Sigurnost krajnjih uređaja u korporativnom okruženju

Lenić, Martina

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:470361

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-12-25**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

SIGURNOST KRAJNJIH UREĐAJA U KORPORATIVNOM OKRUŽENJU

DIPLOMSKI RAD

Martina Lenić

Osijek, 2022.

SADRŽAJ

1. UVOD 1

2. KRAJNJI UREĐAJI I NJIHOVA PRIMJENA U KORPORATIVNOM OKRUŽENJU 3

3. KRAJNJI UREĐAJI I NJIHOVA NESIGURNOST U ORGANIZACIJI 4

3.1. Prijetnje, slabosti i rizici 4

3.2. Kompromitiranje sustava 5

3.3. Kompromitiranje korisničkih identiteta 9

4. SIGURNO UPRAVLJANJE KRAJNJIM UREĐAJIMA 12

4.1. Mrežne sigurnosne kontrole 15

4.2. Fizičke sigurnosne kontrole 24

4.3. Odgovor na incidente i proces oporavka 25

4.4. Evaluacija sigurnosnog rizika 28

5. POSTURA I OKVIR KIBERNETIČKE SIGURNOSTI 31

5.1. Sigurnosne strategije 32

5.2. Sigurnosni okviri organizacije 35

5.3. Osviještenost, trening i edukacija 37

6. KOMPLETNA RJEŠENJA ZAŠTITE, DETEKCIJE I ODGOVORA NA NAPADE NA KRAJNJIM UREĐAJIMA 39

6.1. EDR, XDR i MDR 40

6.2. *CrowdStrike Falcon* 44

7. ZAKLJUČAK 50

LITERATURA 51

SAŽETAK 54

ABSTRACT 55

ŽIVOTOPIS 56

1. UVOD

Sigurnost krajnjih uređaja jedna je od značajnijih aspekata upravljanja organizacijskom infrastrukturom i njezinom zaštitom od ugroza kojima je konstantno izložena. Današnje organizacije svjedoci su enormnom povećanju opasnosti od kibernetičkih napada. Povećanjem mobilnosti zaposlenika i udaljenog rada od doma vjerojatnost od napada na organizacijske krajnje uređaje i mrežu eksponencijalno raste, a napadači se koriste naprednim tehnologijama i alatima za provođenje strategijski isplaniranih napada koji imaju tendenciju napraviti veliku štetu po organizaciju i njezino poslovanje. Krajnji uređaji predstavljaju poseban sigurnosni rizik i izazov jer kao najizloženiji dio organizacije često su prva meta aktivnosti zlonamjernih napadača. Razvojem tehnologija kibernetički napadači odmaknuli su se od tradicionalnih zlonamjernih programa, a sve više približili onim naprednim temeljenim na kompleksnim strukturama koda, strojnom učenju i AI (engl. *Artificial Intelligence*). Prema tome razvijali su se i sigurnosni mehanizmi i modeli sa svrhom zaštite, prevencije i odgovora na svaku prijetnju i napad.

U ovom radu bilo je potrebno analizirati i objasniti različite aspekte zaštite od sigurnosnih prijetnji kojima su izložene korporativne mreže i krajnji uređaji. Nakon uvoda u rad te pregleda trenutnog područja sigurnosti krajnjih uređaja u korporativnim okruženjima slijedi treće poglavlje koje upoznaje s primjerima krajnjih uređaja te prolazi kroz najčešće načine kompromitiranja sustava i korisničkih identiteta u organizaciji. Definiraju se i tri važna pojma koja se kontinuirano protežu kroz kibernetičku sigurnost, a odnose se na postojanost ranjivosti, prijetnje i rizika. Iduće poglavlje, sigurno upravljanje krajnjim uređajima prolazi kroz mrežne i fizičke sigurnosne kontrole koje ne smiju nedostajati u organizacijama koje za cilj imaju održati optimalnu sigurnost u svojem okruženju. Osim detekcije i prevencije za koje je važno implementirati snažne sigurnosne kontrole, sigurnosna zrelost organizacije očituje se i u definiranju procesa i procedura odgovora i oporavka u slučaju stvarnog proboja sigurnosne obrane. Upravo je to tema potpoglavlja koji upoznaje s odgovorima na incidente i proces oporavka te evaluaciju sigurnosnih rizika kojima je korporacija izložena. Peto poglavlje uvodi u posturu i glavne okvire kibernetičke sigurnosti koji implementirani prema definiranim standardima omogućuju organizaciji kontinuiran napredak u osiguravanju IT imovine, mreže i oblaka. Osviještenost, trening i edukacija još su jedan dio ovog rada koji stavlja naglasak na važnost utjecaja zaposlenika i korisnika na zaštitu i prevenciju neželjenih aktivnosti u okruženju korporacije. Konkretan primjer implementacije sigurnosnih kontrola i metoda dan je u šestom poglavlju gdje se opisuju najnovije tehnologije detekcije,

prevencije i odgovora na prijetnje i napade, a koje svojim uslugama i ugrađenim alatima imaju mogućnost zaštite i do nekoliko tisuća krajnjih uređaja, opterećenja u oblaka i mreže.

2. KRAJNJI UREĐAJI I NJIHOVA PRIMJENA U KORPORATIVNOM OKRUŽENJU

Krajnji uređaj (engl. *endpoint*) je svaki udaljeni računalni uređaj koji komunicira putem mreže na koju je povezan, odnosno predstavlja krajnju točku distribuirane računalne mreže. Primjeri krajnjih uređaja u korporativnom okruženju su:

- laptopi,
- tableti,
- pametni uređaji,
- serveri,
- radne stanice (engl. Workstations),
- IoT (engl. *Internet of Things* = Internet objekata) uređaji [1].

To su uređaji koji količinom i važnošću u okruženju organizacije predstavljaju glavne ulazne točke slabosti za kibernetičke kriminalce. Povezani na mrežu podložni su brojnim napadima i iskorištavanjima, kako slabosti uređaja i sustava, tako i činjenici da su u većini slučajeva upravljani od strane korisnika, odnosno zaposlenika organizacije. S povećanjem mobilnosti organizacijskih radnih mjesta, rada od doma, permanentnog oslanjanja na umrežavanje i korištenje informacijskih sustava, BYOD (engl. *Bring your own device*) politike te korisnika koji se u sve većoj mjeri spajaju na interne resurse i mrežu izvan prostora organizacije, povećava se i ranjivost krajnjih uređaja na kibernetičke napade. Svaka otkrivena slabost dovodi do smanjenja kompletne sigurnosti organizacije, a ono će se kroz naredna poglavlja i primjere dodatno objasniti. Upravljanje krajnjim uređajima je praksa koju organizacije provode s ciljem veće transparentnosti u aktivnosti i pristupe uređaja u mreži. Odnosi se na autentikacije i nadziranja prava pristupa krajnjih uređaja u mreži i primjenjivanja sigurnosnih polica koje preveniraju bilo kakve vanjske ili unutarnje prijetnje nastale prilikom pristupa. Sa stotinama, pa i tisućama krajnjih uređaja u organizaciji te uobičajenom praksom pristupa jednog korisnika mreži putem više uređaja javlja se potreba za njihovim kontinuiranim pregledom i upravljanjem. Krajnji uređaji konstantno kreiraju i razmjenjuju podatke, a svakom razmjenom na mreži javlja se potencijalna prijetnja sigurnosti. Prevencija i odgovor na takve situacije dio je zaštite krajnjih uređaja koja radi zajedno s procesom upravljanja. Funkcija zaštite krajnjih uređaja u organizaciji podrazumijeva analiziranje i provjeru promjena i razmjena podataka, skeniranje od zlonamjernih programa te primjena potrebnih ažuriranja i zakrpa gdje je to na uređajima potrebno [2].

3. KRAJNJI UREĐAJI I NJIHOVA NESIGURNOST U ORGANIZACIJI

Krajnji uređaji po svojoj su prirodi glavna ranjivost organizacije te se njihova zaštita odražava u sigurnosnom držanju kompletne organizacije. Kao ulazne i izlazne točke mreže sadrže široku lepezu mogućnosti za napadače, od pristupa imovini i informacijama visoke vrijednosti, eksfiltriranja ili zauzimanja podataka pa do potunog preuzimanja uređaja nakon čega ono postaje uređaj pod kontrolom napadača. Raznolikost vještina, mogućnosti, resursa te motivacije kibernetičkih napadača vodi k sve većoj potrebi za razumijevanjem i širenjem znanja prirode kibernetičkih ugroza s ciljem pravovremenog djelovanja i implementiranja sigurnosne zaštite koja će sveobuhvatno štiti krajnje uređaje u organizaciji. Informacijska sigurnost definira se kao zaštita informacija i informacijskih sustava od nedozvoljenog pristupa, korištenja, razotkrivanja, poremećaja, modificiranja ili uništavanja u cilju pružanja povjerljivosti, integriteta i dostupnosti, a podržana je arhitekturom informacijske sigurnosti koja daje opis strukture i ponašanja organizacijskih sigurnosnih procesa, sustava, osoblja i organizacijskih pod-jedinica koji se usklađuju s misijom i strategijskim planovima cjelokupne organizacije [3].

Sigurnost krajnjih uređaja je klijent/server način osiguravanja informacija u svrhu zaštite organizacijske mreže fokusiranjem na mrežne uređaje, a sve to kroz promatranje statusa, aktivnosti, autorizacija i autentifikacija povezanih na taj krajnji uređaj. S povećanjem broja autoriziranih korisnika izvan mreže organizacije sigurnost krajnjih uređaja razvija se u smjeru zaštite i prevencije upada, softvera za prepoznavanje i blokiranje zlonamjernog ponašanja te praćenje aktivnosti uređaja zbog nedozvoljenih aplikacija ili štetnih namjera.

3.1.Prijetnje, slabosti i rizici

Tri najvažnija pojma u središtu procjene i implementacije sigurnosti u bilo kojem korporativnom okruženju su ranjivosti (engl. *vulnerability*), prijetnje (engl. *threats*) i rizici (engl. *risk*) kojima su organizacija i organizacijski podaci izloženi. Slabost je ranjivost uređaja, aplikacije sustava ili procesa koju napadač lako iskoristi u svrhu napada. To su unutarnji faktori koji se nalaze pod ovlastima kibernetičkih profesionalaca. Primjeri slabosti su zastarjele verzije sustava, nedovoljno snažne lozinke, itd. Organizacija mora pravovremeno reagirati na takve slabosti, ažurirati sustave na najnovije verzije, postaviti uvjete za izgled lozinke te ostalo. Mnoge ranjivosti u informacijskim sustavima povezane su sa sigurnosnim kontrolama koje ili još nisu primijenjene ili jesu implementirane, ali i dalje sadrže određenu razinu slabosti. Također ne smije se zanemariti

i mogućnost ranjivosti koje se pojavljuju prirodno s vremenom kako se organizacijska misija i djelovanje razvijaju, okruženje mijenja, nove tehnologije nastaju i razvijaju te s time i nove prijetnje. Jedna od najpoznatiji svjetskih repozitorija ranjivosti je NVD (engl. *National Vulnerability Database*) koji uključuje baze podataka sigurnosnih referenci, mane u sigurnosnim softverima, pogrešne konfiguracije, imena produkata te metrike utjecaja. Svaka ranjivost sadrži ID (npr. CVE-2022-xxxx) te vlastitu ocjenu prema CVSS-u (engl. *Common Vulnerability Scoring System*) koji predstavlja industrijski standard za procjenu ozbiljnosti ranjivosti [4]. Prijetnja predstavlja vanjske čimbenike koji iskorištavaju slabosti unutar organizacije. Napadač koji želi izvesti DoS (engl. *Denial of Service*) napad na web stranicu i poznaje slabosti *Apache* servisa predstavlja ozbiljnu prijetnju. Događaji izazvani prijetnjama karakteriziraju se kao pokušaji iskorištavanja slabosti. To su kibernetički ili fizički napadi, ljudske greške propusta, strukturne greške u organizacijskim resursima te ostale prirodne i ljudske pogreške koje nisu pod kontrolom organizacije. Rizik je kombinacija prijetnje i pripadajuće slabosti jer oboje trebaju postojati kako bi situacija sadržavala određenu razinu rizika za sigurnost organizacije. Napadač koji ima cilj izvesti DoS napad na *Apache* server i dalje predstavlja prijetnju no ako je server ažuriran na najnoviju verziju tako da nije ranjiv na takvu vrstu napada napadač sa svojim namjerama ne predstavlja rizik, a tzv. formula (3-1) prikazuje da rizik postoji samo u slučaju ako postoje prijetnja i slabost koju napadač može iskoristiti [3][5].

$$Rizik = Prijetnja \times Slabost \tag{3-1}$$

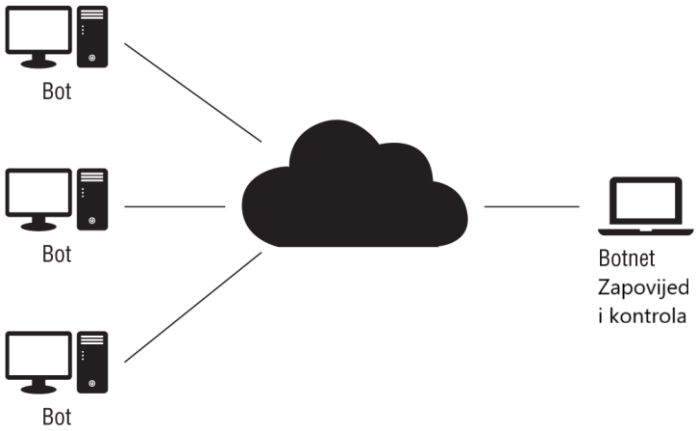
3.2.Kompromitiranje sustava

Današnji kibernetički napadači pokazuju da znanjem i vještinama imaju mogućnosti osigurati pristup ciljanim sustavima ili uređajima puno prije izvođenja ili razotkrivanja napada. Takva sofisticiranost otkriva da mogu ostati u stanju neotkrivenosti dok se ne pojavi pravo vrijeme za napad, odnosno jasno je da postoji strukturiran i zakazan plan s točno određenim ciljem. Ipak, razmatranjima i analizom kompletnih napada otkrivene su epizode sličnih faza koje dovode do uspješno izvedenih napada što je poznato kao *Cybersecurity Kill Chain*. Faze lanca napada uključuju izviđanje ranjivosti sustava i/ili uređaja podložnih iskorištavanju što dovodi do faze prilagođavanja alata i tehnologija na temelju prikupljenih podataka ciljane mete. Dostava zlonamjernih programa i alata na kraj korisnika je prvi konkretan kontakt s metom nakon čega slijedi iskorištavanje otkrivenih ranjivosti i rizika kojima je meta podlegnuta, a najčešće se provodi izvršavanjem zlonamjernog koda na sustavu žrtve. Slijede instalacija i pokretanje zlonamjernih

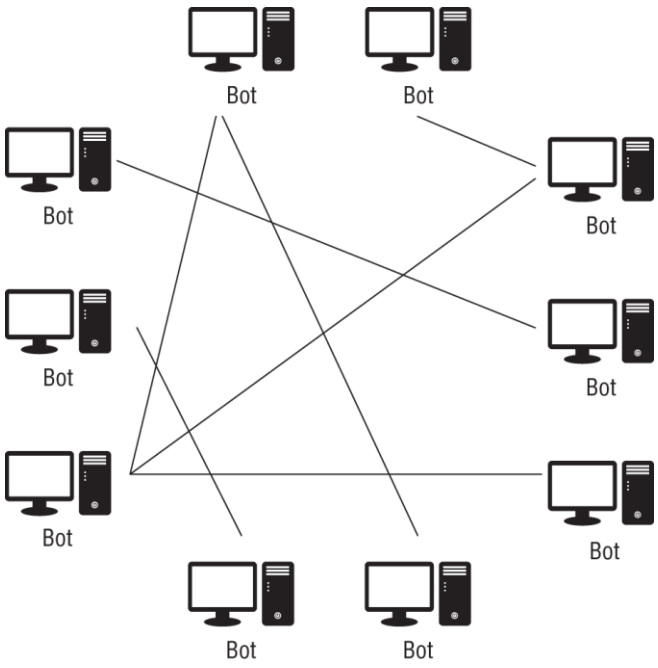
programa te zapovijed i kontrola (C&C) nad inficiranim sustavom što dovodi do potpune manipulacije sustava. Kompromitiranje sustava je izvršavanje stvarnih napada nakon prikupljenih informacija o slabostima u sustavu te odabira tehnika i taktika za isplanirani cilj [6].

Jedan od najčešće ciljanih alata za inficiranje i pristupanje mrežnim uređajima kako od strane napadača tako i sigurnosnih centara su zlonamjerni softveri (engl. *malware*). Kao takvi projektirani su s ciljem oštećenja ili iskorištavanja bilo kojeg uređaja, sustava ili mreže. Kroz godine su napredovali od jednostavnih računalnih virusa pa sve do softvera temeljenih na umjetnoj inteligenciji. Razvoj i širenje kibernetičkih napada i prijetnji potaknulo je organizacije da se proaktivno uključe u njihovo traženje te vlastito educiranje kako bi u svakom trenutku bili korak ispred napadača i njegovih ciljeva. Trenutni trendovi pokazuju povećanje u sofisticiranosti i inovativnosti alata, tehnika i taktika provedenih od strane kibernetičkih napadača, a česti napadi uključuju napade iznude provedene ucjenjivačkim softverom (engl. *ransomware*), manipulacija podataka, napade na IoT uređaje, napade tehnikom stražnjih vrata (engl. *backdoor*), napade na mobilne i svakodnevne uređaje te napadi na cloud. *Ransomware* je konstantno napredovani zlonamjerni softver dizajniran da enkriptira podatke na korisničkom uređaju s ciljem njihovog otimanja i traženja otkupnine. Incidenti povezani s ovom vrstom softvera imaju tendenciju ozbiljno naštetiti poslovanju organizacije jer otete datoteke često su ključne za pružanje usluga kritičnih za poslovanje. Incidenti vezani uz *ransomware* u većini slučajeva uključuju programe za dijeljenje desktopa, korištenje e-maila, web aplikacije te direktna instalacija na računalo [8]. Jedan od najpoznatijih primjera takvog napada u bližoj prošlosti je *WannaCry* ucjenjivački softver koji je 2017. godine inficirao stotine tisuća uređaja u više od 150 država. Napadači nisu uspjeli izvršiti plan u cijelosti zbog pronađenog prekidača u kodu softvera no bez mane softver bi napravio ogromnu sigurnosnu i financijsku štetu u cijelom svijetu [9]. Najefektivniji način obrane od ovakve vrste napada je održavanje sigurnosne kopije sustava koja će pohranjivati datoteke na odvojenu lokaciju i tako izbjeći otuđivanja i osigurati se od nestanka organizacijskih resursa. Kompromitiranost sustava ostvaruje se i manipulacijom podataka što dovodi i do kompromitiranosti integriteta. S privilegiranim pristupom organizacijskim izvještajima i bazama podataka napadač bez većih problema može napraviti izmjene pa čak i u sigurnosnim kopijama podataka. Napad manipulacijom podataka je primjer da bez obzira na održavanje potrebno je sigurnosne kontrole usmjeriti i na sigurnosnu kopiju organizacijske imovine. Kao tehnologija u nastajanju i brzog rasta hakeri često ciljaju dostupne IoT uređaje koji su često iskorišteni u DDoS (engl. *Distributed Denial of Service*) napadima protiv organizacija. Svrha je iskorištavanjem velikog broja IoT uređaja generirati enormne količine nelegitimnog prometa koji može srušiti

servere. Uređaji koji stoje iza ovakvog napada su botovi, mreže ili inficirani uređaji pod kontrolom napadača nad kojim je uspostavljena kompletna kontrola. Grupa botova ili botneti („*robot network*“) mogu se sastojati od nekoliko tisuća botova koje napadač istovremeno koristi za izvođenje napada. Slika *3.1* je primjer klijent-server modela gdje je uspostavljena C&C (engl. *Command and Control*) faza napada, a server je taj koji prati sustave u cijelom botnetu. Uz to postoji i *peer-to-peer* botnet model gdje se botovi spajaju međusobno bez središnjeg servera koji upravlja cijelom mrežom što dodatno otežava rušenje botneta, prikazano na Slika 3.2. Detekcija takvog napada najuspješnija je koristeći antivirusne alate te alate za nadziranje prometa u mreži.



Slika 3.1: Klijent-server botnet [7]



Slika 3.2: *Peer-to-peer* botnet [7]

Ostali individualni zlonamjerni programi koji ciljaju na krajnje uređaje uključuju trojanskog konja, *rootkite,* PUP (engl. *Potentially Unwanted Program*) i bezdatotečne viruse. Borbe protiv trojanskih zlonamjernih programa često se vode na sloju sigurnosti ljudskog faktora, odnosno kombinacijom osvješćivanja zaposlenika o postojanim prijetnjama kroz programe i edukaciju te antivirusnim alatima koji pomažu u detekciji i prevenciji. *Rootkit*-ovi su programi koji neautoriziranom korisniku daju autorizirani pristup uređaju, a skriveni su u samom operacijskom sustavu. Detekcija ovakve vrste zlonamjernog softvera može biti otežana jer inficirani sustav nije povjerljiv te se detekcija oslanja na sigurnosne programe koji pretražuju i provjeravaju ponašanja tipična za uređaje inficirane takvom vrstom softvera ili testiranjem uređaja na povjerljivom sustavu. Jedni od najpoznatijih zlonamjernih programa su virusi koji imaju mogućnost samostalnog kopiranja i repliciranja na inficiranom uređaju ili sustavu. Najčešće rade na način da kada se određeni uvjet ispuni, virus se izvrši. Podvrsta virusa su virusi bez datoteke (engl. *fileless virus*) koji se šire pomoću *spam* mailova ili inficiranih web stranica, a posebnost im je u tome što ne zahtijevaju lokalnu datotečnu pohranu, već se zadržavaju u memoriji kroz cijeli životni ciklus. Infekcija započinje linkom na zlonamjernu web stranicu koja iskorištava postojanu ranjivost dodatka preglednika te *shell* kod izvršava skriptu za preuzimanje i izvršavanje zlonamjernog sadržaja u memoriji korisnikovog sustava. Bezdatotečni virusi mogu nastaviti inficirati sustav ponavljanjem koda i njegovim izvršavanjem kod ponovnog pokretanja uređaja, odnosno sustava. Tok infekcije pokazuje da je za uspješno izvršavanje ovakve vrste virusa potrebno iskoristiti postojanu ranjivost sustava, preglednika ili njegovih dodataka, a što se uvijek može prevenirati pravovremenim ažuriranjem i zaštitom. Osim navedenih zlonamjernih softvera česti su i potencijalno neželjeni programi, PUP (engl. *Potentially Unwanted Programs*), koji mogu biti instalirani bez znanja korisnika, a dio su softverskog paketa ili neke instalacije. Uključuju reklamne softvere (engl. *adware*) ili poveznice na Internet-preglednike koje antivirusni programi automatski blokiraju i uklone. Dodatno postoje i *spyware*, *keyloggers*, crvi (engl.*worms*), *logic bombs* te ostali zlonamjerni softveri čija su ponašanje i aktivnosti moguće detektirati kroz programe za zaštitu uređaja i sustava, a dodatan se oblik zaštite uvijek odnosi i na osvješćivanje i edukaciju korisnika [7].

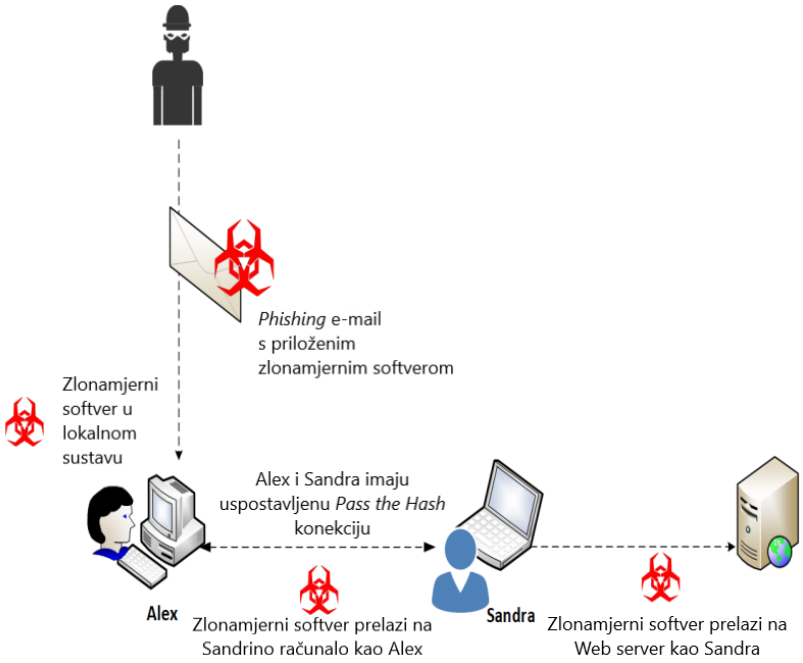
Prevencija neželjenog sadržaja kod individualnih korisnika je uvijek moguća no veće organizacije s većom količinom osjetljivih podataka na korisnikovom krajnjem uređaju ne smiju se uzdati samo u preveniranje napada jer današnji kibernetički napadači iskorištavaju napredne tehnologije na bazi umjetne inteligencije i strojnog učenja koje bez problema zaobilaze postojane programe zaštite i inficiraju sustave i uređaje. Iz tog razloga organizacije moraju težiti optimalnom omjeru

veličine poslovanja i količine osjetljivosti informacija koje iziskuje te njihovoj pravodobnoj i kompletnoj zaštiti.

3.3.Kompromitiranje korisničkih identiteta

Nakon napada *ransomware*-om i metodom *backdoor*-a, korištenje ukradenih korisničkih vjerodajnica je prema Verizon 2022 DBIR [8] jedan od najučestalijih načina kompromitiranja sustava i mreže, a više od 80% incidenata povezanih s organizacijskim web serverima uključuju ukradene vjerodajnice. Ova opasnost tjera organizacije da sve više guraju prema poboljšanju sigurnosnog aspekta korisničkog identiteta. Autentifikacija s korisničkim imenom i zaporkom zamjenjuje se multifaktorskom autentifikacijom koja sve više dobiva na popularnosti no u mnogim korporativnim okruženjima ta metoda i dalje nije zadana kao obavezna. Multifaktorska autentifikacija je dodatan sloj sigurnosti identiteta no ipak korisnik je najslabija karika u takvoj uslojenoj sigurnosti.

Upravo je socijalni inženjering fokusiran na ljudski faktor u informacijskoj sigurnosti, a povezane tehnike napadačima omogućuju fizičke pristupe organizaciji, pristupe sustavima i mrežama pa i naivan pristup osjetljivim informacijama od samog korisnika. Vrsta zlonamjernog sadržaja kao što je socijalni inženjering temelji se na manipulativno-strategijskim metodama kojima zlonamjerni akteri ostvaruju željene aktivnosti, što podrazumijeva utjecaj na korisnika da sam izvrši određenu radnju, a koju inače ne bi. Principi po kojima socijalni inženjeri postižu takvu kontrolu nad korisnicima su pokazivanje autoriteta, zastrašivanje kroz suptilnu prijetnju, povjerenje, hitnost, familijarnost te nestašica čime nešto čini poželjnim. Svaki princip po kojem se napadači vode u većini slučajeva daje određeni rezultat jer čine da korisnik reagira u trenutku bez čekanja i razmišljanja. Važan čimbenik socijalnog inženjeringa je poznavanje ciljanog korisnika, razumijevanje načina na koji ljudi reagiraju te kako stresna situacija može biti iskontrolirana u korist napadača. Najčešće tehnike socijalnong inženjeringa su *phishing*, prikupljanje osjetljivih podataka kao što su korisnička imena i lozinke, napadi na web stranice, neželjene poruke (engl. *spam*), krađa identiteta i impersonacija, izviđanje te tehnike stupanja u fizički kontakt s ciljanom metom, a sve one dovode do kompromitiranja korisničkog identiteta. *Phishing* je širok pojam vezan uz socijalni inžinjering koji opisuje prijevarno stjecanje osjetljivih informacija vezanih uz korisničke račune. Upravo Slika *3.3* prikazuje ozbiljnost prijetnje *phishing* maila.



Slika 3.3: Prelazak *malware*-a s jednog računala na drugo *phishingom* [10]

Najčešće se izvodi putem maila no postoje i verzije phishinga koje se izvode putem SMS poruka (engl. *smishing*) ili telefonskim pozivima (engl. *vishing*). Također, pokušaji phishinga mogu ciljati konkretne osobe ili grupe (engl. *spear phishing*) te zaposlenike na višim pozicijama s većim pravima pristupa (engl. *whaling*). *Pharming* je još jedna vrsta phishinga orijentirana na web stranice gdje promet k legitimnim web stranicama usmjerava prema njihovim zlonamjernim verzijama, dok je *watering hole* inficiranje web stranica koje korisnik često posjećuje. Socijalni inženjering se može provoditi na bilo kakav način gdje postoji bilo kakav kontakt s krajnjim korisnikom na kojeg se može utjecati i manipulirati. Obrana od navedenih napada svodi se na osvješćivanje zaposlenika, educiranje o *phishingu*, kako prepoznati, prijaviti i odgovoriti te inscenirati lažne *phishing* mailove zaposlenicima, a sve u svrhu smanjenja broja uspješno provedenih napada tehnikama socijalnog inženjeringa.

Iako se napadi socijalnim inženjeringom koriste i za dohvaćanje korisničkih lozinki, postoje konkretni načini napada na lozinke. Jedan od takvih je *brute-force* napad koji prolazi kroz listu lozinki ili najčešće korištenih riječi u sklopu lozinke dok ne pronađe izraz koji funkcionira. To je jednostavan način napada koji prolazi kroz velik broj različitih varijacija dok se ne pronađe jedna uspješna. Mnogi programski alati za probijanje lozinki često su korišteni i od strane tehničkog osoblja organizacije s ciljem procjene jačine zaporki u organizaciji. Snažne i kompleksne zaporke dobra su prevencija mnogih napada probijanja lozinki te je u današnje vrijeme većina organizacija

implementirala metodu multifaktorske autentifikacije koja od korisnika zahtjeva dva ili više verifikacijskih faktora za pristup organizacijskim računima, aplikacijama ili VPN-u. Dodatan važan sigurnosni korak je izbjegavanje spremanja lozinki. Kao još jedan napad na lozinke je napad predajom *hasha* (engl. *Pass the Hash*) gdje napadač dolazi u posjed *hasha* lozinke i jednostavno ga iskorištava u postupku autentifikacije. Ovaj napad iskorištava manu u autentifikacijskom protokolu jer *hash* lozinke ostaje isti za svaku sesiju sve dok ne dođe do promjene lozinke. Ova mana najčešće se iskorištava na Windows operacijskom sustavu kod metode jednostruke prijave (engl. *Single-sign-on*). Impakt PtH napada se sprječava modelima najmanje privilegije (engl. *Least privilege*) i odvajanja privilegiranih od neprivilegiranih računa te upravljanjem zaporkama [7][9].

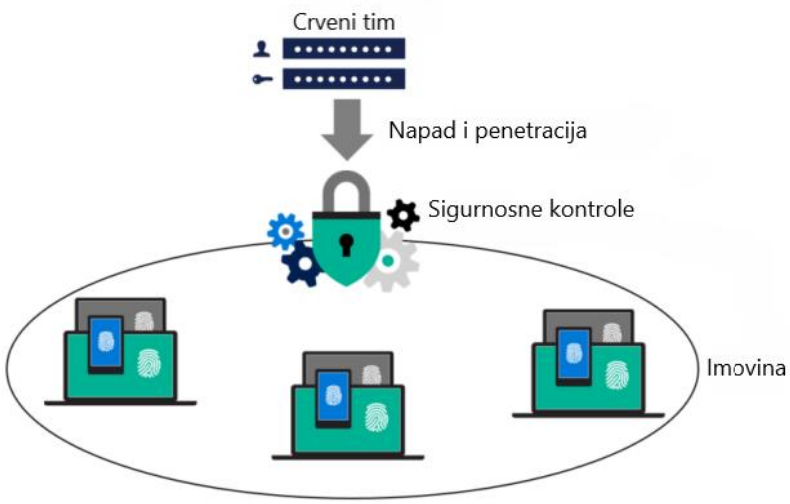
4. SIGURNO UPRAVLJANJE KRAJNJIM UREĐAJIMA

Laptopi, desktop računala, tableti, pametni telefoni i ostali krajnji mrežni uređaji predstavljaju izvor konstantne ugroze organizaciji. Takvi sustavi direktno komuniciraju s krajnjim korisnicima i zahtijevaju snažno konfiguracijsko upravljanje kako bi zadržali optimalnu razinu sigurnosti i smanjili količinu ranjivosti u organizacijskoj mreži. Sigurnosno upravljanje krajnjim uređajima podrazumijeva osnaživanje sistemskih konfiguracija s ciljem povećanja otpornosti na kibernetičke napade, odnosno smanjenja površine napada identifikacijom i sanacijom organizacijskih slabosti. Iako postoje savjeti za pojedinačno osnaživanje konfiguracija operacijskog sustava, baze podataka, BIOS-a, softvera i mreža, općenita strategija i zadaci osnaživanja konfiguracija bilo kojeg računalnog dijela organizacije svodi se na:

- upravljanje pristupima, odnosno fizička sigurnost sustava, informiranje osoblja o sigurnosnim procedurama, postavljanje snažnih lozinki, ograničavanje broja korisnika s privilegiranim načinima pristupa i prekomjernim pristupom te dopuštanje povišenih privilegija po potrebi,
- kontrola mrežnog prometa, instalacija snažnih sustava iza vatrozida ili izoliranih od javne mreže, korištenje VPN-a ili *proxya* pri spajanju te snažna enkripcija komunikacije,
- uklanjanje nepotrebnih i rijetko korištenih softvera, sistemskih komponenata i aplikacijskh značajki koje pridonose izloženosti uređaja slabostima i prijetnjama,
- redovite sigurnosne kopije po modelu 3-2-1, tri sigurnosne kopije na dva tipa medija, a jednom spremljenom izvan organizacije i
- osnažene udaljene sesije putem SSH-a (engl. *Secure Shell*) sa snažnim zaporkama ili certifikatima, a izbjegavanjem korištenja zadanih (engl. *default*) portova.

Upravljanje zakrpama (engl. *Patch Management*) ili nadogradnja softverskih aplikacija i sustava ima za cilj ispraviti postojeće probleme i nedostatke u softveru, a koji su primijećeni tek nakon izdanja verzije. Većina zakrpa se ponajviše odnosi na poboljšanje sigurnosti dijelova sustava te određenih funkcionalnosti. U ovom sloju zaštite bitno je brzo i na vrijeme djelovati s ispravljanjem postojećih problema jer otkrivena ranjivost u bilo kojem dijelu organizacije odmah postaje laka meta za kibernetičke napade. Primjer softvera za upravljanje sustavima i zakrpama je *Microsoft System Center Configuration Manager* (SCCM) koji administratorima daje jednostavan uvid u statuse zakrpa sustava i aplikacija s automatskim saniranjem i nadogradnjom tehnologije ukoliko je ono potrebno [5][11].

Penetracijsko testiranje dio je zaštitne mjere u korporacijama koje rade u smjeru dodatnih provjera postojanih zaštita na krajnjim uređajima. Tehnike testiranja uključuju simulirane napade na organizaciju s informacijama, alatima i tehnikama dostupnim pravim kibernetičkim napadačima. U tu svrhu razvijeni su crveni i plavi tim, a generalna ideja iza timova je demonstrirati efektivnost napada simulacijama. Crveni tim (engl. *Red team*) je sadržan od visoko treniranih individualaca, različitih setova vještina i dobrim poznavanjem i razumijevanjem trenutnih trendova prijetnji koje prijete organizaciji. Slika *4.1* prikazuje tijek rada crvenog tima. Prvi korak je napad i penetriranje u okruženje probojem postojećih sigurnosnih kontrola, odnosno penetracijsko testiranje, a zatim se fokusira na traženje ranjivosti s mogućnošću iskorištavanja kako bi se zadobio pristup organizacijskoj imovini. Faze napada i penetracijskog testiranja uglavnom prate faze *Lockheed Martin* pristupa što je i objašnjeno u pod-poglavlju 3.2.



Slika 4.1: Slikoviti prikaz procesa testiranja crvenog tima, [10]

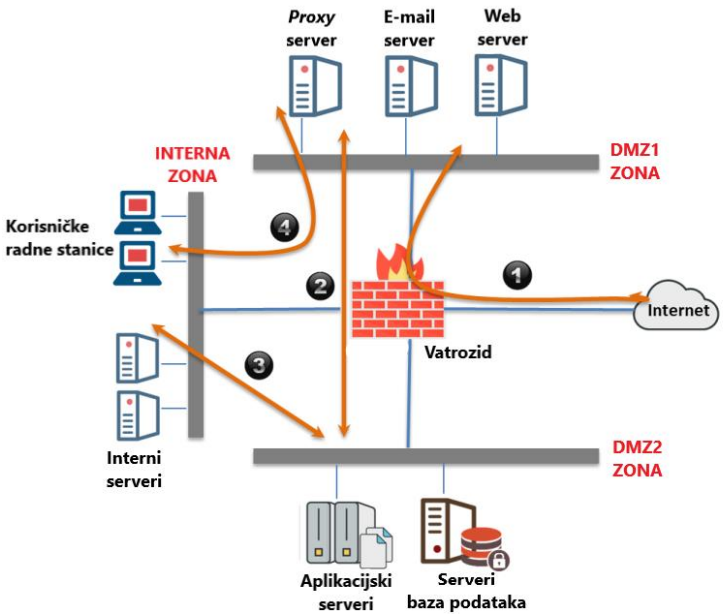
Većina testova uključuje iskorištavanje kombinacije ranjivosti na nekoliko sustava što dovodi do ostvarenja većeg pristupa organizacijskoj imovini nego što bi to uspjeli s iskorištavanjem pojedinačnih slabosti. Rezultati penetracijskog testiranja pokazuju koliko dobro sustavi toleriraju stvarne napade, razinu vještina i alata potrebnih napadaču za uspješno kompromitiranje sustava, potrebu za uspostavom dodatnih sigurnosnih mjera te sposobnost postojećih mjera da detektiraju, preveniraju i odgovore na napade na vrijeme. Upravo je ova vrsta testiranja sigurnosti u organizaciji jedna od najboljih mjera kojima se provjerava struktura kibernetičke sigurnosti u korporaciji. Prema [12], penetracijsko testiranje provodi se u četiri faze. Definiranje pravila i dokumentacije te postavljanje ciljeva testiranja odvija se u fazi planiranja nakon čega slijedi faza

otkrića gdje započinje pravi napad, a sastoji se od skupljanja i skeniranja informacija te analize ranjivosti usporedbom sustava i aplikacija skeniranih uređaja s bazom podataka ranjivosti. Sami napad u idućoj fazi provjerava ranije identificirane slabosti u uređaju pokušavajući ih iskoristiti. Napad se kreće od dobivanja pristupa i eskaliranja privilegija preko pregledavanja sustava i pokušaja širenja na ostale pa sve do inficiranja instalacijom dodatnih alata za veću kontrolu i površinu napada, odnosno prema fazama *Cybersecurity Kill Chain*-a. Objašnjena sigurnosna mjera je bitna za određivanje ranjivosti organizacijske mreže i razine štete koja može nastati u slučaju kompromitiranosti. Plavi tim (engl. *Blue team*) predstavlja drugi dio vježbe, a zadužen je za osiguravanje da je sva imovina pravilno zaštićena. Ukoliko crveni tim otkrije ranjivost i upotrijebi ju protiv organizacije, plavi tim mora u istom trenutku reagirati, sanirati i dokumentirati. Neki od zadataka plavog tima su pohranjivanje, analiziranje i validiranje dokaza prikupljenih tijekom napada crvenog tima, koordinacija s ostalim timovima čija je reakcija potrebna ovisno situaciji, trijaža incidenata, praćenje opsega napada, kreiranje plana oporavka i izvršavanje kako bi se organizacija na što brži i bezbolniji načini oporavila od doživljenog napada. Životni ciklus napada, dokazi, incidenti, invadirani uređaji i sustavi, iskorištene slabosti i sve ostale aktivnosti koje su se odvile tijekom testiranja crvenog i plavog tima moraju biti pravilno i detaljno dokumentirani kako bi se moglo djelovati u smjeru napretka i minimiziranja nedostataka u sigurnosti organizacije [10].

Sigurnost krajnjih uređaja ima nekoliko slojeva zaštite, od ljudskog faktora i educiranja, osnaživanja konfiguracija i zakrpa pa sve do konkretno programiranih alata i tehnologija za zaštitu krajnjih uređaja. Takve tehnologije dizajnirane su da osnaže organizacijske sigurnosne ciljeve, a povećanjem i širenjem svog poslovnog utjecaja organizacija treba djelovati u smjeru veće, snažnije i kompletnije zaštite vlastitih sustava. Spomenuti programi djeluju i impelementirani su na svakom organizacijskom uređaju, a upravljani su i promatrani od strane centraliziranog sustava putem kojeg administratori imaju uvid u statuse aktivnosti uređaja, moguća neželjena ponašanja i radnje. Minimum svakog zaštitnog programa treba uključivati antivirusni softver za skeniranje sustava od poznatih zlonamjernih programa koji mogu ugroziti sigurnost uređaja. Potpoglavlja u nastavku spominju i objašnjavaju najčešće sigurnosne kontrole za zaštitu krajnjih uređaja te administrativne i fizičke kontrole.

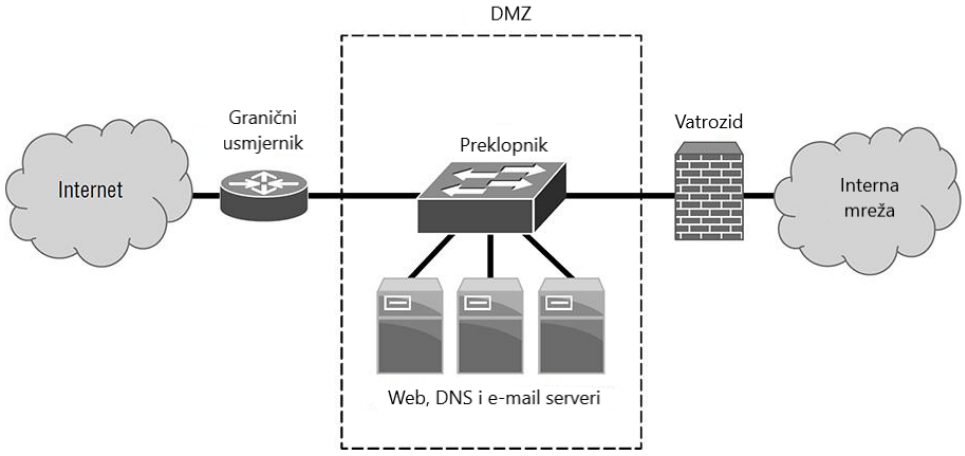
4.1. Mrežne sigurnosne kontrole

Mrežom se ostvaruje konekcija između komponenata organizacijskog informatičkog sustava prenoseći podatke kako unutar organizacije tako i prema vanjskim mrežama. Maksimalna sigurnost mreže prioritet je svakog korporativnog okruženja, a ono se ostvaruje dizajniranjem sigurnog mrežnog sustava. Segmentacija mreže je praksa odvajanja mreže na manje mrežne segmente pri čemu se odvajaju grupe sustava ili aplikacija među kojima nema interakcije. Takav način ograničava kako komunikaciju u mreži tako i mrežne napade jer ako napadač i uspije probiti sigurnosni perimetar ne može iz jednog segmenta pristupiti mrežnim resursima drugog segmenta. Ono se najčešće postiže postavljanjem vatrozida između segmenata mreže s različitim razinama povjerenja ili funkcionalnim zahtjevima. Slika *4.2* prikazuje princip rada segmentacije mreže koja odvaja servere u mreži gdje su korišteni jedan vatrozid, dvije demilitarizirane zone i interna zona. Web i e-mail serveri su odvojeni od servera koji ne zahtijevaju direktan pristup internetu jer su oni najpodložniji napadima te odvojenost od ostatka mreže reducira moguću štetu. Promet između interne i DMZ2 zone omogućen je u oba smjera zbog potreba autentifikacije i *backup*-a. Vatrozid propušta promet iz javne mreže prema DMZ1 zoni putem određenih portova (80, 25, 443, itd.), ali promet prema DMZ2 zoni nije omogućen. Ukoliko korisnik iz interne zone želi pristup internetu, on je omogućen putem HTTP *proxy* servera u DMZ1, a u slučaju kompromitiranosti te zone, interna zona je i dalje sigurna s obzirom da je komunikacija između te dvije zone jednosmjerna.



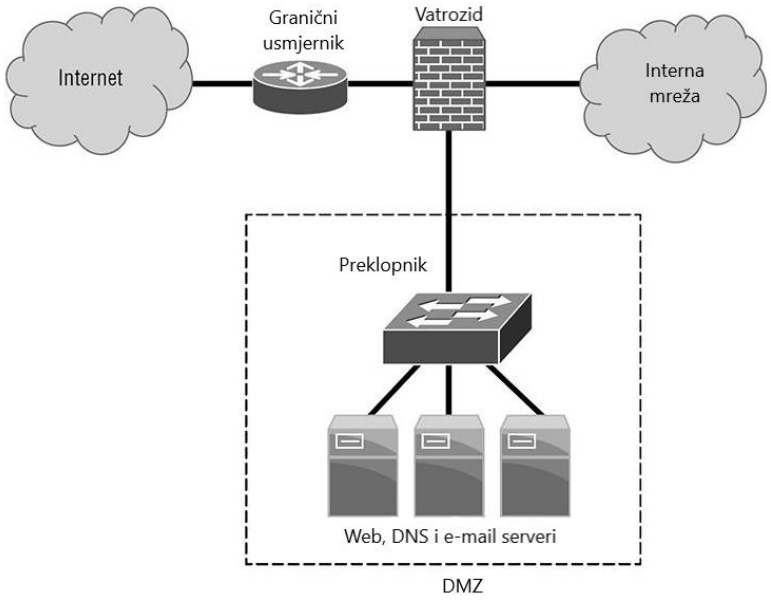
Slika 4.2: Primjer segmentacije organizacijske mreže, [10]

Najjednostavniji dizajn mreže podrazumijeva mrežu s jednostrukim vatrozidom kako je prikazano na Slika *4.3*. Vatrozid je smješten između dvije sigurnosne zone s različitim razinama povjerenja, odnosno implementiran je za internu mrežu sa segmentom mreže DMZ u kojem su smješteni web, e-mail i DNS serveri okrenuti prema vanjskoj mreži. Demilitarizirana zona ili DMZ je manja mreža smještena između privatnog dijela organizacijske mreže i vanjske javne mreže. Koristi se u slučaju potrebe izlaganja sustava područjima s manjim razinama povjerenja, odnosno prevenira neautoriziranog korisnika da dobije direktan pristup organizacijskim serverima. Iz tog razloga je DMZ smatran kao dodatni sloj mreže. Na slikama je prikazano da se najčešće sastoji od web, e-mail i DNS servera, a konfigurirana je tako da je omogućena konekcija za eksterne i interne mreže te se korisnici u DMZ zoni mogu spojiti na eksternu mrežu, ali ne i na internu.



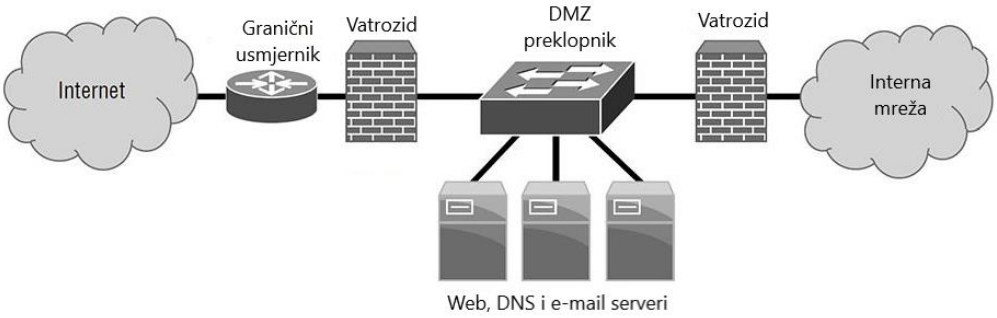
Slika 4.3: Mreža s jednostrukim vatrozidom, [5]

Idući dizajn, Slika *4.4*, prikazuje vatrozid s višestrukim sučeljem gdje se privatna mreža zajedno s DMZ-om nalazi iza istog vatrozida no s različitim pristupima i pravilima na način da bi prema pravilima promet iz vanjske mreže do DMZ-a bio propušten, ali bi bio spriječen da dosegne zaštićenu internu mrežu.



Slika 4.4: Vatrozid s višestrukim sučeljem, [5]

Slika 4.5 prikazuje dizajn mreže upotrebom više vatrozida gdje su isti postavljeni na kritičnim kontrolnim točkama. Takav način kreira više segmenata mreže, a svaki s različitim sigurnosnim razinama. Na slici je prikazana manja korporativna mreža s vatrozidom koji štiti DMZ te internu mrežu zaštićenu dodatnim vatrozidom gdje se nalazi ostatak krajnjih uređaja organizacije. U ovom slučaju interna mreža je najsigurnija zona, DMZ je druga najsigurnija zona, a krajnji usmjernik okrenut prema Internetu je najizloženiji dio mreže.



Slika 4.5: Višestruki vatrozidi, [5]

Standardna ustaljena zaštita u svakoj organizaciji odnosi se na uporabu vatrozida (engl. *firewall*) koji mogu biti u obliku softvera i/ili hardvera, a općenito je korišten u svrhu odvajanja zaštićene mreže od nezaštićene javne mreže. Dizajniran je da nadgleda i filtrira dolazni i odlazni promet u

mreži te u ovisnosti o organizacijskim policama blokira ga ili propušta u mrežu, prevenira neautoriziran pristup unutarnjoj mreži. Vatrozid je kombinacija više tehnologija koje zajedno upotpunjuju svrhu. Tehnologije uključuju filitriranje paketa, posredničke poslužitelje, liste kontrola pristupa, prevođenje mrežnih adresa, aplikacijske pristupnike i VPN. Filtriranje paketa radi se na mrežnom sloju ISO/OSI modela, a filtrira prema definiranim setovima pravila prije prosljeđivanja, a ona se uglavnom odnose na sadržaj zaglavlja paketa koji uključuje izvorišnu i destinacijsku adresu, port, protokol, a pristupna i aplikacijska filtriranja dodatno filtriraju ovisno o specificiranim pravilima uspostavljanja sesije odnosno protokolima i komandama na aplikacijskoj razini [5].

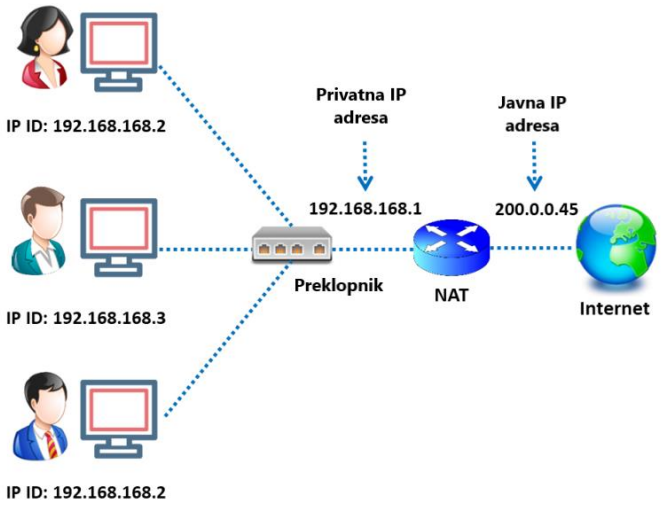
Posrednički poslužitelj ili *proxy* server filtrira konekcije bazirane na servisima i protokolima aplikacije ili sustava na kojem se nalazi i na taj način štiti direktnu vezu između korisnika na Internetu i internetskih resursa. Primjer proxyja je FTP (engl. *File Transfer Protocol*) proxy koji propušta samo FTP promet, a sve ostale pakete i protokole blokira. To je tip servera koji se kao posrednik nalazi između klijenata od kojeg prima zahtjeve te destinacijskog servera kojem prosljeđuje zahtjev za određenim resursom, a pritom skrivajući identitet klijenta u mreži. Svrha *proxy* servera je zaštititi identitet klijenta, odnosno njegovu IP adresu od odredišnih servera kojima se šalju. Web zahtjev od strane klijenta prvo odlazi na posrednički poslužitelj koji taj zahtjev prosljeđuje na Internet i zaprima odgovore u ime klijenta, a pojednostavljeni proces dan je na Slika *4.6* s HTTP zahtjevima i odgovorima. *Proxy* može promijeniti IP adresu klijenta na zahtjevu i generirati novu javnu IP adresu tako da web server nije u mogućnosti locirati korisnika.

Slika 4.6: Primjer posredničkog poslužitelja između klijenta i destinacijskog servera, [13]

Prednji posrednički poslužitelj (engl. *forward proxy*) radi na provjerama korisničkih zahtjeva prije propuštanja na javnu mrežu kako bi se osigurao da zahtjev ide prema legitimnim vanjskim

resursima, dok obostrani posrednik (engl. *open proxy*) prima zahtjeve s Interneta te ih prosljeđuje u zaštićenu mrežu [10][13].

Prevođenje mrežnih adresa (engl. *Network Address Translation*) ili NAT je još jedna tehnologija u sklopu vatrozida koja se odnosi na proces prevođenja privatne IP adresa u javnu pri čemu štiti unutrašnje adrese od vanjskih napadača. Slika *4.7* slikovito objašnjava proces prevođenja privatne IP adrese preklopnika u javnu IP adresu dostupnu na javnoj mreži. Kada korisnik zaštićene mreže pošalje paket prema vanjskoj mreži, NAT modificira izvorišnu IP adresu paketa tako da se čini kao da i dalje dolazi s validnog izvora, a ista situacija se događa kada dolazi paket iz vanjske mreže u unutarnju. NAT modificira destinacijsku IP adresu u pravu vidljivu IP adresu interne mreže. Modificiranje se može raditi i na razini izvorišnog i destinacijskog porta. NAT može biti konfiguriran kao tehnika filtriranja gdje dopušta sve konekcije koje su originalno krenule iz interne mreže, a blokirati sve one pokrenute od strane vanjske nezaštićene mreže.



Slika 4.7: Primjer prevođenja mrežnih adresa, [10]

Dalje, važno je spomenuti i privatnu, VPN (engl. *Virtual Private Network*) mrežu koja koristi javnu mrežu za siguran prijenos osjetljivih informacija preko povjerljive mreže korištenjem enkripcije i enkapsulacije. Umjesto slanja paketa direktno na ISP (engl *Internet Service Provider*), najprije se usmjeravaju na VPN sever tako da se čini kao da je paket originalno krenuo od servera. Server dodatno maskira korisnikovu IP adresu. Preko VPN-a korisnici jedne mreže ostvaruju konekciju s korisnicima druge mreže prilikom čega se provodi enkripcija i zaštita integriteta kako bi se javna mreža iskoristila kao privatna, odnosno postavlja se sigurnosni tunel oko korisnikova

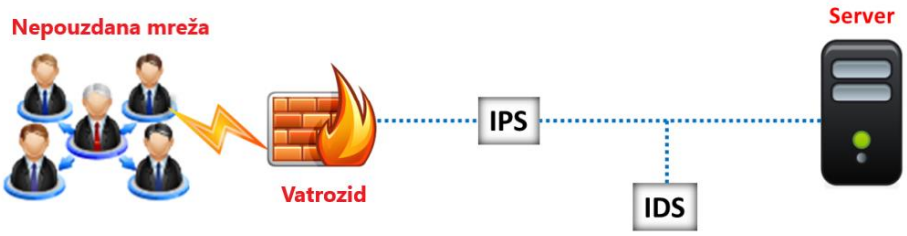
identiteta. Ovakav sigurnosni mehanizam je alat kojeg organizacije nameću svojim zaposlenicima pri udaljenom radu i pristupu organizacijskoj imovini.

Iduća Generacija Vatrozida (engl. *Next-Generation Firewalls*, NGAW) je napredan tip vatrozida koji ide dalje od same inspekcije portova i protokola. Na dodatne tehnologije vatrozida NGAW dodaje inspekciju sadržaja poslanog paketa. Ugrađene značajke su IPS/IDS funkcionalnosti, značajke antivirusnih alata za skeniranje prometa, geolokacijske sposobnosti za uspoređivanje prijetnji u stvarnom svijetu, *proxy* za presretanje paketa, *sandboxing* te web aplikacijske vatrozide dizajnirane za zaštitu web aplikacija. NGAW je najčešće implementieran s ciljem zaštite mreže organizacije, a ne kao individualni domaćinski vatrozid na krajnjim uređajima. Prije planiranja implementacije vatrozida bitno je upoznati se sa značajkama svakog te poznavajuć mogućnosti implementirati onaj koji više odgovara potrebama sigurnosti okruženja ili pak odlučiti se za drugu vrstu sigurnosne kontrole.

Sustavi detekcije i prevencije upada (engl. *Intrusion Detection/Prevention System*, IDS/IPS) su sustavi promatranja mrežnog prometa za sumnjive aktivnosti i upozorenja koja mogu indicirati mrežni ili sustavni sigurnosni proboj. Mogu biti implementirani u same mrežne komponente, module unutar preklopnika i usmjerivača ili kao značajka samog operativnog sustava. U slučaju detekcije uzorka sumnjive radnje u mreži, potpisa ili neobičnog prometa, IDS šalje upozorenje administratoru mreže, dok IPS dodatno poduzima korektivne mjere. Sustav detekcije upada dijeli se na:

- mrežni sustav detekcije upada (*Network Intrusion Detection System,* NIDS*)*, smješten u određenom dijelu mreže za provjeru prometa svih uređaja na mreži,
- domaćinski sustav detekcije upada (*Host Intrusion Detection System,* HIDS*)* na pojedinačnim domaćinima ili uređajima u mreži tako da sustav provjerava ulazne i izlazne pakete vezane uz uređaj,
- protokolni sustav detekcije upada (*Protocol-based Intrusion Detection System,* PIDS*)* koji se sastoji od sustava ili agenta na prednjem kraju servera glumeći protokol između korisnika/uređaja i servera,
- aplikacijsko-protokolni sustav detekcije upada (Application *Protocol-based Intrusion Detection System,* APIDS*)* smješten u grupi servera, a radi na sloju aplikacijskih protokola gdje promatra i interpretira njihovu međusobnu komunikaciju što za primjer može biti SQL protokol i njegova interakcija s bazom podataka na web serveru te
- hibridni sustav detekcije upada koji predstavlja kombinaciju dva ili više tipa IDS-a.

IDS-ovi rade na mehanizmima prepoznavanja poznatih potpisa zlonamjernih aktivnosti u obliku specifičnih uzoraka u mrežnom prometu te prepoznavanja anomalija korištenjem strojnog učenja što pomaže u detektiranju nepoznatih i novih zlonamjernih softvera. Detekcija bazirana na strojnom učenju daje bolje rezultate u odnosu na prepoznavanje specifičnih uzoraka jer takav model po svojoj prirodi može biti treniran prema aplikacijskim i hardverskim konfiguracijama, a sve nepoznato i izvan okvira modela smatra se sumnjivim i potencijalno opasnim. Povećanje i nadogradnja IDS-a pronalazi se u IPS-u. Iako oboje rade na sloju mrežnog prometa snimajući promet i sustavne aktivnosti u svrhu pronalaska sumnjivih radnji, IPS može dodatno odgovoriti na detektiranu prijetnju tako da ju prevenira prije izvršavanja, a razlog tome je lokacija IPS-a koji se nalazi na samom putu između servera i neidentificirane mreže. Slika 4.8 prikazuje razliku u postavljanju IDS-a i IPS-a u mreži, a time i razliku u načinu rada.



Slika 4.8: Razlika IDS – IPS, [10]

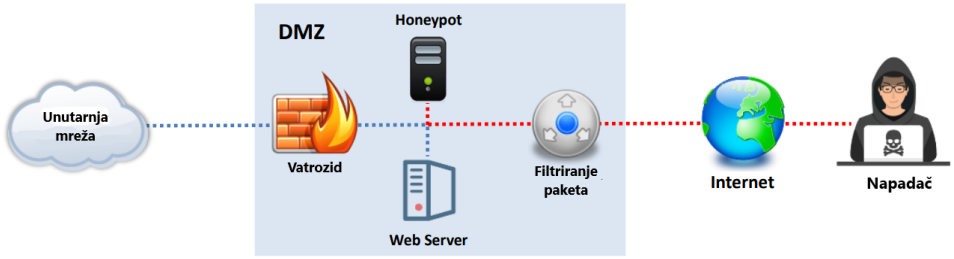
IPS se klasificira na:

- mrežni sustav za prevenciju upada (engl. *Network-based intrusion prevention system*, NIPS), promatra kompletni mrežni promet analizom aktivnosti protokola,
- bežični sustav za prevenciju upada (engl. *Wireless intrusion prevention system*, WIPS) nadgleda bežičnu mrežu za sumnjivi promet analizom protokola za bežično umrežavanje,
- analiza ponašanja mreže (engl *Network behavior analysis*, NBA) odnosi se na nadgledanje mrežnog prometa u svrhu pronalaska dijela koji generira sumnjiv i neobičan tok prometa što navodi na distribuirani DOS napad ili specifične oblike zlonamjernog softvera i
- domaćinski sustav za prevenciju upada (engl. *Host-based intrusion prevention system*, HIPS) koji radi na pojedinačnim hostovima na način da analizira i skenira događaje vezane uz tog domaćina.

Za razliku od IDS-a, IPS ima mogućnost aktivnog preveniranja ili blokiranja detektiranih upada, poduzimanja mjera koje će obavijestiti administratorima o problemima u mreži, ponovnog

pokretanja konekcije, otpuštanja paketa detektiranih kao dio zlonamjernnog softvera ili blokirati promet s određenim IP adresama [10][13].

Mnoge organizacije raspoređuju *honeypote* kao rane sustave upozorenja protiv potencijalnih napada. To je sigurnosni računalni sustav koji se postavlja kao mamac za privlačenje napadača s ciljem penetracije organizacijske mreže. Sam po sebi, *honeypot* ne generira promet niti ima ikakvu autoriziranu aktivnost no ono što može je spremati logove pokušaja pristupa portovima i nadgledati moguće zlonamjerne aktivnosti u sustavu jer svaka interakcija s *honeypotom* je vrlo vjerojatno zlonamjerna. Mogu simulirati pojedine sustave, aplikacije i baze podataka sa značajkama i dodacima ranjivim na napade, cijelu mrežu ciljane organizacije pa i stvarni operacijski sustav. Slika 4.9 pokazuje primjer postavljanja *honeypota* u zaštićenoj mreži.



Slika 4.9: Primjer postavljanja *honeypota* u mreži, [10]

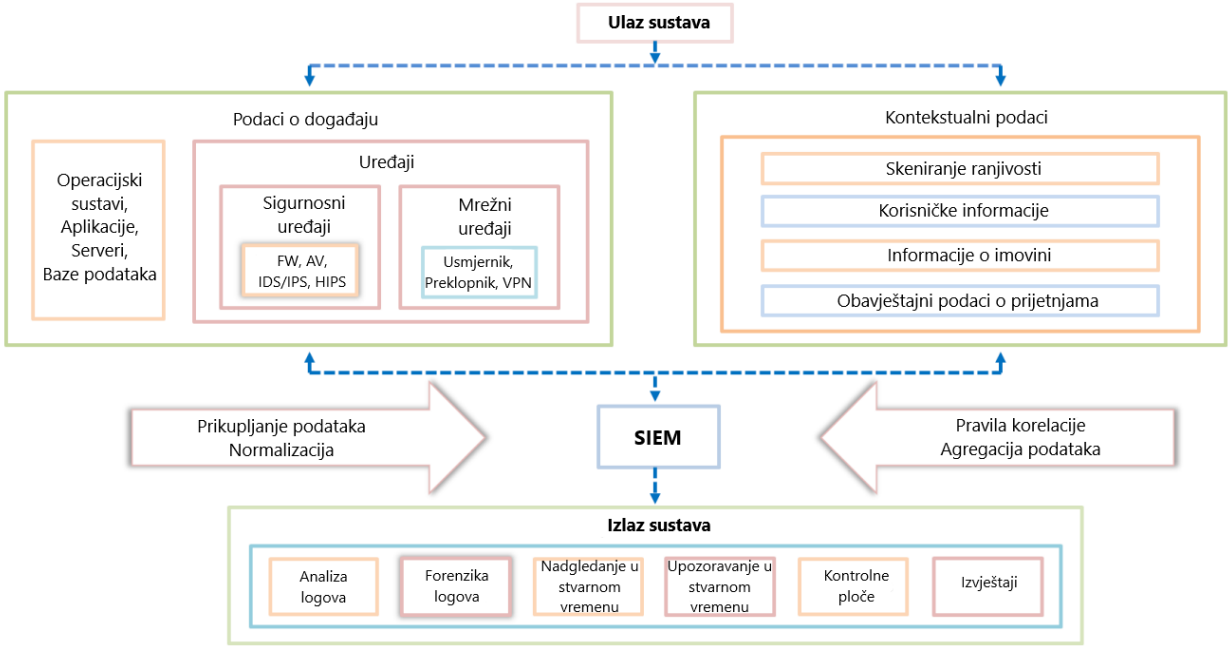
Sigurnost krajnjih uređaja u velikoj je mjeri održana i ovisna o mnogim ustaljenim tehnologijama zaštite krajnjih uređaja pod koje pripadaju i antivirusna rješenja kao zadnji sigurnosni sloj između kranjeg korisnika i napadača. Antivirusni softveri ili AV-ovi skeniraju sadržaj memorije uređaja provjeravajući postojanost određenih uzoraka koji mogu ukazati na prisutnost zlonamjernih programa (engl. *malware*). Provjeravaju se uzorci temeljeni na potpisima ili definicijama poznatih zlonamjernih programa pri čemu se popis takvih programa stalno nadograđuje i važno je uvijek imati najnoviju inačicu sigurnosnog programa. Antivirusni alati fokusirani su na detekcije temeljene na prepoznavanju potpisa poznatih zlonamjernih softvera, a s vremenom su se proširili i na prepoznavanje poznatih uzoraka ponašanja. Tržište spomenutih zaštitnih programa fokusiranih na individualne krajnje uređaje je u današnje vrijeme sve veće i krajnjim korisnicima za osobnu potrebu nudi zadovoljavajuće rezultate. Neka takva rješenja nude *Kaspersky antivirus*, *360 Total Security*, *Avira*, *Microsoft Defender*, *BitDefender*, *Avast* i ostali. Takvi alati za detekciju zlonamjernih softvera i aplikacija građeni su na mehanizmima detekcije potpisa i ponašanja, umjetne inteligencije i strojnog učenja te *sandboxinga*. Detekcije bazirane na potpisu prepoznaju zlonamjerni softver prema otisku njemu pripadajućih datoteka ili komponenata softvera prethodno

povezanih s određenim zlonamjernim radnjama. AV alati rade s globalnim bazama podataka gdje uspoređuju datoteke s poznatim *hashevima* povezanim s određenim nelegitimnim aktivnostima. Ukoliko postoji pozitivno preklapanje datoteka je izolirana. AV-ovi kao prva linija obrane često su i najranjiviji jer napadi su postali sofisticiraniji tako da je ova metoda sve manje efektivna. Većina današnjih zlonamjernih softvera su polimorfna, odnosno opremljeni su mutacijskim dijelom koji ima sposobnost promjene određenih parametara datoteka i *hasha* tako da može kompletno odbaciti antivirusne programe s metodom prepoznavanja programa temeljenog na poznatom potpisu. Detekcije bazirane na ponašanju evaluiraju i analiziraju kod softvera te svaki zahtjev za pristup datotekama, procesima, konekcijama ili sustavima što uključuje svaku izvršenu naredbu na razini operativnog sustava ili drugog programa. Svaki pokušaj izvršavanja određene aktivnosti koju AV identificira kao sumnjivu ili nedopuštenu indicira da je softver zlonamjeran ili bar sumnjiv. Ponašanja koja ukazuju na potencijalnu opasnost su bilo koji pokušaj otkrivanja *sandboxing* okruženja i onemogućavanja AV softvera ili drugih sigurnosnih mehanizama, instalacija *rootkitova,* instalacija nepoznatih softvera, dodavanje i promjena korisničkih računa, uspostava neautorizirane konekcije s ostalim računima i web stranicama te mnoga druga [5].

Sandboxing je pojam koji označava izolirano i kontrolirano okruženje u kojem se bilo koji nepovjerljivi i potencijalno opasni softver može pokrenuti u svrhu njegova promatranja. Koriste se za dopuštanje svih aktivnosti softvera, dokumentiranje i dublju analizu. To je još jedan učestalo korišteni mehanizam koji koriste AV-ovi za evaluaciju sigurnosti softvera pokrećući ih i analizirajući u sigurnom okruženju. Cilj je temeljno provjeriti program i sve njegove komponente u izolaciji, prikupiti događaje u mreži te procesuirati što više prikupljenih podataka dobivenih iz bilo koje aplikacije ili sustava koji šalju podatke u *sandbox*. Virtualizacija može biti korištena u obliku sandboxinga pri čemu virtualni uređaj može postojati kao testno okruženju u kojem se ispituje legitimnost željenih programa ili aktivnosti [14].

Za ispunjavanje strogih zahtjeva, identifikacije prijetnji i vlastite IT imovine, organizacije moraju izvršiti reviziju informacija koje prolaze kroz cijelu organizacijsku mrežu. Upravljanje sigurnosnim incidentima i događajima (engl. *Security incident and event management*, SIEM) je sustav koje mnoge korporacije uključuju u svoje okruženje, a ima mogućnost pohrane i upravljanja velikom količinom logova iz različitih izvora, mreža, aplikacija, uređaja, sigurnosnih kontrola i korisničke aktivnosti u stvarnom vremenu. SIEM je sustav od velike važnosti u mrežnoj sigurnosti jer provodi nadgledanje i detekciju sigurnosnih događaja, forenzičku i post-incidentnu analizu, reviziranje te IT sigurnosnu i regulatorno izvještavanje, a dio je SOC operacija u organizaciji. Slika *4.10* predstavlja SIEM arhitekturu, a kombinira upravljanje sigurnosnim informacijama

(SIM) što se odnosi na upravljanje logovima, analizu, forenzičku istragu i praćenje usklađenosti te upravljanje sigurnosnim događajima (SEM) što predstavlja upravljanje prijetnjama i rukovanje sigurnosnim incidentima prikupljanjem i analizom informacija događaja iz različitih izvora u stvarnom vremenu. SIEM primjenjuje normalizaciju i agregaciju na podatke prikupljene iz različitih eksternih i internih izvora kao što su operacijski sustavi, mrežni uređaji, krajnji uređaji, *malware*-i, ranjivosti, informacije o identitetima i pristupima, itd. te nadgleda pristupe serverima i bazama podataka, korisničke aktivnosti kroz velik broj sustava i aplikacija u stvarnom vremenu i dodatno pruža zaštitu od različitih internih i eksternih prijetnji 51[10].



Slika 4.10: SIEM arhitektura, [10]

4.2.Fizičke sigurnosne kontrole

Fizička sigurnost igra važnu ulogu u svakoj organizaciji. Povlači za sobom zaštitu kritičnih informacija, mrežne infrastrukture, fizičke opreme i uređaja, objekata i osoblja od ekoloških prijetnji, terorizma, vandalizma i krađe. Kao mrežna sigurnost, fizička sigurnost organizacijske imovine postala je sve izazovnija, a upravo zbog količine osjetljivih i teško dostupnih podataka na velikom broju laptopa, računala, USB-ova, itd. Ono je temelj informacijske sigurnosti organizacije jer povreda fizičke sigurnosti direktno prijeti integritetu, dostupnosti i povjerljvosti informacijskog sustava. Fizička sigurnost ne može biti osigurana na jednak način kao što je to opisano u prethodnim pod-poglavljima, a koji su se ticali sigurnosti mreže, aplikacija i baza

podataka. Ona treba biti implementirana na fizičkom dijelu OSI modela što uključuje sve mrežne sustave i sustave kabliranja, fizički pristup i podrška za napajanje takvim sustavima te okruženje koje podržava sustave. Vektori napada fizičke sigurnosti dijele se na prirodne/ekološke prijetnje kao što su poplave, požari, potresi, udari groma, temperatura i vlažnost te prijetnje od strane čovjeka, vandalizam, izgubljeni podaci i uređaji, šteta na fizičkoj opremi, krađa, socijalni inženjering, neautoriziran pristup sustavima i ostali.

Osnove koje organizacija pri planiranju i implementaciji fizičke sigurnosti treba uzeti u razmatranje su lokacija (susjedske zgrade, utjecaj katastrofalnih događaja, itd.), sustavi protiv požara, fizičke barijere i brave (ograde, kontrolna oprema za ulazak i izlazak prijevoznih sredstava, mehaničke/digitalne/elektroničke brave, itd.), sigurnosno osoblje (čuvari, sigurnosni policajci, nadglednik, itd), alarmni sustavi, video nadzor, sustav osvjetljavanja i napajanje. Kritičnu mrežnu imovinu kao što su serveri, rezervna oprema i sigurnosne kopije uvijek držati u odvojenoj prostoriji sa prikladnom kontrolom pristupa i videonadzorom. Također, bitno je osigurati prijenosne mobilne uređaje od mogućeg gubitka ili krađe, kao i definirati sigurnosne police vezane uz ograničavanje korištenja uklonjiivih uređaja (DVD, USB, SD kartica, mobilni uređaj, itd.). Većina organizacija koristi neku vrstu otiska s kojim zaposlenici imaju pravo na pristup prostorijama organizacije. To mogu biti kartice koje se očitavaju na ulazima i izlazima, biometrijski otisci, šifre i ostali sigurnosni mehanizmi koji limitiraju pristupe osoblju ovisno o razini i privilegijama. Uz sve navedeno implementiranim policama razmatra se cjelokupni dizajn fizičke sigurnosti i daju smjernice za adekvatnu sigurnost organizacije na sloju fizičke sigurnosti [10].

4.3. Odgovor na incidente i proces oporavka

Bez obzira na količinu obrane, tehnologije i alata kojima organizacije raspolaže u svrhu detekcije i prevencije bilo kakvog neautoriziranog upada, potrebno je uvijek pretpostaviti da do istog može. Svaki takav događaj po štetu organizacije ima snagu ugroziti temelj sigurnosti organizacije - integritet, povjerljivost i dostupnost informacija i sustava pod njezinom kontrolom. Događaj je svaka uočljiva pojava u sustavu ili mreži. To može biti korisnikov pristup datoteci, zahtjev serveru, slanje e-maila, blokiranje pokušaja upada od strane vatrozida i slično. Sukladno tome, računalni sigurnosni incident definira se kao kršenje ili neizbježnu prijetnju kršenja računalnih sigurnosnih polica, standardnih sigurnosnih praksi ili prihvatljivog korištenja polica. Primjer incidenta je slučaj kada napadač zapovijeda botnetu slanje velike količine zahtjeva za

spajanje na web server što za posljedicu ima njegovo rušenje ili korisnikovo otvaranje privitka u naizgled legitimnom mailu, a koji je zapravo zlonamjerni softver koji je pokretanjem inficirao računalo i uspostavio konekciju s vanjskim hostom. Takvi napadi su česti i nerijetko kompromitiraju sustave, privatne i poslovne podatke pa je od velike važnosti brzo i efektivno odgovoriti na svaku aktivnost koja ide na štetu organizacije. Iz tog je razloga proces odgovora na incidente (engl. *incident response*) postao obavezan dio organizacijskog planiranja implementacije sigurnosnih mehanizama i modela. Proces je sistematski, odnosno prati određenu metodologiju odgovora na incidente tako da su sve prikladne mjere poduzete te pomaže osoblju kod minimiziranja štete. Također još jedna prednost je mogućnost skupljanja i iskorištavanja informacija prikupljenih tokom rukovanja incidentom za bolju pripremu kod pojave budućih sličnih situacija. Proces rukovanja ima nekoliko faza koje detaljno prate sve događaje povezane s navedenim incidentom. Prva faza pripreme podrazumijeva uspostavljen i istreniran tim, prikupljanje potrebnih resursa za uspješno rukovanje te preveniranje incidenata tako da se provjerava jesu li sustavi, mreže i aplikacije dovoljno osigurani. Ovisno o evaluaciji sigurnosnog rizika u organizaciji priprema služi i za postavljanje dodatnih setova kontrola s ciljem prevencije i limitiranja količine kršenja standardnih sigurnosnih polica. Iako organizacija mora biti spremna odgovoriti na svaki nastali incident, vrlo je zahtjevan dio točno detektirati i evaluirati mogući incident, odnosno odrediti je li se dogodio i ako da, kojeg opsega i intenziteta. Znakovi incidenta dijele se na dvije kategorije, prethodnik kao znak da se incident može dogoditi u budućnosti i indikator, znak da se incident dogodio ili da se događa upravo sada. Navedeni znakovi identificiraju se korištenjem različitih izvora koji se dijele na

- upozorenja u obliku IDS/IPS, SIEM, AV softvera, softvera provjere integriteta datoteke, sustava za nadgledanje,
- logove koje generiraju mrežni uređaji, operacijski sustavi, servisi i aplikacije,
- javno dostupne informacije te
- ljude iz organizacije ili drugih organizacija.

Faza detekcije i analize bavi se provjerom legitimnosti i točnosti incidenta na temelju podataka iz pripreme te znakova za moguće kršenje pravila organizacije. Izvođenje inicijalne analize i validacije je kompleksan proces gdje je potrebno detaljno provjeriti dio organizacijske imovine i mreže te ustanoviti postoje li indikacije da se incident stvarno dogodio. Preporuke analize incidenta odnose se na profiliranje sustava i mreže kroz mjerenje karakteristika očekivanih i normalnih aktivnosti u ovisnosti o nepoznatim i sumnjivim događajima, razumijevanje normalnog ponašanja mreže, sustava i aplikacija u organizaciji kako bi sve izvan okvira normalnog moglo

biti što jednostavnije prepoznato, definiranje polica za zadržavanje i održavanje logova sustava, izvršavanje korelacije događaja kroz podatke iz logova nekoliko softvera (vatrozid, aplikacija, IDS/IPS), filtriranje podataka u svrhu uštede vremena te korištenje vanjskih izvora podataka sa što većom bazom podataka izvora prethodnika i indikatora. Osim detekcije događaja koji raspolaže s aktivnostima sumnjivim incidentnom timu te detaljne i kompleksne analize znakova i indikatora incidenta potrebno je dokumentirati svaki korak od trenutka detekcije incidenta pa do njegova razrješenja, uspostaviti sistem obavještavanja pojedinaca o događajima u organizaciji u što ulazi i detekcija incidenata te prioritizirati. Prioritiziranje rukovanja incidentima je jedna od kritičnih točaka u procesu jer incidenti ne smiju biti razrješavani prema redoslijedu pojave nego ovisno o faktorima kao što su funkcijski i informacijski utjecaj incidenta te mogućnost oporavka. Iduća faza razrješenja incidenta podrazumijeva zadržavanje, iskorijenjivanje i oporavak. Zadržati magnitudu incidenta je vrlo važno prije nego preplavi resurse ili poveća već nastalu štetu. Zadržavanje se većinom zahtjeva u ranoj fazi incidenta i daje vremena za razvoj prikladne strategije sanacije i oporavka. Organizacije bi trebale definirati prihvatljive rizike kod rukovanja s incidentima te prema tome razviti planove i strategije. Dalje sijedi iskorjenjavanje svih komponenti incidenta, kao što je uklanjanje zlonamjernog softvera, blokiranje korisničkih računa preko kojih se dogodio sigurnosni proboj kao i identificiranje i krpanje svih ranjivosti koje su iskorištene u procesu napada. Također, dolazi do oporavka i obnavljanja sustava u normalno operativno stanje te post-incidentna analiza kao zaključak u kojem se ide u smjeru napretka i učenja na greškama te nedostacima koji su se pokazali kroz nastali incident.

Kao što je već spomenuto, organizacija ne može u potpunosti ovisiti o zaštiti od napada i rizicima kojima je izložena. Od prirodnih katastrofa do napada predvođenim individualcima ili grupom napadača, organizacija je prisiljena štiti ti se od svakog štetnog utjecaja koji ima sposobnosti ugroziti organizacijske krajnje uređaje, mrežu pa i reputaciju. Iz tog razloga još jedna bitna komponenta obrane organizacije je sposobnost definiranja plana oporavka koji za cilj ima minimizirati štetu po organizaciju. Jedan takav plan je plan oporavka od katastrofe koji dokumentira procese i procedure koji se provode u nastojanju oporavka IT infrastrukture u slučaju katastrofe. S fokusom na informacijski sustav dizajniran je u svrhu vraćanja operativnosti oštećenih sustava, aplikacija i ostale računalne infrastrukture na alternativnoj lokaciji nakon događaja. Uz oporavak organizacije implementiraju i planove za nepredviđene situacije (engl. *contingency planning*), odnosno za situacije za „što ako“ koje se ne smiju ignorirati i umanjivati im značaj. Plan treba uzeti u obzir radne stanice, laptope i pametne uređaje, servere, web stranice, intranet, distribuirane sustave i moguće server sobe te pružiti adekvatnu strategiju i tehnike za

oporavljanje i vraćanje u prvobitno stanje. Uključivanje analize udara na poslovanje (engl. *Business impact analysis*) ili BIA pomaže koordinatorima za planiranje nepredviđenih situacija u jednostavnijoj koordinaciji i kategoriziranju zahtjeva i ovisnosti organizacijskih sustava. BIA je sistematski proces predviđanja posljedica poremećaja funkcija i procesa poslovanja te skupljanja informacija potrebnih za razvoj strategije oporavka, a radi se u tri koraka:

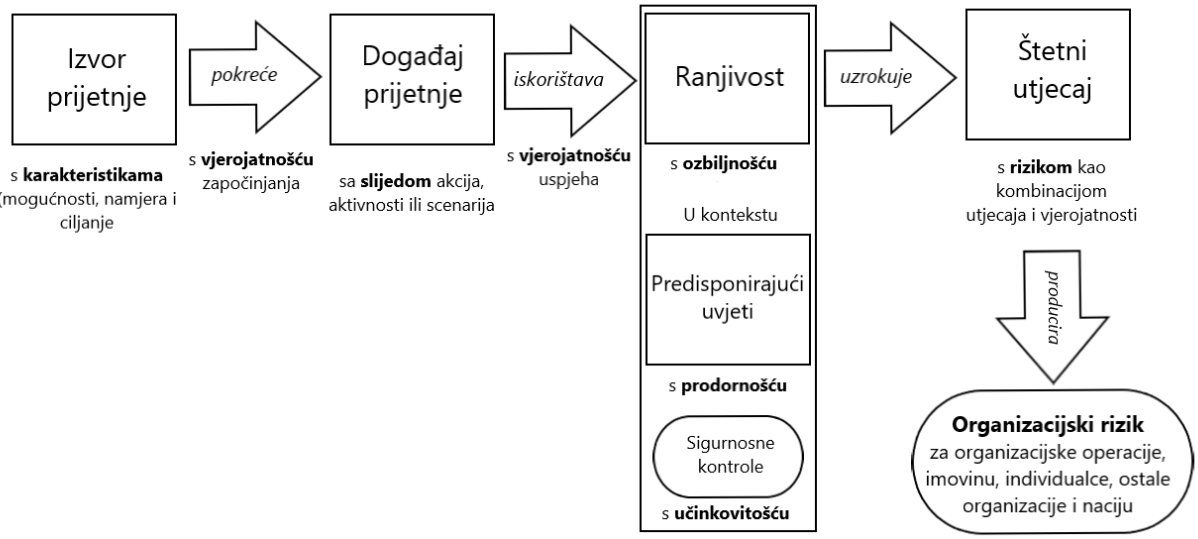
- identificiranje ključnih IT resursa,
- identificiranje utjecaja poremećaja te
- razvoj prioriteta oporavka.

Strategije i plan oporavka moraju biti formulirani tako da pokrivaju sve aspekte organizacije i njezinog poslovanja te da kroz analizu IT infrastrukture i mreže uzimaju u obzir sve posljedice mogućih napada ili poremećaja. Svrha takvih planiranja je očuvati organizacijsku spremnost i potaknuti na kontinuirano nadgledanje i napredak vlastitih strategija, tehnika i planova za situacije koje su više nego izgledne [9][15].

4.4.Evaluacija sigurnosnog rizika

Organizacija treba provoditi procjenu rizika s ciljem uvida u okruženje rizika u kojem postoji i posluje. Prema [3], upravljanje rizikom (engl. *Risk Management*) uzima u obzir okruženje u kojem se rizik i odluke uzrokovane njegovim utjecajem nalaze, procjenu rizika što će se detaljnije objasniti u nastavku, način na koji organizacija odgovara na rizik te kako nastavlja pratiti rizike tijekom vremena i spremnost same organizacije na buduće rizične situacije. Svrha procjene rizika je identificirati prijetnje organizaciji, unutarnje i vanjske slabosti, moguću štetu uzrokovanu prijetnjama i njihovim iskorištavanjem ranjivosti te vjerojatnost nastanka štete. Sve to kao krajnji rezultat daje određivanje rizika u smislu funkcije ili stupnja vjerojatnosti nastanka štete. Informacijski rizici nastaju kao posljedica gubitka povjerljivosti, integriteta ili dostupnosti informacija i reflektiraju različite štetne utjecaje na organizaciju i njezine operacije, imovinu, zaposlenike te ostale povezane partnerske organizacije. Modeli rizika definiraju faktore rizika koje treba procijeniti i njhove međusobne odnose. Uključuju prijetnje, slabosti, štetni utjecaj i vjerojatnost. Modeli se razlikuju prema detaljima i kompleksnosti prema kojima se događaji prijetnje identificiraju, a nakon čega se modeliraju, razvijaju i analiziraju scenariji ugroze. Takvi događaji karakterizirani su prema korištenoj taktici, tehnici i proceduri, a razumijevanje događaja uzrokovanih neprijateljskim prijetnjama daje organizaciji uvid u mogućnosti povezanih s određenim izvorom prijetnje te bolje razumijevanje protivnika i onog što želi postići napadima.

Poznavanje namjere i aspekte ciljanja potencijalnog napada pomaže organizaciji suziti set prijetećih događaja na one najvažnije na koje može prebaciti fokus. U kontekstu stalnih promjena u organizaciji, okruženju i tehnologiji uvijek se mora uzimati u obzir da sigurnosne kontrole mogu postati neadekvatne i trebaju biti reevaluirane u svrhu efektivnosti. Tendencija efektivnosti sigurnosnih kontrola da s vremenom degradiraju pojačava potrebu za konstantnom procjenom rizika u kompletnom životnom ciklusu razvojnih sustava i važnost nastavka nadziranja radi pregleda spremnosti organizacije u svim sigurnosnim aspektima. Osim informacijskih sustava slabosti mogu biti pronađene u samoj organizacijskoj strukturi upravljanja (nedostatak dovoljnog upravljanja rizikom, nekonzistentnost u donošenju odluka o prioritetima poslovnih funkcija, itd.), u vanjskim odnosima (ovisnost o određenom energetskom izvoru, lanac opskrbe, informacijske tehnologije, itd.), procesima poslovanja (loše definirani procesi bez svijesti o riziku) te arhitekturi informacijske strukture (nedostatak raznolikosti i otpornosti). Također pri procjeni rizika organizacije uzimaju se u obzir predisponirajući uvjeti unutar organizacije, misija ili proces, arhitektura, informacijski sustav ili okruženje koje utječe na vjerojatnost prijetnji koje bi mogle napraviti ozbiljnu štetu. Primjeri takvih uvjeta su lokacija same organizacije (povećana mogućnost uragana ili poplava), ili samostalni sustav bez vanjske mrežne konekcije. Slabosti i predisponirajući uvjeti dio su cjeloukupne sigurnosne posture organizacijskih sustava i svakako doprinose vjerojatnosti da će se događaj ugroze i dogoditi. Slika *4.11*daje generički model rizika s ključnim faktorima važnim za evaluaciju i definiranje sigurnosnog rizika organizacijske imovine i mreže. Prema modelu organizacijski rizik je funkcija nekoliko ključnih faktora koji zajedno dovode do situacija štetnim po organizacijske operacije (misije, funkcije, reputacija) te imovinu, individualce i ostale povezane organizacije, odnosno funkcija vjerojatnosti pojave događaja ugroze i potencijalnog štetno utjecaja u slučaju pojave prijetećeg događaja.

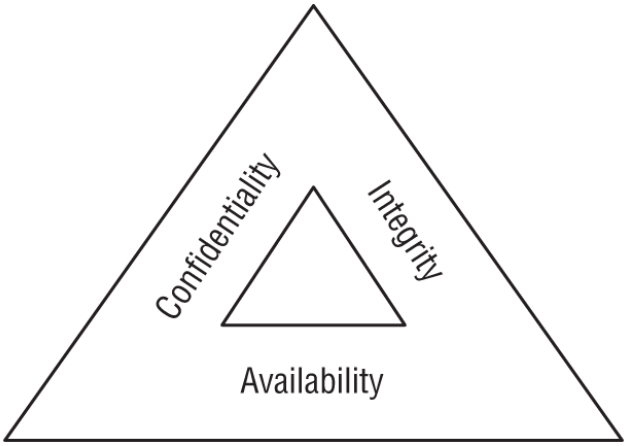


Slika 4.11: Generički model rizika, [3]

Organizacije se razlikuju u postavljanju modela rizika i preferiranim pristupima evaluaciji i analizi. Evaluacija sigurnosnog rizika može biti provedena kroz cijelu hijerarhiju rizika, na organizacijskoj razini, misijskim/poslovnim procesima te na razini informacijskih sustava. Od organizacijskog nivoa prema nižim misijskim/poslovnim procesima i informacijskim sustavima prati se sljedivost i transparentnost odluka donesenih na temelju rizika i njegove evaluacije te osviještenost postojanja prijetnji i rizika kroz cijelu organizaciju. S druge strane, prema najvišim dijelovima hijerarhije prate se povratne informacije o kontinuiranom napretku, utjecaju evaluacije i odluka na najniže razine organizacije te se radi na održavanju među-razinske i unutar-razinske komunikacije. Evaluacija sigurnosnog rizika u organizaciji zahvaća sve dijelove organizacije pa se tako kroz cijeli proces procjene najprije priprema za evaluaciju nakon čega slijedi samo provođenje. Provođenje rizika obavlja se kroz temeljito identificiranje izvora i događaja ugroze, slabosti i predisponirajućih uvjeta te određivanju vjerojatnosti pojave te intenziteta utjecaja. Proces završava komunikacijom rezultata na razini cijele organizacije te kontinuiranim održavanjem evaluacije [3].

5. POSTURA I OKVIR KIBERNETIČKE SIGURNOSTI

Dok je zaštita osjetljivih informacija od neovlaštenog otkrivanja samo jedan od elementa kibernetičke sigurnosti važno je naglasiti njezina tri komplementarna cilja, odnosno koncept informacijske sigurnosti koji se sastoji od povjerljivosti (engl. c*onfidentiality*), integriteta (engl. *integrity*) i dostupnosti (engl. *availability*). Povjerljivost onemogućava neautoriziranim osobama ili uređajima pristup osjetljivim informacijama. Razvojem i implementacijom sigurosnih kontrola kao što su vatrozidi, pristupne kontrolne liste i enkripcija, pristup podacima je ograničen na legimitimne korisnike s autoriziranim pravom pristupa. Integritet osigurava nepostojanje neautoriziranih modifikacija podataka ili sustava. Ovaj koncept referira na to da podaci nisu izmjenjeni tijekom prijenosa od sustava na kojem se nalazi do krajnjeg, destinacijskog sustava. Zadnji koncept osigurava dostupnost informacija i sustava legitimnim korisnicima u trenutku kad su oni zatraženi, a ono je moguće kroz kontrole tolerancije kvarova (engl. *fault tolerance*), grupiranja (engl. *clustering*), sigurnosne kopije (engl. *backup*), balansiranja opterećenja (engl. *load balancing*), itd. Važnost ova tri objektiva pronalazi se u dizajnu, infrastrukturi i implementaciji sigurnosti na način da se svaka faza razvoja i implementacije informacijske sigurnosti treba težiti ispunjenju sva tri objektiva i održavati balans, odnosno fokusirati se podjednako na povjerljivost podataka, integritet te dostupnost informacija i sustava kao što je prikazano na Slika 5.1. S fokusom na informaciju i kako ju zaštiti razvijena je tzv. CIA trojka, a kao dodatan, četvrti koncept, spominje se neporicanje (engl. *non-repudiation*) s fokusom na samog korisniku koji pristupa podatcima, a ono se kontrolira kroz autentifikaciju i autorizaciju.

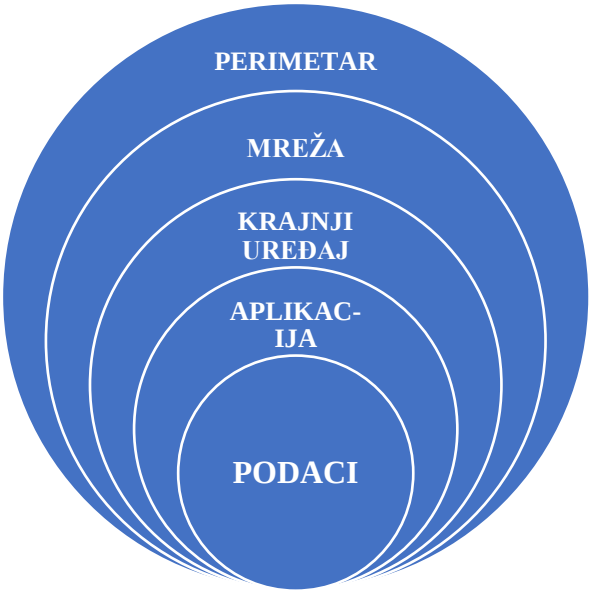


Slika 5.1: CIA trojka, [7]

Osim navedena tri glavna principa koja svaka organizacija treba implementirati kao dio vlastite informacijske sigurnosti, postoje modeli pristupa koji obuhvaćaju sve ono što treba biti uključeno unutar organizacijske mreže, odnosno sigurnosne strategije koje se odnose na Model obrane u dubini (engl. *Defense-in-Depth*), Princip najmanje privilegije (engl. *Principle of Least Privilege*) te Model nultog povjerenja (engl. *Zero Trust Model*) [7].

5.1. Sigurnosne strategije

Ideja modela obrane u dubinu bazira se na slojevitosti sigurnosti, odnosno nastoji se smanjiti ovisnost o posebnom uređaju ili sigurnosnoj mjeri kao jedinoj obrani od napada ili jedinoj koja rješava sve moguće pristupe sigurnosti. S obzirom na velik broj potencijalnih sigurnosnih napada postoji potreba za raslojavanjem obrane kako bi se osiguralo da greška ili problem u jednom dijelu organizacijske sigurnosti ne utječe i ne ugrozi osjetljive podatke, sustave ili mrežu u drugom dijelu. Organizacija ne može biti potpuno zaštićena samo jednim slojem sigurnosti no koristeći se nizom obrambenih mehanizama spomenutim u poglavlju 4 minimizira se mogućnost proboja i smanjuje površina napada. Slika *5.2* prikazuje jedan od načina raslojavanja sigurnosti prema modelu obrane u dubinu. Sloj perimetra podrazumijeva vatrozide, fizičku sigurnost, demilitariziranu zonu (DMZ), odnosno sigurnosne slojeve koje odvajaju javnu od privatne mreže organizacije. Sloj mreže se ponajviše bazira na sigurnosti bežične mreže, a na sloju krajnjeg uređaja najčešće se nalaze sustavi za sprječavanje upada domaćina (HIPS). Aplikacijski sloj podrazumijeva web aplikacijske vatrozide za promatranje i filtriranje prometa prema i od web usluga, a na sloju podatka dolazi do enkripcije i klasifikacije podataka pri čemu se podaci klasificiraju po prioritetu, od najosjetljivijih podataka do onih manje osjetljivih.



Slika 5.2: Model obrane u dubinu, [5]

Za svaku je organizaciju važno procijeniti vlastite potrebe i identificirati gdje fokusirati napore. Pri tome procjena upravljanja rizikom (engl. *risk management*) pomaže odrediti gdje je organizacija najslabija ili gdje može nastati najviše štete u slučaju proboja što je tema prethodnog potpoglavlja. Ono pomaže u formuliranju prikladne sigurnosne strategije koja se fokusira na zadovoljavanje postavljenih ciljeva i identificiranju koje sigurnosne kontrole koristiti. Postoji mnogo načina implementacije ovog modela, a jedan od njih je i sagledavanje sigurnosnih kontrola s aspekata preventativnog, detektivnog i korektivnog. Preventativne sigurnosne kontrole su proaktivne, dizajnirane da zaustave potencijalni proboj prije nego se on i dogodi što bi uključivalo fizičke barijere na ulazu, vatrozidi ili sustavi za sprječavanje upada. Detektivne kontrole kao više reaktivne fokusirane su na pronalazak aktivnosti koje su se već dogodile ili su u procesu (sustavi zaključavanja vrata, senzori pokreta, automatski mailovi logova ili uzbune sa sustava za sprječavanje napada). Korektivne su dizajnirane za ispravak problema i povratak sustava u stanje prije sigurnosnog napada. Strategija obrane u dubinu mora biti implementirana po mjeri svake organizacije i njezinim potrebama. Segmentacija mreže je dobar primjer obrane u dubinu. Uslojena sigurnost raspoređuje se i kod samih krajnjih uređaja. S obzirom da su takvi sustavi korišteni od strane krajnjih korisnika u svakodnevnom radu oni su najčešće i najizloženiji dio organizacijske infrastrukture i mogu stvoriti ozbiljnu prijetnju u slučaju komprimitiranosti. Uslojena sigurnost kod krajnjih uređaja uključuje:

- lozinke i ostale snažne autentifikacijske procedure za osiguravanje pristupa samo autoriziranim korisnicima,
- vatrozide i sustave za sprječavanje napada (HIPS) što dovodi do smanjenja površine napada te sprječava neželjenu ulaznu komunikaciju,
- programe za sprječavanje gubitka podataka koji nadziru i upravljaju zaštićenim podacima,
- softvere za stavljanje na popis dopuštenog (engl. *whitelisting*) odnosno nedopuštenog ponašanja (engl. *blacklisting*),
- antivirusne programe za nadziranje poznatih zlonamjernih programa te ponašanja izvan okvira poznatog i dopuštenog,
- upravljanje zakrpama i alati za procjenu ranjivosti koji osiguravaju da su aplikacije i operacijski sustavi propisno osigurani,
- enkripcije datoteka i cijelog diska te
- logove procesa, aktivnosti i događaja.

Uslojena sigurnost zahtjeva primjereno nadgledanje, upozoravanje i validiranje. Sustavi logiranja trebaju osigurati da su logovi sigurni te dostupni za nadgledanje dok sustavi nadgledanja trebaju imati primjerene pragove upozoravanja i obavještavanja koje zadovoljavaju potrebe organizacije. Raznolikost produkata, odnosno korištenje produkata različitih proizvođača dodatan je sloj sigurnosti koji mnoge organizacije prakticiraju pri čemu se nastoji eliminirati „jedinstvenu točku slabosti“ (engl. „*a single point of failure*“) osiguravajući se da jedna ranjivosti ili nedostatak u dizajnu u jednom produktu ne učini cijelu mrežu ili sustav ranjivim. No takav način ipak donosi svoje nedostatke kao što su troškovi održavanja, trening zaposlenika, podrška te mogućnost rezultiranja s još više ranjivosti. Dodatna sigurnosna razina koja se ne smije zanemariti je ljudski faktor. Zaposlenici trebaju biti istrenirani za zadatke s kojima se suočavaju te osigurati da pravilno reagiraju na sigurnosne probleme i prijetnje. Model Obrane u dubinu svakako ne smije zanemariti CIA trojku i treba se očitovati kroz sva tri elementa [5].

Načelo najmanje privilegije (engl. *Least privilege*) navodi da samo minimalan potreban broj prava treba biti dodijeljen svakom korisniku i programu koji zatraži pristup resursu s minimalnim potrebnim vremenskim periodom trajanja. Dozvoljavanje pristupa korisniku iznad njegovog djelokruga posla i potrebnih prava dopustilo bi pristup ili modifikaciju informacija na neželjene načine. Primarno, time se ograničava šteta nastala napadom ili pogreškom, ali i reducira broj potencijalnih interakcija među privilegiranim programima na minimalno potrebno za pravilnu operativnost kako bi vjerojatnost nenamjernog, neželjenog ili neprikladnog korištenje privilegija

bila što manja. Iz tog razloga, u slučaju zlouporabe privilegija, broj programa koji trebaju biti revidirani je minimalan [16].

Još jedan model strategije za kompletnu zaštitu organizacijskih krajnjih uređaja i ostale infrastrukture je model nultog povjerenja (engl. *Zero trust model*). Strategijski model nultog povjerenja štiti organizaciju eliminirajući implicitno povjerenje i kontinuiranu validaciju svakog koraka digitalne interakcije. Zajedno s modelom najmanje privilegije cilj je prevenirati neautoriziran pristup podacima i sustavima i provedbu kontrole pristupa učiniti što kompletnijom i detaljnijom. Fokus je na autentifikaciji, autorizaciji i sužavanju implicitnih zona povjerenja, a sve uz održavanje dostupnosti i reduciranja vremenskog kašnjenja u procesu potrebne autentifikacije. Model se javio kao odgovor na trendove u organizacijama koji se odnose na udaljen rad, BYOD i imovinu u oblaku, a u odnosu na model u dubinu koji uzima u obzir i segmente mreže, ovaj model je orijentiran primarno na sigurnost resursa (imovina, servisi, računi) [17].

5.2. Sigurnosni okviri organizacije

Okvir politike informacijske sigurnosti u korporacijskom okruženju definiran je nizom dokumenata dizajniranih da opišu program kibernetičke sigurnosti organizacije. Djelokrug i kompleksnost dokumenata ovise o prirodi organizacije i njezinim informatičkim resursima, a uključuju četiri različita tipa dokumenta:

- police,
- standardi,
- procedure i
- smjernice.

Police su organizacijske izjave visoke razine koje sadrže ciljeve i definiranje planova sigurnosti. Predstavljaju skupove direktiva, regulacija, pravila i praksi koje propisuju kako organizacija upravlja, štiti i distribuira informacije. Usklađenost s policama je obavezna, a njihov sadržaj odnosi se na važnost kibernetičke sigurnosti u organizaciji, a varira od zahtjeva za poduzimanje mjere za zaštitu integriteta, dostupnosti i povjerljivosti informacija i informatičkih sustava u organizaciji pa sve do povjeravanja ovlasti glavnom službeniku za informacijsku sigurnost (engl. *chief information security officer*, CISO) ili drugim nadležnicima odgovornim za kibernetiku u organizaciji i kreiranje ostalih dokumenata sa svrhom provedbe polica. Police su pisane i

usklađivane na širokoj razini u korporaciji što za sobom povlači potrebu razvoja standarda, smjernica i procedura koje provode police, odnosno pružaju korisnicima, menadžerima i sistemskim administratorima jasniji pristup kod implementacije polica i organizacijskih ciljeva i misije. Organizacijski standardi pružaju obavezne zahtjeve koji opisuju način na koji organizacija provodi sigurnosne police što uključuje specifične postavke i ponašanja konfiguracija u organizaciji te korištenje tehnologija, parametara i procedura. Često raznolikost informatičkih sustava i organizacijskih resursa otežava i komplicira provođenje standarda na pravilan i efektivan pa iz tog razloga organizacija asistira korisnicima i ostalom sistemskom osoblju smjernicama u efektivnoj zaštiti sustava. One predstavljaju općenite preporuke sastavljene tako da su razumljive korisnicima. Posljednji važan sigurnosni dokument odnosi se na procedure koje konkretno opisuju način implementacije sigurnosnih polica, standarda i smjernica kroz detaljne korake. Navedeni dokumenti opisuju strateški plan organizacije i njezinog djelovanja na području sigurnosti informacija i IT infrastrukture [5][18].

Organizacije često definiraju police u skladu s NIST-ovim okvirom najboljih preporuka koje pokrivaju pet aspekata sigurnosti u organizaciji: identificirati, zaštititi, detektirati, odgovoriti i oporaviti. Ovih pet okvira kibernetičke sigurnosti prati organizaciju kroz proces implementiranja sigurnosti i kontinuiranog napretka u zaštiti svih krajnjih uređaja. Prema tome, police se kreiraju tako da pokrivaju sve uloge i odgovornosti zaposlenika, klijenata i ostalih s pristupom osjetljivim podacima. Organizacije identificiraju s kojim informacijama raspolažu te razinu njihove osjetljivosti kako bi bili u mogućnosti razumjeti prijetnje i vlastite slabosti. Zaštiti znači kontrolirati tko se prijavljuje u mrežu i koristi krajnje uređaje, odnosno police pokrivaju dogovore o korištenju sigurnosnih softvera, enkripciji osjetljivih podataka, provođenju regularnih sigurnosnih kopija, kontinuiranom ažuriranju, edukaciji i treningu te sigurnom odlaganju elektroničkih datoteka i zastarjelih uređaja. Treći aspekt, detekcija, podrazumijeva praćenje krajnjih uređaja za neautoriziran pristup osobnih uređaja i softvera, neautorizirane korisnike i konekcije u mreži te inspekcija sumnjivih aktivnosti u mreži. Odgovor organizacije na prijetnje, napade i ranjivosti je razvoj plana za bilo koju moguću situaciju i posljedicu, a da poslovanje organizacije nastavi s radom. Ono podrazumijeva i dodatnu istragu događaja i sprječavanje širenja napada te nadogradnja polica. Nakon mogućeg napada slijedi faza oporavka koja se odnosi kako na popravak i vraćanje u funkcionalno stanje uređaja i opreme, tako i osvješćivanje zaposlenika i informiranje o poduzetim koracima. Opseg i kompleksnost polica ovisi ponajviše o prirodi organizacije i njezinim informatičkim resursima. Cijeli program kibernetičke sigurnosti uključen je u dokumente polica, standarda, procedura i smjernica koje opisuju način implementacije i

održavanje sigurnosti u korporativnom okruženju, daju preporuke i najbolje prakse ovisno o dijelu sigurnosti te korak-po-korak procese i njihovo detaljno praćenje [19].

5.3.Osvještenost, trening i edukacija

Sigurnosni mehanizmi kao što su antivirusni programi, filtriranje paketa u mreži, inspekcija prometa vatrozidom i ostali, zahvaljujući naprednoj tehnologiji ostaju u koraku s naprednim tehnikama i taktikama kojima se kibernetički napadači služe kako bi ostvarili svoje ciljeve po štetu korporacija. No prema Verizonovom izvještaju iz 2021.godine utjecaj čovjeka i dalje nastavlja biti jedan od glavnih razloga uspješnih kibernetičkih napada, odnosno u 82% kršenja organizacijskih pravila kibernetičkim napadima čovjek je bio glavni pokretač što naglašava potrebu za snažnim programima razumijevanja i osvješćivanja zaposlenika [8]. Slika 5.3 iz Verizonog izvještaja iz 2021. godine prikazuje stopu nasjedanja („kliknuto“) na *phishing* mailove od 2016. do 2021. godine u odnosu na stopu povećanu stopu osvještenih reakcija na zlonamjerne poruke.

Slika 5.3: DBIR, [8]

Ljudski utjecaj na sigurnost još je jedan sloj koji treba uzeti u obzir uz tehničke i proceduralne kontrole. IT osoblje mora biti trenirano na razini zadatka na kojem rade, a ostali zaposlenici educirani i osviješteni glede prijetnji i potencijalnih opasnosti te načinima kako postupati u takvim situacijama. Prema [20], sigurnosno osvješćivanje nije trening. Svrha osvješćivanja je fokusirati pažnju na sigurnost i namijenjeno je za individualce da prepoznaju IT sigurnosne brige i reagiraju u skladu s njima. Primjer jedne takve teme može biti zaštita od virusa gdje je subjekt, odnosno zaposlenik obavješten o tome što je virus, koje su poljedice inficiranja sustava virusom, što

korisnik može napravit kako bi to spriječio te što napraviti ukoliko je virus otkriven. Dodatne teme pokrivaju korištenje i upravljanje zaporkama (zaštita, učestalost njihove promjene i kreacija), police i implikacije njihova nepridržavanja, nepoznati e-mailovi i privitci, *spam* poruke, korištenje web preglednika, odgovor na incidente (kome se obratiti i kako reagirati), promjene u sustavnom okruženju i slično. S druge strane, trening ide u smjeru produciranja relevantnih i potrebnih sigurnosnih vještina i kompetencija pri čemu je fokusiran na učenje što omogućava osobi da obavlja određenu funkciju. Tečaj za sustavne administratore je primjer treninga za IT sigurnosni tečaj gdje se detaljno prolaze kontrole upravljanja (upravljanje rizikom, police, životni ciklus sigurnosti, itd.), operativne (planiranje za nepredviđene situacije, rukovanje incidentima, itd.) i tehničke kontrole (identifikacija i autentifikacija, kontrole pristupa, revizije, itd.). Organizacija pokušava na mnoge načine doprijeti do vlastitog osoblja, a sami programi mogu biti predstavljeni kroz konkretne tečajeve, kolektivne e-mailove, webinare i seminare, a najčešća tema takvih inicijativa je uvijek kontinuirani napredak. Efektivni IT sigurnosni program osvješćivanja i treninga objašnjava pravila ponašanja pri korištenju organizacijskih sustava i informacija, a programi prate IT sigurnosne dokumente, police, standarde, procedure i smjernice [20].

Uz programe postoje i razne kontrole osoblja koje mogu biti implementirane kao dio kompletnog sigurnosnog programa, a čija je provedba pod kontrolom same organizacije. Neke od njih su podjela dužnosti, planiranje sukcesije, provjera pozadine, raskid, *cross* treninzi te obavezni odmor. Ispravno uvedena podjela dužnosti zahtjeva više od jedne osobe na zadatku i s određenom ulogom kako bi se smanjila mogućnost zloupotrebljavanja prava i privilegija koje uloga nudi. Kontinuirano napredovanje uloge u organizacijskom poslovanju neovisno o osobama koje dolaze i odlaze provodi se sukcesivnim planiranjem. Korporacija treba na vrijeme uočiti nedostatak znanja i vještina na određenoj poziciji ili limitiranost na samo jednu osobu koja svojim odlaskom može pozicijske dužnosti ostaviti neispunjenim. Zaštita imovine i osjetljivih informacija provodi se i temeljnom provjerom vlastitih zaposlenika kao i provođenjem kompletnog oduzimanja svih pristupa računima i organizacijskim resursima osoblju po raskidu ugovora. Jednom kada organizacija uspostavi program koji povećava razinu sigurnosnog osvješćivanja i praćenja potrebno je održavati kontinuiranu provjeru programa, polica i postojećih treninga te težiti konstantnom napredovanju i robusnijoj zaštiti. Održavanje i uspostavljanje programa osvješćivanja korisnika, treninga i edukacije o zlonamjernim softverima kritični su za smanjenje broja incidenata koji nastaju kao posljedica ljudske greške [7].

6. KOMPLETNA RJEŠENJA ZAŠTITE, DETEKCIJE I ODGOVORA NA NAPADE NA KRAJNJIM UREĐAJIMA

Načini zaštite opisani u prethodnim poglavljima uzimaju se kao smjernice i najbolje prakse za sigurnost kako u korporativnom okruženju tako i za privatnu informacijsku sigurnost svakog zaposlenika. Uslojena sigurnost implementirana kroz nekolicinu različitih mehanizama koji pokrivaju organizaciju na svim njezinim aspektima, od nepoznatog privitka u e-mailu pa sve do štetnog *ransomware*-a i distribuiranih napada, predstavlja rješenje koje ne smije nedostajati u bilo kojem korporativnom okruženju. Povećanjem tržišta kibernetičke sigurnosti u posljednjih nekoliko godina dolazi se do velikog broja proizvođača koji nude sličan model zaštite kroz veći broj usluga. Jedan od takvih modela je zaštita krajnjih uređaja kroz detekciju, prevenciju i odgovor na napad, a sve na jednom mjestu. Takve su tehnologije EPP (engl. *Endpoint protection platform*) i EDR (engl. *Endpoint Detection and Response*) s XDR-om (engl. *Extended Detection and response*) i MDR-om (engl. *Managed Detection and Response*) kao naprednijim dodacima. S većinom napada koji ciljaju krajnje uređaje čineći ih tako najranjivijim djelom korporacije težište se prebacilo na važnost IT timova s udaljenom vidljivošću i mogućnošću za oporavkom sustava. EPP ili platforme prevencije na krajnjim uređajima pružaju jednostavnost postavljanja agenata ili senzora za upravljanje i nadgledanje krajnjih uređaja. Dizajnirani su za prevenciju poznatih i nepoznatih zlonamjernih softvera, prijetnji te pružanje zaštite od navedenog, a sve to uz mogućnosti dodatnog istraživanja i saniranja incidenata koji izbjegnu sigurnosne kontrole. Dodatne funkcionalnosti jedne takve platforme su:

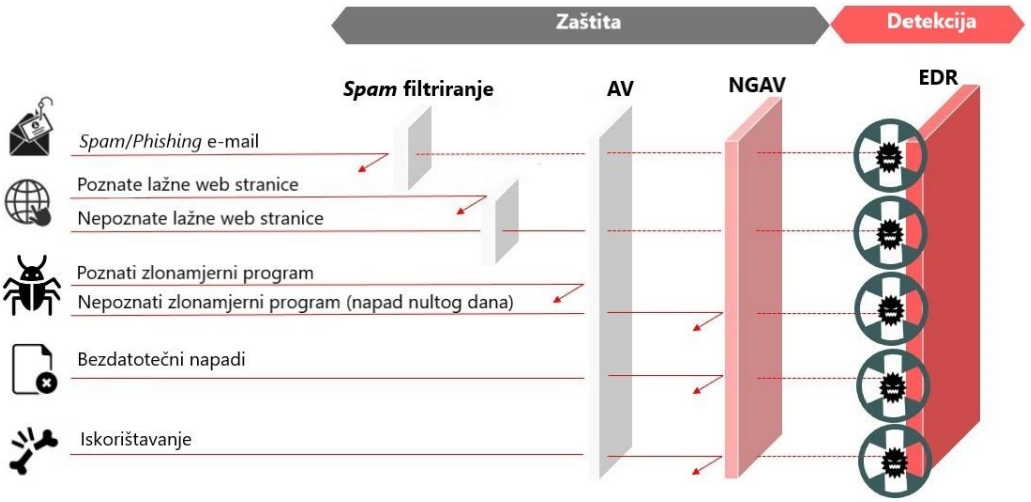
- mogućnost primjene kontrola zaštite na softvere, skripte i procese,
- mogućnost detekcije i prevencije prijetnji koristeći bihevioralnu analizu aktivnosti uređaja, aplikacija i ostalih podataka,
- skupljanje i izvještavanje o imovini, konfiguracijama i upravljanju policama na krajnjim uređajima,
- skeniranje sustava za ranjivosti i izvještavanje o instalaciji sigurnosnih zakrpa,
- veza s globalnom bazom podataka otkrivenih prijetnji i slabosti za izvođenje dodatnih indikacija o potencijalnim zlonamjernim aktivnostima, primjer *Mitre Att&ck* kao baza taktika i tehnika napadača kroz promatranja iz stvarnog svijeta.

EPP su rješenja razvijena za krajnje uređaje gdje za cilj imaju prevenciju zlonamjernih softvera, detekciju i blokiranje nelegitimnih aktivnosti od vjerodostojnih i nevjerodostojnih aplikacija te pružaju istragu i oporavak sustava kao odgovor na sigurnosna upozorenja i incidente. Ova

tehnologija pasivnije prirode radi sa značajkama enkripcije podataka i datoteka, antivirusa, *sandboxinga* i vatrozida za sve krajnje uređaje. EPP se danas često zamjenjuje s EDR-om, odnosno dok EDR podrazumijeva funkcionalnosti vezane uz prevenciju, on sam aktivnije omogućava odgovor na nepoznate prijetnje koje su probile zaštitu EPP-a te cilja na napredne trajnje prijetnje (engl. *advances persistent threat,* APT) razvijene u svrhu prolaska EPP-ove obrane [21].

6.1.EDR, XDR i MDR

EDR (engl. *Endpoint Detection and Response*) kao predihtivna tehnologija fokusirana je na identificiranje naprednih trajnih prijetnji te novih i nepoznatih *malware*-a dizajniranih da izbjegnu tradicionalnu sigurnosnu obranu. Većina ovakvih rješenja kombiniraju snagu obavještajnih podataka o prijetnjama (engl. *threat intelligence*), strojno učenje i napredne analize datoteka u svrhu detekcije naprednih prijetnji. Četiri sposobnosti svake EDR tehnologije su detektirati, zaustaviti i istražiti sigurnosni incident te dati smjernice za oporavak. Ovakvo rješenje pruža kontinuiranu vidljivost u sve aktivnosti na krajnjem uređaju u stvarnom vremenu. U usporedbi s tradicionalnim antivirusnim rješenjima, vidljivo je da su AV-ovi jednostavniji, ali i dio EDR-a. Dok AV-ovi pridonose detekciji zlonamjernih softvera s poznatim potpisom ili ponašanjem, EDR kao superiorna tehnologija uključuje više slojeva zaštite kao što su blokiranje napada, zakrpe, vatrozid, *whitelisting*/*blacklisting*, NGAV, itd. Iz tog razloga, EDR je rješenje prilagođenije rješavanju naprednih prijetnji i ispunjavanju zahtjeva korporativne sigurnosti. Slika *6.1* slikovito prikazuje usporedbu sigurnosnih kontrola u ovisnosti o rasponu kibernetičkih napada i prijetnji od kojih mogu zaštiti i koje mogu na vrijeme detektirati. Vidljivo je obični antivirusni programi imaju mogućnost blokiranja i zaštite od zlonamjernih programa s poznatim potpisima, no već kod naprednijih *malware*-a potrebne su funkcionalnosti NGAV-a za pravovremenu zaštitu. Također iza svih sigurnosnih kontrola nalazi se EDR kao posljednja čvrsta obrambena linija koja kupi sve što uspije proći prethodno postavljenu zaštitu i time dodatno osigurava organizacijsko okruženje.



Slika 6.1: Usporedba sigurnosnih kontrola, [22]

EDR sigurnosno rješenje jedne organizacije pruža centraliziranu platformu za skupljanje, organiziranje i analiziranje podataka prikupljenih na povezanim krajnjim uređajima. Ima mogućnost sinkronizacije odgovora i upozorenja na prijetnje u najkraćem mogućem vremenu. Tri glavna elementa EDR tehnologije su instalirani agent ili senzor na krajnjem uređaju, automatizacija odgovora na incidente te analiza. Senzor instaliran na svakom krajnjem uređaju nagledava uređaj i prikuplja podatke koje šalje na *cloud* za dodatnu obradu. Prikupljene informacije uključuju podatke povezane s pokrenutim procesima, količinom aktivnosti na uređaju, konekcije, što i kako je prenešeno s uređaja i na njega te ostale informacije važne za praćenje statusa kranjeg uređaja. EDR također omogućava uključivanje i konfiguraciju prilagođenih pravila dizajniranih od strane organizacije ili EDR tima administratora za identificiranje prijetnji. Ovisno o postavljenim parametrima, pravila prepoznaju i karakteriziraju prijetnju te okidaju automatske odgovore na određene aktivnosti na krajnjem uređaju kao što su izoliranje inficiranog uređaja, blokiranje prijetnje i slanje obavijesti. Uz sve navedeno, analiziranje podataka na krajnjim uređajima u stvarnom vremenu je još jedan element EDR tehnologije. Ono pomaže u brzoj dijagnostici prijetnji i ranjivosti sustava te uz pomoć alata forenzike dodatno propituje načine na koji je napad izveden. Karakteristike koje EDR čine tehnologiju koja kontinuirano odbija inovativne i sofisticirane zlonamjerne programe i uspješno prepoznaje sumnjive i izvan-okvira ponašanja u sustavima krajnjeg uređaja:

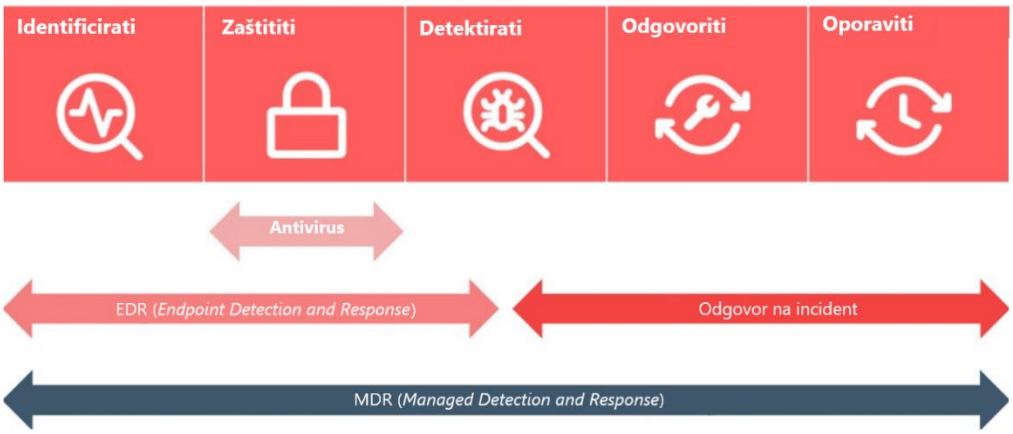
- integracija s višestrukim alatima daje perspektivu kooperacija na više slojeva što je bitan dio sigurnosti koju EDR rješenje pruža jer većina forenzičkih alata koje koristi pomažu u dubljoj analizi i praćenju odvijenih događaja,

- upozorenja, izvještavanje i konzistentan pregled okruženja prikazani su u centraliziranoj platformi koja pokazuje statuse povezanih krajnjih uređaja te generira izvještaje i upozorenja o sumnjivim aktivnostima na uređajima za timove koji nadziru sve aktivnosti,
- napredne mogućnosti odgovora i automatizacije kroz specijalizirane alate za procjenu i reakciju na sigurnosne incidente zajedno s prevencijom, detekcijom, obavještajnim podacima i forenzikom,
- internacionalna dostupnost omogućava neovisnost upravljanja okruženjem danog EDR tehnologijom o mjestu i vremenu upravljanja te
- prevencija kao neizostavan dio sigurnosnih mehanizama tehnologije koja se provodi na temelju bihevioralne analize ulaznog i izlaznog prometa na krajnjim uređajima, odnosno u organizaciji.

Implementacija EDR tehnologije u okruženje organizacije započinje instalacijom senzora na svakom krajnjem uređaju. Senzor promatra aktivnosti na uređaju te sve podatke šalje na *cloud* gdje se oni analiziraju, skupljaju za daljnje istraživanje, a istovremeno se traže bilo kakvi dokazi o zlonamjernim datotekama u sustavu uređaja. Kada je nešto detektirano (bilo koje ponašanje i aktivnost izvan parametara normalnog i uobičajenog) odmah započinje istraga. Tijekom procesa istrage algoritam identificira izvor napada, inficirane dijelove, način na koji je ušao u organizacijsko okruženje i ostale važne informacije koje će upoznati s prijetnjom i spriječiti buduća iskorištavanja od strane napadača. Ukoliko je napad identificiran kao stvarna opasnost ili točno pozitivan (engl. *true positive*) provode se mjere izoliranja uređaja, blokiranja te prekida svih konekcija. U slučaju da napad nije prava prijetnja, odnosno klasificiran je kao netočno pozitivan (engl. *false positive*) analiziraju se podaci koji su doveli do netočne detekcije te se ono iskorištava kao ulaz u model strojnog učenja kao jednog od alata EDR-a za pomoć u budućoj točnijoj detekciji prijetećih događaja. Zadnja sigurnosna razina ove tehnologije je ljudska intervencija, odnosno tim IT analitičara s dovoljno znanja i vještina koji nakon opsežne intervencije okinute detekcije označavaju prijetnju kao točno ili netočno pozitivnu te na zahtjev klijenta/organizacije i na temelju najboljih preporuka sigurnosti postavljaju pravila i sigurnosne police za detekciju i prevenciju prijetnji te ponašanje senzora na krajnjem uređaju. Primjer takve jedne uloge je SOC (engl. *Security Operations Center*) analitičar ili CSIRT (engl. C*omputer Security Incident Response Team*). Neka od postojećih rješenja tehnologije detekcije i odgovora na krajnjim uređajima na tržištu su *SentinelOne, Microsoft Defender, Crowdstrike, Cybereason, TrendMicro, McAfee* i mnogi drugi.

Sigurnosna rješenja MDR i XDR pojavila su se kao naprednije verzije EDR tehnologije gdje sigurnosne mjere osim krajnjih uređaja pokrivaju mrežu i *cloud* usluge zajedno. XDR (engl. *Extended Detection and Response*) priznaje da samo zaštita krajnjih uređaja nije dovoljna da bi se zaštitila cjelukupna moderna IT infrastruktura korporacije jer prijetnje, rizici i ranjivosti ne staju samo na krajnjim uređajima nego zahvaćaju sve aspekte IT infrastrukture organizacije. XDR tehnologija proširuje mjere zaštite na nadgledanje mreže, organizacijskih usluga u oblaku, servera, e-mailova i ostale imovine podložne ugrozama današnjih kibernetičkih napadača. U odnosu na EDR, XDR je fokusiran na poboljšanje reakcije SOC funkcija u stvarnom vremenu kod napada gdje radi na poboljšanju mogućnosti detekcije, prevencije i odgovora, poboljšanoj produktivnosti operativnom sigurnosnom osoblju te sve uz manji trošak organizacijama koje implementiraju ovakav sigurnosni mehanizam. Upravo je poboljšana produktivnosti sigurnosne operativnosti timova te uniformna vidljivost i kontrola kroz sve krajnje uređaje, mrežu i oblak u organizaciji glavni fokus XDR rješenja. Proširena detekcija i prevencija donosi ugrađene naprednije analitičke i korelacijske alate kojima se smanjuje broj netočno pozitivnih detekcija, a poboljšava kritične SOC funkcije u situacijama reagiranja na napade u okruženju pri čemu identificiraju smislenije prijetnje na temelju relevantniji podataka iz sigurnosnih kontrola u mreži, oblaku i krajnjim uređajima u organizacijskom okruženju [23].

Treće ovakvo rješenje, MDR (engl. *Managed Detection and Response*) pomaže u brzom identificiranju i ograničavanju utjecaja prijetnji, ali bez potrebe za dodatnim sigurnosnim osobljem unutar organizacije. Ovo rješenje nudi udaljen pristup cijeloj organizacijskoj mreži s 24/7 pokrivenošću i pristupom sigurnosnim stručnjacima koji odgovaraju na prijetnje i detekcije, vraćaju krajnje uređaje u stanja prije napada te preveniraju daljnja kompromitiranja. Organizacije koje koriste MDR rješenja reduciraju vrijeme za detekciju i odgovor na samo nekoliko minuta čime se reducira i utjecaj prijetnje. Kompleksnost podataka i tehnologija koje EDR nudi te nedostatak stručnosti u organizaciji da u potpunosti iskoristiti takav sustav, MDR rješava uvodeći posebna ljudska znanja i vještine te zrelije procese koji pomažu organizaciji postići željenu razinu sigurnosti bez potrebe za posebnim troškovima sigurnosnog osoblja ili SOC timova. Na Slika *6.2* prikazana je usporedba sigurnosnih rješenja (AV, EDR, Odgovor na incidente i MDR) kroz njihovu pokrivenost pet glavnih aspekata sigurnosti u organizaciji. MDR kao najrazvijeniji model u svojoj implementaciji pokriva sve sigurnosne aspekte, od identifikacije sumnjivih događaja pa sve do oporavka i saniranja sustava i uređaja.



Slika 6.2: Usporedba sigurnosnih rješenja u ovisnosti o pokrivenosti aspekata sigurnosti u organizaciji, [22]

Sva tri rješenja dodatno su objašnjena kroz konkretan primjer u pod-poglavlju 6.2. *Crowdstrike* tehnologija nudi implemenetaciju modela EDR, XDR i MDR kroz različit broj usluga i najnovijih alata i tehnologija, a sve podređeno veličini i potrebi organizacije koja implementira takvo rješenje.

6.2. *CrowdStrike Falcon*

Crowdstrike je globalna kompanija za kibernetičku sigurnost s naprednom platformom u oblaku za zaštitu krajnjih uređaja, radnih opterećenja u oblaku, podataka i identiteta. Uslugama nudi rješenja zaštite kompletnog korporativnog okruženju kroz implementaciju EDR, XDR ili MDR rješenja kao odgovora na kibernetičke napade. *Crowdstrike* je model kompletno razvijen u oblaku, a implementacija se odvija korištenjem laganog agenta, odnosno senzora na krajnjim točkama u organizaciji preko kojeg se dostavljaju sve usluge sigurnosti krajnjih uređaja (NGAV, EDR i kontrola uređaja), sigurnosnih operacija (IT higijena, lov na prijetnje i upravljanje ranjivostima) i obavještajnih podataka o prijetnjama (automatizacija obavještajnih podataka, pretraga i analiza zlonamjernih programa). Slika *6.3* prikazuje prepoznatljiv logo *Crowdstrike* platforme.

Slika 6.3: *Crowdstrike* logo

Sve navedene usluge dostupne su preko *Crowdstrike Falcon* platforme kojom upravlja i pokreće AI u oblaku, a kojeg podupire vlastita baza podataka grafa prijetnji (engl. *Threat Graph*) i tehnologija naprednog filtriranja. Graf prijetnji koji se nalazi u pozadini nativne *Crowdstrike* platforme korelira velike količine sigurnosnih događaja koji se sastoje od indikatora napada, obavještajnih podataka i organizacijske telemetrije kroz sve krajnje uređaje, radne stanice, IT imovinu i konfiguraciju unutar organizacije. Na temelju prikupljenih podataka predviđaju se i preveniraju moderne prijetnje u stvarnom vremenu i obavještavaju korisnici o mogućim rizicima i blokiranim prijetnjama. Ono što graf čini jezgrom ovog modela su:

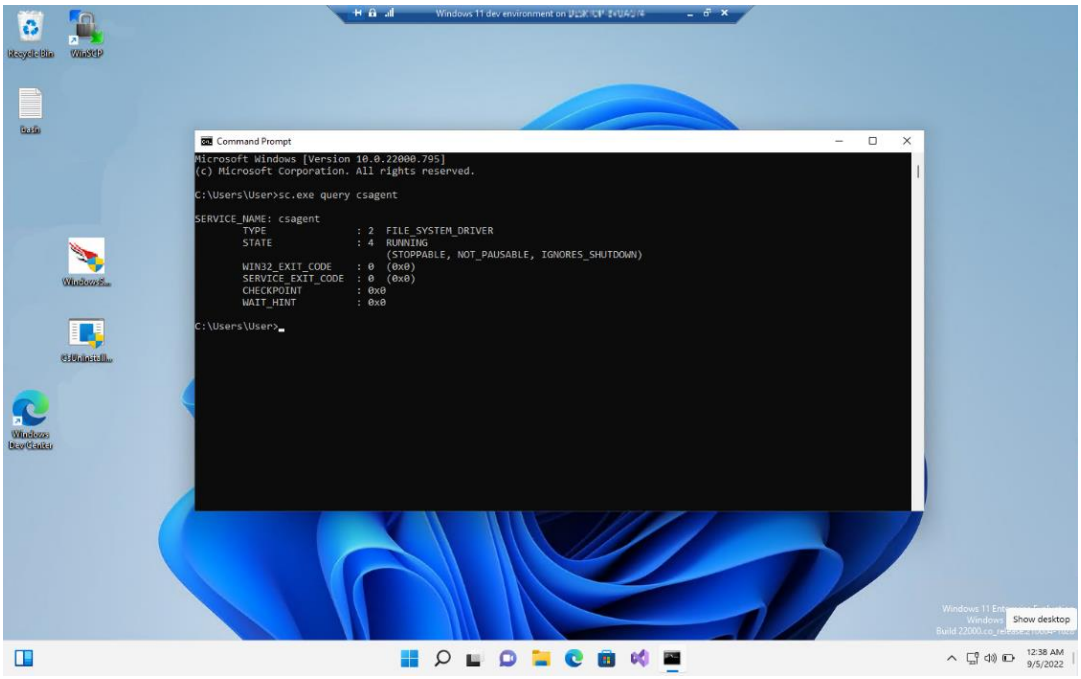
- baza podataka koja se kontinuirano nadopunjuje organizacijskom telemetrijom te obavještajnim podacima iz svijeta stvarnih prijetnji i time povezuje poznate zlonamjerne aktere s događajima u vlastitoj bazi podataka,
- AI i bihevioralna analiza za identificiranje novih prijetnji u stvarnom vremenu koje ovisno o postavljenim sigurnosnim policama blokira ili upozorava,
- snažan pretraživač za SOC timove i lovce na prijetnje,
- implementaciju API-a (engl. *Application Programming Interface*) kao integraciju s trećim sigurnosnim stranama te
- sva rješenja dostupna u oblaku i dostavljena bez potrebe za infrastrukturom na lokaciji.

Rješenje je fleksibilno i proširivo ovisno o sigurnosnim potrebama organizacije. Senzori instalirani na krajnjim uređajima (radne stanice, serveri, kontroleri domene, itd.) promatrani su od strane administratora i ostalih sigurnosnih timova zaduženih za detekcije, incidente te istrage aktivnosti i prijetnji povezanim sa sumnjivim procesima u IT infrastrukturi. Ovisno o definiranim policama senzori prikupljaju telemetriju i reagiraju na događaje i procese u sustavu i uređajima.

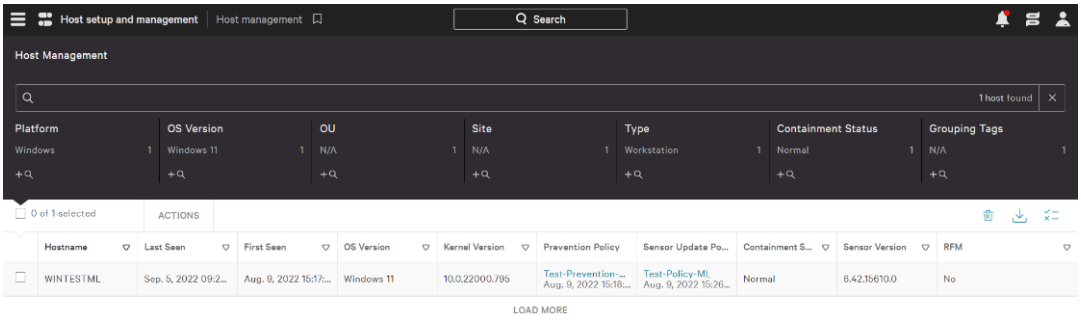
Crowdstrike zaštita krajnjih uređaja namijenjena za poduzeća ujedinjuje više navedenih sigurnosnih kontrola kroz nekoliko značajki, a sve kroz jedinstveni senzor isporučen u oblaku.

Glavne značajke produkta obuhvaćene su modulima koje klijenti zakupljuju u sklopu nekog od ponuđenih paketa zaštite vlastite korporacije. Značajke se odnose na NGAV (engl. *Next-Gen Antivirus*) koji kombinira najbolje preventivne tehnologije za sprječavanje *ransomware*-a i bezdatotečnih napada, a uključuje strojno učenje, AI indikatore napada (engl. *Indicators of attack*, IOA) i skeniranje memorije, EDR koji hvata neobrađene podatke za automatske detekcije zlonamjernih aktivnosti, pruža vidljivost, lov na prijetnje i forenzičku istragu te snažne akcije odgovora i saniranja kompromitiranih sustava. Tim sigurnosnih eksperata proaktivno lovi i istražuje aktivnosti u okruženju kompanije kako ni jedno upozorenje ne bilo predviđeno, a kontrolom uređaja daje detaljnu vidljivost i omogućava provođenje politike kod korištenja USB uređaja u poslovnom okruženju. Tu su dodatno integrirani obavještajni podaci o prijetnjama za potpuno razumijevanje prijetnji i prioritizaciju odgovora s procjenama ozbiljnosti prijetnje te upravljanje vatrozidom preko kojeg se upravlja policama i brani od ugroza u mreži. Implementirana je i IT higijena s nadziranjenjem korisnika, aplikacija i korištenja administrativnih privilegija kroz cijelu organizaciju te zaštita AD-a (engl. *Active Directory*) nadziranjem prometa i kontinuiranim pregledom u slabosti vjerodajnica, odstupanja u pristupima te kompromitiranje zaporki. Paket kompletne *Falcon* zaštite odnosi se na MDR rješenje s *Crowdstrike* tehnologijom, a osim prethodno navedenih modula dodatno uključuje sloj sigurnosnih eksperata koji upravljaju, nadziru i odgovaraju na prijetnje.

Nakon instalacije *Crowdstrike* senzora na krajnjem uređaju provjeravaju se aktivnost statusa na uređaju te vidljivost senzora na samoj platformi od strane administratora što je prikazano na Slika 6.4 i Slika 6.5. Na centraliziranoj platformi definiraju se i postavljaju police prevencije, odgovora i kontrole uređaja, a provode se putem senzora koji nadgleda, prikuplja i šalje sve podatke s krajnjeg uređaja u oblak za daljnju obradu.



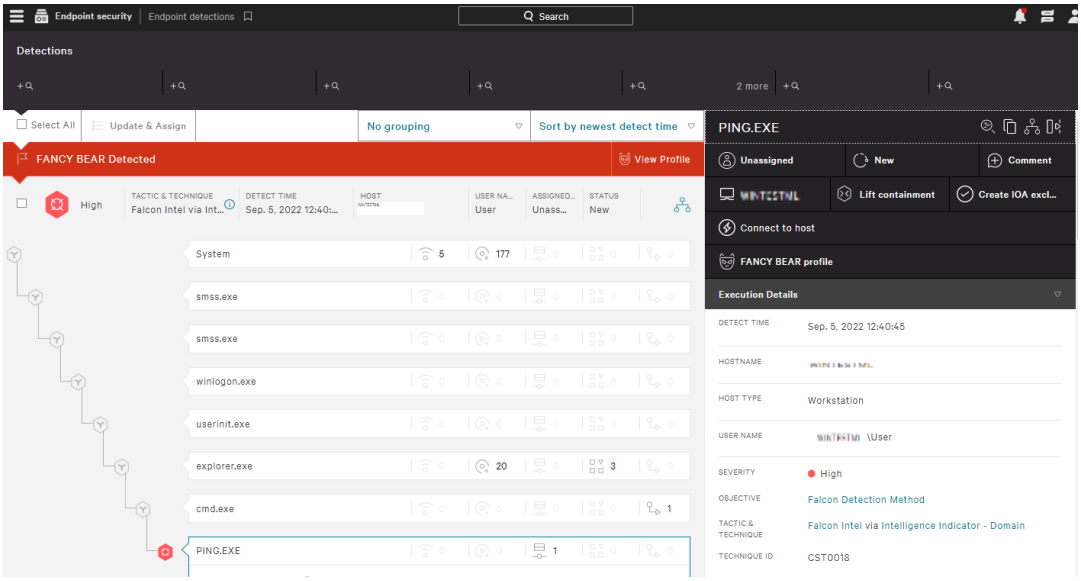
Slika 6.4: Provjera statusa senzora na krajnjem uređaju



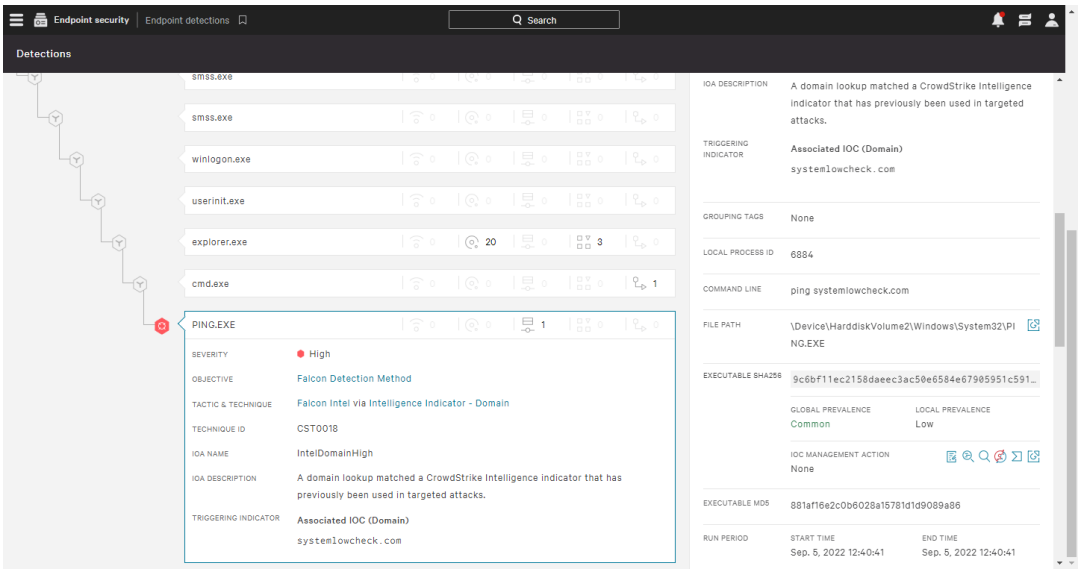
Slika 6.5: Provjera vidljivosti instaliranog senzora na platformi

Ovisno o postavljenim policama, postavkama blokiranja i dopuštanja određenih procesa na krajnjim uređajima, odnosno *blacklistingu* i *whitelistingu* procesa, IP adresa, puteva datoteke, naredbenih linija i *hasheva* te indikatorima napada i ostalim mogućnostima koje tehnologija nudi, Crowdstrike detektira neželjena i sumnjiva ponašanja u sustavu i prema zadanim kriterijima stvara detekciju. Aktivnost je automatski blokirana na krajnjem uređaju, a sigurnosni timovi odmah obaviješteni o događaju. Ovisno o ozbiljnosti i prioritetu, poduzimaju se potrebni koraci za saniranje, odgovor te dodatnu istragu o samoj aktivnosti [26]. Slika *6.6* i Slika *6.7* prikazuju detaljan pregled detektirane sumnjive aktivnosti na jednom krajnjem uređaju. U detaljima

izvršenja aktivnosti dane su točne informacije o krajnjem uređaju, korištenoj taktici i tehnici, vremenu izvedbe, procesu („PING.EXE) te korištenoj naredbenoj liniji („ping systemlowcheck.com“) koja predstavlja glavni izvor zlonamjerne aktivnosti. Crowdstrike je aktivnost povezao s domenom korištenom u prethodnim kibernetičkim napadima, a dodatno je detekciju povezao s profilom prijetnje pod nazivom *Fancy Bear*.

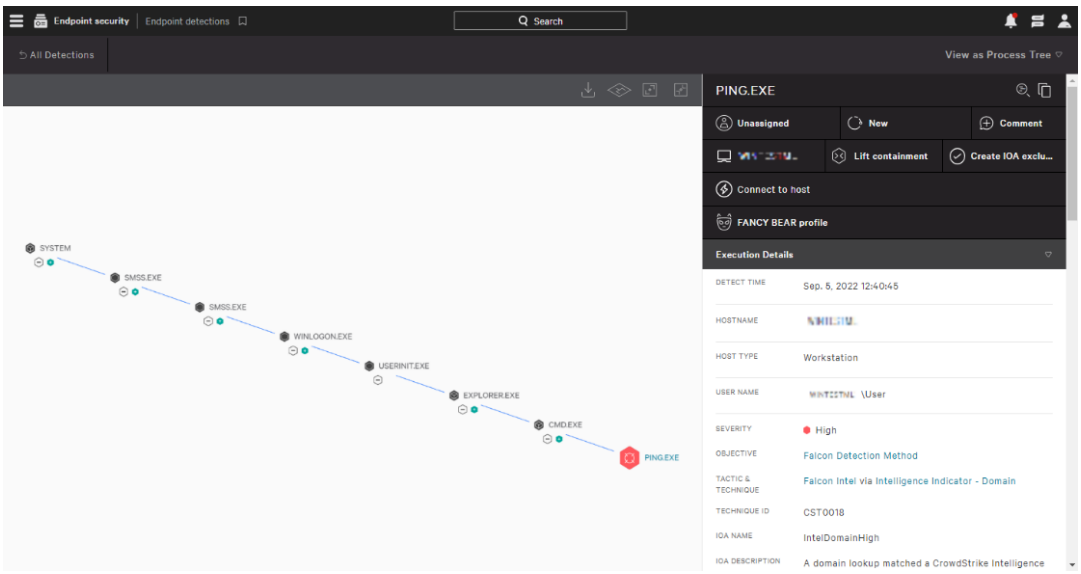


Slika 6.6: Opis detekcije na krajnjem uređaju



Slika 6.7: Opis detekcije na krajnjem uređaju

Slika 6.8 kroz grafički presjek daje dodatan pregled aktivnosti i procesa koji su doveli do nastanka detekcije.



Slika 6.8: Detaljniji uvid u detekciju na krajnjem uređaju

7. ZAKLJUČAK

Povećanjem količine osjetljivih podataka, veličine baza podataka, povezanosti uređaja i mreža unutar organizacije potreba za zaštitom koja pokriva sve navedene aspekte organizacijskog okruženja postaje sve veća. Osim prevencije i detekcije prijetnji kojima je korporacijsko okruženje konstantno izloženo, svaka organizacija s ozbiljnom sigurnosnom strategijom uzima u obzir granične situacije u kojima dolazi do napada i kompromitiranosti vlastite imovine. Kao što je u radu navedeno, kibernetički napadi su tijekom godina postali sve kompleksniji i sofisticiraniji pa tradicionalni i samostalni sigurnosni mehanizmi ne posjeduju dovoljno sposobnosti oduprijeti se takvim napadima. Socijalni inženjering, *ransomware*, DDoS napad, krađa identiteta i napadi na lozinke su samo neki od način kompromitiranja sustava i korisničkih identiteta, a nedovoljna zaštita otvara put zlonamjernim softverima ka širenju i invadiranju ostalih dijelova organizacije. Prethodna poglavlja daju konkretnije smjernice za zaštitu IT infrastrukture i sprječavanje neautoriziranih pristupa organizacijskim podacima. Od implementacije vatrozida, *proxyja*, segmentacije mreže, sustava za prevenciju i detekciju upada pa sve do kombiniranja višestrukih kontrola, a sve ovisno o potrebama svake korporacije. Također, organizacija treba razmišljati dalje od samog raspoređivanja mehanizama i programa, odnosno treba posvetiti dio resursa za planiranje upravljanja kibernetičkom sigurnošću u svojem okruženju. Upravo je peto poglavlje dio u kojem se govori o značaju definiranja okvira sigurnosti, polica, standarda, procedura i smjernica, a koje obrađuju svaku moguću situaciju i događaj koji svojim utjecajem može ozbiljno naštetiti i ugroziti poslovanje i daljnji razvoj organizacije. Izloženost krajnjih uređaja dodatno povećava činjenica da su to dijelovi organizacijske imovine direktno pod kontrolom osoblja što predstavlja najslabiju kariku u lancu sigurnosti. Iz tog razloga, u radu se posebno naglašava važnost postojanja i kontinuiranog napretka edukacije, treninga i osviještenosti osoblja o postojanim prijetnjama i rizicima te načinima prepoznavanja i reagiranja u takvim situacijama. Pred kraj, sve dotadašnje spomenute i objašnjene sigurnosne kontrole prikazane su kao dio jedne cjeline, odnosno tehnologija i rješenja danas popularnih u većini organizacija, EDR, XDR i MDR. To su rješenja koja kombiniraju više mehanizama i metoda, a sve u svrhu maksimalne spremnosti na detekciju, zaštitu i odgovor na sve prijetnje i napade. Kroz konkretan primjer jednog takvog rješenja, *Crowdstrike Falcon*, opisan je način implementacije i funkcioniranja tehnologije koja svojim uslugama nudi kompletnu zaštitu na svim područjima djelovanja i svim aspektima organizacije, od krajnjih uređaja, podataka u oblaku, kontejnera pa sve do zaštite mreže.

LITERATURA

[1] Palo Alto Networks, What is an endpoint, dostupno na: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint [5.9.2022.]

[2] Trellix, What is Endpoint Management, dostupno na: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security-management.html [5.9.2022]

[3] National Institute of Standards and Technology, Information Security, NIST Special Publication 800-30 Rev.1, US Department of Commerce, 2012., dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [18.8.2022.]

[4] National Vulnerability Database, NIST, U.S. Department of Commerce, dostupno na: https://nvd.nist.gov/ [23.8.2022.]

[5] M. Chapple, D. Seidl, CompTIA Cybersecurity Analyst (CSA+) Study Guide: Exam CS0-001, Sybex, Canada, 2017.

[6] Lockheed Martin Corporation, The Cyber Kill Chain, 2022., dostupno na: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [15.8.2022.]

[7] M. Chapple, D. Seidl, CompTIA Security+ Study Guide: Exam SY0-601, 8th Edition, Sybex, Canada, 2021

[8] Verizon, 2022 Data Breach Investigations Report

[9] Y. Diogenes, E. Ozkaya, Cybersecurity – Attack and Defense Strategies, Packt Publishing Ltd., Birmingham, 2018.

[10] CERT, Network Defense Essentials, Version 1, EC-Council

[11] O. Zlotnik, System Hardening Guidelines for 2022: Critical Best Practices, Hysolate, 2021, dostupno na: https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/ [25.8.2022]

[12] National Institute of Standards and Technology, Technical Guide To Information Security Testing and Assessment, NIST Special Publication 800-115, US Department of Commerce, 2008, dostupno na:

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, [25.8.2022]

[13] A. F. Sheikh, CompTIA Security+ Certification Study Guide – Network Security Essentials, Apress, 2020.

[14] ANY.RUN, Why do you need a malware sandbox, Cyber defense magazine, 2022., dostupno na: https://www.cyberdefensemagazine.com/why-do-you-need-a-malware-sandbox/ [22.8.2022]

[15] P. Cichonski, T. Millar, T. Grance, K. Scarfone, Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2, US Department of Commerce, 2012, dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [20.8.2022.]

[16] J. H. Saltzer, M. D. Schroeder, The Protection of Information in Computer Security, University of Virginia, Department of Computer Science, Virginia, 1975., dostupno na: https://www.cs.virginia.edu/~evans/cs551/saltzer/ [23.8.2022.]

[17] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Arhitecture, NIST Special Publication 800-207, 2020., dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [23.8.2022.]

[18] M. Nieles, K. Dempsey, V. Y. Pillitteri, An Introduction to Information Security, NIST Special Publication 800-12 Revision 1, U.S. Department of Commerce, 2017., dostupno na: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf [23.8.2022.]

[19] Cybersecurity for Small Business: NIST Cybersecurity Framework, dostupno na: https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf [23.8.2022.]

[20] M.Wilson, J. Hash, Computer Security, NIST Special Publication 800-50, U.S. Department of Commerce, 2003, dostupno na: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf [23.8.2022.]

[21] Trellix, What is an Endpoint Protection Platform?, dostupno na: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-an-endpoint-protection-platform.html [23.8.2022.]

[22] Syscom, Endpoint Security (NGAV& EDR), dostupno na: https://syscomgs.com/en/solutions/it-security-solutions/endpoint-security-ngav-edr/ [23.8.2022]

[23] Trellix, What is Extended Detection and Response (XDR)?, dostupno na: https://www.trellix.com/en-hk/security-awareness/endpoint/what-is-xdr.html [23.8.2022.]

[24] Crowdstrike, Threat Graph, dostupno na: https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf, [23.8.2022.]

[25] Crowdstrike, Falcon Endpoint Protection Enterprise, dostupno na: https://www.crowdstrike.com/wp-content/uploads/2019/04/crowdstrike-falcon-enterprise-bundle-data-sheet.pdf, [2.9.2022.]

[26] Crowdstrike Blog, Crowdstrike Tech Center, dostupno na: https://www.crowdstrike.com/blog/tech-center/, [5.9.2022.]

SAŽETAK

U ovom diplomskom radu naglasak je bio na važnosti krajnjih uređaja u organizaciji te njihovoj ranjivosti, a što uvelike utječe na reduciranje kompletne sigurnosti korporacijskog okruženja. Krajnji uređaji kao ulazne točke i pritom najranjiviji dio organizacije predstavljaju važan dio okruženja kod procjene i primjene sigurnosnih kontrola. Od zlonamjernih programa koji kompromitiraju sustave i tehnika socijalnog inženjeringa za kompromitiranje korisničkih identiteta, danas se organizacije svakodnevno susreću i bore s raznoraznim prijetnjama koje za cilj imaju ugroziti sigurnost i poslovanje organizacija. Iz tog se razloga javlja potreba za povećanjem opsega kibernetičke sigurnosti u svim aspektima korporacijskog okruženja, a koji osim krajnjih uređaja uključuju mreže, osoblje i oblak. Osim implementacije vatrozida, *proxyja*, sustava detekcije i prevencije upada, VPN, segmentacije mreže, EDR rješenja i ostalih sigurnosnih kontrola postavljenih u svim dijelovima organizacije, važnost se stavlja i na procese oporavka te odgovora na incidente. To su dodatni obrambeni mehanizmi kojima se pokrivaju situacije u kojima dolazi do napada i ozbiljne kompromitiranosti uređaja, sustava i korisničkih identiteta. Aktivnosti, djelovanja, odgovori i implementacije unutar organizacije proizlaze iz posture i okvira kibernetičke sigurnosti kroz police, procedure, procese i smjernice kojima se definiraju pristupi sigurnosti unutar organizacije s naglaskom na identificiranje, zaštitu, detekciju, odgovor i oporavak.

Ključne riječi: krajnji uređaji, kibernetička sigurnost, ugroze, EDR, *Crowdstrike Falcon*

SECURITY OF ENDPOINT DEVICES IN CORPORATIVE ENVIRONMENT

ABSTRACT

In this master's thesis the emphasis was on the importance of endpoint devices in organizations and their vulnerability which greatly affects the reduction of the complete security of the corporate environment. As entry points and with that the most vulnerable organization's asset endpoints represent an important part of the environment when assessing and applying security controls. From malicious programs (malwares) that compromise systems and social engineering techniques that compromise user's identities, organizations encounter and fight a variety of threats that aim to compromise the security and corporate operations on a daily basis. For this reason, there is a need to increase the scope of cybersecurity in all aspects of the corporate environment, which in addition to endpoints include networks, personnel and the cloud workloads. In addition to the implementation of firewalls, proxies, intrusion detection and prevention systems, VPN, network segmentation, EDR solutions and other security controls placed in all parts of the organization, importance is also placed on recovery processes and incident response. These are additional defense mechanisms to cover situations where attacks occur alongside serious compromise of devices, systems and user identities. Activities, actions, responses and implementations within the organization derive from the posture and framework of cybersecurity through policies, procedures, processes and guidelines that define security approaches within the organization with an emphasis on identification, protection, detection, response and recovery.

Keywords: endpoints, cybersecurity, threats, EDR, Crowdstrike Falcon

ŽIVOTOPIS

Martina Lenić rođena je 11. siječnja 1999. u Vinkovcima. Osnovnu školu završava u OŠ fra Bernardina Tome Leakovića u Bošnjacima, a po završetku upisuje Opću Gimnaziju u Županji koju uspješno završava 2017. godine. Iste godine upisuje preddiplomski sveučilišni studij elektrotehnike na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku. Na drugoj godini studija opredijeljuje se za smjer Komunikacije i informatika te 2020. godine stječe titulu prvostupnice. Odmah iste godine upisuje sveučilišni diplomski studij elektrotehnike, smjer Komunikacije i informatika, modul DKB – Mrežne tehnologije. Tijekom zadnje godine diplomskog studija pridružuje se *Cybersecurity* akademiji tvrtke Atos pod čijim sumentorstvom piše ovaj diplomski rad.