USAID
OD AMERIČKOG NARODA

Digital Serbia Initiative

PREDUZMI
IDEJU
smisli. pokreni. ostvari.

Uvod u sajber bezbednost

Abstract

A1

www.preduzmi.rs

SADRŽAJ

Izrada ovog vodiča omogućena je uz podršku američkog naroda putem Američke agencije za međunarodni razvoj (USAID) Sadržaj ovog vodiča je isključivo odgovornost Inicijative „Digitalna Srbija“ i ne predstavlja nužno stavove USAID-a ili Vlade SAD.

Značaj sajber bezbednosti za naš svakodnevni život i poslovanje

Sajber bezbednost igra ključnu ulogu u našem svakodnevnom životu i poslovanju. Računarski sistemi i mreže su neizostavni deo našeg društva i koristimo ih za različite svrhe, poput komunikacije, bankarstva, kupovine, zabave i društvenog života. Međutim, korišćenje računarskih sistema i mreža takođe nosi rizik od sajber napada i krađe ličnih podataka, što može imati ozbiljne posledice po našu bezbednost, finansijsku stabilnost i privatnost.

U poslovanju, sajber bezbednost je još važnija, jer organizacije često obrađuju osetljive informacije o klijentima i partnerima, kao i finansijske informacije i intelektualno vlasništvo.

Sajber bezbednost jedne organizacije je snažna onoliko koliko i njena najslabija karika. Potrebna je samo jedna slaba tačka da se izazove domino efekat koji napadačima daje pristup osetljivim internim resursima.

Organizacije svakodnevno upravljaju velikim brojem zaposlenih koji imaju pristup velikom broju internih resursa. Pod interne resurse možemo svrstati sve od poslovnih naloga elektronske pošte, do poverljivih finansijskih podataka i ugovora sa kojim jedna organizacija raspolaže. Bez odgovarajuće zaštite, ovi resursi mogu biti kompromitovani, a podaci koje sadrže izloženi krađi ili zloupotrebi, što sa sobom povlači lančanu reakciju koja rezultuje u:

- Reputacionoj šteti po kompaniju u očima klijenata i strateških partnera;
- Finansijskoj šteti u vidu plaćanja zakonskih kazni zbog gubitka osetljivih i poverljivih informacija;
- Finansijskom trošku saniranja posledica sajber incidenta.
- Potencijalnim tužbama vlasnika ukradenih podataka;

Uz to, sajber napadi su postali sve sofisticiraniji i učestaliji. Sajber kriminal je prerastao u ogromnu industriju, a napadi o kojima slušamo u vestima samo su vrh ledenog brega u poređenju sa manje spektakularnim incidentima koji svakodnevno izazivaju štetu u iznosima od nekoliko desetina do nekoliko miliona dolara.

Zato je neophodno preduzeti preventivne mere – kako na ličnom, tako i na poslovnom planu. To podrazumeva upotrebu jake lozinke, redovno ažuriranje softvera, instaliranje antivirusa i ostalih bezbednosnih alata, kao i pridržavanje najboljih praksi za zaštitu ličnih i poslovnih informacija.

Definicija sajber bezbednosti

Sajber bezbednost (cyber security) je oblast koja se bavi zaštitom računarskih sistema, mreža i podataka od neovlašćenog pristupa, oštećenja ili krađe. Odnosi se na primenu tehnologije, procesa i politika kako bi se obezbedio integritet, poverljivost i dostupnost informacija i resursa koji su kritični za poslovanje organizacije ili pojedinca.

Sajber bezbednost je štit čiji je zadatak da odgovori na različite vrste pretnji koje mogu doći iz virtualnog sveta, kao što su razni zlonamerni softveri (malware), phishing, ransomware, kao i neovlašćeni pristupi i krađe podataka.

Ove pretnje mogu biti izazvane od spoljnih napadača, alii od internih izvora, poput zaposlenih koji mogu biti neoprezni u svojim aktivnostima ili imati loše namere.

Da bi obezbedili bezbednost poverljivih podataka, sajber stručnjaci koriste različite tehnologije i procese, uključujući šifrovanje, firewall-ove, antivirusne programe, softverske zakrpe, autentifikaciju i autorizaciju korisnika, kao i sigurnosne politike i procedure koje se primenjuju na organizacijskom nivou.

Jednako važna je i edukacija o bezbednom korišćenju računarskih sistema i mreža, pa je zato je fokus ovog vodiča upravo na podizanju svesti korisnika računarskih sistema, tačnije vas koji ovo čitate.

Zapamtite - najbolji način da se zaštitte od pretnji koje vrebaju na internetu jeste da ih temeljno razumete i da usvojite pravila ponašanja koja će vam pomoći da prepoznate sajber napad i reagujete.

Sajber kriminalci i njihov način rada

Sajber bezbednost kao praksa ne bi postojala bez svojih glavnih antagonista – sajber kriminalaca. Najkraća definicija bi okarakterisala sajber kriminalce kao ljude koji koriste tehnologiju u kriminalne svrhe. Sajber kriminalci raspolažu različitim tehnikama i alata za hakovanje računara, krađu podataka, i izradu zlonamernih softvera. Njihova motivacija može biti finansijska, lična, politička ili ideološka, a organizacija im varira od pojedinačnih aktera do strogo-hijerarhizovanih grupa.

Ova kratka uvertira će vam poslužiti da prepoznate svog protivnika, i što je još važnije – da ga ne potcenjujete. U sledećem poglavlju fokusiraćemo se na softverska sredstva kojim sajber kriminalci raspolažu, kao i na metode kojima se služe kako bi postigli svoje ciljeve.

Ali, pre nego što nastavimo, hajde da prođemo kroz nekoliko uobičajenih zabluda vezanih za sajber kriminal:

Zabluda #1: Sajber kriminalce ne zanimaju moji podaci.

U neku ruku, ovo može biti tačno, ali vas to ne čini bezbednim – naprotiv. Sajber kriminal je rasprostranjen koliko i sam internet i predstavlja unosnu industriju koja počiva na krađi i preprodaji ogromnih količina osetljivih, ličnih, finansijskih i drugih tipova podataka. Ovi procesi su poslednjih godina postali automatizovani, pa se tako angažuju “botovi” – programi sa jasnim instrukcijama da pretražuju internet u potrazi za propustima i zatim infiltriraju malver ili kradu dostupne podatke. Neoprez je ono što vas čini privlačnim plenom, a čak i uvođenje minimalnih mera bezbednosti može biti presudno u sprečavanju botova da vas identifikuju kao metu.

Zabluda #2: čak i da ukradu moje podatke, oni su beskorisni

Naši lični podaci su kao vrata drugim, još osetljivijim informacijama i sistemima. Zamislite sledeći tok događaja: desi se curenje korisničkih podataka na šoping sajtu koji ste koristili jednom u životu. Vaše ime, adresa elektronske pošte i lozinka se nađu u rukama sajber kriminalaca.

Pošto koristite jednu istu lozinku za svaki nalog koji posedujete (uključujući i poslovni), napadači uspevaju da pristupe sandučetu vaše elektronske pošte i kompromituju vas na radnom mestu. Odjednom – firma se suočava sa ozbiljnim sajber napadom, a svi prsti su upereni u vas. Bez suvišnog isticanja očiglednih posledica – imajte na umu da vaši lični podaci, ukoliko su kompromitovani, mogu na razne načine prouzrokovati štetu vama, kao i ljudima koji su povezani sa vama u digitalnoj sferi.

Zabluda #3: Sajber kriminalci su nemoćni, ako imam antivirus.

Antivirus je obavezan alat za korisnike interneta, ali nije univerzalno rešenje za svaku pretnju sa kojom ćete se susresti. Kao što postoje antivirusi, tako postoje i alati i programi napravljeni da neutralizuju njihove zaštitne kapacitete i omoguće zlonamernim fajlovima da neopaženo infiltriraju računarske sisteme. S druge strane, sajber kriminalci često koriste naivnost svojih meta, navodeći ih da sami spuste gard svog računara i instaliraju zlonamerne softvere, najčešće kroz phishing prevare.

Iako pojedini antivirusi poseduju kapacitete da prepoznaju phishing mejlove, prvenstveno putem indikatora o kojima ćemo pričati kasnije, ne postoji stopostotno rešenje koje garantuje apsolutnu bezbednost.

Zato u ovu zabludu spada i stav da su internet prevare lako uočljive. Kao što ćete videti dalje u tekstu, sajber kriminalci su veoma vešti i poseduju alate koji im omogućavaju sprovođenje sofisticiranih napada i zaobilaženje raznih bezbednosnih mera, uključujući i antiviruse.

Zabluda #4: Sajber kriminalac je isto što i haker.

Iako se često koriste kao sinonimi, neophodno je napomenuti da pojmovi “sajber kriminalac” i “haker” nisu isti. Većina pomenutih stručnjaka za sajber bezbednost su hakeri koji koriste svoje znanje u etičke svrhe. Sa druge strane, sajber kriminalci su ljudi koji koriste svoje tehničko znanje isključivo u nezakonite svrhe, kao što su krađa podataka, iznuda novca ili sabotiranje sistema.

Sada kada smo raskrstili sa onim što sajber kriminalci nisu, vratimo se na ono što jesu. Tačnije, vratimo se okruženju i alatima koje najčešće koriste.

Dark Web - Mračna strana interneta

Ono što čini sajber kriminal toliko popularnim jeste mogućnost obavljanja ilegalnih radnji relativno anonimno i sa bezbedne distance. Centar zbivanja, odnosno virtualni prostor na kom se odigrava većina sajber kriminalnih radnji se zajednički naziva Dark Web. U pitanju je deo interneta koji nije indeksiran od strane pretraživača i za koji se često kaže da je "sakriven" ili "nevidljiv".
U ovom virtuelnom “prostoru” sajber kriminalci komuniciraju bez otkrivanja svojih identiteta i aktivnosti. To podrazumeva prodaju ili razmenu hakerskih usluga, koordinaciju sajber napada, kao i razmenu informacija o ranjivostima u sistemima koje se mogu iskoristiti za hakovanje.

Još jedna zabluda koju bi mogli dodati na našu listu je da je Dark Web isključivo rezervisan za ilegalne aktivnosti. Neindeksirana “tamna strana interneta” ima daleko širi raspon upotrebe, koji uključuje intelektualnu razmenu između tehnoloških stručnjaka, kao i aktivista koji se bave zaštitom privatnosti na internetu. Takođe, Dark Web predstavlja važan resurs za stručnjake za sajber bezbednost koji upravo odavde izvlače najvažnije informacije i primenjuju ih u borbi protiv sajber kriminala.

Ipak, na Dark Web-u i dalje dominiraju maliciozni hakeri, te svakako nije preporučljivo posećivati ove zabačene uglove interneta dok ste još u početnim fazama upoznavanja sa pojmovima sajber bezbednosti.

Proizvod/Usluga	Prosečna cena na Dark Web-u
Detalji kreditne kartice sa balansom do $5000	$120
Detalji kreditne kartice sa balansom do $1000	$80
Ukradeni kredencijali za e-banking, minimum $2000 na računu	$65
Klonirana American Express kartica sa PIN brojem	$25
Klonirana Mastercard kartica sa PIN brojem	$20
Pristup hakovanom Facebook nalogu	$45
Pristup hakovanom Instagram nalogu	$40
Pristup hakovanom Twitter nalogu	$25
Pristup hakovanom Gmail nalogu	$65
Jednogodišnja pretplata na Netflix	$25
Hakovani HBO nalog	$4
10 miliona adresa elektronske pošte iz SAD	$120

Izvor: Privacy Affairs

Kao što smo pomenuli, Dark Web predstavlja berzu za razmenu sajber kriminalnih usluga. U cenovniku možete zaključiti da su te usluge pristupačne - čak i jeftine. To dalje svedoči o rasprostranjenosti sajber kriminala i veličini ove "industrije" na globalnom nivou; ilegalne radnje su postale svakodnevnica, a primopredaja kradenih podataka omogućena zahvaljujući Dark Web-u.

Međutim, upravo ova rasprostanjenost je doprinela ogromnim ulaganjima u borbu protiv sajber kriminala. Danas, gotovo sve države sveta prepoznaju prestupe u digitalnoj sferi, sa izuzetkom od nekoliko zemalja u centralnoj Aziji i Africi. Zemlje koje prednjače u zakonodavstvu i definisanju sajber kriminala i kaznenih mera protiv ovakvih prestupa su Danska, Norveška, Ujedinjeno kraljevsto, SAD i Japan.

Kazne variraju od novčanih do zatvorskih, a odnose se kako na pružaoce, tako i primaoce usluga. Forumi koji posreduju prodaji podataka su sve češće pod budnim okom vodećih svetskih agencija za borbu protiv kriminala kao što su Interpol, FBI, i slični, pa se tako sve češće u javnosti srećemo sa vestima o hapšenjima sajber kriminalaca i zaplenama sajtova namenjenih ilegalnim aktivnostima.

Pregled osnovnih sajber pretnji

Kada su sajber pretnje u pitanju, važno je razlikovati "način dostave" od "paketa". Prvo se odnosi na metode koje sajber kriminalci koriste kako bi infiltrirali maliciozne softvere na računarske sisteme, dok "paket" predstavlja različite vrste malicioznih softvera o kojim ćete ubrzo saznati više.

Bitno je napomenuti da su sajber napadi gotovo uvek zasnovani na kombinacijama različitih veština infiltracije i upravljanja malicioznim softverima, koji mogu biti krajnje jednostavni i rutinski za korišćenje, ali i veoma kompleksni i zahtevni. Mi ćemo se zadržati na jednostavnijim, svakodnevnim pretnjama, kako bismo vas što efikasnije opremili praktičnim znanjem koje će vam pomoći da zaštitite vaše prisustvo na internetu.

Malver (Malware)

Malver je složenica nastala spajanjem reči maliciozno i softver (engl. malicious software). U pitanju je opšti pojam koji obuhvata različite vrste programa dizajniranih za nanošenje štete računarskiim sistemima, mrežama i korisnicima. Ova šteta se broji ne u milijardama – već u bilionima (trillion) dolara godišnje. Više od šest biliona dolara godišnje iznosi šteta koju malver, u kombinaciji sa drugim oblicima sajber kriminala, nanese na svetskom nivou.

Kako bi bolje razumeli astronomsku štetu koju nanosi, moramo prvo da razumemo tipove, t.j. osnovne funkcije koje malver obavlja, kao i mere zaštite koje sami možete da primenite.

• Ransomver (Ransomware)

U svetu malvera, ransomver je kralj i noćna mora za pojedince, kao i organizacije koje godišnje izgube u proseku 20 milijardi dolara boreći se sa ovom internet pošasti. Ono što ransomver čini dodatno opasnim je mogućnost da u sebe integriše druge tipove malvera, kao što su rootkit, keylogger, infostealer, o kojima ćemo pričati kasnije. S druge strane, zbog svog značaja na tržištu sajber kriminala, ovaj tip malvera konstantno evoluira na polju izbegavanja detekcije. Neke verzije ransomvera su tako potpuno neuočljive od strane antivirus softvera i zahtevaju naprednije alate da bi bili na vreme primećeni.

Ransomver funkcioniše kao kidnapovanje, ali – umesto osobe – kidnapovani su osetljivi podaci.

Nakon što se ransomver aktivira na jednom računarskom sistemu, on enkriptuje ili blokira pristup podacima na tom sistemu, a zatim traži otkupninu od žrtve u zamenu za otključavanje pristupa. Bitno je razbiti predrasudu da se ransomver aktivira odmah nakon što ostvari pristup računarskom sistemu. Ponekad, može čekati mesecima, prikupljajući informacije kako da se najefikasnije proširi i izazove najveću moguću štetu.

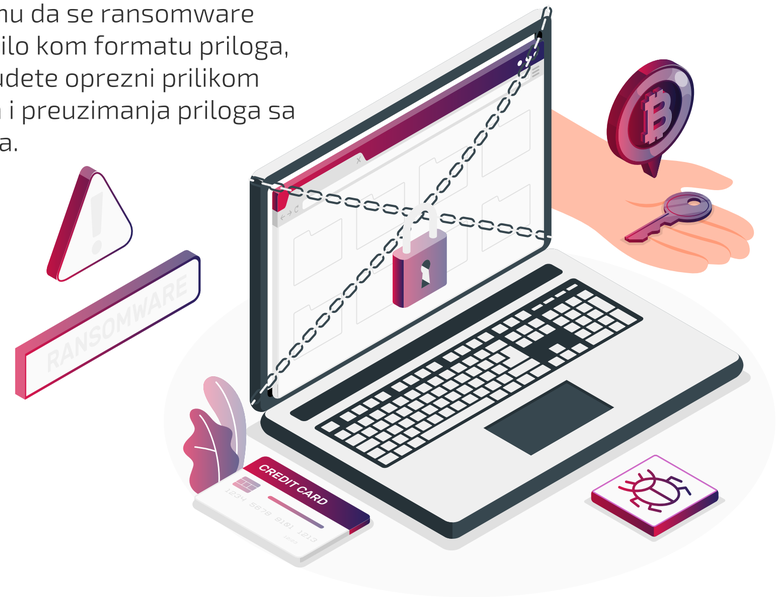
Kada se konačno aktivira, “otmičari” dolaze u poziciju da ucenjuju žrtvu i iznude novac pod pretnjom trajnog uskraćivanje pristupa podacima, brisanja podataka ili objavljivanja istih, što sa sobom povlači niz drugih pravnih komplikacija. Otkupninu obično traže u bitkoinima ili drugim kriptovalutama kako bi što efektnije izbegli praćenje novca, a iznos otkupa varira od nekoliko stotina do nekoliko hiljada dolara.

Odluku o plaćanju otkupnine treba pažljivo razmotriti, jer ne postoji garancija da će žrtva zaista dobiti ključ za dešifrovanje ili da napadači neće pustiti u javnost poverljive podatke koje su ukrali. Uglavnom, pristajanje na uslove napadača je otvorena pozivnica da vas napadnu ponovo.

U nekim slučajevima sajber kriminalci nude znak dobre volje i dekriptuju jedan fajl po izboru, kako bi vas dodatno podstakli da platite otkupninu. Naša je preporuka da nikako ne ulazite u pregovore za sajber kriminalcima, već da potražite profesionalnu pomoć i obavestite nadležne organe, kao što je Uprava za visokotehnološki kriminal MUP-a, koju možete kontaktirati putem e-adrese vtk@mup.gov.rs.

Da biste se proaktivno zaštitili od ovakvog napada, redovno pravite sigurnosne kopije podataka, implementirajte softverska rešenja koja vam pomažu da ažurirate softver i operativni sistem, i omogućite obaveštenja o potencijalnim malicioznim e-porukama i datotekama u inboksu. Poslednja stavka se direktno odnosi na phishing, koji inače služi kao broj jedan prenosilac rasnomware virusa.

Najčešći format e-priloga koji sadrže ransomware je .zip, .doc, .xls i .pdf. Ipak, treba imati na umu da se ransomware može nalaziti u bilo kom formatu priloga, pa je važno da budete oprezni prilikom otvaranja poruka i preuzimanja priloga sa nepoznatih izvora.



• Rutkit (Rootkit)

Rootkit je vrsta zlonamernog softvera koji se koristi za neovlašćeni pristup i kontrolu nad računarskim sistemima. Ovaj tip malvera može biti izuzetno opasan i težak za otkrivanje, jer se često maskira na način da ostane neprimećen u operativnom sistemu. Rootkit može biti instaliran putem različitih kanala, uključujući napade usmerene na softver ili hardver računarskog sistema, kao i phishing kampanje koje korisnike navode da instaliraju zlonamerni softver na svojim računarima.

Hakeri koriste rootkit kako bi održali svoj pristup u računarski sistem i obavljali razne aktivnosti koje uključuju krađu podataka, špijunažu, botnet napade, kao i druge oblike sajber kriminala.

Zbog složenosti i dubokog uticaja na operativni sistem, stariji antivirusi su imali problem sa detektovanjem rootkit-a. Međutim, novije verzije sve uspešnije izlaze na kraj sa ovim tipom malvera, što je dobar podsetnik da obavezno ažurirate svoj antivirus. Posmatrajte to ovako – antivirus kroz svaku svoju novu iteraciju bolje prepoznaje i blokira pretnje (npr. rootkit), što uslovljava sajber kriminalce da pronalaze nova inovativna rešenja kako bi neutralisali nove sposobnosti antivirusa.

Ni jedna ni druga strana obično ne zadržavaju prednost dugo, pa je zato od ključnog značaja da sve pozive na ažuriranje shvatite ozbiljno i uvek budete svesni da, uprkos antivirusu, ste i dalje potencijalno izloženi raznim sajber pretnjama.

• Keylogger i Info Stealer

Keylogger malver je zlonamerni softver koji se koristi za praćenje aktivnosti korisnika na računaru, odnosno beleženje svih unetih tastaturnih znakova. Tako napadači mogu da isprate unos lozinki, korisničkih imena, e-mail adresa, brojeva računa i drugih poverljivih podataka. Naprednija verzija ovog tipa malvera je Info Stealer koji preskače zamorni posao beleženja svakog pritisnutog tastera i beleži samo unesene kredencijale.

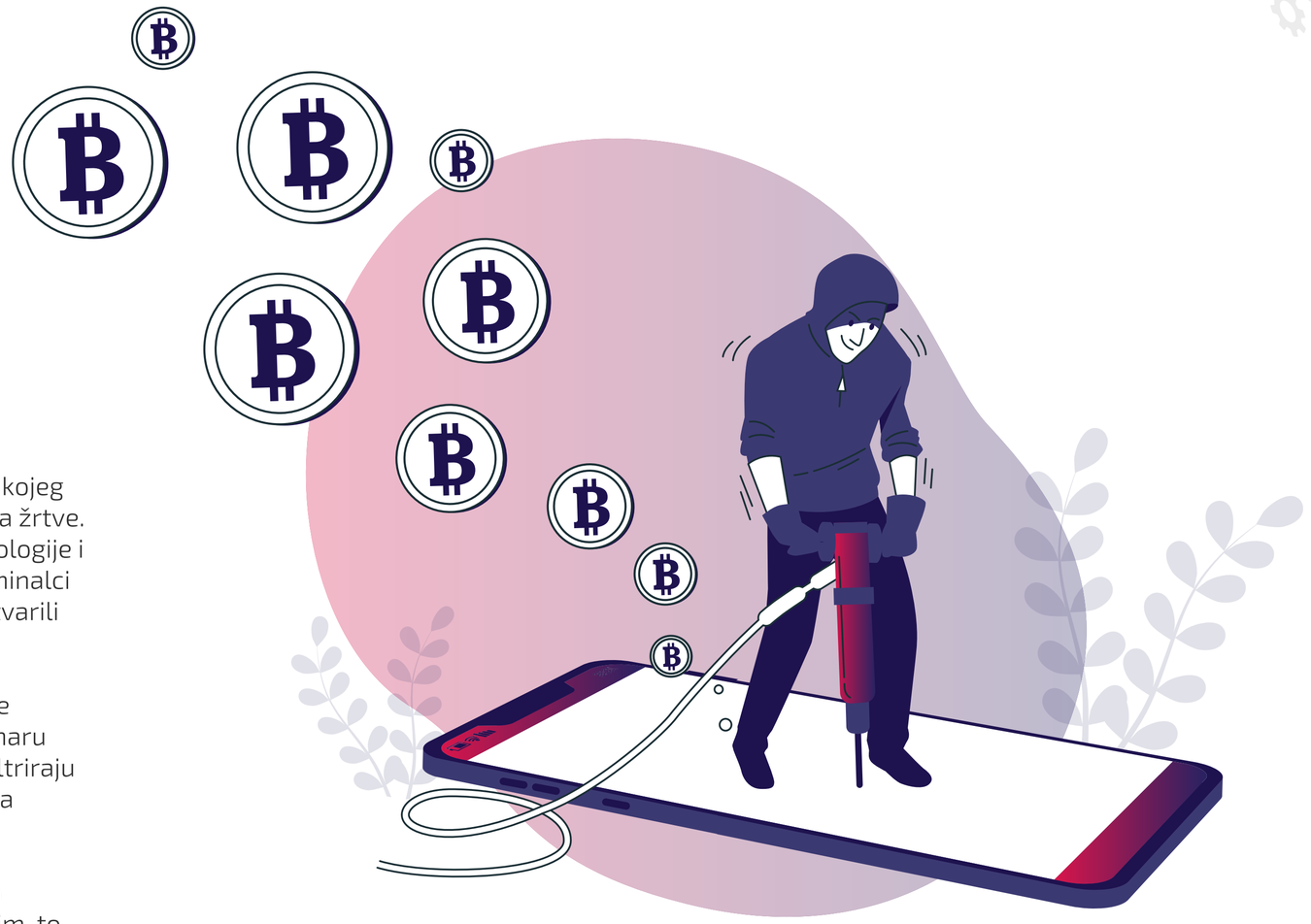
Najčešće se neprimetno instaliraju na računar žrtve, nakon čega počinju sa beleženjem i slanjem prikupljenih podataka napadaču. Nakon što se nađe u posedu kredencijala, napadač može samostalno da pristupi nalozima, zloupotrebi digitalni identitet žrtve za dalje širenje malver fajlova, ili jednostavno preproda sakupljene podatke na jednom do mnogih Dark Web tržišta.

S obzirom da su u pitanju malveri namenjeni za krađu kredencijala, preporučljivo je da aktivirate dvo-faktorsku autentifikaciju na svim relevantnim nalozima.

2FA (dvofaktorna autentifikacija) je proces koji zahteva od korisnika da unese dva faktora autentifikacije kako bi se prijavio na svoj nalog. To može biti nešto što ste sami kreirali, kao što je lozinka, i nešto što se genriše svaki put kada pristupate nalogu, što je najčešće jednokratni kôd poslat na vaš telefon. Često korišćena alternativa jednokratnim SMS kôdovima su aplikacije za autentifikaciju, koje značajno olakšavaju proces i pomažu oko sortiranja zaštićenih naloga.

Kao i kod prevencije phishing-a, preporučuje se upotreba antivirusnog rešenja, kako bi se što ranije detektovalo prisustvo malvera i eliminisalo njegovo dejstvo. Takođe, izbegavajte logovanje na naloge prilikom korišćenja javnih računara. Lako dostupni i slabo branjeni računari - u bibliotekama, internet kafeima i sl, često u sebi skrivaju opasan malver.

• Cryptojacking malver



Cryptojacking predstavlja napad na računarske sisteme tokom kojeg se kriptovalute rudare korišćenjem procesorske snage računara žrtve. Zahvaljujući porastu u popularnosti blokčejn (blockchain) tehnologije i upotrebe kriptovaluta kao što su Bitcoin i Ethereum, sajber kriminalci sve više preferiraju upotrebu cryptojacking malvera kako bi ostvarili direktnu zaradu.

Postoje dva tipa malvera koji se koriste u ovom napadu - prvi se fokusira na instalaciju softvera koji rudari kriptovalute na računaru žrtve bez njenog znanja, dok drugi tip koristi skripte koje se infiltriraju u veb stranice kako bi se procesorska snaga posetilaca tog sajta iskoristila za rudarenje.

Napadači često koriste ovu tehniku jer ona omogućava pasivno zarađivanje novca, bez direktne novčane štete po žrtvu. Međutim, to dovodi do gubitka performansi i nepotrebne potrošnje električne energije, što može imati ozbiljne posledice po računarski sistem.

• Adver (Adware)

Statistički gledano - najčešći. Psihički gledano - najiritantniji. Po pitanju štete - najbezopasniji. Adware je vrsta zlonamernog softvera koji se koristi za prikazivanje reklama na računaru korisnika. Obično se aktivira kada korisnik instalira besplatan softver ili igru sa neproverenih izvora.

Ovaj dosadni malver se može preneti putem e-maila, preuzimanjem softvera sa nepoznatih izvora ili posetom zlonamernim veb stranicama, a manifestuje se tako što vas poplavljuje reklamama i usporava rad vašeg računara.

Adware može prikazivati reklame u novim prozorima ili kao pop-up prozore, a ponekad može da izmeni podešavanja pretraživača bez odobrenja korisnika. Uvek je na granici, kao malver koji tehnički nije ilegalan, ali može preusmeravati korisnika na zlonamerne veb stranice, kako bi izazvali preuzimanje ozbiljnijeg zlonamernog softvera.

Da biste se zaštitili od ovakvih napada, koristite softver protiv adware-a, poznatiji kao Ad Blocker. Preporučujemo vam da instalirate neku od besplatnih ad blocker ekstenzija kao što su AdBlock, AdBlock Plus, Stands Fair Adblocker i Ghostery. S druge strane ukoliko koristite Google Chrome, Operu i Microsoft Edge, možete instalirati besplatne ekstenzije kompatibilne sa navedenim pretraživačima.

Takođe, preporučuje se da izbegavate nepouzdane sajtove za skidanje piratskih verzija softvera, kompjuterskih igara, i sl. Piratski sadržaj se često koristi kao prenosilac adware-a, ali i drugih, opasnijih, malver fajlova.

Phishing i Socijalni inženjering

Vratimo se na analogiju paketa i poštanske službe. Ako smo ustanovili da je malver paket , onda su phishing i socijalni inženjering metode dostave koje se staraju da dotični paket bude umotan tako da žrtva ne posumnja da je u pitanju zlonameran softver.

Phishing

Phishing je tehnika kojom se napadači obično pretvaraju da su legitimne osobe ili organizacije koje žrtva poznaje i u koje ima poverenja, poput banaka, društvenih mreža, ili kompanija. Napadači šalju lažne poruke putem e-pošte, društvenih mreža ili drugih komunikacijskih kanala, koje izgledaju kao da dolaze od legitimne organizacije. U ovim porukama se često traže osetljive informacije, poput lozinki ili finansijskih podataka, a ponekad se traži da se preuzme prilog koji sadrži malwer.

U većini slučajeva, zlonamerne e-poruke se šalju sa plagiranih domena koji na prvi pogled podsećaju na legitimne pošiljaoce.

Najbolje je ilustrovati šta to znači kroz primer. Recimo da sajber kriminalci žele da vam pošalju e-poruku predstavljajući se kao Pošta Srbije. Zvanični domen Pošte je “posta.rs”, i kao takav je registrovan i zaštićen. Međutim, “posta.net”, ili “posta.com” nisu. Zato vam napadači šalju e-poruku sa plagiranog domena, računajući da ovaj detalj može lako da vam promakne.

Kod phishing-a je vaše najbolje oružje oprez i svest da svaka neočekivana e-poruka koja zahteva da dostavite osetljive informacije ili “skinete” prilog vrlo lako može biti phishing prevara. Kada se susretnete sa e-porukom za koju sumnjate da je phishing, potražite jedan ili više sledećih indikatora:

1 Plagiran domen (Spoofed domain)

Kao što smo pomenuli, phishing napadači često koriste lažne domene koji izgledaju vrlo slično pravim imenima domena, tako da korisnici pomisle da dolazi od legitimne organizacije. Setite se primera u prethodnom poglavlju – posta.rs je original, posta.net je plagijat koji koriste napadači.

2 Urgentni ton

Taktike zastrašivanja su čest primer kako phishing prevare funkcionišu. Cilj ovog tona je da izazove osećaj poslušnosti kod targetiranog primaoca e-poruke. To može uključivati pretnje o blokiranju računa, otkazivanje usluga ili kazne, a željeni rezultat je navođenje korisnika da brzo i ishitreno odreaguje i pruži tražene podatke kako bi se izbegle pomenute neprijatnosti.

3 Link koji vodi na nebezbedan sajt

Napadači u e-poruci često uključuju link koji će vas navesti da posetite web lokaciju na kojoj će se tražiti vaši podaci. Ovi linkovi su obično skraćeni kako bi im se sakrilo pravo odredište, ili pak obrnuto – mogu biti neubičajeno dugi jer vode na plagiranu stranicu već postojećeg sajta. Još jedan od indikatora phishing-a je link koji vodi na web stranicu sa HTTP umesto HTTPS protokolom. HTTPS protokol predstavlja sigurnosni protokol koji štiti privatnost korisnika i obezbeđuje enkripciju podataka koji se prenose između veb servera i korisnika. Prepoznaje se po zelenoj ikonici katanca i natpisu "sigurno" u adresnoj traci pregledača.
S druge strane, sajt sa HTTPS protokolom i dalje može biti maliciozan, pa ne uzimajte ovu meru kao garant bezbednosti stranice. Kao što je već napomenuto, ne potcenjujte kapacitete sajber kriminalaca da vas ubede da ste bezbedni, već pristupite sa sumnjom neočekivanim elektronskim porukama koje sadrže linkove, pogotovo ako vode na stranicu koja traži unos ličnih i finansijskih podataka.

4 Sumnjivi prilozi

Phishing napadači često šalju fajlove za preuzimanje kako bi korisnici mislili da su to legitimni dokumenti. Da bi se što efikasnije sakrio maliciozni sadržaj, prilog se obično šalje kompresovan ili arhiviran – dakle sa nastavcima .rar i .zip. Međutim, ovo nisu jedini formati koji mogu skrivati malver – .pdf, .docx, .xlsx i sl, a do aktivacije dolazi kada se prilog otvori u prikladnom čitaču, kao što je Adobe Reader, odnosno Microsoft Office paket, itd.
Neočekivane e-poruke sa ovim tipom priloga treba automatski da vam izazovu sumnju. Ne otvarajte ovakve priloge dok ne budete sigurni da je pošiljalac stvaran, a da biste to utvrdili, najbolje je konsultovati se sa ostalim indikatorima.

5 Gramatički loše napisana e-poruka

Radi sopstvene bezbednosti i izbegavanja nadležnih organa, napadači gotovo uvek sprovode phishing kampanje daleko od zemalja u kojima fizički obitavaju. Zato ove e-poruke često sadrže loše prevedene tekstove, obilate gramatičkim greškama koje mogu automatski da vas navedu na sumnju.
Iako je u pitanju zaštitni znak phishing prevara koji datira iz najranijih dana interneta, karakteristične gramatičke greške bi mogle uskoro postati prošlost zahvaljujući sve pristupačnijim alatima za procesuiranje jezika pomoću veštačke inteligencije. Ovi alati mogu omogućiti efikasnije zaobilaženje jezičkih barijera i značajno ojačati napadačke kapacitete sajber kriminalaca. Pored ovih indikatora, preporučujemo i upotrebu antivirusa ili ekstenzija za pretraživač sa funkcijom prepoznavanja potencijalnih phishing e-poruka.
Ovi alati automatizuju proces prepoznavanja navedenih indikatora i pružaju vam jasno upozorenje ukoliko je e-poruka koju otvorite sumnjivog porekla.
Ako želite da saznate više o phishingu preporučujemo vam A1 kurs Ne pecaj se!, na kom ćete naći dodatne primere phishing poruka i dodatno utvrditi svoje znanje kroz kratak test.

Socijalni inženjering

Socijalni inženjering se odnosi na manipulisanje ljudskim ponašanjem tako da se žrtva navede da preuzme i aktivira malver, ili da oda osetljive informacije. Na primer, napadači se mogu predstavljati kao službenici tehničke podrške i da žele da pomognu žrtvi u rešavanju nekog problema sa računarom, a da zapravo pokušavaju da uvere žrtvu da nesvesno preuzme malver fajl. Ista situacija se može desiti i u fizičkom svetu – napadači mogu pokušati da pristupe serverima i drugoj mrežnoj opremi pod maskom ovlašćenih servisera ili podmetnuti USB fleš na vidno mesto sa malicioznim softverom sa ciljem da taj fleš završi u računaru žrtve.

S druge strane, socijalni inženjering sve više nalazi upotrebu deepfake tehnologije koja omogućava manipulaciju vizualnim i audio materijalima u stvarnom vremenu. Koristeći deepfake filtere, napadači mogu maskirati svoj fizički izgled i glas putem video poziva tako da se primaocu prikaže osoba koju poznaju, ili osoba od autoriteta kojoj veruju.

Važno je zapamtiti da su sajber kriminalci socijalni kameleoni i da će uvek naći način da iskoriste nadolazeće tehnologije kako bi ih primenili u zlonamerne svrhe.

U nekim slučajevima, phishing i socijalni inženjering se koriste kombinovano. Tako možete doživeti da vam stigne sumnjiva e-poruka iz vaše banke, a zatim i telefonski poziv u kom se napadač predstavlja kao zaposleni u istoj banci. Suočeni sa potvrdom iz dva ili više izvora, veće su šanse da ćete postupiti po uputstvu koje vam je dostavljeno i nesvesno ušetati u zamku.

Socijalni inženjering je taktika koju sajber kriminalci koriste kako bi izmanipulisali ljude i prikupili osetljive informacije. Da biste se zaštitili od ovakvih napada, edukujte se o taktikama socijalnog inženjeringa, aktivirajte dvofaktornu autentifikaciju na svim nalozima koji pružaju tu mogućnost, i koristite jake lozinke koje menjate nakon određenog vremenskog perioda (preporuka je na svakih 6 meseci).

S druge strane, vaše ponašanje je ono što sajber kriminalci pokušavaju da eksploatišu, pa je zato neophodno da usvojite određena pravila i da ih se pridržavate. To podrazumeva da ograničite pristup informacijama na društvenim mrežama samo na ljude koje lično poznajete. Broj telefona, škola koju ste pohađali, radno mesto, pozicija, adresa – sve ovo su podaci koji ne treba da budu javno dostupni.

Takođe, istrenirajte sebe da ne odajete lične podatke strancima preko telefona ili uživo. Sajber kriminalci se često predstavljaju kao nadležni organi, predstavnici policije, državne uprave ili slično. Ukoliko ne dobijete dovoljno dokaza koji potvrđuju da je osoba sa kojom razgovarate legitimni predstavnik navedenih institucija (kontekst, razlog zašto ste kontaktirani, legitimacija, potvrda od još jednog ili više izvora) – suzdržite se od odavanja osetljitivih informacija.

Kreiranje snažne lozinke pass-phrase metodom

Kreiranje snažnih i jedinstvenih lozinki predstavlja jednu od osnovnih praksi u osnaživanju lične sajber bezbednosti. One su naš prvi red odbrane protiv onlajn prevara i hakerskih napada, a ukoliko su slabe, predstavljaju otvoreni poziv sajber kriminalcima da pristupe našim nalozima i posluže se našim ličnim i drugim osetljivim podacima.

Kratke, predvidive lozinke, ili generične lozinke kao što su "password" i "123456" mogu biti podložne raznim metodama provaljivanja koje se oslanjaju na računarske procese automatskog testiranja velikog broja mogućih kombinacija. Ove metode su najčešće objedinjene pod nazivom Brute Force, odnosno “napadi sirovom snagom”.

Kao preventivna mera protiv Brute Force metoda, većina naloga ne dozvoljava kreiranje lozinki kraćih od osam karaktera, kao i zaključavanje naloga nakon nekoliko neuspešnih pokušaja logovanja. Uprkos tome, Brute Force alati i dalje predstavljaju ozbiljnu pretnju za naloge zaštićene kratkim i lako predvidiljvim lozinkama.

Primeri slabih lozinki uključuju lozinke koje se sastoje samo od brojeva, slova abecede, imena i datuma rođenja, kao i generičnih lozinki koje je lako pogoditi (npr. lozinka123). Najbolje prakse za kreiranje snažnih lozinki su lozinke duže od 12 karaktera koje koriste kombinaciju velikih i malih slova, brojeva i specijalnih karaktera. Takođe je preporučljivo izbegavanje korišćenja iste lozinke za različite naloge. Na taj način, ako se jedan nalog kompromituje, ostali će i dalje biti sigurni.

S obzirom da prosečan korisnik interneta otvori preko 30 različitih naloga, pamćenje tolikog broja jedinstvenih lozinki može predstavljati velik izazov za ljudsku memoriju. Zato se preporučuje korišćenje softvera pod zajedničkim nazivom “menadžer lozinki”, osmišljen da generiše snažne lozinke i memoriše ih na svakom nalogu, a vama pruža pristup svakom od njih kroz jednu, jedinstvenu master lozinku.

Koristili jednu master lozinku, ili 30 različitih – nije toliko bitno. Ono što je bitno je da vaša lozinka ili lozinke budu snažne i pamtljive. Ovaj rezultat ćete najlakše postići ako kreirate lozinku metodom pasfraze (pass-phrase). U pitanju je kombinacija reči i znakova koju koristimo za zaštitu naših naloga na internetu i predstavlja neprevaziđen recept za kreiranje jedinstvenih, snažnih, ali i lako pamtiljivih lozinki.

Sledeći primer će vam pomoći da napravite svoju jedinstvenu pasfrazu:

• Prvo odaberite frazu koja vam je poznata i koja se lako pamti, kao što je, na primer, brzalica "Na vrh brda vrba mrda".

• Zatim zadržite samo početna slova ove fraze: NVBVM.

• Kako bi dodatno otežali Brute Force programima da pogode vašu lozinku, pomešajte velika i mala slova (nVbVm) i dodajte datum po izboru (npr. 120303): nVbVm120303.

• Sada imate lozinku od 11 karaktera koja kombinuje velika i mala slova, kao i brojeve. Međutim, da biste stvorili zaista neprobojnu lozinku, preporučujemo da proširite broj karaktera tako što ćete još jednom dodati skraćenicu vaše odabrane fraze.

• Konačni rezultat je nVbVm120303nVbVm – lozinka koju samo vi znate, i koju je nemoguće probiti.

Pored ove, postoje i naprednije metode kreiranja pasfraza koje garantuju još već stepen nasumičnosti, što, za uzvrat, povećava otpornost vaše lozinke u slučaju da neko pokuša da je provali. Ukoliko želite da saznate više o kreiranju snažnih lozinki, ali i dodatnim merama zaštite svojih naloga, preporučujemo vam A1 kurs of Digitalnoj privatnosti.

Zaštitite svoju kućnu Wi-Fi mrežu

Često se smatra da je bezbednost bežične mreže zagarantovana, ali činjenica je da fabrička podešavanja rutera sadrže propuste koje sajber kriminalci mogu iskoristiti za krađu osetljivih podataka.

Napadači mogu da prisluškuju i ukradu privatne informacije, kao što su lozinke, i finansijski i lični podaci. Takođe, napadači mogu da iskoriste nezaštićene rutere kako bi preusmerili korisnike na lažne veb stranice koje izgledaju autentično, čime korisnici mogu biti prevareni i dovedeni u opasnost od malvera.

Zato je bitno da izvršite dodatna podešavanja svog rutera tako što ćete ukucati IP adresu 192.168.1.1 u svom pretraživaču, nakon čega će vam se pojaviti login stranica. Da biste se ulogovali u podešavanja svog rutera, neophodno je uneti vaše jedinstveno korisničko ime i lozinku. Ovi kredencijali se nalaze na samom uređaju, najčešće na levoj strani uređaja ili u priručniku za upotrebu.

Što se tiče navedene IP adrese, ona predstavlja najčešću fabričku IP adresu privatnih rutera. Koristi se kako biste pristupili svom ruteru i uneli konfigurativne izmene, kao što su promena lozinke ili aktiviranje dodatnih slojeva zaštite. Sada ćemo ukratko obraditi nekoliko preporučenih postupaka kojima ćete učiniti vašu konekciju na internet znatno bezbednijom.

• Promenite šifru za Wi-Fi mreže

Preporučuje se da zamenite vašu fabričku šifru jedinstvenom, snažnom lozinkom od najmanje 14 karaktera. Nakon što se ulogujete putem IP adrese i fabričkih kredencijala, na ekranu će se pojaviti interfejs sa različitim opcijama. Pronađite opciju za promenu lozinke, unesite novu lozinku i sačuvajte izmene.

• Isključite WPS

Wi-Fi Protected Setup (WPS) je rešenje koje omogućava jednostavno povezivanje svih vaših uređaja na Wi-Fi mrežu, bez unošenja lozinke. Međutim, iako je ova funkcija veoma praktična, pokazala se riskantnom u praksi. Ukratko, hakeri koji detektuju aktiviran WPS mogu da dođu u posed jedinstvenog WPS ključa i penetriraju vašu mrežu. Preporučuje se da isključite ovu opciju kada vam nije neophodna.

Putem istog interfejsa koji ste koristili za personalizaciju lozinke, pronađite opciju za podešavanje WPS-a, isključite WPS i sačuvajte izmene.

• Isključite SSID emitovanje

SSID, takođe poznat i kao “ime mreže” služi da identifikuje vašu mrežu uređaju koji pokušava da se konektuje, u slučaju da je više Wi-Fi mreža aktivno na istom fizičkom prostoru. Još jednom – korisna funkcija, ali podložna hakovanju. Preporučuje se da je isključite kada vam nije neophodna. To ćete uraditi na isti način kao što ste uveli prethodna podešavanja, ali ovaj put ćete pronaći opciju pod nazivom "SSID" ili "Broadcast SSID". Jednostavnim klikom na označeno dugme možete da ugasite SSID i sačuvate izmenu.

• Aktivirajte WPA3 enkripciju

WPA 3 (Wi-Fi Protected Access 3) enkripcija je sigurnosni protokol koji se koristi za zaštitu bežičnih Wi-Fi mreža od neovlašćenog pristupa. Ova enkripcija obezbeđuje visok stepen sigurnosti, što znači da se informacije koje se prenose između uređaja i rutera šifruju i ne mogu biti pročitane od strane neovlašćenih osoba koje pokušavaju da pristupe mreži. Imajte u vidu da je WPA3 savremeniji tip enkripcije. Ukoliko koristite stariji ruter, moguće je da ćete naići na prethodnu verziju, naslovljenu WPA2. U svakom slučaju, proces aktivacije je isti.

Da biste aktivirali WPA3 ili WPA2 enkripciju neophodno je da na nalogu vašeg rutera pronađete opciju za bežične postavke (Wireless Settings), izaberete WPA3 (ili WPA2) enkripciju i unesete lozinku za ponovnu potvrdu identiteta. Kao i obično, sledeći korak je da sačuvate izmene, kako bi se primenjene mere usvojile.

• Aktivirajte mrežu za goste i mrežu za IoT uređaje

Aktivacija mreže za goste omogućava sigurnu i ograničenu upotrebu vaše Wi-Fi mreže, i čini vašu primarnu mrežu bezbednijom. S druge strane, učestalija upotreba kućnih aparata koji se povezuju na Wi-Fi mrežu (štampači, klima uređaji, zvučnici i sl.) iziskuju posebnu mrežu kako bi se uklonio rizik od potencijalnih sigurnosnih pretnji. Zato, pristupite podešavanjima rutera i poduzmite sledeće korake:

• U slučaju mreže za goste, potražite opciju podešavanja "Guest Network" ili "Gostujuća mreža" i omogućite je. Unesite novu lozinku za otključavanje ove mreže i sačuvajte izmene.

• U slučaju IoT mreže, potražite opciju podešavanja "IoT Network" ili "Mreža za IoT uređaje" i omogućite je. Unesite novu lozinku za otključavanje ove mreže i sačuvajte izmene.

• Koristite Firewall

Aktiviranje firewall-a na ruteru je važan doprinos bezbednosti vaše mreže i usmeren je na prepoznavanje i blokiranje internet sadržaja sa potencijalno malicioznim dejstvom. Ukratko, Firewall funkcioniše na principu analize dolaznog i odlaznog mrežnog saobraćaja i blokira ili dopušta pristup internet sadržaju na temelju prethodno postavljenih pravila i sigurnosnih politika. Te sigurnosne politike možete podesiti pristupanjem nalogu vašeg rutera, pod opcijom Firewall.

Nakon što kliknete na opciju, pojaviće vam se lista podešavanja koje možete da implementirate kako bi blokirali određeni sadržaj i primenili dodatni nivo bezbednosti. Na primer, možete blokirati saobraćaj koji dolazi sa sajtova koji nemaju HTTPS enkripciju, ili saobraćaj sajtova koji su poznati po malicioznom sadržaju, kao što su sajtovi za pirateriju, maliciozne kopije legitimnih sajtova i sajtovi sa velikom količinom malicioznog reklamnog sadržaja.

Postoji širok spektar opcija za filtriranje sadržaja i najbolja preporuka je da se dodatno raspitate kako biste najbolje konfigurisali firewall na svom ruteru. U svakom slučaju, nakon što ustanovite svoju personalizovanu sigurnosnu politiku, ne zaboravite da sačuvate izmene.

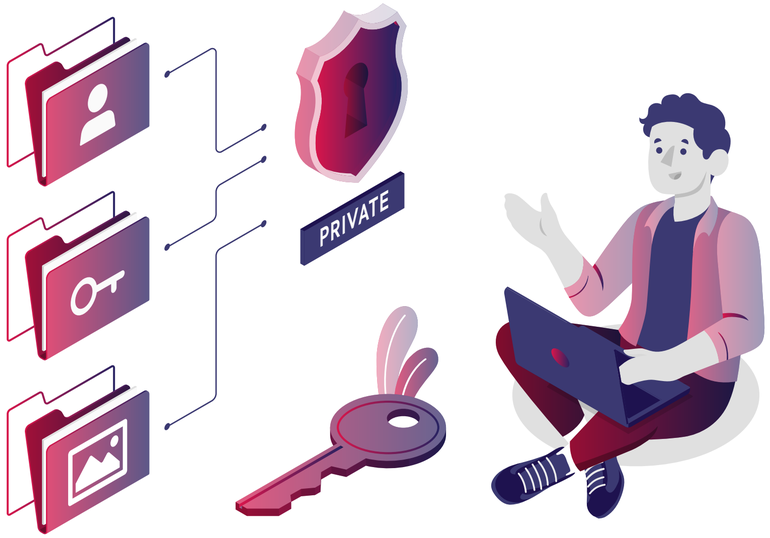
• Ažurirajte softver rutera barem jednom godišnje

Ažuriranje softvera rutera je važno jer pruža poboljšanu sigurnost, stabilnost i funkcionalnost vaše mreže. Ovo može uključivati zakrpe za sigurnosne probleme, ispravke grešaka i nove funkcije. Najčešće se izvodi putem korisničkog interfejsa rutera kojem pristupate putem vaše IP adrese, korisničkog imena i lozinke. Kada pristupite ruteru, može proveriti ima li dostupnih ažuriranja i izvršiti njihovu instalaciju. Kako bi se osigurala optimalna performansa i sigurnost vaše mreže, ažuriranje softvera rutera se preporučuje barem jednom godišnje.

Javne mreže i VPN

Kada radite od kuće ili se povezujete na javne mreže, važno je osigurati da vaši podaci budu sigurni i zaštićeni. VPN (Virtual Private Network) je tehnologija koja omogućava sigurno povezivanje na internet putem enkriptovane konekcije koja štiti vaše podatke od potencijalnih napadača.

Kada se povežete na internet putem VPN-a, vaš uređaj prvo uspostavlja sigurnu vezu sa serverom VPN provajdera. Sav saobraćaj između vašeg uređaja i interneta se tada enkriptuje, što znači da će vaši podaci biti zaštićeni od bilo koga ko pokušava da ih prisluškuje ili ukrade.



Međutim, VPN nije samo korisno sredstvo za obezeđivanje vaše kućne mreže. Takođe je veoma efikasan u zaštiti vašeg uređaja od potencijalnih rizika koji dolaze sa javno-dostupnih mreža, kao što su otvorene Wi-Fi mreže u kafićima, hotelima i drugim javnim mestima.

Napadači kreiraju lažne, otvorene Wi-Fi mreže koje imitiraju mreže dostupne u javnim prostorima. Nakon što se povežete na jednu takvu mrežu, napadač je u mogućnosti da “prisluškuje” i modifikuje komunikaciju između vašeg uređaja i interneta. Ovaj napad se naziva man-in-the-middle, a može dovesti do kompromitovanja raznih kredencijala, pa čak i finansijskih podataka. Kako biste izbegli bilo kakve neprijatnosti, preporučujemo da uključite VPN pre nego što se povežete na bilo koju otvorenu, ili mrežu čija lozinka za pristup je javno dostupna.

Saveti za bezbedno surfovanje i online šoping

Online kupovina nam je omogućila pristup znatno većem broju artikala u odnosu na fizičke prodavnice. Ali, jednostavnost kojom obavljamo kupovinu različitih proizvoda - od odeće, preko tehnologije, pa čak i svakodnevnih namirnica - otvorila je vrata za zlo-upotrebu koju sajber kriminalci redovno koriste, nanoseći ogromnu finansijsku štetu kako korisnicima, tako i e-commerce kompanijama.

Recimo, unošenjem broja kartice i CVV koda na online sajtu, te informacije se prenose preko interneta i mogu biti ugrožene. Ukoliko saobraćaj nije prikladno zaštićen, postoji mogućnost da se informacija o vašoj kartici presretnu i padnu u pogrešne ruke.

Da biste se zaštitili:

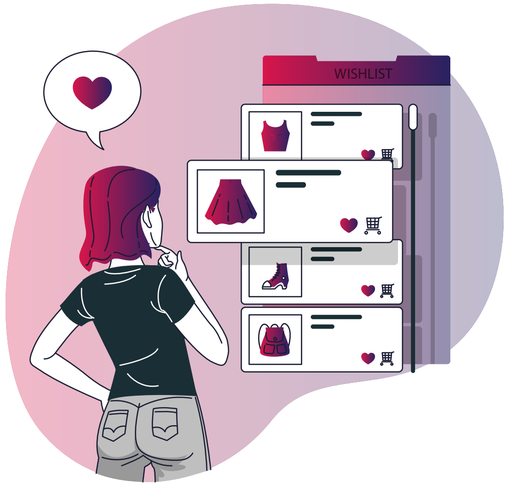
• Uvek proverite da li sajt koji posećujete ima HTTPS sertifikat koji garantuje enkripciju podataka.

• Koristite sigurne internet konekcije i zaštićene sajtove za online kupovinu.

• Ako koristite Apple uređaj, aktivirajte opciju “sakrij moju e-adresu” (hide my email).

• Ako koristite Mozilla pretraživač, ova funkcija se zove Firefox Relay.

• Ako je moguće, koristite alternativne načine plaćanja, poput PayPal-a.



Preporučljivo je i da pratite svoje bankovne izvode i obratite pažnju na bilo kakve sumnjive transakcije. U slučaju da primetite bilo kakve nepravilnosti, odmah kontaktirajte svoju banku i obavestite ih o situaciji.

Naprednije opcije zaštite uključuju otvaranje posebnog računa koji koristite samo za onlajn kupovinu ili otvorite virtualnu kreditnu karticu kojom možete generisati jednokratni broj kartice. Nakon obavljene kupovine, broj postaje nevažeći, a samim tim i neupotrebljiv za sajber kriminalce.

Takođe, kada dobijete e-poštu sa popustima, promocijama ili kuponima, budite posebno oprezni, jer u ovakvim ponudama se često krije prevara. Sajber kriminalci koriste lažne i privlačne ponude da bi došli do vaših osetljivih ličnih i finansijskih podataka, ili zarazili vaš računar zlonamernim softverom.

Stoga, pažljivo proverite da li je pošiljalac pouzdan i da li je ponuda autentična pre nego što kliknete na bilo šta u poruci ili prilogu. Najbolje je da posetite zvanični sajt prodavca i proverite da li postoji ista ili slična ponuda. Budite oprezni i ne otkrivajte svoje lične i finansijske podatke dok ne budete sigurni da je sve legitimno i bezbedno.

Ukoliko želite da unapredite svoje znanje vezano za bezbedno surfovanje internetom, preporučujemo da posetite kurs Wi-Fi dileme, koji će vam pomoći da ovladate fizičkom i virtuelnom zaštitom podataka i utvrdite svoje znanje o bezbednom korišćenju javno-dostupnih Wi-Fi mreža.

KAKO DA **ZAŠTITITE SVOJ BIZNIS**

Pregled poslovnih sajber pretnji

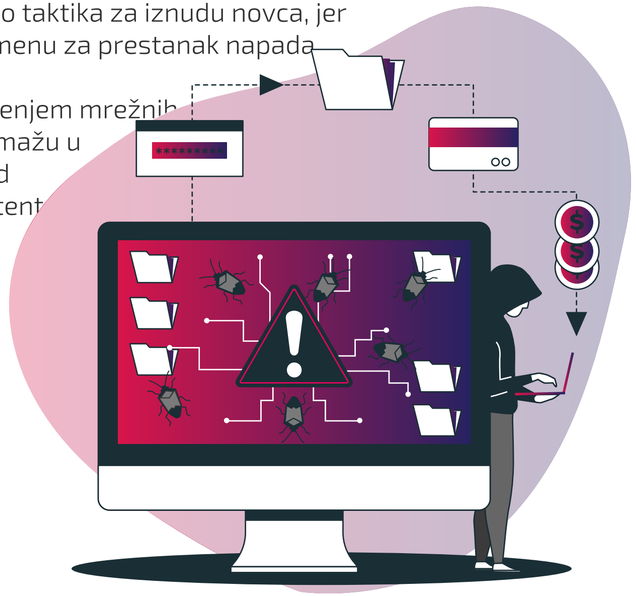
Upoznali ste se sa sajber pretnjama koje vrebaju pojedince na internetu. Sada zamislite da prenosite rizik od sajber napada na kompaniju sa desetinama, stotinama ili hiljadama zaposlenih. Logično, taj rizik, kao i potencijalna šteta se mnogostruko uvećavaju. Zato ćemo se u ovom delu fokusirati na sajber pretnje usmerene protiv organizacija, kao i motive koji stoje iza njih.

Od DDoS napada koji preplavljuju mrežne servere do zero-day propusta koji omogućavaju napadačima da otkriju i iskoriste ranjivosti neutvrđene pre dotične eksploatacije, poslovna okruženja su svakodnevno izložena višestrukim opasnostima. Na primer, ransomver napadi mogu dovesti do kompletnog kolapsa poslovnih sistema, a u slučajevima blokiranja računarskih sistema medicinskih ustanova, čak i ljudske žrtve.

Uzmite u obzir da pod “organizacija” podrazumevamo i državne institucije, uslužni sektor, kao i svaki drugi oblik organizovanja zarad postizanja komercijalnih ili nekomercijalnih ciljeva. U ovom segmentu ćemo detaljnon istražiti pretnje i analizirati kako se mogu sprečiti i ublažiti njihovi uticaji na poslovne sisteme.

• DDoS napad

Distribuirani napad uskraćivanja usluge (DDoS) je napad koji ima za cilj obaranje servera ili sistema tako što se na njih šalje velika količina zahteva za pristup. Ovo dovodi do preopterećenja sistema i onemogućava pristup korisnicima. DDoS napadi su često korišćeni kao taktika za iznudu novca, jer napadači zahtevaju plaćanje u zamenu za prestanak napada. Poslovne organizacije mogu se zaštititi od DDoS napada korišćenjem mrežnih sigurnosnih alata i usluga koje pomažu u sprečavanju ovih napada. Jedno od efikasnijih rešenja je primena Content Delivery Network servisa koji preusmerava saobraćaj i tako rasterećuje napadnuti server. Druga mera zaštita je implementacija Reverse Proxy servera iza kog može da se sakrije originalni sajt organizacije,i tako izbegne iznenadni nalet DDoS saobraćaja.



• Zero-day ranjivost

Zero-day ranjivost, ili “ranjivost nultog dana” su sigurnosni propusti koji su otkriveni od strane napadača, a za koje još uvek nije dostupna zakrpa ili rešenje. To znači da napadači mogu iskoristiti ove ranjivosti da bi pristupili sistemu i izvršili štetne aktivnosti, uključujući krađu podataka, širenje malvera i drugo.

Poslovne organizacije mogu se zaštititi od zero-day ranjivosti uspostavljanjem sistema za otkrivanje i praćenje propusta, kao i korišćenjem sistema za monitoring svih resursa, kako bi što ranije primetili maliciozne aktivnosti u svojim sistemima.

• Kompromitovanje poslovne e-adrese

Poslovne organizacije često koriste e-poštu kao način komunikacije sa klijentima i dobavljačima. Napadači mogu koristiti phishing napade da bi preuzeli kontrolu nad e-poštom i lažno se predstavljali kao zaposleni u organizaciji. Na taj način, mogu perpetuirati svoju prevaru, oštetiti veći broj zaposlenih, ili napasti same šefove organizacije. S druge strane, sajber kriminalci mogu indirektnim putem ostvariti svoje ciljeve kompromitovanjem e-adresa koje pripadaju partnerskim organizacijama ili saradnicima (dobavljači, distributeri, i sl.), i iskoristiti taj pristup da bi oštetili primarnu organizaciju.

Poslovne organizacije mogu se zaštititi od BEC-a obučavanjem zaposlenih da prepoznaju sumnjive e-poruke i korišćenjem sistema za prepoznavanje i blokiranje phishing e-poruka.

• Napad na lanac snabdevanja

Napadači mogu targetirati dobavljače i druge organizacije u lancu snabdevanja kako bi pristupili poslovnoj mreži. Ovo se naziva napadom na lanac snabdevanja i može dovesti do kršenja podataka i drugih sigurnosnih problema.

Poslovne organizacije mogu se zaštititi od ovog tipa napada uspostavljanjem protokola za procenu sigurnosti dobavljača i zahtevanja pravila za bezbednost kako bi se osiguralo da se svaki partner u lancu snabdevanja pridržava određenih standarda sigurnosti.

• Ransomware

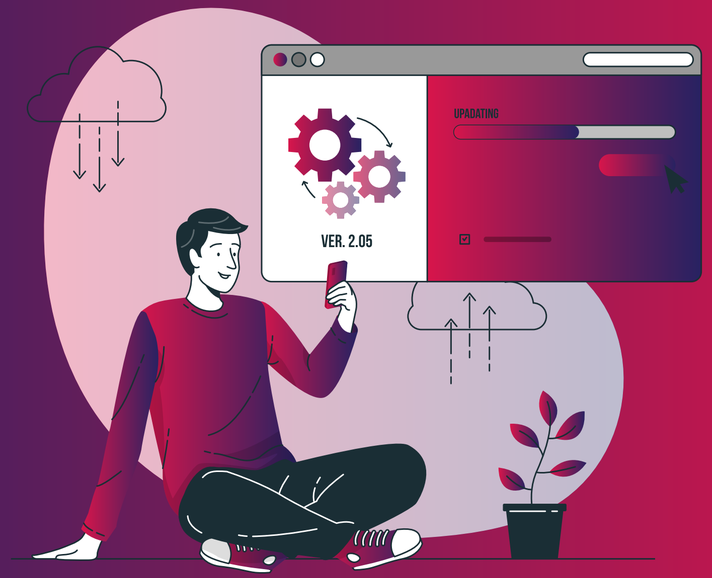
Već ste upoznati sa ovim terminom – funkcioniše isto sa organizacijom kao i sa pojedincem, samo što u slučaju organizacije, posledice mogu biti daleko ozbiljnije. Recimo, čest primer je ransomware napad na medicinske ustanove – uskraćivanjem pristupa medicinskim kartonima pacijenata, njihovi životi se dovode u opasnost, pa je samim tim motivacija za što bržu isplatu otkupnine mnogo veća.

Isto kao i kod pojedinca, najefikasniji lek za ransomware je izrada i redovno ažuriranje rezervnih kopija podataka što omogućava organizaciji da povrati izgubljene podatke bez plaćanja otkupa. S druge strane, obuka zaposlenih je jednako važna, jer se ransomware najčešće infiltrira u računarske sisteme putem phishing e-poruka.

Međutim, sama obuka može biti nedovoljna, pa zato savremene organizacije primenjuju takozvane phishing simulacije – simulirane phishing napade na pojedince zaposlene u organizaciji namenjene testiranju stepena opreznosti koji zaposleni primenjuju prilikom otvaranja svoje elektronske pošte.

Najbolje prakse pri zaštiti poslovnih mreža i podataka

Sajber bezbednost poslovnih sistema danas je neizostavna stavka u godišnjem budžetu svake organizacije koja rukovodi osetljivim podacima i poseduje infrastrukturu na internetu. Od sajtova preko servera, do terabajta zakupljenog skladištenog prostora u "oblaku", kompanije i druge organizacije moraju ozbiljno da pristupe pitanju bezbednosti. Kako bi uspeli u tome, moraju imati jasne sajber bezbednosne politike, protokole i planove za implementaciju bezbednosnih mera, kao i planove za pravilno reagovanje u slučaju napada.



• Ažuriranje softvera i hardvera

Kao i pri ličnoj zaštiti, redovno ažuriranje softvera i hardvera može pomoći u zaštiti sistema od poznatih ranjivosti koje napadači mogu iskoristiti.

• Autentifikacija korisnika

Uvođenje autentifikacije korisnika pomoći će u sprečavanju neovlašćenog pristupa poslovnim mrežama i podacima. To može podrazumevati uspostavljanje jasnih pravila o upotrebi lozinki, upotrebu dvofaktorne autentifikacije, ili uvođenje posebnih softvera za kontrolu autentifikacije korisnika.

• Obuka zaposlenih

Obuka zaposlenih o prepoznavanju sumnjivih e-poruka, phishing kampanja i drugih oblika sajber prevara može pomoći u sprečavanju neovlašćenog pristupa poslovnim mrežama i podacima.

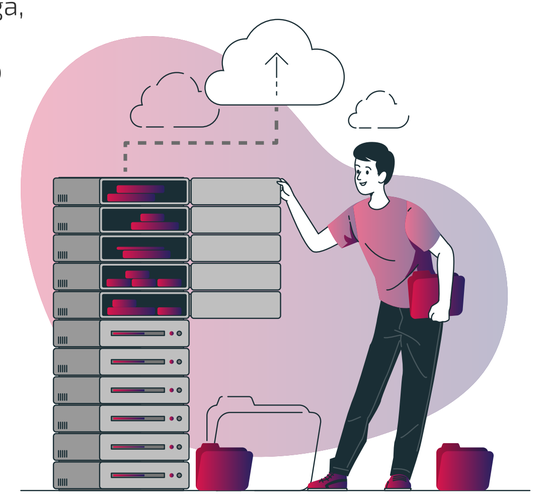
• Uspostavljanje protokola za bezbednost

Protokoli, polise i ostali regulativni interni dokumenti mogu služiti za uspostavljanje uniformnih pravila među svim zaposlenim, te tako značajno poboljšati sveopšte odbrambene kapacitete kompanije. Takođe, uvođenje protokola za procenu sigurnosti dobavljača i zahtevanje pravila za bezbednost od partnera u lancu snabdevanja može pomoći u sprečavanju supply chain napada.

• Redovan backup podataka

Backup podataka predstavlja proces izrađivanja kopija važnih fajlova i informacija sa računarskog sistema i skladištenje tih kopija na sigurno mesto. Svrha ovih kopija je da budu dostupne u slučaju gubitka podataka usled bilo kog razloga. Redovan backup je ključan za zaštitu podataka od cyber napada kao što je ransomware, jer omogućava vraćanje sistema na prethodno funkcionalno stanje i sprečava gubitak važnih podataka.

Backup se može izvršiti putem cloud usluga, eksternih uređaja za skladištenje ili drugih metoda. Redovni backup je standardni deo strategije zaštite podataka, kojim se garantuje celokupan ili delimičan oporavak podataka u kriznim situacijama.



• Uspostavljanje mrežnih sigurnosnih alata i usluga

Korišćenje različitih mrežnih sigurnosnih alata i usluga poput firewall-a, antivirusa, kao i alata za detekciju, monitoring i procenu rizika mogu značajno unaprediti sveobuhvatnu otpornost organizacije na sajber napade.

Navedene prakse su samo neke od mnogih koje poslovne organizacije mogu primeniti da bi se zaštitile od sajber pretnji. Važno je napomenuti da uspostavljanje koherentnog sajber bezbednosnog plana, koji uključuje ove prakse, predstavlja najbolju praksu za zaštitu poslovnih mreža i podataka u današnjem digitalnom svetu.

Značaj sajber bezbednosnog plana

U kontekstu navedenih sajber pretnji, sajber bezbednosni plan je ključan za uspešnu zaštitu poslovanja. Sajber bezbednosni plan predstavlja dokument koji sadrži strategiju, procedure i tehnologije koje organizacija primenjuje za zaštitu svojih informacija i sistema od sajber pretnji.

Cilj plana je da pomaže poslovnoj organizaciji da identifikuje svoje ranjivosti i uspostavi protokole za rešavanje bilo kakvih problema u vezi sa sajber bezbednošću.

Plan takođe obuhvata različite scenarije napada i mere koje organizacija treba da preduzme u kriznim situacijama.

U preventivnom smislu, plan može pomoći organizaciji da smanji rizik od napada tako što će utvrditi procedure za redovno ažuriranje softvera i hardvera, uspostaviti procedure za autentifikaciju korisnika, uspostaviti jasna pravila o upotrebi lozinki i sl.

Ukratko, sajber bezbednosni plan predstavlja ključni alat u zaštiti organizacija od sajber pretnji. Uprkos tome što napadi na sajber bezbednost nastavljaju da evoluiraju, organizacije koje imaju uspostavljen sajber bezbednosni plan mogu brže i efikasnije da reaguju i smanje rizik od sajber napada.

Šta je sajber bezbednosni šampion/ka?

Sajber bezbednosni šampion je dobrovoljna pozicija u firmi, odeljenju, ili timu zadužena za podsticanje svesti o sajber bezbednosti među kolegama. Šampion na rasploganju treba da ima odgovarajuće edukativne programe i da bude upoznat sa aktuelnim bezbednosnim praksama kako bi izgradio sajber bezbednosnu kulturu unutar organizacije.

Iako kompanije imaju posvećene role sa zadatkom uspostavljanja i održavanja sajber bezbednosti, kao što je CISO (Chief Security Officer), praksa uvođenja sajber bezbednosnog šampiona se pokazala efikasnom za implementiranje svesti među zaposlenima na organskom nivou.

Upravo posredstvom kolege, a ne menadžmenta, dolazi do efikasnog usvajanja bezbednosnih praksi odozdo, te je tako ova pozicija postala svojevrstan trend, pogotovo u firmama čiji je glavni fokus na visokim tehnologijama.

Uloga šampiona je da bude proaktivan u prepoznavanju pretnji i rešavanju problema na radnom mestu. Ovo uključuje aktivnu saradnju sa internim sajber bezbednosnim timom, kao i posredovanje u implementaciji i ažuriranju sajber bezbednosne strategije organizacije.

Dakle, šampion je neko ko je vešt u komunikaciji i dobar saradnik.

Dužnosti sajber šampiona/ke obuhvataju:

- **Upoznavanje kolega sa sajber bezbednosnim rizicima.**
- **Rukovođenje edukacijom o osnovama informacione bezbednosti.**
- **Obuci zaposlenih o pravilima kreiranja i korišćenja jakih lozinki.**
- **Upotrebi sigurnosnih alata.**
- **Protokolima za reagovanje na sajber incident.**

Funkcija sajber bezbednosnog šampiona se najčešće primenjuje na nivou tima, pa je tako svaki tim dužan da obezbedi jednu osobu koja će obavljati navedene dužnosti. Iako se primarno primenjuje u kompanijama i timovima zaduženim za razvoj softverskih rešenja i primenu praksi bezbednog kodiranja, ova funkcija sve više nalazi upotrebu i u drugim organizacijama, kao na primer:

- Zdravstvo
- Finansijske institucije
- Maloprodaja

U IT industriji, ovu funkciju u timu obavlja osoba sa tehničkom pozadinom, premda nije isključeno da navedeni spektar organizacija implementira ovu ulogu u podizanju opšte svesti o informacionoj bezbednosti. S obzirom da organizacije u zdravstvu, finansijama i maloprodaji se često nalaze na meti phishing napada koji sa sobom nose opasan malver, sajber bezbednosni šampion bi bio zadužen za edukaciju kolega i zalaganje za uvođenje zdravih sajber bezbednosnih praksi, kao na primer, kreiranje snažnih, nepredvidljivih lozinki, i obaveštavanje IT tima prilikom prijema sumnjive elektronske pošte.

Zapamtite, sajber bezbednost u firmi je kultura, i kao svaka kultura, mora da se gaji unutar radnog kolektiva. Zato, podstaknite kolege, a što je još važnije – sebe, da usvojite prakse preporučene u ovom vodiču i zaštitite osetljive podatke koji bi se mogli naći na meti sajber kriminalaca.

Budući trendovi u sajber bezbednosti

U budućnosti, očekuje se da će sajber pretnje i rizici biti sve veći i sofisticiraniji, što zahteva stalno unapređivanje pristupa sajber bezbednosti kako bi se organizacije mogle adekvatno zaštititi. Primetni su rastući trendovi koji još uvek stidljivo nastupaju, ali imaju potencijal da u narednim godinama prerastu u ozbiljne pretnje. Pre svega, povećana upotreba oblaka (cloud) već sada privlači ogroman broj napada na aplikacije i baze podataka.

Što se neposredne budućnosti tiče, pretpostavka je da će se sajber kriminalci fokusirati na napredne tehnologije poput AI i DeepFake kako bi stvorili sofisticiranije i verodostojnije pretnje koje će biti teže da se prepoznaju i spreče.

Takođe, mogli bismo videti porast cryptojacking-a - zlonamernog rudarenja kriptovaluta - koji izaziva velike probleme za blokčejn zajednicu širom sveta. Napredni oblici špijunskog softvera mogu biti još opasniji, jer se sve češće usmeravaju na specifične mete poput velikih kompanija, vlada i političkih lidera. U tom pravcu, možemo očekivati i učestalije napade na infrastrukturu, kao što su mreža za snabdevanje električnom energijom, naftovodi ili čak vodovodi.

Na kraju, sajber kriminalci će i dalje ugrožavati privatnost korisnika pomoću sofisticiranih tehnika poput phishinga, krađe identiteta i krađe podataka kako bi ostvarili svoje ciljeve. Stoga je ključno da se nastavi ulaganje u tehnologiju i obuku stručnjaka kako bi se borili protiv budućih pretnji u digitalnom svetu.

Zato sajber bezbednosna zajednica konstanto radi na novim tehnologijama i rešenjima u borbi sa rastućim stopama sajber kriminala. Što napadači postaju sofisticiraniji, to postaje važnija implementacija aktuelnih i temeljnih bezbednosnih mera, kao i pojačana predostrožnost u zaštiti osetljivih podataka i sistema. Samo ulaganjem kolektivnih napora i konstantnim ažuriranjem i unapređivanjem odbrambenih sistema možemo stati na put sajber kriminalu i učiniti internet bezbednim, kako za organizacije tako i za pojedince.

Najvažnije je zapamtiti da sajber bezbednost ne pripada samo ekspertima koji se suprotstavljaju sajber kriminalu, već je kolektivna odgovornost svakog ko koristi internet, bilo u poslovne ili lične svrhe. Zato je neophodno da svi sarađujemo i neprestano usvajamo najbolje prakse za prepoznavanje i procenu rizika, kao i sprečavanje sajber napada.

Tek kada svaka karika u lancu sajber bezbednosti postane jednako snažna kao ona do nje, ćemo moći da kažemo da je sajber kriminal prošlost.

Do tada, predlažemo vam da se dodatno upoznate sa konceptima sajber bezbednosti koristeći se resursima dostupnim u ovom vodiču i na internetu i nastavite da budete oprezni i svesni rizika sa kojim se svakodnevno suočavate.

www.preduzmi.rs

PREDUZMI
IDEJU
smisli. pokreni. ostvari.

Naslov: Uvod u sajber bezbednost

Autori: Abstract, A1

Izdavač: Inicijativa „Digitalna Srbija“

Štampa: Inicijativa „Digitalna Srbija“, bulevar Milutina Milankovića 11a, Beograd

Tiraž: 10

Mesto izdavanja: Beograd

Godina izdavanja: 2024.

ISBN 978-86-82900-04-7

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.056(0.034.2)

UVOD u sajber bezbednost [Електронски извор]. - Beograd : Inicijativa "Digitalna Srbija", 2024 (Beograd : Inicijativa "Digitalna Srbija"). - 1 USB fleš memorija ; 1 x 2 x 7 cm

Sistemski zahtevi: Nisu navedeni. - Nasl. sa naslovne strane dokumenta. - Tiraž 10.

ISBN 978-86-82900-04-7

a) Информациона технологија -- Безбедност

COBISS.SR-ID 140814345