiber kriminalci koriste pristup preko društvenih mreža da sakriju svoje prave identitete i motive, predstavljajući se kao osobe od povjerenja.

Korisnice se namame da kliknu maliciozne linkove ili dobiju fizički pristup kompjuteru putem prijevare.

Prijevare na internetu

Prijevare na internetu su različite metodologije dela prijevare koje vrše kiber kriminalci na internetu. Prijevara se može dogoditi putem phishing i-mejlova, društvenih medija, SMS poruka na vašem mobilnom telefonu, lažnih poziva za tehničku podršku i više. Glavni cilj ovih vrsta prijevara je od krađe kreditnih kartica, snimanja korisničkih akreditiva za prijavljivanje i lozinki, pa do krađe identiteta.[1]

Prijevare na internetu funkcionišu jer izgledaju realno i uhvate vas nespremne kada ih ne očekujete. Kiber kriminalci – prevaranti (skemeri) postaju sve pametniji i koriste nove tehnologije, proizvode itd. Saveti kako da vas ne ubede da im date vaše lične informacije ili detalje:

- Prijevare stvarno postoje, budite obazrivi.
- Ne otvarajte sumnjive tekstualne poruke, pop-up prozore i ne klikćite linkove ili priloge u i-mejlovima, već ih obrišite odmah.
- Uvijek budite svjesni s kim imate posla.
- Ne odgovarajte na telefonske pozive gdje druga strana zahtijeva vaše lične informacije ili informacije o kreditnoj kartici; spustite slušalicu.

Phishing napadi

Većina svih kiber napada počinje phishing (fišing – pecanje) i-mejlom. Phishing je vrsta društvenog inženjeringa u kome kiber kriminalci prevare žrtve da im daju osjetljive informacije ili instaliraju maliciozni softver.

I pored toga što tehničke mjere bezbjednosti postaju sve bolje, phishing ostaje jedan od najjeftinijih i najlakših načina da kiber kriminalci dobiju pristup osjetljivim i ličnim informacijama.

Ako korisnici kliknu na link, njihova bezbjednost može biti ugrožena i mogu postati žrtve krađe identiteta.

Klikanjem korisnici isto tako mogu da kompromituju svoje lične informacije, akreditive za najavu kao što su korisnička imena i lozinke i finansijske informacije kao što su brojevi kreditnih kartica).

Napadači često ovo postižu kroz maliciozne i-mejlove koji djeluju kao da su od izvora od povjerenja, ali

1 https://us.norton.com/internetsecurity-online-scams.html#

ponekad koriste i druge metode, koji su objašnjeni dole.

Kako funkcioniše phishing?

Većina phishing kampanja uključuje jedan od dva osnovna metoda:

1. **Maliciozni prilozi (attachment)**

   Maliciozni prilozi u i-mejlovima, koji uobičajeno imaju alarmantne naslove kao „FAKTURA“. Kada budu otvoreni, ovi prilozi instaliraju malware na mašini korisnika.

2. **Linkovi do malicioznih veb stranica**

   Maliciozni linkovi vode do veb stranica koje su često klonovi legitimnih veb stranica. Prelazak na veb stranice može dovesti do preuzimanja malicioznog softvera ili sama stranica za najavu može da sadrži skripte koje kradu akreditive [2].

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[3]. Spear phishing pokušaji ne dolaze od slučajnih napadača, već je vjerovatnije da se vrše od strane kiber kriminalaca koji žele da postignu finansijsku dobit ili prikupe druge vrijedne informacije.

Spear phishing napad funkcioniše tako da se i-mejl šalje od pouzdanog izvora, ali vodi do lažne veb stranice koja je prepuna malicioznog softvera. Ovi i-mejlovi najčešće koriste kreativne metode da privuku pažnju korisnika.

Spear phishing je daleko djelotvorniji od drugih phishing napada, ali zahtijeva da kiber kriminalci ulože vrijeme i resurse na istraživanju prije napada. Kiber kriminalci će biti utoliko uspješniji ako saznaju i nauče o njihovoj meti prije napada.

Whale Phishing/Whaling (kitolov)

Whale phishing (lov na kitove) je sličan spear phishing (ciljano ribarenje)-u, sa nekoliko važnih razlika. Dok je spear phishing uobičajeno usmjeren protiv članova određene grupe, whale phishing je usrijedsređen na konkretnu osobu – uobičajeno „najveću ribu“ u ciljanoj organizaciji ili pojedinca sa značajnim bogatstvom ili moći koju kiber kriminalci žele da iskoriste.

Vishing

Vishing ili „glasovni phishing“ uključuje manipulaciju ljudi preko telefona i njihovo zavođenje da otkriju osjetljive informacije. Kiber kriminalci pokušavaju da pokupe podatke žrtve i iskoriste ih za svoju ličnu korist, uobičajeno finansijsku.

Smishing

Termin smishing se odnosi na SMS phishing i uključuje tekstualnu poruku umjesto i-mejla. Mete uobičajeno

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

3 What is Phishing? (gfidigital.com)

dobiju tekstualnu poruku koja sadrži obmanu i koja ih prinuđuje da daju lične ili finansijske informacije. Kiber kriminalci se pretvaraju da su organ vlasti, banka ili druga kompanija, kako bi djelovali kao legitimni u svojim zahtijevima.

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 prijevare, prijevare sa poklonima i prijevare sa podrškom za klijente.

Preuzimanje podataka u „prolazu“ (drive-by downloads)

Napad sa preuzimanjem podataka u „prolazu“ je kiber napad gdje se preuzimaju maliciozne skripte na kompjutere ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim kiber napadima. To može da se dogodi na svakom uređaju, na bilo kojem operativnom sistemu. Uobičajeno se događa kada korisnik pređe na kompromitovanu veb stranicu i pregledava je.

Napadi čovjek-u-sredini (man in the middle (MITM))

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

Napad sa odbačenim USB

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

Najuobičajenija kiber prijetnja predstavljana ovim napadom je infekcija malicioznim softverom ili virusom. Infekcije preko USB diska mogu biti i namjerne i nenamjerne, u zavisnosti od malicioznog softvera.

Najpametnije je da organizacije prekinu vjerovati zastareloj USB tehnologiji i počnu koristiti moć bezbjednih digitalnih mreža koristeći „cloud“ sprijemanje podataka (na internetu).

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:

- **Botnet softver**
  Botnet softver je osmišljen da inficira veliki broj uređaja koji su povezani s internetom. Neke botnet (mreže botova) su sačinjene od velikog broja uređaja, od kojih svaka 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)**
  Ransomware je vrsta malicioznog softvera koji šifrira informacije korisnika i zahtijevaju plaćanje za ključ za dešifriranje kako bi se povratile informacije. Međutim, plaćanje otkupnine ne garantuje uvijek da ćete vratiti šifrirane podatke.
- **Spyware (špijunski softver)**
  Spyware je vrsta malicioznog softvera koji se koristi za nezakonito praćenje aktivnosti korisnika na računaru i prikupljanje ličnih podataka.

- **Trojanski virus**
  Trojanski virusi su vrsta malicioznog softvera koji deluju kao legitiman softver, ali vrše maliciozne aktivnosti kada budu izvršeni.
- **Virusi i crvi**
  Kompjuterski virus je maliciozni kod instaliran bez znanja korisnika. Virusi se mogu multiplicirati i širiti na druge računare time što se pripijaju na druge kompjuterske datoteke.

  Crvi su slični virusima jer se množe sami, ali ne moraju da se prikače na drugi program kako bi to uradili[4].

4 Types of Cyber Threat in 2019 | IT Governance USA

Kako ostati bezbjedan na internetu

Budite pažljivi sa svojim ličnim informacijama i digitalnim identitetom

Mi, kao pojedinci, možemo da se identifikujemo na različite načine. Naša imena, adrese, uzrast, profesija i više. − naši identiteti su sadržani u različitim oblicima na našim vozačkim dozvolama, karticama za osiguranje, izvodima iz matične knjige rođenih, karticama za posao ili školu, itd.

Kada razmislimo o svim različitim identifikovanjima koje koristimo u svakodnevnom životu, na internetu i van njega, da li možemo sa sigurnošću da kažemo koliko naših privatnih podataka se koristi bez naše saglasnosti i koliko od tih podataka se čuva na lokacijama koje su nama nepoznate i koje možda imaju pristup njima i koriste ih?

Nepotrebno je pominjati da ne smijete nikada dijeliti vaše lozinke, bankovne detalje ili lične informacije na internetu, ili sa drugom osobom. Informacije o vašim ličnim odnosima ili imena ljubimca mogu biti iskorišćene kao odgovori na vaša bezbjednosna pitanja ili mogu dati kiber kriminalcima ideju kada napadaju vaše lozinke.

Hakeri stalno traže nove načine za zloupotrebu ličnih podataka. Krađa identiteta iz evidencija i upad u podatke su velike prijetnje koje kompromituju ono što smo, jer identitet je naše osnovno sredstvo za interakciju:

- Vratite nazad kontrolu nad vašim podacima
- Nemojte koristiti vaše lične podatke kada kreirate profile na internetu
- Nemojte davati vaše lične podatke kako bi dobili popust u prodavnici
- Nemojte nepotrebno dijeliti vaše privatne informacije na društvenim medijima
- Uvijek provjerite kako će biti obrađeni vaši lični podaci kada koristite neku aplikaciju
- Provjerite da li je stranica bezbjedna pre nego što ostavite lične informacije

Ako je besplatna usluga koju koristite, budite ekstra obazrivi. Ako je besplatno, uobičajeno vi ste roba za prodaju (vaši podaci).

Kreirajte i koristite složene lozinke

Uvijek koristite složene lozinke. Ako vaša lozinka sadrži vidljive ili lake za pogađanje kombinacije brojeva (12345, 111111, 123321), popularna ženska imena (Nikolina, Džesika, Hana) ili samo nizove slova koji formiraju horizontalnu ili vertikalnu liniju na QWERTY tastaturi (asdfghjkl, qazwsx , 1qaz2wsx, itd.), trebaćete je promeniti SMJESTA! Iznenađuje što je najočiglednija lozinka – „lozinka“ –još uvijek vrlo popularna. Trebaće da je promijenite odmah (ili ako je vaša lozinka slična bilo čemu gore navedenom).

Ako vam je potrebna pomoć da smislite bezbjedne lozinke, evo nekoliko savjeta:

- Treba da ima najmanje 15 karaktera — duža, ako je moguće.
- Miješajte slova (velika i mala), brojeve i simbole.
- Ne koristite sekvencu brojeva ili slova, kao „qwerty“.
- Izbjegavajte zamjene kao „štreberski govor“ (gdje se slova mijenjaju brojevima ili simbolima sličnog izgleda).

Koristite različite lozinke za različite korisničke naloge. Na taj način, ako je jedan nalog kompromitovan, bar drugi neće biti pod rizikom.

Ako se ne možete sjetiti svojih lozinki, definitivno pokušajte s programom za upravljanje lozinkama. Lozinke je teško zapamtiti same po sebi, posebno ako vam je potrebna posebna lozinka za svaku stranicu. Savjetuje se korišćenje renomiranih programa za upravljanje lozinkama kao što su LastPass ili 1Password[5].

Dvaputa provjerite linkove prije nego što ih kliknete

Kada provjeravate vaš i-mejl ili posjećujete internet stranice, provjerite da li poznajete i vjerujete linku prije nego što kliknete na njega.

Jedan način da provjerite da li je link bezbjedan je da pređete mišem preko njega. To će vam pokazati prikaz celog linka u status polju vašeg internet pretraživača. Provjerite da li prikazani link odgovara veb stranici sa koje bi trebao da dolazi. Isto tako, možete da provjerite link do tačnog sajta ako pretražite njegovo ime.

Ako dobijete i-mejl koji od vas zahtijeva da se prijavite, bezbjednije je da ne kliknete link u i-mejlu i umijesto toga da odete na zvanični sajt i prijavite se tamo. Možete preći na zvanični sajt ili pretražujući njegovo ime ili, ako znate napamet, unošenjem adrese u URL polje vašeg pretraživača. Ovaj savjet uključuje i linkove koje su vam poslali prijatelji u aplikacijama za društvene mreže.

Ako i-mejl ili stranica zahtijeva od vas da se prijavite na vaš bankovni račun, uvijek možete da se javite i provjerite zahtijev.

Što se tiče preuzimanja podataka, trebaće da razmislite dvaputa, prije nego što to uradite. Određeni kiber kriminalci imaju za cilj inficiranje vašeg uređaja malicioznim softverom, time što će vas prevariti da preuzmete kompromitovane aplikacije i drugi softver. Prije nego što preuzmete podatke, provjerite stranicu sa koje skidate novu igru ili aplikaciju i jednostavno nemojte preuzimati ništa što djeluje sumnjivo.

Koristite bezbjedne WI-FI mreže

Nikada nemojte koristiti nebezbjednu, otključanu ili wi-fi mrežu bez lozinke, osim ako uistinu ne morate. Ako koristite takvu mrežu, nemojte se prijavljivati na nijedan korisnički nalog onlajn ili u aplikacijama i nemojte unositi lične ili finansijske informacije.

Kiber kriminalci često postave lažne wi-fi mreže kako bi namamili korisnike. Čim osoba poveže svoj telefon na wi-fi, kiber kriminalci u suštini vide sve što ta osoba radi.

Ako tražite wi-fi mrežu, najbjezbedniji način je da upitate zaposlenog kako se zove njihova wi-fi mreža.

Isto tako, osigurajte se da vaši uređaji nisu postavljeni da se automatski povezuju na wi-fi mreže, osim na poslu ili kod kuće. Namjestite uređaj da vas upita pre nego što se poveže. Na ovaj način ćete biti sigurni na šta se povezujete.

Koristite VPN

VPN, ili virtuelna privatna mreža, bezbjedno povezuje važe uređaje na internetu kako niko ne bi mogao da slijedi aktivnosti ili pristupi vašim informacijama preko internet veze. VPN može biti dobar način za bezbjednu

5 How to Stay Safe Online: Internet Safety Tips and Resources (reviews.org)

vezu kod kuće ili čak i kada ste napolju i koristite javnu wi-fi mrežu.

Jedini nedostatak povećanoj bezbjednosti koju daje VPN je da može usporiti vašu internet vezu. Ovo je često rezultat toga što VPN preusmjerava vaše podatke kroz drugi server kako bi osigurao vaše informacije.

Sve više ljudi radi od kuće u zadnje vrijeme, što kaže da mnogi od nas mogu postati meta kiber kriminalaca. Metod za održavanje zaštite je korišćenje VPN mreže i njeno ažuriranje po preporuci.

Kako bi dobili VPN, treba da odaberete davaoca VPN usluga, preuzeti i instalirati VPN i povezati se na server.

Koristite sajtove koji počinju sa https//

Ako želite da se prijavite na bilo koji sajt, provjerite da li adresa na vrhu vašeg pretraživača počinje sa **https://**, a ne sa **http://**. Možda ćete i vidjeti **simbol katanca** pored adrese sajta.

“S” znači “secure” - sigurno, i znači da sajt šifrira vaše podatke.

Internet kupovina znači da vi dajete vaše lične informacije, kao što su bankovni računi i informacije o kreditnim karticama. Uvijek provjerite dva puta da li je veb sajt na kome se nalazite bezbjedan, a potom popunite podatke.

Isključite vaš Bluetooth

Bluetooth komunikacije se mogu kompromitovati ili čak manipulisati. To ne znači da nikada ne treba da koristite Bluetooth, ali ako niste povezani sa drugim uređajem i aktivno ga koristite, najbolje je da ga isključite.

Koristite antivirus i antimalware softver

Ne preporučuje se pretraživanje interneta bez zaštite. Ukoliko to sebi ne možete priuštiti, bar nađite besplatni i jeftini antivirus softver na internetu. Odaberite pažljivo i mudro.

Plaćanje male svote za softver vrijedi kako bi izbegli glavobolju od suočavanja sa malware-om ili ransomware-om. Ako već imate antivirus ili antimalware softver, ažurirajte ga kontinuirano.

Neki preporučeni antivirus i antimalware softveri uključuju sljedeće:

- Microsoft Defender (dolazi sa Windows, ali ga morate uključiti i ažurirati)
- Norton AntiVirus Plus
- Bitdefender
- AVG
- Malwarebytes
- Avast
- SpyBot Search and Destroy

Napravite bekap (rezervne kopije) svojih podataka

Naši kompjuteri i drugi uređaju su dom svih naših važnih podataka. Ali, ako je taj uređaj kompromitovan, oštećen, izgubljen ili ukraden, vaši važni podaci mogu biti izgubljeni. Bez razlike da li se radi o hardverskom defektu, krađe, prirodne katastrofe ili infekcije vašeg uređaja sa malicioznim softverom, povratak podataka

može biti skup ili nemoguć.

Bekap je digitalna kopija vaših najvažnijih informacija.

Kada radite rezervne kopije podataka, kopije vaših datoteka (pr. fotografije, dokumente, videa itd.) se snimaju na spoljašnji uređaj za čuvanje podataka ili na onlajn servis kao što je cloud.

Ako imate bekap to znači da možete vratiti svoje podatke ako nešto krene po zlu. To je preventivna mjera kako bi vaši podaci bili dostupni u slučaju da se nešto dogodi vašem kompjuteru. Savjetujemo vam da redovno vršite bekap vaših datoteka[6].

Postoji mnogo načina za bekap vaših podataka od korišćenja eksternih diskova do spremanje podataka na udaljenom serveru preko interneta. Ovo su prednosti i nedostaci svakog metoda:

- **Bekap (rezervna kopija) eksternog diska**: kako bi izvršili bekap podataka na eksterni hard disk, možete iskoristiti ugrađene bekap opcije kompjutera. S vrijemena na vrijeme povježite disk sa računarom i upotrebite alat za bekap, ili ostavite disk uključen i bekap će se izvršiti automatski.
  Pozitivne strane: bekap je brz i jeftin.
  Negativne strane: eksterni disk može biti izgubljen ili ukraden.
- **Bekap vaših podataka na vaš računar**: ovo su neka uputstva o različitim načinima za bekap vaših podataka na Mac-u, iOS uređajima ili PC:
  * iCloud (iOS uređaji)
  * Time Machine (Mac)
  * Windows 8.1 (PC)
  * Windows 10 (PC)

  Pozitivne strane: bekap je brz i jeftin.
  Negativne strane: bekap može biti izgubljen ili ukraden.
- **Koristite uslugu za čuvanje podataka na internetu (cloud)**: umijesto da čuvate vaše podatke na hard disku vašeg računara, vi ih možete čuvati i na servisu kao Dropbox, Google Drive, Microsoft OneDrive, ili sličnom servisu za čuvanje podataka na internetu, cloud. Oni će se onda automatski sinhronizovati sa vašim onlajn korisničkim nalozima i vašim drugim uređajima. Ako se vaš hard disk pokvari ili vam ukradu računar, još uvijek će te imati kopije datoteka koje se čuvaju onlajn i na vašim drugim uređajima.
  Pozitivne strane: ovaj je metod brz i lak i u mnogim slučajevima besplatan, a zbog toga što je onlajn, štiti vas od svih vrsta gubitka podataka.
  Negativne strane: Većina cloud servisa nudi samo nekoliko besplatnih gigabajta podataka, tako da ovo funkcioniše samo ako imate mali broj datoteka koje želite staviti na bekap ili ako ste voljni da platite za dopunski prostor[7].

Na kraju, treba da razmislite o tome gdje se nalaze vaši važni podaci i da provjerite/testirate da imate nekoliko kopija u svakom trenutku. Idealno, te kopije moraju biti na nekoliko fizičkih lokacija. Sve dok mislite o tome, šta ako se nešto loše dogodi uređaju, vi biste morali biti isprijed većine ljudi.

6 Back Up and Restore - Microsoft Windows | Cyber.gov.au

7 Best ways to backup your computer. • Nerds in a Flash

Zaključak

Sve veće prijetnje se otkrivaju u novim tehnologijama kao što su društveni mediji, cloud kompjuterski radovi, tehnologija pametnih telefona ili kritične infrastrukture, a te prijetnje često zloupotrebljavaju njihove jedinstvene karakteristike.

Umijesto pokušaja za riješavanje problema na internetu i u kompjuterskim sistemima, bolji je pristup da na vaš uređaj primjenite neke od savjeta iz ovog Priručnika i da sljedite preporučeno ponašanje kako bi ostali bezbjedni na internetu.

Reference

Online Scams, Avoiding Internet Scams, Norton

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

What is Phishing?, gfidigital.com

Types of Cyber Threat in 2019, IT Governance USA

What Is Cyberbullying, StopBullying.gov

Catherine McNally, How to Stay Safe Online: Internet Safety Tips and Resources, reviews.org

Back Up and Restore - Microsoft Windows, Cyber.gov.au

Best ways to back up your computer, Nerds in a Flash

Aneks: Kontrolna lista dobrih praksi

UOBIČAJENI KIBER NAPADI	
DRUŠTVENI INŽENJERING	- Društveni inženjering se koristi da se dovedu u zabludu ili manipuliraju mete, kako bi dobili informacije ili pristup njihovim računarima. Ove vrste napada se pouzdaju u ljudsku interakciju i uobičajeno uključuju manipulaciju korisnika kako bi prekršili bezbjednosne procedure i najbolje prakse i dobili neovlašćeni pristup sistemima ili dali osjetljive informacije.
PHISHING NAPADI	- Phishing je vrsta napada u kome kiber kriminalci prevare žrtve da im daju osjetljive informacije ili instaliraju maliciozni softver: • Spear Phishing (ciljano pecanje) – maliciozni i-mejl koji cilja na određenu organizaciju ili osobu sa ciljem dobijanja pristupa osjetljivim informacijama. • Whale Phishing / Whaling (kitolov) – fokusiran je na konkretnu osobu – uobičajeno „najveću ribu“ u ciljanoj organizaciji ili pojedinca sa značajnim bogatstvom ili moći koju kiber kriminalci žele da iskoriste. • Vishing – je pokušaj za dobijanje podataka žrtve i njihovo korišćenje za finansijsku dobit, a ljudi se prevare preko telefona. • Smishing – je tekstualna SMS poruka koja sadrži obmanu da privuče primače da daju lične ili finansijske informacije (akreditivi korisničkih naloga, brojeve kreditnih kartica, itd...), gdje se kiber kriminalci pretvaraju da su organ vlasti, banka ili druga kompanija kako bi djelovali legitimni u svojim zahtijevima.
PREUZIMANJE PODATAKA U „PROLAZU“	- Napad sa preuzimanjem podataka u „prolazu“ je kiber napad gdje se preuzimaju maliciozne skripte na računare ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim kiber prijetnjama i događa se kada korisnik pređe na kompromitovane veb stranice i kada ih pregledava.
MITM (čovjek u sredini) NAPADI	- MITM napad se događa kada se kiber kriminalac tajno ubaci između dva uređaja, ili između uređaja i nebezbjedne wi-fi mreže, kako bi presretao komunikacije koje potom on može da čita i/ili menja, što može da dovede do toga da korisnik nenamjerno pošalje kiber kriminalcu akreditive ili druge informacije.
NAPAD SA ODBAČENIM USB	- Napad sa odbačenim USB se događa kada se na računaru uključi USB uređaj koji sadrži maliciozni kod.
MALICIOZNI SOFTVER - MALWARE	- **Botnet softver** – on inficira veliki broj uređaja koji su povezani na internet. - **Ransomware napad (napad sa softverom za otkupninu)** – on šifrira informacije korisnika i zahtijevaju plaćanje za ključ za dešifriranje, kako bi se informacije povratile. - **Spyware** - je vrsta malicioznog softvera koji se koristi za nezakonito praćenje aktivnosti korisnika na računaru i prikupljanje ličnih podataka. - **Trojanski virus** – je vrsta malicioznog softvera koji djeluje kao legitiman softver, ali vrši maliciozne aktivnosti kada budu izvršeni. - **Virusi i crvi** – - Virus je maliciozni kod instaliran bez znanja korisnika. Virusi se mogu množiti i širiti na druge računare time što se pripijaju na druge kompjuterske datoteke. - Crvi su slični virusima jer se množe sami, ali ne moraju da se prikače na drugi program kako bi to uradili.

KAKO OSTATI BEZBJEDAN NA INTERNETU	
NEMOJTE DJELITI SVOJE LIČNE INFORMACIJE	- **Nikada ne smijete ni sa kim ili onlajn deliti informacije o:** • vašim lozinkama • bankovnim detaljima • ličnim informacijama - **Vratite nazad kontrolu nad vašim podacima** - **Nemojte koristiti vaše lične podatke kada kreirate profile na internetu** - **Nemojte davati vaše lične podatke kako bi dobili popust u prodavnici** - **Nemojte nepotrebno djeliti vaše privatne informacije na društvenim medijima** - **Uvijek provjerite kako će biti obrađeni vaši lični podaci kada koristite neku aplikaciju** - **Provjerite da li je sajt bezbjedan prije nego što ostavite lične informacije**
KREIRAJTE I KORISTITE SLOŽENE LOZINKE	- **Uvijek treba da koristite složene lozinke:** • Treba da ima najmanje 15 karaktera — duža, ako je moguće. • Miješajte slova (velika i mala), brojeve i simbole. • Ne koristite sekvencu brojeva ili slova, kao „qwerty“. • Izbjegavajte zamene kao „štreberski govor“ (gdje se slova mijenjaju brojevima ili simbolima sličnog izgleda). - **Koristite različite lozinke za različite korisničke naloge** - **Probajte softver za upravljanje lozinkama**
DVAPUTA PROVJERITE LINKOVE PRIJE KLIKTANJA	- **Kada provjeravate vaš i-mejl ili posjećujete internet stranice, provjerite da li poznajete i vjerujete linku prije nego što kliknete na njega**: • Pređite mišem preko linka i provjerite da li ste dobili prikaz celog linka u status polju vašeg internet pretraživača. • Ako dobijete i-mejl koji od vas zahtijeva da se prijavite, bezbjednije je da ne kliknete link u i-mejlu i umjesto toga da odete na zvanični sajt i prijavite se tamo. • Ako i-mejl ili sajt zahtijeva od vas da se prijavite na vaš bankovni račun, uvijek možete da se javite i provjerite zahtijev. • Prije nego što preuzmete podatke, provjerite sajt sa koga skidate novu igru ili aplikaciju i jednostavno nemojte preuzimati ništa što djeluje sumnjivo.
KORISTITE BEZBJEDNE WI-FI MREŽE	- Nikada nemojte koristiti nebezbjednu, otključanu ili wi-fi mrežu bez lozinke, osim ako uistinu ne morate. - Dok ste na wi-fi mreži nemojte se prijavljivati na nijedan korisnički nalog onlajn ili u aplikacijama i nemojte unositi lične ili finansijske informacije. - Osigurajte se da vaši uređaji nisu postavljeni da se automatski povezuju na wi-fi mreže.
KORISTITE VPN	- VPN, ili virtuelna privatna mreža, bezbjedno povezuje važe uređaje na internetu kako niko ne bi mogao da sljedi aktivnosti ili pristupi vašim informacijama preko internet veze. - Kako bi dobili VPN, treba da odaberete davaoca VPN usluga, preuzeti i instalirati VPN i povezati se na server.
AKO POČINJE SA HTTPS, BEZBJEDNO JE	- Ako želite da se prijavite na bilo koji sajt, provjerite da li adresa na vrhu vašeg pretraživača počinje sa https://, a ne sa http://. - Možda ćete i videti simbol katanca pored adrese sajta.
ISKLJUČITE VAŠ BLUETOOTH	- Ako ponekad koristite Bluetooth, isključite ga kad ga aktivno ne koristite, kako bi izbegli njegovo kompromitovanje ili manipulaciju.
KORISTITE ANTIVIRUS I ANTIMALWARE SOFTVER	- Ukoliko to sebi ne možete priuštiti, bar nađite besplatni i jeftini antivirus softver na internetu kako bi izbjegli suočavanje sa malware-om ili ransomware-om.
NAPRAVITE BEKAP (REZERVNE KOPIJE) VAŠIH PODATAKA	- Kada radite rezervne kopije podataka, kopije vaših datoteka (pr. fotografije, dokumenta, videa itd.) se snimaju na spoljašnji uređaj za čuvanje podataka ili na onlajn servisu kao što je cloud. - Postoji mnogo načina za bekap vaših podataka • Bekap eksternog diska • Bekap podataka na vašem računaru • Koristite uslugu za čuvanje podataka na internetu (cloud)

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