Integrirana sigurnosna rješenja za zaštitu krajnjih uređaja

Fabing, Megan - Maria

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

INTEGRIRANA SIGURNOSNA RJEŠENJA ZA ZAŠTITU KRAJNJIH UREĐAJA

Diplomski rad

Megan-Maria Fabing

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za imenovanje Povjerenstva za diplomski ispit

Osijek, 13.09.2022.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za diplomski ispit

Ime i prezime Pristupnika:	Megan - Maria Fabing
Studij, smjer:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. Pristupnika, godina upisa:	D-1289, 13.10.2020.
OIB studenta:	67617340151
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	,
Sumentor iz tvrtke:	Siniša Husnjak
Predsjednik Povjerenstva:	Doc. dr. sc. Višnja Križanović
Član Povjerenstva 1:	Izv. prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	Mr.sc. Anđelko Lišnjić
Naslov diplomskog rada:	Integrirana sigurnosna rješenja za zaštitu krajnjih uređaja
Znanstvena grana diplomskog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	U radu je potrebno analizirati i objasniti različite metode zaštite i integrirana sigurnosna rješenja za krajnje uređaje (endpoint protection), uz konkretne primjere i s naglaskom na MDM (Mobile Device Management). Tema rezervirana za: Megan-Maria Fabing Sumentor iz tvrtke: Siniša Husnjak (Atos)
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene od strane mentora:	13.09.2022.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 26.09.2022.

Ime i prezime studenta:	Megan - Maria Fabing
Studij:	Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika'
Mat. br. studenta, godina upisa:	D-1289, 13.10.2020.
Turnitin podudaranje [%]:	6

Ovom izjavom izjavljujem da je rad pod nazivom**: Integrirana sigurnosna rješenja za zaštitu krajnjih uređaja**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

Tijekom godina krajnji uređaji (stolna i prijenosna računala, pametni telefoni, pametni satovi i slično) postaju dio svakodnevice gotovo svake osobe. S obzirom da se tehnologija svakim danom sve više razvija, sve su češći napadi na spomenute uređaje. Hakeri svakim danom rade sve više kako bi ukrali vrijedne podatke i informacije te na taj način ugrozili organizacije i svakog pojedinca. Jedna od najpoznatijih vrsta napada su phishing napadi. Tim putem, uz pomoć naizgled legitimne poruke na koju osoba može nasjesti i podijeliti svoje osjetljive podatke, hakeri kradu i manipuliraju ukradenim podacima. Ostale poznate vrste napada su DoS napadi, nezakrpljene ranjivosti, gubitak i krađa podataka, zlonamjerni softver te usputna preuzimanja. Zlonamjerni softver stvoren je da nanese štetu računalu, računalnom sustavu, poslužitelju, mreži ili iskoristi neki drugi softver ili hardver. Ima mogućnost razbijanja slabih lozinki nakon čega se može uvući se u sustave i proširiti mrežom. Osim spomenutog, može zaključati važne datoteke, slati neželjenu poštu, usporiti računalo te preusmjeriti korisnika na zlonamjerne stranice. Zbog navedenih prijetnji, javljaju se razna sigurnosna rješenja koja se integriraju u krajnje uređaje kako bi se zaštitili od napada. EPP predstavlja softver koji se temelji na potpisu, a sastoji se od različitih sigurnosnih alata kao što su antivirusni programi, anti-malware, enkripcija podataka, osobni vatrozidi i prevencija upada. EDR predstavlja način otkrivanja i odgovarajućeg reagiranja na unutarnje prijetnje pomoću svojih specifičnih funkcija kao što su kontinuirani nadzor, sanacija i bez smetnje krajnjoj točki. MDM predstavlja softver za osiguravanje, nadziranje, upravljanje i podržavanje mobilnih uređaja čiji je cilj optimizirati funkcionalnost i sigurnost mobilne komunikacijske mreže minimiziranjem troškova i zastoja. Cilj EEM-a je osigurati podatke organizacije na mobilnim uređajima zaposlenika, a integriraju s drugim IT sustavima i aplikacijama poduzeća za isporuku širokog raspona poslovnih funkcionalnosti. UEM predstavlja spoj MDM-a i EEM-a te omogućuje upravljanje svim uređajima organizacije.

U drugom poglavlju nabrojane su vrste krajnjih uređaja i opis svakog od njih. U trećem poglavlju navedene su i objašnjene najpoznatije sigurnosne prijetnje krajnjim uređajima kao i statistika koja pokazuje njihovu učestalost i slično. U četvrtom poglavlju rada opisana su integrirana sigurnosna rješenja za zaštitu krajnjih uređaja. U petom poglavlju dana su programska rješenja za zaštitu mobilnih uređaja. U šestom poglavlju dani su glavni zaključci vezani uz krajnje uređaje i njihovu zaštitu.

1.1. Zadatak diplomskog rada

U radu je potrebno analizirati i objasniti različite metode zaštite i integrirana sigurnosna rješenja za krajnje uređaje (endpoint protection), uz konkretne primjere i s naglaskom na MDM (Mobile Device Management).

2. KRAJNJI UREĐAJI

Krajnji uređaji se nalaze u distribuiranom računalnom sustavu gdje djeluju kao korisnička krajnja točka te se najčešće koriste za tvrdi disk računala koji se spaja na internet pomoću TCP/IP mreže. S obzirom da postoje različite vrste mreža, svaka od njih ima svoje vrste krajnjih uređaja gdje korisnici pristupaju informacijama s mreže [1].

S obzirom na način djelovanja koji je ranije spomenut, krajnji uređaj se može definirati kao udaljeni računalni uređaj koji u oba smjera komunicira s mrežom na koju je povezan. Krajnji uređaji uključuju računala, laptope, mobilne uređaje, uređaje internet objekata i slično. S obzirom da u današnje vrijeme organizacijska radna snaga postaje sve mobilnija te se korisnici povezuju na interne resurse izvan poslovnih prostora, krajnji uređaji postaju laka meta hakerima na kojima izvršavaju kodove koji mogu potencijalno zaraziti uređaje i ukrasti vrijedne podatke [2].

Mrežne konfiguracije se mijenjaju vrlo brzo te se svakodnevno dodaju novi uređaji. M. Kandrich [3] dijeli krajnje uređaje u skupine koje će biti opisane u nastavku. Raspodjela skupina pomaže u razumijevanju uloga krajnjih uređaja unutar pojedine organizacije.

2.1. Windows krajnji uređaji

Prvu skupinu krajnjih uređaja čine Windows krajnji uređaji čiji sustav pokreće neku od verzija Microsoft Windows operacijskog sustava. Kako bi se moglo reći da je neki krajnji uređaj, Windows krajnji uređaj, bitno je istaknuti da mora sadržavati Integrirani DOS s Windows upraviteljem (*eng. Windows Manager*).

Prvi sustav koji je sadržavao prethodno naveden DOS bio je Windows 95. Sustavi prije Windows 95, također su sadržavali DOS s Windows upraviteljem, ali temeljili su se na komandnim linijama. Kasnije inačice Windows sustava imale su razvijeno grafičko sučelje koje je korisnički bilo vrlo jednostavno za korištenje s velikim brojem aplikacija. S obzirom da su se grafička sučelja razvijala sve većom brzinom, Microsoft operacijski sustav je stekao veliku popularnost, kako među pojedincima, tako i tvrtkama te danas čini više od 90% instaliranih operacijskih sustava. S obzirom na veliku raširenost, Windows je postao velika meta za hakere koji žele naštetiti sustavima i manipulirati vrijednim podacima te se iz tih razloga razvijaju metode za zaštitu operacijskih sustava [3].

2.2. Krajnji uređaji ostalih operacijskih sustava

Krajnje uređaje ostalih operacijskih sustava predstavlja svaki uređaj koji se ne temelji na Microsoft Windows operacijskom sustavu. S obzirom da je pojam uređaja koji nisu Windows vrlo širok, M. Kandrich [3] sužava skupinu na stolna računala, prijenosna računala i servere. Takav način klasifikacije određuje da krajnji uređaji koji nisu Windows uključuju sve varijante Unix operacijskih sustava.

Unix je operacijski sustav koji upravlja načinom na koje računalo radi te izvršava zadatke koji su korisni za korisnika; pokreće memoriju, diskovne pogone, tipkovnice, video monitore i slično. Na početku, Unix je bio dizajniran kako bi se olakšao razvoj softvera. Kasnijim razvojem cilj je bio pružiti što jednostavnije, a kvalitetne programe dizajnirane na način da više korisnika može obavljati veliki broj zadataka koji se izvršavaju istovremeno. S vremenom Unix operacijski sustavi postali su vrlo popularni zbog čega dolazi do pojave sve većeg broja raznih operacijskih sustava temeljenih na Unix-u [4]. Neki od njih bit će opisani u nastavku.

Jedan od najpopularnijih i najsigurnijih operacijskih sustava temeljenih na Unix-u je Linux. Linux je operacijski sustav otvorenog koda koji se sastoji od jezgre, osnovne komponente operacijskog sustava, alata, aplikacija i usluga. Nalazi se između aplikacija i hardvera te uspostavlja vezu između softvera koji izravno upravlja hardverom i resursa koji obavljaju određeni posao [5]. S obzirom da je Linux besplatni operacijski sustav otvorenog koda, stvorene su različite inačice: Debian, Gentoo, Ubuntu, Linux Mint, Red Hat Enterprise Linux, CentOS, Fedora, Kali Linux, Arch Linux i OpenSUSE [6]. Osim Linuxa, jedan od sustava temeljenih na Unixu je BSD. BSD (*eng. Berkeley Software Distribution*) je operacijski sustav otvorenog koda koji ima nekoliko inačica: NetBSD, FreeBSD i OpenBSD. Početni BSD je odgovoran za NeXTStep OS koji je osnova razvoja Mac OS X. Apple pomaže u razvoju i stvaranju Darwin operacijskog sustava koji se temelji na otvorenom kodu, a kasnije se razvija uglađena verzija Mac Os X-a koji se naziva MacOS te je zatvorenog tipa. Sljedeći operacijski sustav koji se temelji na Unix-u je AIX (*eng. Advanced Interactive eXecutive*) koji se temelji na proširenjima koja su kompatibilna s 4.3BSD i Unix System V te je ujedno i prvi sustav koji je implementirao datotečni sustav dnevnika. Razvijen je od strane IBM-a te je podržan na IBM Power Systems. S obzirom da je AIX vrlo pouzdan, stabilan i siguran, zamišljen je da bude operacijski sustav za poduzeća te stječe veliku popularnost na komercijalnom tržištu UNIX operacijskih sustava. HP-UX (*eng. Hewlett Packard Unix*) temelji se na System V izdanju 4 te ima izvrsne značajke upravljanja sigurnosti i fleksibilnosti kao i dostupnosti upravljanja

memorijom. Osim prethodno navedenih, razvijeni su operacijski sustavi SGI-ov Irix, Oracle-ov Solaris i Microsoft-ov Xenix koji su kasniji ukinuti [7].

2.3. Mobilni krajnji uređaji

Mobilni krajnji uređaji su vrsta ručnog računala male veličine dizajnirani da budu lako prenosivi i da stanu u ruku. S obzirom na napredak tehnologije pohrane, obrade i prikaza podataka, mobilni uređaji mogu obavljati gotovo svaku funkciju kao klasična i prijenosna računala. U mobilne uređaje se ubrajaju tableti, e-čitači, pametni telefoni, PDA uređaji, prijenosni glazbeni uređaji, pametni satovi i slično, o kojima će kasnije biti više spomenuto u nastavku.

Pametni telefoni su mobilni uređaji nastali iz tradicionalnih mobilnih telefona uz razliku da imaju puno napredniju tehnologiju. Imaju zajedničke značajke kao što su: mogućnost upućivanja i primanja poziva, SMS poruka i govorne pošte. Značajke po kojima se pametni telefoni razlikuju od tradicionalnih su: korištenje interneta, elektroničke pošte, društvenih mreža, kupovina putem online trgovina, preuzimanje aplikacija putem mobilne ili bežične veze i slično. Sljedeća vrsta mobilnih krajnjih uređaja su tableti koji su slični prijenosnim računalima, ali nude nešto drukčije mogućnosti. Ne pokreću se aplikacije za stolna i prijenosna računala, nego aplikacije koje su dizajnirane za tablete. Tableti mogu biti raznih veličina, veći su od pametnih telefona, a nešto manji od prijenosnih računala. Osim u aplikacijama, glavna razlika između prijenosnih računala i tableta je u tome što tableti imaju sučelje zaslona koje je osjetljivo na dodir, a umjesto miša koristi se prst ili olovka. E-čitači su specijalizirana vrsta tableta koji se koriste za čitanje digitalnih knjiga. Digitalne knjige se mogu preuzeti ili kupiti putem interneta. Pametni satovi su jedni od najnovijih izuma mobilnih krajnjih uređaja. Većina se pokreće operacijskim sustavom koji je isti ili slični kao na pametnom telefonu te su sposobni pokretati svoje vlastite aplikacije. Ideja pametnih satova je u povezivanju s drugim pametnim telefonima kako bi se omogućilo dijeljenje podataka i stvorilo što jednostavnije i praktičnije iskustvo korištenja. Prijenosni glazbeni uređaji su mobilni uređaji koji imaju pristup internetu kako bi mogli preuzeti aplikacije koje će pomoći u poboljšanju vrijednosti za osobu koja ih koristi. PDA uređaji bili su vrlo korišteni u poslovnom svijetu, ali su izgubili na značaju dolaskom pametnih telefona. Danas ih se pokušava vratiti nazad uvođenjem bežične veze i dugotrajnosti što ih čini korisnima ljudima koji su u vojsci i na terenu [8].

Pojavom i napretkom tehnologije mobilnih uređaja razvijaju se i operacijski sustavi koji pomažu u pokretanju aplikacijskog softvera. Operacijski sustavi mobilnih uređaja mogu biti

otvorenog koda, zatvorenog koda te djelomično otvorenog koda. Neki od sustava koji su bili prije poznati, a sada se više ne koriste su: Symbian OS, Windows, Blackberry Os i mnogi drugi. Najpoznatiji operacijski sustavi na današnjem tržištu je Android. Android je mobilni operacijski sustav koji se temelji na Linux jezgri i softveru otvorenog koda koji je razvijen od strane Google-a. Google dopušta besplatno korištenje dijelova Android operacijskog sustava kako bi se kreirale inačice operacijskih sustava primjerene za korištenje na svojim mobilnim uređajima, neke od njih su: Huawei, MIUI (Xiaomi) i slično. Drugi najpoznatiji operacijski sustav na tržištu je iOS. IOS operacijski sustav razvijen je od strane Apple-a te je vrlo siguran za korištenje s obzirom da je sustav zatvorenog koda. Zatvoreni kod znači da se može koristiti samo na svojim mobilnim uređajima i nije dostupan za druge mobilne uređaje [9].

2.4. IoT krajnji uređaji

IoT (eng. *Internet of Things*) uređaji su nestandardni računalni uređaji. Bežično se povezuju na mrežu i mogu prenositi podatke. IoT se sastoji od proširenja internetske povezanosti izvan standardnih uređaja kao što su stolna i prijenosna računala, pametni telefoni i tableti do niza fizičkih uređaja i svakodnevnih internet objekata. Jedna od velikih prednosti ovih uređaja je što se mogu promatrati i kontrolirati na daljinu. Način rada svih IoT uređaja je vrlo sličan te su dizajnirani na način da uređaj osjeća događanja u fizičkom svijetu. Uređaji se sastoje od integriranog CPU-a, mrežnog adaptera i firmware-a te se u većini slučajeva povezuju na DHCP poslužitelj (eng. *Dynamic Host Configuration Protocol*). Tamo dobivaju IP adresu pomoću koje se uređaj može koristiti za funkcioniranje na mreži. Većina IoT uređaja dizajnirana je posebno za privatne mreže, dok su neki izravno dostupni preko javnog interneta. Nakon konfiguriranja IoT uređaja većina prometa je odlazna, a neki od njih prihvaćaju unose.

Svi povezani uređaji razgovaraju s drugim povezanim uređajima u okruženju da bi se automatizirali kućni i industrijski zadaci. Uređaji se dijele u tri glavne skupine: potrošačke, poslovne i industrijske. Potrošački uređaji uključuju pametne uređaje, televizore i zvučnike, nosive uređaje i igračke. Poslovni uređaji su dizajnirani na način da ih koriste različite tvrtke gdje se uređaji razlikuju po svojim mogućnostima te su usmjereni na održavanje objekta. Poslovne uređaje čine pametne brave, pametni termostati, pametna rasvjeta i pametna sigurnost. Industrijski IoT uređaji dizajnirani su za korištenje u industrijskim poduzećima i tvornicama te se koriste za praćenje montažne linije ili bilo kojeg drugog procesa u proizvodnji. Pomoću senzora, podaci se prenose u aplikacije za praćenje kako bi se osigurao optimalan rad kritičnih procesa i kako bi se spriječili neplanirani zastoji zamjenom potrebnih dijelova [10].

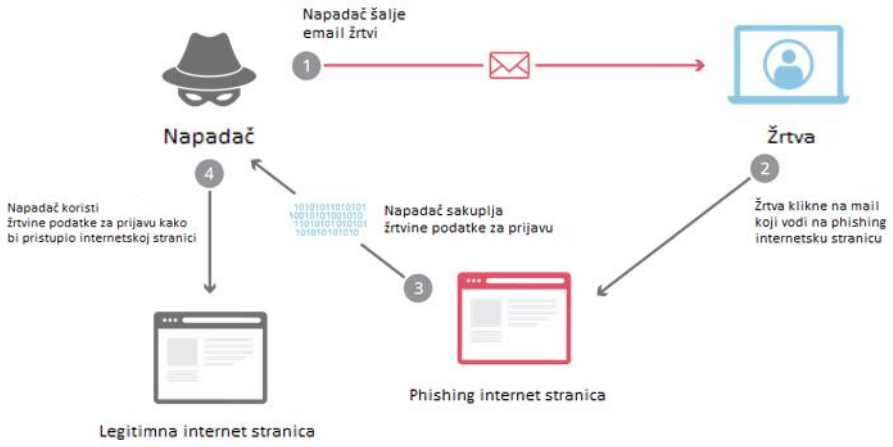
3. SIGURNOSNE PRIJETNJE KRAJNJIM UREĐAJIMA

Sigurnosne prijetnje krajnjim uređajima su velik problem današnjice jer predstavljaju velike rizike, kako za velike organizacije tako i za svakog pojedinog korisnika. Sigurnosni napadi dovode do velikih gubitaka bitnih podataka koji mogu potencijalno ugroziti svakog pojedinca ili organizaciju [11].

Sigurnosna prijetnja definira se kao svaki zlonamjerni napad koji želi pristupiti podacima na ilegalan način te ih tako poremetiti ili oštetiti. U posljednjih nekoliko godina došlo je do velikih prijetnji u kojima su razotkriveni vrlo osjetljivi podaci (datum rođenja, brojevi socijalnog osiguranja i adrese) kojima se narušila sigurnost svakog pojedinca. Ukradeni podaci mogu se koristiti za krađu informacija i pristup financijskim računima. Zbog toga su vrlo važni stručnjaci za računalnu sigurnost koji se bave očuvanjem zaštite privatnih podataka. Napadi se događaju zbog neuspjelog implementiranja i testiranja zaštitnih mjera kao što su enkripcija, autentifikacija i vatrozidi [12]. U nastavku će biti opisano nekoliko vrsta sigurnosnih prijetnji, odnosno napada, krajnjim uređajima.

3.1. Phishing napadi

Pojam phishing napada prvi put se pojavljuje 1996. godine nakon što su hakeri napali AOL korisnička imena i lozinke. Korisnicima su bile poslane elektroničke poruke u kojima su zahtijevali od korisnika podatke o računu te je velik broj korisnika na njih nasjeo. Izvještaji iz toga razdoblja govore da su hakeri skupili dovoljno računa kako bi ih pretvorili u neslužbenu valutu koja je bila poznata samo njima. Mijenjali su određeni dio „phish-a“ za dio softvera ili bi mijenjali jedan dio „phish-a“ za drugi. „Phish“ predstavlja dio ukradene informacije kojom su hakeri manipulirali. Među najranijim prijavama o krađi identiteta spominje se u medijima 16. ožujka 1997. u priči Florida Times-Union-a. U novinama se nalazio odjeljak koji je sadržavao informacije o phishing napadima u obliku traženja lozinke. Najprije su se napadi odvijali slanjem elektroničke pošte, a u posljednjih nekoliko godina napadi se odvijaju putem društvenih mreža (Facebook, Twitter, Instagram...) s obzirom na njihov razvitak [13]. (Slika 3.1.) prikazuje primjer phishing napada putem elektroničke pošte.



Slika 3.1. Phishing napad [14]

Najčešći napadi za krađu identiteta su na velike tvrtke i organizacije nakon čega hakeri dobivaju pristup osjetljivim podacima i informacijama o korisnicima. Ovakav napad ima dugoročnu štetu, kako ljudima čiji su podaci ukradeni, tako i organizaciji koja je hakirana jer se čine nepouzdanima. Gubitak podataka, informacija i javni ugled je rizik koji organizacije pokušavaju prikriti i ublažiti kako bi ostale relevantne među klijentima. Otkrivanje phishing napada ovisi o raspoloživim resursima. Raspoloživi resursi mogu biti provođenje obuke za podizanje svijesti o sigurnosti ili sigurnosna rješenja krajnjih uređaja. Sigurnosna rješenja krajnjih uređaja podrazumijevaju korištenje umjetne inteligencije kako bi otkrili je li poslana poruka prijetnja krađi identiteta i podacima.

Rješenje za taj problem uključivalo bi pretplatu na davatelja usluga koji pruža analizu i zaštitu uređaja. Analizirao bi se ulazni promet te izolirale ulazne adrese elektroničke pošte uvođenjem sigurnosnih rješenja za zaštitu krajnjih uređaja [11]. Više o integriranim sigurnosnim rješenjima bit će opisano u daljnjim poglavljima.

3.2. Nezakrpljene ranjivosti

U operacijskim sustavima i softverima sve su češći napadi na nezakrpljene ranjivosti (eng. *unpatched vulnerabilities*). Na taj način hakeri dobivaju pristup poslovnim mrežama i mijenjaju zero-day ranjivosti velikom brzinom [15]. Prema [16], zero-day ranjivost se može definirati kao rupa u softveru nepoznata dobavljaču, a iskorištavaju je hakeri prije nego sam dobavljač postane svjestan situacije i potraži rješenje za popravak navedene situacije. Zero-day napade najčešće aktiviraju neke nepoznate ranjivosti i vrlo ih je teško otkriti. Hakeri iskorištavaju rupu u softveru kako bi ukrali vrijedne informacije koje mogu dovesti do

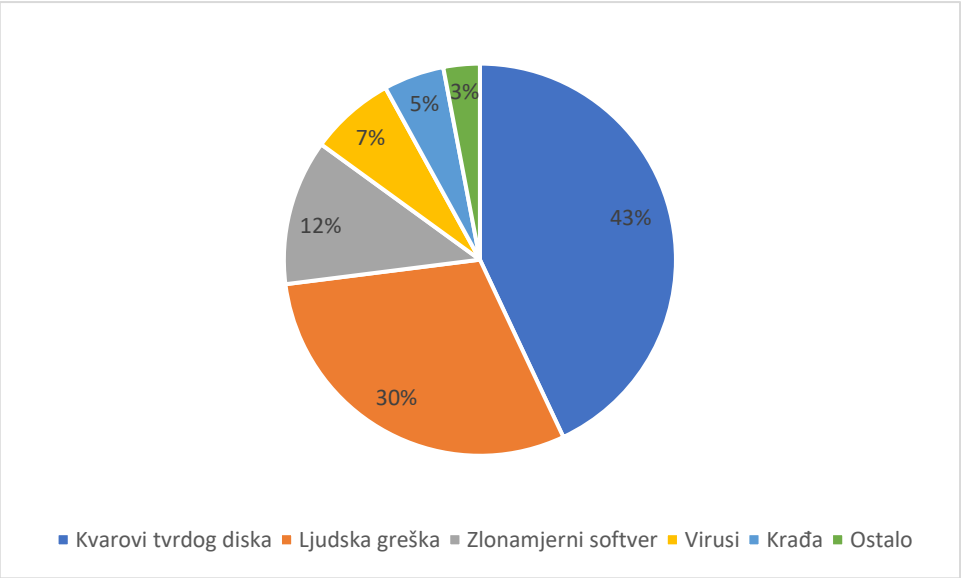
propadanja tvrtke. Nakon što dobavljač dostavi zaobilazna rješenja i popravke, sustav krajnjeg korisnika će i dalje biti ranjiv sve dok popravak ne bude u potpunosti primjenjiv. Zbog takvih situacija bitno je da se sve aplikacije koje se nalaze na digitalnim sustavima stalno ažuriraju.

S obzirom da tvrtke mogu ostaviti ranjivosti nezakrpane dulje vrijeme, napadi su vrlo česti. Šteta koja nastaje zbog takvih napada može biti vrlo velika jer hakeri nastoje prikupiti što više podataka od što većeg broja tvrtki te ih kasnije prodavati na dark webu i sličnim stranicama. Kako bi se spriječio financijski gubitak i gubitak bitnih podataka, važno je da tvrtke ulože u sigurnosni operativni centar i funkcije za otkrivanje prijetnji koje će se pobrinuti da se prijetnje otkriju i zaustave na vrijeme. Rješenje za upravljanje zakrpama su niz automatiziranih alata koji mogu u tome pomoći. Neki od njih su Ringmasterovo automatsko upravljanje, ažuriranje PatchLink-a i Gibraltarov Everguard. Osim toga, važno je da tvrtke provode redovite procjene unutar okruženja kako bi se nepopravljive ranjivosti otkrile prije nego budu iskorištene. Takve procjene mogu se obavljati pomoću penetracijskog testiranja, procjene ranjivosti, pregledom izvornog koda i procjenom crvenog tima [11].

3.3. Gubitak i krađa podataka

Povreda podataka raste te se očekuje da će porasti još više u sljedećim godinama. Gubitak i krađa podataka (eng. *data loss and theft*) mogu imati velikog utjecaja na tvrtke. Neki od utjecaja su regulatorne kazne, ransomware zahtjevi i troškovi istrage. Regulatorne kazne su vrlo velike ako tvrtke namjerno zanemaruju propise za zaštitu kupaca i podataka o kupcima. Ako zbog namjernog zanemarivanja propisa dođe do gubitka podataka, HIPAA može zahtijevati kaznu od 1.5 milijuna dolara samo za jedno kršenje. Kazne mogu rasti do 4.8 milijuna dolara što može vrlo negativno utjecati na financijsku situaciju tvrtke. Ransomware napadi su vrlo česti u današnje vrijeme i mogu dovesti tvrtke do velikih gubitaka. Ako se zatražena otkupnina ne plati, a sigurnosne kopije nisu dobre, može doći do trajnog gubitaka podataka. Na kraju, financijski utjecaj za utvrđivanje metoda kojima su podaci izgubljeni vrlo je skup jer se oporavak podataka naplaćuje na temelju količine podataka za povrat i može ostaviti velike posljedice na tvrtke [11].

Do gubitka podataka dolazi kada su ugrožene vrijedne i osjetljive informacije. Najčešći razlog gubitka podataka je zbog kvarova tvrdog diska, zatim slijedi ljudska pogreška, zlonamjerni softver, virusi, krađa ili gubitak struje i slično [17]. Dijagramom 3.1. prikazani su postotci najčešćih razloga gubitaka podataka.



Dijagram 3.1. Najčešći razlozi gubitaka podataka [18]

Kako bi se tvrtka zaštitila od gubitaka podataka bitno je redovito sigurnosno kopirati datoteke kako bi se omogućio oporavak u slučaju gubitaka podataka. Osim toga bitno je osigurati da su vrijedni i osjetljivi podaci u zaključanoj sigurnoj pohrani gdje će biti zaštićeni od krađe i napada. Pravilno zbrinjavanje zastarjelih podataka i informacija je također od velike važnosti jer ako hakeri dođu u doticaj s tim podacima, oni i dalje mogu imati neželjeni utjecaj na klijente. Na kraju, kako bi gubici podataka bili spriječeni, bitan je siguran pristup podacima putem enkripcije medija [11].

3.4. Zlonamjerni softver

Zlonamjerni softver (eng. *malicious software* - *malware*) je po definiciji zlonamjerna namjera, odnosno vrsta softvera stvorena da nanese štetu računalu, računalnom sustavu, poslužitelju, mreži ili iskoristi neki drugi softver ili hardver. Pomoću zlonamjernog softvera moguće je razbiti slabe lozinke, uvući se u sustave i proširiti mrežom te naštetiti tvrtkama i organizacijama. Osim spomenutog, zlonamjerni softver može zaključati važne datoteke, slati neželjenu poštu, usporiti računalo te preusmjeriti korisnika na zlonamjerne stranice.

Većina vrsta zlonamjernog softvera dijeli slične znakove. Jedan od znakova je iznenadan pad performansi računala jer zlonamjerni softver može zauzeti velik dio procesorske snage računala i tako usporiti njegov rad. Drugi znak je često padanje i zamrzavanje jer zlonamjerni softver koristi previše RAM memorije ili povećava temperaturu procesora. Osim toga dolazi do brisanja i oštećenja datoteka, iskakanja velikog broja skočnih oglasa, preusmjeravanje preglednika radi promjena DNS postavki uzrokovanih zlonamjernim softverom ili pojava

nepoznatih aplikacija. Sljedeći znakovi su širenje zlonamjernog softvera na način da upravlja elektroničkom poštom te šalje razne poruke kontaktima ili zaraženom računalu šalje (stručnjacima prepoznatljiv) *Ransomware*. Neke vrste zlonamjernog softvera su lakše za otkriti od drugih, ali najsigurniji način da bi se otkrili svi zlonamjerni program je imati neki od antivirusnih alata [19].

Prema [20] zlonamjerni softver može uzrokovati gubitak informacija, novac te stvara veliku prijetnju svim korisnicima tehnologije. Zlonamjerni softver se klasificira ovisno o karakteristikama programa koji se izvršava te načinu na koji djeluje na sustav. Takav način omogućuje podjelu zlonamjernog sustava na različite vrste koje će biti opisane u nastavku.

3.4.1. Računalni virus

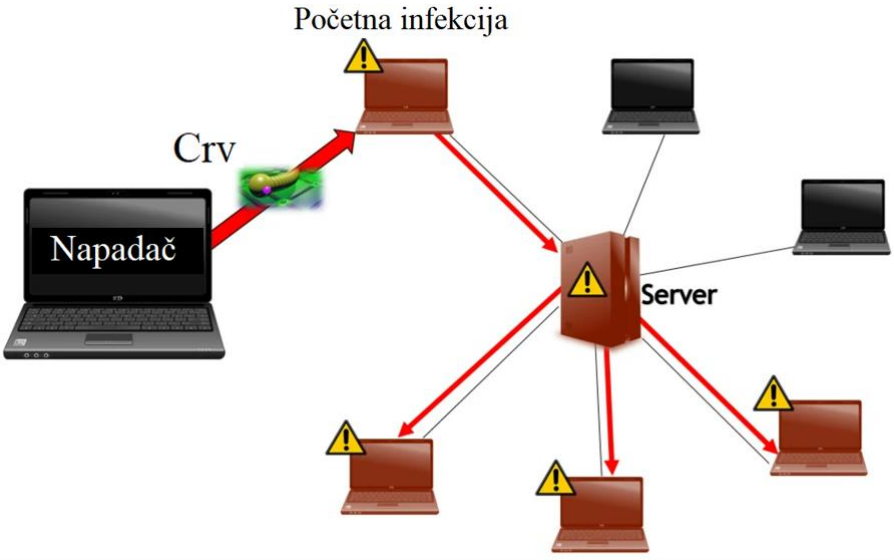
Računalni virus se definira kao zlonamjerni program sa svojstvom samoreplikacije koji postoji kao izvršna datoteka te se širi kopiranjem na druga računala. Virus je pasivan i potreban mu je prijenos kroz mrežne ili medijske datoteke. Koriste se za nanošenje štete računalima i mrežama te krađu informacija, novca i slično [20].

Virus je moguće primiti u obliku elektroničke pošte koja sadrži zlonamjerni privitak. Ako se privitak otvori, na računalu se pokreće virus zbog kojeg može doći do uništenja podataka i usporavanja sustava. Virus radi na način da zahtijeva program glavnog računala, zatim zahtijeva akciju korisnika za prijenos s jednog sustava na drugi te prilaže dijelove vlastitog zlonamjernog koda drugim datotekama ili izravno zamjenjuje datoteke svojim kopijama.

Većina računalnih virusa napada računala sa sustavom Microsoft Windows. Iako Mac računala imaju reputaciju velike otpornosti na viruse, Apple je dao izjavu da i on doživljavaju napade zlonamjernog softvera. Razlog zbog kojeg su napadi na Windows računalne sustave češći je jer u svijetu postoji veći broj korisnika tog sustava te hakeri stvaraju viruse za operacijski sustav koji će potencijalno imati veću količinu žrtava [21].

3.4.2. Računalni crv

Računalni crv *(*eng. *worm)* je aktivni zlonamjerni program sa svojstvom samoreplikacije koji se širi mrežom iskorištavanjem raznih ranjivosti sustava. Na slici 3.2. vidi se da računalni crv kontinuiranim skeniranjem iskorištava propusnost i resurs za obradu što uzrokuje nestabilnost hosta, odnosno pad cjelokupnog sustava.



Slika 3.2. Širenje računalnog crva [22]

Osim štetnih dijelova, crv može sadržavati i korisni teret koji predstavlja dijelove koda napisane da utječu na računalo krađom podataka, brisanjem datoteka ili stvaranjem bota koji može, ali ne mora biti dio botneta. Razlikuju se od virusa jer ne zahtijevaju ljudski utjecaj za širenje s obzirom da imaju neovisnu sposobnost širenja i samoreplikacije [20].

Crv može na različite načine prelaziti s jednog uređaja na drugi: privitkom u elektroničkoj pošti, zlonamjernom poveznicom ili pomoću lokalne mreže (LAN). Jedan od najčešćih načina širenja računalnog crva je putem interneta jer se većina uređaja spaja na internet putem mreže. Takav način omogućuje lako širenje jer se nakon infiltriranja u uređaj, crv može proširiti na druge uređaje preko lokalne mreže. Sljedeći način je širenje putem maila, u elektroničku poruku stavi se zaraženi privitak ili link te se tako crv infiltrira u računalo. Platforme za dijeljenje datoteka su također vrlo čest način širenja jer nema načina da se prepozna sadrži li datoteka koja se preuzima računalnog crva. Pametni telefoni jedan su od najlakših načina prijenosa crva jer se često povezuju na višestruke Wi-Fi mreže što ubrzava njihovo širenje. Prijenosni pogoni lako se zaraze priključivanjem na zaraženo računalo te se dalje prijenose daljnjim spajanjem na ostala računala. Skidanje sadržaja pomoću torrenta vrlo su opasna jer mogu sadržavati računalnog crva s obzirom da većina sadržaja nije zaštićena autorskim pravima. Osim spomenutih, IoT uređaji isto mogu biti jedan od načina zaraze računalnim crvom. U kontroliranom okruženju, istraživači su iskoristili pametnu žarulju kao oružje za širenje računalnog crva na susjedne IoT uređaje [23].

3.4.3. Trojanski konj

Trojanski konj je prema definiciji zlonamjerni program koji se predstavlja kao legitiman, a prilikom preuzimanja i izvršenja ugrađuje zlonamjerne datoteke na računalo. Trojanski konj se često naziva i Trojanac, a kada se izvrši, instalira se virus bez korisnog tereta. Ima mogućnost davanja daljinskog pristupa napadaču koji tada može obavljati zlonamjerne aktivnosti [20].

Trojanac nema mogućnost samoreplikacije i potreban mu je korisnik za preuzimanje poslužiteljske strane aplikacije kako bi radio. Potrebno je implementirati izvršnu datoteku (.exe) i instalirati program kako bi trojanac mogao napasti sustav uređaja. Širi se putem naizgled legitimnih elektroničkih poruka i priloženih datoteka, kao neželjena pošta, kako bi došlo do što više osoba. Nakon što se otvori poruka i preuzme priložena datoteka, trojanski poslužitelj se instalira i automatski pokreće svaki put kada je zaraženi uređaj uključen. Osim širenja putem elektroničke pošte, trojanac može zaraziti uređaj pomoću socijalnog inženjeringa. Socijalni inženjering se koristi na način da se korisnici prisile na preuzimanje zlonamjerne aplikacije. Ona može biti skrivena u banner oglasima, skočnim oglasima ili vezama na web stranicama. Računalo koje sadrži trojanac može ga prenijeti na druga računala. Haker pretvara uređaj u takozvano zombi računalo što znači da ima mogućnost daljinskog upravljanja bez da korisnik to zna. Takva računala koriste se za nastavak širenja zlonamjernog softvera na mreži uređaja koja se zove botnet. Na primjer, korisnik može primiti elektroničku poštu od poznatog pošiljatelja s uključenim privitkom koji izgleda legitimno. Nakon preuzimanja korisnik vjerojatno neće primijetiti da se instalirao trojanac jer računalo može nastaviti raditi bez znakova zaraze. Može ostati neotkriven sve do poduzimanja neke određene radnje kao što su posjet određenoj web stranici ili bankarskoj aplikaciji. Osim računala, trojanac može zaraziti pametne telefone ili tablete putem zlonamjernog softvera. Haker preusmjerava promet na uređaj koji je spojen na WiFi mrežu, a zatim ga koristi za pokretanje napada.

Postoji mnogo vrsta trojanaca koji se koriste za izvođenje raznih radnji i metoda napada. Jedna od vrsta napada je (stručnjacima prepoznatljiv) *Backdoor Trojan.* Omogućuje hakeru daljinsko upravljanje zaraženim računalom i preuzimanje kontrole koristeći „stražnja vrata“. Pomoću toga, haker na računalu može brisati datoteke, ponovno pokretati računalo, krasti podatke ili prenositi zlonamjerni softver. Backdoor Trojan vrlo često se koristi za stvaranje botnet mreže putem takozvanih zombi računala. (Stručnjacima prepoznatljiv) *Banker Trojan* dizajniran je

za ciljanje korisničkih bankovnih računa i financijskih informacija. Pokušava ukrasti podatke o kreditnim i debitnim karticama, sustavima elektroničkog plaćanja i sustavima internet bankarstva. DDoS (eng. *Distributed Denial-of-Service*) trojanac izvodi napade na način da preoptereti mrežu prometom. Pošalje više zahtjeva s računala s ciljem preplavljivanja određene web adrese i izaziva uskraćivanje usluge. (Stručnjacima poznat) *Downloader Trojan* cilja računala koja su već zaražena te preuzima i instalira još više zlonamjernih programa na njega. (Stručnjacima prepoznatljiv) *Exploit Trojan* sadrži kod koji iskorištava ranjivosti unutar aplikacije ili računalnog sustava. Lažni antivirus Trojan oponaša radnje nekog legitimnog antivirusnog programa. Dizajniran je za otkrivanje i otklanjanje prijetnji poput običnog antivirusnog programa te zatim iznuđuje novac od korisnika za uklanjanje prijetnji koje zapravo ne postoje. Trojanac za krađu igara dizajniran je za krađu podataka o korisničkim računima igrača online igara. Trojanac za razmjenu izravnih poruka dizajniran je za krađu korisničkih podataka o prijavi (korisničko ime i lozinka) te cilja poznate platforme za razmjenu poruka. (Stručnjacima poznat) *Infostealer Trojan* koristi se za instalaciju trojanca i sprječava korisnika otkrivanje zlonamjernog programa. (Stručnjacima poznat) *Mailfinder Trojan* dizajniran je za prikupljanje i krađu adresa elektroničke pošte pohranjenih na računalu. (Stručnjacima poznat) *Ransom Trojan* ima cilj narušavanja performansi računala i blokiranje podataka na uređaju kako im korisnik ne bi mogao pristupiti ili ih koristiti. Nakon toga haker ucjenjuje korisnika ili organizaciju dok ne plate naknadu za otkupninu kako bi otključao zahvaćene podatke ili poništio oštećenje uređaja [24].

3.4.4. Špijunski softver

Špijunski softver (eng. *Spyware)* predstavlja zlonamjerni program koji koristi funkcije u operacijskom sustavu s ciljem špijuniranja aktivnosti korisnika. Osim špijuniranja korisnika, može imati i mogućnost ometanja mrežnih veza na način da se izmjene sigurnosne postavke na zaraženom sustavu. Širi se tako da se pričvrsti na legitimni softver, trojanac ili iskorištavanjem poznatih ranjivosti. Špijunski softver ima mogućnost praćenja načina ponašanja korisnika, navike korištenja interneta i slično [20].

Špijunski softver infiltrira se u uređaj nakon posjeta zlonamjernoj web stranici, nesvjesnim instaliranjem zlonamjerne aplikacije ili otvaranjem privitka datoteke. Nakon što se infiltrira počne snimati sve podatke, prati web aktivnost, detalje kreditnih ili debitnih kartica, podatke za prijavu ili pritisak na tipke. Zadnji korak je isporučivanje snimljenih podataka osobi koja je infiltrirala špijunski softver na uređaj. Ta osoba podatke može izravno koristiti ili prodati trećoj

strani. Špijunski softver može zahvatiti bilo koji uređaj koji ima pristup internetu (Windows uređaje, Macove, iOS i Android uređaje, tablete itd.). Jedan od najčešćih načina zaraze uređaja je prihvaćanjem upita ili skočnog prozora bez prethodnog čitanja. Špijunski softver se infiltrira u uređaj odmah nakon klika na zaraženu poveznicu. Osim spomenutog, veliku opasnost za uređaje predstavljaju i piratski mediji u koje spadaju filmovi, glazba ili igre. Kreatori zlonamjernog softvera koriste razne trikove da bi zavarali korisnika jer može biti napravljen da izgleda kao da je koristan i legitiman alat.

Špijunski softver je vrlo teško pronaći i prepoznati na uređaju. Radi tajno i prikuplja podatke bez da korisnik to zna. Iako je vrlo težak za prepoznavanje, postoje načini na koje se može utvrditi je li uređaj zaražen. Uređaj može pokazivati manjak prostora na tvrdom disku, često se pojavljuju skočni prozori, preglednik preusmjerava na nepoznate stranice, preglednik više ne pokazuje uobičajenu početnu stranicu i alatnu traku koja nije dodana od strane korisnika te je moguće naići na aplikacije koje sam korisnik nije instalirao [25].

3.4.5. Reklamni softver

Reklamni softver (eng. *advertising supported software*) služi kao alat za stvaranje prihoda oglašivačima na način da automatski generira oglase na zaslonu računala, najčešće u obliku skočnog prozora. Može se pronaći i na tabletima ili pametnim telefonima. Opasnost alata je što može doći u paketu sa zlonamjernim softverom zbog čega može pratiti aktivnost korisnika i ukrasti korisničke podatke [20].

Reklamni softver se najčešće pojavljuje na uređaju korisnika prilikom instalacije besplatnog programa ili aplikacije. Takav način omogućuje zaradu razvojnom programeru, ali znači i da se može preuzeti bez znanja korisnika. Drugi način pojave reklamnog softvera je ako u sustavu postoji ranjivost koja se može iskoristiti za njegovo ubacivanje. Osoba koja je stvorila takvu vrstu softvera zarađuje novac od treće strane plaćanjem po kliku, što bi značilo da svaki put kada korisnik klikne na oglas, osoba bude plaćena. Sljedeći način je da osoba bude plaćena svaki put kada se oglas prikaže korisniku. Osim spomenutog, osoba može biti plaćena po instalaciji što znači da joj se plaća svaki puta kada se softver u paketu instalira na uređaj. Reklamni softver može pratiti povijest pretraživanja i na taj način prikazivati relevantne oglase. Nakon što osoba dobije lokaciju i povijest pretraživanja, može dodatno zaraditi prodajom spomenutih informacija trećim stranama.

Važno je znati razlikovati bezopasan i štetan reklamni softver. U većini slučajeva, predstavlja smetnju, ali u štetnom i zlonamjernom dijelu spektra može predstavljati veliku prijetnju računalnoj sigurnosti. Postoji legitimni reklamni softver koji omogućuje pristanak na oglase i promociju softvera. Na taj način nadoknađuju se troškovi programera kako bi korisnici mogli preuzeti softver besplatno. S druge strane, ne sadrži svako preuzimanje aplikacije pristanak korisnika. Potencijalno neželjene aplikacije (PUA) sadrže programe za koje korisnik nije dao pristanak za instalaciju na uređaj. Legalni varljivi adware PUA može otežati isključivanje instaliranja bezopasnog softvera treće strane. Spomenuti način je zakonit ako osoba koja je kreirala nije svjesno uključila zlonamjerne oglase ili softver. Legalni zlonamjerni adware PUA konstantno izbacuje korisniku oglase. Pretjerani oglasi najčešće se nalaze u reklamnom softveru ili paketu softvera putem alatne trake web preglednika. Ilegalni zlonamjerni adware PUA ostvaruje profit od zlonamjernih trećih strana koje žele distribuirati zlonamjerni softver na uređaje. Zlonamjerni softver može biti maskiran unutar samog reklamnog softvera ili web stranice koju oglašava. Kreatori i distributeri svjesno šire prijetnju i koriste zlouporabne metode kako bi je ostvarili.

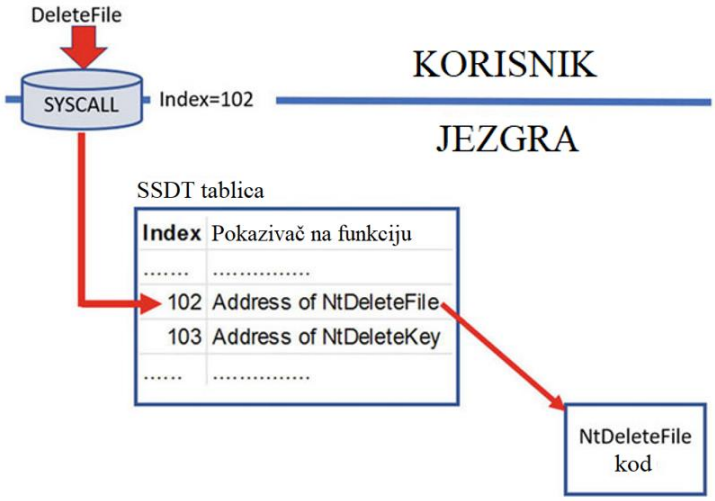
Postoje mnogi znakovi koji mogu ukazivati na zaraženost reklamnim softverom. Najčešći znak je promjena početne stranice web preglednika. Osim spomenutog, ostali znakovi su da se posjećene web stranice se ne prikazuju ispravno, konstantno iskaču skočni oglasi, usporava se rad uređaja i smanjuje brzina interneta. Može doći do pojave aplikacija koje sam korisnik nije instalirao te raznih preusmjeravanja na druge web stranice. Ako dođe do zaraze reklamnim softverom, bitno je poduzeti korake kako bi se sustav očistio od aplikacija koje stvaraju problem. Da bi se korisnik zaštitio od reklamnog softvera, potrebno je često ažurirati softver, biti oprezan prilikom internetskih preuzimanja, voditi računa da aktivnosti budu legalne. Osim navedenog, prilikom preuzimanja besplatnih programa ili aplikacija, važno je pročitati odredbe i uvjete te ih preuzimati iz pouzdanih izvora [26].

3.4.6. Root Kit

Root Kit, prema definiciji, predstavlja naprednu tehniku, značajku, funkcionalnost ili tehnologiju koju koristi zlonamjerni softver s ciljem prikrivanja i zaštite korisnog sadržaja, izvršnih datoteka i binarnih datoteka koje je stvorio na računalu korisnika. Stvara se u korisničkom načinu rada i u načinu rada jezgre. Rootkit u korisničkom načinu rada ovisi o stvaranju API poveznica u procesima ubacivanjem koda u te procese. Takav način rada specifičan je za procese u koje se ubacuje kod rootkita. Na primjer, ako se rootkit korisničkog

načina rada umetne u Upravitelj zadataka s ciljem skrivanja procesa zlonamjernog softvera, tamo neće biti moguće pronaći procese zlonamjernog softvera. Međutim, procesi zlonamjernog softvera mogu biti vidljivi putem drugih alata kao što su Process Hacker i Process Explorer s obzirom da rootkit nije ubačen u njih. Primjena rootkita korisničkog načina rada proteže se samo na proces u koji je umetnut. Zbog učinkovitosti, rootkit kod korisničkog načina rada potrebno je ubaciti u svaki proces korisničkog načina rada koji je povezan s prikrivenošću koja se želi postići. Rootkit u načinu rada jezgre zahtijeva instalaciju jezgrenog modula, odnosno pokretačkog programa u jezgru. Takav način rada specifičan je za globalne rootkitove koji rade pomoću upravljačkih programa za način rada jezgre koje instalira rootkit. Utječu na sve alate i procese koji se izvode na sustavu s obzirom da jezgra predstavlja sloj koji koriste svi procesi na sustavu. Stvaranje koda jezgre složen je i težak proces jer je potreban točan programski kod, inače bi moglo doći do pada sustava.

Funkcije jezgre, koje se nalaze u SSDT (eng. *System Service Descriptor Table*), upravljaju dolaznim syscall-om iz korisničkog prostora i nazivaju se uslugama. Mnoge servisne funkcije definirane su i čuvane u jezgri. Svaka od njih se definira prema funkciji i služi različitim vrstama zahtjeva korisničkog prostora. Na primjer, neki od njih služe za stvaranje i brisanje datoteka, stvaranje, mijenjanje i brisanje unosa u registru, dodjelu memorije i slično. SSDT predstavlja tablicu koja u sebi sadrži pokazivače na servisne funkcije. Svaki pokazivač funkcije usluge ima odgovarajući indeks u SSDT koji pokazuju na memorijske lokacije u kodu jezgre gdje se nalaze servisne funkcije. Servisne funkcije definirane su u modulima jezgre ntoskrnel.exe(ntkrnlpa.exe) i win32k.ksys. Na slici 3.3. prikazano je da syscall iz korisničkog prostora koristi vrijednost indeksa za prijenos zahtjeva u način rada jezgre i time poziva ispravnu servisnu funkciju u SSDT-u [27].



Slika 3.3. Pozivanje ispravne funkcije u SSDT-u pomoću syscall-a [27]

Rootkit se ne može širiti sam te ovisi o tajnim metodama koje služe za zarazu računala. Kada korisnici daju dopuštenje instalacijskim programima rootkita, oni se instaliraju i skrivaju dok ne budu aktivirani. Rootkit sadrži zlonamjerne alate kao što su alat za krađu bankovnih podataka, lozinki, (stručnjacima prepoznatljiv) keylogger, antivirusne deaktivatore i robote za distribuirane napade uskraćivanja usluge. Na računalo se instalira pomoću phishing elektroničkih poruka, zlonamjernih PDF ili Microsoft Word dokumenata i datoteka, povezivanjem s već zaraženim diskovima ili preuzimanjem s rizičnih web stranica. Rootkit može uzrokovati infekciju zlonamjernim softverom koji može sadržavati viruse, trojance i slično. Nakon infekcije može doći do brisanja datoteka i krađe osjetljivih podataka, a da sam korisnik toga nije svjestan. Osim navedenog, često dolazi do promjene konfiguracije sustava čime se može uspostaviti skriveni način rada koji otežava otkrivanje zaraze i omogućava napadaču trajni pristup. Neki od najčešćih simptome zaraze rootkitom je prestanak rada antimalware-a, postavke sustava mijenjaju se same od sebe, problemi s izvedbom što znači da je uređaj postao jako spor te blokade pristupa računalu [28].

3.4.7. Botovi

Bot predstavlja skraćenicu za robot i predstavlja softverski program koji obavlja automatizirane, ponavljajuće i unaprijed definirane zadatke. Obavlja mnogo korisnih funkcija kao što su korisnička služba i indeksiranje tražilica, ali mogu doći i u obliku zlonamjernog softvera za stjecanje potpune kontrole nad uređajem. Botovi mogu biti računalni i internetski te predstavljaju digitalne alate korištene za dobru i lošu namjeru. Botovi koji su dobri obavljaju korisne zadatke za korisnika, dok loši botovi često nose velik rizik i koriste se za hakiranje,

slanje neželjene pošte, špijuniranje korisnika i slično. Polovicu cjelokupnog internetskog prometa čine računalni botovi koji obavljaju razne funkcije. Individualni korisnici i organizacije koriste botove za zamjenu ponavljajućih zadataka koji su relativno jednostavni i izvode se puno brže u usporedbi s ljudskim aktivnostima.

Iako je većina botova korisna, postoje i oni koji su vrlo loši i mogu ozbiljno naštetiti korisnicima. Botovi zlonamjernog softvera i internetski botovi mogu se programirati da provale u korisničke račune i ukradu podatke, mogu skenirati internet u potrazi za kontaktnim informacijama, mogu slati neželjenu poštu i slično. Kako bi se sakrio izvor napada, napadači mogu distribuirati loše botove u botnet. Botnet, prema definiciji, predstavlja niz uređaja koji su povezani na internet od kojih svaki pokreće jednog ili više botova bez znanja korisnika uređaja koji je napadnut. Najčešći način zaraze preko botova su preuzimanja. Zlonamjerni softver najčešće se isporučuje u formatu za preuzimanje putem društvenih medija ili poruka e-pošte klikom na vezu koja je u obliku slike ili videa. Osim preuzimanja, zlonamjerni bot se može pojaviti kao upozorenje da će se računalo zaraziti virusom ako se ne klikne na podijeljenu poveznicu. Nakon klika na poveznicu računalo pokupi virus. Zlonamjerni botovi često prođu neopaženo jer se skrivaju unutar računala i često imaju procese i datoteke koje su slične sistemskim procesima i datotekama. Jedan od najpoznatijih primjera botova su spambotovi koji prikupljaju adrese elektroničke pošte sa stranica kontakata ili knjiga gostiju. Zlonamjerni chatterbotovi se najčešće pojavljuju u aplikacijama za upoznavanje. Pretvaraju se da su osobe i oponašaju ih pa stoga korisnici često ne shvaćaju da razgovaraju sa zlonamjernim programom čiji je cilj dobiti osobne podatke koje će kasnije prodati ili iskoristiti za vlastitu korist. Botovi za dijeljenje datoteka uzimaju korisnikov upit i odgovaraju na njega navodeći da imaju datoteku dostupnu za preuzimanje na način da podijele poveznicu. Klikom na poveznicu, korisnik ga preuzme i otvori te nesvjesno zarazi svoje računalo. DoS ili DDoS botovi koriste se u velikom broju kako bi preopteretili poslužitelja i spriječili rad usluge. Botovi za skeniranje ranjivosti koriste se za skeniranje velikog broja stranica nakon čega izvještavaju osobu koja zatim prodaje informacije ili ih sama koristi za hakiranje web stranica. Botovi za praćenje prometa koriste se za opterećenje poslužitelja pošte ili krađu podataka. Osim spomenutih zlonamjernih botova, postoje i korisni botovi koji mogu korisniku olakšati neke svakodnevne radnje. Društveni botovi rade na platformama društvenih mreža i koriste se za automatsko generiranje poruka, mogu imati djelovanje kao pratitelj nekog korisnika i kao lažni račun za stjecanje sljedbenika. Botovi za kupovinu služe za pronalazak najboljih cijena za proizvode koje korisnik traži. Botovi za praćenje koriste se za praćenje ispravnosti web stranica.

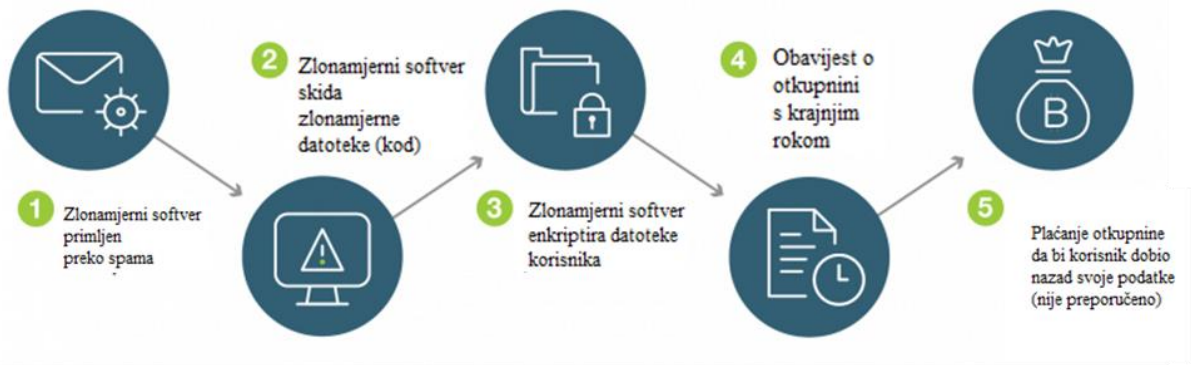
Transakcijski botovi koriste se za dovršavanje transakcija u ime korisnika. Botovi za preuzimanje služe za automatsko preuzimanje mobilni aplikacija ili softvera kako bi im se povećao broj preuzimanja trgovini aplikacija. Mogu se koristiti i za napad stranica za preuzimanje na način da stvaraju lažna preuzimanja kao dio DoS-a.

Najčešći znakovi zaraze botnetom konstantno rušenje i usporene performanse računala, aplikacije ne rade na uobičajen način, internet postaje izuzetno spor, a preglednik sadrži komponente koje korisnik nije preuzeo, postavke sustava su se promijenile i korisnik ih ne može nikako promijeniti, pojavljuju se skočni prozori i reklame bez korištenja preglednika i kontaktima se šalju poruke elektroničke pošte koje korisnik nije poslao. Potrebno je poduzeti nekoliko koraka kako bi se zaštitili podaci prilikom napada botova [29]:

1. Potrebno je odspojiti računalo s mreže
2. Važni podaci trebaju se premjestiti na neko drugo računalo ili tvrdi disk
3. Potrebno je vratiti uređaj na tvorničke postavke
4. Uređaj se treba očistiti pomoću raznih sigurnosnih alata

3.4.8. Ransomware

Ransomware predstavlja program koji inficira uređaj ili mrežu i preuzima kontrolu nad sustavom dok traži otkupninu od korisnika sustava/mreže. Na slici 3.4. vidi se da program enkriptira datoteke na zaraženom sustavu i zaključava sustav zbog čega postaje nedostupan korisnicima. Na kraju prikazuje poruke pomoću kojih želi prisiliti korisnike da plate određenu svotu kako bi ponovno imali pristup svojim sustavima [20].



Slika 3.4. Način rada ransomware-a [30]

Postoje 3 vrste ransomware-a: scareware, ransomware za zaključavanje zaslona i ransomware za enkripciju. Scareware je softver koji predstavlja malo više od zlonamjernog

oglašavanja. Korisnik može vidjeti skočni prozor koji ga obavještava da je otkriven zlonamjerni softver i preusmjerava na web-mjesto ili savjetuje da izvrši plaćanje kako bi se uklonila prijetnja. U većini slučajeva, to je sve što će zlonamjerni softver učiniti, pa može biti nešto više od obične smetnje. Ako uređaj ima takvu vrstu infekcije, vjerojatno postoji još neki zlonamjerni softver kojeg korisnik nije svjestan. Ransomware za zaključavanje zaslona zamrzava uređaj korisnika i često prikazuje poruku kojom poručuje da korisnik mora platiti otkupninu ili da je pod istragom neke nadležne organizacije. Spomenuti način prijetnje značajniji je od scareware-a. U većini slučajeva korisnički podaci su sigurni jer zlonamjerni softver onemogućuje pristup uređaju i pokušava prestrašiti korisnika da izvrši plaćanje. Ransomware za enkripciju predstavlja puno ozbiljniji problem od prethodnih jer je datoteke vrlo teško oporaviti. Jedini način je plaćanjem otkupnine što je vrlo riskantno s obzirom da nije garantirano da će hakeri održati svoju stranu dogovora.

Ransomware ima dvostruku funkciju: šifrira podatke i isporučuje poruke o otkupnini. S obzirom na složenost zlonamjernog softvera i mehanizma za dobivanje pristupa, enkripcija može biti relativno jednostavna ili vrlo složena te može utjecati na jedan uređaj ili cijelu mrežu. Enkripcija predstavlja vrlo koristan alat jer štiti podatke od pristupa i ometanja neovlaštenih osoba. Idealan sustav enkriptira podatke koji se šalju ili pohranjuju, dok ih prijemni uređaj dekriptira, a da korisnik toga nije svjestan. To se oslanja na kriptografske ključeve koji upućuju kako se informacije enkriptiraju i dekriptiraju. Isti ključ se može koristiti za enkripciju i dekripciju te je neophodan za pristup informacijama. Najveći problem kod Ransomware napada je što žrtva nema pristup ključu za dekripciju zbog čega je podatke vrlo teško ili nemoguće vratiti. Nakon što se podaci zaključaju, ransomware kontaktira korisnika, najčešće u obliku skočnog prozora na uređaju, i zahtjeva otkupninu kako bi ih vratio [31].

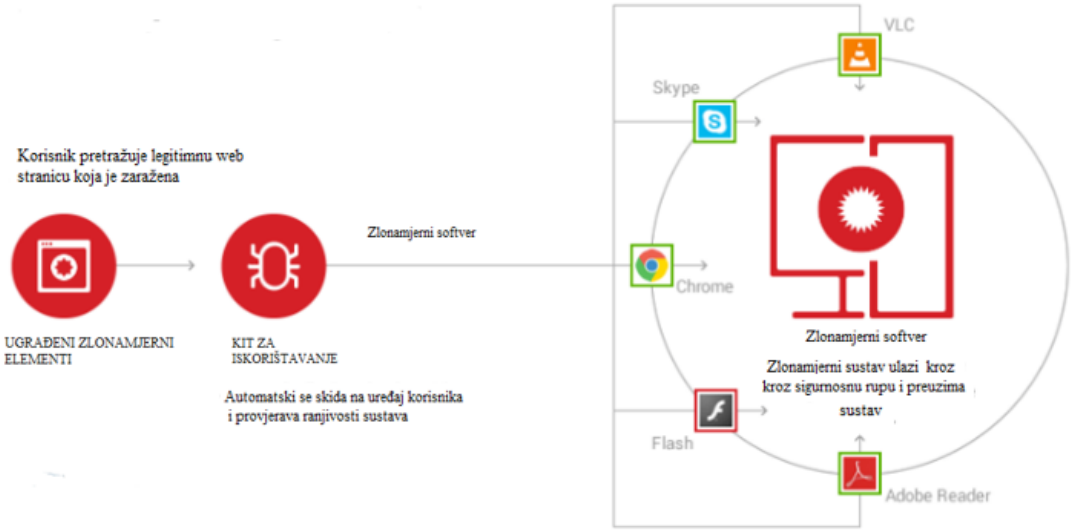
Postoji nekoliko znakova koji mogu ukazivati na zarazu računala ransomware-om. Jedan njih je da se rad uređaja ili mreže naglo usporava. Dolazi do neovlaštene promjene imena i lokacije datoteka te izdvajanja podataka. Korisnik ne prepoznaje enkripciju datoteke i može doći do pojave poruke na početnom zaslonu koja ukazuje na napad [32]. Prema [33] potrebno je poduzeti navedene radnje kako bi uređaj bio zaštićen od ransomware-a:

1. Važno je izbjegavati otvaranje neprovjerenih poruka elektroničke pošte i poveznica
2. Potrebno je izraditi sigurnosne kopije važnih datoteka na više različitih medija
3. Potrebno je redovito nadograđivati softver, programe i aplikacije za zaštitu od ranjivosti

4. Važno je provoditi načelo najmanje privilegije za sprječavanje korisnika da pokrene određene programe koji mogu koristiti razne verzije ransomware-a
5. Potrebno je ograničiti pristup dijeljenim ili mrežnim pogonima i isključiti dijeljenje datoteka što će smanjiti rizik od širenja infekcije ransomware-om na druge uređaje

3.5. Usputna preuzimanja

Usputna preuzimanja (eng. *drive-by downloads*) predstavljaju vrstu napada koji se instaliraju na uređaj bez korisnikovog dopuštenja. Korisnik ne mora kliknuti na preuzimanje ili otvoriti zlonamjerni privitak elektroničke pošte da bi se uređaj zarazio. Usputna preuzimanja uključuju još i nenamjerna preuzimanja bilo kojih datoteka ili softverskih paketa na uređaj. Spomenuta vrsta napada uzrokuje širenje prijetnji čak i sa legitimnih stranica. Postoje dvije vrste napada pomoću usputnih preuzimanja, a to su nezlonamjerni potencijalno neželjeni programi i aplikacije (PUP/PUA) i napadi koji sadrže veliku količinu zlonamjernog softvera (eng. *Malware-loaded attacks*). PUP programi su u većini slučajeva sigurni, a u najgorem slučaju predstavljaju adware. Slika 3.5. prikazuje da usputna preuzimanja mogu iskoristiti aplikacije, operacijski sustav ili web-preglednik koji ima potencijalne sigurnosne nedostatke zbog neuspjelih ažuriranja ili nedostatka ažuriranja i inficirati uređaj.



Slika 3.5. Infekcija sustava pomoću usputnih preuzimanja [34]

Spomenuta vrsta napada se od ostalih razlikuje jer se ne oslanja na to da će korisnik učiniti potencijalno lošu radnju kako bi aktivno omogućio napad. Usputna preuzimanja osmišljena su kako bi hakeri preuzeli kontrolu nad uređajem korisnika, što znači da žele izgraditi botnet,

zaraziti druge uređaje i slično. Osim toga mogu špijunirati aktivnosti korisnika kako bi ukrali osobne i financijske podatke te kako bi uništili i onemogućili korištenje uređaja. Glavni načini zaraze usputnim preuzimanjima mogu biti ovlaštena preuzimanja bez poznavanja svih implikacija i potpuno neovlaštena preuzimanja bez ikakve obavijesti. S ovlaštenim preuzimanjima bez poznavanja svih implikacija poduzima se radnja koja vodi do infekcije, to može biti klik na poveznicu na varljivom lažnom sigurnosnom upozorenju ili preuzimanje trojanca. S potpuno neovlaštenim preuzimanjima bez ikakve obavijesti korisnik može posjetiti stranicu i zaraziti se bez ikakve radnje. Takva preuzimanja mogu se nalaziti bilo gdje uključujući i legitimne stranice. Ovlaštena usputna preuzimanja su pojednostavljena i moguće ih je uočiti prije napada. Haker isporučuje zlonamjerni softver pomoću vektora (online poruka, oglasa ili legitimnih preuzimanja). Na primjer, moguće je dobiti vezu poslanu elektroničkom poštom ili objavom na društvenim medijima koja je maskirana tako da izgleda kao da je poslana iz pouzdanog izvora. Korisnik komunicira s vektorom te klikom na zaraženi link preuzima se zlonamjerni softver koji se instalira na uređaj. Nakon toga haker uspješno ulazi u uređaj korisnika i preuzima kontrolu nad podacima. Neovlaštena preuzimanja bez znanja korisnika funkcionira vrlo jednostavno i sastoji se od nekoliko faza. U prvoj fazi haker kompromitira web stranicu i na nju stavlja zlonamjernu komponentu. Druga faza sastoji se od aktivacije komponente, nakon što korisnik posjeti kompromitiranu web stranicu, koja pronalazi sigurnosne propuste uređaja. U trećoj fazi komponenta preuzima zlonamjerni softver na uređaj te ga inficira. U završnoj fazi zlonamjerni softver dopušta hakeru da ometa, kontrolira i krade uređaj korisnika. Kako bi uređaj bio zaštićen od usputnih preuzimanja potrebno je često ažurirati sve komponente web stranica (teme, dodatke, dodatke ili bilo koju drugu infrastrukturu) jer svako ažuriranje sadrži nove sigurnosne popravke kako bi se spriječio sigurnosni napad. Važno je ukloniti sve zastarjele ili nepodržane komponente web stranice jer bez sigurnosnih zakrpa stari softver se može lako proučiti i iskoristiti za prevare. Potrebno je koristiti jake lozinke i korisnička imena za administratorske račune. Za još veću sigurnost najbolje je koristiti generator zaporki zajedno s upraviteljem zaporki. Važno je instalirati zaštitni softver za sigurnost web stranica. Zaštitni softver će pomoći u praćenju zlonamjernih promjena pozadinskog koda lokacije web stranice. Na kraju potrebno je razmotriti utjecaj upotrebe oglasa na korisnike. Oglasi su jedan od najčešćih alata za povećanje preuzimanja pa je potrebno biti siguran da korisnici ne dobivaju preporučene sumnjive oglase [35].

3.6. Napadi uskraćivanjem resursa

Napadi uskraćivanjem resursa (eng. *Denial of Service*) ili DoS napadi predstavljaju vrstu napada namijenjenu gašenju uređaja ili mreže na način da ga učini nedostupnim korisnicima kojima je namijenjen. Spomenuta radnja postiže se tako da se meta preplavi prometom ili slanjem informacija koje pokreću rušenje. U oba slučaja, DoS napadi uskraćuju korisnicima očekivane usluge i resurse. Najčešće žrtve DoS napada su web poslužitelji organizacija visokog profila (bankarske, trgovačke i medijske tvrtke ili vladine i trgovačke organizacije). DoS napadi najčešće ne rezultiraju krađom ili gubitkom značajnih informacija i drugih sredstava, ali žrtvu mogu koštati puno vremena i novca. Suvremene sigurnosne tehnologije razvile su mehanizme za obranu od većine oblika DoS napada, ali zbog jedinstvenih karakteristika i dalje predstavlja veliku prijetnju [36].

U većini slučajeva, odgovaranje na mrežni zahtjev zahtijeva više procesorske snage od slanja. Prilikom obrade HTTP (eng. *Hypertext Transfer Protocol*) zahtjeva, web poslužitelj mora raščlaniti zahtjev, pokrenuti upite baze podataka, zapisati podatke u zapisnike i konstruirati HTML koji treba vratiti. Potrebno je da korisnički agent generira zahtjev koji se sastoji od tri informacije: HTTP glagol, IP adresu na koju se šalje i URL. Na taj način hakeri da zatrpavaju poslužitelje mrežnim zahtjevima tako da ne mogu odgovoriti legitimnim korisnicima. S obzirom na razvitak tehnologije, hakeri su otkrili načine za pokretanje napada uskraćivanjem usluge na svakoj razini mrežnog skupa, a ne samo preko HTTP-a.

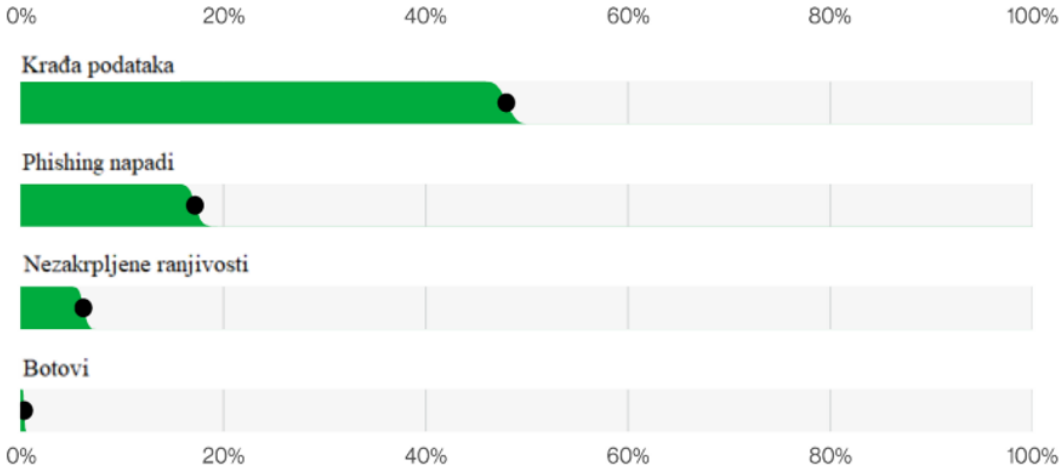
ICMP protokol (eng. *Internet Control Message Protocol*) služi za provjeru je li mrežna adresa online. Koriste ga poslužitelji, usmjerivači i alati linija naredbe. Šalje se zahtjev na IP adresu, a ako je poslužitelj koji odgovara na mreži, poslat će potvrdu da je na mreži. ICMP protokol je najjednostavniji među internetskim protokolima te je najčešće sredstvo za zlonamjerne radnje. Dolazi do pojavljivanja velikog broja pingova koji pokušavaju preplaviti poslužitelj slanjem beskrajnog niza ICMP zahtjeva, a pokreću se s nekoliko linija koda. Nešto sofisticiraniji napad je (stručnjacima prepoznatljiv) *ping of death* napad koji šalje oštećene ICMP pakete u pokušaju da sruši poslužitelj. Spomenuta vrsta napada uglavnom se koristi kod starijeg softvera koji ne radi ispravno provjeru granica u dolaznim ICMP paketima. Većina napada temeljenih na ICMP-u moguće je spriječiti modernim mrežnim sučeljima, pa su se napadači pomaknuli ka mrežnom stogu na TCP (eng. *Transmission Control Protocol*) koji podupire većinu internetske komunikacije. TCP razgovor započinje slanjem SYN poruke poslužitelju, od kojeg se očekuje da odgovori SYN-ACK (sinkroniziraj potvrdu) odgovorom.

Klijent bi tada trebao dovršiti rukovanje slanjem posljednje ACK poruke poslužitelju. Kada se poslužitelj preplavi SYN porukama bez dovršenog rukovanja TCP-om, alati za hakiranje ostavljaju poslužitelj s velikim brojem poluotvorenih veza. Nakon što se legitimni klijent pokuša povezati, poslužitelj odbija vezu. Ako se DoS napad pokrene s jedne IP adrese, moguće je promet s te IP adrese staviti na crnu listu i zaustaviti napad. Moderni DoS napadi se obično pokreću s botneta te ih napadač može kontrolirati. Budući da se danas mnoge vrste pametnih uređaja s mogućnošću spajanja na internet (hladnjaci, automobili, zvona na vratima) imaju veliku sklonost sigurnosnim propustima pa postoji mnogo mjesta na kojima se botovi mogu sakriti [37].

3.7. Statistika sigurnosnih prijetnji

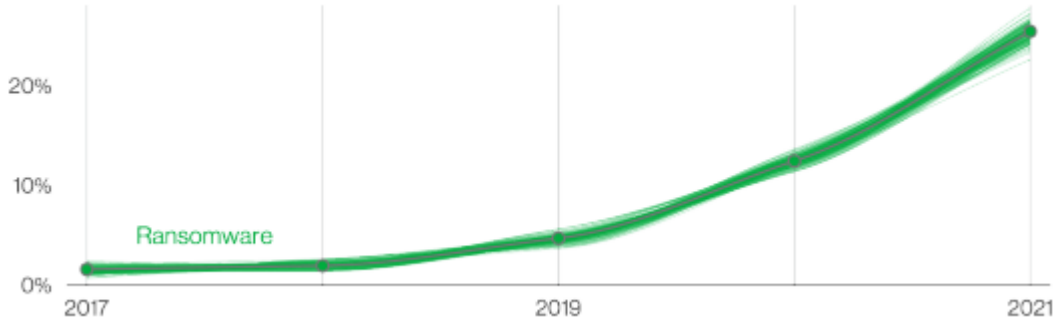
U prethodnim poglavljima bile su opisane razne prijetnje koje mogu ugroziti sigurnost uređaja, od phishing napada do DoS napada. U sljedećim poglavljima bit će prikazane prijetnje u praksi, odnosno statistika njihove učestalosti i koliki je utjecaj pojedinih parametara i komponenti na sigurnost uređaja.

Prema [38], u 2021. godini, najčešće prijetnje koje ugrožavaju uređaje su krađa podataka, phishing napadi, nezakrpljene ranjivosti i botovi. Slika 3.6. prikazuje postotak prijetnji koje napadaju uređaje. Najveći postotak napada događa se zbog krađe podataka te čine oko 50% ukupnih napada, zatim slijede phishing napadi koji čine nešto manje od 20% ukupnih napada, slijede ih nezakrpljene ranjivosti s nešto manje od 15% ukupnih napada, zatim botovi koji čine manje od 5% napada i na kraju nešto više od 10% ostalih vrsta napada.



Slika 3.6. Najčešće prijetnje krajnjim uređajima [38]

2021. godine dolazi i do porasta napada zlonamjernim softverom, specifičnije ransomware-om. Slika 3.7. prikazuje da je porast čak 13% u odnosu na prošlu godinu što mu daje ukupan porast od 25%. Ransomware predstavlja model monetizacije pristupa organizacije, a blokiranje četiri gore spomenutih napada pomaže u njegovom blokiranju.



Slika 3.7. Krivulja ransomware napada [38]

Najčešći razlog zbog kojeg dolazi do napada je zbog ljudske pogreške te ona čini više od 80% ukupnih razloga napada. Najčešće je to korištenje ukradenih podataka, phishing napadi, zlouporaba ili jednostavno slučajnom pogreškom. Nadalje bitno je napomenuti da ljudska pogreška i dalje igra jako veliku ulogu u incidentima i napadima [38].

4. INTEGRIRANA SIGURNOSNA RJEŠENJA ZA ZAŠTITU KRAJNJIH UREĐAJA

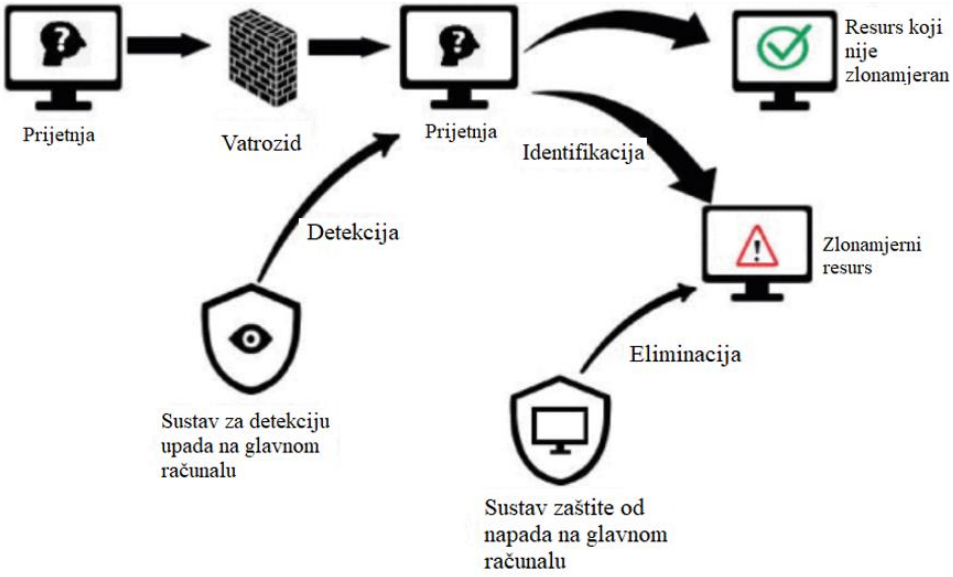
Sigurnost krajnjih krajnjih uređaja označava osiguravanje zaštite krajnjih uređaja ili ulaznih točaka uređaja krajnjih korisnika od zlonamjernih radnji. Krajnji uređaji mogu biti stolna i prijenosna računala, mobilni uređaji, IoT uređaji i slično. Kako bi se zaštitili od računalnih napada, sigurnosni sustavi krajnjih uređaja štite se na mreži ili u oblaku. Sigurnost krajnjih uređaja razvijena je iz tradicionalnog antivirusnog softvera kako bi se pružila zaštita od sofisticiranog zlonamjernog softvera i rastućih zero day prijetnji. Sigurnost krajnjih uređaja smatra se najvažnijim dijelom računalne sigurnosti i predstavlja jedno od prvih mjesta na kojima organizacije žele osigurati svoje poslovne mreže. S obzirom da se računalne prijetnje sve više razvijaju i šire, dolazi do sve veće potrebe za naprednijim sigurnosnim rješenjima krajnjih uređaja. Današnji sustavi zaštite krajnjih točaka dizajnirani su za brzo otkrivanje, analizu, blokiranje i zaustavljanje napada u tijeku. Kako bi se omogućile navedene radnje, potrebna je suradnja sa drugim sigurnosnim tehnologijama za omogućavanje uvida administratora u napredne prijetnje da bi se ubrzalo otkrivanje i vrijeme odgovora na sanaciju.

Platforma za zaštitu krajnjih uređaja predstavlja značajan dio računalne sigurnosti poduzeća. U današnjem vremenu najvrjednija imovina tvrtke su podaci, a njihov gubitak ili gubitak pristupa podacima može cijelo poslovanje dovesti u opasnost od raspada ili čak i bankrota. Tvrtke su se također morale boriti ne samo s rastućim brojem krajnjih uređaja, već i s porastom broja tipova krajnjih uređaja. Sve navedeno otežava sigurnost krajnjih uređaja poduzeća koji su složeni za rad na daljinu te pomoću BYOD (eng. *Bring Your Own Device)* pravila čine perimetarsku sigurnost sve nedostatnijom i stvaraju ranjivosti. Prijetnje postaju sve složenije jer hakeri uvijek smišljaju nove načine kako bi pristupili povjerljivim podacima i ukrali vrijedne informacije [39].

4.1. EPP

EPP (eng. *endpoint protection platform*) je prema definiciji platforma koja se sastoji od različitih sigurnosnih alata kao što su antivirusni programi, anti-malware, enkripcija podataka, osobni vatrozidi i prevencija upada. EPP predstavlja tradicionalni softver koji se temelji na potpisu. Radi na način da prati podudara li se postojeći potpis prijetnji koje su već pohranjene u bazi podataka te tako utvrđuje je li prijetnja štetna. Slika 4.1. prikazuje tretiranje prijetnje pomoću EPP-a. Nakon što prijetnja počne prodirati kroz vatrozid, sustav za detekciju upada

na glavno računalo (HIDS) otkriva prijetnju i utvrđuje je li zlonamjerna ili ne. Oni koji su zlonamjerni bit će ublaženi sustavom zaštite od upada na glavno računalo (HIPS).



Slika 4.1. Način tretiranja prijetnje pomoću EPP-a [40]

Detekcija je najznačajniji dio krajnje točke. EPP ima potpunu funkciju identifikacije potpisa. Postoje velike količine baze podataka s potpisom virusa koje se mogu koristiti za identifikaciju već poznatih virusa. Postupak uparivanja temelji se na različitim algoritmima. Svaka tvrtka koja provodi zaštitu ima svoje algoritme pomoću kojih može otkriti prijetnje. Mehanizam koji koristi većina EPP-a je detekcija upada. Detekcija upada predstavlja proces praćenja događaja koji se odvijaju u računalnom sustavu ili mreži i analiziranja u potrazi za znakovima upada. Detekcija upada pomaže korisnicima u obrani od napadača i dovršava proceduru detekcije upada. Sustav zaštite od upada na glavnom računalu prati i prikuplja karakteristike korisnika koji sadrže osjetljive informacije i poslužitelje koji pokreću javne usluge i sumnjive aktivnosti. Kako bi organizacije zadržale sigurnost svog sustava, moraju eliminirati mogućnost bilo kakvog vanjskog upada putem krajnjih točaka. Cilj funkcije zaštite je eliminirati već postojeći virus u sustavu koji može uzrokovati značajnu devastaciju sustava jer ako EPP sustav ne poduzme ništa, virusi će zaraziti cijeli sustav. Nudi se rješenje za ispravljanje pogrešaka gdje EPP koristi drugi algoritam za sustav zaštite od upada na glavno računalo koji radi zajedno sa sustavom za detekciju upada na glavnom računalu. Osim mnogo prednosti, EPP ima i nekih nedostataka kada se suoči s naprednijim metodama napada. Ponekad se potpisi virusa ne mogu usporediti na vrijeme jer virusi vrlo brzo mutiraju, ali najznačajnija mana EPP-a je to što ne može obraniti unutarnje prijetnje. Neke od ostalih slabosti EPP-a su da odgovarajući potpis zahtijeva previše resursa, udio napada bez datoteka je u porastu, mnoge funkcije zahtijevaju internet te unutarnje prijetnje mogu izazvati veću štetu nego vanjske prijetnje [40].

4.2. EDR

EDR (eng. *endpoint detection and response*) predstavlja način otkrivanja i odgovarajućeg reagiranja na unutarnje prijetnje pomoću svojih specifičnih funkcija kao što su kontinuirani nadzor, sanacija i uklanjanje smetnji krajnjoj točki. EDR je napredni softver za pozitivnu zaštitu krajnje točke. Jedna od bitnijih značajki EDR-a su obavještajni podaci o prijetnjama koje mogu omogućiti otkrivanje anomalija i upozorenje te sanaciju interne mreže koja je zaražena. Osim navedenog, kako bi se mogle predvidjeti i izbjeći prijetnje, može se koristiti strojno učenje.

Jedna od značajki EDR-a su obavještajni podaci o prijetnjama koji predstavljaju organizirane, analizirane i pročišćene informacije o potencijalnim ili trenutačnim napadima koji prijete organizaciji. EDR predstavlja zaštitni softver s funkcijom obavještavanja o prijetnjama koja omogućuje upozoravanje poduzeća na potencijalne rizike i prijetnje te pruža informacije o prijetnji koje prikuplja poslužitelj EDR-a. Takva vrsta obavještajnih podataka olakšat će uklanjanje unutarnje prijetnje analizom informacija i podataka o unutarnjim prijetnjama koje su se dogodile u prošlosti umjesto predviđanja latentnog rizika. Pomoću kontinuiranog praćenja moguće je otkriti abnormalno ponašanje krajnje točke i tako onemogućiti širenje prijetnje. Ako je jedna krajnja točka zaražena, EDR će odmah otkriti neuobičajenu aktivnost te krajnje točke i odmah je izolirati. Oni mogu dinamički nadzirati krajnje točke i osigurati CPU zaštitu koja može obraniti jezgru poslužitelja. Snažni EDR alati omogućuju jednostavan pristup podacima te im pružaju neposrednu vidljivost bilo kojeg područja organizacije. Nakon sanacije i čišćenja krajnjih točaka prestaje eskalacija virusa. Sustav može izgledati sigurno i čisto, ali bilo koji ostatak može generirati novi virus. Prisutnost uznapredovalog virusa može se širiti na drugi dio i tako na brz način zaraziti internu mrežu. EDR može skenirati sve interne mreže kako bi garantirao da nema ostataka virusa te popraviti štetu koju su uzrokovali kako bi se održala sigurnost unutarnjeg sustava. Promatranje bez smetnji predstavlja jednu od značajki EDR-a. EDR se može izvršiti samo u jezgri mreže sa svojom komponentom za otkrivanje krajnje točke. Mrežni upravitelj može instalirati EDR na poslužitelj tvrtke što će zaštititi cijelu unutarnju mrežu organizacije. Kako bi se otkrile nepoznate prijetnje, koristi se strojno učenje. Strojno učenje predstavlja prediktivni model koji koristi sofisticirane analitičke tehnike kako bi računalima dao mogućnost učenja s podacima te kako bi razumjeli karakteristike zlonamjernog softvera i predvidjeli vjerojatnost zlonamjernog softvera iz nepoznatih aplikacija. Takav način im omogućuje da blokiraju dosad neviđene napade s visokim stupnjem

sigurnosti. Jedna od najvažnijih značajki EDR-a je to da se može prilagoditi na okruženje organizacije što zahtijeva strojno učenje i sposobnost umjetne inteligencije [40].

4.3. MDM

MDM (eng. *Mobile Device Management*) je svaki softver koji osigurava, nadzire, upravlja i podržava mobilne uređaje kao što su pametni telefoni, tableti i slično. Cilj MDM-a je optimizirati funkcionalnost i sigurnost mobilne komunikacijske mreže na način da minimizira troškove i zastoje. Uređajima upravljaju administratori koji pokreću pozadinsku MDM platformu koja omogućuje daljinsko upravljanje funkcijama uređaja. Na uređaj se instalira aplikacija ili softver za prekrivanje kako bi se omogućila funkcionalnost MDM-a i integrirala s pozadinskim uslugama organizacijske mreže. U pozadinske usluge ulaze pristup informacijama, prijenos podataka, zajedničko korištenje zapisnika uređaja te neke ostale mogućnosti ako su potrebne. MDM smanjuje rizike koji su povezani s obnavljanjem osjetljivih poslovnih zadataka na mobilnim uređajima uključujući BYOD (eng. *Bring Your Own Device*) i pametne telefone koji su u vlasništvu organizacije. MDM je vrlo često sastavni dio EMM-a (eng. *Enterprise Mobility Management*) koji uključuje kolektivni skup alata za zaštitu i upravljanje mobilnim aplikacijama, uređajima koje pruža tvrtka i BYOD uređajima, sadržajem, podacima i pristupom. MDM može ponuditi značajke za upravljanje aplikacijama (MAM), sadržajem (MCM) i sigurnosti (MSM) mobilnih uređaja [41]. Potrebno je sva područja povezati u cjelinu kako bi se zajamčila točna razina sigurne mobilnosti poduzeća.

MAM (eng. *Mobile Application Management*) se usredotočuje na dodjelu resursa, upravljanje i održavanje mobilnih aplikacija na mobilnim uređajima. Glavna svrha mu je automatsko pružanje javnih i interno stvorenih aplikacija krajnjim korisnicima, a uz pomoć unaprijed definiranih zahtjeva moguće je postići kontrolu upotrebe. MAM uključuje mnoge aspekte i funkcionalnosti. Jedna od njih je instalacija aplikacije i instalacija u pozadini preko MDM-a što je često vrlo korisno. Tehnički inženjeri imaju mogućnost definiranja pravila za instalaciju aplikacije tijekom procesa prijave mobilnog uređaja. Kako bi se omogućila instalacija u pozadini, potrebno je automatski instalirati potrebne aplikacije nakon što se novi mobilni uređaj uvede u EMM. Sljedeća funkcionalnost je postojanje korporativne trgovine aplikacija u kojoj se nalaze poslovne aplikacije potrebne mobilnom korisniku. Na taj način, organizacija može ograničiti izbor i upotrebu dopuštenih aplikacija. Često korištene funkcionalnosti su uključene postavke aktivnog sinkroniziranja, upravljanje elektroničkom poštom gdje se potrebne postavke automatski uvode krajnjim korisnicima. Većina organizacija

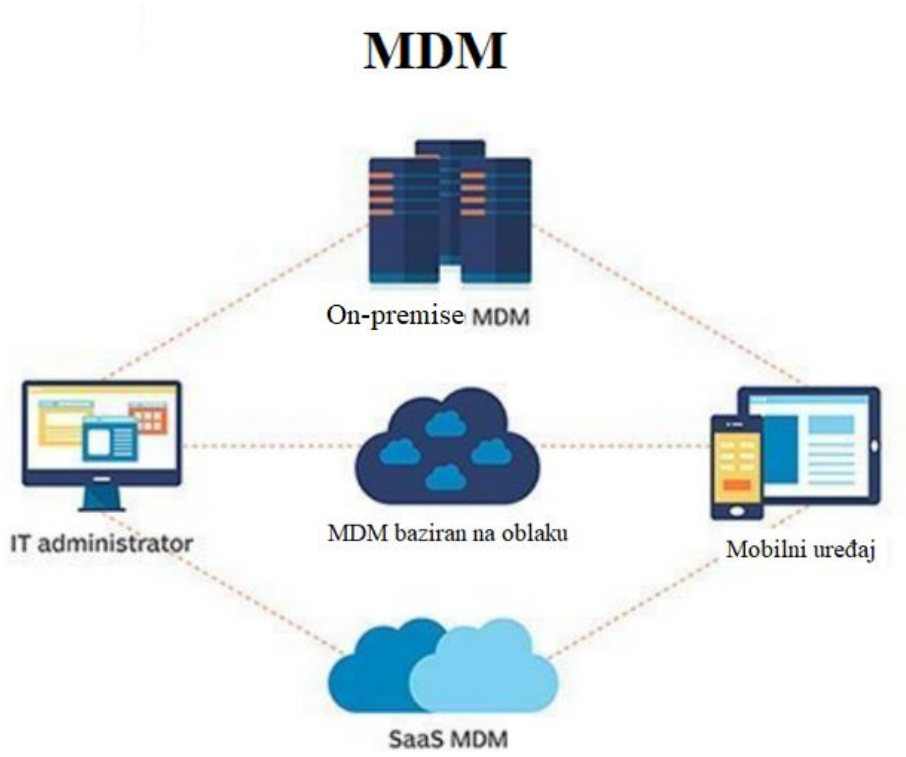
koristi VPN za odobravanje pristupa internim strukturama informacijske tehnologije za mobilne uređaje. Svaka aplikacija se povezuje unutarnjom strukturom te šalje i prima podatke preko šifriranog kanala. Neke od ostalih funkcionalnosti su blokiranje postavke kopiraj/zalijepi, nadzor korištenja aplikacija, pristup radnoj površini na daljinu te upravljanje kontrolom troškova.

MCM (eng. *Mobile Content Management*) predstavlja skup tehnologija koje se fokusiraju na osiguranje, kontrolu i nadzor za siguran pristup podacima organizacije i prijenos podataka na mobilnim uređajima. Cilj MCM-a je pružiti i dijeliti datoteke među različitim mrežnim vezama. To može biti datoteka dijeljenja na lokalnoj mreži organizacije ili spremišta podataka za mobilne korisnike. MCM definira skup pravila za pristup podacima te kontrolira i nadzire neovlašteni pristup. Nadalje, osigurava sigurnost razmjene datoteka između mobilnih krajnjih točaka što znači da MCM pruža mobilnim aplikacijama potrebne podatke za uključivanje lokalne infrastrukture informacijske tehnologije. MCM uključuje neka područja interesa. Jedno od njih je upravljanje podacima koje osigurava učinkovitost i produktivnost organizacije. Kako bi se pružila podrška poslovnim procesima, potrebno je stvaranje, promjena, brisanje i označavanje datoteka kao i planiranje resursa poduzeća. Sljedeće bitno područje interesa je upravljanje osobnim podacima (PIM). Ono označava temeljni dio svakog mobilnog korisnika te služi za pohranu kontakt podataka kupaca, administrativni kalendar i provjeru elektroničke pošte što omogućuje svakom zaposleniku ispunjavanje zadanih zadataka. Osim navedenih važna područja su programska podrška za upravljanje dokumentima, sinkronizacija sadržaja, sigurno pregledavanje na web pregledniku, automatski pristup potrebnim podacima i enkripciju sadržaja elektroničke pošte.

MSM (eng. *Mobile Security Management*) predstavlja pristup upravljanju za zaštitu i provjeru mobilnih korisnika. Provodi politiku registriranih mobilnih uređaja te ima za cilj ograničiti ili omogućiti definiranu razinu postavki kroz cijelo okruženje. MSM ima mnoge značajke i funkcije koje će biti opisane u nastavku. Jedna od značajki MSM je KIOSK način rada koji ima definirana ograničenja i funkcionalnosti. Korisnici ne smiju napustiti postavljen način rada i koristiti svoj uređaj za neke druge svrhe. Samsung KNOX dostupna je samo za uređaje koji podržavaju KNOX (Samsung uređaji). Jamči visoku razinu sigurnosti hardvera i softvera te način spremnika odvaja privatne od poslovnih podataka koji su automatski šifrirani i dostupni samo na tom mjestu. Resetiranje mobilnog uređaja omogućuje tehničkom inženjeru daljinsko resetiranje koje je korisno ako se mobilni uređaj izgubi. Taj način osigurava privatnost i zaštitu podataka. Osim navedenih ostale funkcionalnosti su održavanje zaključavanja mobilnog

uređaja, zabrana instalacije/deinstalacije aplikacije, održavanje certifikata, enkripcija mobilnih uređaja, antivirusna podrška, sprječavanje gubitaka podataka, mobilni VPN i podrška za jedinstvenu prijavu.

Na početku svakog projekta potrebno je definirati vrstu poslužitelja za upravljanje mobilnim uređajima. Slika 4.2. prikazuje da MDM može doći u tri oblika, može se bazirati na oblaku (eng. *cloud*), (stručnjacima prepoznatljivo) *on-premise* i na SaaS-u (eng. *Software as a Service*). On-premise rješenje pruža maksimalnu fleksibilnost lokalnih informacija za povezivanje tehnološke infrastrukture i upravljanje zakrpama MDM poslužitelja, a organizacije mogu same kontrolirati cijelo svoje okruženje. MDM poslužitelji koji se baziraju na oblaku mnogo su povoljniji i lakši za održavanje pa se češće koriste u organizacijama. SaaS je usluga koju nudi većina MDM dobavljača gdje MDM server poslužuje dobavljač i pruža potrebne aplikacije za pokretanje mobilnog uređaja. U rješenju koje se bazira na oblaku, dobavljač softvera brine se o održavanju i ažuriranju. Podaci se pohranjuju na vanjskim poslužiteljima zbog čega je potrebno potpisati ugovor o razini usluge kako bi se izbjegla zloupotreba korištenja podataka [42].



Slika 4.2. Prikaz MDM oblika [43]

4.4. EMM

EMM (eng. *Enterprise Mobility Management*) definira proces osiguravanja podataka organizacije na mobilnim uređajima zaposlenika, koji su u vlasništvu zaposlenika ili tvrtke. EMM rješenja najčešće uključuju široki paket usluga koje su osmišljene za očuvanje sigurnosti intelektualnog vlasništva organizacije i osobnih podataka korisnika (PII) dok se integriraju s drugim IT sustavima i aplikacijama poduzeća za isporuku širokog raspona poslovnih funkcionalnosti. Svaka organizacija ima različita EMM rješenja, neka od njih su usmjerena na osiguranje specifičnih aplikacija, dok druga pokušavaju potpuno osigurati ili zaključati uređaje zaposlenika. EMM se tijekom proteklih nekoliko godina razvio od isključivo fokusa na mobilne uređaje do omogućavanja mobilnosti u širem smislu, uključujući Windows i MacOS prijenosna računala i tablete, upravljanje pristupom i poboljšanje korisničkog iskustva (UX) za mobilne aplikacije i uređaje.

EMM rješenje daje jedinstvenu platformu koja služi za upravljanje mobilnosti poduzeća. Sastoji se od centralizirane konzole koja upravlja mobilnim uređajima, elektroničkom poštom, aplikacijama, sadržajem i pregledavanjem. EMM nudi fleksibilan pristup upravljanja uređajima i siguran radni prostor na uređajima za rješavanje raznih slučaja upotrebe na razini cijele organizacije. U odnosu na ostale sustave, EMM nudi vrlo jednostavno upravljanje i sigurnost. Jedna od prednosti EEM-a je što nudi podršku za velik broj mobilnih i stacionarnih uređaja s kojim može upravljati preko zajedničke platforme. Nudi mogućnost zaštite osobnih i poslovnih podataka na uređajima, zaštitu svih informacija postavljanjem lozinka, pomoću multifaktorske autentifikacije te mogućnošću selektivnog brisanja korporativnih podataka bez utjecaja na osobne podatke zaposlenika. Osigurava ažurnost sigurnosnog softvera tako da se ažurira čim se pojave nove nadogradnje kako bi se spriječili (stručnjacima prepoznatljivi) *zero-day* napadi. Trgovine aplikacija mogu se iskoristiti kako bi se, na siguran način, ubrzala implementacija poslovnih aplikacija i ograničio broj aplikacija koje se mogu instalirati na poslovne uređaje. Usklađenost se osigurava na način da se osigura sigurna infrastruktura za uređaje koji se koriste na daljinu. Osiguravaju se podaci o korištenju, analitici i izvještajima kako bi se otkrili obrasci koji će poboljšati korištenje ili koji će ukazivati na moguća kršenja ili krađu podataka. Na kraju, primjena mehanizma za pravila jedna je od važnih prednosti jer može postavljati, implementirati, modificirati i prilagoditi ih prema radnoj funkciji, odjelu i slično.

EMM se sastoji od mnogo komponenti i tehnologija koje se svakodnevno razvijaju. Neki od elemenata EMM sustava su MDM, MCM i MAM koji su opisani u prethodnom poglavlju. Jedan od elemenata EMM sustava je i MIM (eng. *Mobile Identity Management*). MIM upravlja autentifikacijom i prijavom korisnika, uključuje v fcx, autentifikaciju i jedinstvenu prijavu kako bi se pristup resursima organizacije omogućio samo ovlaštenim i pouzdanim korisnicima. Posljednji element EMM je MEM (eng. Mobile Expense Management) koji prati troškove mobilne komunikacije i organizacijama pruža uvid u korištenje uređaja, potrošene usluge i pravila kao što su naknade za BYOD. MEM prikuplja podatke koji se mogu koristiti za povratne uplate ili revizije korištenja mobilnog uređaja [44].

4.5. UEM

UEM (eng. *Unified Endpoint Management*) predstavljaju vrstu softverske aplikacije koja omogućuje upravljanje svim uređajima organizacije. S obzirom da organizacije koriste veći broj uređaja i aplikacija koje su na razini poduzeća, UEM predstavlja vrlo dobru i učinkovitu metodu za njihovo upravljanje. UEM predstavlja novu generaciju softvera za upravljanje uređajima organizacija, a čiji su prethodnici EEM i MDM. Svaka od spomenutih metoda razvijena je kako bi zadovoljila poslovne potrebe svake organizacije, s obzirom na povećanje upotrebe mobilnih uređaja i pojave novih SaaS metoda, metoda baziranih na oblaku i mobilnih aplikacija. U odnosu na prethodne metode, UEM ima prednost zbog povećanja broja i vrsta uređaja i aplikacija koji može upravljati (Windows i MacOS računala, prijenosni telefoni, IoT uređaji). UEM ima mogućnost upravljanja identitetom i funkcijom pristupa, kao i nizom sigurnosnih značajki i konfiguracija koje se mogu ugraditi u aplikacije klijenata i na uređaje koji nisu u vlasništvu ili pod upravom organizacije.

UEM je nastao kombinacijom EEM-a s postojećim alatima za upravljanje klijentima. Jedan od slučajeva uključuje dodavanje podrške za mobilne uređaje korištenjem MDM protokola. U drugom slučaju, organizacije su povezivale EMM platforme sa svojim platformama za upravljanje klijentima te su na taj način omogućili vidljivost i upravljanje objema. Daljnjim razvojem, operacijski sustav za stolna računala počeo je uključivati mogućnost daljinskog upravljanja koji je koristio vlastite MDM protokole i API-je. Sve navedeno je omogućilo UEM-u uključivanje stolnih računala u niz podržanih uređaja. Nakon toga uslijedio je kaskadni učinak zbog dodavanja više MDM opcija za proširenje vrsta podržanih uređaja, a zatim za dodavanje više aspekata upravljanja klijentima. Najčešći aspekti koji se uključuju su

upravljanje pristupom i identitetom, sigurnosni proizvodi, alati za produktivnost i praćenje performansi.

Ovisno o načinu poslovanja, većina organizacija želi visok stupanj sigurnosti i upravljanja povjerljivim informacijama. S obzirom na druga rješenja UEM ima nekoliko prednosti. UEM nudi upravljanje s više uređaja što je lakše i brže u odnosu na ručno upravljanje. Objedinjuje preglednost svih uređaja koji su bitni za poslovanje, omogućuje daljinsko upravljanje i integriranu automatizaciju. Nudi jednostavnu integraciju koja omogućuje sigurnost i analitiku te (stručnjacima prepoznatljivu) *cloud-native* arhitekturu. Temelji se na modernijim konceptima i idejama za razliku od prethodnih tradicionalnih alata za upravljanje klijentima. Na kraju lakše upravljanje bazama podataka i njihovom pohranom može uključivati poznavanje značenja ACID transakcija [45].

4.6. Usporedba EPP i EDR integriranih sigurnosnih rješenja

EPP sigurnosna rješenja najčešće sprječavaju sigurnosne prijetnje krajnjih točaka kao što su poznati ili nepoznati zlonamjerni softver. EDR sigurnosna rješenja mogu otkriti i odgovoriti na prijetnju koju EPP nije uočio. Najčešće se u praksi kombiniraju oba pristupa ovisno o potrebi organizacije, ali postoje neke razlike između njih koje su prikazane u tablici 4.1.

Tablica 4.1. Usporedba EPP i EDR sigurnosnih rješenja [46]

EPP	**EDR**
Ne zahtjeva aktivni nadzor	Aktivno otkrivanje prijetnji
Sprječava poznate i neke nepoznate prijetnje	Omogućuje trenutni odgovor na incidente koje EPP ne može otkriti
Prevencija pasivnih prijetnji	Pomaže u istraživanju i sprječavanju kršenja koja su se već dogodila
Ne pruža vidljivost aktivnosti na krajnjim točkama	Pomaže sigurnosnom timu skupiti podatke o događajima s krajnjih točki u cijeloj organizaciji
Rješenje prve linije za sprječavanje prijetnji (eng. *First-line threat prevention solution*)	Aktivno korišteni od strane sigurnosnih timova za odgovor na incidente
Pomoću izolacije štiti svaku krajnju točku	Pruža kontekst i podatke za napade koji obuhvaćaju veći broj krajnjih točaka

EPP rješenja otkrivaju potpise i druge pokazatelje upada poznatih prijetnji, dok EDR rješenja daju dodatni sloj obrane uz pomoć alata za traženje prijetnji koje se baziraju na ponašanju krajnje točke (eng. *behaviour-based endpoint threat detection*). Oba alata zahtijevaju aspekte međusobne funkcionalnosti kako bi se smatrali holističkim sigurnosnim rješenjem krajnje točke. EDR zahtijeva aktivnu istragu i analizu od strane sigurnosnih stručnjaka kako bi ispravno odgovorili na prijetnje. Nasuprot tome, EPP softver radi uz minimalno potreban nadzor nakon početne instalacije i konfiguracije. Obje vrste sustava zaštite krajnjih točaka više se nadopunjuju nego zamjenjuju. Moderne organizacije i poduzeća trebaju kombinirati i EDR i EPP u svojoj strategiji računalne sigurnosti kako bi dobili što kvalitetniju zaštitu [46].

4.7. Usporedba MDM, EMM i UEM integriranih sigurnosnih rješenja

Tijekom godina, dobavljači koji upravljaju krajnjim točkama ugrađuju sve veći broj funkcija u svoje alate. MDM sigurnosno rješenje bio je jedan od najranijih alata za upravljanje krajnjih točka. Nakon MDM, na tržištu se pojavljuje EEM koji obuhvaća alate za upravljanje mobilnosti poduzeća. Najnovije sigurnosno rješenje koje se pojavljuje je UEM koji obuhvaća oba prethodnika i još mnogo dodatnih funkcija. Tablica 4.2. prikazuje usporedbu između karakteristika spomenutih sigurnosnih integriranih rješenja.

Tablica 4.2. Usporedba MDM, EMM i UEM sigurnosnih rješenja [47]

MDM	EMM	UEM
Nameće korištenje lozinki	Nameće korištenje višefaktorske autentifikacije	Primjenjuje kontrole EMM-a na uređaje
Instalira aplikacije	Upravlja sinkronizacijom i dijeljenjem datoteka poduzeća	Konfigurira i ažurira računalne i mobilne aplikacije u isto vrijeme
Izvršava udaljeno brisanje uređaja	Upravlja sigurnosnim postavkama internetskog preglednika	Upravlja IoT uređajima i printerima
Konfigurira poslovne profile za BYOD	Primjenjuje pravila uvjetnog pristupa	

MDM sigurnosna rješenja omogućuju visoko segmentirani pristup upravljanju uređajima u kojem su aplikacije, operativni sustavi i osobni podaci odvojeni jedni od drugih. Mnoge

aplikacije u MDM koriste i MAM koji predstavlja alat za upravljanje aplikacijama kao sastavni dio MDM-a. EMM sigurnosna rješenja predstavljaju alat koji kombinira spomenute dvije funkcije te još dodaje dodatne funkcije za što bolje upravljanje sigurnošću. Dodatne funkcije uključuju sinkronizaciju i dijeljenje datoteka poduzeća te alate za upravljanje identitetom i pristupom. Cilj je ograničiti pristup određenim podacima i aplikacijama kako bi se dodao još jedan sloj sigurnosti u slučaju da je mobilni uređaj ugrožen. UEM, EMM i MDM sigurnosna rješenja imaju mogućnost upravljanja mobilnim uređajima, ali samo UEM uključuje mogućnost upravljanja ostalim krajnjim točkama (osobna i prijenosna računala) i korisničkim podacima za ista. UEM dakle predstavlja alat koji uključuje sve karakteristike EMM-a uz upravljanje osobnim računalima [47].

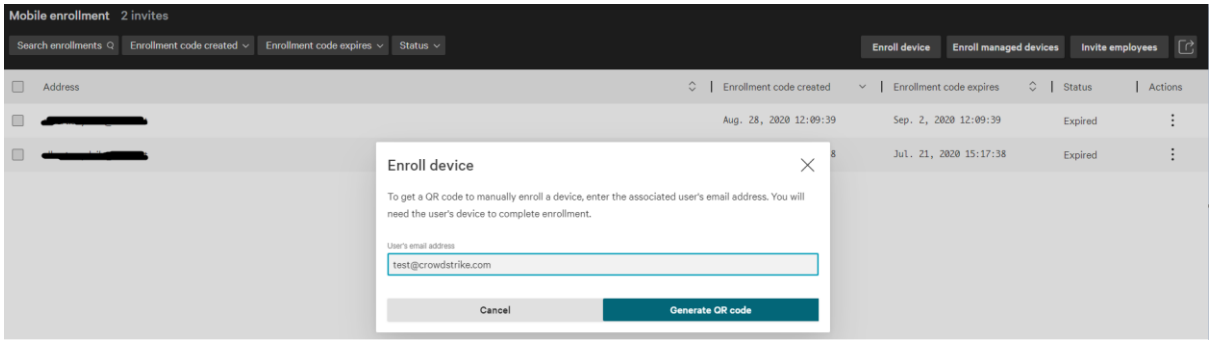
5. PROGRAMSKA RJEŠENJA ZA ZAŠTITU MOBILNIH UREĐAJA

U prethodnim poglavljima bio je opisan teoretski dio o raznim prijetnjama koje pogađaju krajnje uređaje korisnika, kao i o sigurnosnim rješenjima koji će ih štititi od istih. Kako bi se primijenila spomenuta integrirana rješenja za mobilne uređaje, potrebno je koristiti rješenja postojećih programa, odnosno platformi. U nastavku bit će opisana neka od programskih rješenja koja pomažu u zaštiti mobilnih uređaja.

5.1. CrowdStrike Falcon

Falcon za mobilne uređaje omogućuje upravljanje događajima na Android i iOS mobilnim uređajima u okruženju organizacije. Nakon što se postavi Falcon za mobilne uređaje i prijave mobilni uređaji, koristi se Falcon konzola za konfiguraciju mobilnih pravila. Tamo se nalaze senzori koji se primjenjuju na hostove na temelju dodijeljenih grupa hostova. Falcon za mobilne uređaje omogućuje organizacijama iskorištavanje izvještaja te istragu i lov na prijetnje u cijeloj organizaciji.

Slika 5.1. prikazuje Falcon platformu za dodavanje korisnika. Pokazuje način na koji se uređaji dodaju u Falcon platformu.Kako bi se uređaj korisnika dodao u platformu potrebno je kliknuti na „*Enroll device*“ gdje se upisuje elektronička adresa korisnika i klikne se na „*Generate QR code.“*

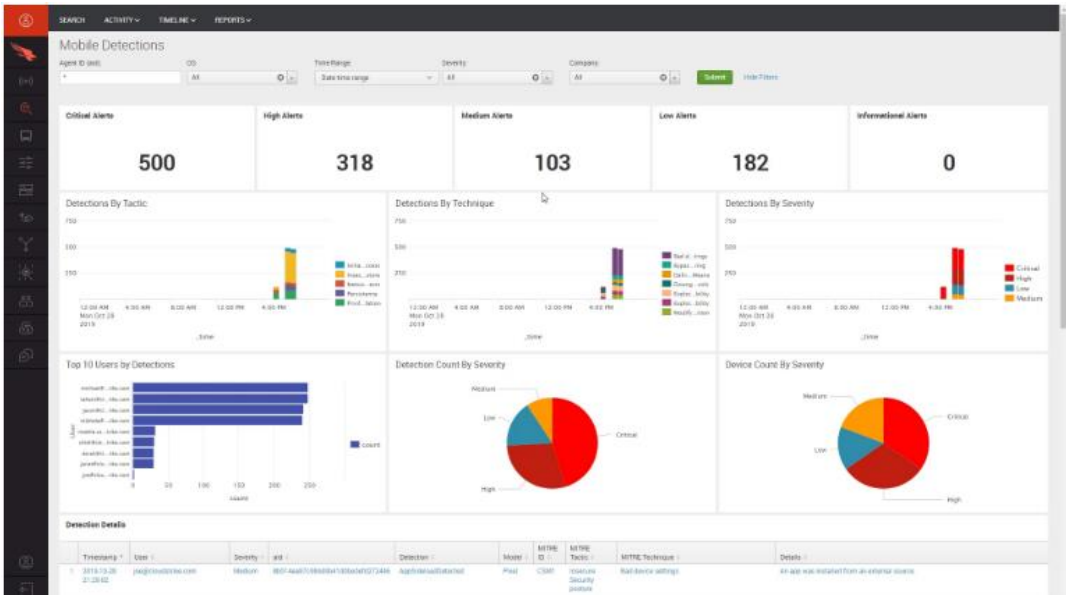


Slika 5.1. Dodavanje korisnika u Falcon platformu [48]

Prema slici 5.2. nakon što se klikne na „Generate QR code“ pojavljuje se slika s QR kodom i uputama koje je potrebno slijediti. Potrebno je instalirati Falcon za mobilne uređaje na App Store-u za Apple uređaje, a u Google play-u za Android uređaje. Nakon toga potrebno je otvoriti aplikaciju i slijediti potrebne korake, na kraju potrebno je skenirati dani QR kod.

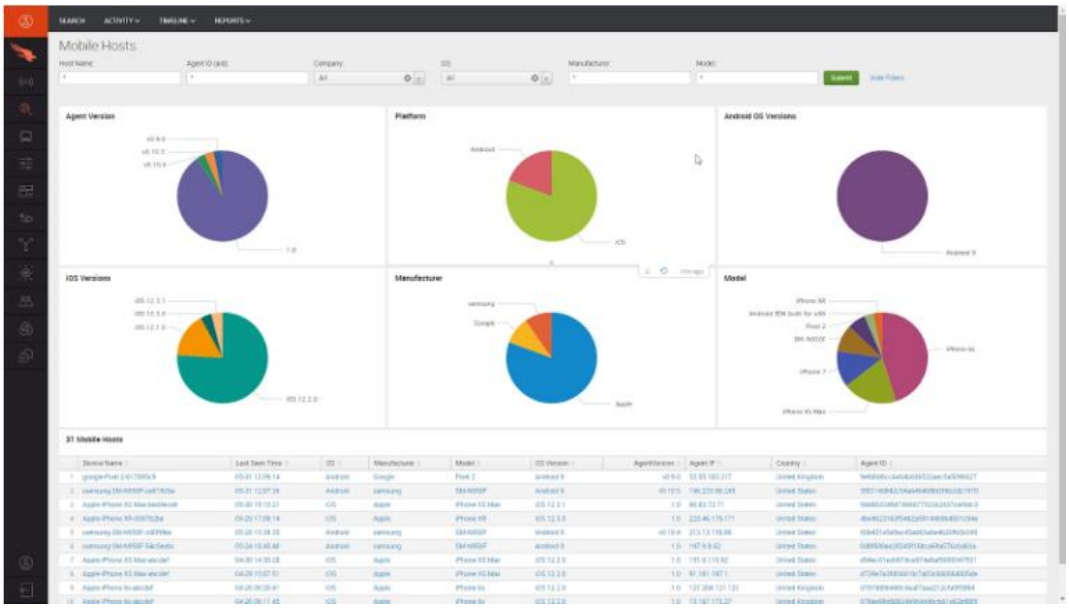
Slika 5.2. Prikaz uputstva i qr koda [48]

Nakon što je korisnik uspješno konfiguriran moguće je pratiti događaje na njegovom uređaju. Slika 5.3. prikazuje nadzornu ploču za mobilne detekcije. Otkrivene detekcije, mapiraju se prema okviru MITER ATT&CK za mobilne uređaje, što olakšava razumijevanje taktika i tehnika koje se koriste. Na nadzornoj ploči može se detaljno analizirati svaki prikazani graf kako bi se dobile potrebne informacije o navedenim detekcijama. Osim toga, moguće je detaljno proučiti pojedinosti o uređaju na način da se prouči povijest aktivnosti na uređaju. Na taj način je najlakše utvrditi je li potrebno poduzeti neke radnje protiv postojećih prijetnji i na taj način spriječiti daljnje ugrožavanje.



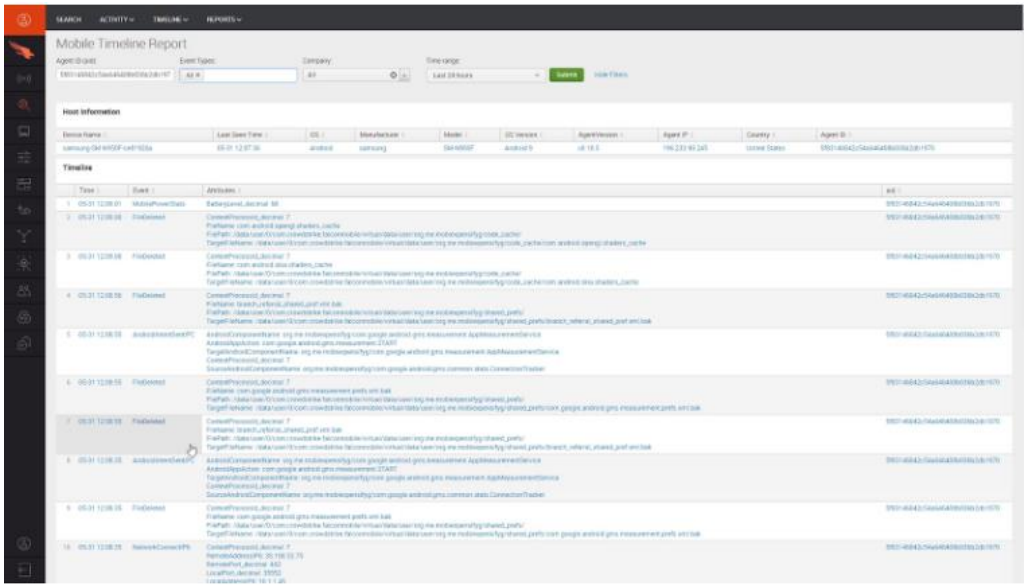
Slika 5.3. Nadzorna ploča za mobilne detekcije [48]

Slika 5.4. prikazuje nadzornu ploču mobilnih korisnika koja omogućuje pregled svih uređaja u cijeloj organizaciji. Raščlanjeni su prema vrsti platforme, operacijskom sustavu uređaja, proizvođaču, modelu i verziji agenta. Za svaki graf može se detaljnije analizirati određeni podskup da bi se vidjele bitne informacije.



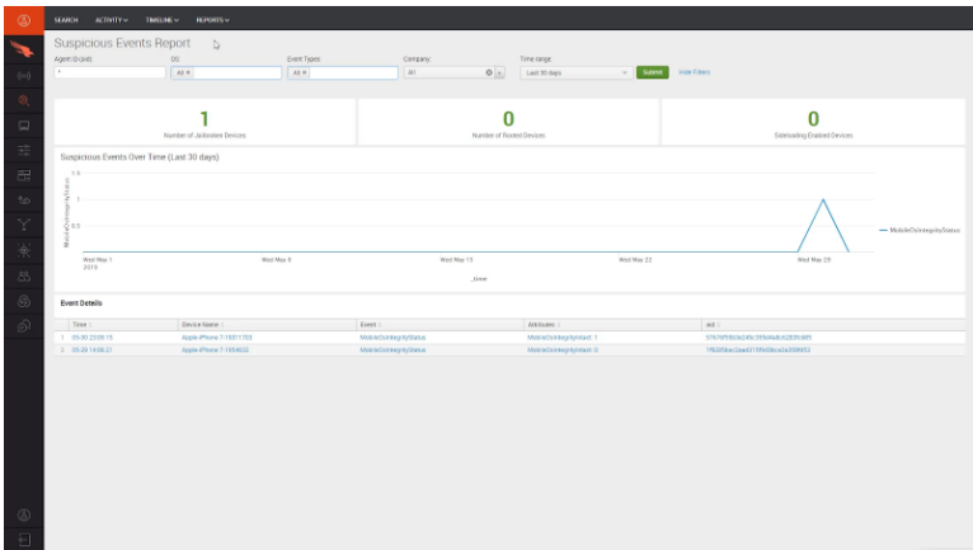
Slika 5.4. Nadzorna ploča mobilnih korisnika [48]

Slika 5.5. prikazuje izvješće „*Mobile Timeline*“ koje služi za razumijevanje svih nedavnih događaja koji su se dogodili na nekom od mobilnih uređaja. Ključna razlika u mobilnim operacijskim sustavima je u tome da se aplikacije često izvode dulje vrijeme, a kao rezultat toga ima manje izvršavanja procesa. Nakon pokretanja aplikacije, komunikaciju s operacijskim sustavom ostvarit će pomoću API poziva.



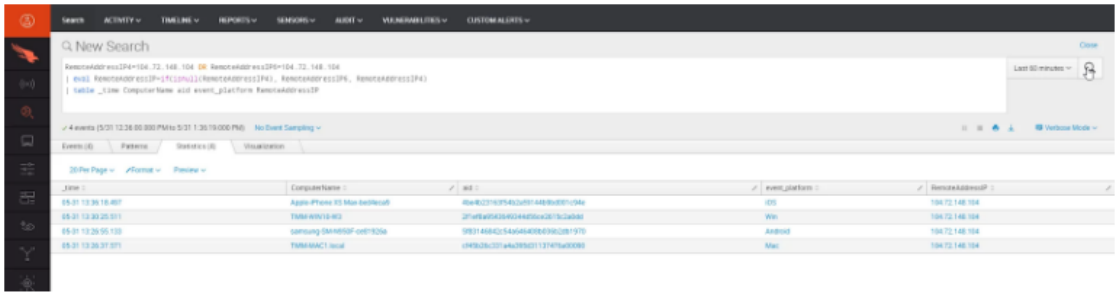
Slika 5.5. Prikaz izvješća „*Mobile Timeline*“ [48]

Još jedna od prednosti Falcon-a za mobilne uređaje je detaljno izvješćivanje i mogućnosti istraživanja prikazani na slici 5.6. Korištenjem izvješća o nekim sumnjivim radnjama, odnosno događajima, dobiva se pregled glavnih statistika koji ističe uređaje koji su „jailbreak-ani“, „root-ani“ i imaju omogućeno bočno učitavanje. Uz pomoć tog izvješća, sva pažnja se usmjerava na sve rizične mobilne uređaje. Kao bi se pogledao određeni događaj, klikne se na „*Agent ID*“ što omogućuje istraživanje sumnjivog uređaja sa svim povezanim podacima o događajima.



Slika 5.6. Prikaz sumnjivih događaja [48]

Na kraju, CrowdStrike omogućuje lov na prijetnje mobilnim uređajima uzduž cijele organizacije. Slika 5.7. prikazuje lov na prijetnje. „*ThreatGraph*“ omogućuje jednostavno pretraživanje svih podataka o događajima kako bi bilo lakše shvatiti je li neki od korisnika komunicirao s IP adresom koja izgleda kao poslužitelj za naredbe i kontrolu. Na Falcon platformi vidi se četiri događaja na različitim platformama uključujući Windows radne stanice/poslužitelje, Mac, Android i iOS uređaje. Falcon Insight omogućuje izvršavanje jednog pretraživanja kroz CrowdStrike platformu za upravljanje koje se isporučuje u oblaku kako bi se dobili potpuni rezultate za sve krajnje točke [48].

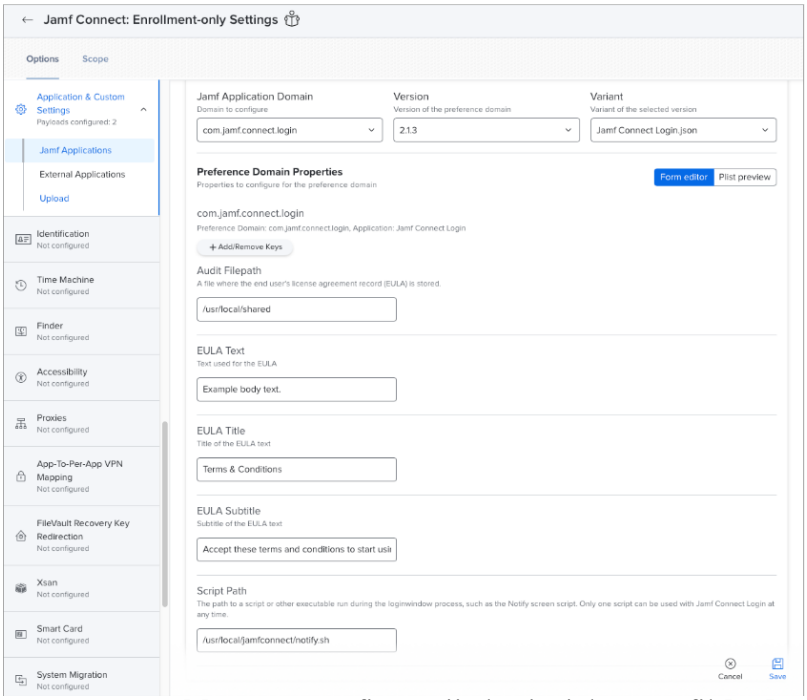


Slika 5.7. Prikaz lova na prijetnje uz pomoć „*ThreatGraph*-a“ [48]

5.2. Jamf Pro

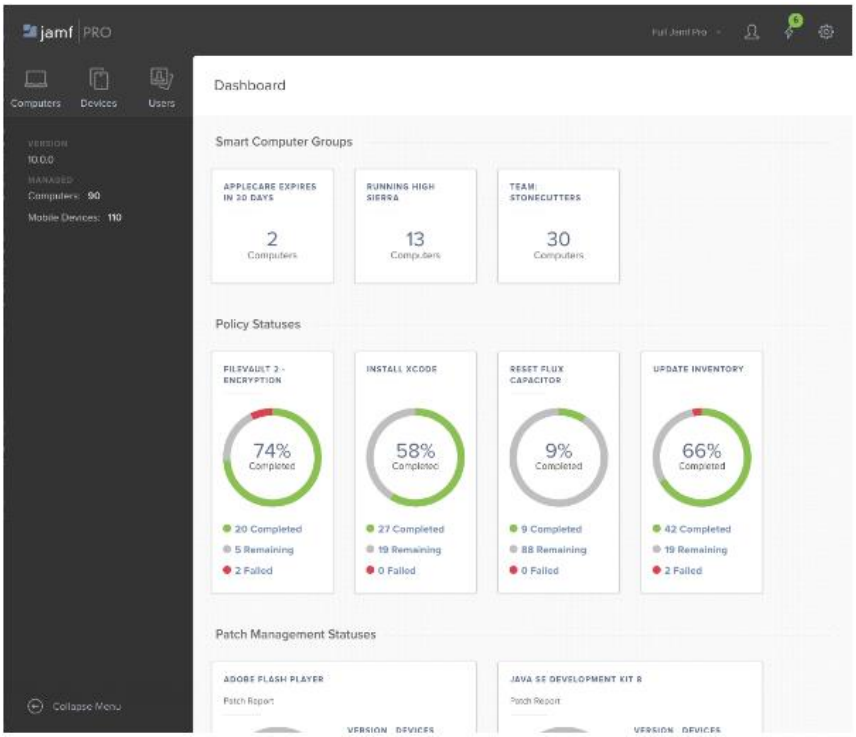
Jamf Pro je platforma koja služi za zaštitu Apple mobilnih uređaja. MDM neprimjetno će implementirati konfiguracijske profile, dodjeljivati aplikacije i slati daljinske naredbe svim uređajima (ili određenim grupama i pojedincima). Jamf Pro omogućava izvršenje raznih zadataka kao što su pokretanje skripti i instalacija paketa bez potrebne interakcije korisnika čiji se mobilni uređaj štiti.

Slika 5.8. prikazuje prikazuje platformu za dodavanje i konfiguraciju korisnika. Ona omogućuje administratorima upravljanje autentifikacijom na način da povezuje korisnički lokalni MacOS račun s identitetom organizacije u oblaku. Jamf Connect uključuje prozor za prijavu koji mijenja zadani postupak prijave za MacOS i korisničko sučelje prozora za prijavu i aplikaciju trake izbornika koja služi korisnicima za pomoć u upravljanju svojim lokalnim i mrežnim lozinkama. Kako bi se dodao novi korisnik potrebno je kliknuti na „*New*“, zatim je potrebno konfigurirati osnovne postavke (razina na kojoj se primjenjuje profil i način distribucije). Kako bi se konfigurirala Jamf aplikacija potrebno je upotrijebiti sadržaj aplikacije i prilagođenih postavki i nakon što se odaberu sve željene postavke klikne se na „*Save*.“



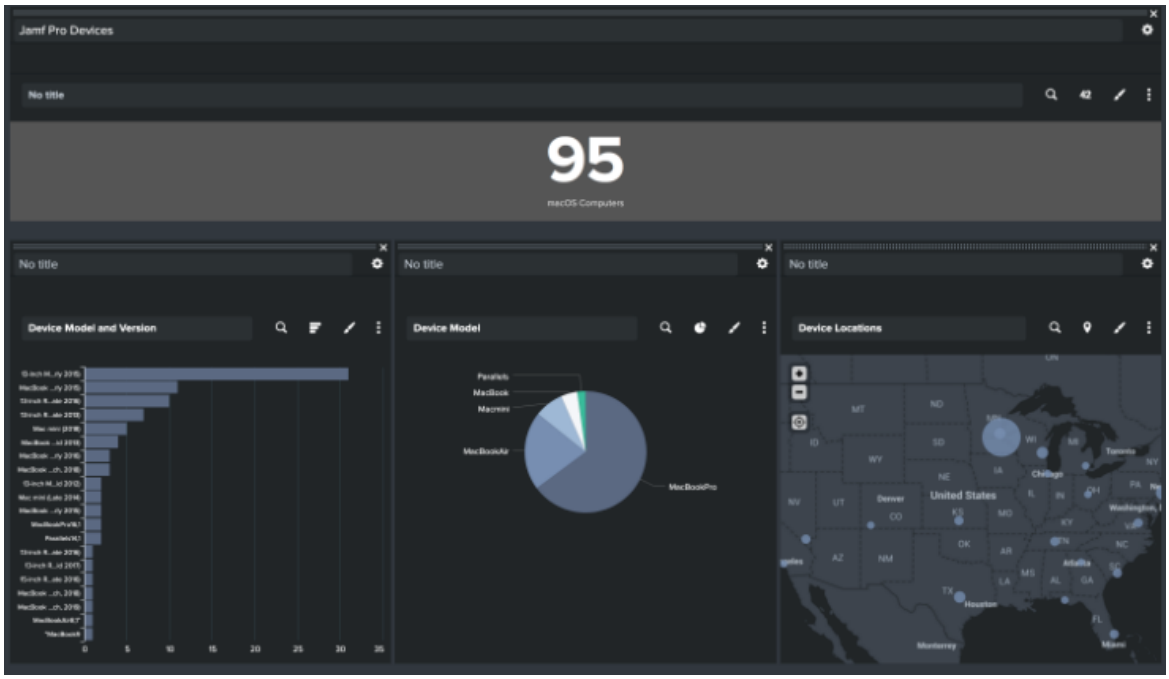
Slika 5.8. Konfiguracija korisničkog profil [49]

Nakon što je korisnik uspješno konfiguriran moguće je pratiti događaje i radnje na njegovom uređaju. Slika 5.9. prikazuje nadzornu ploču u Jamf Pro-u. Ona omogućuje praćenje statusa često pregledanih stavki (pametne grupe, pravila, konfiguracijski profili, izvješća o zakrpama i licencirani softver). Nadzorna ploča daje detaljni prikaz potrebnih informacija za postojeće detekcije. Osim navedenog prikazuje verziju uređaja te broj uređaja.



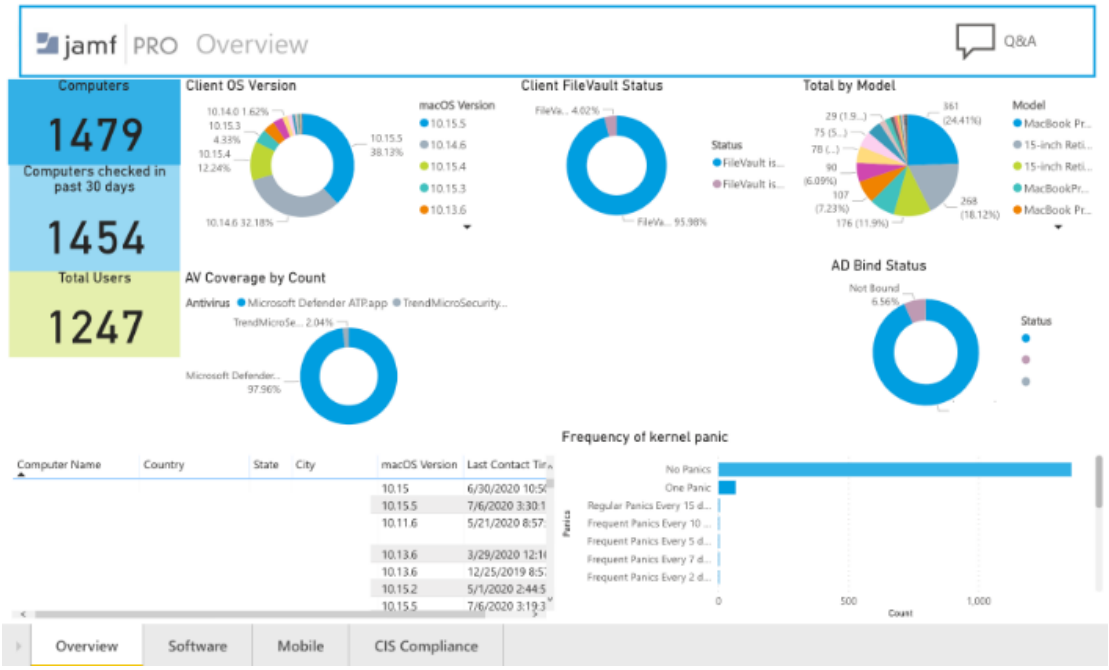
Slika 5.9. Nadzorna ploča u Jamf Pro [49]

Jamf Marketplace nudi širok izbor alata s kojim se mogu povezivati kako bi se lakše prikazala izvješća o potrebnim informacijama koje su potrebne organizacijama. Slika 5.10. prikazuje Splunk alat. Splunk predstavlja najfleksibilniji alat za izvještavanje. Prikazuje broj ukupnih uređaja, verzije uređaja, lokacije, detekcije i slično.



Slika 5.10. Splunk alat za prikaz informacija [49]

Osim Splunk alata, jedan od najčešće korištenih je Power BI koji je integriran Microsoftov ekosustav i prikazan je na slici 5.11. Power BI daje izrazitu vizualizaciju uz pomoć grafikona.

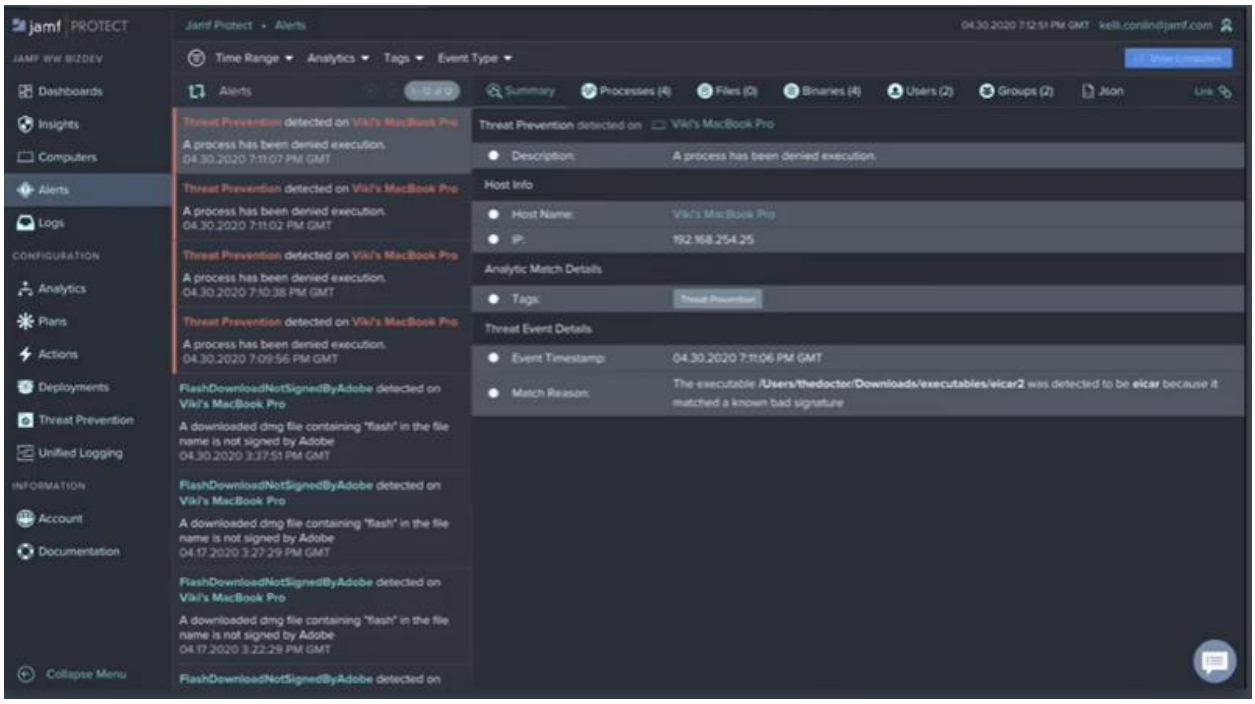


Slika 5.11. Power BI alat za prikaz informacija [49]

Sljedeći alat za korištenje prikazan na slici 5.12. je Numerics by Cynpase i predstavlja nadzornu ploču specijaliziranu isključivo za Apple uređaje. Olakšava rad s nadzornim pločama jer ima unaprijed izgrađenu integraciju za usluge u oblaku pa ih korisnik može jednostavno pregledavati na svojim uređajima. Numerics čuva korisničke podatke koji su lokalno enkriptirani na uređaju korisnika.

Slika 5.12. Numerics alat za prikaz informacija [49]

Na kraju, Jamf Pro omogućuje lov na prijetnje mobilnim uređajima u cijeloj organizaciji. Slika 5.13. prikazuje lov na prijetnje. Jamf Protect sprječava i stavlja u karantenu poznati Mac zlonamjerni softver kako bi se smanjio utjecaj na uređaj. Osim navedenog omogućuje identifikaciju i sprječavanje pokretanja raznih aplikacija kako bi organizacija u potpunosti mogla upravljati sadržajem mobilnih uređaja [49].

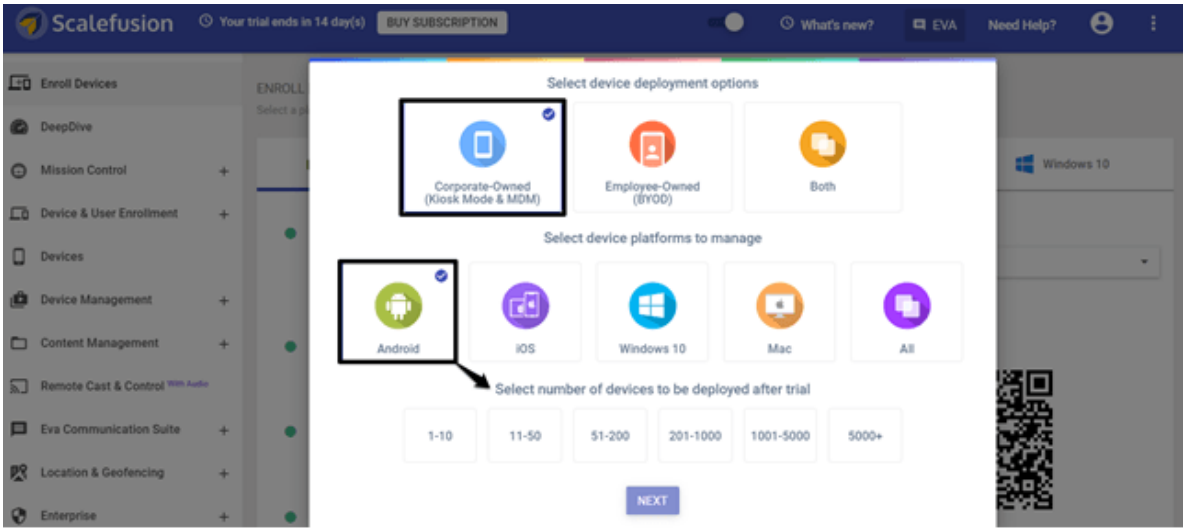


Slika 5.13. Prikaz lova na prijetnje [49]

5.3. Scalefusion MDM

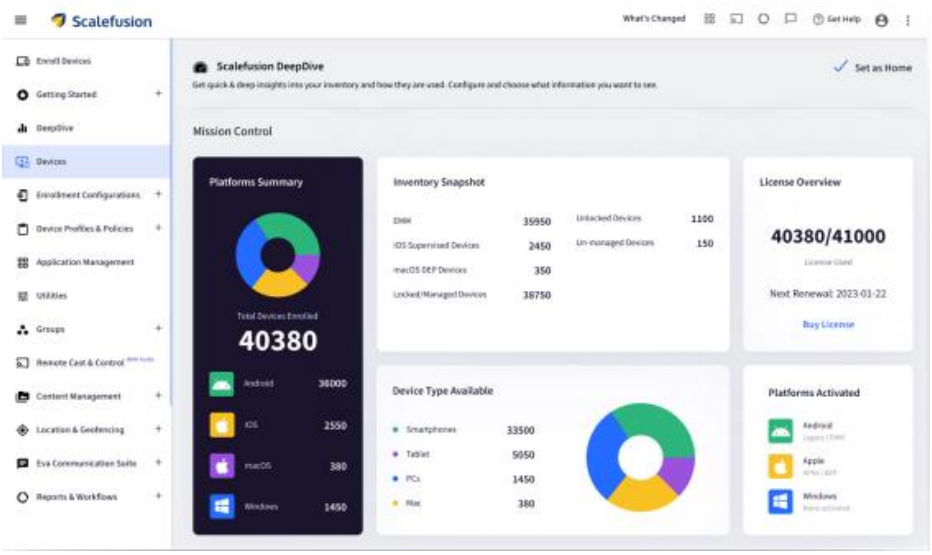
Scalefusion MDM predstavlja softver koji omogućava vidljivost i kontrolu potrebnu za osiguranje, upravljanje i nadzor svih uređaja u vlasništvu poduzeća ili zaposlenika koji pristupaju podacima poduzeća. Softver nudi velik raspon sigurnosnih pravila koja administratorima omogućuju zaštitu podataka te sprječavanje gubitka i krađe podataka [50].

Slika 5.14. prikazuje platformu za dodavanje korisnika. Nakon što se postavi Scalefusion na mobilne uređaje, konfiguracija korisnika se obavlja skeniranjem QR koda i slijedeći upute na zaslonu. Nakon toga potrebno je odabrati opcije za postavljanje uređaja: (npr. U vlasništvu tvrtke), odabrati platforme uređaja za upravljanje (npr. Android) i odabrati broj uređaja koji će biti implementirani nakon probnog roka. Nadalje se konfigurira profil koji omogućuje velik broj opcija kao i sve potrebne informacije [51].



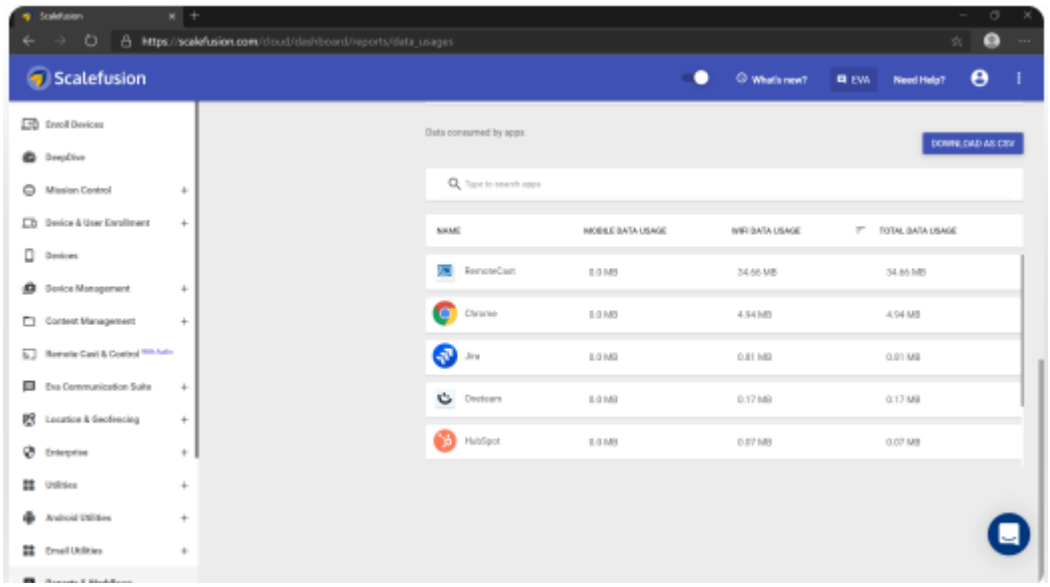
Slika 5.14. Platforma za dodavanje uređaja i korisnika [51]

Nakon što su uređaj i korisnik uspješno konfigurirani, moguće je pratiti događaje u okruženju. Slika 5.15. prikazuje nadzornu ploču koja omogućuje upravljanje uređajima, aplikacijama i sadržajem. Uz pomoć značajke mobilne analize temeljene na podacima DeepDive, može se dobiti pregled od 360 stupnjeva cjelokupnog inventara uređaja.



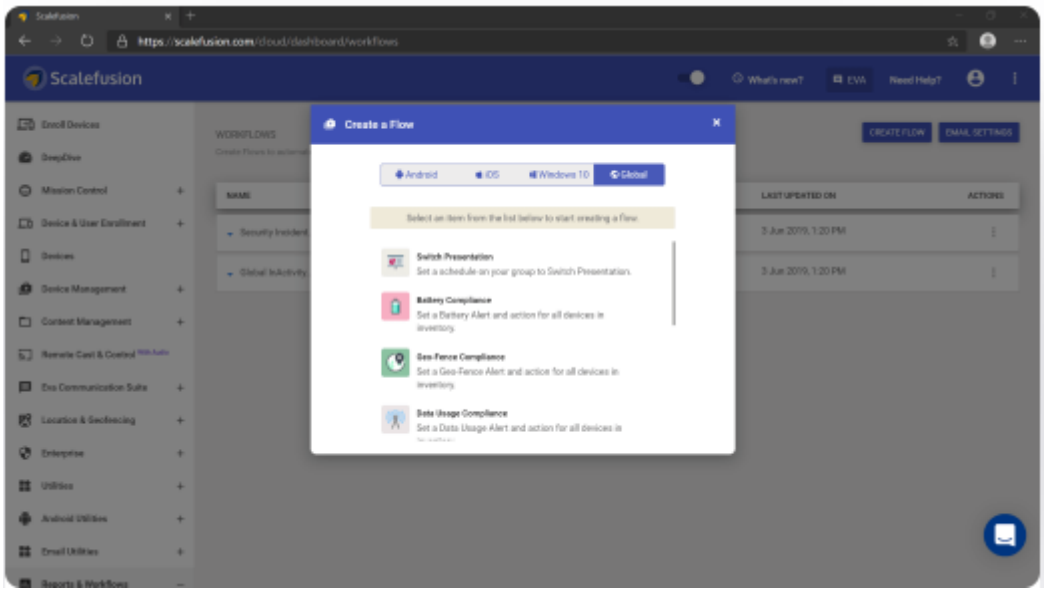
Slika 5.15. Nadzorna ploča u Scalefusion MDM [50]

Scaledusion MDM pruža analitiku i pregled izvješća. Slika 5.16. daje prikaz izvješća. Scalefusion MDM omogućava generiranje izvješća o performansama i korištenju uređaja. Moguće je izvući podatke o uređaju, upotreba uređaja, predvidjeti zastoje uređaja i slično.



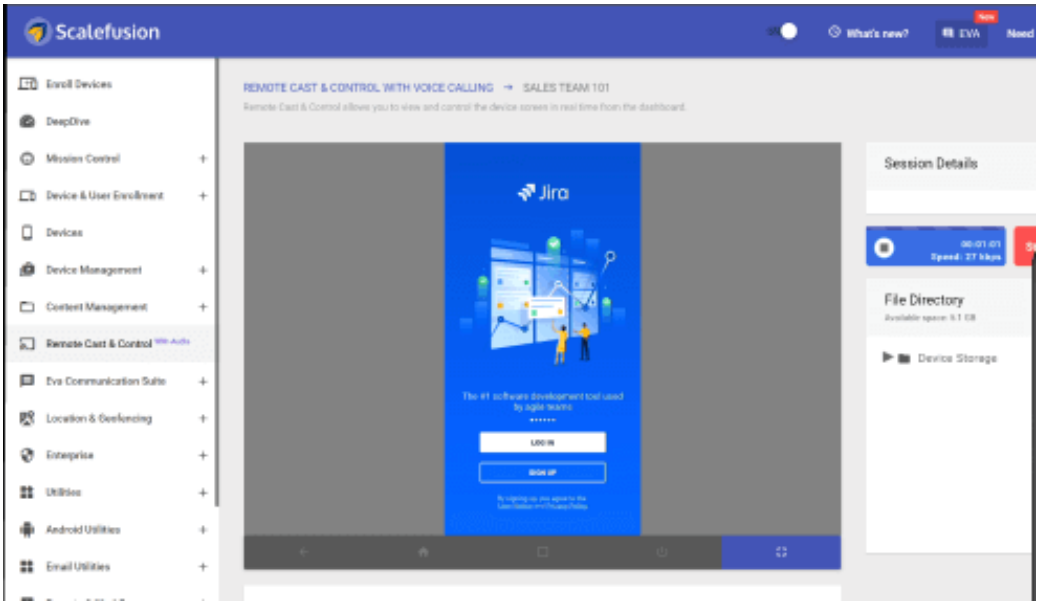
Slika 5.16. Prikaz izvješća u Scalefusion MDM [50]

Kako bi se pojednostavila analitika i praćenje izvješća moguće je ubrzati IT operacije. To se može postići na način da ručno generirano izvješće zamjeni automatiziranim izvješćima pomoću Scalefusion Workflows što je prikazano sa slici 5.17. Moguće je i zakazati vrstu i vrijeme izvješća te primati redovita izvješća koja se dostavljaju izravno u pristiglu poštu.



Slika 5.17. Prikaz Scalefusion Workflows [50]

Na kraju MDM pruža podršku za daljinsko upravljanje i značajke za rješavanje problema što je prikazano na slici 5.18. Rješavanje problema je ključno kako bi se osigurao siguran rad uređaja u svakom trenutku. Osim toga može prikazati prijetnje i ukloniti ih [50].



Slika 5.18. Daljinsko upravljanje i rješavanje problema [50]

5.4. Usporedba CrowdStrike, Jamf Pro i Scalefusion MDM programskih rješenja

Svako od tri spomenuta programska rješenja služi kao zaštita za mobilne uređaje od raznih prijetnji. CrowdStrike Falcon za mobilne uređaje ima mogućnost zaštite mobilnih uređaja koji koriste Android i iOS operacijski sustav [52]. Jamf Pro ima mogućnost zaštite mobilnih uređaja koji koriste iOS operacijski sustav, a Scalefusion MDM pruža zaštitu mobilnim uređajima Android i iOS operacijskih sustava [53]. S obzirom na cijenu, CrowdStrike pruža probni rok od 30 dana i početnu cijenu od 37.82 dolara godišnje za 5 - 299 mobilnih uređaja, ali pruža i razne dodatke koji se dodatno plaćaju [52]. Jamf Pro ima probni rok od 30 dana, a mjesečna cijena se kreće od 3.33 dolara mjesečno po mobilnom uređaju. Scalefusion MDM daje probni rok od 14 dana, a mjesečna cijena po uređaju se kreće 2.00 - 4.00 dolara [53].

Jedna od glavnih prednosti Falcon za mobilne uređaje je vidljivost koja pruža trenutni uvid u ponašanje poslovnih aplikacija te brzu i jednostavnu identifikaciju ranjivih uređaja, pružajući uvid u stanje i sigurnost uređaja u stvarnom vremenu. Ima mogućnost proaktivnog traženja prijetnji na mobilnim uređajima koristeći jedinstveno sučelje koje sadrži nove vrste telemetrije kao što su aktivnost mobilne mreže, radnje međuspremnika i praćenje perifernih uređaja. Falcon za mobilne uređaje pruža dobru integraciju i izuzetno visoke performanse. Nedostatci spomenutog rješenja su što ne može prepoznati neke od prijetnji te ima ograničene mogućnosti izvješća [52]. Jamf Pro pruža API integracije i napredno konfiguriranje. Daje jaku podršku i upravljanje aplikacijama i sukladnošću. Jedina mana je što je ograničen samo na uređaje iOS

operacijskih sustava. Scalefusion MDM pruža pojednostavljeno upravljanje uređajima pomoću nadzorne ploče s kratkom krivuljom učenja. Daje bežičnu implementaciju i dodjelu za mobilne uređaje Android i iOS operacijskih sustava. Scalefusion MDM pruža implementaciju aplikacija te upravljanje i ažuriranja za javne i privatne aplikacije, upravljanje sadržajem i daljinsko rješavanje problema. Jedini nedostatak spomenutog programskog rješenja je što nema omogućeno upravljanje zakrpama [53].

Falcon za mobilne uređaje predstavlja dobro rješenje za organizacije koje koriste velik broj mobilnih uređaja kako bi se zaštitili od napada [52]. Jamf Pro je dobar izbor za organizacije koje koriste širok raspon mobilnih rješenja za mobilne uređaje iOS operacijskog sustava. Prikladan je za upravljanje uređajima u obrazovnim ustanovama, tvrtkama i državnim organizacijama te pruža dobre značajke prilagodbe. Scalefusion MDM pruža dobar izbor za timove bilo koje veličine za implementaciju, dodjelu i upravljanje popisom uređaja u bilo kojoj industriji [53].

6. ZAKLJUČAK

Napretkom tehnologije sve više organizacija počinje koristiti uređaje kao što su stolna i prijenosna računala, pametni telefoni, tableti, IoT uređaji i slično. S obzirom na veliko korištenje navedenih uređaja oni postaju laka meta hakerima koji žele naštetiti svakom pojedincu ili organizacijama kojima mogu ugroziti poslovanje.

Jedan od najčešćih napada koji pogađa uređaje su phishing napadi kojima hakeri uz pomoć legitimne poruke na koju osoba može nasjesti kradu i manipuliraju ukradenim podacima. Ostali napadi koji se koriste su nezakrpljene ranjivosti, napadi uskraćivanjem resursa, gubitak i krađa podataka, zlonamjerni softver te usputna preuzimanja. Zlonamjerni softver je još jedna od češćih vrsta napada koji je stvoren za nanošenje štete uređajima korisnika. Kako bi se uređaji obranili od svih spomenutih napada, koriste se neka od ugrađenih rješenja. Korištena ugrađena rješenja su EPP, EDR, MDM, EEM i UEM. EPP i EDR koriste se za otkrivanje i reagiranje na unutarnje prijetnje koje mogu naštetiti organizacijama. MDM, EEM i UEM rješenja nude zaštitu za mobilne uređaje te na taj način detektiraju i sprječavaju napade hakera.

U okviru diplomskog rada provedeno je istraživanje o platformama za zaštitu mobilnih uređaja pomoću MDM-a. Postoje mnoga programska rješenja koja mogu riješiti problem zaštite uređaja, a u diplomskom radu obuhvaćena su tri od njih i objašnjena uz pomoć primjera. Spomenute platforme su CrowdStrike Falcon, Jamf Pro i Scalefusion MDM. Svaka od platformi ima vrlo sličan način pristupa. Najprije je potrebno konfigurirati korisnika unutar platforme nakon čega se dobiva uvid u sve događaje i informacije o korištenju uređaja pomoću nadzorne ploče. Nadzorna ploča daje podatke o broju konfiguriranih uređaja, korištenim pravilima, napadima i slično. Osim toga, postoji mogućnost ograničenja korištenja pojedinih aplikacija i web stranica kako korisnik ne bi zarazio uređaj. Postoji mogućnost izvještaja zato da organizacije imaju uvid u događanja i informacije o uređajima. Na kraju svaka od platforma ima mogućnost lova na napade kako bi se spriječio napad koji može potencijalno ugroziti i oštetiti, kako korisnika tako i organizaciju.

LITERATURA

[1] Endpoint Device: What Does Endpoint Device Mean?, Techopedia, 2018., dostupno na: https://www.techopedia.com/definition/29619/endpoint-device [04.05.2022.]

[2] What is an Endpoint?, Palo Alto Networks, dostupno na: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint [04.05.2022.]

[3] M., Kadrich, Endpoint Security, Pearson Education, Boston, MA, USA, 2007

[4] Geophysical Computing: Introduction to the Unix OS, University of Utah, 2010, dostupno na: https://www.studocu.com/en-us/document/university-of-utah/geophysical-computing/lecture-notes-lectures-1-5/783141 [15.05.2022.]

[5] What is Linux?: Red Hat, 2022, dostupno na: https://www.redhat.com/en/topics/linux/what-is-linux [15.05.2022.]

[6] J., Kiarie, 10 Linux Distributions and Their Targeted Users, Tecmint, 2020, dostupno na: https://www.tecmint.com/linux-distro-for-power-users/ [15.05.2022.]

[7] B., Jones, Top 10 Unix Based Operating Systems, FOSS Linux, 2020, dostupno na: https://www.fosslinux.com/44623/top-unix-based-operating-systems.htm [15.05.2022.]

[8] P., Viswanathan, What Is a Mobile Device?, Lifewire, 2021, dostupno na: https://www.lifewire.com/what-is-a-mobile-device-2373355 [15.05.2022.]

[9] Mobile Operating System, JavaTPoint, dostupno na: https://www.javatpoint.com/mobile-operating-system [15.05.2022.]

[10] B., Posey, S., Shea, IoT devices (internet of things devices), TechTarget, 2022, dostupno na: https://www.techtarget.com/iotagenda/definition/IoT-device [15.05.2022.]

[11] L., Obbayi, 5 endpoint threats inpacting security, Infosec, 2018, dostupno na: https://resources.infosecinstitute.com/topic/5-endpoint-threats-impacting-security/ [07.06.2022.]

[12] 7 Types of Cyber Security Threats: What Is a Cyber Security Threat?, University of North Dakota, dostupno na: https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/ [18.05.2022.]

[13] S., Sjouwerman, Cyberheist, KnowBe4, Clearwater, FL, USA, 2011

[14] What is a phishing attack?, Cloudflare, dostupno na: https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/ [21.05.2022.]

[15] S., Alder, Unpatched Vulnerabilities are the Most Common Attack Vector Exploited by Ransomware Actors, HIPAA Journal, 2022, dostupno na: https://www.hipaajournal.com/unpatched-vulnerabilities-are-the-most-common-attack-vector-exploited-by-ransomware-actors/ [07.06.2022.]

[16] M., Ismail, O. U., Franklin The Zero-Day Vulnerability, International Journal of Information System and Engineering, sve. 9, izd.1, 2021.

[17] J., Frankenfield, Data Loss, Investopedia, 2020, dostupno na: https://www.investopedia.com/terms/d/data-loss.asp#:~:text=What%20Is%20Data%20Loss%3F,or%20equipment%20of%20an%20edifice. [07.06.2022.]

[18] BAAlghamdi, The most common reasons for data loss, LostData, dostupno na: https://lostdata.com.sa/en/2021/06/07/the-most-common-reasons-for-data-loss/ [07.06.2022.]

[19] J., Regan, I., Belcic, What Is Malware? The Ultimate Guide to Malware, 2022, dostupno na: https://www.avg.com/en/signal/what-is-malware [30.06.2022.]

[20] A., P., Namanya, A., J., Cullen, I., Awan, J., P., Diss, The World of Malware: An Overview, Barcelona, Spain, 2018.

[21] Computer Virus, Malwarebytes, dostupno na: https://www.malwarebytes.com/computer-virus [30.06.2022.]

[22] Worm, Cyber SecTech, dostupno na: https://cyber-sectech.fandom.com/wiki/Worm [01.07.2022.]

[23] A., Vigderman, G., Turner, What Is a Computer Worm?, Security.org, 2022, dostupno na: https://www.security.org/antivirus/computer-worm/ [01.07.2022.]

[24] Trojan Horse Virus, Fortinet, dostupno na: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus [01.07.2022.]

[25] C., Stouffer, Spyware: What is spyware + how to protect yourself, Norton, 2021, dostupno na: https://us.norton.com/internetsecurity-malware-spyware.html#

[26] What is Adware? – Definition and Explanation, AO Kaspersky Lab, dostupno na: https://www.kaspersky.com/resource-center/threats/adware [11.07.2022.]

[27] A., Mohanta, A., Saldanha, Malware Analysis and Detection Engineering—A Comprehensive Approach to Detect and Analyze Modern Malware, Apress, New York, USA, 2020.

[28] M., E., Shacklett, Rootkit, TechTarget, dostupno na https://www.techtarget.com/searchsecurity/definition/rootkit [18.07.2022.]

[29] What are bots? – Definition and Explanation, AO Kaspersky Lab, dostupno na: https://www.kaspersky.com/resource-center/definitions/what-are-bots [18.07.2022.]

[30] What is Ransomware?, Yubico, dostupno na: https://www.yubico.com/resources/glossary/ransomware/ [18.07.2022.]

[31] A., Calder, The Ransomware Threat Landscape: Prepare for, Recognise and Survive Ransomware attacks, IT Goverance, Ely, UK, 2021.

[32] How to Identify Signs of Ransomware Attacks, RSI Security, 2021, dostupno na: https://blog.rsisecurity.com/how-to-identify-signs-of-ransomware-attacks/ [11.08.2022.]

[33] Ransomware, Trend Micro, dostupno na: https://www.trendmicro.com/vinfo/us/security/definition/ransomware [11.08.2022.]

[34] T., Mezquita, Drive-By Download, CyberHoot, 2020, dostupno na: https://cyberhoot.com/cybrary/drive-by-download/ [12.08.2022.]

[35] What Is a Drive by Download, Kaspersky, dostupno na: https://www.kaspersky.com/resource-center/definitions/drive-by-download [12.08.2022.]

[36] What is a denial of service attack (DoS)?, Palo Alto Networks, dostupno na: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos [12.08.2022.]

[37] M., McDonald, Web Security for Developers: Real Threats, Practical Defense, No Starch Press, San Francisco, USA, 2020.

[38] Data Breach Investigations Report, Verizon, 2022., dostupno na: https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/ [13.08.2022.]

[39] What Is Endpoint Security?, Trellix, dostupno na: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html [27.08.2022.]

[40] S., Chandel, S., Yu, T., Yitian, Z., Zhili, H., Yusheng, Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019.

[41] M., Raza, Mobile Device Management (MDM) Explained, BMC Blogs, 2021, dostupno na: https://www.bmc.com/blogs/mdm-mobile-device-management/ [27.08.2022.]

[42] M., Pierer, Mobile Device Management, Springer Vieweg, Vienna, Austria, 2016.

[43] E., Mixon, C., Steele, mobile device management (MDM), Techtarget, dostupno na: https://www.techtarget.com/searchmobilecomputing/definition/mobile-device-management [28.08.2022.]

[44] What is Enterprise Mobility Management (EMM)?, VMware, dostupno na: https://www.vmware.com/topics/glossary/content/enterprise-mobility-management.html [28.08.2022.]

[45] J., Bunnell, Emerging Tech: What is Unified Endpoint Management (UEM), IEEE Computer Society, 2022., dostupno na: https://www.computer.org/ublications/tech-news/trends/what-is-unified-endpoint-management [28.08.2022.]

[46] P., Penziol, EDR vs. EPP: What is the Difference?, Exebam, 2022, dostupno na: https://www.exabeam.com/information-security/edr-vs-epp/ [29.08.2022.]

[47] J., Powers, Understand how UEM, EMM and MDM differ from one another, TechTarget, 2019, dostupno na: https://www.techtarget.com/searchenterprisedesktop/feature/Understand-how-UEM-EMM-and-MDM-differ-from-one-another [29.08.2022]

[48] J., Scholten, How to gain visibility into Mobile Devices, CrowdStrike, 2020, dostupno na: https://www.crowdstrike.com/blog/tech-center/how-to-gain-visibility-into-mobile-devices/ [30.08.2022.]

[49] Manage and Secure Apple at Work, Jamf Pro, 2020, dostupno na: https://www.jamf.com/ [02.09.2022.]

[50] Mobile Device and Endpoint Management for 360o Monitoring and Security of Your Device Fleet, Scalefusion MDM, dostupno na: https://scalefusion.com/ [03.09.2022.]

[51] G., Figuerpa, Scalefusion MDM Setup Guide - User's Manual, Nutickets, dostupno na: https://www.nutickets.com/support/settings/devices/setup-guide-scalefusion-user-manual [03.09.2022.]

[52] Falcon for Mobile FAQ, CrowdStrike, dostupno na: https://www.crowdstrike.com/products/endpoint-security/falcon-for-mobile/faq/ [12.09.2022.]

[53] 10 Best MDM Software: Mobile Device Management Solutions In 2022, Software Testing Help, 2022, dostupno na: https://www.softwaretestinghelp.com/mobile-device-management-mdm-software/ [12.09.2022.]

SAŽETAK

U ovom radu spomenute su i opisane vrste krajnjih uređaja (računala, mobilni uređaji, IoT uređaji) i najčešći napadi koji ih pogađaju. Najčešći napadi koji pogađaju krajnje uređaje su phishing napadi, nezakrpljene ranjivosti, gubitak i krađa podataka, zlonamjerni softver, usputna preuzimanja i napadi uskraćivanjem resursa. S obzirom da gotovo svaki pojedinac ili organizacija koristi krajnje uređaje, napravljena su neka ugrađena rješenja koja služe za detekciju i zaštitu od napada. Opisane su vrste ugrađenih rješenja za napade na spomenute uređaje koje uključuju EPP, EDR, MDM, EEM i UEM.. U praktičnom dijelu rada opisana su i potkrijepljena primjerom neka od programskih rješenja za zaštitu krajnjih uređaja s naglaskom na MDM. Opisan je način korištenja i pregled događaja i detekcija unutar svake platforme.

Ključne riječi: krajnji uređaji, računala, mobilni uređaji, IoT uređaji, phishing napadi, nezakrpljene ranjivosti, gubitak i krađa podataka, zlonamjerni softver, usputna preuzimanja, napadi uskraćivanjem resursa, EPP, EDR, MDM, EEM, UEM

Integrated security solutions for protection of endpoint devices

ABSTRACT

This thesis mentions and describes types of endpoint devices (computers, mobile devices, IoT devices) and the most common attacks that are affecting them. The most common attacks affecting endpoints are phishing attacks, unpatched vulnerabilities, data loss and theft, malware, drive-by downloads, and denial of service attacks. Considering that almost every individual or organization uses end devices, some built-in solutions have been created to detect and protect against attacks. Types of built-in solutions for attacks on the mentioned devices are described which include EPP, EDR, MDM, EEM and UEM. In the practical part of the work, some of the software solutions for the protection of end devices with an emphasis on MDM are described and supported by examples. The method of use and overview of events and detections within each platform is described.

Keywords: endpoint devices, computers, mobile devices, IoT devices, phishing attacks, unpatched vulnerabilities, data loss and theft, malware, drive-by downloads, denial of service, EPP, EDR, MDM, EEM, UEM

ŽIVOTOPIS

Megan-Maria Fabing rođena je 8. siječnja 1999. godine u Našicama, Republika Hrvatska. Pohađala je Osnovnu školu Augusta Harambašića u Donjem Miholjcu te nakon završetka osnovne škole upisuje Opću gimnaziju u Donjem Miholjcu. Godine 2017. upisuje Prediplomski studij elektrotehnike na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, a na drugoj godini prediplomskog studija opredjeljuje se za smjer Komunikacije i informatika. Godine 2020. završava tri godine prediplomskog studija i upisuje Diplomski sveučilišni studij Elektrotehnike, smjer Mrežne tehnologije. Trenutno radi u Atosu u Osijeku kao inženjer za sigurnost.