SAJBER (CYBER) BEZBJEDNOST - PRIJETNJE I ZAŠTITA SAJBER (CYBER) BEZBJEDNOST – PRIJETNJE / CYBER SECURITY - THREATS AND PROTECTION CYBER SECURITY - THREATS

Dr Vlado Jovanić[1], Glavni inspektor, Zamjenik načelnika, Ma Boris Tušinski[2],
[1]Uprava za policijsku podršku, MUP RS, Jug Bogdana 108, 78 000 Banja Luka, Republika Srpska,
[2]OSA/OBA Bosna i Hercegovina
e-mail: vlado.jovanic@hotmail.com, vlado.jovanic@gmail.com
boris.tusinski@gmail.com

Pregledni članak
https://www.doi.org/10.58952/zr20251403369
UDK / UDC 004:343.4

Sažetak

Kada govorimo o sajber (cyber) bezbjednosti krucijalno pitanje je: "Šta svaki IT administrator i korisnik treba da znaju o sigurnosti i zaštiti sistema (koji održavaju i koriste) od sajber napada?" Međutim, samo poznavanje opcija sajber sigurnosti više nije dovoljno jer standardni mehanizmi zaštite se mogu lako premostiti-zaobići ukoliko se zanemaruje permanentna nadogradnja sistema bezbjednosne zaštite i podizanje svijesti zaposlenih o bezbjednosti i zaštiti, kako ličnoj tako i sistemskoj. Svaki propust (softverski, hardverski ili ljudski) može dovesti do bezbjednosnog upada-proboja i kontaminiranja sistema sa nesagledivim posljedicama i štetom. Praktično ne postoji potpuna-apsolutna bezbjednosna zaštita, postoje samo sistemi koji su manje ili više ranjivi, odnosno koji imaju niži ili viši stepen zaštite sa razvijenim sistemom detekcije i odvraćanja. Represija, odnosno intervencija nakon napada sa štetnim posljedicama kao krajnje sredstvo može se izbjeći uspostavljanjem efikasnog sistema zaštite. Za efikasnu prevenciju i suprotstavljanje sajber napadima i VTK neophodno je da svi korisnici IKT (informaciono komunikacione tehnologije) ulože maksimalan napor i sredstva u bezbjednosnu zaštitu sistema i okruženja u kojem posluju. U radu ćemo analizirati neke najčešće sajber napade na tredicionalne sisteme-platforme bezbjednosne zaštite (članak: Sajber bezbjednost-prijetnje) ljudskih, materijalno tehničkih, infrastrukturnih i finansijskih resursa i predložiti poboljšanje, odnosno najbolji sistem zaštite kako bi se izbjegli potencijalni napadi i eventualne intervencije (članak: Sajber bezbjednost-zaštita).

Ključne riječi: *sajber (cyber) bezbjednost, standardni mehanizmi zaštite, nadogradnja sistema, sajber napadi, analiza tradicionalnih sistema zaštite, prijedlog za poboljšanje sistema zaštite.*
JEL Klasifikacija: K14, K24, K40, K42

Abstract

When we talk about Cyber Security, the crucial question is: "What should every IT administrator and user know about the security and protection of the systems (they maintain and use) from Cyber Attacks?" However, only knowledge of cyber security options is no longer enough because standard protection mechanisms can be easily bypassed if the permanent upgrade of the security protection system and the raising of employees' awareness of security and protection, both personal and systemic, are neglected. Any failure (software, hardware or human) can lead to a security intrusion-breakthrough and contamination of the system with incalculable consequences and damage. In practice, there is no complete-absolute security protection, there are only systems that are more or less vulnerable, that is, that have a lower or higher level of protection with a developed system of detection and deterrence. Repression, that is, intervention after an attack with harmful consequences, is a last resort and should be avoided. For the effective prevention and countering of Cyber Attacks and VTK, it is necessary that all users of ICT (information communication technology) invest maximum effort and funds in the security protection of the system and environment in which they operate. In the paper, we will analyze some of the most common Cyber Attacks on traditional systems- platforms of security protection (article: Cyber security-threats) of human, material, technical, infrastructural and financial resources and propose an improvement, that is, the best protection system in order to avoid potential attacks and eventual interventions (article: Cyber security-protection).

Keywords: *Cyber Security, standard protection mechanisms, system upgrade, Cyber Attacks, analysis of traditional protection systems, proposal for improving the protection system*

UVOD

Vrijeme u kojem živimo pretpostavlja veoma brzo prilagođavanje bezbjednosnim trendovima prijetnji sajber (cyber) napadima na dnevnom nivou. Svaki novi dan predstavlja u bezbjednosnom smislu novi izazov za bezbjednost poslovne infrastrukture i njen menadžment. Sa druge strane, bezbjednosne strukture društva koje štite društvo od svih oblika ugrožavanja i zakonodavac kao autoritet koji kroz kreiranje pravnih okvira u materijalnom (inkriminacija određenih ponašanja u vidu krivičnih djela iz oblasti visokotehnološkog kriminaliteta) i procesnom smislu (procedure za sprječavanje, dokumentovanje i dokazivanje krivičnih djela) to omogućava, imaju takođe obavezu da u pogledu sajber bezbjednosti i zaštite iz svog domena rada prate bezbjednosne trendove i djeluju proaktivno, preventivno i u krajnjem slučaju represivno. Od vizije, fleksibilnosti i spremnosti upravljačke strukture za bezbjednosne promjene u poslovnom subjektu, bezbjednosnom razmišljanju, aktivnostima i prihvatanju novih trendova, posebno u tehnološkom pogledu omogućit će i bezbjedan rad i održiv opstanak djelatnosti u poslovnom subjektu a takođe i olakšati rad bezbjednosnim strukturama na identifikaciji i otkrivanju bezbjednosnih prijetnji i izvršilaca. Upravljanje i vođenje segmenta sajber (cyber) bezbjednosti u poslovnom subjektu zahtijeva prilagodljivost, izgradnju povjerenja i visok stepen razvijene bezbjednosne samosvijesti svih zaposlenih. Za uspostavu visokog nivoa karakteristika kvaliteta u pogledu sajber (cyber) bezbjednosti, rukovodioci i menadžeri moraju upravljati okruženjima visokog stresa i inspirisati timove koje vode u poslovnom subjektu na podizanju bezbjednosne kulture. Pored navedenog za viši nivo bezbjednosti neophodna je i uvezanost poslovnih subjekata sa bezbjednosnim stukturama u pogledu saradnje i razvijanja mehanizama zaštite i brzog reagovanja u kriznim situacijama. Ovo je svakako imperativ a dobre prakse u javno-privatnom partnerstvu to i dokazuju. Bezbjednost nije povlastica i nema alternativu, a ukoliko izostane u bilo kojem segmentu sistema ugrozit će sve aktere sistema. Da ne bi dolazilo do krivičnih djela neophodno je da se svaki korisnik (fizičko ili pravno lice) upozna sa određenim mjerama i protokolima zaštite i da pronađe i implementira one bezbjednosne mehanizme i sistem koji su za njega s obzirom na poslove i okruženje u kojem te poslove obavlja najoptimalniji.[248]

1. SAJBER (CYBER) BEZBJEDNOST - PRIJETNJE

Sajber bezbjednost nije samo reagovanje, već dizajniranje proaktivnih slojeva zaštite koji ublažavaju rizike i poboljšavaju bezbjednost. U oblasti sajber bezbjednosti i upravljanja u kriznim situacijama kod napada i rizicima od posljedica, neophodno je kontinuirano integrisati određene principe u poslovanje, strategije i korisnička rješenja. Najveće i najčešće prijetnje u pogledu cyber bezbjednosti za poslovne subjekte i pojedince su:

1. Fišing-Phishing[249] (pecanje-lov) koji u ukupnom sistemu prijetnji predstavljaju oko 90% ugrožavanja podataka i sistema za razmjenu podataka. Pored e-mail poruka u ovu vrstu napada spadaju i prevare koje su tako koncipirane i osmišljene da mogu dovesti u zabludu i iskusne korisnike IKT.

Rješenje ovog problema u pogledu zaštite uglavnom se svodi na sistem filtriranja podataka i e-pošte uz dvostepensku ili više slojnu autentifikaciju što ponekad predstavlja i opterećenje i gubitak vremena.

[248] Jovanić, V.: *Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta*, Doktorska disertacija, Travnik, 2024., strana 156.

[249] Phishing (od engleske riječi *fishing*-pecanje, obe riječi se izgovaraju isto ali se pišu različito) ili mrežna krađa kredencijala (identiteta) je sofisticirana prevara koja se plasira putem elektronske pošte u vidu određene porukemamca. Kreator poruke navodi žrtvu-korisnika da unese-otkrije lične identifikacione podatke (finansijski podaci o transakcionom ili nekom drugom računu) upisivanjem na lažnoj internet stranici (sadržaj i adresa stranice je sličan uobičajenim-autentičnim stranicama koje korisnik koristi ili posjećuje) koja predstavlja poveznicu poruke. u korisnikov račun elektronske pošte).

2. **Ransomware napadi**[250] (ucjenjivački napad) su uglavnom napadi sa određenim ucjenama za otkup, odnosno deblokiranje napadnutih podataka ili sistema (iznuda novca ili neka druga korist), iako ova direktna šteta (isplata traženog iznosa ili koristi) izaziva i druge propratne štete u pogledu zastoja u radu, uspostavljanje novnog sistema zaštite, kopiranje podataka, filtriranje i provjera ugroženih podataka i sistema, vrijeme oporavka sistema i drugo. Rješenje problema u pogledu zaštite je bio u pravljenju redovnih kopija podataka i pripremljenim aktivnostim u vidu planova za brzi odgovor. Kao i kod predhodnog napada i ovaj napad pored direktnih problema izazivao je i probleme zastoja u radu, gubitku vremena, kao i angažovanje dodatnih resursa za otklanjanje prijetnje i napada.
3. **Raspodijeljeni napad** uskraćivanjem resursa ili distribuirani napad uskraćivanjem resursa (eng. *distributed denial-of-service attack*, DDoS attack) je sprječavanje pristupa kompjuterskom sistemu korištenjem brojnih dostupnih resursa koji se većinom nalaze na internetu. Uobičajeni način na koji se sprječava pristup kompjuterskom sistemu ili sistemima je kroz preopterećivanje kompjuterske mreže slanjem mnogostrukih zahtjeva prema serverima, tako da se zaustavi legitimni promet prema tim serverima. Mete DDoS napada većinom su visokoprofilni mrežni serveri, banke, firme i kompanije koje obrađuju informacije s kreditnim karticama, te izvorni (*root*) DNS serveri. Cilj DDoS napada je razbiti sigurnosne sisteme koji štite servere kako bi došli do određenih informacija koje se skladište i nalaze na serveru. DDoS metode napada takođe se koriste u cyber ratovanju (napadu) za onesposobljavanje internetskog sistema neke države. Za napade se koriste preuzetim-opsjednutim kompjuterima zvanim „zombiji“ (eng. *zombie*) čiji vlasnici-korisnici nisu upoznati s činjenicom da njihov kompjuter generira napade uskraćivanjem resursa na neki drugi kompjuter ili druge kompjutere na Internetu. Ovako je moguće generisati velike količine prometa na napadnutim mrežnim segmentima čiji je dio i napadnuti kompjuter ili neki drugi mrežni uređaj. Druga vrsta raspodijeljenog DdoS napada uskraćivanjem resursa je DRDoS[251] (eng. *Distributed Reflection DoS*) napadi su vrlo slični DDoS napadima prema učinku na kranju žrtvu-korisnika i količinu generisanog saobraćaja. DRDoS napadi se zasnivaju na uspostavi veze-komunikacije u tri koraka. Napadač (ili više napadača) stvara TCP[252] paket s postavljenom SYN zastavicom kako bi inicirao vezu prema nekom postojećem kompjuteru na Internetu. Međutim, paket je tako konfigurisan da je na mjesto izvorne adrese postavljena IP adresa žrtve-korisnika. SYN paket dospijeva na odredište, a ono odgovara na adresu iz izvorišnog polja. Ukoliko server može uspostaviti vezu, paket s postavljenim SYN i ACK[253] zastavicama će biti proslijeđen prema žrtvi-korisniku. Isto tako je moguće za isporuku ICMP[254] paketa koristiti potpuno istu logiku. Tada će ECHO REPLY[255] paketi zatrpavati žrtvu. Razlog uspjeha ovih napada se nalazi u tome što se

[250] Ransomware-ucjenjivački softver (potiče od engleske riječi *ransomware*) predstavlja vrstu štetnog softvera koja ciljanom-napadnutom korisniku onemogućuje pristup kompjuterskim ili drugim sistemskim resursima uz zahtijev za isplatu otkupnine (finansijska ili neka druga korist) za uklanjanje ograničenja. Pojedini oblici ovog napada vrše kriptovanje datoteka a neki blokiraju-zaključavaju sistem uz poruku korisniku sa uputstvom za plaćanje da bi se izvršilo deblokiranje pristupa sistemu.

[251] CARNet - Hrvatska akademska i istraživačka mreža: Napadi uskraćivanjem resursa, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-162.pdf, strana 15-16, 31.07.2025., 12.00.

[252] TCP je jedan od osnovnih protokola unutar IP grupe protokola. Naziv je kratica od engleskog naziva *Transmission Control Protocol*. Korištenjem protokola TCP aplikacija na nekom serveru uključenom u kompjutersku mrežu stvara virtualnu vezu prema drugom serveru, te putem te ostvarene veze prenosi podatke. Stoga ovaj protokol spada u grupu tzv. spojnih protokola, za razliku od bespojnih protokola kakav je primjerice UDP. TCP garantira pouzdanu i isporuku podataka u kontroliranom redoslijedu od pošiljatelja prema primatelju. Osim toga, TCP pruža i mogućnost višestrukih istovremenih povezivanja prema jednoj aplikaciji više klijenata na jednom serveru, gdje su najčešći primjeri za to web ili serveri e-pošte. TCP podržava neke od najčešće korištenih aplikacijskih protokola na Internetu, kao što su HTTP (protokol za pregled web stranica), SMTP (protokol za razmjenu elektroničke pošte), telnet i SSH (protokole za udaljeni rad na kompjuteru) i brojne druge. U IP grupi protokola TCP se u slojevitom prikazu nalazi između samog IP protokola ispod, te aplikacijskih protokola na sloju iznad.

[253] https://bs.martech.zone/acronym/syn-ack/, 31.07.2025., 13.00

[254] ICMP (engleski: *Internet Control Message Protocol*) – komunikacijski protocol koji je ugrađen u svaki IP modul da bi omogućio mrežnim prolazima (usmjerivačima) ili kompjuterima slanje kontrolnih poruka o greškama. Zadužen je samo za prijavljivanje grešaka, ali ne i za njihovo ispravljanje. ICMP je dio IP protokola koji detektovane greške šalje na izvornu IP adresu paketa za koji je greška prijavljena.

[255] https://www.google.com/search?q=echo+request+and+reply&rlz=1C1GCEA_enBA1116BA1116&oq=ECHO+REPLY+paketi&gs_lcrp=EgZjaHJvbWUqCggBEAAYgAQYogQyBggAEEUYOzIKCAEQABiABBiiBDIKCAIQABiABBiiBDIHCAMQABjvBTIKCAQQABiABBiiBDIKCAUQABiABBiiBNIBCDUyNTVqMGo3qAIIsAIB8QVFp QQaJvmE6g&sourceid=chrome&ie=UTF-8, 31.07.2025., 14.07

ne generira veća količina podataka na pojedinim posrednim kompjuterima od kojih se odbijaju paketi pa nema nikakve sumnje u odvijanje napada.

4. **Društveni (socijalni) inženjering** Ova vrsta napada u pogledu informatičke bezbjednosti, podrazumijeva određeni vid psihološke manipulacije korisnika društvenih mreža u cilju otkrivanja njihovih povjerljivih ličnih ili poslovnih informacija. Društveni ili socijalni inžinjering je tip kompjuterske prevare koji ima za cilj da sa ukradenim povjerljivim informacijama izvrši neko krivično djelo (pronevjera) sa ciljem sticanja protivpravne imovinske ili neke druge koristi za sebe ili drugoga ili neovlašteno pristupi sistemu i ciljanim informacijama u sistemu sa namjerom da te informacije zloupotrebi, ošteti, kontaminira ili u potpunosti uništi ili omogući sebi ili drugome sticanje protivpravne imovinske ili neke druge koristi. Pored navedenog ova vrsta napada se definiše i kao svaki čin kojim se utiče na ciljanog korisnika da preduzme i izvrši određenu radnju koja može biti štetna za njega. Ova vrsta napada zavisi od bezbjednosne kulture i ponašanja zaposlenih.
5. **Zloupotreba kredencijala**[256] Kredencijal za logovanje predstavlja objedinjene korisničke identifikacije, odnosno akreditive (korisničko ime, email adresa, pasvord...) koji se koriste za provjeru i potvrdu identiteta ovlašćenog korisnika prilikom pristupa kompjuteru, sistemu, veb stranici-sajtu ili aplikaciji. Ove informacije su jedine validne za dobijanje pristupa i zaštitu naloga. Zloupotreba kredencijala je posljednja faza u napadima zasnovanim na kredencijalima. Ova vrsta napada podrazumijeva korišćenje kompromitovanih (ukradenih putem fišinga) kredencijala kako bi se napadač autentifikovao-pristupio na ciljanu mrežu ili aplikacije i ukrao podatke. Nakon uspješnog pribavljanja-krađe kredencijala napadač neovlašteno preuzima lozinke korisnika. U navedenom kontekstu napadač ima mogućnost da krađom i prevarom pribavljene kredencijale proda na crnom sajber tržištu ili da ih iskoristi za zlonamjerno kompromitovanje ciljane mreže, odnosno za zaobilaženje odbrambenih mehanizama za nesmetano korištenje i kretnje u mreži i krađu podataka. U neslojevitom sistemu (okruženju) bezbjednosne zaštite, napadač može slobodno da se kreće kroz ciljanu mrežu i duži vremenski period. Napadači za krađu kredencijala uobičajeno koriste fišing zato što je to jeftina i veoma uspješna taktika. Fišing napadi su efekasni zbog toga što se zasnivaju na interakciji između zaposlenogkorisnika i napadača koji pokušava da ga obmane (i često uspijeva u tome), za razliku od malvera ili alata za eksploataciju koji ciljaju ranjivosti u sistemu bezbjednosne odbrane. Krađa korporativnih kredencijala je najčešće planirana (ciljana) aktivnost. Napadači pretražuju profile tačno određenih pojedinaca na društvenim mrežama poput LinkedIna kako bi došli do kredencijala za pristup kritičnim (osetljivim) podacima i informacijama. Kada napadač iskoristi ukradene kredencijale da se uloguje kao legitimni korisnik, vrlo ga je teško identifikovati i potvrditi da li je u pitanju uljez ili korisnik koji ima odobrenja. Fišing imejl poruke i fišing sajtovi koji se koriste za krađu korporativnih kredencijala su mnogo sofisticiraniji od onih koji se koriste za krađu kredencijala privatnih korisnika (pojedinca). Napadači ulažu puno napora kako bi ovi imejlovi bili uverljivi i kako bi phishing sajtovi izgledali skoro identično kao legitimni sajtovi i profili kompanije.

6. Zlonamjerni softver (Malware)

Termin zlonamjerni softver, ili malware obuhvata grupu malicioznih-štetnih programasoftvera koji se plasiraju korisnicima u kompjutere bez njihovog znanja kako bi se infiltrirali i oštetili sistem, preuzeli-ukrali podatke za logovanje, omogućili neovlašteni pristup ili prouzrokovali neku drugu štetu (krađa lozinki-kredencijala za internetsko bankarstvo ili plasiranje neželjenih mejlova). Najčešći zlonamjerni softveri-programi iz ove kategorije mogu se podjeliti: prema načinu širenja (virus, crvi, trojanci) i prema načinu djelovanja i cilju (špijunski softveri, reklamni softveri i rootkitovi).

[256] IT Klinika: šta su napadi zasnovani na krađi kredencijala?, Net++ technology, Beograd, Srbija, 2025., https://www.it-klinika.rs/blog/sta-su-napadi-zasnovani-na-kradji-kredencijala, 30.09.2025., 14.00.

7. Prijetnje iznutra (Insajderska prijetnja)[257]

Prijetnja iznutra (insajderska prijetnja) kao bezbjednosna prijetnja ili napad predstavlja bezbjednosni rizik koji nastaje unutar strukture poslovne organizacije. Obično uključuje zaposlene, izvođače nekih radova (angažovani izvana) u poslovnom subjektu, dobavljače ili partnere koji imaju direktan pristup određenim osjetljivim informacijama, kritičnimosjetljivim sistemima ili važnim transakcijskim bankovnim računima. Insajderske prijetnje predstavljaju jedinstveni izazov za bezbjednosnu zaštitu budući da ih realizuju ljudi koji su dio konkretnog poslovnog okruženja i kojima se vjeruje a imaju legitiman pristup poslovnim resursima. Sa aspekta sajber bezbjednosti veoma važno je na vrijeme shvatiti i razumjeti prirodu i nivo unutrašnjih prijetnji i u tom kontekstu razvijati bezbjednosnu svijest svih zaposlenih. Svijest o značaju i ozbiljnosti unutrašnjih bezbjednosnih prijetnji je značajna sa nekoliko aspekata:

- Šteta koju prouzrokuje insajder daleko je veća u odnosu na vanjski napad zbog detaljnog poznavanja: sistema, procesa i rutina rada, bezbjednosnih protokola, ustroja organizacije i pristupa svim resurskim potencijalima.
- Standardne bezbjednosne mjere (firewall-vatrozid i antivirusi softver) često su nefikasne protiv insajderskih prijetnji i napada, jer su osmišljene i uspostavljene kako bi spriječile vanjske naspade i napadače, ali nisu koncipirani i bezbjednosno orjentisani da detektuju i rješavaju slučajeve zloupotrebe-napada koji dolaze iznutra.
- Cijena insajderskog napada može biti velika, ne samo u materijalno-finansijskom gubitu već i znatno veća u kontekstu ugleda i reputacijske štete. Činjenica da je neko od zaposlenih izazvao napad i prouzrokovao štetu bi moglo dovesti do gubitka povjerenja u poslovnu saradnju od strane partnera a unutar poslovnog subjekta do napovjerenja između zaposlenih, što se direktno odražava na ukupno poslovanje i bezbjednsot.
- U kontekstu navedenog, prijetnje iznutra je teško otkriti i spriječiti, jer insajderi u toku napada koriste legitimne protokole i resurse.

8. Napad nultog dana eksploatacije[258]

Napad nultog dana kao zlonamjerni eksploit predstavlja metodu zlonamjernih napadačahakera koja se ogleda u pronalaženju i korištenju bezbjednosne ranjivosti u ciljanom softveru, hardveru ili firmveru koja je još uvijek nepoznata dobavljaču ili programeru. Dobavljač ima veoma malo vremena, „nulti dan“ da popravi grešku, tako da ranjivost ostaje neotkrivena i neispravljena, što omogućava napadačima da aktiviraju eksploit za pokretanje „nultog dana napada“. Kao posljedica ovog napada nastaje krađa podataka, instaliranje zlonamernog softvera ili prekid rada sistema. Ranjivost nultog dana kao vrsta sajber napad može da postoji u novoj verziji operativnog sistema, aplikacije ili uređaja od momenta objavljivanja, ali kreator-proizvođač softvera ili hardvera to nije identifikovao u gotovom proizvodu i ne zna za sistemsku ranjivost koju praktično plasira. Ovakva vrsta ranjivosti može ostati neotkrivena i neidentifikovana danima, mjesecima ili godinama prije nego što je neko otkrije i zloupotrebi ili je eliminiše. U najboljem slučaju, administratori sajber bezbjednosti ili kreatori-programeri softvera pronalaze bezbjednosnu grešku i prije nego što postane prijetnja.

9. Napadi tipa „čovjek u sredini“ (MITM-Man-in-the-middle)[259]

Ova vrsta sajber napada često se naziva napad „prisluškivanjem“ u kojem se napadač infiltrira u ciljanu internet komunikaciju dva korisnika bez njihovog znanja i postavi se između njih, odnosno

[257] https://layerxsecurity.com/hr/glossary/what-is-an-insider-threat/ 02.10.2025. 07.50

[258] https://www.ibm.com/think/topics/cybersecurity#7281535 02.10.2025., 12.17

[259] https://recnikinterneta.rs/definicija/mitm-attack-man-in-the-middle-attack-mitm-napad-napad-coveka-u-sredini/ 14.10.2025., 11.20

postaje posrednik u komunikaciji. Neznejući korisnici komuniciraju preko posrednika (napadača) koji koristi situaciju da presretne i preuzme njihove podatke. U principu postoje dva tipa ove vrste napada:

- Napad koji je preduzet korištenjem nezaštićene ili slabo zaštićene bežične veze (Wi-Fi) na ruteru, javnim mjestima, kompanijama ili privatnim prostorima. Napadač skenira ciljane korisnike i njihove rutere tražeći slabosti-ranjivosti u konfiguraciji (jednostavne lozinke za pristup, bezbjednosni propusti u konfiguraciji) i to koristi kako bi se infiltrirao u komunikaciju između korisnika računara i veb lokacije koju posjećuje.
- Napad kojim napadač pronalazi način da ubaci malver (Malware) u računar korisnika koji se nakon toga instalira u njegov veb-pregledač (web browser) bez njegovog znanja, snima i preusmjerava sve podatke koje korisnik šalje veb-lokacijama koje posjećuje (pasvordi i drugi kredencijali za elektronsko plaćanje i bankarstvo).

Pored infiltracije u razmjeni poruka između korisnika i aplikacije, napadač može prisluškivati i privatnu komunikaciju između dva korisnika. Kod ovog scenarija napada, izvršilac-napadač koristi preusmjeravanje i prenos poruka između lica koja komuniciraju, mijenjajući sadržaj ili kreirajući nove poruke kako bi kontrolisao i usmjeravao komunikaciju u smjeru koji želi.

10. Preuzimanja putem interneta (Drive-by Download)

Sajber napad ovog tipa se dešava tokom posjeta određenim kompromitovanim ili zlonamjernim veb stranicama bez interakcije sa korisnikom (nije potreban pristup stranici putem klika na link). Napadač koristi bezbjednosne propuste i ranjivost kod starih operativnih sistema, preglednika ili softverskih dodataka sa niskim stepenom bezbjednosne zaštite kako bi se automatski preuzeo i instalirao zlonamjerni softver koji su postavili na takvim stranicama. Nakon infiltriranja u sistem softver se koristi za tajno preuzimanje povjerljivih podataka, nadzor nad korisnikom ili preuzimanje kontrole nad radnom stanicom-računarom.

11. Napredne trajne prijetnje (Advanced Persistent Threats - APT)[260]

Napredna trajna prijetnja je sofisticiran i ciljano usmjeren sajber napad koji izvodi grupa dobro finansiranih i visoko sofisticiranih napadača, uključuje velike napore te se obično izvodi protiv država, velikih korporacija ili drugih značajnih meta. Osnovni cilj APT napada je neovlašten pristup određenom cilju sa namjerom da se izvuku vrijedne informacije, poremete operacije ili nanese šteta tokom dužeg vremenskog perioda. APT-ovi se često karakterišu svojom prikrivenom prirodom, upornošću i naprednim tehnikama koje koriste akteri kako bi izbjegli otkrivanje i održali dugotrajan pristup. Ovo su ključni aspekati APT-a:

- Ciljani Pristup. APT napadi nisu slučajni. Napadači pažljivo biraju svoje ciljeve na osnovu njihove strateške vrijednosti, kao što su intelektualna svojina, poslovne tajne, osetljivi podaci ili državne tajne. Ovaj ciljani pristup pomaže napadačima da maksimiziraju uticaj svojih napora.
- Dugotrajna upornost. Za razliku od mnogih drugih sajber napada koji su usmjereni na brze dobitke, APT napadi su dizajnirani za dugotrajnu upornost. Napadači ciljaju da uspostave kontinuirano prisustvo unutar ciljnog mrežnog sistema, često održavajući pristup mjesecima ili čak godinama. Ovo produženo prisustvo omogućava im da tokom vremena prikupljaju vrijedne informacije.
- Sofisticirane tehnike. Grupe APT-ova koriste napredne tehnike kako bi prodrli u svoje ciljeve. Ovo uključuje eksploataciju ranjivosti nultog dana (ranjivosti koje prethodno nisu poznate), korištenje sofisticiranih malware-a i primenu naprednih taktika socijalnog inženjeringa kako bi prevarili korisnike i stekli početni pristup.

[260] Tušinski B.: *Savremene hibridne prijetnje - Sajber prijetnje,* Master rad, Banja Luka, 2023., strana 42.

- Prilagođeni malware-i. APT-ovi često razvijaju ili koriste malware koji su prilagođeni za izbegavanje tradicionalnih sigurnosnih mjera. Ovi malwari su dizajnirani da ostanu neprimjećeni od strane sigurnosnih rješenja i stalno se ažuriraju kako bi se prilagodili promjenama u odbrani cilja.
- Napadi u više faza. Napadači mogu započeti sa istraživanjem kako bi prikupili informacije o mreži mete i ranjivostima. Kada imaju dovoljno informacija, prelaze na početni pristup, eskalaciju privilegija, lateralno kretanje unutar mreže, eksfiltraciju podataka i eventualno čak postavljanje backdoor-a za budući pristup.
- Lateralno kretanje. Napadači APT koriste tehnike lateralnog kretanja kako bi se kretali unutar ciljnog mrežnog sistema. Ovo uključuje kompromitovanje više sistema i širenje njihovog prisustva na različite dijelove mreže, povećavajući šanse da pronađu vrijedne podatke i održe prisustvo.
- Infrastruktura komande i kontrole. Grupe APT-ova uspostavljaju infrastrukturu komande i kontrole kako bi sa udaljenosti komunicirale sa kompromitovanim sistemima i upravljale svojim zlonamjernim aktivnostima. Ova infrastruktura im omogućava da kontrolišu ponašanje malware-a, ažuriraju svoje alate i iznose ukradene podatke.
- Izazovi u identifikaciji. Identifikacija stvarnog izvora APT napada, poznata kao atribucija, je izuzetno teška. Napadači APT često preduzimaju mjere kako bi sakrili svoj pravi identitet koristeći tehnike kao što su rutiranje napada kroz više kompromitovanih sistema ili korištenje lažnih tragova kako bi zaveli istražitelje.
- Motivacije. APT napade mogu izvoditi državne agencije, organizovane kriminalne grupe, konkurentske kompanije ili hakeri. Državne APT-ove često pokreću politički, ekonomski ili vojni interesi, dok druge grupe mogu biti motivisane finansijskim dobitkom, konkurentskim prednostima ili ideološkim razlozima.
- Otkrivanje i ograničavanje. Otkrivanje i ograničavanje APT napada zahtijeva višeslojni pristup odbrane. Ovo uključuje implementaciju snažne perimetralne sigurnosti, kontinuirano praćenje neobičnih aktivnosti, obuku korisnika, segmentaciju mreže, sigurnost krajnjih tačaka, sisteme za detekciju intruzije, potragu za prijetnjama i planiranje odgovora na incidente.

12. Napadi na lozinku[261]

Napadi na lozinku uključuju iskorištavanje ranjivosti oštećene autorizacije u sistemu u kombinaciji s automatskim alatima za napad koji ubrzavaju nagađanje i razbijanje lozinki. Napadač koristi različite tehnike da pristupi i razotkrije kredencijale legitimnog korisnika, preuzimajući njihov identitet i privilegije. Napadač može „pogoditi“ lozinku na nasumičan ili sistematičan način. Napadi na lozinku uključuju:

- Brute-Force napad. Ova vrsta napada „grubom silom“ koristi metode pokušaja i pogreške kako bi se pogodile informacije o autentifikaciji korisnika. Akter koristi automatizovane skripte kako bi prošao kroz što više permutacija u cilju pogađanja korisničke lozinke. Iako je u pitanju relativno stara metoda koja zahtijeva puno strpljenja i vremena, napad grubom silom je još uvijek standardan jer je automatizovan i jednostavan.
- Napad rječnikom. Ovaj metod napada koristi unaprijed definisanu listu riječi koje će meta najvjerovatnije koristiti kao lozinke. Lista je sastavljena od obrazaca ponašanja korisnika web stranice i lozinki dobijenih ranijim curenjem podataka. Kreira se varijacijom uobičajenih kombinacija riječi po veličini slova, dodavanjem numeričkih sufiksa i prefiksa i korištenjem uobičajenih fraza. Ove liste se prosljeđuju automatizovanom alatu, koji pokušava da se autentifikuje prema listi poznatih korisničkih imena.
- Raspršivanje lozinki. U ovom napadu, akter pokušava da se autentifikuje koristeći istu lozinku na različitim nalozima prije nego što pređe na drugu lozinku. Raspršivanje lozinki je efikasno jer

[261] Ibid.

većina korisnika web stranica postavlja jednostavne lozinke, a tehnika ne krši pravila zaključavanja jer se koristi nekoliko različitih naloga. Napadači uglavnom orkestriraju raspršivanje lozinki na web lokacijama gdje administratori postavljaju standardnu zadanu lozinku za nove korisnike i neregistrovane naloge.

- Keylogging. Prilikom ovog napada akter instalira alate za praćenje u korisnikov računar kako bi snimio ključeve koje je korisnik tajno unio. Keylogger bilježi sve informacije koje korisnici upisuju u polja za unos, a zatim ih šalje zlonamjernoj trećoj strani.

Dok keyloggeri često imaju bitnu upotrebu u poslovnim postavkama (poboljšanje korisničkog iskustva, praćenje zaposlenih, itd.), napadači ih često koriste da bi zlonamjerno izvukli informacije kao što su kredencijali za prijavu za neovlašteni pristup.

- Pass-the-hash napad. Napadač iskorištava protokol autentikacije u sesiji i hvata hash[262] lozinke (za razliku od znakova lozinke direktno), a zatim ga prosljeđuje za autentifikaciju i lateralni pristup drugim umrežanim sistemima. U ovim tipovima napada, akter prijetnje ne mora dešifrovati hash da bi dobio lozinku za običan tekst.
- Golden ticket napad. Napad zlatnim tiketom počinje na isti način kao napad pass-the-hash, gdje na Kerberos (Windows) sistemu napadač koristi ukradeni hash lozinke da pristupi centru za distribuciju ključeva kako bi krivotvorio ticket-granting-ticket (TGT) hash. Iskorištava slabosti Kerberos protokola za provjeru identiteta, koji se koristi za pristup Microsoft Active Directory-u, omogućavajući napadaču da zaobiđe normalnu autentifikaciju. Mimikatz napadi često koriste ovaj vektor napada.

Pored navedenih napada kao najčešćih bezbjednosnih prijetnji postoje i napadi koji ne koriste greške korisnika i nedostatke u sistemima koji nisu adekvatno podešeni i obezbjeđeni. Većina napada koristi neki od oblika interakcije korisnika u komunikaciji sa drugim korisnicima ili sistemom kao što je ulazak (klik) na zlonamjeran link, otvaranje inficirane datoteke ili logovanje (unos ličnih kredencijala) na lažne sajtove (fišing, email, SMS,...). Međutim, napadi bez interakcije korisnika, odnosno napad bez klika ne zahtijeva bilo kakvu aktivnost korisnika. Ova vrsta bezbjednosnog napada iskorištava nedostatke u operativnom sistemu i aplikacijama koji se automatski pokreću na uređaju koji se koristi u poslovanju ili u druge svrhe. Praktično to znači da se nakon što stigne odaslana poruka na ciljani uređaj putem neke aplikacije, ta aplikacija se aktivira momentom prijema poruke u ciljanom uređaju a ne momentom njenog otvaranja. Aplikacija obrađuje poruku u pozadini momentaom prijema na uređaj i upravo ta mogućnost automatskog aktiviranja, odnosno reakcija aplikacije se koristi za pokretanje i instalaciju zlonamjernog softvera i bez znanja korisnika i bez njegove interakcije, odnosno otvaranja (klik) poruke kako bi se pogledao sadržaj. Napadi ovog tipa su rijetki ali predstavljaju veoma ozbiljnu prijetnju po sajber bezbjednost.

[262] Heš (Hash) vrijednost predstavlja jedinstveni digitalni potpis koji se dodjeljuje nekom digitalnom podatku. Heš (Hash) funkcija je svaki algoritam koji podacima proizvoljne dužine dodeljuje podatke fiksne dužine. Vrijednost koju vraća hash funkcija zove se hash vrijednost ili hash kod. Heš (Hash) funkcije se prvenstveno koriste za generisanje fiksne dužine izlaznih podataka koji se ponašaju kao reference na originalne podatk

ZAKLJUČAK

Svaka planirana i na spoznajnoj platformi kroz analizu svih faktora uticaja izgrađena strategija bezbjednosti u bilo kojem poslu ili organizacionom konceptu postavlja se i zavisi od tri ključna elementa: ljudi (zaposleni, izvršioci, korisnici), procesa (poslovne aktivnosti i bezbjednosne procedure) i tehnologije (sredstva koja su na raspolaganju za realizaciju). Svaki element je podjednako važan i mora se sinhronizovano sa ostalima uspostavljati i razvijati.

- Ljudi (zaposleni, izvršioci, korisnici)

Kvalitetno izabrani, adekvatno obučeni i kontinuirano bezbjensosno osvješćeni zaposlenici u pogledu politika i mjera zaštite posla, procesa i imovine (informacije ili neka druge vrijednosti) od sajber i svih drugih bezbjednosnih prijetnji, svakako predstavljaju najveći kvalitet i vrijednost koju neka poslovna struktura može da posjeduje. Digitalna higijena zaposlenih u pogledu kontinuirane obuke, identifikacije zlonamjernih linkova, održavanju visokog nivoa bezbjednosti lozinki, kontrole logovanja i prepoznavanje svih drugih bezbjednosnih izvora prijetnji i ugrožavanja, garantuje i adekvatne brze i efikasne reakcije na svaki vid bezbjednosnog ugrožavanja i internog i eksternog i održiv kontinuitet poslovnih procesa. Zaposleni su ključni element u strategiji sajber bezbjednosti.

- Procesi (poslovne aktivnosti i bezbjednosne procedure)

Efikasnost poslovnog subjekta je proporcionalna efikasnosti i održivosti politika i procedura koje regulišu te procese kao i u pogledu neophodnih procesa i procedura u oblasti inplementacije sajber bezbjedbnosti u sve procesne aspekte tog poslovanja. Bezbjednosni procesi i procedure moraju biti jednostavni i jasni sa fokusom na korištenje i upravljanje tehnologijom i podacima u kontekstu formailzovanja politike lozinki za pristup (logovanje), razrađen plan reagovanja na moguće bezbjednosne incidente, definisan sistem procedura za pristup i korištenje uređaja za daljinski pristup podacima i drugim uređajima, dosljedna primjena bezbjednosnih protokola i visok stepen bezbjednosne kulture zaposlenih.

- Tehnologija

Posjedovanje najnovije tehnologije i najnaprednijih alata u eri korporativne sajber bezbjednosti ne podrazumijeva automatski i garantovanu bezbjednost od ugrožavanja. Poslovni subjekti izdvajaju ogromna sredstva u zaštitne zidove (Firewall), detekciju, odvraćanje i sprječavanje napada stvarajući složenu i skupu digitalnu zaštitu. Međutim i pored toga sajber napadi i dalje pronalaze ranjivosti i uspjevaju napraviti štetu. Razlog za ovakvu situaciju je u stavu da tehnologija nije ciljani ishod bezbjednosti - već predstavlja samo skup alata-mehanizama kojima mora da upravlja ljudsko zanje i stručnost. Mnogi poslovni subkjekti su zbog ovoga u veoma nepovoljnoj bezbjednosnoj situaciji. Posjeduju tehnologiju ali nemaju potrebnu stručnost u internom okruženju za optimizaciju. Timovi zaduženi za bezbjednost su često nestručni, preopterećeni bez dovoljnog vremena za praćenje, identifikaciju i reakciju na bezbjednosnu prijetnju. Posljedica ovakvog stanja neminiovno dovodi do parcijalnog i izolovanog pristupa u sprovođenju bezbjednosti (nema uvezanosti u dojavnom sistemu za sve učesnike u radu) što opterećuje odvijanje procesa ukupne bezbjednosti. Za postizanje svrsishodne i otporne sajber bezbjednosti neophodno je stvoriti simbiozu u poslovnom subjektu između ljudske stručnosti i dostupnih tehnoloških mogućnosti kako bi se dostigla otporna bezbjednosna granica. Uobičajeni-tradicionalni bezbjednosni modeli zaštite, uspostavljeni oko neke perimetarske platforme kao odbrane (Firewall, i VPN) nisu više dovoljni da zaštite poslovni subjekt od trendova novih sajber prijetnji.

Bezbjednosni napadi i prodori su sve češći i sofisticiraniji što predpostavlja i novi pristup za izbor novih bezbjednosnih platformi, mehanizama, mjera i protokola za zaštitu osjetljivih podataka i sigurno djeljenje podataka sa drugima.

LITERATURA

[1] Jovanić, V. (2024): *Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta*, Doktorska disertacija, Travnik, 2024.
[2] Tušinski B.: *Savremene hibridne prijetnje - Sajber prijetnje*, Završni Master rad, Banja Luka, 2023.
[3] CARNet - Hrvatska akademska i istraživačka mreža: Napadi uskraćivanjem resursa, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-162.pdf, 31.07.2025., 12.00.
[4] https://recnikinterneta.rs/definicija/mitm-attack-man-in-the-middle-attack-mitm-napadnapad-coveka-u-sredini/ 14.10.2025., 11.20.
[5] https://layerxsecurity.com/hr/glossary/what-is-an-insider-threat/ 02.10.2025., 07.50.
[6] IT Klinika: šta su napadi zasnovani na krađi kredencijala?, Net++ technology, Beograd, Srbija, 2025., https://www.it-klinika.rs/blog/sta-su-napadi-zasnovani-na-kradji-kredencijala, 30.09.2025., 14.00.
[7] https://www.ibm.com/think/topics/cybersecurity#7281535 02.10.2025., 12.17.