VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

KIBERNETSKI NAPADI IN KAKO SE ZAŠČITITI PRED NJIMI

Kandidat: Vid Weilguny

Vrsta študija: študent izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: Grega Rudolf, inž. inf.

Lektorica: Živa Trstenjak, prof. ang. in nem.

Maribor, 2025

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Vid Weilguny, sem avtor diplomskega dela z naslovom Kibernetski napadi in kako se zaščititi pred njimi, ki sem ga napisal pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, Marec 2025 Podpis študenta:

ZAHVALA

Posebej se zahvaljujem mentorjema, mag. Dušanu Brglezu in Gregu Rudolfu, inž. inf., za njuno pomoč pri nastajanju tega diplomskega dela. Njuna strokovna podpora, nasveti ter spodbudne besede so mi bili v veliko oporo. Iskrena zahvala gre tudi podjetju, v katerem sem zaposlen, za omogočeno raziskovanje in pridobivanje znanja, ki je bilo ključnega pomena za uspešno izvedbo tega dela.

POVZETEK

Diplomsko delo zagotavlja celovit pregled okolja kibernetske varnosti. Opredeli in definira različne vrste kibernetskih groženj, kot so lažno predstavljanje, izsiljevalska programska oprema in porazdeljeni napadi zavrnitve storitve (DDoS), ter analizira njihove mehanizme in možne učinke. Velik poudarek je na izboljšanju ukrepov kibernetske varnosti, kar vključuje sprejetje orodij, kot so protivirusna programska oprema, požarni zidovi, večfaktorska avtentikacija (MFA) in upravitelji gesel. Delo opredeljuje tudi človeške dejavnike, ki prispevajo k varnostnim ranljivostim, in poudarja izobraževanje za izboljšanje digitalne higiene.

Diplomsko delo raziskuje praktične strategije za zmanjševanje tveganj, vključno s konfiguracijo naprednih sistemov požarnega zidu, kot je Palo Alto, in odzivom na kibernetske incidente s takojšnjimi ukrepi za zadrževanje, izkoreninjenje in obnovitev. Nadalje vključuje empirične ugotovitve iz ankete o ozaveščenosti javnosti o praksah kibernetske varnosti, vrzelih v organizacijski pripravljenosti in odnosu do zaščitnih ukrepov. Raziskovalna metodologija združuje kvalitativne in kvantitativne pristope ter ponuja uporabna priporočila za posameznike in organizacije za krepitev njihove obrambe v razvijajočem se okolju groženj.

Preučuje dvojno vlogo umetne inteligence v kibernetski varnosti, pri čemer poudarja njeno uporabo v obrambnih strategijah, kot so odkrivanje anomalij, napovedna ocena ranljivosti in avtomatizirani odzivi na grožnje, ter njeno izkoriščanje s strani kibernetskih napadalcev za razvoj napredne zlonamerne programske opreme, sofisticiranega lažnega predstavljanja in izogibanje varnostnim ukrepom. Ta razvijajoča se dinamika zahteva prilagodljive, v prihodnost usmerjene strategije.

Raziskava poudarja pomen spodbujanja kulture, ki se zaveda kibernetske varnosti, z nenehnim usposabljanjem in orodji, ki podpirajo umetno inteligenco, zlasti v organizacijah, ki obdelujejo občutljive podatke. Z integracijo tehničnih, izobraževalnih in politično usmerjenih rešitev raziskava zagotavlja smernice za krmarjenje v hitrih spremembah na področju kibernetske varnosti.

Ključne besede: spletna varnost, zlonamerna programska oprema, lažno predstavljanje, šifriranje, požarni zidovi, večfaktorska avtentikacija, napadi zavrnitve storitve.

ABSTRACT

Cyber Attacks and How to Protect Against Them

The thesis provides a comprehensive overview of the cybersecurity landscape. The paper describes various types of cyber threats, such as phishing, ransomware, and distributed denial-of-service (DDoS) attacks, and analyses their mechanisms and potential impacts. There is a strong focus on improving cybersecurity measures, including the adoption of tools such as antivirus software, firewalls, multi-factor authentication (MFA), and password managers. The study also assesses human factors that contribute to security vulnerabilities and highlights importance of education to improve digital hygiene.

The thesis explores practical strategies for mitigating risks, including configuring advanced firewall systems such as Palo Alto and responding to cyber incidents with immediate containment, eradication, and recovery actions. It further includes empirical findings from a survey that presents public awareness of cybersecurity practices, gaps in organisational preparedness, and attitudes toward safeguards. The research methodology combines qualitative and quantitative approaches and offers suggestions for individuals and organisations to strengthen their defences in the evolving threat environment.

It examines the dual role of AI in cybersecurity, highlighting its use in defensive strategies like anomaly detection, predictive vulnerability assessment, and automated threat responses, as well as its exploitation by cybercriminals for developing advanced malware, sophisticated phishing, and evading security measures. This evolving dynamic necessitates adaptive, forward-looking strategies.

The research underscores the importance of fostering a cybersecurity-aware culture through continuous training and AI-enabled tools, particularly in organisations handling sensitive data. By integrating technical, educational, and policy-oriented solutions, the study provides guidance for navigating the rapid changes in the cybersecurity landscape.

Keywords: web security, malware, phishing, encryption, firewalls, multi-factor authentication, denial of service attacks.

KAZALO VSEBINE

KAZALO SLIK

KAZALO GRAFIKONOV

Uporabljene kratice

- AI (Artificial intelligence): umetna inteligenca
- DDoS (Distributed Denial-of-Service): napad zavrnitve storitve
- DHCP (Dynamic Host Configuration Protocol): protokol dinamične konfiguracije gostitelja
- IDS (Intrusion Detection System): sistem za zaznavanje vdorov
- IP (Internet Protocol): internetni protokol
- LDAP (Lightweight Directory Access Protocol): lahek protokol za dostop do imenika
- MFA (Multi-factor authentication): večfaktorska avtentikacija
- NAT (Network address translation): prevajanje omrežnega naslova
- RADIUS (Remote Authentication Dial-In User Service): storitev klicnega uporabnika za oddaljeno preverjanje pristnosti
- RAT (Remote access Trojan): Trojan za oddaljeni dostop
- SSL (Secure Sockets Layer): plast varnih vtičnic
- TLS (Transport Layer Security): varnost transportnega sloja
- VPN (Virtual private network): navidezno zasebno omrežje

1 UVOD

Namen tega diplomskega dela je raziskati večplastno področje kibernetskih napadov ter preučiti različne vrste groženj in metode, ki jih uporabljajo kibernetski napadalci. Če razumemo mehaniko teh napadov, lahko bolje ocenimo ranljivosti v naši digitalni infrastrukturi.

V nadaljevanju diplomsko delo bolj podrobno obravnava strategije in tehnologije, namenjene zaščiti pred kibernetskimi grožnjami. Od robustnih ogrodij kibernetske varnosti in tehnik šifriranja do izvajanja požarnih zidov in sistemov za zaznavanje vdorov je celovit pristop k kibernetski varnosti bistvenega pomena za varovanje naših digitalnih sredstev.

Cilj te raziskave je zagotoviti temeljito razumevanje kibernetskih napadov in ponuditi praktična priporočila posameznikom in organizacijam za izboljšanje njihovih ukrepov kibernetske varnosti. S spodbujanjem ozaveščenosti in spodbujanjem najboljših praks lahko skupaj ublažimo tveganja, povezana s kibernetskimi grožnjami, in ustvarimo varnejše digitalno okolje.

1.1 Opis področja in opredelitev problema

Kibernetska varnost je dinamično področje, osredotočeno na zaščito digitalnih sistemov in podatkov pred različnimi grožnjami, kot so zlonamerna programska oprema, lažno predstavljanje in izsiljevalska programska oprema. Z napredkom tehnologije in taktike kibernetskega kriminala postanejo tradicionalni varnostni ukrepi neustrezni, kar zahteva stalne inovacije v obrambnih strategijah. Diplomsko delo obravnava naraščajočo razširjenost in zahtevnost kibernetskih napadov, ki predstavljajo velika tveganja za posameznike, organizacije in nacionalno varnost. Namen raziskave je analizirati te grožnje in predlagati učinkovite strategije za krepitev ukrepov kibernetske varnosti, kar bi na koncu prispevalo k močnejši obrambi pred to naraščajočo grožnjo.

1.2 Namen, cilji in osnovne trditve

To diplomsko delo raziskuje kibernetsko varnost, preučuje vpliv spletne dejavnosti na dovzetnost za lažno predstavljanje, korelacijo med močjo gesla in nepooblaščenim dostopom, učinkovitost posodobitev programske opreme pri blaženju zlonamerne programske opreme in vlogo umetne inteligence v obeh: kibernetskih napadih in obrambnih strategijah. Namen raziskave je zagotoviti uporabne vpoglede za izboljšanje praks kibernetske varnosti, ublažitev tveganj in ozaveščanje o nastajajočih grožnjah v današnjem digitalnem okolju.

Hipoteze, ki jih bom skozi diplomskega dela zavrgel ali potrdil:

- **H1**: Posamezniki, ki redno sodelujejo v spletnih dejavnostih, kot so družbeni mediji, spletno nakupovanje in bančništvo, doživljajo več lažnih napadov v primerjavi s tistimi, ki omejujejo svojo spletno prisotnost.
- **H2**: Posamezniki, ki uporabljajo močna, edinstvena gesla za vsak spletni račun, ne bodo doživeli nepooblaščenega dostopa ali kršitve podatkov v primerjavi s tistimi, ki uporabljajo isto geslo v več računih.
- **H3**: Posamezniki, ki redno posodabljajo svojo programsko opremo in operacijske sisteme, so manj dovzetni za napade zlonamerne programske opreme v primerjavi s tistimi, ki ne posodabljajo.
- **H4**: Umetna inteligenca (AI) prispeva k naprednim kibernetskim napadom in obrambi.
- **H5**: Organizacije, ki izvajajo MFA, bodo manj utrpele kršitve varnosti v primerjavi s tistimi, ki se zanašajo samo na avtentikacijo na podlagi gesla.
- **H6**: Organizacije, ki uporabljajo napredne sisteme požarnega zidu, so učinkovitejše pri preprečevanju nepooblaščenega dostopa do omrežja in blaženju kibernetskih groženj v primerjavi s tistimi, ki uporabljajo vsaj osnovno zaščito.

1.3 Predpostavke in omejitve

Kibernetske grožnje se nenehno razvijajo in napadalci vztrajno razvijajo nove metode za izkoriščanje ranljivosti. Domneva se, da človeška napaka ostaja veliko tveganje, saj lahko posamezniki kljub napredni tehnologiji postanejo žrtve lažnega predstavljanja in socialnega inženiringa. Učinkovita kibernetska varnost je odvisna tudi od ustreznih virov, kot so financiranje in usposobljeno osebje, ki morda niso na voljo vsem organizacijam, zlasti manjšim.

Za boj proti tem tveganjem je bistvenega pomena izvajanje močnih zaščitnih strategij. Redne posodobitve programske opreme, usposabljanje zaposlenih in MFA lahko pomagajo ublažiti pogoste ranljivosti. Dodatni ukrepi, kot so segmentacija omrežja, redne varnostne kopije, močan nadzor dostopa in šifriranje, zagotavljajo sloje obrambe za zaščito pred sofisticiranimi kibernetskimi napadi in notranjimi grožnjami.

Omejitve raziskave vključujejo omejen dostop do zaupnih podatkov ustanove, kjer je bila raziskava opravljena. Nadalje, specifični rezultati o ozaveščenosti zaposlenih o kibernetski varnosti so omejeni samo na vzorčno skupino in ne predstavljajo celostne slike organizacije.

Pri pisanju bodo omejitve tudi pri iskanju ustreznih virov in literature, predvsem v slovenskem jeziku.

1.4 Uporabljene raziskovalne metode

V diplomskem delu bom uporabil več raziskovalnih metod, kvalitativne in kvantitativne metode za celovito raziskovanje kibernetske varnosti. Prednostno bo obravnavano praktično reševanje problemov in prilagodljivosti na razvijajoče se grožnje. Metodologije bodo vključevale pregled literature, ankete, intervjuje, študije primerov in eksperimentalne študije, vse namenjene ustvarjanju praktičnih vpogledov za učinkovito reševanje izzivov kibernetske varnosti v resničnem svetu.

2 RAZUMEVANJE POGOSTIH KIBERNETSKIH NAPADOV

Razumevanje običajnih kibernetskih napadov je ključnega pomena za učinkovito kibernetsko varnost. Napadi z lažnim predstavljanjem, pri katerih napadalci zavajajo posameznike, da razkrijejo občutljive podatke prek zavajajoče e-pošte ali sporočil, so med najpogostejšimi. Napadi z izsiljevalsko programsko opremo so še ena pomembna grožnja, kjer zlonamerna programska oprema šifrira podatke žrtve in zahteva plačilo za njeno sprostitev. Ti napadi izkoriščajo ranljivosti v sistemih in so pogosto usmerjeni tako na posameznike kot na organizacije ter povzročajo znatno finančno in operativno škodo (Sikorski & Honig, 2012).

Prav tako pogost napad je zlonamerna programska oprema, namenjena škodi ali nepooblaščenemu dostopu do sistemov. To vključuje viruse, črve in trojance, od katerih ima vsak svoje metode ogrožanja in širjenja. Poleg tega napadi DDoS preplavijo sisteme s prometom, ki povzroči, da postanejo sistemi zakonitim uporabnikom nedostopni. Razumevanje teh metod napada pomaga pri izvajanju ustreznih obrambnih ukrepov, kot so zanesljivi varnostni protokoli, redne posodobitve sistema in usposabljanje zaposlenih za prepoznavanje in izogibanje morebitnim grožnjam »prav tam«.

Spodaj je nekaj najpogostejših kibernetskih napadov:

1. lažni napadi,
2. napadi izsiljevalske programske opreme,
3. napadi zlonamerne programske opreme:

- virusi: Pripnejo se na legitimne programe in se podvojijo, ko se izvajajo.
- črvi: Neodvisno se širijo po omrežjih in izkoriščajo varnostne ranljivosti.
- trojanci: Prikrivajo se kot zakonita programska oprema, vendar po namestitvi izvajajo škodljiva dejanja.

4. Distributed Denial-Of-Service (DDOS) napadi,
5. napadi Man-in-the-Middle,
6. napadi z vbrizgavanjem SQL,
7. podvigi ničelnega dne.

2.1 Nastajajoče grožnje kibernetski varnosti

Poleg tradicionalnih kibernetskih napadov se pojavljajo nove in razvijajoče se grožnje:

- Kibernetski napadi, ki jih poganja umetna inteligenca: Kibernetski kriminalci izkoriščajo umetno inteligenco za razvoj bolj izpopolnjenih napadov z lažnim predstavljanjem, avtomatizirajo uvajanje zlonamerne programske opreme in se izognejo odkrivanju varnostnih sistemov.
- Napadi Deepfake: Napadalci uporabljajo tehnologijo Deepfake za ustvarjanje realističnih lažnih videoposnetkov ali zvočnih posnetkov, da se predstavljajo za vodilne ali uradne osebe, s čimer zavedejo posameznike, da razkrijejo občutljive informacije.

2.2 Strategije ublažitve

Za zaščito pred temi kibernetskimi napadi morajo organizacije in posamezniki izvajati naslednje varnostne ukrepe:

- Uporabiti večstopenjsko avtentikacijo (MFA), da preprečijo nepooblaščen dostop;
- Posodabljati programsko opremo in sisteme, da popravijo ranljivosti;
- Izobraziti zaposlene o kibernetskih grožnjah, da zmanjšajo število človeških napak;
- Namestiti požarne zidove in sisteme za zaznavanje vdorov za spremljanje omrežne dejavnosti;
- Redno varnostno kopirati podatke, da ublažijo grožnje izsiljevalske programske opreme.

Razumevanje teh napadalnih metod pomaga pri izvajanju ustreznih obrambnih ukrepov, kar zagotavlja proaktiven pristop h kibernetski varnosti.

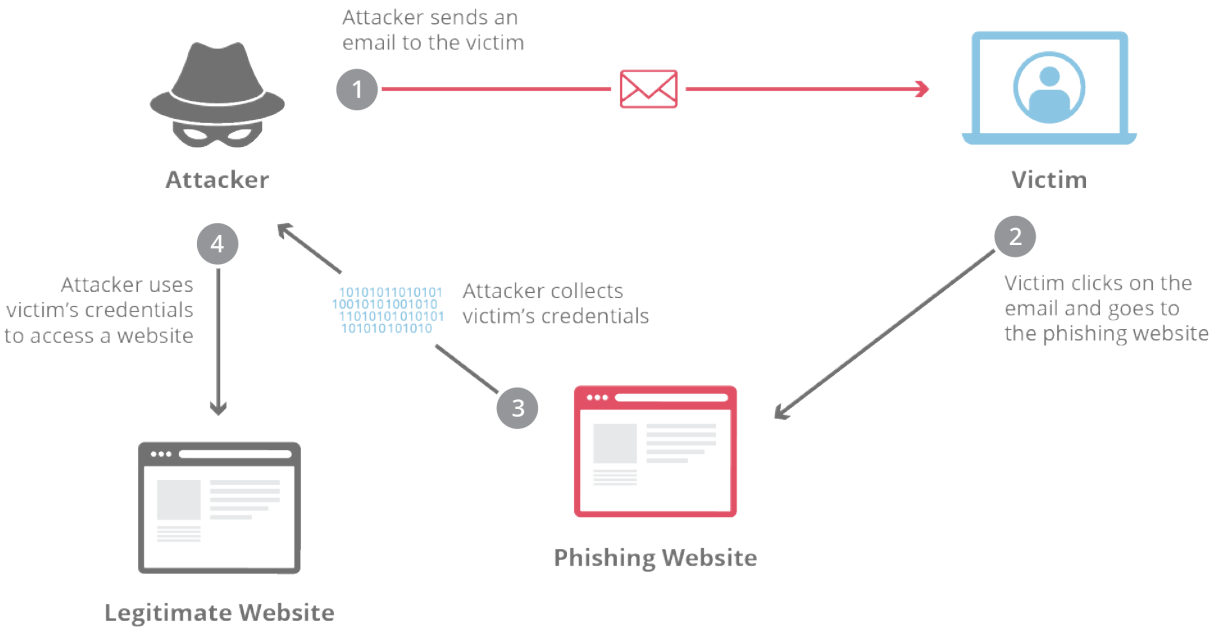
2.3 Pojav kibernetskega napada in metode izkoriščanja

Kibernetski napadi običajno izhajajo iz kombinacije razvijajočih se tehnologij in zlonamernih namenov. Napadalci pogosto izkoriščajo ranljivosti v programski, strojni opremi ali v človeškem vedenju, da pridobijo nepooblaščen dostop ali motijo sisteme. Pojav sofisticiranih orodij in tehnik, kot so napredna zlonamerna programska oprema in avtomatizirani napadalni skripti, je znatno povečal obseg in pogostost napadov. Metode izkoriščanja pogosto vključujejo socialni inženiring, kjer napadalci manipulirajo s posamezniki, da razkrijejo zaupne podatke ali izvedejo dejanja, ki ogrožajo varnost (Hadnagy, 2018).

Metode izkoriščanja vključujejo različne tehnike, ki jih napadalci uporabljajo za vdor v sisteme. Ena teh pogostih metod je izkoriščanje ranljivosti programske opreme, kjer napadalci uporabljajo znane napake za izvajanje nepooblaščenih ukazov ali dostop do občutljivih podatkov. Druga tehnika je lažno predstavljanje, kjer zavajajoča e-poštna sporočila zavedejo uporabnike, da razkrijejo poverilnice za prijavo ali namestijo zlonamerno programsko opremo. Poleg tega lahko napadalci uporabijo napade s surovo silo, da razbijejo gesla ali uporabijo izkoriščanja ničelnega dne, da izkoristijo nezakrpane ranljivosti. Razumevanje teh metod je ključnega pomena za razvoj učinkovitih strategij kibernetske varnosti in zaščito pred morebitnimi grožnjami »prav tam«.

2.4 Napadi z lažnim predstavljanjem

Napadi z lažnim predstavljanjem vključujejo pošiljanje zavajajočih e-poštnih sporočil ali sporočil, za katera se zdi, da prihajajo iz zakonitih virov, kot so banke ali zaupanja vredne organizacije, da bi posameznike zavedli in razkrili občutljive podatke, kot so gesla ali številke kreditnih kartic. Ti napadi pogosto ustvarjajo občutek nujnosti ali uporabljajo znane blagovne znamke, da prepričajo prejemnike, da kliknejo zlonamerne povezave ali prenesejo okužene priloge (Mitnick, 2001).

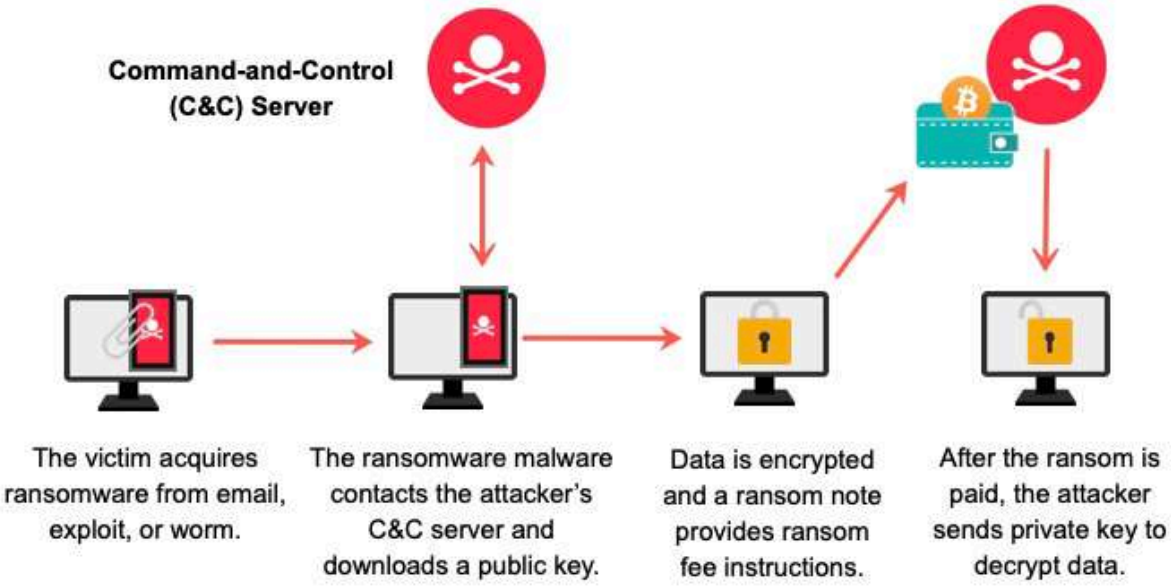


Slika 1: Kako poteka napad z lažnim predstavljanjem

Vir: (https://medium.com/gravel-engineering/learn-8-common-types-of-phishing-25a2dd4d6778)

2.5 *Napadi izsiljevalske programske opreme*

Napadi z izsiljevalsko programsko opremo šifrirajo podatke žrtve, zaradi česar so nedostopni, dokler napadalcu ni plačana odkupnina. Zlonamerna programska oprema je pogosto dostavljena prek lažnih e-poštnih sporočil ali ogrožene programske opreme. Ko izsiljevalska programska oprema šifrira podatke, napadalec zahteva plačilo, običajno v kriptovaluti, za ključ za dešifriranje. Tovrstni napadi lahko močno motijo poslovanje in povzročijo velike finančne izgube (Mitnick, 2001).

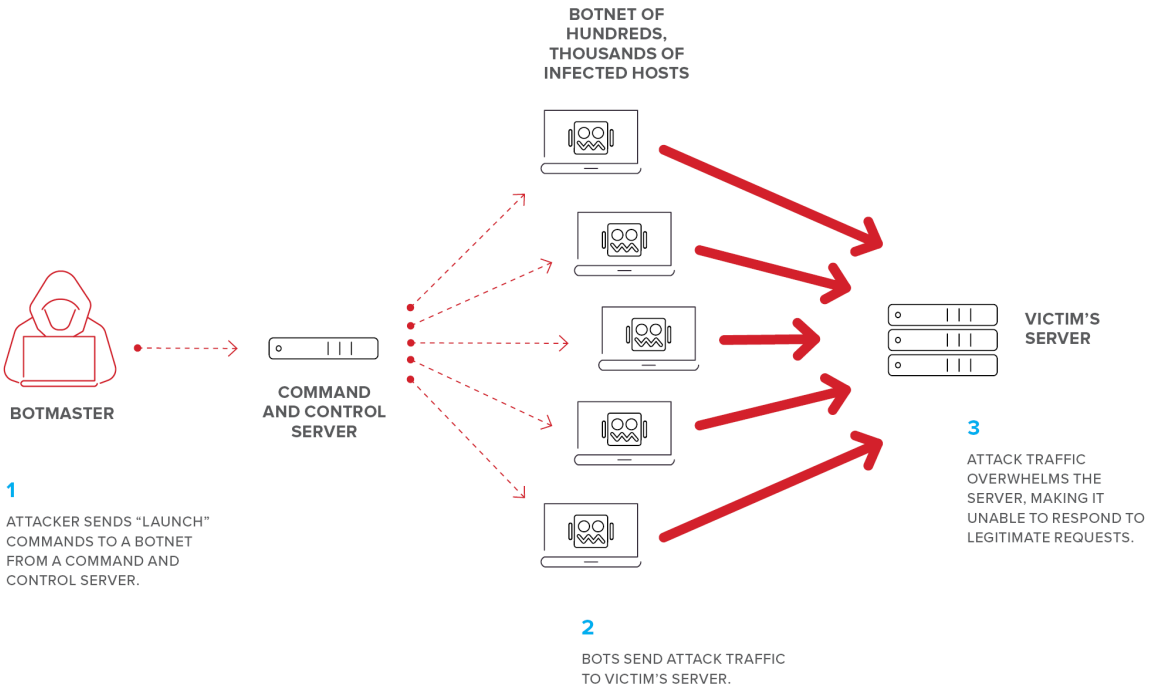


Slika 2: Kako poteka napad izsiljevanja programske opreme

Vir: (https://assets.extrahop.com/images/blogart/ransomware/how-ransomware-works.jpg)

2.6 *Napadi zavrnitve storitve (DDoS)*

Napadi z zavrnitvijo storitve preplavijo ciljni sistem, omrežje ali spletno mesto s prekomernim prometom, zaradi česar so nedostopni zakonitim uporabnikom. Pri napadu DDoS se uporabi več sistemov za preplavitev tarče s prometom, s čimer se povečata obseg in učinek napada. Napadi DDoS lahko povzročijo izpade, vplivajo na poslovanje in škodijo ugledu tarče (Mitnick, 2001).



Slika 3: Kako poteka napad zavrnitve storitve

Vir: (https://www.nicehash.com/blog/post/a-deep-dive-into-lightning-network-ln-security)

3 ČLOVEŠKI DEJAVNIK V KIBERNETSKI VARNOSTI

V današnjem digitalnem svetu je kibernetska varnost ključnega pomena za posameznike in organizacije. Čeprav so tehnološke obrambe, kot so požarni zidovi, šifriranje in sistemi za zaznavanje vdorov, izboljšale digitalno varnost, ostaja človeški dejavnik pomembna ranljivost. Ljudje so pogosto najšibkejši člen kibernetske varnosti, saj taktike socialnega inženiringa izkoriščajo človeško psihologijo, posamezniki pa včasih ne sledijo ustreznim varnostnim protokolom. To diplomsko delo raziskuje človeški dejavnik v kibernetski varnosti, pri čemer se osredotoča na običajne taktike socialnega inženiringa, kot so lažno predstavljanje, vabe in sledenje, ter pomen usposabljanja za ozaveščanje o kibernetski varnosti pri zmanjševanju človeških napak in izboljšanju varnosti.

3.1 Taktika socialnega inženiringa

Socialni inženiring se nanaša na manipuliranje s posamezniki, da razkrijejo zaupne podatke ali izvajajo dejanja, ki ogrožajo varnost. Za razliko od tradicionalnega hekanja, ki izkorišča ranljivosti sistema, socialni inženiring cilja na človeško vedenje in psihološke slabosti. Običajne taktike vključujejo lažno predstavljanje in lovljenje.

3.1.1 Lažno predstavljanje

Lažno predstavljanje je bolj ciljno usmerjena oblika socialnega inženiringa, kjer napadalci ustvarijo zavajajoča e-poštna sporočila, namenjena določenim posameznikom ali organizacijam. Ti napadi temeljijo na podrobnih raziskavah o žrtvi, kot so njena služba, interesi ali nedavne dejavnosti. S prilagajanjem sporočila posamezniku postane lažno predstavljanje veliko bolj prepričljivo kot splošni poskusi lažnega predstavljanja. Na primer, zdi se lahko, da e-poštno sporočilo prihaja od šefa ali sodelavca in zahteva občutljive podatke ali finančni prenos. Ker se sporočilo zdi legitimno, je bolj verjetno, da ga bo prejemnik upošteval in napadalcem omogočil dostop do občutljivih podatkov ali sistemov.

3.1.2 Vabe

Vabe so taktika socialnega inženiringa, ki ponuja nekaj vabljivega, da zvabi žrtve v past. Napadalec lahko obljubi brezplačno programsko opremo, medije ali ekskluzivne posle v zameno za občutljive podatke ali dostop do sistema. Pogost primer vabe je puščanje okuženega pogona USB na javnem mestu v upanju, da ga bo nekdo našel in priključil v svoj računalnik.

To napadalcu prek zlonamerne programske opreme omogoči dostop do žrtvinega sistema. Do vab lahko pride tudi na spletu, kjer so na voljo navidezno »brezplačni« prenosi, ki pogosto vsebujejo zlonamerno kodo.

3.1.3 Tailgating

Tailgating (sledenje) je taktika socialnega inženiringa, pri kateri napadalec sledi pooblaščenemu posamezniku v varno območje, brez ustreznega preverjanja pristnosti. Na delovnem mestu se to lahko zgodi, ko zaposleni potegne svojo varnostno kartico, da bi vstopil v stavbo, in napadalec preprosto vstopi za njim, mimo točke varovanja. Tailgating izkorišča človeško prijaznost ali malomarnost, pri čemer se napadalec zanaša na vljudnost ali nepozornost zaposlenega. Ko je v zavarovanem objektu, lahko napadalec pridobi dostop do občutljivih podatkov ali infrastrukture.

3.2 Vloga usposabljanja za ozaveščanje o kibernetski varnosti

Usposabljanje za ozaveščanje o kibernetski varnosti je ključnega pomena za ublažitev tveganj, ki jih povzročajo človeške napake. Z izobraževanjem zaposlenih o pogostih kibernetskih grožnjah, najbolj pogostih praksah, ter o tem, kako prepoznati varnostna tveganja in se nanje odzvati, lahko organizacije znatno zmanjšajo ranljivosti, povezane z vedenjem ljudi.

3.2.1 Prepoznavanje groženj

Glavni cilj usposabljanja o kibernetski varnosti je pomagati zaposlenim pri prepoznavanju groženj, kot so lažna e-poštna sporočila, zlonamerne priloge in sumljive povezave. Programi usposabljanja učijo posameznike, kako preveriti pošiljatelje e-pošte, se izogibati klikanju na neznane povezave in skrbno oceniti zahteve za občutljive podatke. Pri zaposlenih, ki so usposobljeni za prepoznavanje znakov socialnega inženiringa, je verjetnost, da bodo postali žrtve lažnega predstavljanja ali napadov z vabami, veliko manjša.

3.2.2 Zmanjšanje človeške napake

Človeška napaka je najbolj pogost vzrok za kršitve kibernetske varnosti, saj je pogosto posledica pomanjkanja znanja ali nepravilnih dejanj, kot je klikanje zlonamernih povezav ali neupoštevanje varnostnih postopkov. Usposabljanje za ozaveščanje je namenjeno zmanjšanju teh napak s spodbujanjem dobrih varnostnih praks. Zaposleni se naučijo uporabljati močna, edinstvena gesla, kako uporabljati večfaktorsko preverjanje pristnosti in se izogibati tveganemu

vedenju, kot je, na primer, uporaba javnega omrežja Wi-Fi za opravila, povezana z delom. Jasne smernice in redni opomniki dodatno krepijo te prakse in zmanjšajo možnosti naključnih napak, ki bi lahko povzročile kršitve.

3.2.3 Gradnja kulture, ki se zaveda varnosti

Usposabljanje za ozaveščanje o kibernetski varnosti pomaga ustvariti kulturo budnosti v organizacijah. Ko so zaposleni obveščeni o tveganjih kibernetske varnosti in svoji vlogi za zmanjševanje le-teh, je večja verjetnost, da bodo sprejeli proaktivno varnostno vedenje. Tak kulturni premik spodbuja zaposlene, da prijavijo sumljive dejavnosti, vestno sledijo protokolom in sodelujejo pri nenehnih varnostnih prizadevanjih. Varnostno ozaveščeno okolje zmanjšuje možnosti človeških napak in krepi splošno obrambo organizacije.

3.2.4 Obravnavanje notranjih groženj

Usposabljanje o kibernetski varnosti obravnava tudi notranje grožnje, ki so lahko prav tako škodljive kot zunanji napadi. Zaposleni, ki razumejo tveganja, povezana z deljenjem gesel, odobritvijo nepooblaščenega dostopa ali napačnim ravnanjem z zaupnimi podatki, bodo manj verjetno naredili te napake. Usposabljanje za ozaveščanje poudarja pomen varovanja občutljivih informacij in spodbuja poročanje o vseh sumljivih notranjih dejavnostih.

Človeški dejavnik ostaja ena najpomembnejših ranljivosti v kibernetski varnosti. Taktike družbenega inženiringa, kot so lažno predstavljanje, vaba in zakrivanje, izkoriščajo človeško psihologijo za dostop do občutljivih podatkov ali sistemov. Ozaveščanje o kibernetski varnosti pomaga ublažiti ta tveganja z izobraževanjem posameznikov o tem, kako prepoznati običajne varnostne grožnje, se jim izogniti ali se nanje odzvati. Človeška napaka ima lahko resne posledice, četudi je tehnična obramba vzpostavljena. Z vlaganjem v redno usposabljanje o kibernetski varnosti in spodbujanjem kulture, ki se zaveda varnosti, lahko organizacije znatno zmanjšajo tveganja, ki jih predstavljajo človeške ranljivosti, in okrepijo svojo splošno varnostno držo.

4 IZBOLJŠANJE POSAMEZNIH UKREPOV KIBERNETSKE VARNOSTI

Izboljšanje posameznih ukrepov kibernetske varnosti je ključnega pomena v dobi, ko digitalne grožnje postajajo vse bolj izpopolnjene. Eden od glavnih korakov, ki jih lahko naredijo posamezniki je krepitev svojih gesel. Kombinacija velikih in malih črk, številk in posebnih znakov, z minimalno dolžino dvanajstih znakov, lahko bistveno poveča varnost. Prav tako je pametno uporabiti edinstvena gesla za različne račune, kar prepreči, da bi ena sama kršitev ogrozila več storitev. Uporaba upraviteljev gesel lahko pomaga posameznikom slediti tem zapletenim geslom, ne da bi si jih bilo potrebno zapomniti (Meeuwisse, 2015).

Drug pomemben ukrep je omogočanje MFA. MFA omogoča dodatno raven varnosti tako, da pred odobritvijo dostopa do računa zahteva še dodatno obliko preverjanja, kot je, na primer, koda besedilnega sporočila ali biometrično skeniranje. Zaradi tega je napadalcem veliko težje pridobiti nepooblaščen dostop »prav tam«.

Poleg upravljanja gesel je bistvenega pomena biti pozoren na uporabljeno programsko opremo in nameščene posodobitve. Posodabljanje operacijskih sistemov, brskalnikov in drugih aplikacij je bistvenega pomena, saj te posodobitve pogosto vključujejo popravke za varnostne ranljivosti, ki bi jih hekerji lahko izkoristili. Uporaba uglednih protivirusnih programov in programov za zaščito pred zlonamerno programsko opremo zagotavlja dodatno obrambo pred zlonamernimi napadi »prav tam«.

Previdnost pri izbiri spletnih strani, ki jih obiščemo in pri kliku na določene povezave je prav tako ključnega pomena. Napadi z lažnim predstavljanjem so še vedno prevladujoča metoda kibernetskih napadalcev za krajo osebnih podatkov. Izobraževanje o pogostih kibernetskih grožnjah in obveščanje o najnovejših varnostnih trendih posameznike okrepi, da prepoznajo morebitna tveganja in se jim izognejo »prav tam«.

"Security is a process, not a product." (Schneier, 2000, str. 257) je zapisal Bruce Schneier v knjigi *Secrets and Lies: Digital Security in a Networked World.* Popolnoma se strinjam, saj menim, da se premalo zavedamo izrednega pomena kibernetske varnosti v današnji dobi in dejstva, da jo je potrebno neprestano razvijati. S sprejetjem proaktivnih ukrepov kibernetske varnosti lahko posamezniki bolje zaščitijo svoje osebne podatke in ohranijo svojo digitalno zasebnost.

4.1 Orodja in najboljše prakse za kibernetsko varnost

Med najpogostejšimi orodji za zagotavljanje kibernetske varnosti so protivirusna programska oprema, požarni zidovi, sistemi za zaznavanje in preprečevanje vdorov ter orodja za šifriranje. Ta orodja imajo ključno vlogo pri zaščiti občutljivih podatkov pred kibernetskimi grožnjami. Organizacije in posamezniki morajo sprejeti najboljše prakse, kot so uporaba močnih gesel, omogočanje večfaktorske avtentikacije, redno posodabljanje programske opreme in izvajanje usposabljanja za ozaveščanje o varnosti za zmanjšanje tveganj. Nadzor omrežja in varnostna kopiranja podatkov dodatno povečujejo odpornost kibernetske varnosti. Ker se kibernetske grožnje razvijajo, je obveščanje o nastajajočih grožnjah in nenehno izboljševanje varnostnih ukrepov bistvenega pomena za zaščito digitalnih sredstev pred zlonamernimi napadi in nepooblaščenim dostopom.

4.1.1 Protivirusna programska oprema

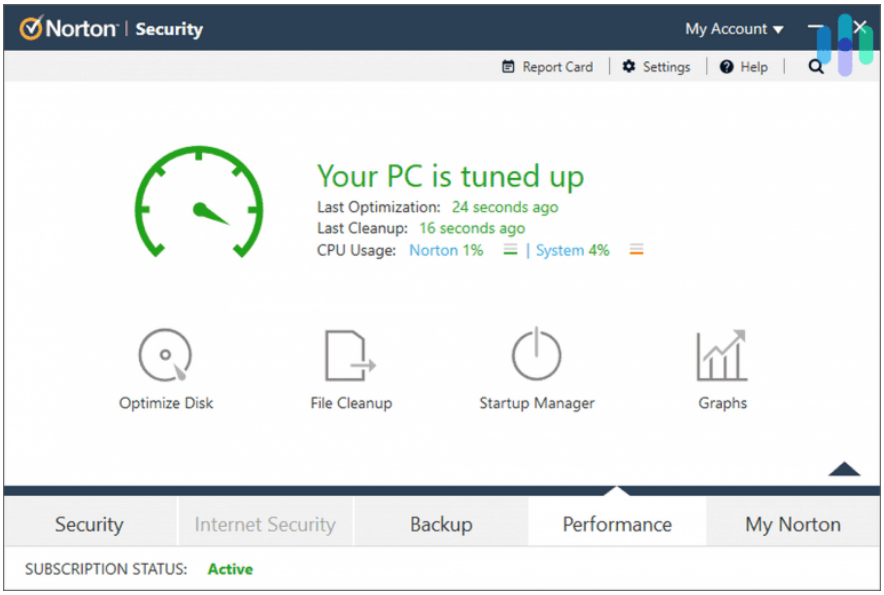
Protivirusna programska oprema je zasnovana za odkrivanje, preprečevanje in odstranjevanje zlonamerne programske opreme, vključno z virusi, črvi, trojanci in vohunsko programsko opremo. Ugledni protivirusni programi, kot so Norton, McAfee in Bitdefender, ponujajo zaščito v realnem času in redne posodobitve za obrambo pred najnovejšimi grožnjami. Protivirusna programska oprema s skeniranjem datotek in spremljanjem aktivnosti sistema pomaga zagotoviti, da zlonamerna koda ne ogrozi varnosti in funkcionalnosti sistema. Uporaba zaupanja vrednega protivirusnega programa je temeljni korak pri varovanju digitalnega okolja (Sikorski & Honig, 2012).

Slika 4: Protivirusni programi

Vir: (https://1000logos.net/best-antivirus-software/)

Lastnosti Norton protivirusnega programa:

- Upravitelj gesel: Varno shranjuje zapletena gesla, podatke o kreditni kartici in druge poverilnice, kar pomaga zaščititi vse račune, ki se uporabljajo.
- Zaščita pred lažnim predstavljanjem in izkoriščanjem: Blokira goljufiva spletna mesta in ščiti pred napadi, ki izkoriščajo ranljivosti v aplikacijah ali operacijskem sistemu.
- Zaščita pred prevarami: Blokira morebitne spletne grožnje, preden zadenejo računalnik, ter preprečuje nepooblaščeno uporabo in prevare.
- Varnost naprave: Zagotavlja sprotno zaščito naprave pred izsiljevalsko programsko opremo, virusi, vohunsko programsko opremo, zlonamerno programsko opremo in drugimi spletnimi grožnjami.

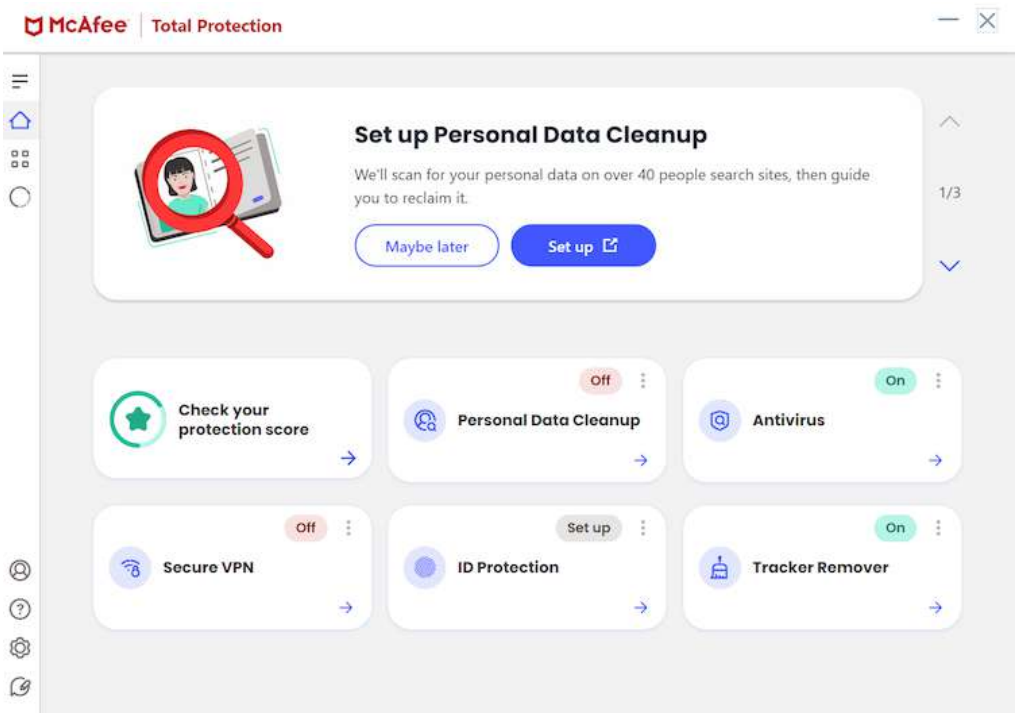


Slika 5: Norton vmesnik

Vir: (https://www.cloudwards.net/bitdefender-vs-norton-antivirus/)

Lastnosti McAfee protivirusnega programa:

- Celovita zaščita pred virusi: Ščiti računalnik pred najnovejšimi grožnjami, vključno z virusi, trojanci, sledilnimi piškotki, rootkiti, boti, vohunsko programsko opremo.
- Avtomatska popravila: Samodejno zazna in nevtralizira večino varnostnih groženj, pri čemer ni potrebno skrbništvo.
- Zaščita pred skeniranjem skriptov: Pregleduje in preprečuje izvajanje potencialno škodljivih skriptov ter blokira sumljive dejavnosti, kot so spreminjanje datotek in spremembe registra.
- Zaščita elektronske pošte: Samodejno pregleda e-pošto in priloge glede aktivnosti virusov, s čimer zagotovi, da komunikacija ostane varna.

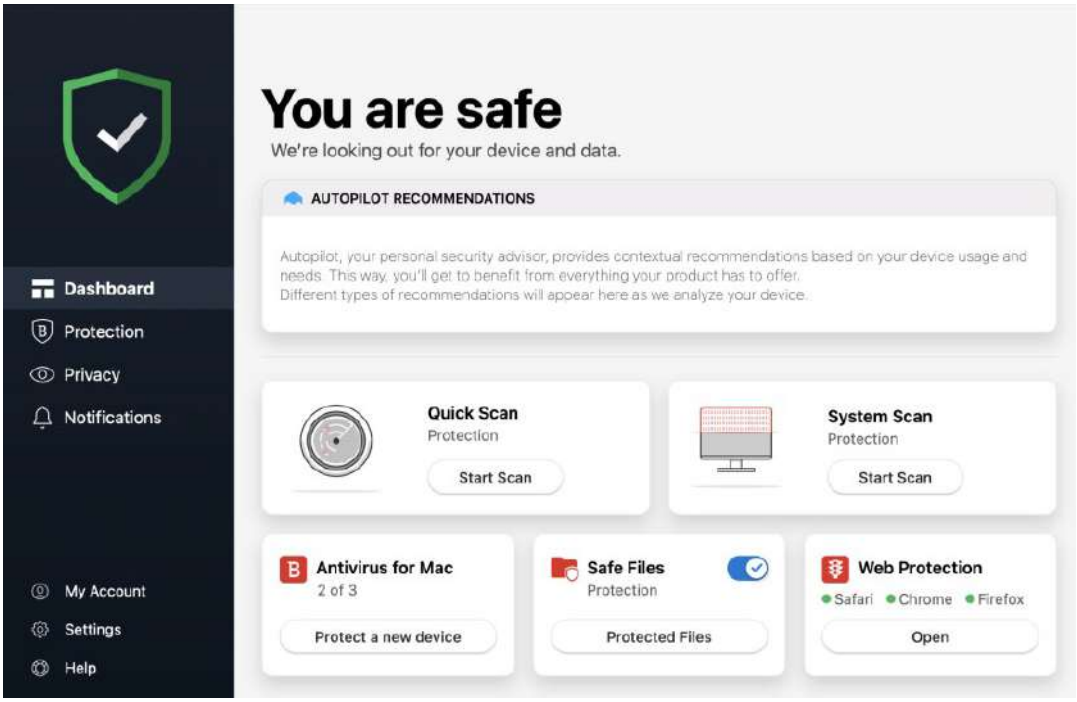


Slika 6: McAfee vmesnik

Vir: (https://cybernews.com/best-antivirus-software/mcafee-vs-norton/)

Lastnosti Bitdefender protivirusnega programa:

- Zaščita v realnem času: Ponuja napredno zaščito v realnem času pred virusi, zlonamerno programsko opremo, izsiljevalsko programsko opremo in drugimi spletnimi grožnjami.
- Večplastna zaščita proti izsiljevalski programski opremi: Funkcija zagotavlja dodatno varnost pred napadi izsiljevalske programske opreme s spremljanjem procesov za sumljivo vedenje in samodejno obnovitvijo vseh ogroženih datotek.
- Napredna zaščita pred grožnjami: Uporablja zaznavanje na podlagi vedenja za prepoznavanje in blokiranje zlonamerne programske opreme in drugih groženj z analiziranjem njihovih dejanj v realnem času.
- Spletna zaščita: Funkcija spletnega filtriranja blokira dostop do zlonamernih spletnih mest in lažnega predstavljanja, kar zagotavlja varno izkušnjo brskanja.

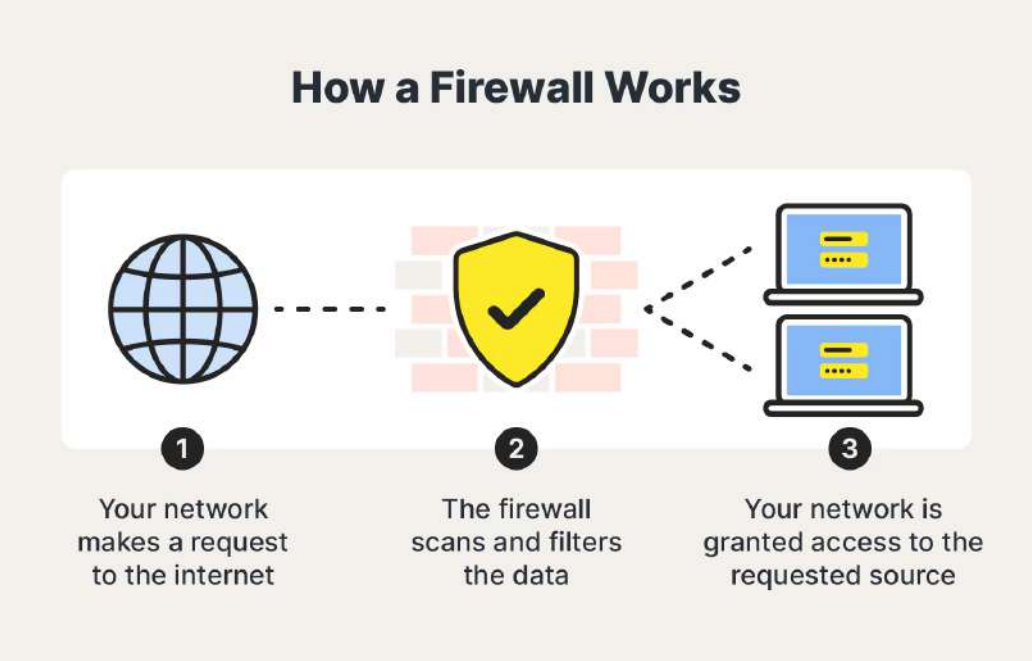


Slika 7: Bitdefender vmesnik

Vir: (https://www.pcmag.com/reviews/bitdefender-antivirus-for-mac)

4.1.2 Požarni zidovi

Požarni zidovi delujejo kot ovira med računalnikom ali omrežjem in potencialnimi grožnjami z interneta. Spremljajo dohodni in odhodni omrežni promet ter dovoljujejo ali blokirajo podatkovne pakete na podlagi niza varnostnih pravil. Požarni zidovi lahko temeljijo na strojni opremi, programski opremi ali kombinaciji obojega. So bistvenega pomena za preprečevanje nepooblaščenega dostopa do omrežja in jih je mogoče konfigurirati za filtriranje prometa do in iz določenih aplikacij ali s spletnih mest, s čimer izboljšajo splošno varnost omrežja. Po presoji je postavitev robustnega požarnega zidu ključnega pomena za zaščito omrežja pred zunanjimi grožnjami (Parker, 2015).



Slika 8: Primer delovanja požarnega zidu

Vir: (https://www.xecor.com/blog/raspberry-pi-firewall-configuration-protection-and-usage)

4.1.3 Upravitelj gesel

Upravitelji gesel, kot so LastPass, Dashlane in 1Password, varno shranjujejo in upravljajo gesla. Ustvarijo močna, edinstvena gesla za vsak račun in po potrebi samodejno izpolnijo poverilnice za prijavo. Z uporabo upraviteljev gesel odpravimo potrebo po pomnjenju več kompleksnih gesel in zmanjšamo tveganje uporabe šibkih ali ponovno uporabljenih gesel. Ta orodja pogosto vključujejo funkcije, kot so varni zapiski, podpora za dvofaktorsko preverjanje pristnosti in opozorila o zlorabi gesla. Zanesljiv upravitelj gesel je nepogrešljiv za vzdrževanje močnih, edinstvenih gesel v vseh računih in izboljšanje splošne kibernetske varnosti (Mitnick, 2017).

Slika 9: Prikaz upravitelja gesel

Vir: (https://www.linkedin.com/pulse/password-managers-how-do-work-safe-paul-riedl-jr-)

5 PREPOZNAVANJE IN ODZIVANJE NA KIBERNETSKE GROŽNJE

Prepoznavanje in odzivanje na znake ogroženosti sistema je ključnega pomena za zaščito pred kibernetskimi grožnjami. Kibernetski kriminalci nenehno razvijajo nove metode napadov, zato je ključnega pomena, da ostanemo pozorni in proaktivni. V nadaljevanju je pregled ključnih indikatorjev in predlaganih odgovorov za pomoč pri ohranjanju celovitosti in varnosti sistemov. Dobro pripravljena odzivna strategija zmanjša škodo, prepreči nadaljnje vdore in zagotovi neprekinjeno poslovanje. Organizacije bi morale oblikovati jasne načrte za odzivanje na incidente, usposobiti zaposlene o ozaveščenosti o varnosti in uporabiti napredna orodja za odkrivanje groženj. Z razumevanjem narave kibernetskih groženj in načinov njihovega učinkovitega reševanja lahko podjetja in posamezniki okrepijo svoj splošni varnostni položaj.

5.1 Ključni indikatorji ogroženih sistemov

Najpogostejši znaki, da je sistem ogrožen, vključujejo nenavaden omrežni promet, zaznavo poskusa nepooblaščenega dostopa in nenavadno vedenje sistema. Drugi indikatorji vključujejo nepričakovane spremembe datotek, pogoste zrušitve sistema, počasno delovanje, nepooblaščene namestitve programske opreme in sumljive poskuse prijave z neznanih lokacij. Uporabniki lahko opazijo tudi povečano porabo procesorja ali pomnilnika, nepričakovana pojavna okna ali onemogočene varnostne funkcije. E-poštni računi, ki pošiljajo neželeno pošto ali nenadne spremembe sistemskih konfiguracij, so tudi opozorilni znaki. Hitro prepoznavanje in obravnavanje teh indikatorjev je ključnega pomena za preprečevanje nadaljnje škode. Redne varnostne revizije in spremljanje v realnem času lahko pomagajo odkriti in ublažiti grožnje, preden se stopnjujejo.

5.1.1 Nenavaden omrežni promet

Indikatorji:

- Skoki odhodnega prometa: Če pride do nepričakovanega povečanja odhodnega prometa, zlasti na neznane ali sumljive naslove IP, lahko to pomeni, da gre za izkoriščanje podatkov.
- Nenavadni protokoli ali vrata: Uporaba neobičajnih protokolov ali nepričakovanih vrat lahko nakazuje nepooblaščeno komunikacijo ali prenos podatkov.

- Povečan promet izven delovnega časa: Napadalci lahko delujejo v času izven konic, da bi se izognili odkritju, kar vodi do neobičajnih prometnih vzorcev v teh obdobjih.

Odziv:

- Analiza prometa: Uporabimo orodja za nadzor omrežja, kot je Wireshark ali sisteme za zaznavanje vdorov (IDS), da prepoznamo in natančno preučimo vir nepravilnosti.
- Segmentacija omrežja: Izoliramo ogrožene segmente, da preprečimo širjenje grožnje.
- Prilagoditve požarnega zidu: Posodobimo pravila požarnega zidu, da blokiramo komunikacijo z znanimi zlonamernimi naslovi IP, s čimer zagotovimo, da sistemi IDS/IPS opozarjajo na sumljiv promet.

5.1.2 Poskusi nepooblaščenega dostopa

Indikatorji:

- Neuspeli poskusi prijave: Veliko število neuspešnih poskusov prijave, zlasti z enega naslova IP ali nenavadnih lokacij, lahko pomeni napade s surovo silo ali napade s polnjenjem poverilnic.
- Uspešne prijave z neznanih naprav/lokacij: Prijave z nepričakovanih lokacij ali naprav, ki uporabljajo zakonite poverilnice, lahko pomenijo ogroženost poverilnic.
- Neprepoznani uporabniški računi: Novi, nepooblaščeni računi s povišanimi privilegiji so pomemben pokazatelj kršitve.

Odziv:

- Zaklepanje računa: Takoj zaklenemo prizadete račune in zahtevamo ponastavitev gesla. Raziščemo, da ugotovimo, ali so bile poverilnice ogrožene.
- Pregled nadzora dostopa: Pregledamo in poostrimo politike nadzora dostopa, da zagotovimo, da imajo uporabniki samo potrebne privilegije in da so vsi računi zakoniti.
- Omogočena večstopenjska avtentikacija (MFA): Implementiramo MFA v vse sisteme, da dodamo dodatno varnostno plast in otežimo nepooblaščen dostop.

5.1.3 Neobičajno vedenje sistema

Indikatorji:

- Težave z zmogljivostjo: Nepričakovana počasnost, visoka poraba procesorja ali pomnilnika ali pogoste zrušitve lahko kažejo na delo zlonamernih procesov.
- Nepričakovani vnovični zagoni sistema: Ponavljajoči se, nepojasnjeni vnovični zagoni so lahko znak namestitve zlonamerne programske opreme ali drugih zlonamernih dejavnosti.
- Nepooblaščene spremembe: Spremembe sistemskih nastavitev ali konfiguracij brez dovoljenja pogosto kažejo na kršitev.

Odziv:

- Prekinitev procesa: Prepoznamo in zaključimo sumljive procese z orodji, kot sta Upravitelj opravil (Windows) ali top/htop (Linux).
- Skeniranje zlonamerne programske opreme: Izvedemo celovito skeniranje zlonamerne programske opreme z najnovejšimi protivirusnimi orodji in odstranimo vse zaznane grožnje.
- Obnovitev iz varnostne kopije: Če so kritični sistemi ogroženi, jih obnovimo iz čiste, posodobljene varnostne kopije. Redno testiramo in posodabljamo varnostne kopije.

5.1.4 Sumljive datoteke ali programska oprema

Indikatorji:

- Nove ali neprepoznane datoteke: Pojav neznanih datotek, zlasti v sistemskih imenikih, lahko nakazuje zlonamerno dejavnost.
- Nepričakovana programska oprema: Nepooblaščena namestitev programske opreme je lahko znak orodij za oddaljeni dostop (RAT), zapisovalcev tipk ali drugih zlonamernih aplikacij.
- Spremenjene sistemske datoteke: Spremembe kritičnih sistemskih datotek brez pooblastila so močan znak ogroženosti.

Odziv:

- Datotečna karantena: Izoliramo sumljive datoteke, da preprečimo nadaljnje izvajanje, in jih analiziramo v okolju peskovnika glede zlonamernega vedenja.

- Odstranitev programske opreme: Odstranimo nepooblaščeno programsko opremo in raziščemo, kako je bila nameščena, da preprečimo prihodnje incidente.
- Nadzor celovitosti datotek: Naložimo orodja, ki spremljajo in opozarjajo na spremembe kritičnih sistemskih datotek, kar pomaga pri zgodnjem odkrivanju nepooblaščenih sprememb.

5.2 Takojšnji in dolgoročni ukrepi

Za učinkovito odzivanje na kibernetske grožnje je potrebna kombinacija takojšnjih ukrepov in dolgoročnih strategij. Tukaj je podroben pristop k obvladovanju teh situacij.

5.2.1 Takojšnje zadrževanje in preiskava

Zadrževanje je prva prednostna naloga, ko se odkrije grožnja. Hitro zadrževanje omeji širjenje napada in zmanjša potencialno škodo.

Koraki:

1. Izoliranje prizadetih sistemov: Takoj izključimo ogrožene sisteme iz omrežja. To lahko storimo tako, da onemogočimo omrežne vmesnike ali fizično odstranimo povezave. Izolacija teh sistemov pomaga preprečiti, da bi se napadalec premaknil stransko po omrežju.
2. Prestavitev sumljivih datotek v karanteno: Uporabimo orodja za zaščito končne točke v karanteno vseh datotek, ki se zdijo sumljive. To dejanje ustavi izvajanje ali širjenje datotek in zagotovi čas za oceno situacije.

Preiskava sledi zadrževanju in se osredotoča na razumevanje kršitve.

Koraki:

1. Izvedba forenzične analize: Začnemo temeljito forenzično preiskavo, da ugotovimo, kako je prišlo do kršitve, kateri sistemi so bili prizadeti in kateri podatki so morda bili ukradeni ali dostopni. Razumevanje vektorja napada je ključnega pomena za preprečevanje prihodnjih incidentov.
2. Ohranitev dokazov: Skrbno zbiramo in shranimo dnevnike, izpise pomnilnika in druge kritične podatke za analizo. Ti dokazi so bistveni tako za razumevanje napada kot za morebitne pravne postopke. Zagotovimo, da ti dokazi ostanejo nespremenjeni.

5.2.2 Odstranjevanje in okrevanje

Ko je grožnja obvladana, je naslednja faza odstranjevanje.

Koraki:

1. Odstranitev zlonamerne programske opreme in groženj: Uporabimo posodobljena orodja proti zlonamerni programski opremi, da odstranimo morebitno zlonamerno programsko opremo. Zagotovimo temeljit pregled celotnega omrežja in sistemov, da odstranimo vse dolgotrajne grožnje.
2. Popravljanje ranljivosti: Identificiramo in popravimo ranljivosti, ki so bile izkoriščene med napadom. To lahko zahteva uporabo varnostnih popravkov, ponovno konfiguracijo nastavitev ali nadgradnjo zastarele strojne ali programske opreme. Odpravljanje teh ranljivosti je ključnega pomena za preprečitev ponovitve.

Sledi faza okrevanja, ki se osredotoča na ponovno vzpostavitev normalnega delovanja.

Koraki:

1. Obnovitev prizadetih sistemov: Uporabimo čiste, varne varnostne kopije za obnovitev prizadetih sistemov. Pred uporabo teh varnostnih kopij preverimo, ali so brez zlonamerne programske opreme in ali so posodobljene.
2. Preizkus sistema pred ponovnim povezovanjem: Pred ponovnim povezovanjem sistemov z omrežjem izvedemo temeljito testiranje, da potrdimo, da je bila grožnja popolnoma izkoreninjena in da sistemi delujejo pravilno. Ta korak pomaga preprečiti ponovno vnašanje ranljivosti v omrežje.

5.2.3 Pregled in izboljšave po incidentu

Ko mine neposredna kriza, je pomembno opraviti pregled po incidentu in narediti izboljšave. Namen pregleda po incidentu je razumeti, kaj se je zgodilo in kako izboljšati prihodnje odzive.

Koraki:

1. Analiza incidenta: Opravimo podroben pregled kršitve. Ugotovimo, kaj se je zgodilo, kako je bilo ravnano in kje so bile pomanjkljivosti. Prepoznavanje teh incidentov je ključno za krepitev obrambe in strategij odzivanja.

2. Posodobitev načrta za odzivanje na incidente: Na podlagi pridobljenih izkušenj pregledamo svoj načrt za odzivanje na incidente. Te ugotovitve vključimo v prihodnje programe usposabljanja in simulacije za izboljšanje pripravljenosti.

Izboljšanje se osredotoča na krepitev obrambe in zagotavljanje dolgoročne varnosti.

Koraki:

1. Izboljšava varnostnih ukrepov: Po potrebi uvedemo strožje varnostne ukrepe. To lahko vključuje boljše nadzorne sisteme, strožji nadzor dostopa in povečano usposabljanje zaposlenih, da se zagotovi, da so vsi na tekočem z najboljšimi praksami.
2. Izvajanje rednih vaj: Redno preizkušamo posodobljen načrt odzivanja na incidente s simuliranimi kibernetskimi napadi. Te vaje pomagajo zagotoviti, da je organizacija pripravljena na učinkovit odziv na prihodnje grožnje.

Usposabljanje in ozaveščanje zaposlenih je stalna potreba po ohranjanju močne varnostne drže.

Koraki:

1. Stalno usposabljanje: Zagotovimo stalno izobraževanje o najnovejših kibernetskih grožnjah in najboljših praksah glede varnosti. Dobro obveščeni zaposleni so kritična obrambna linija.
2. Simulacija lažnega predstavljanja: Izvajamo redne simulacije lažnega predstavljanja, da usposobimo zaposlene, da prepoznajo poskuse lažnega predstavljanja in se nanje odzovejo. Lažno predstavljanje je običajna metoda, ki jo uporabljajo napadalci, in usposabljanje lahko znatno zmanjša tveganje za uspešne napade.

6 VLOGA UMETNE INTELIGENCE V KIBERNETSKI VARNOSTI

S hitro digitalno transformacijo v različnih gospodarskih panogah so grožnje kibernetski varnosti postale bolj izpopolnjene in pogoste. Tradicionalni varnostni ukrepi pogosto težko sledijo razvijajočim se kibernetskim grožnjam. Umetna inteligenca (AI) se je izkazala kot močno orodje na področju kibernetske varnosti, ki zagotavlja izboljšane zmožnosti odkrivanja groženj, odzivanja in preprečevanja. Varnostni sistemi, ki jih poganja AI, pomagajo organizacijam pri proaktivni obrambi pred kibernetskimi napadi, zaradi česar so bistveni sestavni del sodobnih strategij kibernetske varnosti.

6.1 Ključna področja, kjer se AI uporablja v kibernetski varnosti

6.1.1 Odkrivanje in preprečevanje groženj

Sistemi, ki jih poganja AI, lahko analizirajo ogromne količine podatkov v realnem času in prepoznajo potencialne grožnje, preden povzročijo škodo. Algoritmi strojnega učenja zaznajo vzorce, ki kažejo na zlonamerno programsko opremo, lažno predstavljanje in druge kibernetske grožnje.

6.1.2 Vedenjska analiza

Umetna inteligenca lahko spremlja vedenje uporabnikov in zazna nepravilnosti, ki lahko kažejo na kršitev varnosti. Na primer, če zaposleni nenadoma dostopa do občutljivih datotek izven običajnega delovnega časa, lahko AI to vedenje označi za nadaljnjo preiskavo.

6.1.3 Samodejni odziv na incidente

Varnostni sistemi, ki jih poganja AI, lahko avtomatizirajo odzive na kibernetske grožnje, skrajšajo odzivni čas in zmanjšajo škodo. Umetna inteligenca lahko na primer izolira okuženi sistem iz omrežja, da prepreči širjenje zlonamerne programske opreme.

6.1.4 Odkrivanje goljufij

Finančne institucije uporabljajo AI za odkrivanje goljufivih transakcij v realnem času z analizo vzorcev transakcij. Umetna inteligenca lahko prepozna neobičajno vedenje pri porabi in označi morebitne goljufive dejavnosti za pregled.

6.1.5 Zaznavanje lažnega predstavljanja

E-poštni filtri, ki temeljijo na umetni inteligenci, analizirajo dohodna sporočila, da zaznajo poskuse lažnega predstavljanja. Obdelava naravnega jezika pomaga prepoznati sumljiva e-poštna sporočila, ki posnemajo zakonite vire.

6.1.6 Upravljanje ranljivosti

AI pomaga pri prepoznavanju ranljivosti programske opreme s pregledovanjem in analiziranjem sistemov za morebitne slabosti. Prednost daje ranljivostim na podlagi dejavnikov tveganja, s čimer pomaga organizacijam najprej odpraviti kritične varnostne napake.

6.2 Prednosti umetne inteligence in kibernetske varnosti

- Hitrost in učinkovitost: Umetna inteligenca lahko analizira in obdela velike količine podatkov hitreje kot ljudje ter prepozna grožnje v realnem času.
- Razširljivost: Rešitve kibernetske varnosti, ki jih poganja AI, se lahko prilagodijo naraščajočemu obsegu in kompleksnosti kibernetskih groženj.
- Zmanjšanje števila človeških napak: Avtomatizirano zaznavanje groženj in odziv nanje zmanjša odvisnost od človeških analitikov, kar zmanjša napake in nadzor.
- Proaktivno preprečevanje groženj: Umetna inteligenca predvidi in prepreči kibernetske napade, preden se zgodijo, s čimer izboljša splošno varnost.

6.3 Izzivi in omejitve

- Lažni pozitivni in lažni negativni učinki: Umetna inteligenca lahko zakonite dejavnosti označi kot grožnje ali ne zazna prefinjenih napadov.
- Zaskrbljenost glede zasebnosti podatkov: AI se opira na velike nabore podatkov, kar vzbuja pomisleke glede zasebnosti in varnosti podatkov.

- Visoki stroški implementacije: Razvoj in vzdrževanje rešitev kibernetske varnosti, ki jih poganja AI, je lahko drago.
- Kontradiktornost AI: Kibernetski kriminalci uporabljajo AI tudi za razvoj naprednejših tehnik napadov, kar zahteva nenehno izboljševanje varnostnih ukrepov AI.

Umetna inteligenca spreminja kibernetsko varnost z zagotavljanjem hitrejših, pametnejših in bolj proaktivnih obrambnih mehanizmov. Medtem ko umetna inteligenca ponuja pomembne prednosti, predstavlja tudi izzive, s katerimi se morajo organizacije soočiti, da bi povečale svojo učinkovitost. Ker se kibernetske grožnje še naprej razvijajo, bo imela umetna inteligenca vedno bolj ključno vlogo pri zaščiti digitalnih sredstev in zagotavljanju odpornosti kibernetske varnosti.

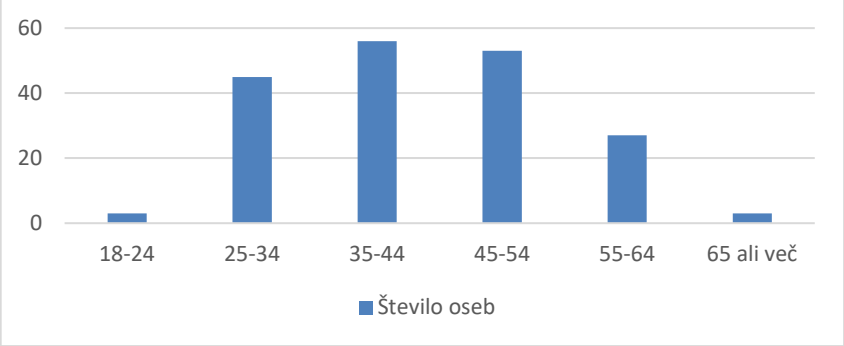
7 REZULTATI ANKETE O OZAVEŠČENOSTI O KIBERNETSKI VARNOSTI

V današnjem vse bolj digitalnem svetu je kibernetska varnost postala bistvenega pomena ne le za zaščito organizacijskih sredstev, temveč tudi za varovanje zasebnosti in podatkov posameznikov. Ker kibernetske grožnje postajajo vse bolj izpopolnjene, pomena ozaveščenosti o kibernetski varnosti med splošno javnostjo in na delovnih mestih ni mogoče preceniti.

Ta anketa je bila izvedena za oceno trenutne ravni ozaveščenosti o kibernetski varnosti, praks in potreb po usposabljanju med raznoliko skupino anketirancev. Izvedena je bila v javnem zavodu, ki vsebuje obsežne podatkovne baze z občutljivimi informacijami strank, in je lahko potencialna tarča kibernetskih napadov. Zato je ključnega pomena, da ima ustanova vzpostavljene robustne kibernetske varnostne ukrepe za zaščito svojih sistemov in podatkov, s čimer zagotavlja nemoteno delovanje in varnost strank. Anketa je bila izvedena med zaposlenimi v ustanovi, preko spleta. Vzorec vsebuje 187 anketirancev, anketo je izpolnilo 142 žensk in 45 moških. Zbrani podatki zagotavljajo vpogled v seznanjenost anketirancev s terminologijo kibernetske varnosti, njihove osebne in organizacijske izkušnje s kibernetskimi incidenti, njihovo uporabo zaščitnih praks, kot sta večfaktorska avtentikacija in upravljanje gesel, ter njihovo zaupanje v prepoznavanje kibernetskih groženj.

Vprašanje: starost

Med anketiranimi je bilo 45 oseb starih med 25–34 let, 56 oseb med 35–44, 53 med 45–54 let ter 27 oseb starih med 55–64. Na podlagi javnih raziskav prevladuje mnenje, da je raven ozaveščenosti o kibernetski varnosti najvišja pri skupini med 25–34 let, ki je odraščala z digitalno tehnologijo.

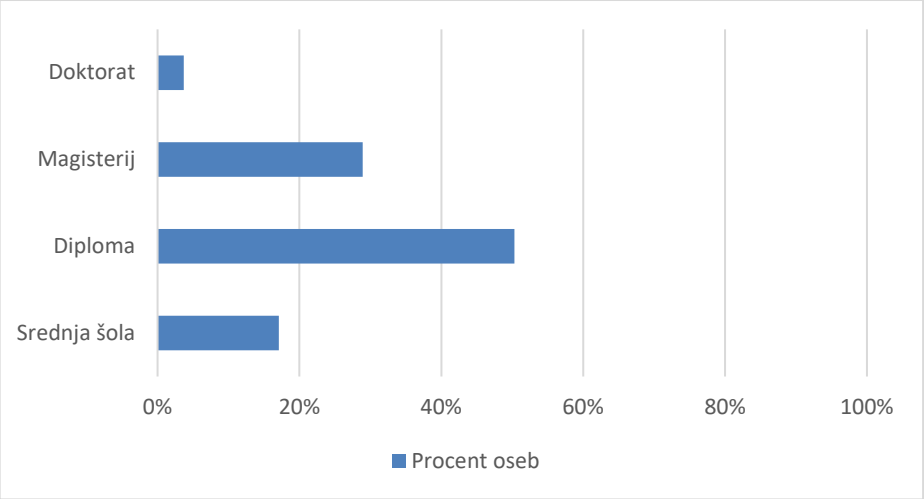


Grafikon 1: Prikaz starosti anketirancev

Vir: (Lasten vir)

Vprašanje: stopnja izobrazbe

Med anketiranimi ima 17 % zaključeno srednješolsko izobrazbo, 50 % jih ima diplomo, 29 % magisterij ter 4 % doktorat. Stopnja izobrazbe anketirancev naj bi bila povezana s stopnjo ozaveščenosti o kibernetski varnosti in lastnimi izkušnjami na tem področju.

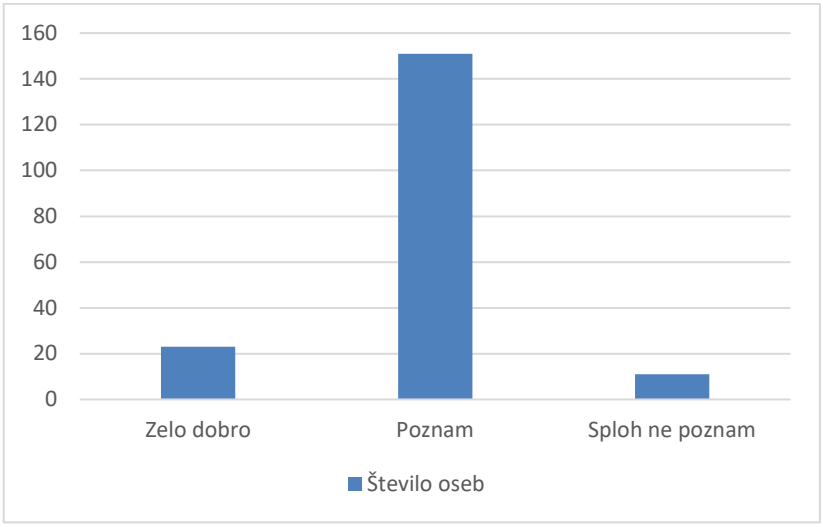


Grafikon 2: Prikaz izobrazbe anketirancev

Vir: (Lasten vir)

Vprašanje: poznavanje koncepta "kibernetski napad"

Večina anketirancev (151 oseb) je seznanjena s konceptom "kibernetski napad", 11 anketirancev ne pozna tega koncepta, zelo dobro pa je ozaveščenih 23 anketirancev. Načeloma ta rezultat kaže na dobro ozaveščenost o konceptu "kibernetski napad", ki pa jo je mogoče nadgraditi z dodatnim izobraževanjem.

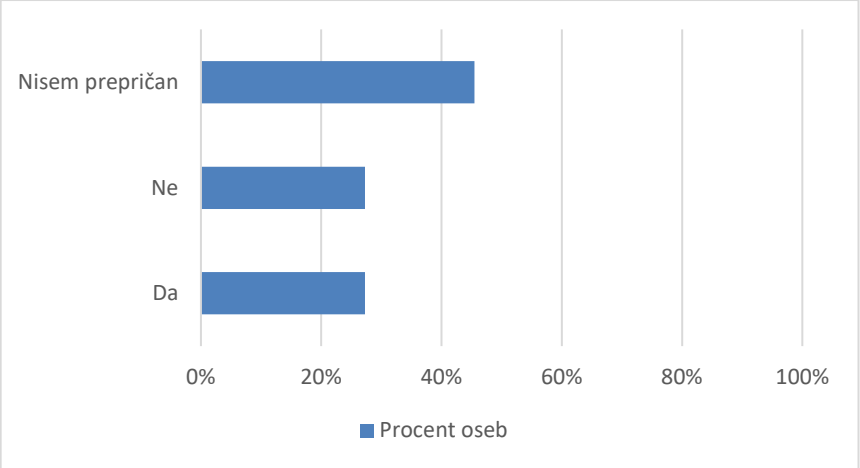


Grafikon 3: Prikaz poznavanja koncepta "kibernetski napad"

Vir: (Lastni vir)

Vprašanje: Ali ste bili vi ali vaša organizacija že kdaj žrtev kibernetskega napada?

46 % anketirancev ni prepričanih, ali so že bili žrtev kibernetskega napada, 27 % jih ni bilo izpostavljenih takemu napadu in 27 % jih je že bilo žrtev kibernetskega napada. Visoka stopnja negotovosti (46 %) glede preteklih napadov kaže na pomanjkanje ozaveščenosti o kibernetski varnosti in o prepoznavanju kibernetskih incidentov.

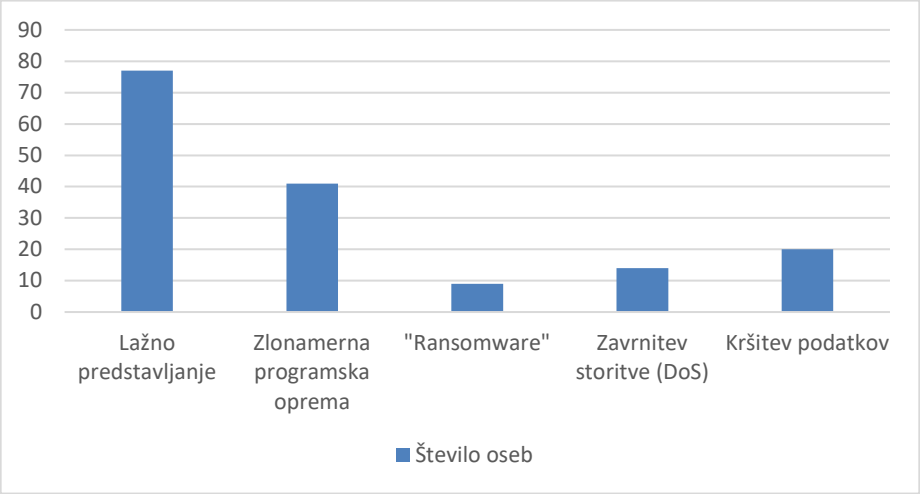


Grafikon 4: Prikaz ozaveščanja ali so bili anketiranci kibernetsko napadeni

Vir: (Lasten vir)

Vprašanje: Vrste doživetih kibernetskih incidentov

Na to vprašanje je odgovorilo 94 anketirancev, veliko jih je označilo po več različnih napadov. Največ incidentov (77 odgovorov) so bile prevare z lažnim predstavljanjem in zlonamerna programska oprema (41 odgovorov).

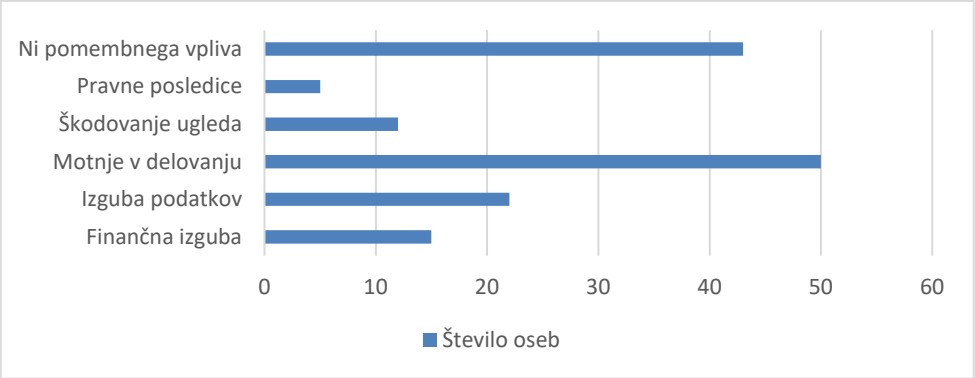


Grafikon 5: Prikaz napadov, ki so jih doživeli anketiranci

Vir: (Lasten vir)

Vprašanje: vpliv in posledice kibernetskega napada

Med skupno 105 odgovori jih 50 navaja motnje v delovanju, 43 je odgovorov, da napad ni pustil pomembnih posledic, 22 odgovorov je izguba podatkov, 15 finančna izguba, 12 škodovanje ugleda ter 5 odgovorov pravne posledice. Glede na števila odgovorov so anketiranci dokaj dobro ozaveščeni o možnostih kibernetskih napadov (104), veliko jih je čutilo posledice. Iz grafikona pa je razvidno tudi visoko število odgovorov, ki jih lahko razumemo kot morebitno podcenjevanje tveganj. Vsekakor bi bilo priporočljivo dodatno izobraževanje in usposabljanje osebja na temo kibernetske varnosti.

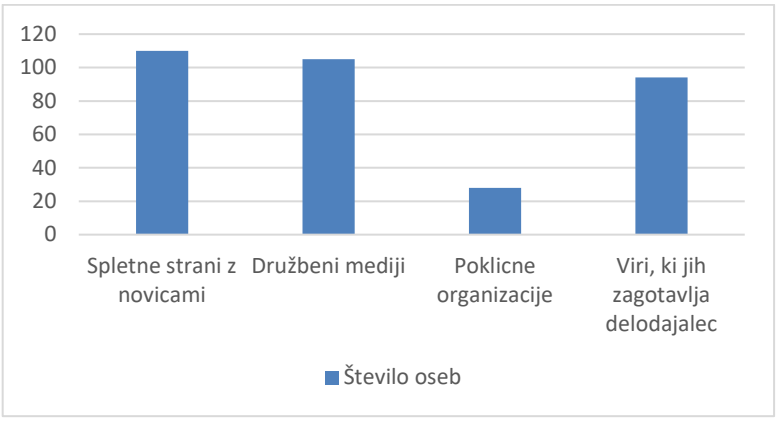


Grafikon 6: Prikaz vpliva kibernetskega napada na anketirance

Vir: (Lasten vir)

Vprašanje: Primarni viri informacij o kibernetski varnosti

Možnih je bilo več odgovorov. Večina anketirancev je informirana o kibernetski varnosti preko spleta (110 odgovorov), preko družbenih medijev (105 odgovorov) ter iz virov, ki jih zagotavlja delodajalec (94 odgovorov). Glede na verodostojnost podatkov iz spleta in družbenih medijev bi bilo pomembno, da zaposleni preverja kredibilnost podatkov (viri pri delodajalcu in poklicne organizacije).

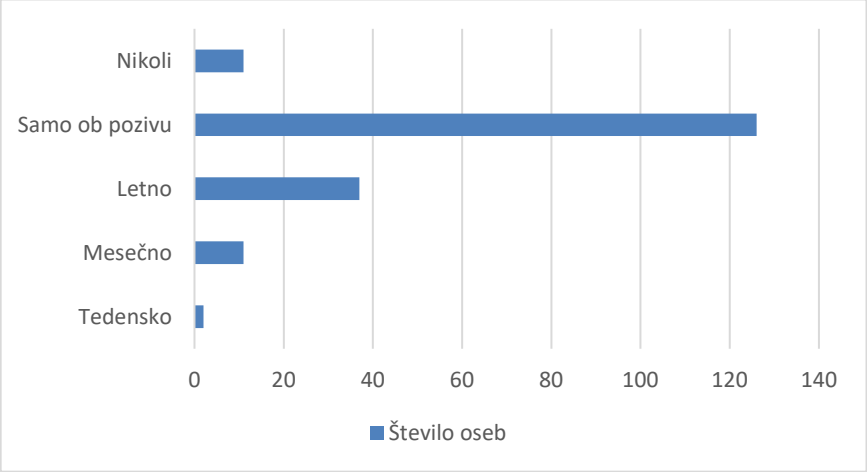


Grafikon 7: Prikaz od kod anketiranci dobijo informacije o kibernetski varnosti

Vir: (Lasten vir)

Vprašanje: Pogostost menjave gesel

126 anketirancev menja geslo samo ob pozivu, 37 jih menjuje letno, 11 anketirancev menja geslo mesečno, 11 anketirancev še ni nikoli menjalo gesla. Posodabljanje gesel samo ob pozivu je dovolj kredibilno le v primeru, da ima organizacija strukturirano poklicno organizacijo. Posodabljanje gesel na lastno iniciativo izven organizacije sicer odraža pozitivne navade, bi pa lahko zanašanje na varno shranjevanje (kot je upravitelj gesel) dodatno okrepilo varnost računa.

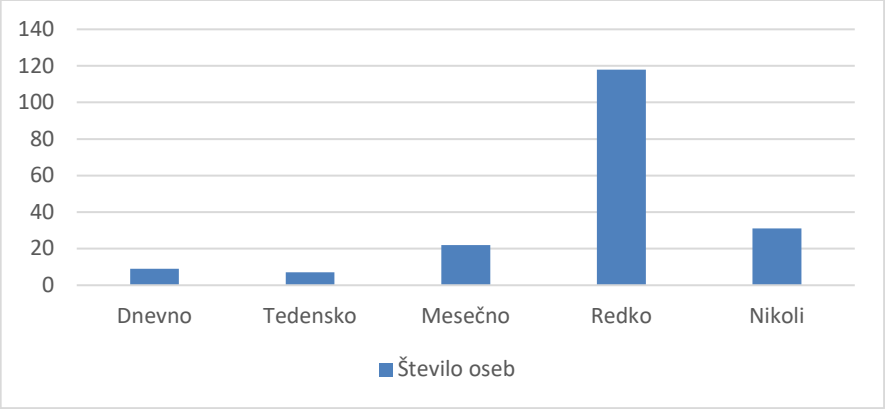


Grafikon 8: Prikaz pogostosti menjave gesla

Vir: (Lasten vir)

Vprašanje: Pogostost varnostnih kopij podatkov

Večina anketirancev (156) varnostno kopira svoje podatke, kar kaže na splošno zavedanje pomena varstva podatkov. Podmnožica (31) je nakazala nedosledne prakse, kar kaže na možna tveganja pri preprečevanju izgube podatkov.

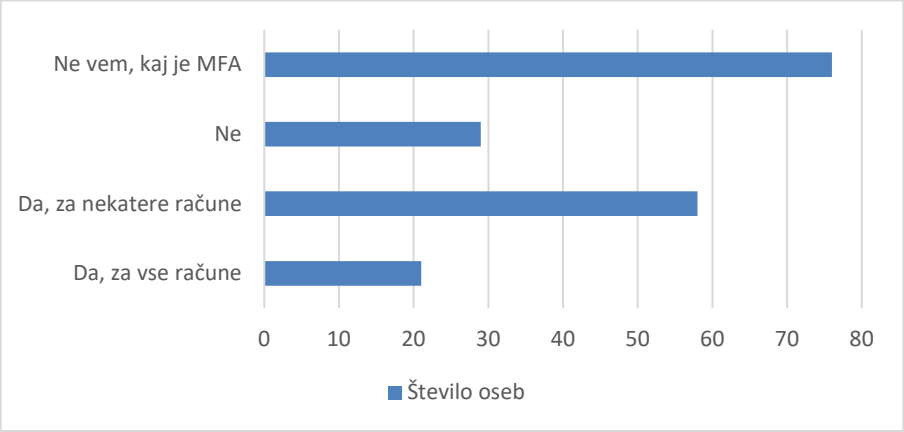


Grafikon 9: Prikaz kolikokrat anketiranci varnostno kopirajo podatke

Vir: (Lasten vir)

Vprašanje: Uporaba večfaktorske avtentikacije (MFA)

21 anketirancev uporablja MFA za vse račune, 58 anketirancev uporablja MFA za nekatere račune, 29 anketirancev sploh ne uporablja MFA in 76 anketirancev je odgovorilo, da ne poznajo večfaktorske avtentikacije. Rezultat, da se več kot polovica anketirancev ne zaveda, kaj je MFA oziroma je ne uporablja, predstavlja jasno področje za izboljšave, saj je MFA temeljni ukrep proti nepooblaščenemu dostopu.

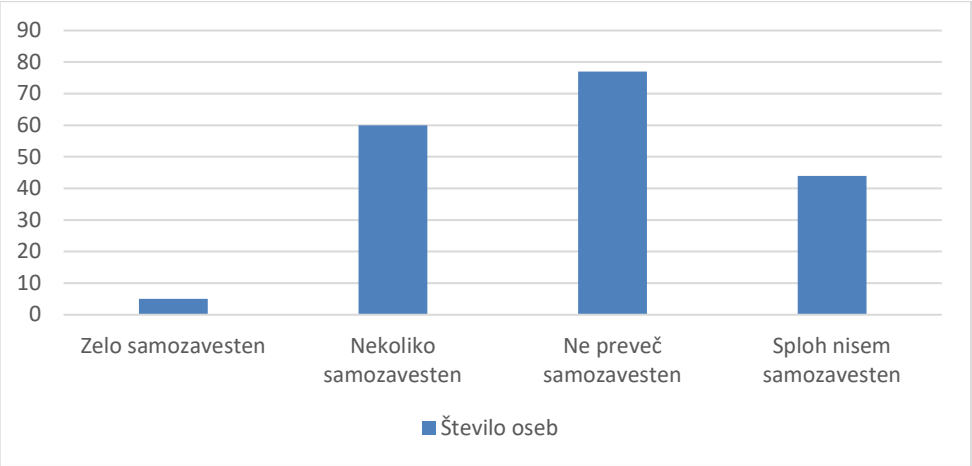


Grafikon 10: Prikaz uporabe MFA med anketiranci

Vir: (Lasten vir)

Vprašanje: Zaupanje v prepoznavanje in preprečevanje kibernetskih napadov

Zelo samozavestnih je 5 anketirancev, 60 jih je nekoliko samozavestnih, 77 jih ni preveč samozavestnih in 44 jih sploh ni samozavestnih. Celostno gledano je samozavest o prepoznavanju in preprečevanju kibernetskih napadov dokaj nizka, kar kaže na visoko potrebo po usposabljanju na tem področju.

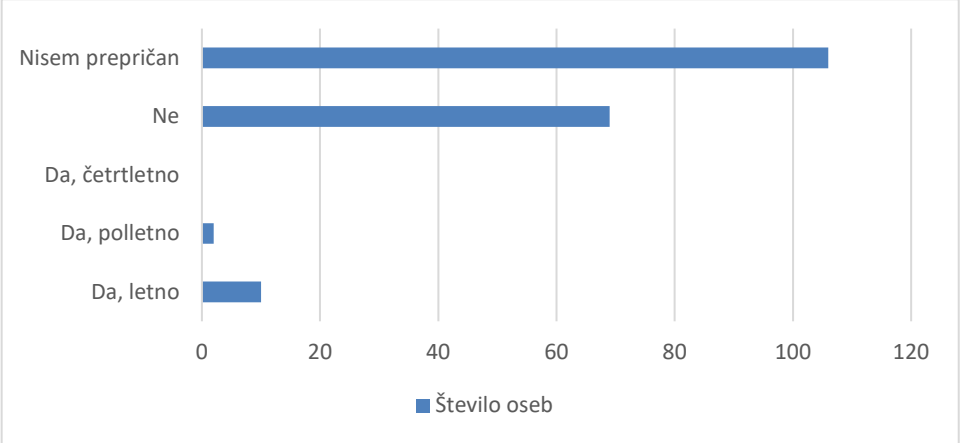


Grafikon 11: Prikaz samozavesti anketirancev glede kibernetskih napadov

Vir: (Lasten vir)

Vprašanje: Pogostost usposabljanja o kibernetski varnosti v organizaciji

Večina anketirancev (106) ni prepričana ali organizacija ponuja takšno usposabljanje, 69 anketirancev meni, da organizacija ne ponuja tovrstnega usposabljanja. Le 12 anketirancev trdi, da organizacija nudi usposabljanje o kibernetski varnosti. Podatki kažejo, da je potrebno izboljšati informiranje o tovrstnih usposabljanjih v tej organizaciji.

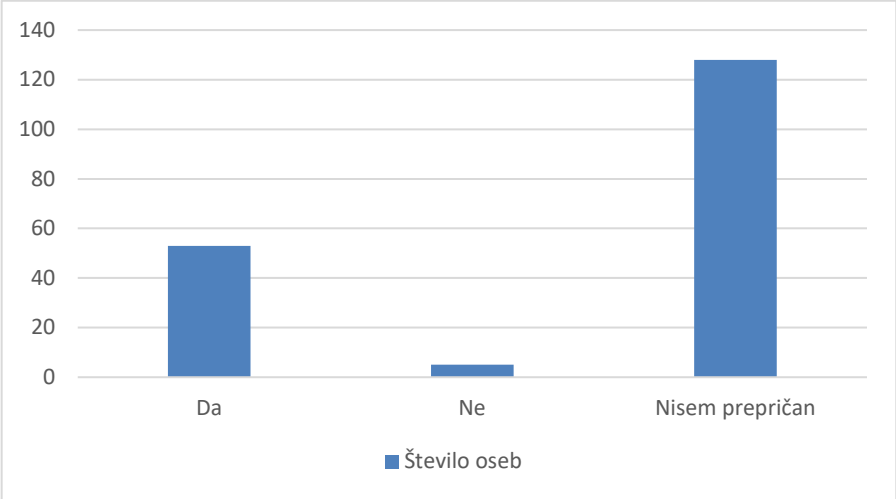


Grafikon 12: Prikaz informiranosti o usposabljanju o kibernetski varnosti v organizaciji

Vir: (Lasten vir)

Vprašanje: Obstoj poklicne organizacije

V ustanovi obstaja poklicna organizacija. 128 anketirancev ni prepričanih, 5 anketirancev je odgovorilo, da takšne organizacije ni, 53 anketirancev je seznanjenih, da takšna organizacija v ustanovi obstaja. Podatki kažejo, da je potrebno izboljšati informiranje o poklicni organizaciji.

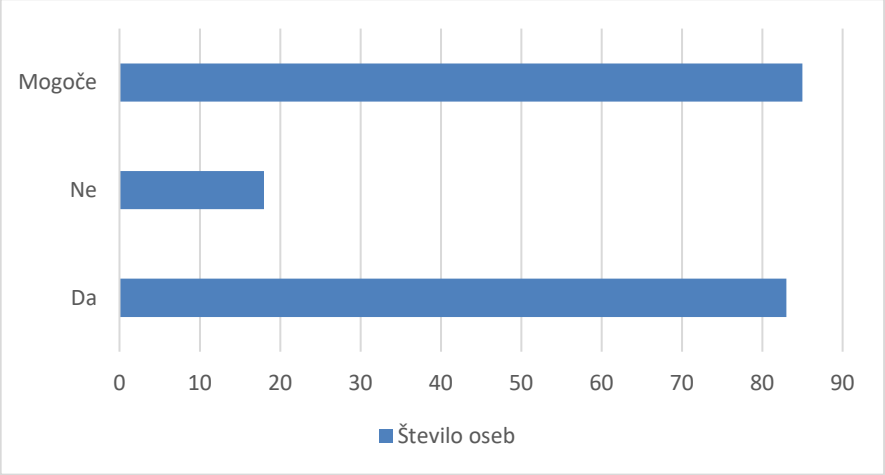


Grafikon 13: Prikaz ali so anketiranci seznanjeni z obstojem poklicne organizacije

Vir: (Lasten vir)

Vprašanje: Zanimanje za usposabljanje ali delavnice o kibernetski varnosti

Spodbuden podatek je, da je večina anketirancev pokazala zanimanje za usposabljanje ali delavnice o kibernetski varnosti (83 je odgovorilo »da« in 85 je odgovorilo »mogoče«). Le 18 anketirancev takšno usposabljanje ne zanima. Ustanova bi lahko izkoristila to zanimanje za praktična usposabljanja, osredotočena na prepoznavanje groženj in varno vedenje.



Grafikon 14: Prikaz zanimanja anketirancev za kibernetske delavnice

Vir: (Lasten vir)

Rezultati ankete poudarjajo ključne vidike ozaveščenosti anketirancev o kibernetski varnosti. Večina anketirancev pozna koncept kibernetskih napadov, vendar pa jih 46 % ni prepričanih, ali so bili tarča, kar kaže na pomanjkanje ozaveščenosti pri odkrivanju kibernetskih groženj. Prevare z lažnim predstavljanjem in zlonamerna programska oprema so bili najpogosteje prijavljeni incidenti.

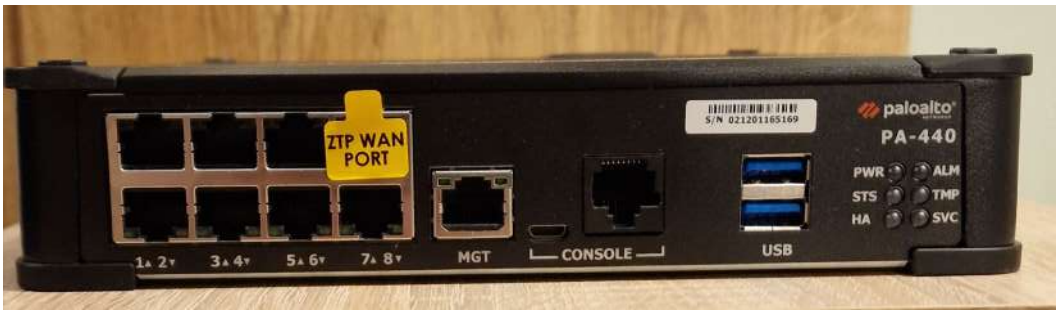
Veliko anketirancev se za informacije o kibernetski varnosti zanaša na spletne vire in družbene medije, večina spremeni gesla le ob pozivu, uporaba večfaktorske avtentikacije (MFA) je nizka, prav tako pa je na splošno nizko tudi lastno zaupanje v prepoznavanje in preprečevanje kibernetskih napadov. Vse to kaže na potrebo po dodatnem izobraževanju in usposabljanju.

Zdi se, da je organizacijsko usposabljanje na področju kibernetske varnosti omejeno, saj mnogi niso prepričani, ali takšna usposabljanja obstajajo. Podobno je pri ozaveščenosti o poklicnih organizacijah za kibernetsko varnost v sami ustanovi, saj večina anketirancev ni prepričana ali takšna organizacija obstaja. Vendar je dober podatek, da večina anketirancev kaže zanimanje za dodatno usposabljanje o kibernetski varnosti. To predstavlja priložnost za izboljšanje znanja o kibernetski varnosti s strukturiranim izobraževanjem, ter spodbujanje k boljšim varnostnim navadam in odpornosti proti kibernetskim grožnjam.

8 VZPOSTAVLJANJE POŽARNEGA ZIDU PALO ALTO

8.1 Postopek namestitve požarnega zidu Palo Alto

Požarni zidovi Palo Alto Networks so napredne varnostne naprave, zasnovane za zaščito omrežij s kombiniranjem tradicionalnih zmogljivosti požarnega zidu z inovativnimi funkcijami, kot so zaznavanje aplikacij, preprečevanje groženj in identifikacija uporabnikov. Za razliko od tradicionalnih požarnih zidov, ki so odvisni samo od vrat in protokolov, požarni zidovi Palo Alto uporabljajo lastniško tehnologijo, imenovano App-ID, ki identificira in nadzoruje promet na podlagi same aplikacije, ne glede na vrata, šifriranje ali protokol. To omogoča natančen nadzor nad omrežnim prometom in boljšo zaščito pred naprednimi grožnjami.



Slika 10: Palo Alto PA-440

Vir: (Lasten vir)

Sledi obsežen vodnik za konfiguriranje požarnega zidu Palo Alto za varen dostop do interneta. Ta nastavitev vključuje konfiguracijo vmesnika, nastavitev virtualnega usmerjevalnika, omogočanje strežnika DHCP, ustvarjanje NAT in varnostne politike ter končno preverjanje.

8.1.1 Konfiguracija vmesnika

1. Odpremo konfiguracijsko ploščo

Prijavimo se v spletni vmesnik požarnega zidu Palo Alto z uporabo vrat za upravljanje. Pomaknemo se do razdelka Omrežje, da konfiguriramo vmesnike.

2. Konfiguracije vmesnika

- Ethernet 1/1:
- Tip: Layer3
- Naslov IP: 10.10.0.19/24
- Virtualni usmerjevalnik: Default Rout
- Cona: znotraj

- Ethernet 1/4:
- Tip: Layer3
- Naslov IP: 192.168.1.100/24
- Virtualni usmerjevalnik: Default Rout
- Cona: Zunaj

Po konfiguraciji obeh vmesnikov se prepričamo, da so njune vloge, naslovi IP in dodelitve con pravilni, preden potrdimo spremembe.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3			10.10.0.19/24	default	Untagged	none	Inside
ethernet1/2	Tap			none	none		none	none
ethernet1/3	Tap			none	none		none	none
ethernet1/4	Layer3			192.168.1.100/24	default	Untagged	none	Outside
ethernet1/5	Tap			none	none		none	none

Slika 11: Konfiguracija vmesnikov

Vir: (Lasten vir)

8.1.2 Konfiguracija navideznega usmerjevalnika

1. Ustvarimo navidezni usmerjevalnik

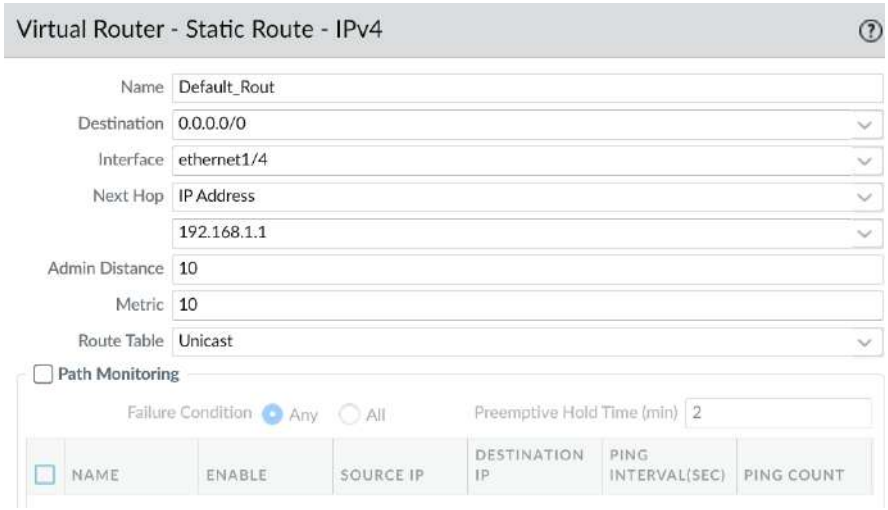
V razdelku Omrežje > Navidezni usmerjevalniki ustvarimo navidezni usmerjevalnik z imenom Default Rout za upravljanje prometa med notranjim in zunanjim območjem.

2. Dodamo statično pot

V virtualnem usmerjevalniku konfiguriramo privzeto statično pot za odhodni promet. Uporabimo naslednje nastavitve:

- Destinacija: 0.0.0.0/0
- Vmesnik: Ethernet 1/4
- Naslednji skok: 192.168.1.1
- Administrativna razdalja: 10
- Metrika: 10

Potem ko shranimo konfiguracijo, preverimo usmerjevalno tabelo, da potrdimo, da je privzeta pot aktivna.



Slika 12: Konfiguracija navideznega usmerjevalnika

Vir: (Lasten vir)

8.1.3 Konfiguracija strežnika DHCP

1. Omogočimo strežnik DHCP

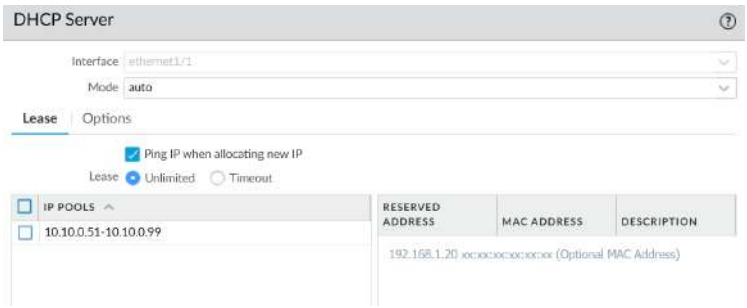
Pomaknemo se do Omrežje > DHCP, izberemo Ethernet 1/1 in omogočimo strežnik DHCP za naprave v notranjem območju.

2. Konfiguriranje parametra DHCP

Določimo naslednje nastavitve DHCP:

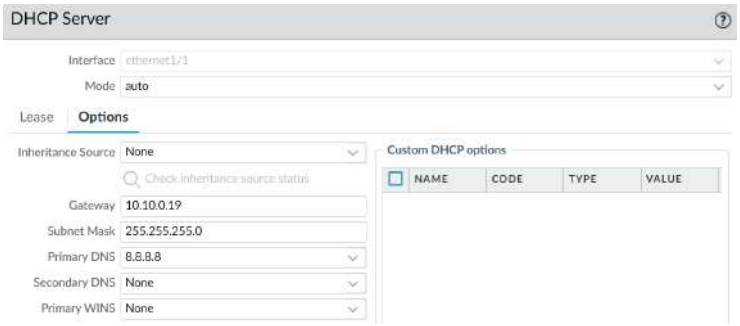
- Obseg naslovov IP: 10.10.0.51 - 10.10.0.99
- Privzeti prehod: 10.10.0.19
- Maska podomrežja: 255.255.255.0
- Primarni strežnik DNS: 8.8.8.8

Po končani konfiguraciji uporabimo nastavitve. Preverimo delovanje strežnika DHCP tako, da povežemo napravo v notranjem območju in zagotovimo, da prejme naslov IP znotraj navedenega obsega.



Slika 13: Konfiguracija DHCP serverja 1

Vir: (Lasten vir)



Slika 14: Konfiguracija DHCP serverja 2

Vir: (Lasten vir)

8.1.4 Konfiguriranje pravilnika NAT

1. Ustvarimo pravilnik NAT

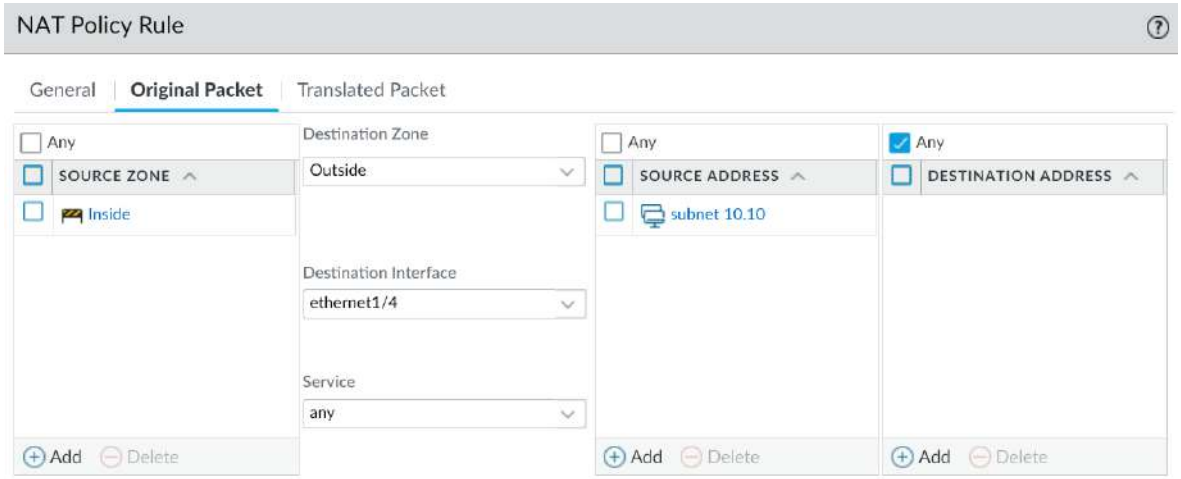
Pomaknemo se do Politike > NAT in ustvarimo novo pravilo NAT, da omogočimo dostop do interneta za naprave v notranjem območju.

Uporabimo naslednje parametre:

- Izvorna cona: znotraj
- Ciljna cona: zunaj
- Izvorni naslov: 10.10.0.0/24
- Vrsta prevoda: dinamični IP in vrata
- Naslov vmesnika: Ethernet 1/4
- Naslov NAT: 192.168.1.100

2. Preizkusimo pravilo NAT

Uporabimo pravilo NAT in preverimo njegovo delovanje s testiranjem povezljivosti z napravo v notranjem območju. Za dostop do zunanjega spletnega mesta uporabimo orodja, kot je ping, ali odpremo spletni brskalnik.



Slika 15: Konfiguracija pravilnika NAT

Vir: (Lasten vir)

8.1.5 Konfiguracija varnostne politike

1. Ustvarimo varnostno politiko

Če želimo uveljaviti nadzor dostopa, se pomaknemo do Politike > Varnost in ustvarimo pravilo z naslednjimi parametri:

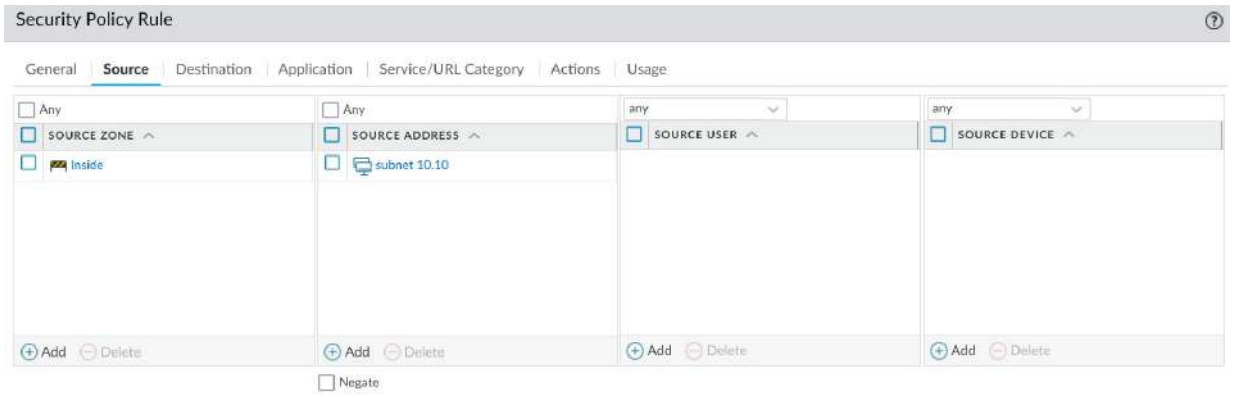
- Izvorna cona: znotraj
- Izvorni naslov: 10.10.0.0/24
- Ciljna cona: zunaj
- Ukrep: Dovoli

2. Določimo in uporabimo varnostno politiko

Shranimo in potrdimo varnostno politiko. To pravilo zagotavlja, da lahko promet, ki izvira iz notranjega območja, varno dostopa do zunanjih omrežij.

3. Preverimo varnostne politike

Sprožimo odhodni promet (npr. brskanje po spletu) iz naprave v notranjem območju. Preverimo, ali je promet dovoljen, tako da pregledamo dnevnike v Monitor > Promet.



Slika 16: Konfiguracija varnostne politike

Vir: (Lasten vir)

8.1.6 Končno preverjanje

1. Testiranje povezljivosti

Izvedemo celovit pregled, da zagotovimo, da vse konfigurirane komponente delujejo po pričakovanjih:

- Preverimo, ali naprave v notranjem območju prejemajo naslove IP od strežnika DHCP.
- Preizkusimo zunanjo povezljivost preko NAT.
- Potrdimo, da varnostni pravilnik dovoljuje odhodni promet.

2. Spremljanje prometnih dnevnikov

Pregledamo prometne dnevnike v Monitor > Promet, da potrdimo, da so uporabljena konfigurirana pravila in da je promet obdelan, kot je bilo predvideno.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
11/24 19:10:45	end	Inside	Outside	10.10.0.51			20.54.37.64			443	windows-push-notifications	allow	Inside_to_Outside
11/24 19:10:40	end	Inside	Outside	10.10.0.51			20.54.37.64			443	windows-push-notifications	allow	Inside_to_Outside
11/24 19:10:30	end	Inside	Outside	10.10.0.51			193.77.14.137			80	ms-update	allow	Inside_to_Outside
11/24 19:09:20	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:20	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:15	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:15	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:15	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:15	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:15	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:15	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:09:10	end	Inside	Outside	10.10.0.51			104.85.248.82			80	ms-update	allow	Inside_to_Outside
11/24 19:09:10	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside
11/24 19:08:50	end	Inside	Outside	10.10.0.51			104.85.248.82			80	web-browsing	allow	Inside_to_Outside

Slika 17: Prikaz nadzorovanja prometa

Vir: (Lasten vir)

Če sledimo tem korakom, je požarni zid Palo Alto učinkovito konfiguriran za zagotavljanje varnega in zanesljivega dostopa do interneta. Nastavitev dinamično usmerja promet med notranjimi in zunanjimi območji, dodeljuje naslove IP prek DHCP, prevaja notranje IP-je z uporabo NAT in uporablja stroge varnostne politike za upravljanje dostopa.

9 VZPOSTAVITEV VPN-JA NA PALO ALTU

Uporaba VPN (navideznega zasebnega omrežja) na požarnem zidu Palo Alto je bistvena za zagotavljanje varne in šifrirane komunikacije prek javnih in zasebnih omrežij. Rešitve VPN podjetja Palo Alto zagotavljajo robustne varnostne funkcije, vključno z naprednimi šifrirnimi protokoli, preprečevanjem groženj in varnim oddaljenim dostopom za uporabnike in podružnice. To pomaga zaščititi občutljive podatke pred kibernetskimi grožnjami, kot so prestrezanje, napadi »človek v sredini« in nepooblaščen dostop. Poleg tega požarni zidovi Palo Alto ponujajo centralizirano upravljanje in spremljanje, kar skrbnikom omogoča uveljavljanje doslednih varnostnih politik v vseh povezavah VPN. S funkcijami, kot je GlobalProtect, Palo Alto zagotavlja brezhibno in varno povezljivost za oddaljene delavce, izboljšuje produktivnost, hkrati pa ohranja celovitost in zaupnost organizacijskih podatkov. Na splošno integracija zmogljivosti VPN s požarnimi zidovi Palo Alto izboljša varnost omrežja, zagotavlja skladnost z industrijskimi standardi in zanesljive rešitve za oddaljeni dostop.

9.1 Nastavitev VPN z uporabo GlobalProtect

1. Predpogoji:

- Požarni zid Palo Alto z licencama GlobalProtect Gateway in Portal.
- Potrdila SSL/TLS, konfigurirana na požarnem zidu.
- Uporabniški računi, nastavljeni v požarnem zidu ali integriranem sistemu za preverjanje pristnosti (npr. LDAP, RADIUS).

2. Konfiguracija portal GlobalProtect:

- Pomaknemo se na Omrežje > GlobalProtect > Portali.
- Kliknemo »Dodaj« in vnesemo ime portala in naslov IP.
- Konfiguriramo profil storitve SSL/TLS.
- Dodamo profil za preverjanje pristnosti (npr. LDAP ali RADIUS).
- Določimo nastavitve konfiguracije odjemalca (področja IP, DNS itd.).

3. Konfiguracija GlobalProtect Gateway:

- Pomaknemo se na Network > GlobalProtect > Gateways.
- Kliknemo »Dodaj« in konfiguriramo ime prehoda in naslov IP.

- Izberemo profil storitve SSL/TLS.
- Dodelimo profil za preverjanje pristnosti.
- Konfiguriramo vmesnik tunela in skupino IP-jev odjemalca.
- Omogočimo dostop uporabnika/uporabniške skupine.

4. Konfiguracija varnostne politike:

- Pomaknemo se na Politike > Varnost.
- Ustvarimo pravila za dovoljenje prometa VPN.
- Prepričamo se, da je območje VPN pravilno konfigurirano, da omogoča zahtevane aplikacije in storitve.

5. Konfiguracija uporabniškega dostopa:

- Pomaknemo se na Naprava > Profil za preverjanje pristnosti.
- Ustvarimo ali spremenimo nastavitve preverjanja pristnosti uporabnikov.
- Zagotovimo, da imajo uporabniški računi pravice dostopa do VPN.

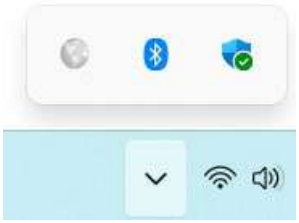
9.2 Namestitev GlobalProtect-a za oddaljeno povezavo

1. Namestitev GlobalProtect-a:

- Prenesemo GlobalProtect s spletnega portala požarnega zidu Palo Alto.

2. Povezava z GlobalProtect VPN:

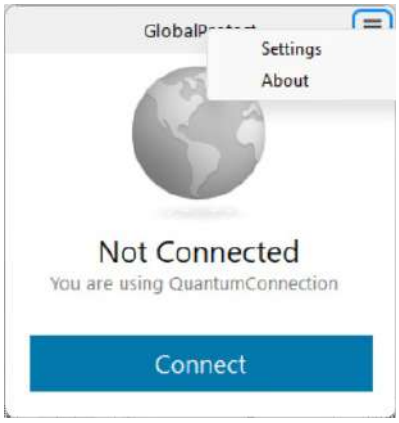
- V spodnjem desnem kotu zaslona z desno miškino tipko kliknemo ikono GlobalProtect v sistemski vrstici.



Slika 18: Ikona GlobalProtect v sistemski vrstici

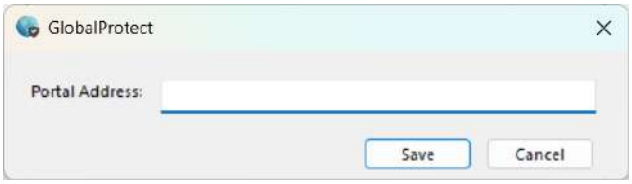
Vir: (Lasten vir)

- Premaknemo miškin kazalec nad vodoravne črte in kliknemo z levim gumbom miške.
- Izberemo »Nastavitve« in dodamo naslov portala: *Ime portala*.



Slika 19: Možnosti nastavitev GlobalProtect

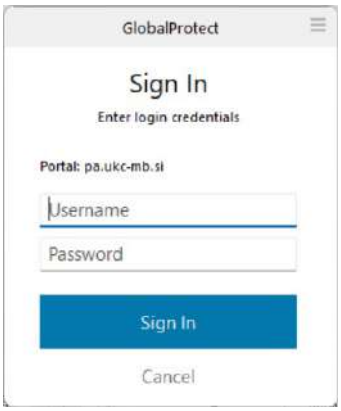
Vir: (Lasten vir)



Slika 20: Vnos naslova portala

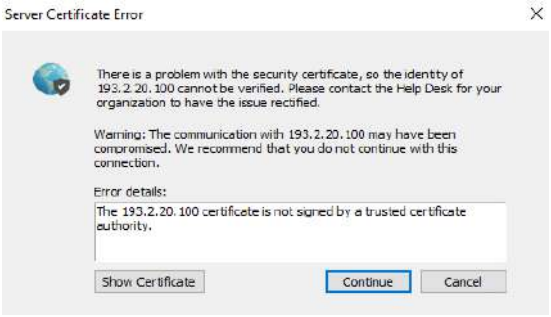
Vir: (Lasten vir)

- Ko smo dodali portal, se prijavimo s poverilnicami svojega podjetja.
- Uporabniško ime in geslo sta enaka prijavi v službeni računalnik.
- Ob prvi prijavi bomo morda videli varnostno opozorilo. Kliknemo »Nadaljuj«.



Slika 21: Prijavno okno

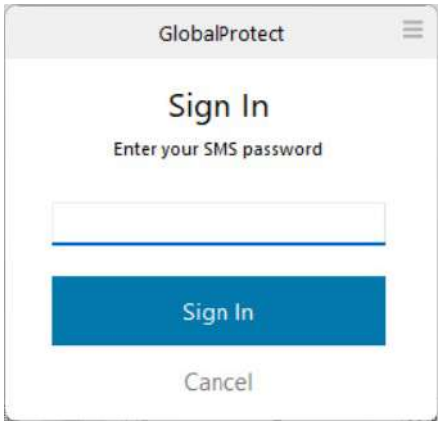
Vir: (Lasten vir)



Slika 22: Varnostno opozorilo

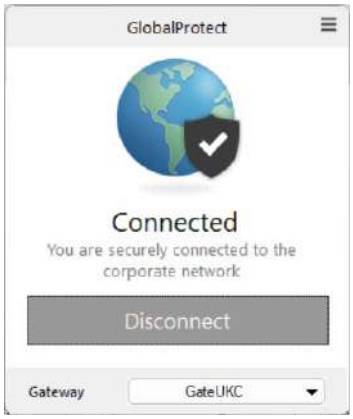
Vir: (Lasten vir)

- Ko vnesemo svoje poverilnice, bomo prejeli sporočilo s kodo za preverjanje.
- Vnesemo kodo v označeno polje in kliknemo »Prijava«.
- Ko se povežemo, bomo videli potrditveno okno.



Slika 23: Okence vnosa poverilnice

Vir: (Lasten vir)

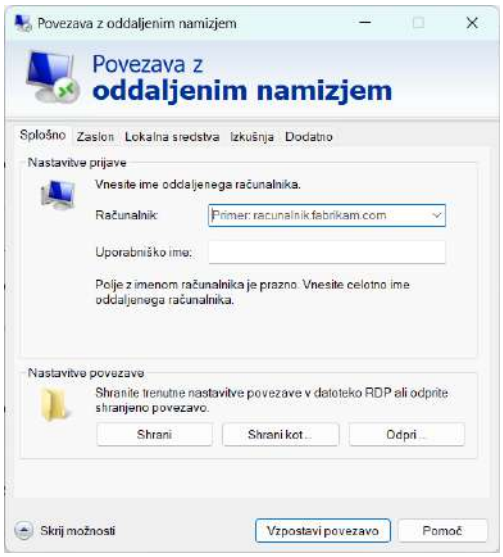


Slika 24: Potrditveno okence uspešne povezave

Vir: (Lasten vir)

3. Dostop do oddaljenega namizja:

- Odpremo aplikacijo za oddaljeno namizje.
- Vnesemo naslednje podatke:
  - Računalnik: *Ime računalnika v podjetju ali naslov IP*
  - Uporabniško ime: *Uporabniško ime za vpis v službeni računalnik*
  - Geslo: *Geslo za vpis v službeni računalnik*



Slika 25: Povezava z oddaljenim namizjem

Vir: (Lasten vir)

4. **Preizkus povezljivost VPN-ja:**

- Preverimo uspešno povezavo in pravilno dodelitev IP-ja.

5. **Nadzor in odpravljanje težav:**

- Pomaknemo se na Monitor > Sistem > Dnevniki, da preverimo težave s povezavo.
- Za spremljanje aktivnih povezav se pomaknemo na Omrežje > GlobalProtect > Prehod.

GlobalProtect VPN zagotavlja varno in razširljivo rešitev za oddaljeni dostop. Upoštevanje teh korakov zagotavlja brezhibno uvajanje in varno povezljivost za oddaljene uporabnike.

10 SKLEP

Diplomsko delo obravnava pomen sistematičnega in večplastnega pristopa k obravnavi groženj kibernetski varnosti. Raziskava je uspešno dosegla osnovne cilje, ki so bili: analizirati mehanizme pogostih kibernetskih napadov, oceniti učinkovitost trenutnih zaščitnih ukrepov in predlagati praktične strategije za posameznike in organizacije za krepitev njihove kibernetske varnosti.

Analiza je potrdila, da so kibernetski napadi, vključno z lažnim predstavljanjem, izsiljevalsko programsko opremo in napadi DDoS, vse bolj izpopolnjeni in predstavljajo veliko tveganje za posameznike in organizacije. Te grožnje izkoriščajo ranljivosti v tehnologiji in človeškem vedenju. Izpostavljenih je bilo več orodij in strategij za ublažitev teh tveganj, kot je uporaba požarnih zidov, protivirusne programske opreme, večfaktorske avtentikacije (MFA) in upravitelji gesel. Podrobneje je bil obravnavan pomen proaktivnih ukrepov, vključno z rednimi posodobitvami programske opreme, celovitim usposabljanjem zaposlenih in spodbujanjem kulture ozaveščenosti o kibernetski varnosti.

Diplomsko delo podaja pregled učinkovitosti požarnih zidov in podrobno predstavi konfiguracijo požarnega zidu Palo Alto kot modela za varovanje omrežij. Namen je bil praktični prikaz primera naprednih tehnologij pri obrambi pred nepooblaščenim dostopom in zmanjševanju tveganj, povezanih z zunanjimi in notranjimi grožnjami.

Raziskava je sistematično obravnavala in ovrednotila hipoteze, zastavljene v uvodu diplomskega dela: H1: Posamezniki, ki so zelo aktivni na spletu, imajo večjo verjetnost, da bodo doživeli lažno predstavljanje.

Ta hipoteza je bila potrjena, saj so ugotovitve pokazale jasno povezavo med pogosto spletno aktivnostjo in izpostavljenostjo poskusom lažnega predstavljanja.

- H2: Uporaba močnih, edinstvenih gesel znatno zmanjša število nepooblaščenih dostopov.

  Ta hipoteza je bila tudi potrjena z raziskavami, ki podpirajo kritično vlogo zanesljivega upravljanja gesel pri preprečevanju kršitev.

- H3: Redne posodobitve programske opreme zmanjšujejo dovzetnost za napade zlonamerne programske opreme.

  Raziskave so potrdile to hipotezo in poudarile potrebo po pravočasnih posodobitvah za odpravo znanih ranljivosti.

- H4: Umetna inteligenca (AI) prispeva k naprednim kibernetskim napadom in obrambi.

  Ta hipoteza je bila delno potrjena. Čeprav umetna inteligenca omogoča bolj napredne napade, podpira tudi inovativne obrambne mehanizme, kot so avtomatizirani sistemi za zaznavanje groženj in odziv.

- H5: Manj verjetno je, da bodo organizacije, ki uporabljajo MFA, doživele kršitve varnosti.

  Hipoteza je bila potrjena, saj so na podlagi raziskav organizacije, ki uporabljajo MFA bolj zaščitene in varne, kot organizacije, ki tega ne uporabljajo.

- H6: Napredni sistemi požarnih zidov so učinkovitejši od osnovnih rešitev pri preprečevanju nepooblaščenega dostopa do omrežja.

  Ta hipoteza je bila potrjena s praktično implementacijo in analizo požarnega zidu Palo Alto, ki je pokazal na podlagi testiranja vrhunske zmogljivosti pri obvladovanju in zmanjševanju omrežnih tveganj.

Ugotovitve potrjujejo potrebo po večplastnem pristopu k kibernetski varnosti. Ključni predlogi za posameznike in organizacije so:

- redno posodabljanje programske in strojne opreme, da se odpravijo ranljivosti, ki jih je mogoče izkoristiti;
- izvajanje MFA in uporaba upraviteljev gesel za izboljšanje varnosti računa;
- spodbujanje izvajanja programov izobraževanja in usposabljanja za obravnavo ranljivosti, povezanih s človekom, kot je dovzetnost za lažno predstavljanje;
- integracija napredne tehnologije, vključno z umetno inteligenco in robustnimi požarnimi zidovi, za nenehno sledenje razvijajočim se kibernetskim grožnjam;
- vzpostavitev jasnih protokolov za odzivanje na incidente, s poudarkom na zadrževanju, izkoreninjenju in okrevanju.

Kibernetska varnost ni enkraten napor, ampak stalen proces prilagajanja in izboljšav. Z združevanjem tehnološko usmerjenih rešitev s človeško zavestjo in organizacijsko predanostjo je mogoče znatno zmanjšati tveganja, povezana s kibernetskimi grožnjami. Raziskava potrjuje ključno vlogo ozaveščanja, izobraževanja in inovacij pri ustvarjanju varnega digitalnega okolja.

11 VIRI IN LITERATURA

Literatura

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking.* United States: Wiley.

Meeuwisse, R. (2015). *Cybersecurity for Beginners.* United States: Lulu Publishing Services.

Mitnick, K. (2001). *The Art of Deception: Controlling the Human Element of Security.* United States: Wiley.

Mitnick, K. (2017). *The Art of Invisibility.* United States: Little, Brown and Company.

Parker, C. (2015). *Firewalls Don't Stop Dragons: A Step-by-Step Guide to Computer Security for Non-Techies.* United States: Apress.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley.

Sikorski, M., & Honig, A. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.* United States: No Starch Press.

Viri slik

Andreas, R. (3. oktober 2022). *Medium*. Pridobljeno iz Medium: https://medium.com/gravel-engineering/learn-8-common-types-of-phishing-25a2dd4d6778

Cybersecurity. (13. oktober 2024). *1000Logos*. Pridobljeno iz 1000Logos: https://1000logos.net/best-antivirus-software/

Ferreira, L., Silva, D., & Itzazelaia. (5. junij 2023). *Springer Nature Link*. Pridobljeno iz Springer Nature Link: https://link.springer.com/article/10.1007/s10115-023-01906-6#article-info

Moser, J. (2. oktober 2024). *NICEHASH*. Pridobljeno iz NICEHASH: https://www.nicehash.com/blog/post/a-deep-dive-into-lightning-network-ln-security

Paul Riedl, J. (26. marec 2023). *Linked in*. Pridobljeno iz Linked in: https://www.linkedin.com/pulse/password-managers-how-do-work-safe-paul-riedl-jr-

Reynolds, P. D. (5. maj 2024). *Xecor*. Pridobljeno iz Xecor: https://www.xecor.com/blog/raspberry-pi-firewall-configuration-protection-and-usage

Rubenking, N. J. (15. december 2024). *PC MAG*. Pridobljeno iz PC MAG: https://www.pcmag.com/reviews/bitdefender-antivirus-for-mac

Stockton, B. (26. avgust 2024). *Cloudwards*. Pridobljeno iz Cloudwards: https://www.cloudwards.net/bitdefender-vs-norton-antivirus/

Tamašiūnienė, A. (24. maj 2024). *Cybernews*. Pridobljeno iz Cybernews: https://cybernews.com/best-antivirus-software/mcafee-vs-norton/