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

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

Sadržaj

Sažetak

Svet zavisi od povezanih digitalnih sistema i tehnologija u svakom aspektu svakodnevnog života kao što su trgovanje, finansije, komunikacija, itd.

Mi živimo u digitalnom svetu gde su lični podaci najvažniji. Važno je razumeti da su lični podaci ranjiviji od bilo kada pre. Često čujemo o upadima u podatke i sajber pretnjama koje utiču na milione korisnika. Većina kompanija i institucija se bori da zaštiti svoje podatke od hakera i sajber kriminalaca, a i vi trebate isto tako da igrate ulogu u tome. Sajber bezbednost se ne odnosi samo na organizacije, već i na lične kompjutere, mobilne telefone i tablet uređaje.

Sajber pretnja ili pretnja po sajber bezbednost je maliciozna aktivnost osmišljena za krađu ili oštećivanje podataka ili narušavanje sistema jednog pojedinca ili cele organizacije.

U ovom Priručniku biće vam predstavljene različite sajber pretnje. Sajber pretnje uključuju široki spektar različitih napada, a najčešće su:

- Društveni inženjering
- Phishing napadi (pecanje – fišing)
- Preuzimanje podatka u prolazu (Drive by downloads)
- Napadi Čovek-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 sajber pretnji i različitim načinima kako da ostanete bezbedni na internetu.

Uobičajeni sajber 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 prekršili bezbednosne procedure i najbolje prakse i dobili neovlašćeni pristup sistemima ili dali osetljive informacije.

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

Ovo se vrši varanjem korisnika da kliknu maliciozne linkove ili dobijanjem fizičkog pristupa kompjuteru putem prevare.

Prevare na internetu

Prevare na internetu su različite metodologije dela prevare koje vrše sajber kriminalci na internetu. Prevara se može dogoditi putem phishing i-mejlova, društvenih medija, SMS poruka na vašem mobilnom telefonu, lažnih poziva za tehničku podršku i više. Glavni ciljevi ovih vrsta prevara su od krađe kreditnih kartica, snimanja korisničkih akreditiva za prijavljivanje i lozinki, pa do krađe identiteta.[1]

Prevare na internetu funkcionišu jer izgledaju realno i uhvate vas nespremne kada ih ne očekujete. Sajber 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:

- Prevare stvarno postoje, budite obazrivi.
- Ne otvarajte sumnjive tekstualne poruke, pop-up prozore i ne klikćite linkove ili privitke u i-mejlovima, već ih obrišite odmah.
- Uvek budite svesni s kim imate posla.
- Ne odgovarajte na telefonske pozive koji se tiču vaših ličnih informacija ili informacija o kreditnoj kartici; spustite slušalicu.

Phishing napadi

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

I pored toga što tehničke mere bezbednosti postaju sve bolje, phishing ostaje jedan od najjeftinijih i najlakših načina da sajber kriminalci dobiju pristup osetljivim i ličnim informacijama.

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

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

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

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

Kako funkcioniše phishing?

Većina phishing kampanja uključuje jedan od dva osnovna metoda:

1. **Maliciozni privitci (attachment)**

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

2. **Linkovi do malicioznih veb sajtova**

   Maliciozni linkovi vode do 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[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 osetljivim informacijama[3]. Spear phishing pokušaji se ne vrše od slučajnih napadača, već je verovatnije da se vrše od sajber kriminalaca koji žele da postignu finansijsku dobit ili prikupe druge vredne informacije.

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

Spear phishing je daleko efektivniji od drugih phishing napada, ali zahteva od sajber kriminalaca da potroše vreme i resurse na istraživanju pre napada. Sajber kriminalci će biti utoliko uspešniji ako nauče o njihovoj meti pre napada.

Whale Phishing/Whaling (kitolov)

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

Vishing

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

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

3 What is Phishing? (gfidigital.com)

Smishing

Termin smishing se odnosi na SMS phishing i uključuje tekstualnu poruku umesto i-mejla. Mete uobičajeno dobiju tekstualnu poruku koja sadrži obmanu i koja ih prinuđuje da daju lične ili finansijske informacije. Sajber kriminalci se pretvaraju da su organ vlasti, banka ili druga kompanija kako bi delovali legitimni u svojim zahtevima.

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

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

Napad sa preuzimanjem podataka u „prolazu“ je sajber napad gde se preuzimaju 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. Uobičajeno se događa kada korisnik pređe na i pretražuje kompromitovani veb sajt.

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

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

Napad sa odbačenim USB

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

Najuobičajenija sajber pretnja predstavljana ovim napadom je infekcija malicioznim softverom ili virusom. Infekcije preko USB diska mogu biti i namerne i nenamerne, ovisno o dotičnom malicioznom softveru.

Najpametnije je da organizacije prekinu verovati zastareloj USB tehnologiji i počnu koristiti moć bezbednih digitalnih mreža koristeći cloud spremanje 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 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)**

  Ransomware je vrsta malicioznog softvera koji šifrira informacije korisnika i zahteva plaćanje za ključ za dešifriranje, kako bi se povratile informacije. Međutim, plaćanje otkupnine ne garantuje uvek da ćete vratiti šifrirane podatke.

- **Spyware (špijunski softver)**

  Spyware je vrsta malicioznog softvera koji se koristi za nezakonito praćenje aktivnosti korisnika na kompjuteru 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 množiti i širiti na druge kompjutere 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 bezbedan 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 identifikacijama 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 nikada ne trebate deliti 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 bezbednosna pitanja ili mogu dati sajber 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 pretnje koje kompromituju to 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 deliti vaše privatne informacije na društvenim medijima
- Uvek proverite kako će biti obrađeni vaši lični podaci kada koristite neku aplikaciju
- Proverite da li je sajt bezbedan pre nego što ostavite lične informacije

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

Kreirajte i koristite složene lozinke

Uvek trebate koristiti složene lozinke. Ako vaša lozinka sadrži očigledne 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.), trebate je promeniti ODMAH! Iznenađuje što je najočiglednija lozinka – „password“ – još uvek vrlo popularna. I nju trebate promeniti odmah (ili ako je vaša lozinka slična bilo čemu gore navedenom).

Ako vam je potrebna pomoć da smislite bezbedne lozinke, evo nekoliko saveta:

- Treba da bude najmanje 15 karaktera — duža, ako je moguće.
- Pomešajte slova (velika i mala), brojeve i simbole.
- Ne koristite sekvencu brojeva ili slova, kao „qwerty“.
- Izbegavajte zamene kao „štreberski govor“ (gde se slova menjaju 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 ne možete da setite vaših lozinki, definitivno trebate probati program za upravljanje lozinkama. Lozinke je teško zapamtiti same po sebi, osobito ako vam je potrebna posebna lozinka za svaki sajt. Savetuje se korišćenje renomiranih programa za upravljanje lozinkama kao što su LastPass ili 1Password[5].

Dvaput proverite linkove pre kliktanja

Kada proveravate vaš i-mejl ili posećujete internet strane, proverite da li poznajete i verujete linku pre nego što kliknete na njega.

Jedan način da proverite da li je link bezbedan je da pređete mišem preko njega. To će vam pokazati prikaz celog linka u status polju vašeg internet pretraživača. Proverite da vidite da li prikazani link odgovara veb sajtu sa kojeg bi trebao da dolazi. Isto tako, možete da proverite link do tačnog sajta ako pretražite njegovo ime.

Ako dobijete i-mejl koji od vas zahteva da se prijavite, bezbednije je da ne kliknete link u i-mejlu i umesto 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 savet uključuje i linkove koje su vam poslali prijatelji u aplikacijama za društvene mreže.

Ako i-mejl ili sajt zahteva od vas da se prijavite na vaš bankovni račun, uvek možete da se javite i proverite zahtev.

Što se tiče preuzimanja podataka, trebate razmisliti dvaput pre nego što to uradite. Određeni sajber kriminalcu imaju za cilj da inficiraju vaš uređaj malicioznim softverom time što će vas prevariti da preuzmete kompromitovane aplikacije i drugi softver. Pre nego što preuzmete podatke, proverite sajt sa koga skidate novu igru ili aplikaciju i jednostavno nemojte preuzimati ništa što deluje sumnjivo.

Koristite bezbedne WI-FI mreže

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

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

Ako tražite wi-fi mrežu, najbezbedniji način je da pitate 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. Namestite uređaj da vas pita pre nego što se poveže. Na ovaj način ćete biti sigurni na šta se povezujete.

Koristite VPN

VPN, ili virtuelna privatna mreža, bezbedno povezuje važe uređaje na internet kako niko ne bi mogao da

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

sledi aktivnosti ili pristupi vašim informacijama preko internet veze. VPN može biti dobar način za bezbednu vezu kod kuće ili čak i kada ste vani i koristite javnu wi-fi mrežu.

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

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

Kako bi dobili VPN, trebate odabrati 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, proverite da li adresa na vrhu vašeg pretraživača počinje sa **https://,** a ne sa **http://**. Možda ćete i videti **simbol katanca** pored adrese sajta.

“S” znači “secure” - bezbedno 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. Uvek proverite dva puta da li je veb sajt na kome se nalazite bezbedan, a potom popunite podatke.

Isključite vaš Bluetooth

Bluetooth komunikacije se mogu kompromitirati ili čak manipulirati. To ne znači da nikada ne trebate koristiti 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. Ako si ga ne možete priuštiti, bar nađite besplatni i jeftini antivirus softver na internetu. Odaberite pažljivo i mudro.

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

Neki preporučeni antivirus i antimalware softveri uključuju sledeće:

- 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) vaših 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 pravite rezervne kopije podataka, kopije vaših datoteka (pr. fotografije, dokumenti, 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 mera kako bi vaši podaci bili dostupni u slučaju da se nešto dogodi vašem kompjuteru. Savetujemo vas da redovno vršite bekap vaših datoteka[6].

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

- **Bekap na eksterni disk**: kako bi izvršili bekap podataka na eksterni hard disk, možete iskoristiti ugrađene bekap opcije kompjutera. S vremena na vreme povežite disk na vaš kompjuter i upotrebite alat za bekap, ili ostavite disk uključen i bekap će se raditi automatski.
  Pozitivne strane: bekap je brz i jeftin.
  Negativne strane: eksterni disk može biti izgubljen ili ukraden.
- **Bekap vaših podataka na vaš kompjuter**: ovo su neka uputstva o različitim načinima za bekap vaših podataka na Mac, 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)**: umesto da čuvate vaše podatke na hard disku vašeg kompjutera, vi ih možete čuvati i na servisu kao Dropbox, Google Drive, Microsoft OneDrive, ili sličnoj usluzi 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 kompjuter, još uvek 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, trebati razmisliti o tome gde se nalaze vaši važni podaci i da proverite/testirate da imate nekoliko kopija u svakom trenutku. Idealno, te kopije trebaju biti na nekoliko fizičkih lokacija. Sve dok mislite o tome šta ako se nešto loše dogodi uređaju, trebali bi biti ispred 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 pretnje se otkrivaju u novim tehnologijama kao što su društveni mediji, cloud kompjuterski rad, tehnologija pametnih telefona ili kritične infrastrukture, a te pretnje često zloupotrebljavaju njihove jedinstvene karakteristike.

Umesto pokušaja za rešavanje problema na internetu i u kompjuterskim sistemima, bolji je pristup da na vaš uređaj primenite neke od saveta iz ovog Priručnika i da sledite preporučeno ponašanje kako bi ostali bezbedni 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: Spisak dobrih praksi

UOBIČAJENI SAJBER 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 prekršili bezbednosne procedure i najbolje prakse i dobili neovlašćeni pristup sistemima ili dali osetljive informacije.
PHISHING NAPADI	- Phishing je vrsta napada u kome sajber kriminalci prevare žrtve da im daju osetljive informacije ili instaliraju maliciozni softver: • Spear Phishing (ciljano pecanje) – maliciozni i-mejl koji cilja na određenu organizaciju ili osobu sa ciljem dobijanja pristupa osetljivim informacijama. • Whale Phishing / Whaling (kitolov) – usredsređen je na konkretnu osobu – uobičajeno „najveću ribu“ u ciljanoj organizaciji ili pojedinca sa značajnim bogatstvom ili moći koju sajber 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...), gde se sajber kriminalci pretvaraju da su organ vlasti, banka ili druga kompanija kako bi delovali legitimni u svojim zahtevima.
PREUZIMANJE PODATAKA U „PROLAZU“	- Napad sa preuzimanjem podataka u „prolazu“ je sajber napad gde se preuzimaju maliciozne skripte na kompjutere ili druge uređaje bez znanja korisnika, čime se korisnik izlaže različitim sajber pretnjama i događa se kada korisnik pređe na i pretražuje kompromitovane veb sajtove.
MITM (čovek u sredini) NAPADI	- MITM napad se događa kada se sajber kriminalac tajno ubaci između dva uređaja, ili između uređaja i nebezbedne wi-fi mreže, kako bi presretao komunikacije koje potom on može da čita i/ili menja, što može da dovede do toga da korisnik nenamerno pošalje sajber kriminalcu akreditive ili druge informacije.
NAPAD SA ODBAČENIM USB	- Napad sa odbačenim USB se događa kada se uključi na kompjuter 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 zahtevaju plaćanje za ključ za dešifriranje, kako bi se povratile informacije. - **Spyware** - je vrsta malicioznog softvera koji se koristi za nezakonito praćenje aktivnosti korisnika na kompjuteru i prikupljanje ličnih podataka. - **Trojanski virus** – je vrsta malicioznog softvera koji deluje kao legitiman softver, ali vrši maliciozne aktivnosti kada budu izvršen. - **Virusi i crvi** – - Virus je maliciozni kod instaliran bez znanja korisnika. Virusi se mogu množiti i širiti na druge kompjutere 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 BEZBEDAN NA INTERNETU	
NEMOJTE DELITI SVOJE LIČNE INFORMACIJE	- **Nikada ne trebate ni sa kim ili onlajn deliti informacije o:** • vašim lozinkama • bankovne detalje • lične informacije - **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 deliti vaše privatne informacije na društvenim medijima** - **Uvek proverite kako će biti obrađeni vaši lični podaci kada koristite neku aplikaciju:** • Proverite da li je sajt bezbedan pre nego što ostavite lične informacije
KREIRAJTE I KORISTITE SLOŽENE LOZINKE	- **Uvek trebate koristiti složene lozinke:** • Treba da bude najmanje 15 karaktera — duža, ako je moguće. • Pomešajte slova (velika i mala), brojeve i simbole. • Ne koristite sekvencu brojeva ili slova, kao „qwerty“. • Izbegavajte zamene kao „štreberski govor“ (gde se slova menjaju brojevima ili simbolima sličnog izgleda). - **Koristite različite lozinke za različite korisničke naloge** - **Probajte softver za upravljanje lozinkama**
DVAPUT PROVERITE LINKOVE PRE KLIKTANJA	- **Kada proveravate vaš i-mejl ili posećujete internet strane, proverite da li poznajete i verujete linku pre nego što kliknete na njega**: • Pređite mišem preko linka i proverite da li ste dobili prikaz celog linka u status polju vašeg internet pretraživača. • Ako dobijete i-mejl koji od vas zahteva da se prijavite, bezbednije je da ne kliknete link u i-mejlu i umesto toga da odete na zvanični sajt i prijavite se tamo. • Ako i-mejl ili sajt zahteva od vas da se prijavite na vaš bankovni račun, uvek možete da se javite i proverite zahtev. • Pre nego što preuzmete podatke, proverite sajt sa koga skidate novu igru ili aplikaciju i jednostavno nemojte preuzimati ništa što deluje sumnjivo.
KORISTITE BEZBEDNE WI-FI MREŽE	- Nikada ne trebate koristiti nebezbednu, otključanu ili wi-fi mrežu bez lozinke, osim ako stvarno 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, bezbedno povezuje važe uređaje na internet kako niko ne bi mogao da sledi aktivnosti ili pristupi vašim informacijama preko internet veze. - Kako bi dobili VPN, trebate odabrati davaoca VPN usluga, preuzeti i instalirati VPN i povezati se na server.
AKO POČINJE SA HTTPS, BEZBEDNO JE	- Ako želite da se prijavite na bilo koji sajt, proverite 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 kompromitiranje ili manipulaciju.
KORISTITE ANTIVIRUS I ANTIMALWARE SOFTVER	- Ako si ga ne možete priuštiti, bar nađite besplatni i jeftini antivirus softver na internetu kako bi izbegli suočavanje sa malware ili ransomware.
NAPRAVITE BEKAP (REZERVNE KOPIJE) VAŠIH PODATAKA	- Kada pravite rezervne kopije podataka, kopije vaših datoteka (pr. fotografije, dokumenti, videa itd.) se snimaju na spoljašnji uređaj za čuvanje podataka ili na onlajn servis kao što je cloud. - Postoji mnogo načina za bekap vaših podataka • Bekap na eksterni disk • Bekap podataka na vašem kompjuteru - 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