Sigurnosni aspekti korporativnih podataka mobilnih uređaja u privatnom vlasništvu

Tomas, Kristijan

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Kristijan Tomas

SIGURNOSNI ASPEKTI KORPORATIVNIH PODATAKA MOBILNIH UREĐAJA U PRIVATNOM VLASNIŠTVU

ZAVRŠNI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 6757

Pristupnik: **Kristijan Tomas (0135257163)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Sigurnosni aspekti korporativnih podataka mobilnih uređaja u privatnom vlasništvu**

Opis zadatka:

Opisati korištenje privatnih uređaja u korporativnom okruženju. Identificirati poslovne i privatne podatake na uređaju. Istražiti mogućnosti platformi za upravljanje uređajima i podacima. Analizirati sigurnosne prijetnje korporativnim podacima. Objasniti metode zaštite korporativnih podataka.

Mentor:

doc. dr. sc. Siniša Husnjak

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

SIGURNOSNI ASPEKTI KORPORATIVNIH PODATAKA MOBILNIH UREĐAJA U PRIVATNOM VLASNIŠTVU

SECURITY ASPECTS OF CORPORATE DATA OF PRIVATELY OWNED MOBILE DEVICES

Mentor: doc. dr. sc. Siniša Husnjak

Student: Kristijan Tomas
JMBAG: 0135257163

Zagreb, 2022.

SIGURNOSNI ASPEKTNI KORPORATIVNIH PODATAKA MOBILNIH UREĐAJA U PRIVATNOM VLASNIŠTVU

SAŽETAK

Korištenje mobilnih uređaja u korporativnom okruženju je u rastućem trendu. Svaka korporacija želi povećati produktivnost zaposlenika i tako dolazi do uvođenja metoda za obavljanje poslovnih zadataka preko privatnih uređaja zaposlenika. Većina zaposlenika nije svjesna mogućih sigurnosnih prijetnji i kako njihove radnje na uređajima mogu znatno ugroziti sigurnost podataka, poslovanje korporacije i na kraju krajeva, reputaciju korporacije. Sve više korporacija ulaže u zaštitu osjetljivih podataka koje su od iznimne važnosti za poslovanje. Sigurnost podataka korporacije s kojima zaposlenici raspolažu na mobilnim uređajima ne bi smjela biti upitna. Svrha ovog rada je prikazati korištenje privatnih uređaja zaposlenika u poslovnom okruženju i kako to utječe na sigurnost korporativnih podataka. Prikazat će se načini odvajanja privatnih od poslovnih podataka, sigurnosne prijetnje s kojima se korporacije suočavaju i metode zaštite korporativnih podataka.

Ključne riječi: podaci, sigurnost podataka, privatni i poslovni profil

SUMMARY

The use of mobile devices in the corporate environment is a growing trend. Every corporation wants to increase the productivity of its employees, and thus comes the introduction of methods for performing business tasks through employees' private devices. Most employees are unaware of potential security threats and how their actions on devices can significantly jeopardize data security, corporate operations, and ultimately, corporate reputation. More and more corporations are investing in the protection of sensitive data that is extremely important for business. The security of corporate data held by employees on mobile devices should not be in doubt. The purpose of this thesis is to show the use of private devices of employees in a business environment and how this affects the security of corporate data. Ways to separate private from business data, security threats that corporations are facing and methods of protecting corporate data will be presented in this thesis.

Keywords: data, data security, private and work profile

SADRŽAJ

1. UVOD

Napredak digitalizacije učinio je obavljanje posla praktičnijim nego ikada. Bilo da se radi o poslovnom računalu, kućnom prijenosnom računalu ili čak pametnom telefonu, sve više kompanija dopušta svojim zaposlenicima da posluju na svojim osobnim pametnim telefonima. Korporacije sve više uvode razne alate i modele za obavljanje posla na privatnim uređajima zaposlenika. Omogućuju svojim korisnicima obavljanje poslovnih zadataka uz fleksibilnost i povećanje produktivnosti. To se naziva "donesite svoj uređaj" ili BYOD (Bring Your Own Device). Međutim, to stvara drugačiji sigurnosni rizik, jer osobni uređaji nisu tako dobro zaštićeni i mogu se lako probiti. Poslovni podaci nisu dovoljno zaštićeni i uz malo vještine napadači vrlo lako iskoriste privatne uređaje kako bi pristupili poslovnim podacima. Naravno, postoje razni alati za odvajanje privatnog i poslovnog profila, ali potrebni su i dodatni koraci zaštite kako bi podaci bili maksimalno osigurani.

U ovom završnom radu cilj i svrha je analiza i istraživanje sigurnosnih aspekta korporativnih podataka mobilnih uređaja u privatnom vlasništvu.

Rad se sastoji od 7 poglavlja:

1. Uvod
2. Korištenje privatnih uređaja u poslovnom okruženju
3. Segmentacija poslovnih i privatnih podataka na uređaju
4. Mogućnosti platformi za upravljanje uređajima i podacima
5. Analiza sigurnosnih prijetnji korporativnim podacima
6. Metode zaštite korporativnih podataka
7. Zaključak

U drugom poglavlju opisat će se korištenje privatnih uređaja u poslovnom okruženju. Prikazat će se najčešći modeli koje koriste korporacije za korištenje privatnih uređaja za posao.

U trećem poglavlju objasnit će se pojam segmentacije podataka i kako se radi segmentacija poslovnih i privatnih podataka na uređaju. Opisat će se tvorba privatnog i radnog profila na uređajima i pojam Android Enterprise.

U četvrtom poglavlju prikazat će se mogućnosti platformi za upravljanje uređajima i podacima. Također će se objasniti komponente platformi za upravljanje uređajima. Objasnit će se Maas360 koji je jedan od alata za upravljanje uređajima.

U petom poglavlju analizirat će se najčešće sigurnosne prijetnje korporativnim podacima s kojima se korporacije suočavaju. Svaka prijetnja će biti ukratko objašnjena uz prikazivanje primjera u praksi.

U šestom poglavlju prikazat će se metode zaštite korporativnih podataka koje bi korporacije trebale uzeti u obzir. Svaka metoda će biti ukratko opisana kako bi se prikazala njihova važnost korištenja pri zaštiti podataka.

2. KORIŠTENJE PRIVATNIH UREĐAJA U KORPORATIVNOM OKRUŽENJU

Većina današnjih korporacija nudi svojim zaposlenicima službene uređaje, poput laptopa i mobilnog uređaja. Takvi uređaji imaju povećanu razinu sigurnosti podataka i zaposlenici ih ne koriste u privatne svrhe. To dovodi do određenog stupnja ograničenosti i nepraktičnosti jer zaposlenici nose sa sobom službene uređaje korporacije i svoje vlastite privatne uređaje poput privatnog mobilnog uređaja.

Kako ljudi postaju sve više vezani za vlastite pametne telefone, tvrtke moraju uzeti u obzir želje svojih zaposlenika kada odlučuju kako žele upravljati vlastitom komunikacijom. Postoje četiri glavna modela:

- Bring Your Own Device (BYOD),
- Company Owned/Personally Enabled (COPE),
- Choose Your Own Device (CYOD),
- Corporate Owned, Business Only (COBO).

2.1. Bring Your Own Device (BYOD)

BYOD označava pojam u kojem zaposlenik smije koristiti uređaje u privatnom vlasništvu za obavljanje službenih poslova, umjesto korištenja uređaja tvrtke. Privatni uređaj može biti laptop, mobitel ili tablet. U BYOD metodi, tvrtka omogućava korištenje privatnog uređaja za osobnu i službenu uporabu.

Pojam BYOD prvi put se pojavljuje 2004. godine. Neke tvrtke koje su uspješno implementirale BYOD politike uključuju Apple, VMware, IBM, Citrix, SAP, Bluebox itd. BYOD se odnosi na politiku dopuštanja zaposlenicima da donesu uređaje u privatnom vlasništvu kao što su prijenosna računala, tablete, pametne mobitele za rad i korištenje tih uređaja za pristup informacijama tvrtke i aplikacijama na njemu.

Budući da su istraživanja pokazala da tvrtke ne mogu spriječiti zaposlenike da dovode svoje privatne uređaje na radno mjesto, što dovodi do smanjenja produktivnosti za posao, nastala je ideja korištenja privatnih uređaja za rad. Za to je potrebna samo dobra BYOD politika. Prema nedavnom istraživanju oko 95% zaposlenika koristi barem jedan privatni uređaj na poslu. U početku su neke tvrtke poput IBM-a dopuštale zaposlenicima da donesu vlastite uređaje na radno mjesto i promatrana je produktivnost i ušteda troškova. Ideja je u početku odbijena zbog sigurnosnih razloga, ali sve više i više tvrtki sada žele uključiti BYOD

pravila. Oko 76% zaposlenika na tržištima visokog rasta već koriste vlastitu tehnologiju na djelu (Slika 1.) [1]. Svakako su pandemija COVID-19 i rad od kuće pomogli bržem razvitku BYOD-a. Neke industrije usvajaju BYOD brže od drugih. Bliski istok ima najveću stopu implementacije BYOD-a (oko 80%). Neka izvješća ukazuju na povećanje produktivnosti zaposlenika. Obrazovna industrija ima 95,25%, što je najveći postotak ljudi koji koriste BYOD za rad prema studiji koju su izradili Cisco partneri BYOD prakse.

Slika 1. Trendovi BYOD-a

Izvor: [1]

Studija također sugerira da prednosti BYOD-a uključuju povećanu produktivnost zaposlenika, zadovoljstvo i uštedu troškova za tvrtku. Povećana produktivnost dolazi od toga što se korisnik osjeća ugodnije s vlastitim privatnim uređajem. BYOD povećava zadovoljstvo zaposlenika i zadovoljstvo poslom, jer zaposlenik koristi uređaj koji je osobno odabrao kao svoj, a ne onaj koji su odabrali tvrtka i IT tim. Također im omogućuje nošenje jednog uređaja umjesto jednog za posao i jednog za osobnu upotrebu.

Budući da BYOD pruža priliku zaposlenicima da rade bilo gdje i na bilo kojem uređaju što rezultira u stvarnim poslovnim koristima i produktivnim rezultatima, također donosi značajne i vrlo ozbiljne rizike. Prema istraživanju IDG-a, više od polovice korporacija prijavili su ozbiljne povrede korištenja osobnih mobilnih uređaja. Glavni problem s BYOD-om je da osoba koristi isti uređaj za pristup i privatnim podaci kao i podacima tvrtke. Poslovni podaci mogu

sadržavati važne informacije tvrtke i mogu biti iznimno osjetljivi na ozbiljne sigurnosne rizike. Na primjer, ako zaposlenik koristi pametni telefon za pristup mreži tvrtke, a zatim izgubi taj telefon tada napadači mogu lako dobiti poslovne podatke tvrtke. Druga vrsta sigurnosne povrede događa se kada zaposlenik napusti tvrtku, a ne mora vratiti uređaj, tako da aplikacije tvrtke i drugi podaci mogu još uvijek biti prisutni na njihovom uređaju i može doći do zloupotrijebe pristupa.

Jedan od glavnih problema je problem broja mobilnog uređaja BYOD-a, koji postavlja pitanje o vlasništvu nad brojem. Problem postaje očit kada zaposlenici koji su povezani sa klijentima i kupcima odu iz tvrtke i zaposle se kod konkurenata. Kupci koji zovu taj broj tada će potencijalno zvati konkurente, što može dovesti do potencijalnog gubitka kupaca za BYOD poduzeća. Nadalje, ljudi mogu prodati svoje uređaje i zaboraviti obrisati osjetljive podatke prije primopredaje. Još jedan sigurnosni rizik uključuje članove obitelji, jer članovi obitelji obično dijele svoje uređaje kao što su tableti, mobiteli i prijenosna računala, jedni s drugima u obitelji i dijete bi vrlo lako moglo imati pristup uređaju roditelja i slučajno i nenamjerno dijeliti osjetljivi sadržaj putem e-pošte ili na platformama društvenih medija kao što su Facebook, WhatsApp.

Tvrtke moraju provoditi stroge sigurnosne mjere kako bi spriječile pristup osjetljivim informacijama. IT odjeli koji podržavaju organizacije s BYOD politikom moraju imati različite sustave i procese za primjenu zakrpa koje štite sustave od poznatih ranjivosti uređaje koje korisnici mogu koristiti. Idealno bi bilo da takvi odjeli imaju sustave koji mogu brzo prilagoditi potrebnu podršku za nove uređaje. Međunarodna istraživanja otkrivaju da je samo oko 20% zaposlenika potpisalo BYOD politiku [2]. Politike BYOD mogu se uvelike razlikovati od organizacije do organizacije ovisno o problemima, rizicima, prijetnjama i kulturi. Pristupi mogu biti toliko različiti u razini fleksibilnosti koja se daje zaposlenicima za odabir vrste uređaja ovisno o navedenim uvjetima. Dobra BYOD politika jasno navodi koja su područja usluge i podrške zaposlenicima, odgovornosti zaposlenika i koje su odgovornosti poduzeća.

2.2. Company Owned/Personally Enabled (COPE)

COPE je poslovni model u kojem organizacija svojim zaposlenicima osigurava mobilne i računalne uređaje te omogućuje zaposlenicima da ih koriste kao da se radi o osobnim prijenosnim računalima, tabletima ili pametnim telefonima. Budući da korporacija često može nabaviti IT proizvode po veleprodajnim ili nižim cijenama, poslovni model COPE može biti isplativa opcija i za organizaciju i za zaposlenike. Iako tvrtka tehnički posjeduje uređaje i

odgovorna je za mjesečne troškove korištenja, zaposlenici ih slobodno mogu koristiti izvan posla.

COPE model može olakšati inicijative organizacije za upravljanje mobilnim uređajima (Mobile Device Management – MDM) i upravljanje mobilnim aplikacijama (Mobile Aplication Management – MAM) i dati organizaciji veću moć zaštite podataka organizacije i tehnički i pravno. Budući da organizacija posjeduje COPE uređaje i liniju usluga, ona također ima moć odabira dobavljača s kojima će raditi i koje će modele uređaja i podatkovne planove pružiti. I BYOD i COPE modeli odražavaju stalni trend prema fluidnijim granicama između osobne i poslovne upotrebe tehnologija. COPE također može pojednostaviti tehničku podršku budući da organizacija podržava samo određene vrste uređaja i operativne sustave. Nasuprot tome, korisnici u BYOD okruženju mogu koristiti gotovo bilo koju vrstu uređaja. Još jedna prednost COPE-a je ta što organizacija može odrediti da uređaji pokreću određene verzije operativnog sustava i konfiguracije uređaja. To može uvelike pomoći u održavanju sigurnosti uređaja i rješavanju svih ranjivosti.

Jedan od najvećih izazova povezanih s modelom COPE je da je organizacija odgovorna za primjenu ažuriranja na uređajima i za podršku tim uređajima. To može dodatno opteretiti IT osoblje organizacije. To također znači da će organizacija morati uložiti u softver za upravljanje mobilnošću poduzeća (Enterprise Mobility Management – EMM), ako već nije. Još jedan izazov povezan s usvajanjem COPE-a jest to što će neki korisnici možda radije nastaviti koristiti svoje osobne uređaje. Može biti teško podržati i COPE i BYOD u isto vrijeme. Službi za podršku možda nedostaju kadrovski resursi za podršku obje metode ili bi IT služba mogla ograničiti na korištenje ili BYOD ili COPE, ali ne oboje.

Pristup COPE može se usporediti s modelom BYOD (Tablica 1.), u kojem zaposlenici kupuju vlastite mobilne uređaje i koriste ih za radne zadatke, i tradicionalnim modelom pružanja IT usluga, u kojem organizacije zaposlenicima dodjeljuju računalne uređaje koji ostaju trajno smješteni na radnom mjestu. U COPE modelu, organizacija posjeduje i osigurava uređaje prije nego što ih dodijeli krajnjem korisniku. Kao takva, organizacija je u mogućnosti osigurati da je uređaj konfiguriran na način koji minimizira rizike, a istovremeno se pridržava sigurnosne politike mobilnih uređaja organizacije. Slično tome, budući da je organizacija vlasnik uređaja, aplikacije povezane s poslom imaju prioritet. U BYOD okruženju relativno je uobičajeno da uređaj korisnika sadrži toliko mnogo osobnih aplikacija i podataka da nema dovoljno prostora za smještaj aplikacija povezanih s radom. S modelom COPE, međutim, prvo se instaliraju radne aplikacije, ostavljajući korisniku da se snađe s preostalom pohranom na uređaju.

Neke organizacije također smatraju da je model COPE bolji od modela BYOD jer znatno olakšava provođenje politike prihvatljive upotrebe. Iako većina organizacija ima prihvatljivu politiku upotrebe i za BYOD uređaje, te politike može biti teško provesti s obzirom da organizacija zapravo ne posjeduje uređaj. Politika COPE može pomoći u smanjenju pravnih rizika i rizika sigurnosti podataka ograničavanjem vrsta aplikacija koje korisnici smiju instalirati na uređaje. Neke će organizacije također ograničiti vrste sadržaja kojima korisnici mogu pristupiti na mreži.

Tablica 1. BYOD vs COPE

	BYOD	**COPE**
Definicija	➢ Politika koja dopušta zaposlenicima da na svoje radno mjesto donesu mobilne uređaje u privatnom vlasništvu	➢ Korporacija kupuje i osigurava računalne resurse i uređaje koje zaposlenici koriste i njima upravljaju
Prednosti	👍 Veći angažman korisnika 👍 Pogodnost 👍 Niži troškovi održavanja	👍 Ravnoteža između posla i privatnog života na jednom uređaju 👍 Pojačana kontrola i autoritet nad uređajima
Nedostatci	👎 Teža provedba sigurnosti 👎 Manja centraliziranost s BYOD-om nego s COPE-om 👎 Zamjena uređaja može biti problematična kad se uređaj razbije/pokvari	👎 Mogućnost problema s produktivnošću s obzirom na manju slobodu korisnika 👎 Korporacija potpuno odgovara za održavanje koraka s inovacijama na tržištu

Implementacija COPE politike uključuje puno više od pukog izdavanja uređaja krajnjim korisnicima. Jedan od prvih koraka u stvaranju takve politike je stvaranje prihvatljive politike korištenja za krajnje korisnike. Iako je korisnicima dopušteno obavljanje osobnih zadataka s uređajem, ne bi trebali imati slobodnu vlast nad uređajem. IT administratori će vjerojatno

morati postaviti pravila koja zabranjuju korisnicima mijenjanje konfiguracijskih postavki, uklanjanje softvera koji je postavila organizacija ili pristup nepoželjnom sadržaju. Još jedna stvar koju IT administratori moraju učiniti kada kreiraju COPE politiku je definirati uvjete usluge za uređaj. Drugim riječima, IT administratori će trebati izraditi politiku koja opisuje što korisnik može realno očekivati dok koristi uređaj.

Na primjer, ako je politika pokrenuti daljinsko brisanje na uređajima koji su izgubljeni, korisnici će morati znati da bi mogli pretrpjeti gubitak podataka ako pohranjuju osobne podatke na uređaj. Dobra COPE politika također bi se trebala baviti pitanjem tehničke podrške. Budući da organizacija posjeduje i konfigurira uređaj, IT odjel će vjerojatno biti odgovoran za podršku uređaju. Unatoč tome, važno je postaviti ograničenja u pogledu toga što će IT odjel podržavati. U suprotnom bi služba za pomoć mogla početi primati pozive za podršku u vezi s osobnim aplikacijama korisnika.

Konačno, politika COPE trebala bi se baviti pitanjem privatnosti krajnjeg korisnika. Krajnji korisnici koji koriste COPE uređaj za pristup svojim osobnim računima na društvenim mrežama, na primjer, mogu postaviti pitanje špijunira li ih organizacija. Dobro napisana pravila o privatnosti služe za određivanje očekivanja krajnjih korisnika, a istovremeno postavljaju granice za organizaciju [3].

2.3. Choose Your Own Device (CYOD)

CYOD je sličan BYOD-u—omogućuje zaposlenicima da rade s bilo kojeg mjesta koristeći mobilni uređaj. Međutim, za razliku od BYOD-a gdje korisnik može koristiti bilo koji uređaj, CYOD uređaje mora odobriti organizacija. U većini slučajeva organizacija osigurava mobilni uređaj, a zaposlenik odabire s popisa odobrenih uređaja. Tvrtka kupuje uređaj i njime upravlja. Dok krajnji korisnik ima fleksibilnost korištenja mobilnog uređaja bilo gdje, organizacija zapravo posjeduje taj uređaj. CYOD mreže pružaju veću stabilnost, sigurnost i pojednostavljeni IT pristup za tvrtke. IT osoblju daju veću kontrolu nad uređajima u mreži. Pristup aplikacijama, podacima i funkcijama može biti ograničen, a s manje odobrenih uređaja u mreži podrška postaje brza i laka. CYOD je posebno koristan za tvrtke koje rade s osjetljivim informacijama.

Budući da tvrtka posjeduje i upravlja uređajem, podaci tvrtke su sigurni. Uz mogućnost instaliranja i upravljanja sigurnosnim rješenjima na uređaju, podaci tvrtke su slobodni od zlonamjernog softvera i hakerskih prijetnji, a ako je uređaj izgubljen ili ukraden, podaci tvrtke neće dospjeti u neovlaštene ruke. Organizacije bi trebale razmotriti nekoliko aspekata prije nego što izaberu između BYOD i CYOD pravila. Mali IT proračuni i naslijeđena infrastruktura obično zahtijevaju politiku BYOD, dok viši sigurnosni zahtjevi i ulaganja unaprijed zahtijevaju politiku CYOD.

Iako CYOD donosi više kontrole i sigurnosti IT mrežama, dolazi i s određenim izazovima. Prvo, organizacije moraju unaprijed uložiti ogromna sredstva za kupnju i upravljanje hardverom. To je u suprotnosti s računalstvom u oblaku, gdje su ulazni troškovi obično niski. Drugo, ograničavanje korištenja uređaja zaposlenicima može rezultirati nezadovoljstvom koje zauzvrat utječe na produktivnost. Treće, vrijeme odobrenja uređaja još je jedan negativan aspekt. Vrijeme potrebno za odobravanje uređaja može dovesti do propuštanja nove tehnologije ili aplikacije. Na Slici 2. su prikazane glavne značajke CYOD modela.

	Zaposlenik	Korporacija
Vlasnik uređaja		✓
Vlasnik podataka na uređaju	✓	✓
Održavanje uređaja		✓
Plaćanje troškova uređaja		✓
Vlasnik broja na uređaju		✓

Slika 2. Glavne značajke CYOD modela

Izvor: [5]

CYOD pristup zahtijeva od zaposlenika da biraju iz ograničenog raspona uređaja. Na primjer, tvrtka može dopustiti zaposlenicima korištenje BlackBerryja, iPhonea ili drugih Appleovih uređaja – ali ne i Androida. Tvrtka također može ograničiti upotrebu uređaja na radne aktivnosti. Pristup CYOD pruža druge sigurnosne opcije za tvrtke koje su zabrinute zbog mogućih posljedica BYOD-a. Zbog različitih problema povezanih s višenamjenskim uređajima, osiguranje BYOD sustava može biti teško. Ovo je ključni razlog zašto CYOD dobiva toliko pažnje u današnjem poslovnom svijetu. Za poduzeća, najveća prednost CYOD-a je sigurnost. Uređaji se mogu opremiti sigurnosnim značajkama kako bi osjetljivi podaci bili ispravno zaštićeni. Međutim, budući da tvrtka posjeduje uređaje, odgovornost trošenja na sigurnost i optimizaciju pada na samu tvrtku. Ovo možda nije idealno za male tvrtke ili one s ograničenim proračunom [4].

2.4. Corporate Owned, Business Only (COBO)

COBO model je model u kojem su uređaji vlasništvo tvrtke i koriste se isključivo u poslovne svrhe. Uređaje nabavlja, osigurava, osigurava i nadzire tvrtka. Uređaji su isključivo poslovni i ograničavaju korisnike u pristupu aplikacijama za osobnu upotrebu. Tvrtka odabire

i plaća uređaje, a zatim postavlja svoje najrestriktivnije sigurnosne politike. To jednostavno znači da tvrtka zaposleniku izdaje uređaj i ima vlasništvo i održavanje uređaja. Takve uređaje u potpunosti administrira i njima upravlja tvrtka, a korisnici imaju ograničen pristup dodavanju/izmjeni aplikacija.

Uređaji u COBO modelu nadziru se i zabranjuju zaposlenicima pristup aplikacijama ili web stranicama za osobnu upotrebu. Mobilni uređaji imaju instalirane samo poslovne aplikacije i zahtijevaju IT vjerodajnice za preuzimanje drugih aplikacija. Politika COBO mobilnih uređaja idealna je za organizacije koje žele poboljšati usklađenost ili sigurnost. Iako zaposlenici imaju ograničenu fleksibilnost u COBO programu, produktivnost i mobilnost zaposlenika često se povećavaju zbog odvajanja osobnog i poslovnog sadržaja.

Kad su se mobilni uređaji tek počeli pojavljivati, organizacije su upravljale njima kao i bilo kojim drugim hardverom. Prema COBO politici, tvrtke opskrbljuju radnike uređajem za korištenje i ograničavaju ovaj hardver samo za poslovnu upotrebu. Zaposlenici često nisu imali mogućnost izbora koji će uređaj imati. Za mnoge tvrtke taj je uređaj bio BlackBerry. Uspon BlackBerryja kao mobilnog uređaja poslovne razine zaglavio je u organizacijama niz godina i ostaje snažna prisutnost unutar COBO pristupa. BlackBerry je klasičan primjer uređaja koji se koriste unutar COBO okruženja. Naravno, tehnologija se znatno promijenila otkako je BlackBerry postao de facto izbor za poslovnu upotrebu [6]. Slika 3. prikazuje glavne značajke COBO modela.

	Zaposlenik	Korporacija
Vlasnik uređaja		✓
Vlasnik podataka na uređaju		✓
Održavanje uređaja		✓
Plaćanje troškova uređaja		✓
Vlasnik broja na uređaju		✓

Slika 3. Glavne značajke COBO modela

Izvor: [5]

COBO je uvelike zastario u današnjem svijetu visoke povezanosti s omogućenim oblakom jer je zaposlenicima teško pristupiti više vrsta sadržaja s istog uređaja. Organizacije koje imaju zahtjevne zahtjeve usklađenosti i mogućnost curenja podataka najvjerojatniji su kandidati za korištenje COBO-a. Ovaj pristup vraća kontrolu IT odjelima i ograničava upotrebu

pametnog telefona na aktivnosti povezane s poslom. Tvrtke učinkovito smanjuju rizik dok pružaju mogućnost mobilnosti.

3. SEGMENTACIJA POSLOVNIH I PRIVATNIH PODATAKA NA UREĐAJU

Segmentacija podataka je postupak grupiranja podataka u najmanje dva podskupa, iako će možda biti potrebno više odvajanja na velikoj mreži s osjetljivim podacima. Podatke treba grupirati na temelju slučajeva upotrebe i vrsta informacija, ali i na temelju osjetljivosti tih podataka i razine ovlasti potrebne za pristup toj vrsti informacija. Nakon što su podaci segmentirani, potrebno je uspostaviti različite sigurnosne parametre i pravila autentifikacije ovisno o segmentu podataka koji je pri ruci. Ako haker prođe tradicionalni vatrozid mreže i ta je mreža preskočila proces segmentacije podataka, haker ima pristup svemu, a ne samo malom dijelu podataka unutar segmenta. Ovaj nedostatak segmentacije podataka ostavlja više podataka ranjivim na sigurnosne provale, a također otežava pronalaženje i zaustavljanje izvora provale u širem mrežnom okruženju.

Ideja iza segmentacije podataka je kategorizirati podatke, odvojiti najosjetljivije podatke od ostalih i definirati ih kao zaštitnu površinu, a zatim primijeniti dodatne sigurnosne mjere oko svih zaštitnih površina koje su identificirane. Čak i ako dođe do proboja, najosjetljiviji podaci su zaštićeni dodatnim slojevima sigurnosnih mjera.

3.1. Segmentacija privatnih i poslovnih podataka na mobilnom uređaju

Zaštita podataka tvrtke važna je kao i uvijek, a ta zaštita počinje s uređajima koji koriste i pohranjuju te podatke. Bez obzira na uređaj i tko ga posjeduje, osigurati da podaci tvrtke ostanu zaštićeni postaje sve teže. Mnogi zaposlenici ne žele staviti na raspolaganje svoj osobni uređaj u takvo rješenje. Povjerenje u tome igra važnu ulogu, kako iz perspektive zaposlenika, tako i iz perspektive poslodavca. Mnogi zaposlenici nemaju povjerenja u MDM rješenje svoje tvrtke, uz razne brige vezane uz privatnost i kontrolu nad privatnim podacima. S gledišta poslodavca, mora postojati razina kontrole nad poslovnim podacima, bez obzira na uređaj.

Odvajanje poslovnih i privatnih profila na mobilnim uređajima nikada nije bilo lakše. Shvaćajući izazove ravnoteže između posla i privatnog života, proizvođači mobilnih uređaja dodali su niz pametnih značajki koje pomažu da privatne i poslovne aplikacije i podatke budu odvojene [7]. Jedan od načina da se to učini je sa sigurnim, autentificiranim i šifriranim područjem mobilnog uređaja ili usluge u oblaku koja izolira osjetljive korporativne podatke od osobnih podataka. Takav spremnik (kontenjer, container) omogućuje tvrtki da izolira aplikacije, onemogući određene funkcije aplikacije i daljinski obriše dijelove telefona u slučaju gubitka ili krađe. Ova se "kontejnerizacija“ može izvesti izvorno na mobilnom uređaju, putem aplikacija trećih strana ili čak u oblaku. Ovi spremnici podataka neophodni su za održavanje

sigurnog vatrozida između poslovnih i privatnih podataka. Ako se napravi kako treba, uravnotežuju sigurnost poduzeća i osobno iskustvo na pametnom telefonu. Odvajanje korporativnih i privatnih informacija mora biti jasno, a korisničko iskustvo mora biti na visokom nivou.

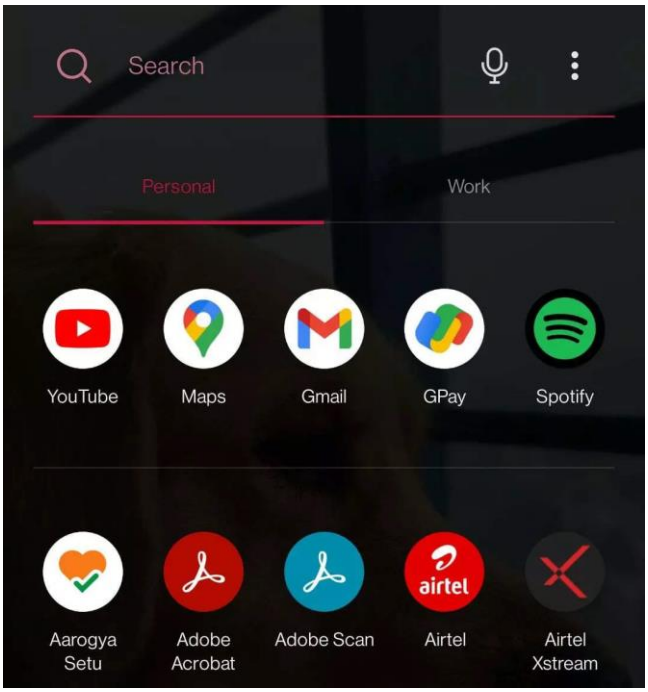
Radni profil može se vrlo jednostavno postaviti na Android uređaju za odvajanje poslovnih aplikacija i podataka od privatnih aplikacija i podataka. S radnim profilom može se sigurno i privatno koristiti isti uređaj za poslovne i privatne svrhe. Korporacija upravlja poslovnim aplikacijama i podacima dok privatne aplikacije, podaci i upotreba ostaju privatni. U nastavku su prikazani jednostavni koraci kako aktivirati radni profil na mobilnom uređaju i pristupiti radnom profilu:

- Na mobilnom uređaju potrebno je otvoriti Postavke --> Računi. Ako već postoji radni profil, bit će naveden u odjeljku Posao. Na nekim su uređajima radni profili također navedeni izravno u postavkama.
- Pristup radnom profilu: Prelazi se prstom od dna zaslona prema gore,
- Dodirne se karticu Posao,
- Odabere se aplikacija koja treba biti aktivirana.

Ukoliko na mobilnom uređaju u postavkama uređaja nije vidljiv odjeljak Posao, tj. radni profil, onda se vrlo lako napravi drugom metodom:

- Otvara se Google Play Store (Trgovinu),
- U tražilicu se upiše naziv aplikacije Google Apps Device Policy (ova aplikacija omogućuje administratoru upravljanje uređajem),
- Jednom kad je aplikacija instalirana, upisuje se odgovarajuća e-mail adresa za prijavu,

- Nakon toga, stvorit će se dva profila na mobilnom uređaju – privatni i radni (Slika 4.) [8].



Slika 4. Privatni i radni profil na mobilnom uređaju

Izvor: [9]

3.2. Android Enterprise

Prilika za Android operativne sustave na poslovnom tržištu veća je nego ikad. U svijetu postoji preko milijardu pametnih mobitela koji se koriste za posao. Prema IDC-u (International Data Corporation, vodeći globalni pružatelj usluga i analiza za informacijsku tehnologiju i telekomunikacije), preko 75% tih uređaja pokreće Android [10]. Android obuhvaća širok izbor uređaja za posebnu upotrebu i unutar poduzeća. Od namjenskih uređaja za radnike na prvoj liniji u trgovini ili na terenu, do premium uređaja za uredske zaposlenike i zdravstvene radnike, Android može podržati širok izbor slučajeva upotrebe. U svakoj industriji postoji Android uređaj koji služi za obavljanje poslovnih zadataka.

Android Enterprise je asortiman sigurnosnih i upravljačkih značajki Androida. Zajedno s API-jima (Application Programming Interface – upravljačko programsko sučelje) u oblaku koji razvojnim programerima aplikacija omogućuju izradu najučinkovitijih aplikacija i radnih procesa za bilo koji poslovni scenarij. Kako bi se nadopunile ove značajke platforme, Google također surađuje s nizom pružatelja sustava poznatih kao tvrtke za upravljanje mobilnošću

poduzeća ili EMM, koji koriste mnoge značajke Androida za poduzeća za pružanje rješenja za upravljanje mnogim IT organizacijama. Android i Android Enterprise nisu zasebni proizvodi; za razliku od Android TV (sada Google TV), Android Auto, Android Automotive, Android Wear (WearOS) ili drugih Android izdanja, Android Enterprise kao rješenje jednostavno je dio Androida. Nadalje, Android Enterprise nije upravljanje Androidom samo po sebi, to je skup API-ja koji zahtijevaju moderan EMM kako bi njima ispravno upravljali. Android Enterprise predstavljen je u Androidu 5.0 kao premosnik za pripremu Android uređaja za poslovnu upotrebu integracijom s rješenjima za upravljanje mobilnim uređajima.

Sigurnost je jedno od prvih područja oko kojih je zabrinutost najveća kada se raspravlja o proširenju mobilnosti na zaposlenike tvrtke. To je istinito kada se počne razgovarati o pristupu radnika koji rukuju osjetljivim podacima, kao što su evidencija kupaca, financijski podaci ili intelektualno vlasništvo. Android ima obrambeni i dubinski pristup sigurnosti za pružanje sveobuhvatne zaštite. Ti slojevi potječu od hardvera na OS platformu, na Google Play Protect, i konačno, API-jima za upravljanje Android poduzećima. Android uređaji koriste pouzdano izvršno okruženje (TEE – Trusted Execution Environment) za pokretanje sigurnosno osjetljivih operacija kao što je potvrda PIN-a (Personal Identification Number – osobni identifikacijski broj), pohranjivanje kriptografskih ključeva, i potvrđeno pokretanje kako bi se osiguralo da uređaji nisu ugroženi. Programeri mogu iskoristiti te alate i integrirati ih s vlastitim aplikacijama.

Operativni sustav Android prema zadanim postavkama provodi enkripciju i izolira aplikacije kroz sandboxing (praksa kibernetičke sigurnosti u kojoj se pokreće kod, promatra, analizira i kodira u sigurnom, izoliranom okruženju na mreži koja oponaša radna okruženja krajnjeg korisnika. Sandboxing je osmišljen kako bi spriječio prijetnje da uđu u mrežu i često se koristi za pregled neprovjerenog ili nepouzdanog koda. Sandboxing zadržava kôd u testnom okruženju kako ne bi zarazio ili oštetio glavno računalo ili operativni sustav.) koristeći Linux.

Google Play Protect objedinjuje skeniranje aplikacija na uređaju uz analizu aplikacija temeljenu na oblaku i strojno učenje za borbu protiv potencijalno štetnih aplikacija od instaliranja na Android uređaje.

Konačno, Android Enterprises API-ji za upravljanje omogućava korporaciji da provede svoje IT politike na uređaju te osiguravaju dodatnu kontrolu nad uređajima koji se koriste unutar korporacije. U kombinaciji s naprednim sigurnosnim značajkama, Google je također uložio velika sredstva kako bi osigurao što jednostavnije upravljanje mobilnim krajnjim točkama. U srži jednostavnog upravljanja je centraliziranje sposobnosti tako da se cjelokupno upravljanje može postići uz što je moguće manje troškova. Google je stvorio API za upravljanje

Androidom kako bi se pružateljima EMM-a omogućilo stvaranje širokog spektra pouzdanih alata jednostavnih za korištenje za upravljanje korporativnim implementacijama Androida.

Kao dio centraliziranog upravljanja, administratori mogu odlučiti hoće li uspostaviti radni profil. Ovo stvara poseban prostor na uređaju za poslovne aplikacije koji je odvojen od svih osobnih aplikacija koje je krajnji korisnik možda instalirao. Neovisno o tome jesu li uređaji u vlasništvu tvrtke ili tvrtke podržava BYOD politiku donošenja vlastitog uređaja, radni profil omogućuje krajnjim korisnicima instaliranje vlastitih aplikacija bez dovođenja korporativnih podataka u opasnost. IT administratori mogu odlučiti hoće li dopustiti krajnjim korisnicima dijeljenje podataka između osobnih i radnih aplikacija, ili potpuno odvojiti radne podatke od osobnih. IT administratori također mogu izbrisati radni profil te time učinkovito ukloniti sve korporativne aplikacija s uređaja bez brisanja podataka uređaja u cijelosti. Za uređaje u vlasništvu tvrtke, IT administratori također mogu koristiti radni profil za pružanje segmentacije podataka dok imaju kontrolu nad širim funkcijama uređaja kao što su vraćanje uređaja na tvorničke postavke ili uspostavljanje popisa dopuštenih ili nedopuštenih aplikacija. Konačno, IT administratori mogu odabrati potpuno upravljanje uređajem bez osobnih aplikacija [10].

Osim uspostavljanja vlasništva i modela aplikacije za poslovne uređaje, Android Enterprise nudi niz drugih značajki koje mogu pomoći u implementaciji Androida unutar organizacije. Administratori mogu automatski izbaciti aplikacije i ažuriranja aplikacija na uređaje tijekom godine, koristeći upravljanje Google Playom i ograničiti korisničku instalaciju aplikacija samo na Google Play. I programeri i IT administratori mogu daljinski konfigurirati poslovne aplikacije tijekom godine. IT administratori mogu kontrolirati putem popisa dopuštenih ili zabranjenih instalacija aplikacija na uređaj. Oni mogu postaviti prilagođena pravila za sprječavanje gubitka podataka i kontrolirati dijeljenje informacija između radnog i osobnog profila uređaja.

I konačno, imaju kontrolu nad računima koji se mogu dodati na uređaj. Ovakve značajke nude veliku fleksibilnost za IT administratore u smislu prilagođavanja ponašanja uređaja njihovim potrebama. Ali ta promjena u ponašanju može uzrokovati da se aplikacije ponašaju na neočekivani način, osobito ako programeri to ne uzmu u obzir [10].

Korištenje Android Enterprisea donosi zaista mnoge benefite za tvrtke, ali nužno je biti upoznat s onim što Android Enterprise nudi i primijeniti najbolje prakse pri njegovom korištenju što na kraju omogućava bolje korištenje uređaja za poslovne zadatke.

4. MOGUĆNOSTI PLATFORMI ZA UPRAVLJANJE UREĐAJIMA I PODACIMA

Posljednjih su godina mobilni uređaji postali sveprisutni u poslovnoj upotrebi. Korporacije i zaposlenici oslanjaju se na mobilne uređaje kao što su pametni telefoni, tableti i prijenosna računala za širok izbor zadataka. A kako je rad na daljinu postao bitan, mobilni uređaji postali su sastavni dio većine organizacija — ključni alati za produktivnost i učinkovitost. No budući da poslovni mobilni uređaji pristupaju kritičnim poslovnim podacima, mogu ugroziti sigurnost ako su hakirani, ukradeni ili izgubljeni. Stoga je važnost upravljanja mobilnim uređajima evoluirala tako da IT administratori koji brinu o sigurnosti sada imaju zadatak osigurati, upravljati i osigurati mobilne uređaje unutar svojih korporativnih okruženja. Upravljanje mobilnim uređajima (MDM) dokazana je metodologija i skup alata koji se koriste za pružanje alata i aplikacija za mobilnu produktivnost zaposlenika, a istodobno čuvaju korporativne podatke sigurnima [11]. Sa MDM platformom, IT i sigurnosni odjeli mogu upravljati svim uređajima tvrtke, bez obzira na njihovu vrstu ili operativni sustav. Učinkovita MDM platforma pomaže u održavanju sigurnosti svih uređaja dok zaposlenike održava fleksibilnima i produktivnima.

MDM je rješenje koje koristi softver kao komponentu kod mobilnih uređaja dok istovremeno štiti imovinu korporacije, kao što su podaci. Korporacije prakticiraju MDM primjenom softvera, procesa i sigurnosnih pravila na mobilne uređaje i njihovu upotrebu. Osim upravljanja inventarom uređaja i pružanja usluga, MDM rješenja štite aplikacije, podatke i sadržaj uređaja. U tom su smislu MDM i mobilna sigurnost slični. Međutim, MDM je pristup usmjeren na uređaj, dok su se mobilna sigurnost i objedinjeno upravljanje krajnjim točkama razvili u stav usmjeren na korisnika.

U MDM programu zaposlenici mogu dobiti namjenski radni uređaj, kao što su prijenosna računala ili pametni telefoni, ili imati daljinski upisan osobni uređaj. Osobni uređaji dobivaju pristup temeljen na ulogama poslovnim podacima i e-pošti, siguran VPN (Virtual Private Network – virtualna privatna mreža), GPS (Global Positioning System – globalni položajni sustav) praćenje, aplikacije zaštićene lozinkom i drugi MDM softver za optimalnu sigurnost podataka. Softver MDM zatim može nadzirati ponašanje i poslovne podatke na prijavljenim uređajima. A sa sofisticiranijim MDM rješenjima, mogu se analizirati strojnim učenjem i umjetnom inteligencijom. Ovi alati osiguravaju zaštitu uređaja od zlonamjernog softvera i drugih kibernetičkih prijetnji.

Na primjer, tvrtka može dodijeliti prijenosno računalo ili pametni mobitel zaposleniku, unaprijed programiran s podatkovnim profilom, VPN-om i drugim potrebnim softverom i aplikacijama. U ovom scenariju, MDM nudi najveću kontrolu poslodavcu. Pomoću MDM alata

poduzeća mogu pratiti, nadzirati, rješavati probleme i čak obrisati podatke uređaja u slučaju krađe, gubitka ili otkrivene povrede [12].

Politike MDM-a odgovaraju na pitanja o tome kako će organizacije upravljati mobilnim uređajima i upravljati njihovom upotrebom. Kako bi konfigurirala i objavila svoje politike i procese, korporacije će postavljati pitanja, kao što su:

- Trebaju li uređaji zaštitu šifrom?
- Trebaju li kamere biti onemogućene prema zadanim postavkama?
- Je li važna WiFi (Wireless Fidelity – tehnologija bežičnog umrežavanja) veza?
- Koje mogućnosti prilagodbe nudi uređaj?
- Trebaju li uređaji imati aktiviranu lokaciju?

4.1. Komponente MDM-a

Praćenje uređaja – svaki uređaj prijavljen ili izdan od strane poduzeća može se konfigurirati da se uključi GPS praćenje te drugi programi. Programi omogućuju IT stručnjacima korporacija da prate, ažuriraju i rješavaju probleme uređaja u stvarnom vremenu. Također mogu otkriti i prijaviti visokorizične uređaje, pa čak i daljinski zaključati ili obrisati uređaj ako je izgubljen ili ukraden.

Mobilno upravljanje – IT odjeli nabavljaju, postavljaju, upravljaju i podržavaju mobilne uređaje za zaposlenike, kao što je rješavanje problema s funkcionalnošću uređaja. Ovi odjeli osiguravaju da svaki uređaj dolazi s potrebnim operativnim sustavima i aplikacijama za zaposlenike — uključujući aplikacije za produktivnost, sigurnost i zaštitu podataka, sigurnosno kopiranje i obnavljanje.

Sigurnost aplikacija – sigurnost aplikacija može uključivati omotavanje aplikacije, u kojem IT administrator primjenjuje sigurnosne ili upravljačke značajke na aplikaciju. Zatim se ta aplikacija ponovno postavlja kao kontejnerski program. Ove sigurnosne značajke mogu odrediti je li provjera autentičnosti korisnika potrebna za otvaranje aplikacije; mogu li se podaci iz aplikacije kopirati, zalijepiti ili pohraniti na uređaj; i može li korisnik dijeliti datoteku.

Upravljanje identitetom i pristupom (IAM – Identity and Access Management) – sigurno upravljanje mobilnim uređajima zahtijeva upravljanje identitetom i pristupom (IAM). IAM omogućuje korporaciji upravljanje korisničkim identitetima povezanim s uređajem. Pristup svakog korisnika unutar korporacije može se u potpunosti regulirati.

Sigurnost krajnje točke – sigurnost krajnjih točaka obuhvaća sve uređaje koji pristupaju korporativnoj mreži, uključujući nosive uređaje, senzore Interneta stvari (IoT –

Internet of Things) i netradicionalne mobilne uređaje. Sigurnost krajnje točke može uključivati standardne mrežne sigurnosne alate kao što su antivirusni softver, kontrola pristupa mreži, odgovor na incidente i sigurnost u oblaku.

4.2. IBM Security MaaS360 with Watson MDM

U današnje vrijeme radno mjesto može biti bilo gdje: kod kuće, u uredskom prostoru pa čak i na ulici. Ali zajedno s napretkom tehnologije, kibernetički kriminalci postali su sofisticiraniji. Zato tvrtke trebaju sigurna rješenja upravljanja uređajima i podacima koja fleksibilno isporučuju aplikacije, sadržaj i resurse na više uređaja. IBM MaaS360 je platforma za upravljanje uređajima i podacima korporacija koju je jednostavno implementirati. Uz IBM MaaS360, korporacije mogu upravljati i zaštititi svoje mobilne uređaje, aplikacije i sadržaj s fleksibilnim rješenjima kako bi zadovoljile svoje specifične potrebe. I to se ne odnosi samo na tablete i pametne telefone. Moguće je upravljati prijenosnim računalima, stolnim računalima i IoT uređajima. Watsonova umjetna inteligencija i prediktivna analitika su funkcije IBM Maas360 MDM-a koje upozoravaju o potencijalnim prijetnjama te pružaju sanaciju kako bi se spriječile sigurnosne povrede i smetnje.

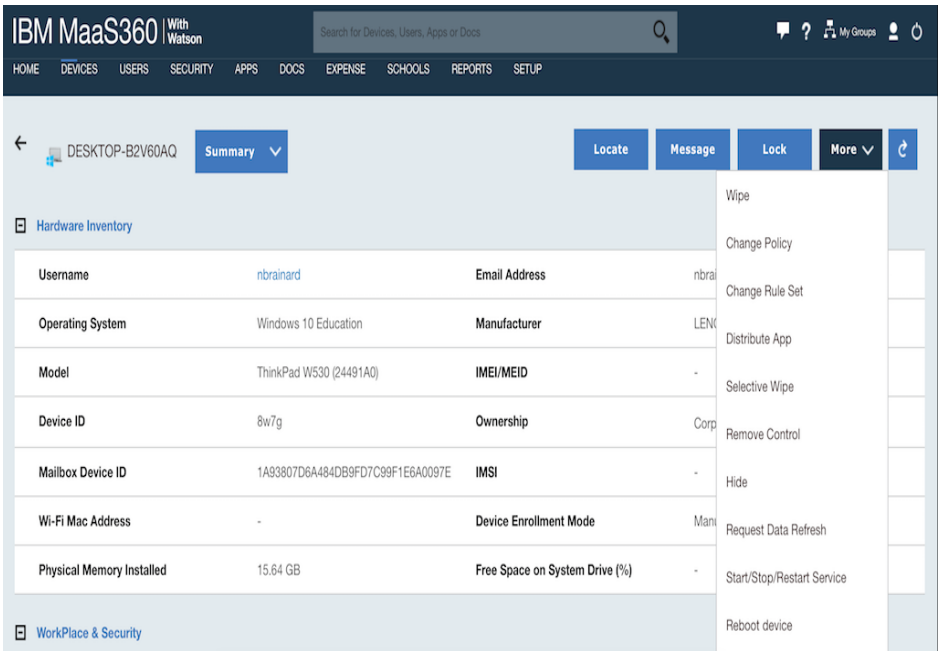
MaaS360 osigurava aplikacije, sadržaj i podatke kako bi bilo moguće upravljanje uređajima na daljinu. Omogućuje se obrana od prijetnji na razini korporacije, IT administratori mogu otkriti prijetnje i obaviti sanaciju. Moguće je šifriranje, sprječavanje neovlaštenog kopiranja i prosljeđivanja e-pošte i dokumenata. Tisuće korporacija diljem svijeta, od multinacionalnih korporacija do malih i srednjih poduzeća, oslanjaju se na ovaj softver kao temelj za svoje mobilne inicijative—pomažući u omogućavanju aplikacija i sadržaja koji su korisnicima potrebni za produktivnost, a istovremeno održavaju sigurnost podataka i osobnu privatnost [13].

4.2.1. Upravljanje i alati

Za razliku od ostalih MDM rješenja, IBM je opremio MaaS360 potpuno prilagodljivom konzolom za upravljanje koja omogućuje premještanje stvari poput određenih upozorenja unutar područja My Alert Center. Prema zadanim postavkama, početni zaslon uključuje ploču Moj savjetnik koju pokreće IBM-ova umjetna inteligencija Watson AI (Artificial Intelligence). Ovo će pokazati sva sigurnosna upozorenja ili upozorenja o riziku koje sustav otkrije, kao što su nezakrpani uređaji koji predstavljaju uobičajenu i opasnu prijetnju i za korisnika i za korporativnu mrežu. Još jedna zgodna vizualizacija je My Activity Feed koji prikazuje zadnjih osam radnji administratora kao veze na koje se može kliknuti. Prelaskom miša iznad veze prikazuje se brzi sažetak radnje, dok klik na vezu vodi na stranicu s detaljima za taj događaj.

Za razliku od većine konkurencije u malim tvrtkama, izvješćivanje je jedna od glavnih značajki MaaS360. To je zbog povezanosti s IBM-ovom Watson platformom za strojno učenje i umjetnu inteligenciju. Ovo je spojeno u nekoliko jedinstvenih mogućnosti, uključujući Mobile Metrics za MaaS360. To omogućuje usporednu analizu u oblaku za implementaciju uređaja. Ovaj alat analizira okruženje tražeći sigurnosne probleme i nudi usporedne informacije u domenama specifičnim za industriju. Ove smjernice pomažu administratorima da konfiguriraju pravila u skladu s industrijskim normama. Otprilike jedina mana koju se može spomenuti o izvješćivanju jest ograničena dostupna prilagodba. Međutim, čak i uz to, MaaS360 zadržava značajno vodstvo u izvješćivanju u odnosu na manju konkurenciju, poput AppTec360.

Još jedna pomoć u izvješćivanju i svakodnevnom upravljanju je napredni alat za pretraživanje, koji omogućuje brzo pretraživanje uređaja na temelju više kriterija. Na stranici Inventar uređaja mogu se brzo poduzeti radnje na pojedinačnim ili grupama uređaja. Ovo je zgodno kada je potrebno poslati grupnu poruku ili potencijalno onemogućiti neke funkcije uređaja zbog korporativnih zahtjeva [14]. Klasičan izgled početne stranice MaaS360 prikazan je na Slici 5.



Slika 5. Izgled početne strane MaaS360

Izvor: [15]

4.2.2. Značajke MaaS360

Prvo, MaaS360 je cloud (oblak) platforma. Svi front-end (korisničko sučelje, itd.) i back-end sustavi (aplikacije, baze podataka, naplata, itd.) su uvijek dostupni. Dakle, korisnici ne moraju čekati posluživanje usluge. Oblak MaaS360 elastično se širi s korisnicima i ne zahtijeva

nikakve preduvjetne operacije da korisnik prijeđe s 1 uređaja na 10 000 ili više uređaja prijavljenih čak i u vrlo kratkom vremenskom okviru.

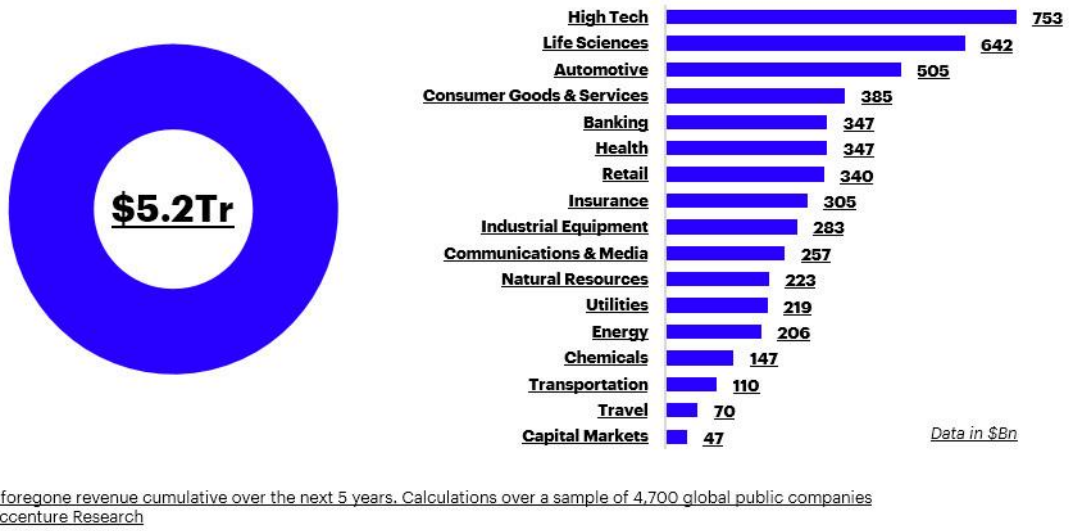
Drugo, tehnologija MaaS360 Cloud Extender omogućuje korporacijama da samostalno integriraju korporativne sustave s MaaS360 oblakom na siguran način bez ikakvih promjena konfiguracije korporativnog vatrozida i mrežnih konfiguracija [16].

Treće, korisničko iskustvo MaaS360 ima integrirane i vođene upute za korisnike, čime se stekla reputacija jednostavnosti i intuitivnosti u postavljanju i svakodnevnoj upotrebi.

5. ANALIZA SIGURNOSNIH PRIJETNJI KORPORATIVNIM PODACIMA

Prijetnja sigurnosti podataka je svaka radnja koja bi mogla ugroziti povjerljivost, cjelovitost ili dostupnost podataka. Sigurnost podataka organizira se prema tri sigurnosna zahtjeva — povjerljivost, integritet i raspoloživost. Povjerljivost podataka uključuje sprječavanje pristupa osjetljivim podacima neovlaštenim stranama, bilo unutarnjim ili vanjskim. Cjelovitost podataka uključuje sprječavanje neželjenih izmjena ili brisanja podataka. Raspoloživost podataka osigurava da vrijednim podacima uvijek mogu pristupiti oni kojima su potrebni, unutar i izvan korporacije [17].

Prijetnje sigurnosti podataka mogu doći iz različitih izvora, uključujući hakere, prijetnje iznutra, prirodne katastrofe i ljudske pogreške. Povrede podataka mogu imati ozbiljne posljedice za tvrtke i potrošače, uključujući financijske gubitke, ugrožene identitete i narušenu reputaciju. Kompanije, velike i male, često zanemaruju prijetnju koja proizlazi iz kibernetičkog kriminala. Kibernetički kriminal postaje sve veća prijetnja, budući da se predviđa da će troškovi štete od kibernetičkog kriminala koštat tvrtke 5,2 trilijuna dolara u roku od 5 godina (Slika 6.) [18].



Slika 6. Šteta kibernetičkog kriminala izražena u američkim dolarima

Izvor: [19]

Mala poduzeća jednako su izložena prijetnjama kibernetičkoj sigurnosti kao i velika poduzeća. Uobičajena pogrešna pretpostavka za mala poduzeća je ideja da je tvrtka premala da bi je hakeri napali ili uopće primijetili. Kako napadači sve više automatiziraju napade, lako im je ciljati stotine, ako ne i tisuće malih poduzeća odjednom. Male tvrtke često imaju manje strogu tehnološku obranu, manje su svjesne prijetnji te imaju manje vremena i resursa za kibernetičku sigurnost. To ih čini lakšom metom za hakere nego veće korporacije. Ali, u isto

vrijeme, one nisu ništa manje unosne mete. Čak i najmanja poduzeća mogu baratati velikim svotama novca ili imati pristup ogromnim količinama podataka o klijentima. Male tvrtke također često rade s većim tvrtkama, pa ih hakeri mogu koristiti kao način za ciljanje tih tvrtki. Mala poduzeća vjerojatno mogu najviše izgubiti ako budu pogođena štetnim kibernetičkim napadom. Nedavno izvješće otkrilo je da tvrtke s manje od 500 zaposlenika gube u prosjeku 2,5 milijuna dolara po napadu [20]. Gubitak ove količine novca poguban je za mala poduzeća te dovodi do reputacijske štete do koje dolazi zbog kibernetičkog napada.

Postoje mnoge opipljive prednosti BYOD-a, uključujući smanjene troškove opreme, povećanu učinkovitost i zadovoljstvo zaposlenika, smanjenu kvadraturu uredskog prostora (ako radnici prijeđu izvan lokacije) i smanjeno opterećenje IT osoblja jer će zaposlenici sami održavati svoju opremu. Međutim, uz ove prednosti dolazi i rizik. Uređaji u vlasništvu zaposlenika potencijalno mogu izložiti sigurnosne ranjivosti koje IT osoblje ne nadzire izravno ili ih ne rješavaju korporativna antivirusna rješenja. Ovdje dolazi do potrebe za upravljanjem mobilnim uređajima (MDM).

Privatni uređaji koje koriste zaposlenici za obavljanje poslovnih zadataka su pod velikom prijetnjom. Takvi uređaji su iznimna opasnost za očuvanje korporativnih podataka jer često nisu dovoljno zaštićeni, a imaju pristup važnim informacijama korporacije. MDM rješenja su ta koja olakšavaju korporacijama borbu sa sigurnosnim prijetnjama. U nastavku će biti analizirane sigurnosne prijetnje korporativnim podacima i koliko zapravo MDM pomaže u takvim borbama.

5.1. Socijalni inženjering

Socijalni inženjering je vrsta napada koja se oslanja na navođenje ljudi na otkrivanje osjetljivih informacija. To se može učiniti putem mobitela ili e-pošte. Napadi socijalnim inženjeringom često se koriste za dobivanje pristupa povjerljivim podacima ili sustavima. Socijalni inženjering je taktika manipulacije, utjecaja ili obmane žrtve kako bi se stekla kontrola nad računalnim sustavom ili kako bi se ukrali osobni i financijski podaci. Koristi se psihološkom manipulacijom kako bi se prevarili korisnici da naprave sigurnosne pogreške ili odaju osjetljive informacije. Cilj je zadobiti povjerenje meta, a zatim potaknuti žrtve na poduzimanje nesigurnih radnji kao što je otkrivanje osobnih ili poslovnih podataka ili otvaranje privitaka koji mogu biti zlonamjerni.

5.2. Phishing napadi

Najveća, najštetnija i najraširenija prijetnja s kojom se mala poduzeća suočavaju su **phishing napadi**. Istraživanje IBM-a je utvrdilo da porast od 2% u phishing napadima između 2019. i 2020., djelomično potaknut COVID-19 pandemijom. CISCO-vo izvješće o trendovima sigurnosnih prijetnji za 2021. je uputilo da je barem jedna osoba kliknula poveznicu za krađu identiteta u oko 86% organizacija. 90% svih kršenja s kojima se organizacije suočavaju zauzimaju phishing napadi. Čine više od 12 milijardi dolara poslovnih gubitaka [21]. Phishing napadi se događaju kada se napadač pretvara da je pouzdani kontakt i navodi korisnika da klikne zlonamjernu poveznicu, preuzme zlonamjernu datoteku ili mu da pristup osjetljivim informacijama, detaljima računa ili vjerodajnicama. Napadi krađe identiteta posljednjih su godina postali mnogo sofisticiraniji, a napadači postaju sve uvjerljiviji pretvarajući se da su legitimni poslovni kontakti kako bi ukrali lozinke računa poslovne e-pošte od zaposlenika na visokoj razini, a zatim koristili te račune za lažno traženje isplata od zaposlenika.

Posebno su rizični privatni uređaji zaposlenika koji imaju slabu zaštitu ili nemaju MDM rješenja jer onda napadači imaju vrlo lagan posao. Uz MDM rješenje, čak i ako zaposlenik na neki način omogući pristup napadaču, MDM će znatno otežati proboj informacija.

5.3. Malware napadi

Malware je zlonamjerni softver, odnosno svaki štetan softver koji je na računalo instaliran od trećih strana za izvođenje zlonamjernih zadataka. Malware je velika prijetnja s kojom se poduzeća suočavaju. Obuhvaća razne cyber prijetnje poput trojanaca (trojanski konj ili trojanac je vrsta zlonamjernog koda ili softvera koji izgleda legitimno, ali može preuzeti kontrolu nad računalom. Trojanac je dizajniran da šteti, poremeti, ukrade ili općenito nanese neku drugu štetnu radnju podacima ili mreži.) i virusa [22]. Zlonamjerni softver obično dolazi od zlonamjernih preuzimanja web stranica, neželjene e-pošte ili povezivanja s drugim zaraženim uređajima. Ovi napadi su posebno štetni za mala poduzeća jer mogu onesposobiti uređaje, što zahtijeva skupe popravke ili zamjene. Oni također mogu napadačima dati stražnja vrata za pristup podacima, što može dovesti klijente i zaposlenike u opasnost. Veća je vjerojatnost da će mala poduzeća zapošljavati ljude koji za rad koriste vlastite uređaje jer to pomaže u uštedi vremena i troškova. To, međutim, povećava njihovu vjerojatnost da će biti izloženi napadu zlonamjernog softvera, budući da je veća vjerojatnost da će osobni uređaji biti izloženi riziku od zlonamjernih preuzimanja [23].

Uz MDM rješenja, malware napadi će biti brže otkriveni i otklonjeni. U nastavku su navedena neka od MDM rješenja koja znatno pomažu u sprječavanju malware napada:

- **Upravljanje pristupom poštanskim sandučićima** – potrebno je osigurati da samo uređaji kojima upravlja tvrtka mogu pristupiti poštanskim sandučićima koji sadržavaju korporativne podatke.
- **Kontrola preuzimanja –** samo aplikacije i dokumenti odobreni za tvrtke smiju biti instalirani/preuzeti na uređajima tvrtke. Uz MDM rješenja moguće je staviti na listu blokirane aplikacije koje nisu odobrene i ograničiti pristup korisnicima na samo odabrane aplikacije stavljajući ih na popis dopuštenih aplikacija.
- **Siguran pristup mreži** – onemogućava pristup javnim Wi-Fi mrežama i osigurava da se korporativnim podacima pristupa samo putem VPN-a. Također moguće je blokirati određene web stranice.

5.4. Ransomware

Ransomware je jedan od najčešćih kibernetičkih napada koji svake godine pogađa tisuće tvrtki. Ransomware uključuje šifriranje podataka tvrtke tako da ih se ne može koristiti ili pristupiti, a zatim prisiljavanje tvrtke da plati otkupninu za otključavanje podataka. To tvrtke stavlja pred težak izbor – platiti otkupninu i potencijalno izgubiti ogromne svote novca ili ugroziti usluge gubitkom podataka. Ransomware se širi zlonamjernim privicima e-pošte, zaraženim softverskim aplikacijama, zaraženim vanjskim uređajima za pohranu, zaraženim web stranicama i ranjivostima u često korištenim aplikacijama. Podatak iz 2018. godine govori da su male tvrtke 71% napada ransomwareom, s prosječnom potražnjom za otkupninom od

116 000 dolara [24]. Na slici 7. prikazan je klasičan izgled obavijesti koju dobije žrtva ransomware napada.

Slika 7. Primjer obavijesti korisniku u slučaju Ransomware napada

Izvor: [25]

Ransomware napadi su ogromna prijetnja korporacijama, a pogotovo ako zaposlenici nemaju potrebnu zaštitu na vlastitim mobilnim uređajima. Svaka korporacija koja ne ulaže u zaštitu mobilnih uređaja zaposlenika riskira ogromne gubitke, kako u novcima, tako i u gubitku važnih korporativnih podataka. Zato je potrebno osigurati maksimalnu zaštitu mobilnih uređaja, a putem MDM rješenja moguće je poduzeti sljedeće korake:

- **Virtualno ograđivanje** – MDM rješenje koristi lokacije i identifikatore Wi-Fi usluga te vrijeme za stvaranje granica i zaštitu podataka. Moguće je postaviti "okidač ograde" koji će biti obavještavati IT tim kada uređaj uđe ili napusti granice.
- **Izvješćivanje** – izvješćivanje omogućuje da se statistika o svim uređajima u vlasništvu tvrtke pretvori u uvide i pomogne u zaštiti i poboljšanju poslovanja.
- **Mobile Web Security** – ovaj dio MDM rješenja omogućuje blokiranje ključnih riječi, domena i više, što znatno smanjuje mogućnost ransomware napada.

5.5. DDoS napadi

DDoS (Distributed Denial-of-Service – distribuirano uskraćivanje usluge) napadi su napadi u kojima napadač preplavljuje poslužitelja internetskim prometom kako bi se korisnicima spriječio pristup internetskim uslugama i stranicama. Motivacije za provođenje DDoS-a uvelike variraju, kao i tipovi pojedinaca i organizacija koji žele izvršiti ovaj oblik kibernetičkog napada. Neke napade izvode nezadovoljni pojedinci koji žele srušiti poslužitelje tvrtke samo kako bi dali izjavu, zabavili se iskorištavanjem sigurnosnih slabosti ili izrazili neodobravanje. Drugi distribuirani napadi uskraćivanja usluge financijski su motivirani, kao što su konkurenti koji ometaju ili zatvaraju mrežne operacije druge tvrtke kako bi u međuvremenu ugrozili posao [26]. Drugi uključuju iznudu, u kojoj počinitelji napadaju tvrtku i instaliraju ransomware na njihove poslužitelje, a zatim ih prisiljavaju da plate veliku financijsku svotu kako bi se šteta poništila. DDoS napadi obično traju između 6 sati i 24 sata i osmišljeni su da preplave tvrtke velikim količinama prometa na web stranici iz više različitih izvora, posljedično drastično usporavajući funkcionalnost web stranice. U većini slučajeva, promet je toliko velik da su ključne usluge za tvrtku prisiljene biti izvan mreže [27].

Tvrtke bez dobre zaštite su vrlo lak plijen napadačima. Privatni uređaji koje koriste zaposlenici su „ulaz“ za napadače kod DDoS napada. Svaki nezaštićeni uređaj predstavlja prijetnju korporativnim podacima i ugrožavanje poslovanja. Korporacije moraju biti jako oprezne kod davanja pristupa svojoj mreži uređajima zaposlenika. Nužni su osigurati zaštitu i MDM rješenja jer neće dobro završiti za njih.

5.6. Botnet mreža

Botnet ("mreža robota") je mreža računala zaraženih zlonamjernim softverom koja su pod kontrolom jedne strane koja napada. Botnet je skup uređaja povezanih s internetom, uključujući računala, mobilne uređaje, poslužitelje i IoT uređaje koji su zaraženi i daljinski kontrolirani uobičajenom vrstom zlonamjernog softvera. Upravo zbog takvih uređaja koji imaju pristup mreži korporacije, nužno je osigurati potrebnu zaštitu kako se ne bi ugrozili podaci korporacije.

Tipično, botnet malware traži ranjive uređaje diljem interneta. Cilj napadača koji stvaraju botnet je zaraziti što više povezanih uređaja, koristeći računalnu snagu i resurse tih uređaja za automatizirane zadatke koji općenito ostaju skriveni korisnicima uređaja. Napadači koji kontroliraju ove botnetove koriste ih za slanje neželjene e-pošte, sudjelovanje u kampanjama prijevara klikova i generiranje zlonamjernog prometa za distribuirane napade uskraćivanja usluge [28].

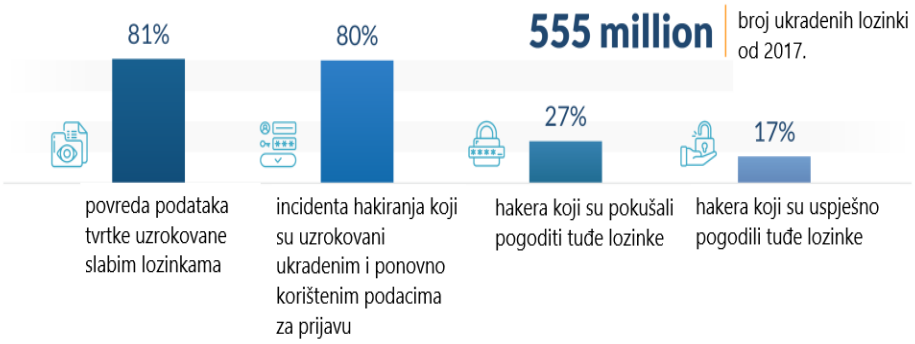
5.7. Unutarnje prijetnje

Još jedna velika prijetnja s kojom se mala poduzeća suočavaju je **unutarnja prijetnja**. Unutarnja prijetnja je rizik za organizaciju koji je uzrokovan radnjama zaposlenika, bivših zaposlenika, poslovnih suradnika ili suradnika. Ovi akteri mogu pristupiti kritičnim podacima o korporaciji i uzrokovati štetne učinke zbog pohlepe ili zlobe, ili jednostavno zbog neznanja i nemara. To je rastući problem i može ugroziti zaposlenike i klijente ili nanijeti financijsku štetu tvrtki. Unutar malih poduzeća, unutarnje prijetnje rastu jer sve više zaposlenika ima pristup višestrukim računima koji sadrže više podataka. Istraživanje je pokazalo da je 62% zaposlenika izjavilo da ima pristup računima koji vjerojatno nisu trebali [29].

Zbog ovakvog problema svaka tvrtka mora uložiti u zaštitu svojih podataka jer i zaposlenici predstavljaju opasnost. Njihov pristup podacima je rizičan, ali bez obzira na pristup, potrebno je osigurati alate koji neće dopustiti da zaposlenik napusti tvrtku s ukradenim podacima koje je pohranio na svoj privatni uređaj.

5.8. Slabe lozinke

Prijetnja s kojom se mala poduzeća suočavaju su zaposlenici koji koriste **slabe lozinke** ili lozinke koje je lako pogoditi. Mnoge male tvrtke koriste više usluga temeljenih na oblaku, za koje su potrebni različiti računi. Ove usluge često mogu sadržavati osjetljive podatke i financijske informacije. Korištenje lozinki koje je lako pogoditi ili korištenje istih lozinki za više računa može dovesti do ugrožavanja ovih podataka. Tvrtke su često izložene riziku od kompromisa koji dolaze od zaposlenika koji koriste slabe lozinke, zbog općeg nedostatka svijesti o šteti koju mogu prouzročiti. Prosječno 19% zaposlenika (slika 8.) koristi lozinke koje je lako pogoditi ili dijeli lozinke na više računa [29].



Slika 8. Statistika slabih lozinki

Izvor: [30]

6. METODE ZAŠTITE KORPORATIVNIH PODATAKA

U digitalnom dobu u kojem se sva papirologija, zapisi i projekti u tijeku odvijaju na lokalnim mrežama i mrežama u oblaku, ništa nije važnije od kibernetičke sigurnosti za zaštitu poslovnih podataka. Korporacije su stalno u posjedu ogromne količine podataka koja raste i većina njih je privatna. Pripada kupcima, zaposlenicima ili ako se radi o vlasničkim idejama, samoj korporaciji. Svaka vrsta podataka koja se pohrani nije vrijedna samo korporacijama, nego i napadačima. Bilo koji haker će pokušati sve što im padne na pamet da ukrade važne podatke. Kompanije, velike i male, često zanemaruju prijetnju koja proizlazi iz kibernetičkog kriminala. Kibernetički kriminal postaje sve veća prijetnja, budući da se predviđa da će troškovi štete od kibernetičkog kriminala do 2025. dosegnuti 15 trilijuna dolara [31]. Kršenje sigurnosti podataka može ozbiljno naštetiti korporacijama, posebno po pitanju reputacije.

Korporacije koje imaju uveden model BYOD-a moraju biti svjesne i rizika. Svaki zaposlenik koji koristi privatni uređaj za pristup korporaciji i njenim podacima ujedno predstavlja i veliku opasnost za sigurnost tih osjetljivih podataka. Na primjer, zaposlenik može pristupati raznim web stranicama, servisima i preuzimati aplikacije koje nisu sigurne a mogu naštetiti korporativnim podacima ukoliko nije jasno definirana BYOD politika.

Privatni uređaji zaposlenika koji imaju pristup korporativnim podacima su ogromna prijetnja sigurnosti korporacija ako nemaju neko MDM rješenje zaštite podataka. Ukoliko zaposlenici u slobodno vrijeme nisu osviješteni o opasnostima za podatke, ti podaci vrlo lako mogu biti ugroženi.

Zaštita mobilnih uređaja odnosi se na mjere osmišljene za zaštitu osjetljivih informacija pohranjenih na prijenosnim računalima, pametnim telefonima, tabletima, nosivim i drugim prijenosnim uređajima. Temeljni aspekt sigurnosti mobilnih uređaja sprječava neovlaštene korisnike da pristupe poslovnoj mreži. U modernom IT okruženju, ovo je ključni aspekt mrežne sigurnosti. Postoje mnogi alati za sigurnost mobilnih podataka, osmišljeni za zaštitu mobilnih uređaja i podataka identificiranjem prijetnji, stvaranjem sigurnosnih kopija i sprječavanjem prijetnji na krajnjoj točki da dosegnu korporativnu mrežu. IT osoblje koristi softver za sigurnost mobilnih podataka kako bi omogućilo siguran mobilni pristup mrežama i sustavima. Kako bi se smanjili rizici, važno je znati koje su najbolje metode zaštite korporativnih podataka.

6.1. Identificiranje osjetljivih podataka i klasifikacija

Korporacija mora točno znati koje vrste podataka ima kako bi ih učinkovito zaštitila. Za početak, sigurnosni tim skenira spremišta podataka i pripremi izvješća o nalazima. Kasnije se

organiziraju podaci u kategorije na temelju njihove vrijednosti za korporaciju. Klasifikacija se može ažurirati kako se podaci stvaraju, mijenjaju, obrađuju ili prenose. Što su podaci rizičniji, potrebno im je pružiti veću zaštitu. Osjetljive podatke je potrebno pomno čuvati, dok se podacima niskog rizika može priuštiti manja zaštita. Glavni razlog za ovakav tip procjene je isplativost, budući da bolja sigurnost podataka znači veći trošak. Međutim, to je dobar test za utvrđivanje koje podatke treba pomnije čuvati i čini cijeli sustav obrade podataka učinkovitijim. Dvije su osi na kojima bi se trebala temeljiti procjena rizika: potencijalna ozbiljnost u slučaju povrede podataka i vjerojatnost povrede. Što je veći rizik na svakoj od ovih komponenti, to su podaci osjetljiviji. Ove će procjene često zahtijevati pomoć službenika za zaštitu podataka jer pogrešno okarakterizirani podaci, ako se izgube, mogli bi se pokazati katastrofalnima.

Potrebno je prepoznati i one uređaje zaposlenika koji nemaju MDM rješenja jer su onda podaci izravno u opasnosti. Takvi uređaji predstavljaju ulaz hakerima i pristup osjetljivim korporativnim podacima. Upravo zbog toga, svaka korporacija bi trebala obavezno poduzeti mjere zaštite podataka i uvesti MDM rješenja.

6.2. Enkripcija podataka

Velike tvrtke ne rukuju samo velikim brojem podataka, već i različitim podacima. Ogromna količina podataka s kojim raspolažu, čini ih glavnim metama napadača. Od šifriranih tvrdih diskova, USB-ova (Universal Serial Bus) i pametnih telefona koje zaposlenici koriste do podataka šifriranih prije prijenosa u oblak ili na prijenosne uređaje, enkripcija je postala ključna za zaštitu osjetljivih podataka tvrtke i sigurnost podataka o klijentima. Dobro šifrirani podaci sami su po sebi sigurni; čak i u slučajevima povrede podataka, podaci će biti beskorisni i nepovratni napadačima. Iz tog razloga, enkripcija se čak eksplicitno spominje kao metoda zaštite podataka u GDPR-u (General Data Protection Regulation – opća uredba o zaštiti podataka) [32], što znači da će njena pravilna uporaba sigurno donijeti naklonost u očima regulatora. Enkripcija rješava dvije uobičajene ranjivosti zaštite podataka u današnjem globalnom gospodarstvu: radnu snagu koja je stalno u pokretu i porast rada na daljinu. Uz uređaje koji često napuštaju sigurnost mreža tvrtke, enkripcija osigurava da, u slučaju krađe ili gubitka, osjetljivi podaci koje sadrže budu nedostupni vanjskim osobama.

Upravo ta neupotrebljivost podataka je razlog zašto je enkripcija dio MDM rješenja. Na primjer, privatni uređaj zaposlenika koji nema enkripciju podataka, odnosno MDM rješenje, a ima pristup korporativnim podacima će biti vrlo lak plijen za napadače. Uz MDM rješenje i enkripciju podataka, takve radnje će biti spriječene, a u najgorem slučaju znatno otežane.

6.3. Sigurnosne kopije

Sigurnosne kopije su način sprječavanja gubitka podataka do kojeg često može doći zbog pogreške korisnika ili tehničkog kvara. Sigurnosne kopije treba redovito izrađivati i ažurirati. Redovno sigurnosno kopiranje nametnut će dodatni trošak tvrtki, no potencijalni prekidi u normalnom poslovanju koštat će još više. Sigurnosno kopiranje treba izvoditi u skladu s osjetljivošću podataka – podaci male važnosti ne moraju se često sigurnosno kopirati, ali osjetljivi podaci moraju. Takve sigurnosne kopije trebaju biti pohranjene na sigurnom mjestu i po mogućnosti šifrirane. Osjetljivi podaci se nikad ne pohranjuju u oblak. Povremeno je potrebna provjera da li su mediji za pohranjivanje oštećeni, u skladu sa smjernicama proizvođača te je potrebno pobrinuti se da se podaci pohranjuju u skladu sa službenim preporukama (vlažnost, temperaturu itd.). Izrada sigurnosne kopije osigurava da se podaci lako mogu obnoviti i da to ne utječe toliko na ostale operacije u izvođenju. U idealnom slučaju, korporacije bi trebale sigurnosno kopirati svoje podatke onoliko često koliko im to resursi dopuštaju. Iako je mnogim tvrtkama, posebno manjim, dovoljno svakodnevno sigurnosno kopiranje, one koje se bave podacima koji se stalno mijenjaju, poput financijskih organizacija, trebale bi sigurnosno kopirati čak i češće—ponekad i nekoliko puta dnevno. Postoje je softveri koji automatski izrađuje sigurnosnu kopiju podataka u odabranim intervalima kako bi se olakšalo upravljanje procesom.

6.4. Korištenje sigurnosnih sustava krajnjih točaka

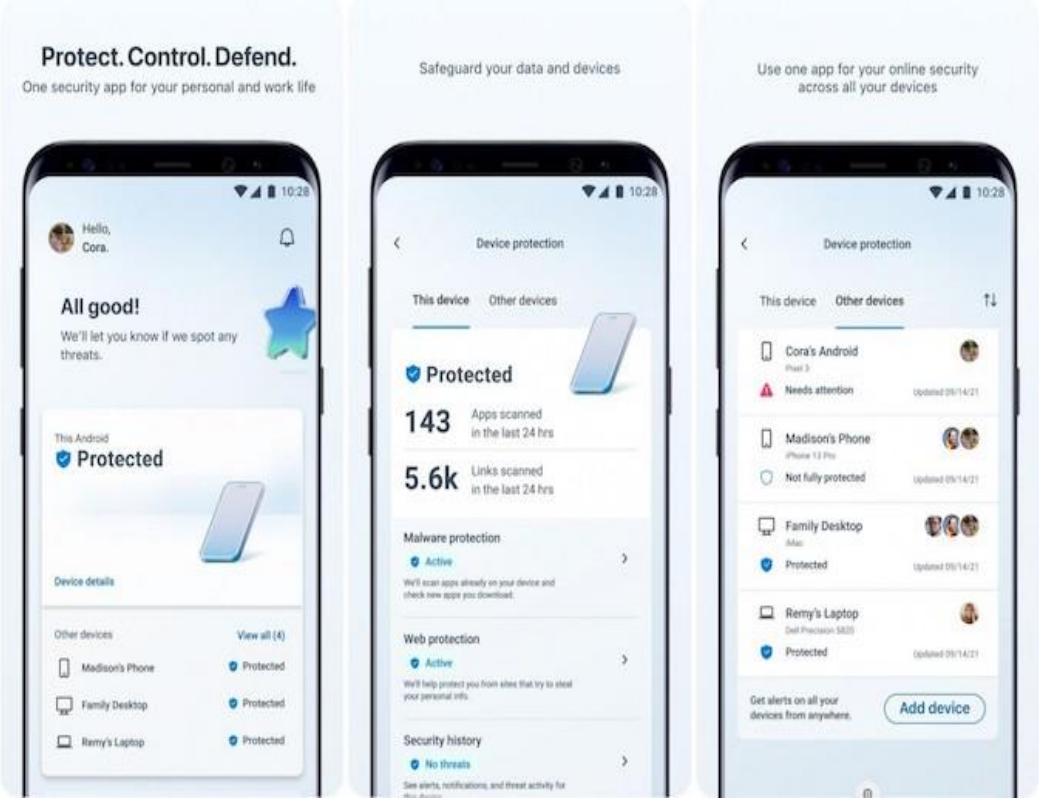
Krajnje točke mreže korporacije stalno su pod prijetnjom. Privatni uređaji zaposlenika koje zaposlenici u slobodno vrijeme koriste za spajanje na neprovjerene mreže i za pristup raznoraznim nesigurnim stranicama su velika prijetnja. Ukoliko uređaji zaposlenika koji imaju pristup svim osjetljivim podacima nemaju potrebnu zaštitu, sve će biti ugroženo. Stoga je važno postavljanje robusne sigurnosne infrastrukture krajnjih točaka kako bi se umanjile šanse za moguće povrede podataka.

Sigurnosni sustavi koji su poželjni za korištenje za prevenciju povrede podataka:

- **Antivirusni softver** (npr. MS Defender, na slici 9. prikazane su glavne funkcije MS Defendera i izgled sučelja) – instalacija antivirusnog softvera na svakog značajno pomaže pri otkrivanju i prevenciji prijetnji. Potrebno je provoditi redovita skeniranja kako bi se održalo zdravstveno stanje sustava korporacije i na vrijeme došlo do otkrivanja virusnih infekcija kao što je ransomware.
- **Antispyware** – spyware je vrsta zlonamjernog računalnog softvera koji se obično instalira bez znanja korisnika. Njegova je svrha obično pronaći pojedinosti o ponašanju korisnika i prikupiti osobne podatke. Antispyware i

antiadware alati mogu pomažu pri uklanjanju i blokiranju takvih zlonamjernih softvera.

- **Blokatori prozora** – skočni prozori su neželjeni programi koji se pokreću na sustavu bez ikakvog vidljivog razloga osim što ugrožavaju dobrobit sustava. Instalacija blokatora prozora čini sustav sigurnijim.
- **Vatrozid (firewall)** – vatrozid predstavlja prepreku između podataka i kibernetičkih kriminalaca, zbog čega većina stručnjaka preporučuje vatrozid kao jednu od najboljih praksi za sigurnost podataka. Također moguća je instalacija internog vatrozida za dodatnu zaštitu.



Slika 9. MS Defender na mobilnom uređaju

Izvor: [33]

6.5. Skeniranje novih uređaja u mreži korporacije

Zaraženi uređaj predstavlja rizik zbog rastućeg trenda BYOD-a. Posljednje što korporacija želi je provesti mjesece osiguravajući mrežu od vanjskih napada samo da bi se

pokupili opasni zlonamjerni softver s privatnog mobilnog uređaja zaposlenika. Ograničavanjem Wi-Fi pristupa, IT tim će imati priliku otkriti zaražene uređaje prije nego što se povežu i čak očistiti uređaje od zlonamjernih softvera za zaposlenike. Poželjno je češće izvođenje skeniranja uređaja i redovito provjeravanje svih uređaja tvrtke kako bi se spriječili zlonamjerni softveri i virusi da uđu u mrežu.

Istodobno se mogu primijeniti pravila kontrole uređaja, koja osiguravaju da se vjeruje samo uređajima koji zadovoljavaju određenu razinu sigurnosti. Na ovaj način zaposlenici imaju mogućnost usklađivanja sigurnosti svojih osobnih uređaja s potrebnom razinom unutar tvrtke. Ako ih odluče ne primijeniti, to dovodi do ograničenosti pristupa osjetljivim podacima.

6.6. Ograničeno dijeljenje datoteka

Što se više datoteka, poslužitelja i uređaja dijeli na mreži korporacije, to je mreža izloženija. Još ako privatni uređaj zaposlenika sadrži zlonamjerni softver, podaci su pod iznimnom opasnosti. Ako postoji uljez, sav taj praktičan pristup datotekama olakšat će pronalazak osjetljivim datotekama. Naravno, dijeljenje datoteka je neophodno za moderno poslovanje pa će neke stvari uvijek morati biti dostupne. Ali ograničavanje i onemogućavanje dijeljenja datoteka uvelike će smanjiti rizik za krađu istih. Za datoteke koje se trenutno dijele ili za one koje se selektivno dijele u određeno doba dana, poželjno je implementirati alate poput Microsoft Cloud App Security. Takav alat će dati uvid u ono što se dijeli i tko pristupa dijeljenim datotekama.

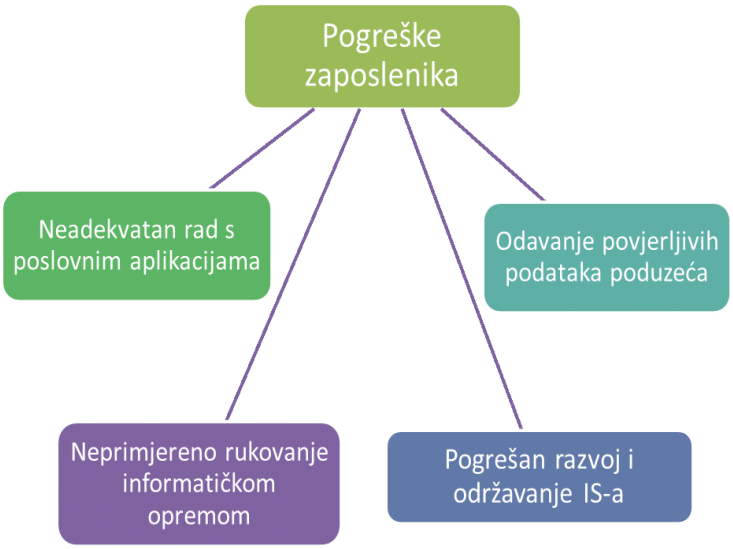
6.7. Sigurnosna politika

Podaci mogu biti strukturirani ili nestrukturirani i mogu se nalaziti u bazi podataka, pohrani u oblaku, lokalnoj pohrani itd. Većina organizacija upravlja velikim količinama podataka, a uobičajeno je da se neki podaci zaborave ili izgube. Zaštita tvrtke od povrede podataka zahtijeva sve podatke—uključujući velike skupove podataka i pojedinačne datoteke i mape. Ne može se unaprijed znati gdje će se pronaći osjetljivi podaci. Potrebna je izrada inventara koji uključuje sve podatke tvrtke. Slijedi, identificiranje lokacije pohranjivanja podataka, kao što su osobni uređaji zaposlenika ili pohrana na tvrdom disku, i izgradnja strategije kako bi se osiguralo da se podaci tvrtke ne mogu tamo pohraniti ili da se pohranjuju na siguran način. Nakon što se stekne sveobuhvatan pregled svih podataka u cijeloj organizaciji, može se implementirati jedinstvena sigurnosna politika kako bi si osiguralo da su podaci na odgovarajući način zaštićeni i postaviti nadzor koji će upozoriti kada dođe do pristupa osjetljivim podacima.

Sigurnosna politika bi se trebala pobrinuti i za to da svaki privatni mobilni uređaj obavezno treba imati neko MDM rješenje. Zaposlenici, čak i da nisu svjesni, svojim radnjama na mobilnim uređajima mogu ugroziti korporativne podatke. Zbog takvih razloga, sigurnosna politika bi se trebala bazirati na MDM rješenjima kako bi podaci na mobilnim uređajima zaposlenika bili maksimalno zaštićeni.

6.8. Edukacija zaposlenika

Konačno, ljudski faktor je često najveća slabost u metodama zaštite podataka (slika 10.). Nije dovoljno imati sigurnosne politike. Tvrtke moraju obučiti svoje zaposlenike, objasniti politike i njihovu važnost te im pokazati kako upravljati osjetljivim podacima i odgovoriti na sumnjive aktivnosti. Zaposlenici mogu slijediti najbolje prakse za sigurnost podataka kako bi spriječili unutarnje i vanjske napade.



Slika 10. Pogreške zaposlenika koje nastaju ukoliko zaposlenici nisu pravilno educirani

Izvor: [34]

Potrebno je educirati zaposlenika da koriste jake lozinke, izbjegavaju njihovu ponovnu upotrebu te pojasniti im važnost provjere autentičnosti s više faktora. Zaposlenike treba osposobiti za prepoznavanje i izbjegavanje phishing napada te zaključavanje aplikacija i računalnih uređaja kada ih ne koriste. Ova osnovna obuka trebala bi se kontinuirano pružati novim i postojećim zaposlenicima. Nije dobro pretpostavljati da zaposlenici "već znaju" pravila

– mora se stalno osvježavati njihovo znanje i dodavati nove upute i smjernice na temelju razvoja prijetnji.

Privatni mobilni uređaji zaposlenika koji nisu ispravno zaštićeni, a pristupaju nesigurnim stranicama ili preuzimaju zaražene aplikacije su jako velika sigurnosna prijetnja. Mobilnost donosi brojne prednosti na radnom mjestu, povećavajući produktivnost zaposlenika dopuštajući zaposlenicima da rade bilo gdje i bilo kada s vlastitim uređajima. Iako, s ovom povećanom produktivnošću dolazi prijetnja smanjene sigurnosti i veće korporativne odgovornosti, a tu dolazi upravljanje mobilnim uređajima (MDM).

Nakon uvida u rizike poslovanja bez odgovarajućeg MDM rješenja, postaje jasno zašto koristiti MDM. Bez MDM-a informacije o ukradenim ili izgubljenim uređajima nisu sigurne, što bi moglo omogućiti da lako padnu u pogrešne ruke. Također, uređaji bez MDM-a imaju povećanu izloženost zlonamjernom softveru i drugim virusima koji bi mogli ugroziti povjerljive podatke. A kada su ti povjerljivi podaci ugroženi, lakoća do koje se može doći do povrede podataka ili incidenta hakiranja uvelike se povećava – događaji koji mogu trajno utjecati na ugled tvrtke kod potrošača i drugih poslovnih partnera.

7. ZAKLJUČAK

Obavljanje posla na privatnim uređajima nikad nije bilo lakše i dostupnije. Svaka korporacija ima IT timove koji raspolažu mobilnim uređajima i njihovim upravljanjem te omogućuju zaposlenicima obavljanje poslovnih zadataka na privatnim uređajima. Naravno, sigurnost podataka korporacije je na prvom mjestu. Uređaji pohranjuju ogromne količine jako osjetljivih i važnih informacija te je sigurnost podataka stalna meta napadača.

Postoje razne metode i modeli korištenja privatnih uređaja za korporativne poslove. Uz odvajanje privatnog od poslovnog profila moguće je ostvariti i sigurnost podataka korporacije ali i povećati produktivnost te zadovoljstvo zaposlenika. Iako svaki od modela zaštite nudi dobru sigurnost i očuvanje podataka uz istodobno neometano obavljanje posla, postoje razne sigurnosne prijetnje. Uređaji su pod konstantnim rizikom od sigurnosnih prijetnji koje mogu znatno ugroziti korporacije. Korporacije su obvezne konstantno pratiti stanje svojih uređaja i sustava te biti ažurne oko sigurnosnih prijetnji.

Metode zaštite korporativnih podataka imaju ogromnu važnost da ne dođe do ugrožavanja osjetljivih informacija. Svaka zaštita između podataka i napadača će iznimno pomoći kod očuvanja podataka i otežati krađu podataka, a u današnje vrijeme, informacije su od neprocjenjive važnosti. Iako korporacije pokušavaju uvijek biti korak ispred napadača, propusti su mogući i nažalost mogu biti katastrofalni za korporacije.

LITERATURA

1. BenQ. *BYOD Isn't Just a Policy: Is Your Company BYOD Friendly?* Preuzeto s: https://www.benq.com/en-ap/business/resource/trends/byod-projector-wireless.html [Pristupljeno: 01. kolovoza 2022.]
2. Peraković, D., Husnjak, S., Mišić, V. & Kuljanić, Tibor, Mijo (2016). *Employee's awareness on security aspects of use bring your own device paradigm in Republic of Croatia*. Preuzeto s: 849915.Employees awareness on [Pristupljeno: 01. kolovoza 2022.]
3. Nebula. *BYOD vs COPE – the enterprise device debate.* Preuzeto s: https://www.nebula.co.za/2017/02/09/byod-vs-cope-the-enterprise-device-debate/ [Pristupljeno: 01. kolovoza 2022.]
4. Techopedia. *Corporate Owned, Personally Enabled (COPE).* Preuzeto s: https://www.techopedia.com/definition/29071/corporate-owned-personally-enabled-cope [Pristupljeno: 01. kolovoza 2022.]
5. Motus. *CYOD: How Does a Choose Your Own Device Program Work?* Preuzeto s: https://www.motus.com/cyod-chose-your-own-device/ [Pristupljeno: 01. kolovoza 2022.]
6. Jumpcloud. *Device Management: BYOD, COPE, COBO and CYOD.* Preuzeto s: https://jumpcloud.com/blog/defining-byod-cope-cobo-cyod [Pristupljeno: 01. kolovoza 2022.]
7. Peraković D., Husnjak S., Cvitić I. (2014). *Comparative Analysis of Enterprise Mobility Management Systems in BYOD Environment.* Preuzeto s: https://www.bib.irb.hr/739995 [Pristupljeno: 01. kolovoza 2022.]
8. Blackberry. *COBO: For Ultimate Security & Control in a Breach-Happy Era.* Preuzeto s: https://blogs.blackberry.com/en/2014/07/cobo-ultimate-security [Pristupljeno: 03. kolovoza 2022.]
9. Gadgets now. *How to keep personal and work profiles different on your Android phone.* Preuzeto s: https://www.gadgetsnow.com/how-to/how-to-keep-personal-and-work-profiles-different-on-your-android-phone/articleshow/89807547.cms [Pristupljeno: 03. kolovoza 2022.]
10. The Motley Fool. *IDC: Android on 75 Percent of Smartphones in Q3.* Preuzeto s: https://www.fool.com/investing/general/2012/11/02/idc-android-on-75-percent-of-smartphones-in-q3.aspx [Pristupljeno: 03. kolovoza 2022.]

11. ManageEngine. *Android Enterprise Mobile Device Management.* Preuzeto s: https://www.manageengine.com/mobile-device-management/mdm-android-enterprise.html [Pristupljeno: 03. kolovoza 2022.]
12. Android. *Best-in-class device and data protection.* Preuzeto s: https://www.android.com/enterprise/security/ [Pristupljeno: 03. kolovoza 2022.]
13. Integra group. *Mobile Device Management.* Preuzeto s: https://www.integragroup.hr/usluge-i-rjesenja/sigurnost/mobile-device-management [Pristupljeno: 06. kolovoza 2022.]
14. Techtarget network. *Mobile device management.* Preuzeto s: https://www.techtarget.com/searchmobilecomputing/definition/mobile-device-management [Pristupljeno: 06. kolovoza 2022.]
15. AT&T Business. *IBM MaaS 360.* Preuzeto s: https://www.business.att.com/products/ibm-maas360.html# [Pristupljeno: 06. kolovoza 2022.]
16. IBM. *Mobile device management (MDM) solutions.* Preuzeto s: https://www.ibm.com/security/mobile-device-management [Pristupljeno: 06. kolovoza 2022.]
17. G2. *IBM Security MaaS360 with Watson.* Preuzeto s: https://www.g2.com/products/ibm-security-maas360-with-watson/reviews [Pristupljeno: 06. kolovoza 2022.]
18. IBM. *About the Cloud Extender.* Preuzeto s: https://www.ibm.com/docs/hu/maas360?topic=guide-about-cloud-extender [Pristupljeno: 06. kolovoza 2022.]
19. Terminalni uređaji. *Sigurnost primjene terminalnih uređaja.* Preuzeto s: https://moodle.srce.hr/2021-2022/pluginfile.php/5443921/mod_resource/content/2/7_Sigurnost_terminalnih_ure%C4%91aja_21_22.pdf [Pristupljeno: 06. kolovoza 2022.]
20. Herod technology. *7 Common Cyber Security Threats for Businesses.* Preuzeto s: https://herrodtech.com/7-common-cyber-security-threats-for-businesses/ [Pristupljeno: 06. kolovoza 2022.]
21. Peraković D., Husnjak S. & Remenar V. (2012). *Research of Security Threats in the Use of Modern Terminal Devices.* Preuzeto s: 600737.DAAAM_2012_Perakovic_Husnjak_Remenar%20(2) [Pristupljeno: 06. kolovoza 2022.]

22. The State of Security. *IBM Study Shows Data Breach Costs on the Rise.* Preuzeto s: https://www.tripwire.com/state-of-security/security-data-protection/data-breach-costs-rise/ [Pristupljeno: 06. kolovoza 2022.]
23. Tessian. *Must-Know Phishing Statistics: Updated 2022.* Preuzeto s: https://www.tessian.com/blog/phishing-statistics-2020/ [Pristupljeno: 09. kolovoza 2022.]
24. Sigurnost i privatnost podataka pametnih mobilnih terminalnih uređaja. Preuzeto s: 928026.bosnjak_zvonimir_fpz_2016_zavrs_sveuc [Pristupljeno: 09. kolovoza 2022.]
25. Health IT Security. *71% of Ransomware Attacks Targeted Small Businesses in 2018.* Preuzeto s: https://healthitsecurity.com/news/71-of-ransomware-attacks-targeted-small-businesses-in-2018 [Pristupljeno: 09. kolovoza 2022.]
26. Huawei. *What Is Ransomware and How to Remove Ransomware?* Preuzeto s: https://support.huawei.com/enterprise/en/doc/EDOC1100143343 [Pristupljeno: 09. kolovoza 2022.]
27. Pro-ping. *Što su DDoS napadi i možemo li se zaštititi od njih?* Preuzeto s: https://www.pro-ping.hr/blog?sto-su-ddos-napadi-i-mozemo-li-se-zastititi-od-njih [Pristupljeno: 09. kolovoza 2022.]
28. Ucionica. *Sigurnost: što je Botnet mreža i kako se zaštiti?* Preuzeto s: https://www.ucionica.net/sigurnost/sigurnost-sto-je-botnet-mreza-i-kako-se-zastiti-2549/ [Pristupljeno: 10. kolovoza 2022.]
29. Networkdepot. *Your Small Business's Great Cybersecurity Threat Comes from Inside.* Preuzeto s: https://www.networkdepot.com/small-business-insider-threats/ [Pristupljeno: 10. kolovoza 2022.]
30. TechRepublic. *Report: 19% of business passwords 'easily compromised'.* Preuzeto s: https://www.techrepublic.com/article/report-19-of-business-passwords-easily-compromised/ [Pristupljeno: 10. kolovoza 2022.]
31. Cybercrime Magazine. *Cybercrime To Cost The World $10.5 Trillion Annually By 2025.* Preuzeto s: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [Pristupljeno: 12. kolovoza 2022.]
32. Information Commissioner's Office. *Encryption.* Preuzeto s: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/ [Pristupljeno: 12. kolovoza 2022.]
33. Mob.hr. *Microsoft Defender – jedinstvena online zaštita za sve platforme.* Preuzeto s: https://mob.hr/microsoft-defender-jedinstvena-online-zastita-za-sve-platforme/ [Pristupljeno: 12. kolovoza 2022.]

34. Otvoreni sustavi i sigurnost. *Pristupi povećanju svijesti o informacijskoj sigurnosti kod zaposlenika u poduzećima.* Preuzeto s: https://security.foi.hr/wiki/index.php/Pristupi_pove%C4%87anju_svijesti_o_informacijskoj_sigurnosti_kod_zaposlenika_u_poduze%C4%87ima.html [Pristupljeno: 13. kolovoza 2022.]

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je Završni rad (*vrsta rada*) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom

Sigurnosni aspekti korporativnih podataka mobilnih uređaja u privatnom vlasništvu,

u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 5.9.2022. Kristijan Tomas Tomas

(ime i prezime, *potpis*)