Istraživanje sigurnosnih aspekata primjene vlastitih uređaja u korporativnom okruženju

Mišić, Vlatka

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:786663

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Vlatka Mišić

ISTRAŽIVANJE SIGURNOSNIH ASPEKATA PRIMJENE VLASTITIH UREĐAJA U KORPORATIVNOM OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2016.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ISTRAŽIVANJE SIGURNOSNIH ASPEKATA PRIMJENE VLASTITIH UREĐAJA U KORPORATIVNOM OKRUŽENJU

THE STUDY OF SECURITY ASPECTS OF THE BYOD TRENDS IN THE CORPORATE ENVIRONMENT

Mentor: prof. dr. sc. Dragan Peraković

Studentica: Vlatka Mišić

JMBAG: 0135225986

Zagreb, rujan 2016.

SAŽETAK

U ovom radu provedeno je istraživanje pojma korištenja vlastitog uređaja u korporativnom okruženju (BYOD). Korištenje vlastitih terminalnih uređaja varira ovisno o korporaciji, no vrlo je važno podići svijest zaposlenika o mogućim sigurnosnim prijetnjama koje izviru iz navedenog. BYOD predstavlja rizik za poslovanje, najčešće prisutan kao rizik od krađe podataka, neovlaštenog pristupa aplikacijama i sustavima korporacije, od gubitka reputacije i slično. BYOD, kao i svaki drugi sustav, treba sistematski planirati, implementirati, nadzirati i poboljšavati. Za potrebe diplomskog rada analizirana su dosadašnja istraživanja o trendovima korištenja vlastitih uređaja u korporativnom okruženju, modeli vlasništva navedenih uređaja te sigurnosne prijetnje uzrokovane korištenjem vlastitih uređaja. Kroz anketno istraživanje ispitana je zastupljenost korištenja vlastitih terminalnih uređaja na radnom mjestu te svjesnost zaposlenika o sigurnosnim prijetnjama koje dolaze kao posljedica korištenja vlastitih uređaja. Predložene su preporuke za povećanje svjesnosti korisnika o sigurnosnim prijetnjama te metode zaštite koje bi povećale sigurnost informacija u korporativnom okruženju.

KLJUČNE RIJEČI

BYOD – (eng. *Bring Your Own Device*) – korištenje vlastitih terminalnih uređaja u korporativnom okruženju

Terminalni uređaji – krajnji uređaji na strani korisnika, u ovom radu pametni mobilni uređaji, laptopi i tableti

Sigurnosni aspekt – pitanje sigurnosti korporativnih podataka

Povećanje svijesti korisnika – povećanje razumijevanja i opreza zaposlenika kada se radi o manipulaciji korporativnim podacima

Metode zaštite – metode koje se provode u korporativnom okruženju s ciljem povećanja sigurnosti korporativnih podataka, bilo od strane IT stručnjaka i vodstva tvrtke ili samih zaposlenika

ABSTRACT

The aim of this Master's Thesis was to conduct research on trends of employees bringing their own devices into the corporate enviroment (BYOD). Using their own terminal devices varies depending on a corporation, but it is very important to raise awareness of employees about possible security threats that BYOD brings. BYOD poses a risk to business, usually presented as the risk of data theft, unauthorized access to applications and corporation systems and loss of reputation. BYOD, like any other system, needs to be systematically planed, implemented, monitored and improved. This Master's Thesis offers the analysis of previous research on trends of employees bringing their own devices into the corporate enviroment and models of ownership of those devices and security threats caused by using their own devices. The aim of the survey was to examine the presence of employees' own terminal devices in the workplace and their awareness of security threats that come as a result of using their own devices. Recommendations were proposed for raising the awareness of employees about security threats and security methods that would increase the security of information in the corporate environment.

KEYWORDS

BYOD - (Bring Your Own Device) – employees use their own terminal devices in the corporate environment

Terminal devices - terminals on the user side, in this Master's Thesis, smart mobile devices, laptops and tablets

The security aspect - the question of security of corporate data

Increase of user awareness - increasing the understanding and caution of employees when it comes to manipulating corporate data

Protection methods - methods that are implemented in the corporate environment in order to increase the security of corporate data, be it by the IT professionals and the company management or employees themselves

SADRŽAJ

1. UVOD 1

2. PRIMJENA I ZASTUPLJENOST KORIŠTENJA TERMINALNIH UREĐAJA U SVIJETU 2

2.1. Faze razvoja pametnih mobilnih terminalnih uređaja.....3

2.1.1. Prva faza razvoja pametnih mobilnih terminalnih uređaja 3

2.1.2. Druga faza razvoja pametnih mobilnih terminalnih uređaja 4

2.1.3. Treća faza razvoja pametnih mobilnih terminalnih uređaja 4

2.2. Trendovi korištenja pametnih mobilnih terminalnih uređaja.....5

2.3. Korištenje pametnih mobilnih terminalnih uređaja u korporativnom okruženju 7

3. *BRING YOUR OWN DEVICE* TRENDOVI U HRVATSKOJ I SVIJETU 9

3.1. Korištenje BYOD paradigme s gledišta korporacije 11

3.1.1. Prednosti korištenja BYOD-a s gledišta korporacije 12

3.1.2. Nedostaci korištenja BYOD-a s gledišta korporacije.....13

3.2. Korištenje BYOD paradigme s gledišta zaposlenika.....13

3.2.1. Prednosti korištenja BYOD-a s gledišta zaposlenika 14

3.2.2. Nedostaci korištenja BYOD-a s gledišta zaposlenika 14

3.3. Korištenje BYOD-a u Hrvatskoj 15

4. SIGURNOSNI ASPEKTI PRIMJENE *BRING YOUR OWN DEVICE* PARADIGME 18

4.1. Fizički zasnovane prijetnje.....19

4.2. Aplikacijski zasnovane prijetnje.....20

4.2.1. *Malware* napadi 21

4.2.2. Nenamjerno odavanje podataka 23

4.2.3. Nadziranje korištenjem pametnih mobilnih terminalnih uređaja.....24

4.3. *Web* zasnovane prijetnje.....24

4.3.1. Iskorištavanje ranjivosti u *web* preglednicima 24

4.3.2. Automatsko preuzimanje aplikacija 25

4.4. Socijalni inženjering 25

5. METODE ZAŠTITE OSJETLJIVIH PODATAKA U KORPORATIVNOM OKRUŽENJU 28

5.1. Pojam i važnost korporativnih podataka i informacija 28

5.2. Sigurnosna politika i standardi 30

5.3. Edukacija zaposlenika i osoblja 32

5.4. Sigurnosno upravljanje korporativnim podacima 32

5.4.1. Virtualna privatna mreža 33

5.4.2. Sustav za upravljanje mobilnim sadržajem 34

5.4.2.1. Sustav za upravljanje mobilnim terminalnim uređajem 34

5.4.2.2. Sustav za upravljanje mobilnim aplikacijama 36

5.4.2.3. Sustav za upravljanje informacijama na mobilnom terminalnom uređaju 36

6. DESKRIPTIVNA ANALIZA SVJESNOSTI ZAPOSLENIKA O SIGURNOSNIM ASPEKTIMA PRIMJENE *BRING YOUR OWN DEVICE* PARADIGME 37

6.1. Analiza rezultata dobivenih provedenim istraživanjem 37

6.1.1. Trendovi korištenja pametnih mobilnih terminalnih uređaja 37

6.1.2. Svjesnost sigurnosnog aspekta primjene vlastitih terminalnih uređaja u korporativnom okruženju 39

6.2. Preporuke za povećanje sigurnosti korporativnih podataka 43

7. ZAKLJUČAK 45

LITERATURA 46

POPIS KRATICA 49

POPIS SLIKA 50

POPIS GRAFIKONA 50

PRILOG 1. PRIMJER ANKETNOG UPITNIKA 52

1. UVOD

U ovom diplomskom radu provedeno je istraživanje sigurnosnih aspekata primjene vlastitih uređaja u korporativnom okruženju. Primjena vlastitih uređaja u korporativnom okruženju uvodi se kao BYOD pojam, a označava povezivanje uređaja zaposlenika na mrežu korporacije. Istraživanje je provedeno anketom, a ispitana je zastupljenost korištenja vlastitih terminalnih uređaja na radnom mjestu te svjesnost zaposlenika o sigurnosnim prijetnjama koje korištenje vlastitih uređaja na radnom mjestu donosi.

Svrha je istraživanja prikazati na koje načine i u kojoj mjeri zaposlenici koriste vlastite uređaje za pristup korporativnoj mreži. Cilj je istraživanja ukazati na statističke informacije o korištenju vlastitih terminalnih uređaja zaposlenika u Republici Hrvatskoj za pristup osjetljivim korporativnim podacima te istražiti sigurnosne aspekte koji dolaze u pitanje zbog BYOD trendova. Rad je podijeljen u 7 cjelina:

1. Uvod
2. Primjena i zastupljenost korištenja terminalnih uređaja u svijetu
3. *Bring Your Own Device* trendovi u Hrvatskoj i svijetu
4. Sigurnosni aspekti primjene *Bring Your Own Device* paradigme
5. Metode zaštite osjetljivih podataka u korporativnom okruženju
6. Deskriptivna analiza svjesnosti zaposlenika o sigurnosnim aspektima primjene *Bring Your Own Device* paradigme
7. Zaključak

U drugom poglavlju prikazat će se povijesni razvoj primjene pametnih mobilnih uređaja i trendovi korištenja vlastitih uređaja u korporativnom okruženju. U trećem poglavlju navest će se prednosti i nedostaci BYOD trenda, te će se analizirati primjena BYOD trenda u Hrvatskoj na temelju provedenog istraživanja. U četvrtom poglavlju prikazat će se sigurnosne prijetnje korporativnim podacima, a u petom poglavlju prikazat će se metode zaštite tih podataka. U šestom poglavlju provedena je analiza ankete te su na temelju rezultata predložene preporuke za povećanje svjesnosti korisnika o sigurnosnim prijetnjama te metode zaštite koje bi povećale sigurnost informacija u korporativnom okruženju.

2. PRIMJENA I ZASTUPLJENOST KORIŠTENJA TERMINALNIH UREĐAJA U SVIJETU

Terminalni su uređaji krajnji uređaji u telekomunikacijskoj mreži koji se uglavnom nalaze na strani korisnika. U ovom radu pod pojmom terminalni uređaji podrazumijevat će se prijenosni terminalni uređaji kao što su prijenosna računala (laptopi), pametni mobilni terminalni uređaji (eng. *smartphones*) i prijenosna tablet računala (tableti).

Danas su pametni mobilni terminalni uređaji najkorišteniji terminalni uređaji. Imaju široku primjenu i više se ne koriste samo za klasičnu komunikaciju, odnosno za pozive i SMS poruke kao što je to bio slučaj prije desetak godina. Količina je podataka pohranjenih na mobilnim uređajima velika, a korisnici često nisu svjesni osobnih podataka koji se kriju u njihovim mobilnim uređajima. Gubitak ili krađa uređaja može uvelike oštetiti vlasnika, postoji opasnost od krađe identiteta, novčanog oštećenja, narušenja ugleda ili nekog drugog oblika manipulacije podataka od strane zlonamjernih korisnika. Posebno velika opasnost od manipulacije podataka javlja se u korporativnom okruženju, gdje podaci koji se nalaze na terminalnim uređajima mogu biti posebno osjetljivi.

Pojam *smartphone* uveden je na tržište kao termin koji je podrazumijevao novu klasu mobilnih terminalnih uređaja koji su pružali integriranu uslugu, od glasovne komunikacije, razmjene poruka, upravljanja osobnim informacijama pa sve do raznih aplikacija i mogućnosti bežične komunikacije [1]. Iako ne postoji točna definicija pametnog mobilnog terminalnog uređaja, može se reći da je to svaki terminalni uređaj koji proširuje mogućnosti klasičnog mobilnog terminalnog uređaja. Dodatne funkcionalnosti koje se očekuju kod pametnog mobilnog terminalnog uređaja nisu točno definirane i mijenjaju se s vremenom [2]. Ključne značajke pametnih terminalnih uređaja jesu sljedeće [3]:

a. operacijski sustav (OS)

b. aplikacije

c. puna QWERTY[1] tipkovnica

d. stalni pristup Internetu

e. sposobnost razmjene poruka

Razvojem tehnologije i sve većim korisničkim zahtjevima mijenjaju se funkcionalnosti pametnih telefona, pa tako i definicija navedenog termina.

2.1. Faze razvoja pametnih mobilnih terminalnih uređaja

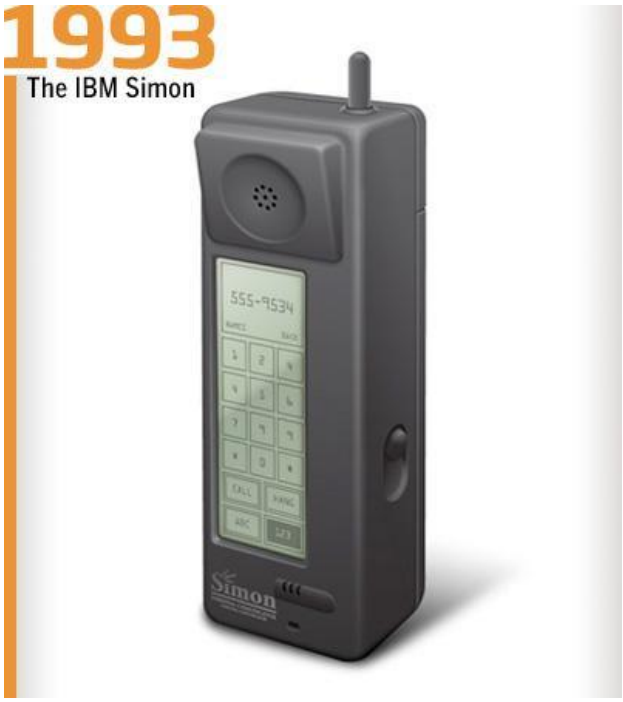
Pametni mobilni terminnalni uređaj tržištu je predstavio Apple prije devet godina, odnosno u lipnju 2007. godine. No prema nekim izvorima, pametni mobilni terminalni uređaji su, u drugačijem obliku, bili na tržištu još od 1993. godine. Razlika je u tome što su tadašnji pametni mobilni terminalni uređaji bili namijenjeni poslovnim korisnicima i cijena im je bila vrlo visoka, previsoka za većinu rezidencijalnih korisnika. Ogroman uspjeh iPhone uređaja potaknuo je proizvođače da na razne načine subvencioniraju kupnju pametnih mobilnih terminalnih uređaja kako bi dugoročno zadržali korisnike i kako bi ih koristilo što više fizičkih osoba [4]. Razvoj pametnih mobilnih terminalnih uređaja podijeljen je u tri glavne faze.

2.1.1. Prva faza razvoja pametnih mobilnih terminalnih uređaja

U prvoj su fazi pametni mobilni terminalni uređaji bili namijenjeni isključivo poduzećima, a aplikacije i funkcionalnosti zadovoljavale su poslovne potrebe. Ova era započela je dolaskom prvog pametnog mobilnog terminalnog uređaja na tržište 1993. godine pod nazivom “The Simon”, a proizvođač je tog uređaja IBM. Svrha ovog uređaja bila je ujediniti govorne usluge i usluge prijenosa podataka, a imao je funkcionalnosti mobilnog telefona, dlanovnika (eng. *Personal Digital Assistant* – PDA) i telefaksa. Uređaj je čak imao ekran osjetljiv na dodir koji se mogao koristiti za biranje telefonskih brojeva. Iako je imao nove funkcionalnosti, ovaj uređaj bio je težak i velik, a cijena mu je bila visokih 899 dolara. Na Slici 1. prikazan je izgled prvog pametnog mobilnog terminalnog uređaja. Revolucionarni uređaj prve generacije pametnih mobilnih terminalnih uređaja je BlackBerry kojim su

[1] QWERTY tipkovnica standardna je engleska tipkovnica na kojoj je poredak prvih šest slova QWERTY (na hrvatskoj tipkovnici QWERTZ).

uvedene mnoge značajke kao što su elektronička pošta, pristup Internetu, faks, *web* tražilica i kamera [1], [4].



Slika 1. Prvi pametni mobilni terminačni uređaj, IBM Simon iz 1993. godine [4]

2.1.2. Druga faza razvoja pametnih mobilnih terminalnih uređaja

Druga generacija pametnih mobilnih terminalnih uređaja započela je izumom iPhone uređaja koji je bio velika prekretnica na tržištu pametnih mobilnih terminalnih uređaja 2007. godine. Tada je prvi puta pametni mobilni terminalni uređaj bio predstavljen širem tržištu, a ne samo poslovnim korisnicima. Krajem 2007. godine Google je predstavio Android operacijski sustav čija je namjena bila približiti se korisnicima pametnih mobilnih terminalnih uređaja. Fokus je bio na zadovoljavanju korisničkih želja i potreba uz prihvatljivu cijenu za šire tržište. Uređaji druge faze razvoja dolaze s dodatnim mogućnostima za privatne korisnike kao što su slanje i primanje elektroničke pošte, integracija društvenih mreža, audio/video reprodukcija, pristup internetu i razni servisi za slanje poruka u realnom vremenu (eng. *Instant Messaging* - IM) [1].

2.1.3. Treća faza razvoja pametnih mobilnih terminalnih uređaja

Ponuda pametnih mobilnih terminalnih uređaja na tržištu u trećoj fazi razvoja gotovo je jednaka za privatne i poslovne korisnike. Dolazi do poboljšanja uređaja u vidu poboljšanja

kvalitete prikaza slike, operacijskih sustava, ugrađuju se snažnije baterije i poboljšano je korisničko sučelje (eng. *User Interface* – UI). Ova faza započinje 2008. godine nadogradnjom iOS, Android i BlackBerry operacijskih sustava, a od tada je bilo nekoliko nadogradnji tijekom godina. Najpopularniji operacijski sustavi (iOS, Android, BlackBerry OS, Windows Mobile) i ključni proizvođači pametnih mobilnih terminalnih uređaja (Apple, Samsung, HTC, Motorola, Nokia, LG, Sony i tako dalje) bili su usmjereni na poboljšanje operacijskih sustava i samih uređaja kako bi ponudili nove i potrošačima zanimljive funkcionalnosti. Android je od tada doživio ogroman uspjeh jer je proizvođačima pametnih mobilnih terminalnih uređaja pružio mogućnost izrade uređaja na *open source*[2] Android tehnologiji [1].

2.2. Trendovi korištenja pametnih mobilnih terminalnih uređaja

U posljednjih nekoliko godina razvojem tehnologije pametni mobilni terminalni uređaji imaju sve više funkcionalnosti. Sve više se koriste za elektroničko plaćanje, internet bankarstvo, kupnju putem interneta i tako dalje. Tako se povećava vrijednost uređaja, odnosno podataka koji se na njemu nalaze. Potreba za zaštitom od neautoriziranog pristupa uređaju je puno veća nego kada im je namjena bila uglavnom razmjena SMS poruka i poziva. Zaštita osobnih podataka pohranjenih u memoriju uređaja u slučaju gubitka ili krađe uređaja postaje ključna, osobito kada se radi o vrlo osjetljivim podacima kao što su primjerice podaci o kreditnoj kartici [5]. Posebno su osjetljivi podaci tvrtke, bilo da se nalaze na uređaju u vlasništvu zaposlenika ili u potpunom ili djelomičnom vlasništvu tvrtke. Osim financijskih gubitaka, postoji opasnost od neovlaštenog upada u sustav ili narušenja ugleda tvrtke, što potencijalno tvrtku može odvesti u propast.

Pametni su mobilni terminalni uređaji trenutno vodeći terminalni uređaji na korisničkoj strani (kod privatnih i poslovnih korisnika), a tako će vjerojatno ostati još neko vrijeme jer su postali univerzalni terminali uređaji koji imaju funkcionalnosti mobilnog telefona i stolnog računala.

Može se reći da je pametni mobilni terminalni uređaj mobilni telefon s naprednim značajkama i funkcijama izvan tradicionalnih funkcionalnosti poput telefonskih poziva i slanja SMS poruka. Pametni mobilni terminalni uređaji imaju sposobnost prikaza fotografija u

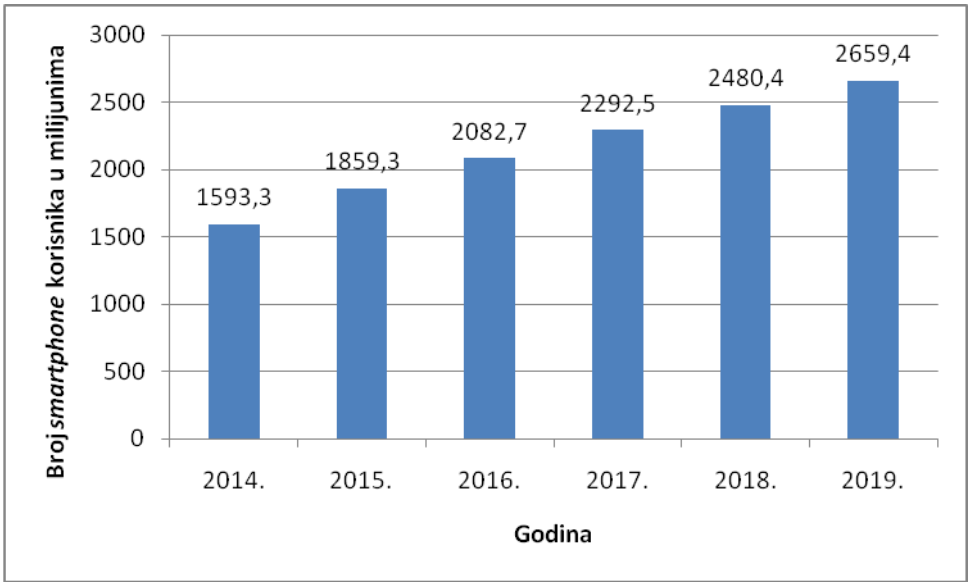
[2] Open source – otvoreni kod – softver čiji je izvorni kod dostupan za uvid, korištenje i izmjene

visokoj rezoluciji, pokretanja igrica, prikazivanja videa, navigiranja, audio/video reprodukcije i snimanja, pretraživanja interneta, mogućnost slanja/primanja elektroničke pošte, ugrađene kamere, aplikacije za društvene mreže, i još mnogo toga. Iz tih razloga pametni mobilni terminalni uređaj je sada postao logičan izbor za šire potrošače, iako je u početku bio namijenjen samo za poslovne korisnike [1].

Prema [1], istraživanja iz 2013. godine pokazuju da popularnost i zainteresiranost za pametne mobilne terminalne uređaje mnogo brže raste kod privatnih korisnika nego u korporativnom okruženju. U početku su pametni mobilni terminalni uređaji bili predviđeni za poslovne svrhe prvenstveno zbog visoke cijene i aplikacija koje su nudili. Danas na tržištu konkuriraju mnogi proizvođači terminalnih uređaja koji pružaju niz naprednih mogućnosti i funkcionalnosti na jednom hardveru.

Nakon 2007. godine, odnosno nakon pojave iPhone uređaja i Android operacijskog sustava na tržištu, korištenje pametnih mobilnih terminalnih uređaja raste gotovo linearno. U trećem kvartalu 2011. godine 26% svih prodanih mobilnih terminalnih uređaja bili su pametni mobilni terminalni uređaji. Godinu prije, 19% prodanih uređaja bili su pametni mobilni terminalni uređaji, što je čak 72% više nego 2009. godine. Istraživanja iz 2013. godine pokazuju da 42% pretplatnika u Sjedinjenim Američkim Državama koristi pametne mobilne terminalne uređaje, dok ih u pet vodećih zemalja Europske unije (Francuska, Njemačka, Italija, Španjolska i Ujedinjeno Kraljevstvo) koristi 44% pretplatnika [1], [2].

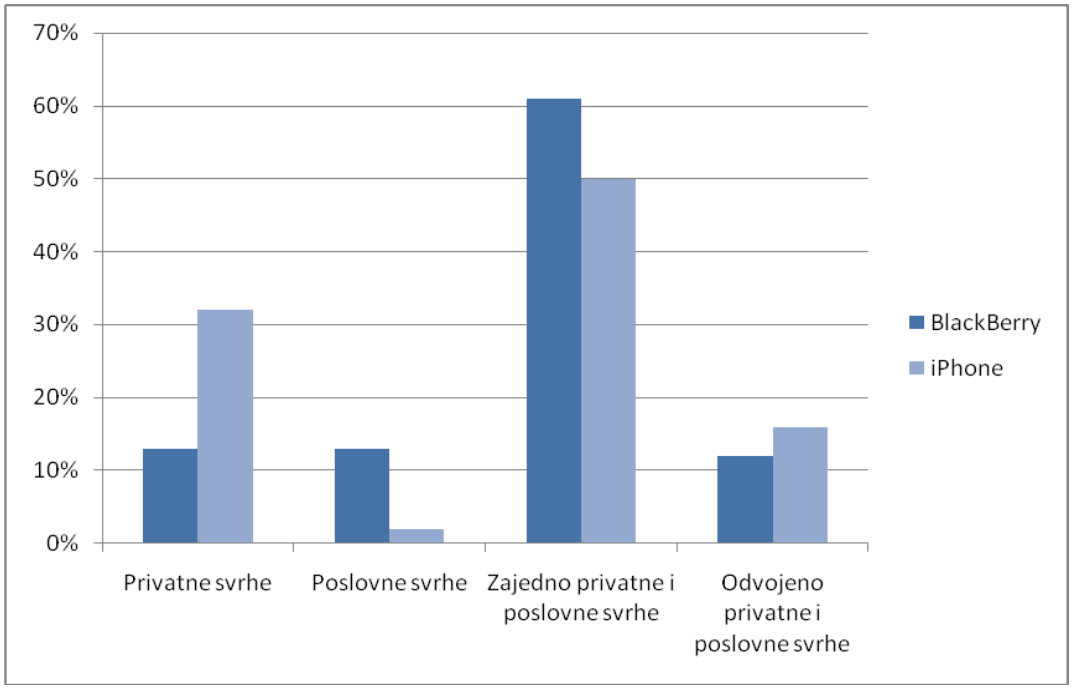
Grafikon 1. prikazuje broj korisnika pametnih mobilnih terminalnih uređaja diljem svijeta do 2016. godine te predviđanja do 2019. godine. Iz grafikona je vidljiv gotovo linearan rast broja korisnika pametnih mobilnih terminalnih uređaja iz godine u godinu, stoga se može pretpostaviti da će se predviđanja ostvariti te da će broj korisnika rasti za oko 200 milijuna godišnje.



Grafikon 1. Broj korisnika pametnih mobilnih terminalnih uređaja u milijunima od 2014. do 2016. godine i predviđanja do 2019. godine
Izvor: [6]

2.3. Korištenje pametnih mobilnih terminalnih uređaja u korporativnom okruženju

Zaposlenici u korporativnom okruženju dugi niz godina koriste vlastite uređaje za obavljanje poslovnih obaveza. IBM-ov Simon bio je prema nekim izvorima prvi pametni mobilni terminalni uređaj. Bio je namijenjen prvenstveno poslovnim korisnicima, najviše zato što mu je cijena bila previsoka za privatne korisnike. Šest godina nakon Simona, točnije 1999. godine tržištu je predstavljen BlackBerry 850. BlackBerry uređaji uglavnom su bili orijentirani na poslovne korisnike, a veliku popularnost u raznim poslovanjima postižu zbog usmjeravanja na komunikaciju elektroničkom poštom. Nakon pojave iPhone uređaja, BlackBerry je nekoliko godina i dalje bio popularniji kod poslovnih korisnika. Iz Grafikona 2. vidljivo je da su BlackBerry, prema anketama iz 2009. godine, više koristili poslovni korisnici, ali je popularnost iPhone uređaja ubrzano rasla. Iz grafikona je vidljivo da ispitanici pametni mobilni terminalni uređaj koriste uglavnom i za privatne i za poslovne svrhe.



Grafikon 2. Svrha korištenja BlackBerry i iPhone uređaja kod poslovnih korisnika
Izvor: [7]

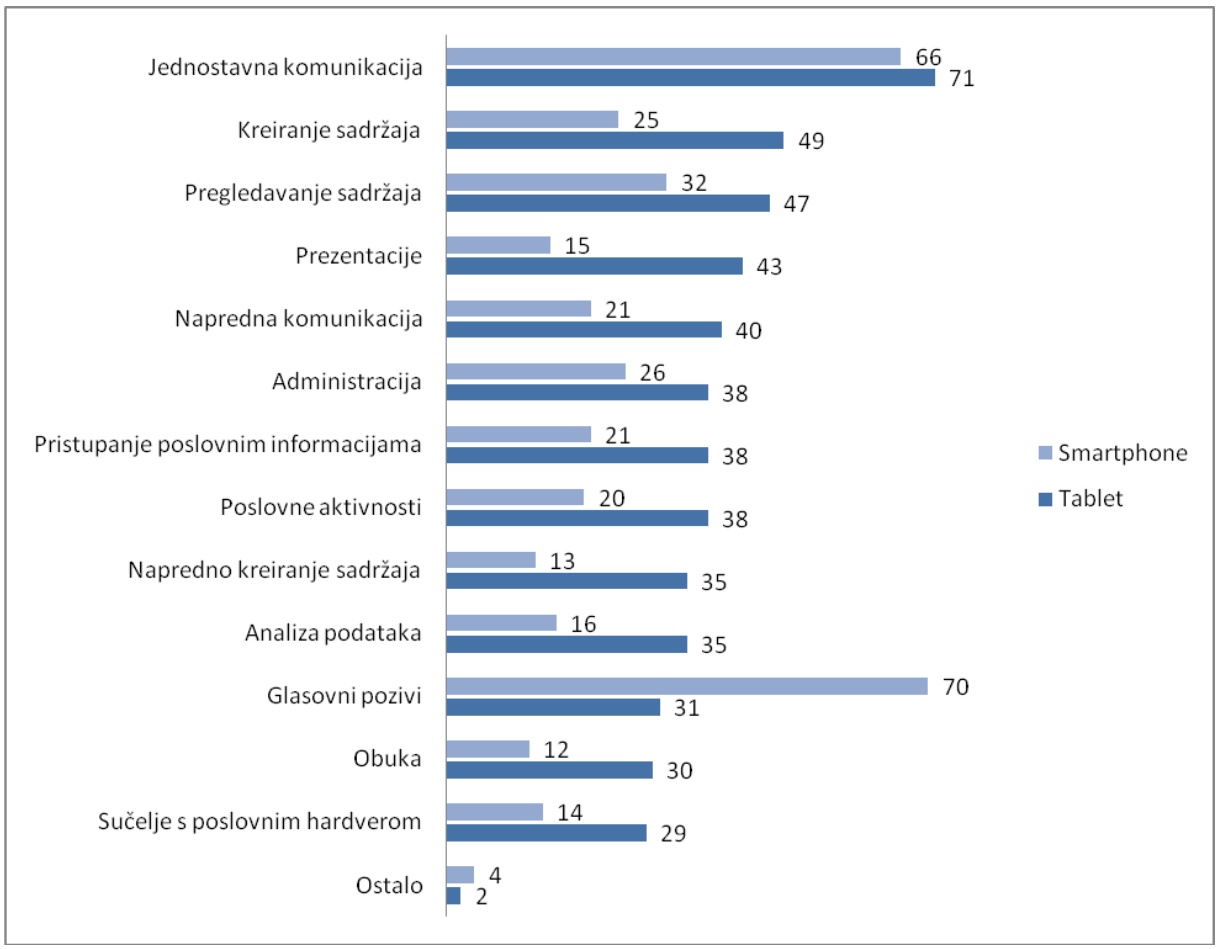
Kod poslovnih korisnika veliku popularnost imali su dlanovnici (PDA) no služili su prvenstveno kao adresari i uređaji za sinkronizaciju nekih podataka sa stolnim računalima. Napretkom tehnologije poslodavci se sve više odlučuju za uvođenje mobilnih terminalnih uređaja u poslovanje. Osim pristupa elektroničkoj pošti i mogućnosti sinkronizacije kontakata, uvođenje mobilnih terminalnih uređaja u poslovanje donosi mnoge prednosti kao što su pristup korporativnim podacima na terenu, optimizacija i smanjenje troškova poslovanja, zadovoljstvo djelatnika i korisnika, obavljanje svakodnevnih zadataka izvan ureda i tako dalje [8].

Nakon uvođenja pametnih terminalnih uređaja u poslovanje, zaposlenici su mogli raditi od kuće. Poslodavci su uglavnom kontrolirali korištenje mobilnih terminalnih uređaja i sprječavali spajanje na mrežu tvrtke. Zaposlenici su morali koristiti više uređaja, odvojenih za privatne i poslovne svrhe. Zaposlenici su također bili primorani koristiti terminalne uređaje koje je odredio poslodavac, te su se sve više počeli koristiti vlastiti terminalni uređaji za poslovne potrebe [9].

3. *BRING YOUR OWN DEVICE* TRENDOVI U HRVATSKOJ I SVIJETU

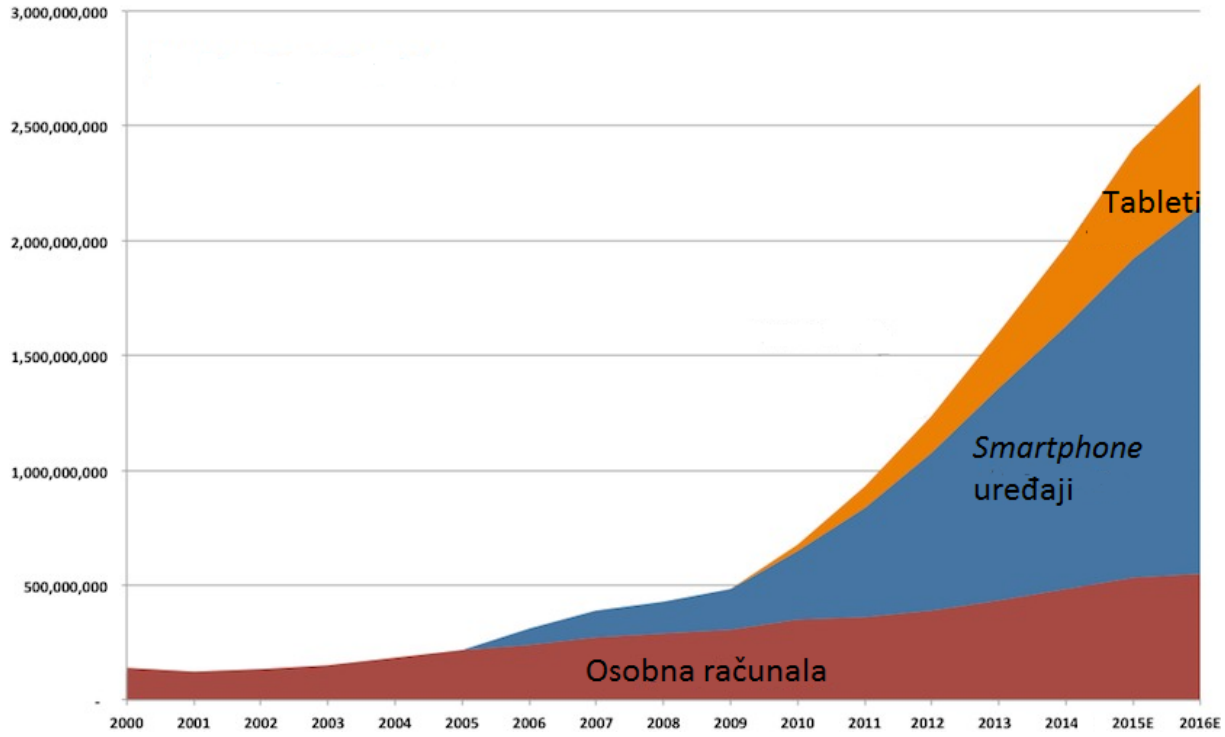
Pametni mobilni terminalni uređaji razvijaju se ovisno o ponašanju korisnika i njihovim sklonostima prema novim tehnologijama. U posljednjih nekoliko godina došlo je do novog trenda u IT okruženju – BYOD – koji su mnoge korporacije i organizacije implementirale u svoje poslovanje. BYOD dozvoljava zaposlenicima da donose svoje vlastite terminalne uređaje kao što su laptopi, pametni mobilni terminalni uređaji i/ili tableti kako bi radili na njima i povezivali se na mrežu tvrtke umjesto da koriste uređaje u korporativnom vlasništvu [10].

Na Grafikonu 3. vidljivo je da je najviše zaposlenika 2012. godine koristilo vlastite terminalne uređaje (tablet i pametni mobilni terminalni uređaj) za jednostavnu komunikaciju. Glasovni pozivi koriste se gotovo 40% više na pametnim mobilnim terminalnim uređajima nego na tabletima. Za sve ostale poslovne aktivnosti više se koriste tableti. Pod pretpostavkom da kod navedenog istraživanja tableti dobivaju prednost zbog preglednosti, danas se ovi rezultati zasigurno uvelike razlikuju od prije četiri godine. Trendovi u području tehnologije mijenjaju se iz godine u godinu, tako pametni mobilni terminalni uređaji imaju sve veće dijagonale ekrana, pregledniji su i kvaliteta prikaza slike sve je veća.



Grafikon 3. Svrha korištenja vlastitih terminalnih uređaja (tableta i pametnog mobilnog terminalnog uređaja) u korporativnom okruženju 2012. godine
Izvor: [11]

Na Grafikonu 4. vidljivo je kako raste prodaja tablet i pametnih mobilnih terminalnih uređaja, te se tableti koriste više od pametnih mobilnih terminalnih uređaja, kao što je prikazano i u Grafikonu 3. Tableti zasigurno imaju prednost u poslovanju zbog veće dijagonale ekrana, a to je jedan od ključnih kriterija s obzirom na pregledavanje poslovnih dokumenata ili pokretanje aplikacija. Iako prema [11] 40% zaposlenika tvrdi da korištenje tableta i pametnog mobilnog terminalnog uređaja smanjuje potrebu za donošenje laptopa na sastanak, ili čak na godišnji odmor, još ga se uvijek ne može potpuno izbaciti iz upotrebe. Osim što laptopi imaju veće dijagonale ekrana, često se na njima nalaze korporativni programski alati koji se ne mogu instalirati na tablet ili pametni mobilni terminalni uređaj, ili ih ima mnogo pa im je lakše pristupiti putem laptopa.



Grafikon 4. Trendovi prodaje pametnih mobilnih terminalnih uređaja i tablet uređaja u odnosnu na osobna računala
Izvor: [12]

3.1. Korištenje BYOD paradigme s gledišta korporacije

Brojne su svjetske korporacije i organizacije kao što su Intel, Citrix Systems, Unisys, Bijela kuća i Apple preuzele vodstvo u implementaciji BYOD programa [10].

Prema istraživanjima iz 2013. godine, više od 70% organizacija usvojilo je BYOD, a prema tadašnjim Gartnerovim predviđanjima, do 2014. godine BYOD će koristiti 90% organizacija [9].

Najnovija Gartnerova istraživanja predviđaju da će do 2017. godine pola poslodavaca zahtijevati od zaposlenika da osiguraju vlastite terminalne uređaje za potrebe rada, dok 38% kompanija u 2016. godini prestaje zaposlenicima pružati uređaje za poslovne svrhe [13]. Tako se smanjuje rizik financijskih gubitaka u slučaju da se zaposleniku osigura uređaj za poslovne svrhe a on ode iz kompanije ubrzo nakon toga. Tvrtkama je isplativije zaposleniku uvjetovati korištenje vlastitog terminalnog uređaja i preuzeti dio korisničkih troškova. Iako na početku uvođenja BYOD trenda poslodavci nisu shvaćali njegove prednosti, danas uglavnom shvaćaju da zaposlenici koriste poslovne uređaje za privatne svrhe i obrnuto.

Korištenjem BYOD paradigme poslodavac ima veću kontrolu nad uređajima i može zaštititi podatke na više načina osim zaključavanja cijelog uređaja.

3.1.1. Prednosti korištenja BYOD-a s gledišta korporacije

Tvrtka može uštedjeti mnogo novca koje bi morala potrošiti na kupnju skupih uređaja da ne koristi BYOD. Kako zaposlenici sami plaćaju svoje uređaje, tvrtke bi mogle uštedjeti i do 80 dolara mjesečno po zaposleniku [9]. No prema [12], čak 66% IT menadžera tvrdi da ušteda nije najveća prednost uvođenja BYOD paradigme u poslovanje. Najveće tri prednosti BYOD-a za korporaciju jesu produktivnost, fleksibilnost i udaljeni rad zaposlenika (Grafikon 5.).

Grafikon 5. Razlozi za uvođenje BYOD-a u poslovanje
Izvor: [12]

Većina ljudi ima tendenciju pratiti trendove najnovije tehnologije. Dakle, može se očekivati da će mnogi zaposlenici uvijek imati najnovije modele uređaja i verzije softvera koje se izvode na tim uređajima. Tako tvrtkama nestaju problemi i troškovi povezani s neprestanom nadogradnjom [9].

Važna je prednost i zadovoljstvo zaposlenika. Cilj je kompanija da implementacijom BYOD-a povećaju fleksibilnost, praktičnost i prenosivost koji utječu na rad zaposlenika, te da se povećava produktivnost i moral. Nedavna istraživanja pokazuju da 80% ispitanika tvrdi da je uvođenje BYOD-a povećalo produktivnost. Više od 2/3 ispitanika porast prihoda pripisuje BYOD-u. Neke kompanije smatraju kako zaposlenici radije ostaju dulje na poslu, odnosno rade prekovremeno, ako koriste vlastite uređaje jer su vrlo dobro upoznati s njima i rade s alatima koje sami biraju [9], [10].

3.1.2. Nedostaci korištenja BYOD-a s gledišta korporacije

Iako se na BYOD može gledati kao na mjeru koja smanjuje troškove za brojne organizacije i korporacije, zapravo može biti skuplja opcija zbog poteškoća s upravljanjem različitim platformama. Osim toga, javljaju se brojni sigurnosni problemi o kojima je potrebno voditi računa. Neke velike korporacije i organizacije izbjegavaju prelazak na BYOD i izmjene u njihovim sigurnosnim protokolima jer ne žele riskirati povećano izlaganje *cyber* prijetnjama i povredama podataka [10].

Još jedan važan razlog zašto neke korporacije izbjegavaju BYOD jest taj što je to relativno novi pojam i potencijalno predstavlja brojne sigurnosne prijetnje, počevši od sigurnosti podataka koji se nalaze u uređajima ili unutar aplikacija. Tvrtke moraju odgovoriti na brojna pitanja prije nego uvedu BYOD politiku. Vrlo je važno uzeti u obzir na koju će se mrežu dozvoliti spajanje uređaja. Potrebno je odrediti uloge uređaja u mreži te im dodijeliti ovlasti, potrebno je kupiti određene licence, odrediti sigurnosnu politiku i usklađenost uređaja s mrežom tvrtke te obrazovati i obučiti zaposlenike o sigurnosti [10].

3.2. Korištenje BYOD paradigme s gledišta zaposlenika

Nakon proširenja trenda korištenja vlastitih mobilnih terminalnih uređaja, kada je gotovo svaki zaposlenik posjedovao mobilni telefon, korporacije su uglavnom kontrolirale njihovu uporabu na radnom mjestu i nisu dozvoljavale spajanje na mrežu tvrtke. Zaposlenici su uglavnom koristili dva ili više uređaja, za privatne i poslovne svrhe, što može biti vrlo nepraktično. Uglavnom nisu mogli birati s kojim će uređajem raditi i kakva će biti njegova konfiguracija. Na uređajima u vlasništvu tvrtke uglavnom nisu dozvoljene instalacije aplikacija po vlastitom izboru, personalizacija ili bilo kakve izmjene koje bi zaposleniku

pojednostavile korištenje. Mnogi zaposlenici počinju koristiti vlastite uređaje u poslovne svrhe bez znanja poslodavaca. Tako se s vremenom usvaja BYOD program u korporacije.

Prema istraživanju koje je proveo Cisco 2013. godine, tri od pet zaposlenika tvrdi da više ne moraju biti u uredu kako bi bili produktivni. Prema predviđanjima do 2015. godine, *International Data Corporation* (IDC) procjenjuje da će u Sjedinjenim Američkim Državama biti preko 200 milijuna zaposlenika koji ne rade samo u uredu. Najveći postotak tih zaposlenika koristi Apple iPhone i Android uređaje. Zanimljivo je da mnogi zaposlenici smatraju da je korištenje vlastitih terminalnih uređaja na poslu njihovo pravo, a ne privilegija [9].

3.2.1. Prednosti korištenja BYOD-a s gledišta zaposlenika

Prednosti donošenja vlastitog uređaja od strane zaposlenika jasne su. Zaposlenici su dobro upoznati s uređajem i mogu sami izabrati koji uređaj žele koristiti [10].

Razvoj tehnologije i brz razvoj pametnih mobilnih terminalnih uređaja pružaju zaposlenicima veću mobilnost i fleksibilnost, a time i veću učinkovitost pri obavljanju svakodnevnih poslovnih zadataka. Zaposlenici su u mogućnosti pristupiti korporativnim podacima izvan radnog mjesta i radnog vremena, tako na primjer mogu raditi od kuće.

3.2.2. Nedostaci korištenja BYOD-a s gledišta zaposlenika

Iako se čini da ne postoje nedostaci pri korištenju vlastitih terminalnih uređaja, zaposlenicima je važno da odvajaju osobne podatke od podataka tvrtke. Pola zaposlenika želi na neki način razdvojiti podatke, na primjer korištenjem dva različita klijenta elektroničke pošte.

Zbog sigurnosti podataka, tvrtka mora imati određen nadzor nad terminalnim uređajima koji se spajaju na mrežu tvrtke i na koje se pohranjuju osjetljivi podaci. Tu se javlja pitanje privatnosti osobnih podataka zaposlenika, ako oni nisu na neki način odvojeni od poslovnih podataka na terminalnom uređaju.

Poslodavci ograničavaju poslovne aktivnosti koje se izvode na vlastitim terminalnim uređajima. Zaposlenici očekuju što manje ograničenja na vlastitim mobilnim terminalnim

uređajima, osobito ako sami plaćaju za njih. Nerijetko se događa da zaposlenici izvode neku od nedozvoljenih radnji, što u pitanje dovodi sigurnost podataka.

Najčešće tvrtka ima listu odobrenih terminalnih uređaja s kojima zaposlenici mogu raditi. Iako zaposlenici imaju pravo na vlastiti izbor terminalnih uređaja, taj je izbor ograničen. Često nesvjesni sigurnosnih rizika i kompleksnosti uvođenja BYOD programa u tvrtku, zaposlenici smatraju da su ograničenjima narušena njihova prava na izbor uređaja, a ako sami plaćaju terminalni uređaj smatraju da imaju potpuno pravo na slobodan izbor.

Sa sigurnosnog aspekta, postoji rizik od curenja korporativnih podataka. Većina zaposlenika spaja se na mrežu tvrtke putem Wi-Fi pristupa, a ta veza često nije kriptirana.

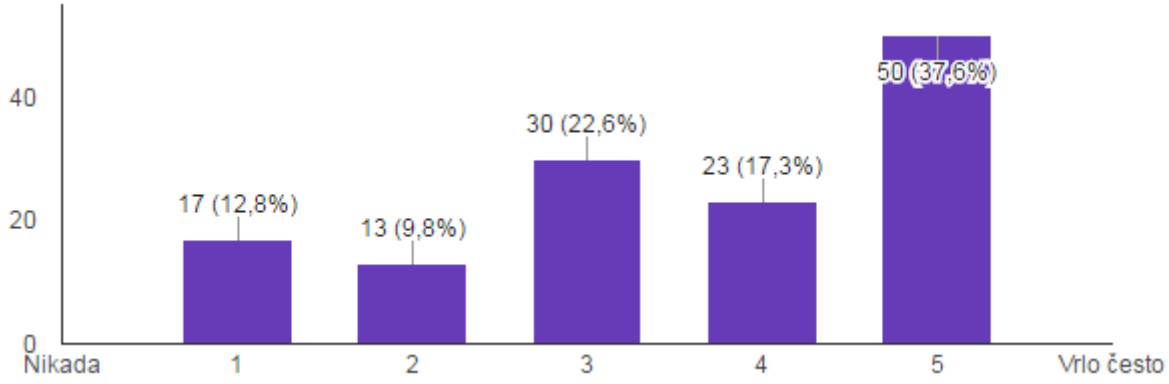
Fizički gubitak ili krađa mobilnog terminalnog uređaja predstavlja nedostatak za zaposlenike kao i poslodavce. Dimenzije mobilnog terminalnog uređaja relativno su male i zaposleniku se lako može dogoditi da ga izgubi. Ako je uređaj bio spojen na mrežu tvrtke i zaposlenik ga izgubi, postoji rizik od zloupotrebe neosiguranih podataka od treće strane. Rizik od zloupotrebe podataka prisutan je i kada zaposlenik ode iz kompanije, ne mora vratiti uređaj s obzirom na to da je u njegovu vlasništvu pa aplikacije i podaci tvrtke mogu ostati na uređaju [14].

3.3. Korištenje BYOD-a u Hrvatskoj

Korištenje vlastitih terminalnih uređaja u korporativnom okruženju u Hrvatskoj nije u tolikoj mjeri dozvoljeno kao što je u vodećim zemljama Europske unije ili u Sjedinjenim Američkim Državama.

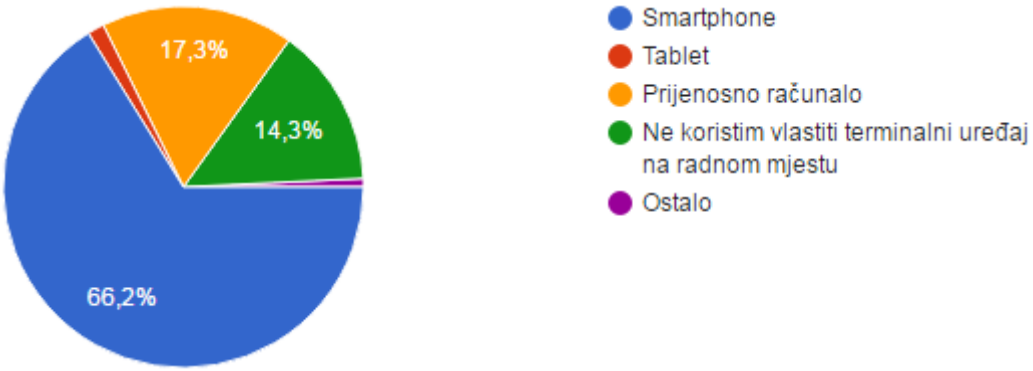
U nekim većim organizacijama kao što su banke i osiguranja, zaposlenicima nije dozvoljeno spajanje vlastitih terminalnih uređaja na mrežu tvrtke. Osim toga, ograničene su radnje na službenim terminalnim uređajima, tako na primjer odjel financija ne može pristupiti YouTube-u, dok marketing može radi potreba istraživanja tržišta. Filtrirane su određene stranice te se njima ne može pristupiti unutar mreže tvrtke. Nikakva prijenosna memorija nije dozvoljena, tako zaposlenici ne mogu donijeti svoju prijenosnu memoriju kako ne bi došlo do prijenosa poslovnih podataka izvan okvira tvrtke. Tako zaštićene firme obično imaju otvorenu Wi-Fi mrežu za goste, ali uz kontrolu podataka.

Prema istraživanju provedenom za potrebe ovog diplomskog rada može se zaključiti da BYOD trendovi u Hrvatskoj nisu razvijeni kao što su razvijeni u Sjedinjenim Američkim Državama ili drugim zemljama Europske unije. Zaposlenici često koriste vlastite terminalne uređaje na radnom mjestu, no mali broj ispitanika vlastiti terminalni uređaj koristi u poslovne svrhe kao što su slanje službenih poruka elektroničke pošte ili preuzimanje poslovnih dokumenata. 17 od 133 ispitanika (12,8%) nikada ne koristi vlastiti terminalni uređaj (pametni mobilni terminalni uređaj, tablet, prijenosno računalo i tako dalje) na radnom mjestu, 13 ispitanika (9,8%) rijetko koristi vlastite terminalne uređaje, 30 (22,6%) ih koristi povremeno, 23 (17,3%) često, a čak 50 ispitanika (37,6%) vlastiti terminalni uređaj na radnom mjestu koristi vrlo često. Navedeni rezultati prikazani su na Grafikonu 6.



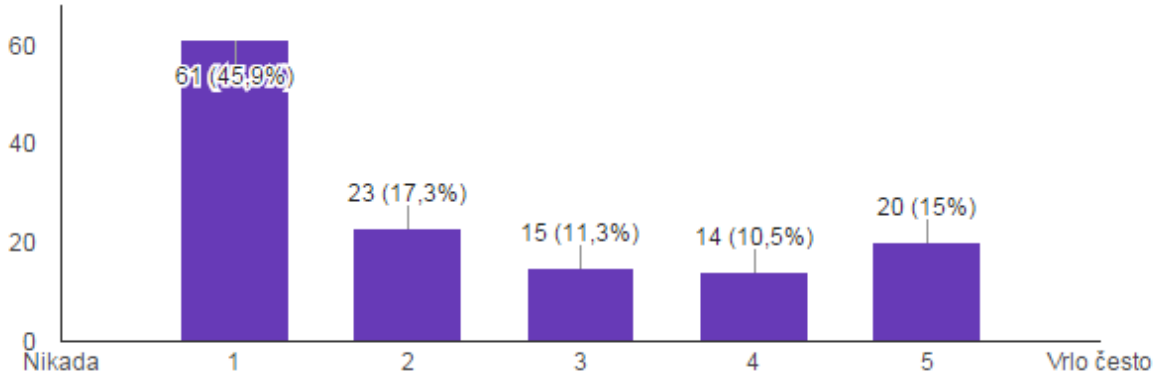
Grafikon 6. Korištenje vlastitog terminalnog uređaja na radnom mjestu

Na radnom mjestu najčešće se koriste pametni mobilni terminalni uređaji (88 ispitanika – 66,2%) i prijenosna računala odnosno laptopi (23 ispitanika – 17,3%). Vrsta vlastitih terminalnih uređaja korištenih na radnom mjestu prikazana je na Grafikonu 7.

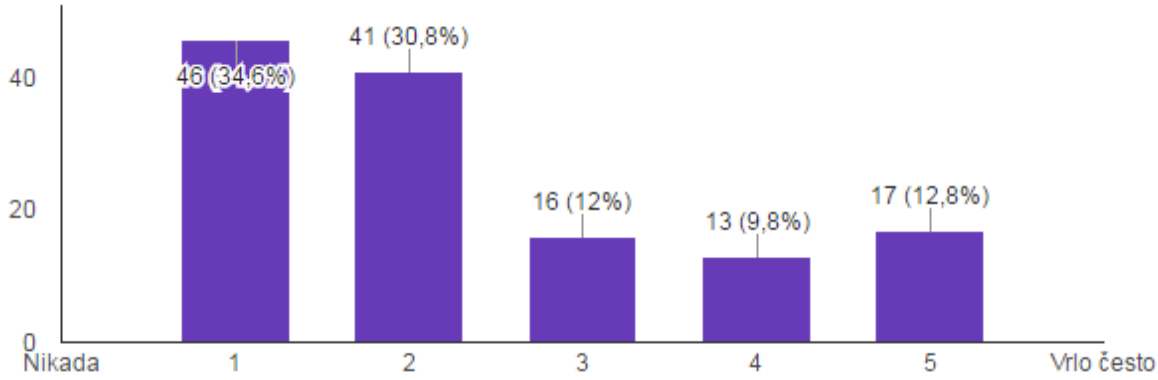


Grafikon 7. Vrsta vlastitih terminalnih uređaja korištenih na radnom mjestu

Iako zaposlenici koriste vlastite terminalne uređaje na radnom mjestu, iz Grafikona 8. vidljivo je da samo 20 ispitanika (15%) vrlo često koristi vlastiti uređaj za slanje službenih poruka elektroničke pošte, dok 61 ispitanik (45,9%) za navedenu svrhu vlastiti terminalni uređaj ne koristi nikada. Iz Grafikona 9. može se iščitati da 46 ispitanika (34,6%) nikada ne preuzima datoteke vezane uz posao na vlastiti uređaj a njih 41 (30,8%) to radi rijetko.



Grafikon 8. Korištenje vlastitog terminalnog uređaja za slanje službenih poruka elektroničke pošte



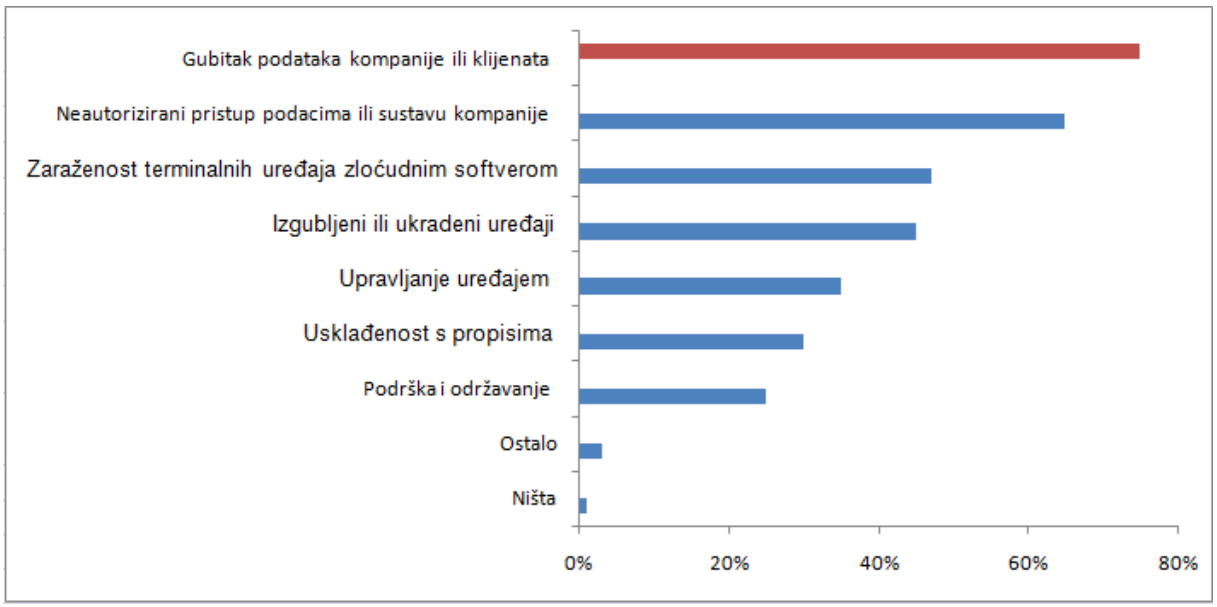
Grafikon 9. Korištenje vlastitog terminalnog uređaja za preuzimanje poslovnih datoteka i dokumenata

4. SIGURNOSNI ASPEKTI PRIMJENE *BRING YOUR OWN DEVICE* PARADIGME

Glavno su sredstvo rada svake kompanije podaci. Kao posljedica korištenja BYOD paradigme, dramatično se povećao broj skupih sigurnosnih incidenata. Osjetljive informacije i podaci o klijentima korporativne mreže mogu lako biti preneseni do nelegitimnog korisnika ili izgubljeni.

Prema [15], 93% mobilnih terminalnih uređaja povezuje se na mrežu tvrtke. Kako BYOD trend brzo raste, stvaraju se dodatni sigurnosni problemi za kompaniju. Podatke o klijentima na svojim mobilnim terminalnim uređajima ima 53% ispitanika. Kao najveći sigurnosni incident zbog kojeg je zabrinuto 94% ispitanika navodi se gubitak ili krađa mobilnog terminalnog uređaja.

Prema anketi provedenoj 2013. godine tri najveća sigurnosna incidenta koja izazivaju zabrinutost kod zaposlenika su gubitak podataka kompanije ili klijenata (75%), neautorizirani pristup podacima ili sustavu kompanije (65%) i zaraženost terminalnih uređaja zloćudnim softverom (47%). Rezultati navedenog istraživanja prikazani su na Grafikonu 10. [15].



Grafikon 10. Sigurnosna pitanja vezana uz BYOD paradigmu
Izvor: [15]

Zbog prenosivosti, malih dimenzija i mogućnosti povezivanja kroz nekoliko dostupnih tehnologija, mobilni su terminalni uređaji osjetljiviji na sigurnosne prijetnje od drugih uređaja kao što su osobna i prijenosna računala. Neke od sigurnosnih prijetnja za mobilne terminalne uređaje jesu sljedeće [16]:

- krađa ili gubitak mobilnog terminalnog uređaja,
- napadi na uređaje namijenjene za recikliranje,
- napadi putem zlonamjernog (malicioznog) sadržaja (virusi, crvi, *spyware*, *adware* i trojanski konji),
- praćenje podataka kroz određene senzore (GPS, brzinomjer, mikrofon, kamera),
- *phishing* napadi,
- iskorištavanje ranjivosti u *web* preglednicima,
- automatsko preuzimanje aplikacija,
- napadi kroz lažirane informacije o mreži,
- eksploatacija mrežnih propusta,
- socijalni inženjering.

Utjecaj tih prijetnji može se odraziti na privatne podatke, intelektualno vlasništvo tvrtke, financijsku imovinu, dostupnost i funkcionalnost terminalnih uređaja i usluga te na osobni i politički ugled.

4.1. Fizički zasnovane prijetnje

Fizički zasnovane prijetnje odnose se na krađu ili gubitak mobilnog terminalnog uređaja. Uvođenjem BYOD aspekta u korporativno okruženje povećava se potreba za prevenciju krađe mobilnih terminalnih uređaja. Mobilne je terminalne uređaje zbog njihovih dimenzija lako izgubiti i lako otuđiti. S obzirom na to da mnogo zaposlenika osim velike količine osobnih podataka na uređaju čuvaju i osjetljive podatke kompanije, zanimljiva su meta kradljivcima, osobito ako znaju kakve se informacije čuvaju na mobilnom uređaju.

Prema [15], svake se godine samo u Ujedinjenom Kraljevstvu ukrade 1,3 milijuna mobilnih terminalnih uređaja. Velikim kompanijama u Sjedinjenim Američkim Državama prosječno je ukradeno 1075 pametnih mobilnih terminalnih uređaja i 640 laptopa svakog tjedna.

Izgubljeni ili ukradeni terminalni uređaji razlog su za većinu izgubljenih podataka. Bez obzira na to, rijetko se poduzimaju mjere za zaštitu podataka tvrtke ili klijenata. Iz tog razloga krađa ili gubitak terminalnog uređaja predstavlja jedan od najvećih BYOD sigurnosnih rizika.

Osim krađe i gubitka mobilnog terminalnog uređaja, fizički zasnovanu prijetnju mogu predstavljati terminalni uređaji namijenjeni recikliranju ili prodaji. Bez obzira na razlog prodaje ili recikliranja terminalnog uređaja, potencijalna opasnost prisutna je ako osoba koja dođe do terminalnog uređaja na neki način zloupotrijebi osobne podatke. Na BYOD terminalnim uređajima uglavnom se nalazi mnogo kontakata iz poslovnog okruženja, korisničkih računa, lozinki, aplikacija namijenjenih poslu i tako dalje. Kod prodaje ili recikliranja osobnog računala ili laptopa korisnici većinom izbrišu osobne podatke s tvrdog diska, ali kod pametnih mobilnih terminalnih uređaja uređaja to uglavnom nije slučaj.

Prema [17], 54% terminalnih uređaja namijenjenih prodaji sadrži osobne informacije. Istraživanje je provedeno kupnjom 35 korištenih mobilnih terminalnih uređaja od kojih je 19 sadržavalo osobne podatke kao što su tekstualne poruke, poruke elektroničke pošte pa čak i bankovne račune. Od 50 kupljenih SIM kartica, 27 ih je sadržavalo osobne podatke unatoč tome što 81% korisnika tvrdi da su svi osobni podaci izbrisani prije prodaje.

Potencijalna opasnost od curenja poslovnih informacija postoji i kada zaposlenik da ili dobije otkaz ili kada odlazi u mirovinu. Mobilni terminalni uređaj može prodati i reciklirati nakon određenog vremena ne znajući da se na uređaju još uvijek nalaze poslovne povjerljive informacije. Ne treba zanemariti ni činjenicu da bivši (ili trenutni) zaposlenik može namjerno odati poslovne informacije, osobito ako se na neki način osjeća zakinuto od strane tvrtke.

4.2. Aplikacijski zasnovane prijetnje

Aplikacijski zasnovanim prijetnjama podrazumijevaju se razni *malware* napadi, a s obzirom na to da se mobilni terminalni uređaji koriste gotovo kao računala i imaju mnogo mogućnosti i funkcionalnosti, prijetnje navedenim uređajima gotovo su iste kao i prijetnje računalima.

Osim napada zloćudnih softvera na terminalne uređaje korištene u korporativnom okruženju, postoji rizik od nenamjernog odavanja podataka od strane zaposlenika i rizik od nadziranja putem određenih senzora na pametnim mobilnim terminalnim uređajima.

4.2.1. *Malware* napadi

Zloćudni softver (eng. *malware*[3]) široka je grupa programa čija je osnovna namjena maliciozno, odnosno zlonamjerno djelovanje, prikriveno od korisnika. Najčešći napadi putem zloćudnog (malicioznog) sadržaja jesu virusi, crvi, spyware, *adware* i trojanski konji.

Virusi su zlonamjerni programi koji bez dopuštenja ili znanja korisnika kopiraju sami sebe u memoriju terminalnog uređaja. Virusi se mogu proširiti sustavom ili mrežom koristeći se ovlastima zaposlenika čiji je uređaj zaražen, što predstavlja veliki sigurnosni rizik ako zaposlenik ima veće ovlasti pristupa korporativnim podacima.

Računalni su crvi programi koji umnožavaju sami sebe i šire se kroz mrežu. Za razliku od virusa, ovi zlonamjerni programi ne trebaju interakciju korisnika kako bi se širili. Crvi iskorištavaju neki sigurnosni nedostatak u samom operacijskom sustavu ili u aplikacijama koje korisnik koristi na terminalnom uređaju.

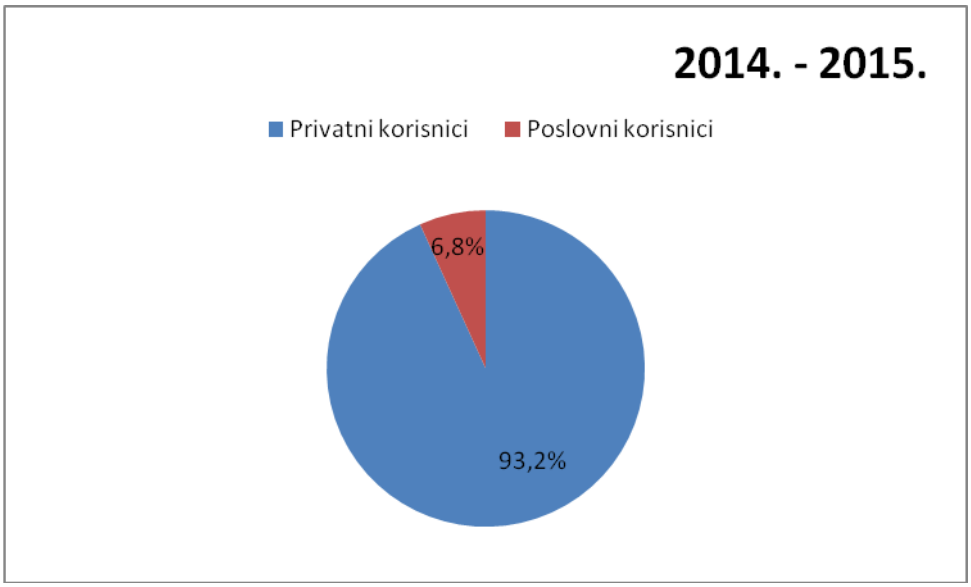
Spyware predstavlja veliki sigurnosni rizik za korporativno okruženje s obzirom na to da se radi o vrsti zlonamjernog programa koji iskorištava zaražene terminalne uređaje za komercijalnu dobit. Zaražene uređaje *spyware* iskorištava za krađu lozinka i osobnih informacija. Ako je dizajniran da prikazuje *pop-up* reklamne prozore ili da preusmjerava na reklamne stranice, radi se o *adware* programu.

Trojanski konj oblik je zloćudnog softvera koji se korisniku lažno predstavlja kao neki korisni softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Za razliku od virusa i crva, trojanski konji ne mogu se sami razmnožavati, ali ih korisnik može prenijeti s jednog uređaja na drugi. Ovaj zlonamjerni program može imati razne primjene, a najčešće se koristi za krađu lozinki i drugih osobnih informacija ili jednostavno za zauzimanje resursa uređaja čime ga vidno usporava.

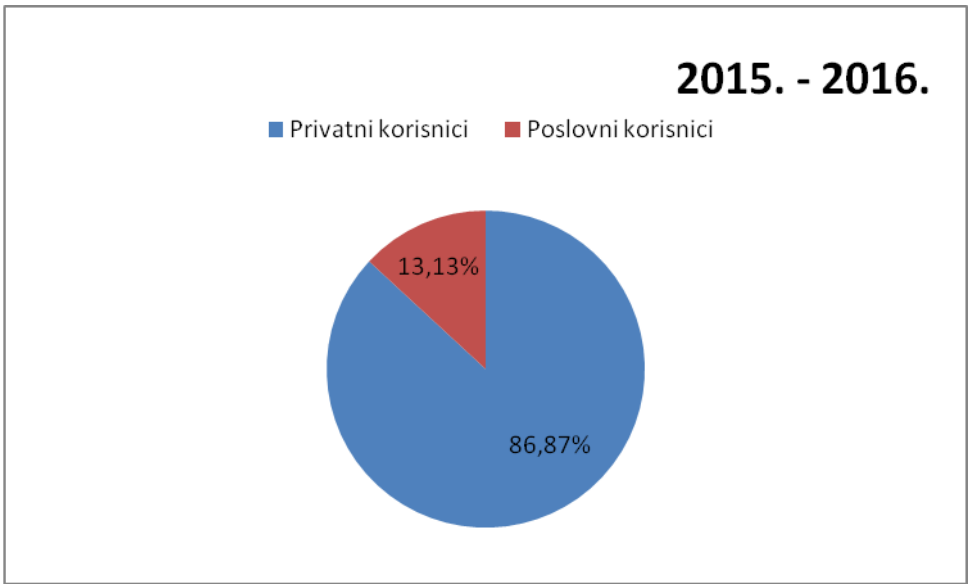
Navedeni zloćudni softveri samo su dio metoda kojim zlonamjerni korisnici pokušavaju ostvariti neku korist, a napadi su sve češći i teže je provoditi sigurnosnu politiku koja bi u potpunosti zaštitila korporativnu mrežu. Jedan je od novijih zloćudnih softvera *ransomware* koji korisniku uskraćuje pristup računalnim resursima te za ponovni pristup traži

[3] Pojam *malware* nastaje od engleskih riječi *malicious* i *software* što u prijevodu znači zloćudni softver

otkupninu. Iako je većina *ransomware* napada usmjerena na privatne korisnike, na Grafikonima 11. i 12. vidljiv je gotovo dvostruki porast *ransomware* napada u korporativnom okruženju, s 6.8% 2014. godine na 13.13% 2016. godine [18].

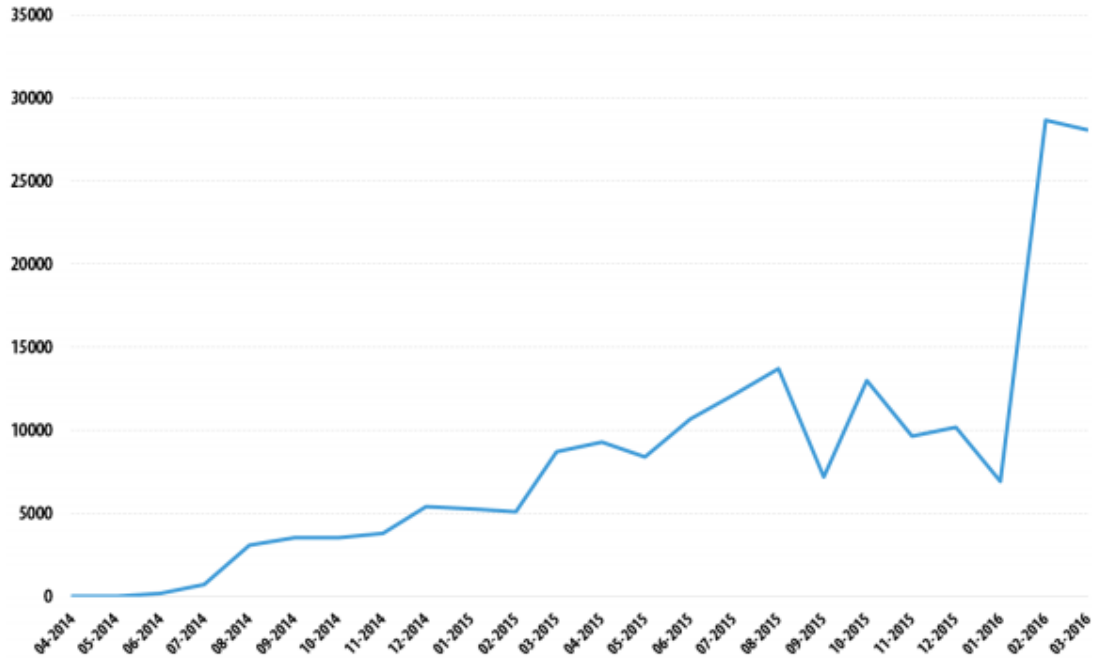


Grafikon 11. Postotak *ransomware* napada na privatne i poslovne korisnike od 2014. do 2015. godine
Izvor: [18]



Grafikon 12. Postotak *ransomware* napada na privatne i poslovne korisnike od 2015. do 2016. godine
Izvor: [18]

Broj korisnika koji su žrtve *ransomware* napada na mobilnim terminalnim uređajima povećao se skoro četiri puta. Broj *ransomware* žrtava se povećao s 35 413 korisnika u razdoblju od 2014. do 2015. godine na 136 532 korisnika u razdoblju od 2015. do 2016. godine, što je prikazano na Grafikonu 13. [18].



Grafikon 13. Broj korisnika koji su barem jednom bili žrtve *ransomware* napada na mobilnom terminalnom uređaju u razdoblju od travnja 2014. godine do ožujka 2016. godine [18]

4.2.2. Nenamjerno odavanje podataka

Nenamjerno odavanje podataka vrsta je aplikacijski baziranih prijetnji kod kojih korisnici samostalno odobravaju pristup osobnim podacima određenim aplikacijama, bilo iz neznanja ili nemara. Većina mobilnih aplikacija zahtijeva pristup nekim osobnim informacijama i korisnici najčešće bez čitanja prihvaćaju uvjete korištenja jer u suprotnom nisu u mogućnosti instalirati željenu aplikaciju na mobilni terminalni uređaj.

Ne razmišljajući o sigurnosnom aspektu, korisnici dozvoljavaju pristup aplikacijama za koje je očigledno da im za normalan rad nije potrebna tolika količina osobnih informacija. Aplikacije zahtijevaju pristup lokaciji, fotoaparatu, galeriji, identitetu, vanjskoj pohrani uređaja i tako dalje. Zaposlenici, odnosno korisnici BYOD uređaja, trebali bi biti oprezniji pri instalaciji aplikacija na mobilni terminalni uređaj i dobro pročitati uvjete korištenja.

4.2.3. Nadziranje korištenjem pametnih mobilnih terminalnih uređaja

Nadziranje korištenjem pametnih mobilnih terminalnih uređaja podrazumijeva praćenje podataka pomoću određenih senzora (GPS, brzinomjer, mikrofon, kamera). Tehnološki napredak senzora na mobilnim terminalnim uređajima omogućuju aplikacije koje se temelje na lokaciji. Navedeni senzori donose brojne prednosti za napredno korištenje uređaja, ali se javlja pitanje privatnosti osobnih podataka.

Zlonamjerni korisnik je u mogućnosti putem senzora na pametnom mobilnom terminalnom uređaju utvrditi korisnikovu lokaciju, pa čak i otkriti njegov identitet. Praćenjem svakodnevnih kretnji može se ustanoviti u kojoj tvrtki zaposlenik radi. Privatnost podataka obično se regulira pravilima o privatnosti koja informiraju korisnika o načinu na koji pružatelj usluge raspolaže podacima. Odluka o korištenju senzora na terminalnim uređajima ostaje na korisniku [19].

4.3. *Web* zasnovane prijetnje

Web zasnovane prijetnje podrazumijevaju iskorištavanje ranjivosti u *web* preglednicima i automatsko preuzimanje aplikacija. Kod obje prijetnje korisnik, odnosno zaposlenik, smatra da se nalazi na legitimnoj *web* stranici. Neka korporativna okruženja zbog provođenja sigurnosne politike blokiraju *web* odredišta koja nisu usko vezana uz posao koji tvrtka obavlja.

4.3.1. Iskorištavanje ranjivosti u *web* preglednicima

Postoje dva najčešća načina iskorištavanja ranjivosti *web* preglednika – proučavanje pregledničkih datoteka i navođenje korisnika na postupke koji ga dovode u kompromitirajuću situaciju. Obje metode najčešće rezultiraju otkrivanjem povjerljivih korisničkih podataka. Informacije o korisniku, kako navodi [20], moguće je otkriti pomoću nekoliko pregledničkih datoteka – datoteka iz priručne memorije (eng. *cache files*), datoteka s poviješću surfanja (eng. *history file*) i *bookmark* oznaka. U takozvanoj *history* datoteci čuvaju se poveznice koje je korisnik posjetio (kod većine preglednika pamte se podaci za prethodnih 30 dana), što napadaču daje informacije o korisničkim interesima. *Bookmarks* oznake predstavljaju sličan problem jer otkrivaju napadaču koje stranice korisnik najčešće posjećuje. Priručna memorija omogućava brže pristupanje informacijama kojima je korisnik nedavno pristupio. Budući da se pregledom neke *web* stranice ona sprema lokalno, kod

sljedećeg pristupa preglednik ne mora dohvaćati podatke preko mreže. Tako *bookmarks* oznake i priručna memorija predstavljaju sigurnosnu prijetnju - ako je označena neka stranica koja zahtjeva korisničko ime i zaporku za pristup, napadač najčešće može uvidom u priručnu memoriju otkriti te zaporke ili barem korisnička imena.

Navođenje korisnika na postupke koji ga dovode u kompromitirajuću situaciju najčešće se svodi na preusmjeravanje prema zlonamjerno oblikovanoj *web* stranici na kojoj tada korisnik ostavlja svoje osobne podatke. Na primjer, korisnik se nalazi na *web* stranici banke u kojoj ima otvorene račune. Želi pregledati stanje svojih računa, ali klikom na poveznicu koja ga je trebala preusmjeriti na stranicu s računima zapravo je preusmjeren na stranicu sličnog izgleda, ali pod kontrolom napadača [20].

4.3.2. Automatsko preuzimanje aplikacija

Automatsko preuzimanje aplikacija podrazumijeva nenamjerno preuzimanje ili instalaciju malicioznog softvera koji može naštetiti uređaju. Pri ovoj vrsti napada, dovoljno je samo posjetiti *web* stranicu i bez opcije prihvaćanja preuzimanja, maliciozni kod započinje svoje djelovanje u pozadini uređaja. Obično se, prema [21], iskorištavaju preglednici, aplikacije i operacijski sustavi koji nisu ažurirani i imaju sigurnosne propuste.

Početni maliciozni kod malen je i neprimjetan, a obično se koristi za obavještavanje drugih uređaja uključenih u zlonamjerne radnje koji zatim vrše instalaciju ostatka koda na pametni mobilni terminalni uređaj, tablet ili računalo. Nerijetko *web* stranica sadržava nekoliko različitih vrsta malicioznog koda, što daje veću mogućnost pronalaska sigurnosnog propusta na uređaju. Ovakva preuzimanja mogu biti smještena na *web* stranicama koje izgledaju legitimno, a korisnik može primiti poruku elektroničke pošte s poveznicom na stranicu, tekstualnu poruku ili kao novost na društvenim mrežama. Dok korisnik pregledava stranicu za koju smatra da je legitimna, u pozadini se preuzima aplikacija bez njegovog pristanka i znanja [21].

4.4. Socijalni inženjering

Ljudska ranjivost, neznanje i nepažnja jedan je od najlakših načina na koji zlonamjerni korisnici dolaze do željenih podataka. Socijalni je inženjering postupak manipulacije osoba u svrhu nedozvoljenog prikupljanja pristupnih ili nekih drugih povjerljivih informacija od strane

zlonamjernih korisnika bez izravnog proboja u sustav. Kako bi osoba bila socijalni inženjer nije potrebno veliko tehničko znanje, dovoljno je primijeniti neku od brojnih taktika napada i iskoristiti ljudsko povjerenje, želju za pomoć ili naivnost.

Zaposlenici koji koriste BYOD terminalne uređaje mogu napraviti ozbiljan sigurnosni propust kompaniji ako postanu žrtve socijalnog inženjeringa. Često zaposlenici prijenosne terminalne uređaje, zbog brojnih funkcionalnosti i mogućnosti koje pružaju, koriste kao računala. Prema tome, osim nasjedanja na SMS poruku poslanu od strane zlonamjernog korisnika, neovlašteni pristup trećoj strani mogu dozvoliti slijeđenjem poveznice iz poruke elektroničke pošte ili otvaranjem *pop-up* prozora koji nose poruku o prekidu mrežne povezanosti i zahtjev za ponovnim unošenjem lozinki. S obzirom na to da postoji velik broj aplikacija za *smartphone* uređaje, korisnici lako postaju žrtve neke vrste socijalnog inženjeringa instalacijom zlonamjernih aplikacija na svoj uređaj ili omogućavanjem vidljivosti svojih informacija a da toga nisu svjesni.

Osnovni je cilj socijalnog inženjeringa povećati prava pristupa sustavu ili informacijama s mogućnošću [22]:

1. izvođenja prijevara – dobivanje vjerodostojnica legitimnih korisnika najčešće se koristi za izvođenje prijevara koje nanose novčanu štetu.

2. upada u mrežu – poznavanje osjetljivih korisničkih podataka (korisničko ime i lozinka) omogućuje prijavu na sustav s jednakim pravima koja su dodijeljena legitimnom korisniku.

3. industrijskog špijuniranja – otkrivanje povjerljivih podataka neke organizacije moguće je iskoristiti za razne svrhe poput ostvarivanja konkurentnosti na tržištu ili prodaje ideja konkurentskim organizacijama.

4. krađe identiteta – dobivanjem korisničkih imena, lozinki ili drugih vjerodostojnica napadač se može predstaviti kao korisnik.

5. jednostavnog narušavanja sustava ili mreže – dobivanje pristupa sustavu omogućuje napadaču nanošenje štete te izvođenje svih akcija koje su dozvoljene korisniku čije je podatke otkrio. To može uključivati brisanje, izmjenu ili pregled

datoteka, umetanje lažnih podataka, blokiranje mreže, stvaranje nepotrebnih konekcija i slično.

Novčana šteta najveća je šteta koja se može nanijeti kompaniji, osobito ako se radi o velikoj količini novca. Uspješno izvođenje takvih prijevara može ozbiljno oštetiti ugled kompanije, a na taj način kompaniija može izgubiti povjerenje korisnika i poslovnih partnera.

Ovisno o tome kakve se povjerljive informacije nalaze na mreži tvrtke, upad u mrežu poznavanjem osjetljivih korisničkih podataka kao što su korisnička imena i lozinke može izazvati ozbiljnu financijsku štetu, povredu podataka, narušenje ugleda, a zaposleniku čiji je korisnički račun kompromitiran zasigurno nije osigurana budućnost u kompaniji. Kompanije bi trebale voditi računa o edukaciji zaposlenika kako ne bi došlo do krađe identiteta.

Tipične žrtve napada su [22]:

- telefonske kompanije,
- tvrtke s uslugama oglašavanja,
- poznate organizacije,
- financijske institucije,
- vojne i vladine agencije,
- bolnice.

Najraširenija vrsta socijalnog inženjeringa je *phishing* [4]napad. *Phishing* je vrsta prijevare kod koje zlonamjerni korisnik odnosno napadač putem elektroničke pošte (najčešće) korisnika preusmjerava na lažna *web* odredišta. Lažna *web* stranica nalazi se na poslužiteljima napadača, a najčešće se od korisnika traži da unese svoje korisničke podatke. U BYOD okruženju vjerojatnije je da će se napadač koristiti *spear phishing* metodom. *Spear phishing* metoda usmjerena je na jednog korisnika, napad je personaliziran pa je veća vjerojatnost da zaposlenik nasjedne na prevaru, a ako unese korisničke podatke za pristup poslovnim aplikacijama napadač lako može doći do korporativno osjetljivih podataka.

[4] Naziv „*phishing*“ dolazi od iskrivljene engleske riječi „*fishing*“ što znači pecanje.

5. METODE ZAŠTITE OSJETLJIVIH PODATAKA U KORPORATIVNOM OKRUŽENJU

Može se reći da je vrijednost podataka i informacija u korporativnom okruženju veća od osobnih podataka nekog pojedinca. Valjana informacija u pravom trenutku i na pravom mjestu može donijeti prednost na tržištu onom koji je posjeduje, a samim tim raste i cijena takve informacije.

Potrebno je provoditi određene metode zaštite osjetljivih podataka u korporativnom okruženju ako je cilj kompanije uspješno poslovanje i konkurentnost na tržištu. Vrijednost informacije, posebno u informacijskom dobu u kojem živimo, često prelazi vrijednost fizičke imovine, a gubitak ili izmjena korporativnih podataka nerijetko je nenadomjestiv.

Prema tome, potrebno je uvesti sigurnosnu politiku i standarde u korporativno okruženje kojih su se svi dužni pridržavati, od zaposlenika i poslodavaca pa sve do poslovnih partnera i klijenata. Zaposlenicima i osoblju teško se pridržavati nečega o čemu ne znaju, stoga je nužno zaposlenike educirati i ukazati im na povećanje sigurnosnih rizika u slučaju nepoštivanja pravila i standarda.

Korporativnim podacima potrebno je na neki način upravljati, osobito kada se prakticiraju BYOD trendovi. Broj uređaja koji se spajaju na korporativnu mrežu je velik, osobito kada zaposlenici donose vlastite terminalne uređaje na radno mjesto. Organizacije iz tog razloga trebaju imati određenu kontrolu nad terminalnim uređajima kako bi mogli upravljati sadržajem i na taj način smanjiti sigurnosne rizike za poslovne informacije.

5.1. Pojam i važnost korporativnih podataka i informacija

U informacijskom dobu u kojem živimo, sigurnost korporativnih podataka postaje sve važnija sastavnica ekonomske sigurnosti i gospodarske dinamike. Suvremeno poslovanje sve više ovisi o poslovnim informacijama, a neki autori, prema [23], smatraju kako se budući ratovi neće voditi vojnim, već gospodarskim i financijskim sredstvima.

Informacija je postala jedna vrsta robe koja ima svoju uporabnu vrijednost, a samim time i cijenu. Informacija je roba koja se prodaje i kupuje, a često predstavlja i najvredniju robu kompaniji, vrjedniju od fizičke imovine. Informacijom se trguje kao i svakom drugom robom, a njezina specifičnost u odnosu na ostale vrste roba ogleda se u tome što joj korištenjem vrijednost uglavnom ne opada, već raste i što onaj tko je proda, ne ostaje bez nje. Informacija se procjenjuje na temelju rezultata koji se uz pomoć nje ostvaruju. Razni korisnici, pa čak i jedan isti, mogu imati različitu korist od iste informacije, što ovisi o osobnom iskustvu i znanju, postojanju prethodnih informacija, o trenutku u kojem su je dobili, o načinu kako su je dobili, mogućnosti da se iskoristi, kao i o okruženju [24].

Vrijednost, odnosno upotrebljivost poslovne informacije u prvom redu ovisi o [24]:

- njezinoj aktualnosti,
- njezinoj točnosti,
- njezinoj pouzdanosti,
- njezinoj trajnosti,
- njezinoj raspoloživosti i
- mjeri u kojoj zadovoljava potrebe korisnika.

Danas o podacima i informacijama ovisi uspješnost poslovanja građana kao pojedinca, poduzeća, država, nacionalnih i svjetskih poslovnih sustava i svjetske zajednice. Ugrožavanje ili poremećaj u sustavu informiranja izaziva lančanu negativnu reakciju u svim navedenim sustavima. Informacije i njihov razvoj predstavljaju osnovu za razvoj društva u cjelini, zato je pitanje zaštite i sigurnosti podatka i informacija jedno od najvažnijih pitanja opće sigurnosti [23].

Prema Zakonu o informacijskoj sigurnosti Republike Hrvatske informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda [25].

Značaj informacije u vrlo brzom razvoju svjetskog gospodarstva i društvenih odnosa sve je veći i danas ne postoji niti jedna razvijena zemlja, ali isto tako i korporacija koja nema izrazito razvijene sustave zaštite podataka, naročito onih koji su ocijenjeni kao vrlo značajni za organizaciju. Moderno je poslovanje u velikoj mjeri utemeljeno na razmjeni velikog broja

poslovnih informacija unutar kompanije, između različitih kompanija te između kompanija i njihovih klijenata. Biti ukorak sa svjetskim trendovima i modernizacijom svih oblika komunikacija zahtijeva i shvaćanje značaja sigurnosti informacijsko-komunikacijskih sustava. Kod sigurnosti informacija od ključne je važnosti održati integritet, povjerljivost i raspoloživost resursa informacijskog sustava [23]. Upravo su integritet[5], povjerljivost[6] i raspoloživost[7] tri osnovna načela informacijske sigurnosti.

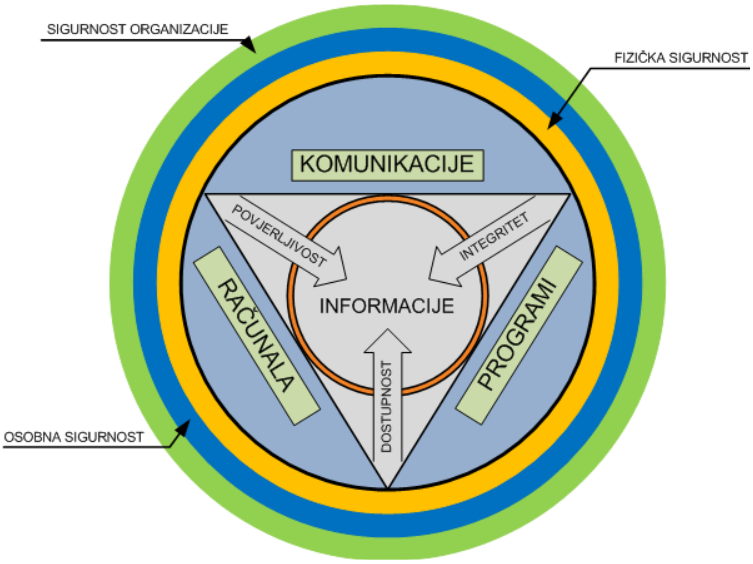
5.2. Sigurnosna politika i standardi

Sigurnosna je politika skup pravila i postupaka kojima se određuje razina sigurnosti nekog informacijskog sustava, istovremeno pridajući pažnju sigurnosti tehnologije i informacija koje informacijski sustav sadrži. Sigurnosnom politikom korisniku se nameću obvezna pravila ponašanja i odgovornosti kako bi se zaštitio informacijski sustav, to jest informacije pohranjene u informacijskom sustavu, od vanjskih utjecaja (udaljenih napada, zlonamjernih programa i tako dalje), ali također i korisnika (neovlašteni pristup podacima, krađa podataka, izmjena podataka i tako dalje). Sigurnosnom politikom osiguravaju se tri svojstva informacija koje sadrži neki sustav (integritet, povjerljivost i raspoloživost), što je prikazano Slikom 2. [27].

[5] Integritet je zaštita postojanja, točnosti i kompletnosti informacije kao i procesnih metoda [26].

[6] Povjerljivost označava osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj [26].

[7] Raspoloživost podrazumijeva osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva [26].



Slika 2. Sigurnosne informacijske komponente - CIA (eng. *Confidentiality, Integrity, Availability*) [27]

Sigurnosna politika tvrtke ili institucije prilagođava se potrebama, te nije jednaka za sve. Sigurnosnu politiku predstavlja službena izjava ili plan organizacije koji obuhvaća ciljeve, smjernice i prihvatljive postupke. Ona uključuje sljedeće zahtjeve [27]:

- potrebno je poštovati pravila definirana sigurnosnom politikom,
- nepoštivanje pravila može rezultirati sankcijama ili kaznama nadležnih institucija,
- potrebno je usredotočiti se na rezultate, a ne na način provedbe sigurnosne politike i
- određivanje sigurnosne politike se temelji na unaprijed definiranim standardima i smjernicama.

Sigurnosna politika uobičajeno ima više značenja, no kod zaštite informacija u korporativnom okruženju koriste se specifična sigurnosna pravila za određeni sustav, na primjer elektronička pošta, identifikacija, pravo pristupa i slično. Efikasna sigurnosna politika pridonosi razvoju i implementaciji boljeg i učinkovitijeg sigurnosnog programa i zaštite sustava i informacija cjelokupne organizacije [23].

Standardi, smjernice[8] i procedure[9] koriste se kako bi se opisali načini na koji će sigurnosna politika biti implementirana unutar organizacijskih okvira. One omogućavaju

[8] Standardi i smjernice specificiraju tehnologiju i metodologiju koja se koristi kako bi se zaštitili sustavi.

[9] Procedure su detaljni koraci koji slijede pri ostvarenju zadataka koji imaju veze sa sigurnošću.

korisnicima, menadžerima i zaposlenicima jasniji pristup prilikom implementacije politike i zadovoljenja organizacijskih ciljeva. Standardi, smjernice i procedure mogu se objaviti i razglasiti kroz cijelu organizaciju putem priručnika, regulacija ili uputa [23].

5.3. Edukacija zaposlenika i osoblja

Kako bi sigurnosna politika bila efikasna, potrebno je provesti postupke edukacije. Neke organizacije zahtijevaju da se svi zaposlenici upoznaju sa sigurnosnom politikom svake godine. Stvaranje svijesti o prijetnjama, ponašanju koje napadači iskorištavaju te metodologijama čini važan dio strategije zaštite od istih prijetnji. Postoje mnogi alati koji se mogu iskoristiti pri edukaciji poput video zapisa, brošura, znakova (natpisa na radnom mjestu, zaslonu računala, podsjetnika) i slično. Programi edukacije imaju ulogu [22]:

- upoznavanja zaposlenika sa sigurnosnom politikom,
- stvaranje svijesti o rizicima i mogućim gubicima,
- treniranja s ciljem prepoznavanja sigurnosnih prijetnji.

Nije dovoljno zaposlenicima ukazati što i kako činiti, nego ih je potrebno upoznati s posljedicama koje donose prijetnje. Organizacija mora imati jedinstveni identifikator za svakog zaposlenika koji će biti povezan s pravima pristupa tog zaposlenika. Identifikatorom se zaposleniku određuju prava pristupa informacijama na sustavu. U tome se vidi prednost korištenja posebnog identifikatora za svakog zaposlenika. U slučaju da napadač sazna identifikator nekog korisnika, on ima pravo pristupa samo onim informacijama koje su dodijeljene tom korisniku dok su ostali dijelovi sustava zaštićeni [22].

5.4. Sigurnosno upravljanje korporativnim podacima

Iako BYOD model donosi mnoge prednosti zaposlenicima i poslodavcima, pojavljuje se pitanje sigurnosti osjetljivih informacija. Kroz uređaj koji nije u vlasništvu organizacije pohranjuju se, obrađuju i šalju osjetljive informacije, a neautorizirani pristup takvim informacijama mogao bi imati ogromne negativne posljedice na organizaciju. Organizacije iz tog razloga žele i trebaju imati određenu kontrolu nad uređajima kako bi smanjila rizik od neautoriziranog pristupa ili manipulacije informacijama [15].

Osim kontrole BYOD uređaja, poslodavci, odnosno IT stručnjaci koji brinu o sigurnosti podataka korporacije, moraju omogućiti sigurnu komunikaciju unutar tvrtke i izlaz na javne

mreže uspostavljanjem virtualne privatne mreže (eng. *Virtual Private Network* – VPN). S obzirom na to da virtualna privatna mreža ne osigurava podatke na BYOD terminalnim uređajima, potrebno je vršiti nadzor takvih terminalnih uređaja.

Nadzor terminalnih uređaja može ugroziti privatnost njegovog vlasnika, odnosno zaposlenika tvrtke. Navedeni problem može se riješiti razdvajanjem privatnih i poslovnih podataka. Razdvajanjem se smanjuje rizik od narušavanja korisničke privatnosti i neautoriziranog pristupa osjetljivim informacijama tvrtke [15].

5.4.1. Virtualna privatna mreža

Virtualna privatna mreža koristi se za zaštitu od prisluškivanja i upadanja drugih korisnika u mrežu. Svaka kompanija koja brine o sigurnosti trebala bi koristiti VPN mrežu. Dobra konfiguracija VPN mreže omogućuje sigurnost, pouzdanost, skalabilnost[10] te mogućnost upravljanja mrežom i sigurnosnom politikom.

Ako je ispravno konfigurirana, implementacija VPN mreže u poslovno okruženje potpomaže očuvanju triju osnovnih načela informacijske sigurnosti (integritet, povjerljivost i raspoloživost). Povjerljivost je najvažnije svojstvo VPN mreže s obzirom na to da se privatni podaci tvrtke šalju putem javne mreže. Povjerljivost se može postići enkripcijom[11], odnosno šifriranjem podataka. Integritet podataka postiže se IPsec protokolom koji osigurava da ne dođe do izmjene poruke u prijenosu. Ako se kod prijenosa podataka poruka izmjeni, paket se otpušta. Kod VPN mreže provodi se autentikacija, autorizacija i revizija (eng. *Authentication, authorization, and accounting* – AAA). Kada se ne bi koristila autentifikacija, svaki korisnik koji pristupi uređaju s unaprijed konfiguriranom VPN mrežom može joj lako pristupiti. Korisnička imena i lozinke mogu biti pohranjeni na VPN terminalnom uređaju ili na vanjskom

[10] Skalabilnost je sposobnost sustava da obrađuje povećan broj zahtjeva, odnosno da se prilagođava povećanju i smanjenu opterećenja.

[11] Enkripcija je proces izmjene podataka iz izvornog oblika u oblik koji je nečitljiv za korisnike kojima poruka nije namjenjena, već da je mogu pročitati samo uređaji koji posjeduju ključ za dekripciju.

AAA poslužitelju koji može pružiti autentifikaciju drugim bazama podataka kao što su na primjer LDAP[12] baze [28].

VPN mreža pomaže osigurati komunikaciju između BYOD terminalnih uređaja i korporativne mreže, ali ne osigurava podatke pohranjene na BYOD terminalne uređaje [29]. Iz tog razloga, nije dovoljno koristiti samo VPN mrežu, već je potrebno upravljati podacima koji se nalaze na BYOD uređajima.

5.4.2. Sustav za upravljanje mobilnim sadržajem

Sustav za upravljanje mobilnim sadržajem (eng. *Mobile Content Management System* – MCM) vrsta je CMS sustava (eng. *Content Management System* – CMS) koji služi za pohranu i isporuku sadržaja i usluga na mobilne terminalne uređaje. MCM sustav može biti izveden kao diskretan sustav ili kao dio većeg CMS sustava. Kod BYOD terminalnih uređaja koriste se tri glavne metode upravljanja mobilnim sadržajem, a to su sustav za upravljanje mobilnim uređajem, sustav za upravljanje mobilnim aplikacijama i sustav za upravljanje informacijama na mobilnom uređaju.

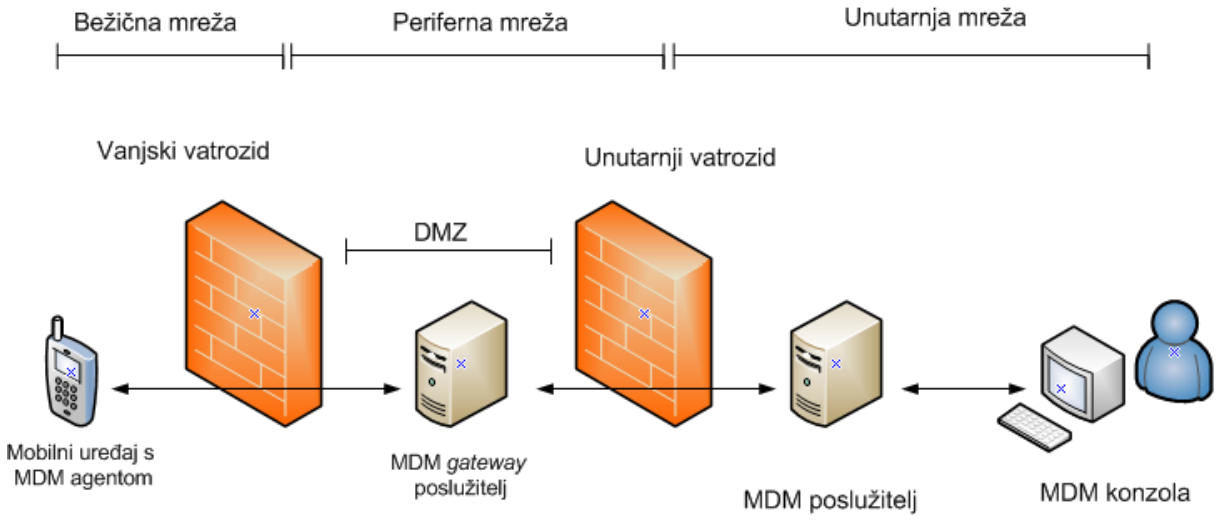
5.4.2.1. Sustav za upravljanje mobilnim terminalnim uređajem

Sustav za upravljanje mobilnim terminalnim uređajem (eng. *Mobile Device Management* – MDM) sustav je za daljinsko nadziranje funkcija mobilnih terminalnih uređaja. Sastoji se od dviju glavnih komponenti, MDM agenta i MDM poslužitelja. MDM agent aplikacija je koja je instalirana na mobilnom uređaju i šalje svoj status i podatke do MDM poslužitelja. MDM poslužitelj upravlja primljenim podacima te sukladno njima aktivira naredbe na registriranom mobilnom terminalnom uređaju. Ovisno o potrebi, ima mogućnost zaključavanja terminalnih uređaja, kontrole nad njime i šifriranja podataka [30].

MDM sustav sastoji se od nekoliko komponenti, kao što su MDM poslužitelj i *gateway* poslužitelj (takozvani relej poslužitelj), MDM konzole i MDM agenta, odnosno softvera koji može biti instaliran na mobilni terminalni uređaj. Na Slici 3. prikazana je opća *shema* MDM arhitekture unutar mreže poduzeća. U navedenoj arhitekturi, softverski program (agent) se distribuira preko treće strane, kao što je trgovina aplikacija, i instalira se na mobilni

[12] LDAP (eng. Lightweight Directory Access Protocol) je aplikacijski protokol koji se koristi za čitanje i pisanje imenika putem IP mreže.

terminalni uređaj. Glavni je cilj agenta prenijeti podatke s mobilnog terminalnog uređaja i informacije o korisniku do MDM poslužitelja i primijeniti odgovarajuću politiku te provoditi administrativne poslove kao što su udaljeno brisanje podataka [30].



Slika 3. Arhitektura sustava za upravljanje mobilnim terminalnim uređajem (eng. *Mobile Device Management* – MDM)
Izvor: [31]

Mobile Device Management (MDM) višenamjenski je sustav koji tvrtkama daje mogućnost da strogo kontroliraju mobilne terminalne uređaje. MDM upravlja protokolima, osigurava konstantan nadzor i praćenje, izvodi ažuriranja, sinkronizira datoteke, pokreće udaljeno brisanje podataka, podržava VPN vezu, provodi *anti-malware* skeniranje, te osigurava izvještaj svih aktivnosti. MDM je koristan za kompanije koje zahtijevaju centralizirano i pojednostavljeno rješenje za sigurnosne prijetnje [31].

MDM obično podržava kontrolu nad cijelim mobilnim terminalnim uređajem i oslanja se na gotova softverska rješenja, a bazira se na nadziranje, kontrolu i zaštitu podataka. Ovaj sustav ima mogućnost vidjeti aplikacije instalirane na uređaju i prema tome provoditi sigurnosnu politiku. Sigurnosni pristup baziran na MDM sustavu omogućava kontrolu nad terminalnim uređajima bez obzira na to koji servisi i usluge se na njemu nalaze, stoga se pojavljuje pitanje privatnosti zaposlenika [32].

5.4.2.2. Sustav za upravljanje mobilnim aplikacijama

Sustav za upravljanje mobilnim aplikacijama (eng. *Mobile Application Management* – MAM) rješenje je koje koriste IT administratori kako bi mogli udaljeno instalirati, ažurirati, uklanjati i nadzirati aplikacije na mobilnim terminalnim uređajima koje su povezane s poduzećem.

Za razliku od MDM-a koji vrši kontrolu mobilnih terminalnih uređaja na hardverskom sloju, MAM prati i kontrolira određene aplikacije sukladno pravilima i zahtjevima tvrtke. Tvrtka može, na primjer, koristiti MAM za ograničenje aplikacija vezanih uz poslovanje, a druge aplikacije ostaviti bez nadzora. Aplikacije izvan granica MAM nadzora ostaju privatne što zaposlenicima daje određenu privatnost [30], [31].

5.4.2.3. Sustav za upravljanje informacijama na mobilnom terminalnom uređaju

Upravljanje informacijama na mobilnom terminalnom uređaju (eng. *Mobile Information Management* – MIM) omogućuje korporacijama da umjesto nadziranja mobilnih terminalih uređaja osiguraju ključne osjetljive podatke tvrtke. Glavni je cilj MIM-a sačuvati poslovne informacije na nekoj centralnoj lokaciji (na primjer u privatnom *cloudu*) i sigurno ih dijeliti između različitih krajnjih točaka i platformi [30].

Primarna je zadaća MIM-a integritet i enkripcija podataka, određivanje primjene i pristupa aplikacijama od strane zaposlenika, osiguranje sinkronizacije dokumenata između više uređaja dok istovremeno obavlja sigurnosne procedure kao što su skeniranje zloćudnih softvera [31].

6. DESKRIPTIVNA ANALIZA SVJESNOSTI ZAPOSLENIKA O SIGURNOSNIM ASPEKTIMA PRIMJENE *BRING YOUR OWN DEVICE* PARADIGME

Za potrebe ovog diplomskog rada istraživanje je provedeno elektroničkim putem, slanjem poveznice na anketu naziva „Istraživanje sigurnosnih aspekata primjene vlastitih uređaja u korporativnom okruženju“.

6.1. Analiza rezultata dobivenih provedenim istraživanjem

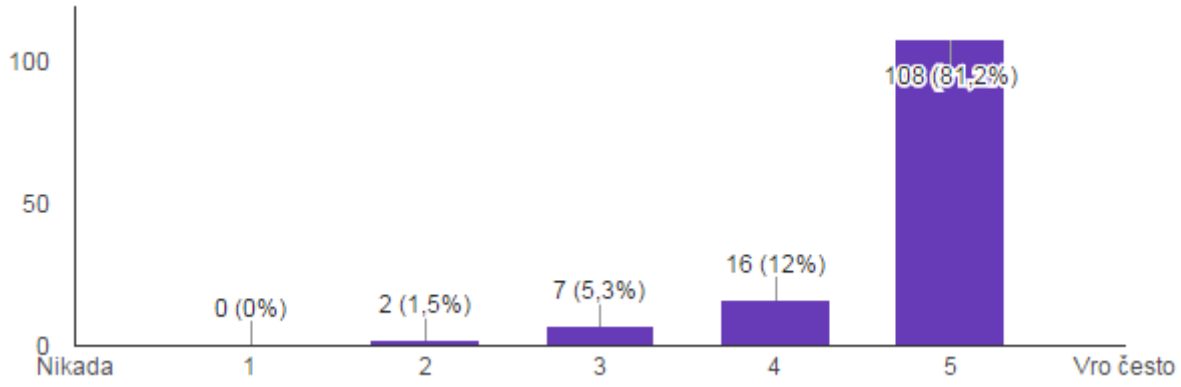
Ciljana skupina korisnika za ovo istraživanje bile su isključivo zaposlene osobe. U istraživanju je sudjelovalo 133 ispitanika, od čega su 67 žene i 66 muškarci. Najviše ispitanika, njih 59 (44.4%) pripada dobnoj skupini od 26 do 35 godina, dok njih sedam (5.3%) pripada dobnoj skupini od 46 do 55 godina. Anketu nije ispunila ni jedna osoba mlađa od 18 godina ni starija od 55 godina.

74 ispitanika navelo je da su zaposlenici Hrvatske akademske i istraživačke mreže – CARNet, 6 ih je zaposleno u različitim osiguravajućim kućama ili bankama, dok su 4 ispitanika zaposlenici Hrvatskog Telekoma. Ostali ispitanici zaposleni su u velikim poduzećima kao što su Dukat d.d., Ericsson Nikola Tesla d.d. i McDonald's ili u velikim i srednjim tvrtkama poput Omiko d.o.o., Chromos MB d.o.o., Medical Intertrade d.o.o., Human Resources Cloud d.o.o., Autoturist turizam d.o.o., Quehenberger Logistics d.o.o. i tako dalje.

Stupanj obrazovanja kod većine ispitanika je visoka stručna sprema (44.4%), dok 22.6% ima srednju stručnu spremu, 19.5% visoku školsku spremu, 12.8% magisterij, a samo jedan ispitanik (0.8%) ima doktorat.

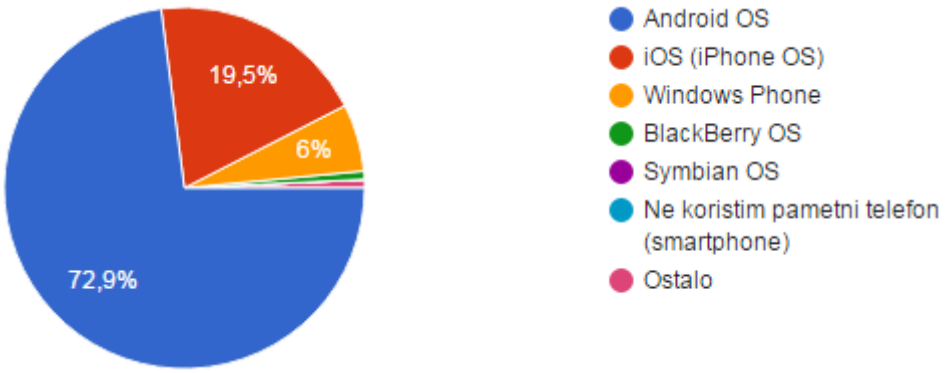
6.1.1. Trendovi korištenja pametnih mobilnih terminalnih uređaja

Iz rezultata ankete može se zaključiti da svi ispitanici koriste pametni mobilni terminalni uređaj (*smartphone*), a njih 108 (81.2%) pametnim mobilnim terminalnim uređajem koristi se vrlo često što je vidljivo iz Grafikona 14.



Grafikon 14. Učestalost korištenja pametnog mobilnog terminalnog uređaja

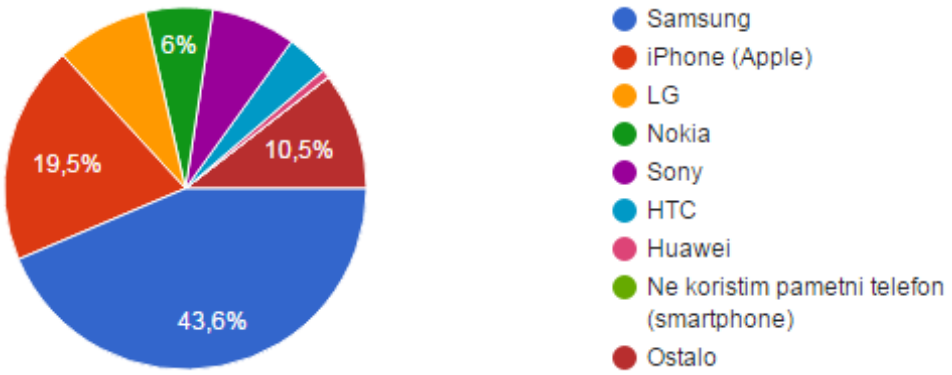
Može se reći da su rezultati o korištenju operacijskog sustava očekivani s obzirom na trenutnu situaciju na tržištu. Vodeći je Android OS s 97 korisnika (72.9%). Drugi po redu je iOS s 26 korisnika (19.5%). Ovdje je vidljiva promjena situacije na tržištu u posljednjih nekoliko godina, odnosno pad broja korisnika iOS operacijskog sustava. Windows Phone OS koristi osam ispitanika (6%), dok jedan ispitanik koristi BlackBerry OS. Jedan ispitanik korisnik je operacijskog sustava koji nije naveden u istraživanju. Rezultati korištenja navedenih operacijskih sustava vidljivi su na Grafikonu 15.



Grafikon 15. Korištenje određenih operacijskih sustava

Vodeći proizvođač pametnih mobilnih terminalnih uređaja je Samsung (58 ispitanika – 43,6%), što nije iznenađujuće s obzirom na trenutnu dominaciju na tržištu. U posljednjih nekoliko godina vidljiv je pad broja iPhone korisnika (26 ispitanika – 19,5%), što je vrlo malo ako se u obzir uzme dosadašnja dominacija na tržištu. Treći najpopularniji proizvođač je LG (11 ispitanika – 8,3%). 10 ispitanika (7,5%) koristi Sony, osam (6%) Nokiju, pet (3,8%) HTC i

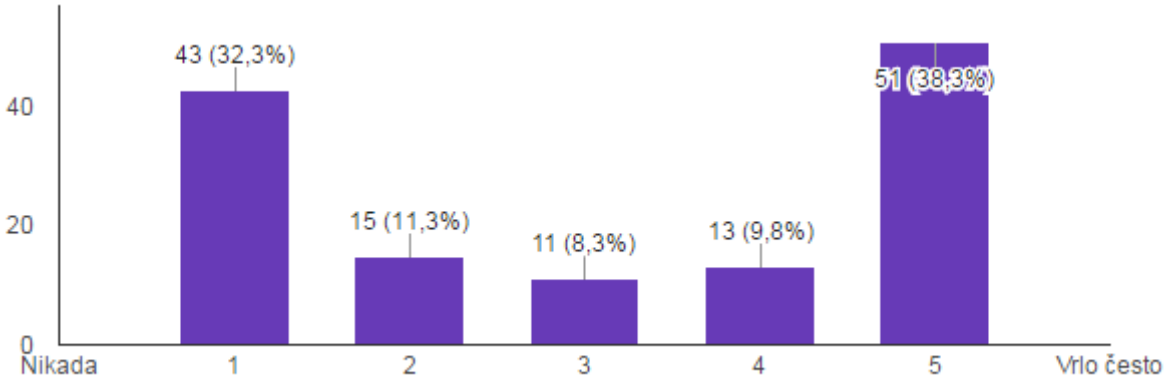
jedan (0,8%) Huawei. Preostalih 14 ispitanika (10,5%) ne koristi ni jednog od navedenih proizvođača koji su vidljivi u legendi na Grafikonu 16.



Grafikon 16. Korištenje određenih proizvođača pametnih mobilnih terminalnih uređaja

6.1.2. Svjesnost sigurnosnog aspekta primjene vlastitih terminalnih uređaja u korporativnom okruženju

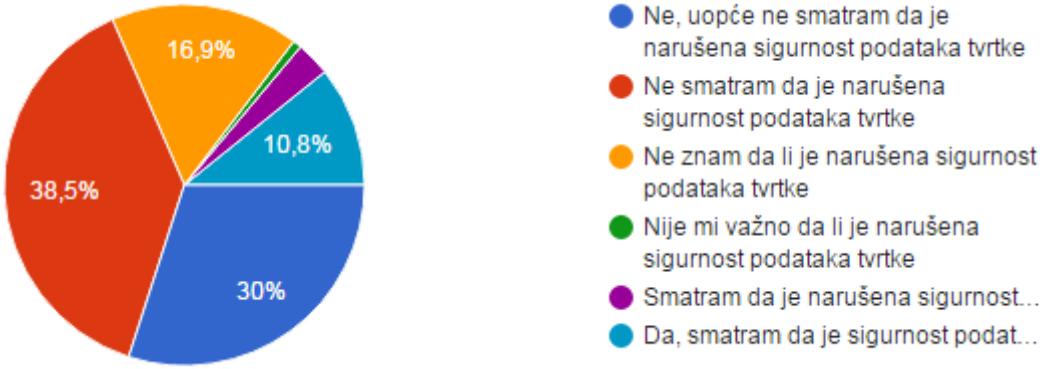
Provedeno istraživanje pokazuje da većina korisnika (njih 51 – 38.3%) spaja vlastiti terminalni uređaj na mrežu tvrtke vrlo često ili se ne spaja uopće (43 ispitanika – 32,3%) što je vidljivo na Grafikonu 17.



Grafikon 17. Učestalost pristupanja mreži vlastitim uređajem u korporativnom okruženju

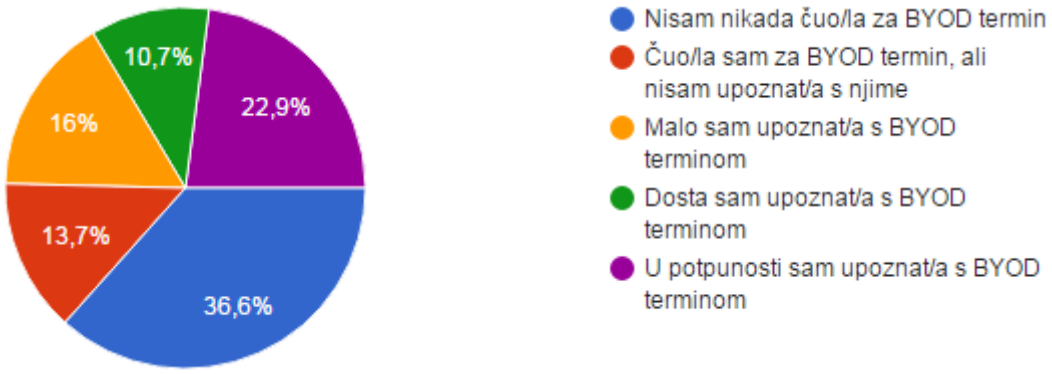
Zabrinjavajući su rezultati svjesnosti korisnika o sigurnosnim aspektima povezivanja vlastitog terminalnog uređaja na mrežu tvrtke (Grafikon 18.). 30% ispitanika uopće ne smatra (s većim uvjerenjem) da je narušena sigurnost podataka tvrtke, dok 38,55% ne smatra (s manjim uvjerenjem) da je narušena sigurnost podataka. Moglo bi se reći da 68,55%

ispitanika nije svjesno sigurnosnog aspekta primjene vlastitih terminalnih uređaja u korporativnom okruženju. 16,9% ispitanika ne zna je li narušena sigurnost podataka tvrtke, 0,8% navodi da nije važno je li narušena sigurnost podataka, 3,1% smatra da je narušena sigurnost podataka tvrtke ali ne smatra to važnim, dok samo 10,8% ispitanika smatra da je sigurnost podataka tvrtke uvelike narušena. Rezultati o svjesnosti sigurnosnog aspekta vlastitih podataka pristupanjem na mrežu tvrtke vrlo su slični.



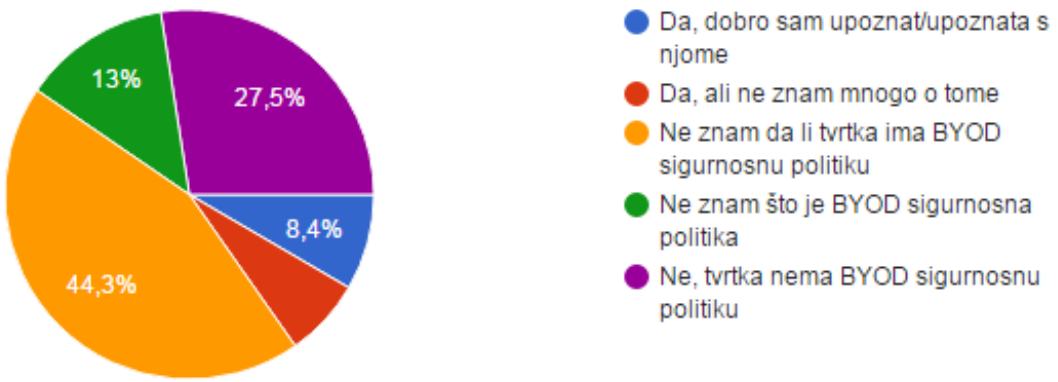
Grafikon 18. Svjesnost narušavanja sigurnosti podataka tvrtke pristupanjem na mrežu vlastitim terminalnim uređajem

Više od polovice ispitanika nije upoznato s terminom BYOD (Grafikon 19.). Njih 36,6% nikada nije čulo za termin BYOD, a 13,7% ih je čulo za navedeni termin, ali nisu upoznati s njime. 16% ispitanika je slabo upoznato s BYOD terminom. 10,7% ispitanika je dobro upoznato s BYOD terminom, dok njih 22,9% navodi kako je u potpunosti upoznato s tim terminom.



Grafikon 19. Postotak ispitanika upoznatih s BYOD terminom

Prema provedenom istraživanju iz Grafikona 20. može se zaključiti da zaposlenici nisu dovoljno educirani, odnosno ne znaju kakva je sigurnosna politika tvrtke i na koje načine se osigurava sigurnost podataka tvrtke. Čak 44,3% ispitanika ne zna da li tvrtka u kojoj su zaposleni ima BYOD sigurnosnu politiku. 27,5% ispitanika tvrdi da tvrtka u kojoj su zaposleni ne provodi BYOD sigurnosnu politiku, a 13% navodi da ne zna što je BYOD sigurnosna politika. 6,9% ispitanika tvrdi da tvrtka ima BYOD sigurnosnu politiku, ali zaposlenik ne zna mnogo o tome, dok samo njih 8,4% navodi da tvrtka provodi BYOD sigurnosnu politiku i zaposlenik je dobro upoznat s njome.



Grafikon 20. Postotak tvrtki koje provode BYOD sigurnosnu politiku

Tvrtke uglavnom provode određene metode zaštite korporativnih podataka. 51,6% ispitanika navodi kako tvrtka u kojoj su zaposleni provodi određene radnje kako bi zaštitili podatke od zloćudnih softvera i smatra da je to od ključne važnosti. 28,9% ispitanika navodi kako tvrtka u kojoj su zaposleni provodi određene radnje kako bi zaštitili podatke od zloćudnih softvera i smatra to vrlo važnim. 18,8% zaposlenika ne zna je li i na koji način se tvrtka štiti od zloćudnih softvera. Grafikon 21. prikazuje provodi li tvrtka u kojoj su ispitanici zaposleni određene metode zaštite od zloćudnih softvera.

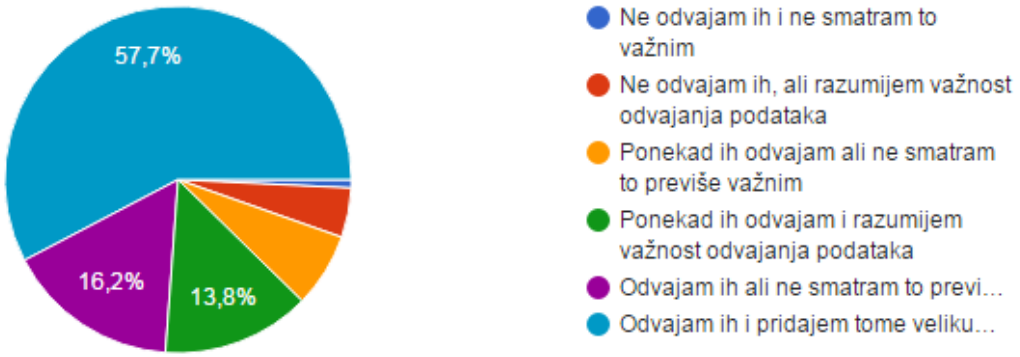
Grafikon 21. Provođenje određenih metoda zaštite od zloćudnih softvera u tvrtkama u kojima su ispitanici zaposleni

Tvrtke u kojima su ispitanici zaposleni uglavnom provode određene metode za zaštitu privatnosti podataka, 38% zaposlenika smatra da je to od ključne važnosti. 25,6% ispitanika navodi kako tvrtka provodi zaštitu privatnosti korporativnih podataka i smatra da je to korisno. 33,3% ispitanika ne zna provodi li tvrtka određene metode za zaštitu privatnosti podataka. Rezultati su prikazani na Grafikonu 22.

Grafikon 22. Provođenje određenih metoda zaštite privatnosti korporativnih podataka u tvrtkama u kojima su ispitanici zaposleni

Zaposlenici su uglavnom svjesni razlike između privatnih i poslovnih podataka i odvajaju ih što je prikazano Grafikonom 23. 57,7% ispitanika odvaja privatne podatke i podatke tvrtke i smatra to vrlo važnim. 16,2% ispitanika odvaja privatne podatke i podatke tvrtke, ali ne smatra to previše važnim. 13,8% ispitanika ponekad odvaja podatke, ali

razumije važnost odvajanja podataka. 6,9% ih ponekad odvaja, ali ne smatra to važnim. 4,6% ispitanika ne odvaja privatne podatke i podatke tvrtke ali razumije važnost odvajanja podataka, dok 0,8% ispitanika ne odvaja podatke i ne smatra to važnim.



Grafikon 23. Odvajanje privatnih podataka i podataka tvrtke

6.2. Preporuke za povećanje sigurnosti korporativnih podataka

Bez obzira na koji način, tvrtkama bi prioritet trebala biti zaštita osnovnih načela informacijske sigurnosti (integritet, povjerljivost i raspoloživost). U današnje vrijeme informacije predstavljaju veću vrijednost kompanijama nego fizička imovina, i kako bi se osigurala konkurentnost na tržištu od ključne je važnosti te informacije štititi.

Prema provedenom istraživanju može se zaključiti da zaposlenici nisu dovoljno educirani o sigurnosti korporativnih podataka ili ih to ne zanima jer smatraju da se to ne odnosi i ni na koji način ne utječe na njih.

Tvrtka koja zaposlenicima dozvoljava korištenje vlastitih terminalnih uređaja na radnom mjestu trebala bi osigurati stalnu edukaciju i upoznati ih s promjenama koje se događaju. Kontinuirana edukacija smanjila bi broj sigurnosnih incidenata jer do njih, u najvećem broju slučaja, dolazi upravo zbog neznanja ili nepažnje zaposlenika ili osoba unutar korporativnog okruženja. Zaposlenicima treba pokazati primjer kompromitiranja podataka kako bi bili svjesni svih rizika koji prijete podacima u korporativnom okruženju.

Osim edukacije zaposlenika, tvrtka mora provoditi određene metode za suzbijanje zloćudnih softvera. Iako ne postoji metoda koja je 100% sigurna jer uvijek prijete novi zloćudni softveri i zlonamjerni korisnici imaju nove metode napada, važno je podići razinu

sigurnosti na najveću moguću mjeru. Većina tvrtki provodi sigurnosnu politiku iako zaposlenici često toga nisu svjesni i ne znaju što se događa u pozadini.

Ako tvrtka zaposlenicima dozvoljava korištenje vlastitih uređaja na radnom mjestu trebala bi provoditi određene mjere za upravljanjem mobilnim sadržajem, bilo da se radi o kontroli nad cijelim uređajem (sustav za upravljanje mobilnim uređajem) ili samo određenim aplikacijama (sustav za upravljanje mobilnim aplikacijama). Prema provedenom istraživanju može se zaključiti da tvrtke uglavnom ne provode BYOD sigurnosnu politiku. BYOD trend nije razvijen u Hrvatskoj pa zaposlenici ne znaju da se provodi upravljanje sadržajem ili poslodavci nisu svjesni rizika koje donose vlastiti terminalni uređaji zaposlenika pa ne pridaju tome toliku pažnju, što također nije dobar pokazatelj za sigurnost korporativnih podataka.

7. ZAKLJUČAK

U ovom diplomskom radu provedeno je istraživanje sigurnosnog aspekta primjene vlastitih uređaja u korporativnom okruženju. BYOD predstavlja jedan od novijih uzroka ranjivosti podataka gdje zaposlenici unutar korporacije pristupaju osjetljivim korporativnim podacima korištenjem vlastitih uređaja, odnosno prijenosnih računala, pametnih mobilnih terminalnih uređaja, tablet uređaja i slično. Prema rezultatima istraživanja može se zaključiti da zaposlenici u Hrvatskoj ne koriste vlastite terminalne uređaje na radnom mjestu u onoj mjeri u kojoj se koriste u Sjedinjenim Američkim Državama i ostalim državama Europske unije. U slučajevima kada se koriste vlastiti terminalni uređaji, nije usvojen BYOD termin.

Vlastiti pametni mobilni terminalni uređaji i laptopi najviše se koriste u korporativnom okruženju. Navedene terminalne uređaje zaposlenici uglavnom uopće ne povezuju na mrežu tvrtke ili ih povezuju vrlo često. Rezultati svjesnosti rizika koji postoji spajanjem vlastitih uređaja na korporativnu mrežu su zabrinjavajući, zaposlenici ne smatraju da na bilo koji način mogu naštetiti korporativnim podacima. Kako bi se ta situacija i način razmišljanja promijenili, potrebna je kontinuirana edukacija zaposlenika.

Tvrtke uglavnom provode sigurnosnu politiku i koriste razne metode za zaštitu osjetljivih korporativnih podataka. Može se zaključiti da su zaposlenici uglavnom nezainteresirani ili smatraju da ih se sigurnost podataka ne tiče, pa ne znaju kako i u kojoj mjeri tvrtka provodi sigurnosnu politiku. Provođenje sigurnosti zadaća je IT stručnjaka i zaposlenici ne trebaju i ne smiju znati na koji način se štite podaci, ali moraju biti svjesni vlastitih postupaka i posljedica koje namjerne ili nenamjerne greške donose.

Zaposlenici su svjesni razlike između privatnih i poslovnih podataka i uglavnom ih razdvajaju. S obzirom na to da ispitanici nisu svjesni sigurnosnih rizika korporativnih podataka, a odvajaju vlastite podatke, može se zaključiti da su više zabrinuti za vlastite nego za korporativne podatke. Zaposlenici smatraju da korporativni podaci nisu u njihovom vlasništvu i da njihovo kompromitiranje ni na koji način ne utječe na njih. Posljedice sigurnosnih propusta mogu biti vrlo velike ne samo za tvrtku nego i za njene zaposlenike, čime se ponovno prikazuje važnost kontinuirane edukacije zaposlenika.

LITERATURA

[1] Sarwar, M., Soomro, T. R.: *Impact of Smartphones on Society*, European Journal of Scientific Research, 98(2), 216-226., 2013.

[2] Peraković, D., Šarić, S., Husnjak, S.: *Analysis of the evolution of terminal devices in the use of SMS service*, Fakultet prometnih znanosti, Sveučilište u Zagrebu, 2012.

[3] Peraković, D., Husnjak, S., Remenar, V.: *Research of security threats in the use of modern terminal devices*, Fakultet prometnih znanosti, Sveučilište u Zagrebu, 2012.

[4] Brad Reed, 2010, *—A brief history of Smartphones*, http://www.networkworld.com/slideshows/2010/061510-smartphone-history.html#slide1 (pristupljeno lipanj 2016.)

[5] Sugio, T., Kondo, S., Iguchi, M., Nishi, T., Toma, T., & Sasai, H.: *Mobile Terminal Device*, U.S. Patent Application No. 11/661,919., 2007.

[6] *Data and Research on Digital for Business Professionals*, eMarketer http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (pristupljeno srpanj 2016.)

[7] Business Insider, *Chart of the day*, http://www.businessinsider.com/chart-of-the-day-iphone-surprisingly-popular-for-business-2009-8 (pristupljeno srpanj 2016.)

[8] *Mobilna rješenja u poslovnom okruženju* http://www.infotrend.hr/clanak/2008/4/mobilna-rjesenja-u-poslovnom%20okruzenju,13,446.html (pristupljeno srpanj 2016.)

[9] Keys, J.: *Bring Your Own Devices (BYOD)Survival Guide*, International Standard Book Number-13: 978-1-4665-6503-6, 2013.

[10] J. P. Shim, Mittleman, D., Welke, R., French, A. M., Guo, J. C.: *Bring Your Own Device* (BYOD): *Current Status, Issues, and Future Directions*, Georgia State University, 2012.

[11] McKinsey and Company: BYOD: *From company-issued to employee-owned devices*, Telecommunications, Media, and Technology Practice, 2012.

[12] Macquarie Telecom Group: *BYOD Top 6 Trends you need to know about in 2015*, https://macquarietelecomgroup.com/news/byod-top-6-trends/ (pristupljeno kolovoz 2016.)

[13] Gartner Inc.: http://www.gartner.com/newsroom/id/2466615, (pristupljeno srpanj 2016.)

[14] Ajaykumar, M., Kuntesh, J.: *Comparative Study on Bring Your Own Technology* (BYOT): *Applications & Security,* Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015

[15] Singh, M. M.,Siang, S. S., San, O. Y., Hashimah, N., Malim, A. H., Shariff, A. R. M.: *Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model*, International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 4, No.5, 2014.

[16] Peraković, D., Husnjak, S., Cvitić, I.: *Comparative analysis of enterprise mobility management systems in* BYOD *environment,* Research Conference In Technical Disciplines, 2014.

[17] BullGuard Security Centre: *The dangers involved with selling or recycling your mobile phone,* http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/the-dangers-of-recycling-your-smartphone.aspx, (pristupljeno kolovoz 2016.)

[18] Kaspersky, *KSN Report: Ransomware in 2014-2016*, Kapersky Lab., 2016.

[19] Gruteser, M., Schelle, G., Jain, A., Han, R., Grunwald, D.: Privacy-Aware Location Sensor Networks, University of Colorado at Boulder, Colorado, 2003.

[20] Hrvatska akademska i istraživačka mreža – CARNet, *Metode za poboljšanje sigurnosti web preglednika*, CCERT-PUBDOC-2009-09-276, CARNet CERT–a i LS&S–a, 2009.

[21] McAfee Labs: *What is a "Drive-By" Download?*, https://blogs.mcafee.com/consumer/drive-by-download/, (pristupljeno kolovoz 2016.

[22] Hrvatska akademska i istraživačka mreža – CARNet, *Napredne tehnike socijalnog inženjeringa*, NCERT-PUBDOC-2010-02-292, CARNet CERT–a i LS&S–a, 2010.

[23] Bilandžić, M., Cvrtila, V., Kralj, R., Javorović, B., Lebeda, N.: Business inteligence i zaštita tajnih i osobnih podataka i informacija, Defimi, Zagreb, 2005.

[24] Lebeda, N.: *Sigurnost i korištenje podataka*, Veleučilište Velika Gorica, 2013.

[25] Republika Hrvatska: Zakon o informacijskoj sigurnosti - NN79/07, Narodne novine, Zagreb, 2007

[26] Laboratorij za sustave i signale: *Informacijska sigurnost u Hrvatskoj*, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, 2010.

[27] Hrvatska akademska i istraživačka mreža – CARNet, *Sigurnosna politika,* CCERT-PUBDOC-2009-05-265, CARNet CERT–a i LS&S–a, 2009.

[28] Cisco Systems: *How Virtual Private Networks Work*, http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html, (pristupljeno kolovoz 2016.)

[29] Wang, Y., Jinpeng Wei, J., Vangury, K.: *Bring Your Own Device Security Issues and Challenges*, IEEE CCNC- Mobile Device, Platform and Communication, 2014.

[30] Eslahi, M., Var Naseri, M., Hashim, H., Tahir, N. M., Hisham, E., Saad, M.: BYOD*: Current State and Security Challenges*, IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2014.

[31] Downer, K., Bhattacharya, M.: BYOD *Security: A New Business Challenge*, IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015 and SC2 2015, 2015.

[32] Scarfò, A.: *New security perspectives around BYOD*, International Conference on Broadband, Wireless Computing, Communication and Applications, Napulj, 2012.

POPIS KRATICA

PDA (Personal Digital Assistant) - Osobni digitalni pomoćnik, dlanovnik

IM (Instant Messaging) - Slanje poruka u realnom vremenu

UI (User Interface) - Korisničko sučelje

VPN (Virtual Private Network) - Virtualna privatna mreža

AAA (Authentication, authorization, and accounting) - Autentikacija, autorizacija i revizija

LDAP (Lightweight Directory Access Protocol) - Aplikacijski protokol za čitanje i pisanje imenika

MCM (Mobile Content Management System) - Sustav za upravljanje mobilnim sadržajem

CMS (Content Management System) - Sustav za upravljanje sadržajem

MDM (Mobile Device Management) - Sustav za upravljanje mobilnim terminalnim uređajem

MAM (Mobile Application Management) - Sustav za upravljanje mobilnim aplikacijama

MIM (Mobile Information Management) – Sustav za upravljanje informacijama na mobilnom uređaju

OS (Operation System) – Operacijski sustav

POPIS SLIKA

Slika 1. Prvi pametni mobilni terminalni uređaj, IBM Simon iz 1993. godine.....4

Slika 2. Sigurnosne informacijske komponente - CIA (eng. *Confidentiality, Integrity, Availability*).....31

Slika 3. Arhitektura sustava za upravljanje mobilnim terminalnim uređajem (eng. *Mobile Device Management* - MDM).....35

POPIS GRAFIKONA

Grafikon 1. Broj korisnika pametnih mobilnih terminalnih uređaja u milijunima od 2014. do 2016. godine i predviđanja do 2019. godine.....7

Grafikon 2. Svrha korištenja BlackBerry i iPhone uređaja kod poslovnih korisnika.....8

Grafikon 3. Svrha korištenja vlastitih terminalnih uređaja (tableta i pametnog mobilnog terminalnog uređaja) u korporativnom okruženju 2012. godine.....10

Grafikon 4. Trendovi prodaje pametnih mobilnih terminalnih uređaja i tablet uređaja u odnosnu na osobna računala.....11

Grafikon 5. Razlozi za uvođenje BYOD-a u poslovanje.....12

Grafikon 6. Korištenje vlastitog terminalnog uređaja na radnom mjestu.....16

Grafikon 7. Vrsta vlastitih terminalnih uređaja korištenih na radnom mjestu.....16

Grafikon 8. Korištenje vlastitog terminalnog uređaja za slanje službenih poruka elektroničke pošte.....17

Grafikon 9. Korištenje vlastitog terminalnog uređaja za preuzimanje poslovnih datoteka i dokumenata.....17

Grafikon 10. Sigurnosna pitanja vezana uz BYOD paradigmu.....18

Grafikon 11. Postotak *ransomware* napada na privatne i poslovne korisnike od 2014. do 2015. godine.....22

Grafikon 12. Postotak *ransomware* napada na privatne i poslovne korisnike od 2015. do 2016. godine.....22

Grafikon 13. Broj korisnika koji su barem jednom bili žrtve *ransomware* napada na mobilnom terminalnom uređaju u razdoblju od travnja 2014. godine do ožujka 2016. godine.....23

Grafikon 14. Učestalost korištenja pametnog telefona (*smartphone*-a).....38

Grafikon 15. Korištenje određenih operacijskih sustava.....38

Grafikon 16. Korištenje određenih proizvođača pametnih mobilnih terminalnih uređaja.....39

Grafikon 17. Učestalost pristupanja mreži vlastitim uređajem u korporativnom okruženju.....39

Grafikon 18. Svjesnost narušavanja sigurnosti podataka tvrtke pristupanjem na mrežu vlastitim terminalnim uređajem.....40

Grafikon 19. Postotak ispitanika upoznatih sa BYOD terminom.....40

Grafikon 20. Postotak tvrtki koje provode BYOD sigurnosnu politiku.....41

Grafikon 21. Provođenje određenih metoda zaštite od zloćudnih softvera u tvrtkama u kojima su ispitanici zaposleni.....42

Grafikon 22. Provođenje određenih metoda zaštite privatnosti korporativnih podataka u tvrtkama u kojima su ispitanici zaposleni.....42

Grafikon 23. Odvajanje privatnih podataka i podataka tvrtke.....43

PRILOG 1. PRIMJER ANKETNOG UPITNIKA

U nastavku se nalazi primjer anketnog upitnika koji je poslan svim ispitanicima istraživanja. Anketna pitanja formulirana su u Google obrascima na sljedećoj poveznici:

https://docs.google.com/forms/d/e/1FAIpQLSezL7VyLVh57Fxttb65CaBt5tHQRhzCc-AVmbXQvG9C9By37w/viewform

Poveznica je ispitanicima poslana putem službene adrese elektroničke pošte, odnosno na *mailing* listu svih zaposlenika (CARNet) i putem društvenih mreža (ostale tvrtke).

Istraživanje se provodilo u razdoblju od 5. srpnja 2016. do 15. kolovoza 2016. godine. Očekivano vrijeme potrebno za ispunjavanje ankete bilo je pet do 10 minuta.

Svi odgovori u ovom istraživanju anonimni su, a rezultati su korišteni isključivo za potrebe izrade ovog diplomskog rada.

ISTRAŽIVANJE SIGURNOSNIH ASPEKATA PRIMJENE VLASTITIH UREĐAJA U KORPORATIVNOM OKRUŽENJU

Ispred Vas se nalazi anketni upitnik „ISTRAŽIVANJE SIGURNOSNIH ASPEKATA PRIMJENE VLASTITIH UREĐAJA U KORPORATIVNOM OKRUŽENJU“. Termin BYOD (eng. Bring Your Own Device) odnosi se na zaposlenike koji donose vlastite računalne uređaje (npr. smartphone, tablete, prijenosna računala) na radno mjesto za korištenje i povezivanje na mrežu tvrtke. Istraživanje se provodi u svrhu izrade diplomskog rada na Fakultetu prometnih znanosti Sveučilišta u Zagrebu. Svi odgovori su anonimni i koristit će se samo u svrhu ovog istraživanja. Očekivano vrijeme potrebno za ispunjavanje ankete je 5-10 minuta. Hvala na sudjelovanju!

1. **1. Kojoj dobnoj skupini pripadate?**
   Označite samo jedan oval.
   - < 18 godina
   - 18 - 25 godina
   - 26 - 35 godina
   - 36 - 45 godina
   - 46 - 55 godina
   - 56 - 65 godina
   - 66 > godina

2. **2. Vaš spol?**
   Označite samo jedan oval.
   - M
   - Ž

3. **3. Koji je Vaš stupanj obrazovanja?**
   Označite samo jedan oval.
   - Nezavršena osnovna škola
   - Osnovna škola
   - NSS (KV radnik, PKV radnik)
   - SSS
   - VŠS
   - VSS
   - Magisterij
   - Doktorat

4. **4. Naziv tvrtke u kojoj radite?**

   _____

5. **5. Naziv odjela u kojem radite?**

.....

6. **6. Pozicija na kojoj radite?**

.....

7. **7. Koliko često koristite pametni telefon (smartphone)?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vro često

8. **8. Koji operacijski sustav (OS) koristite?**
Označite samo jedan oval.

- ◯ Android OS
- ◯ iOS (iPhone OS)
- ◯ Windows Phone
- ◯ BlackBerry OS
- ◯ Symbian OS
- ◯ Ne koristim pametni telefon (smartphone)
- ◯ Ostalo: .....

9. **9. Kojeg proizvođača pametnog mobilnog telefona koristite?**
Označite samo jedan oval.

- ◯ Samsung
- ◯ iPhone (Apple)
- ◯ LG
- ◯ Nokia
- ◯ Sony
- ◯ HTC
- ◯ Huawei
- ◯ Ne koristim pametni telefon (smartphone)
- ◯ Ostalo:

10. **10. Koji model pametnog mobinog telefona koristite?**

.....

11. **11. Koliko često koristite vlastiti terminalni (smartphone, tablet, prijenosno računalo itd.) uređaj na radnom mjestu?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

12. **12. Koji vlastiti terminalni uređaj najčešće koristite na radnom mjestu?**
Označite samo jedan oval.

- ◯ Smartphone
- ◯ Tablet
- ◯ Prijenosno računalo
- ◯ Ne koristim vlastiti terminalni uređaj na radnom mjestu
- ◯ Ostalo:

13. **13. Koliko često pristupate na Wi-Fi mrežu tvrtke vlastitim terminalnim uređajem?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

14. **14. Smatrate li da pristupanjem na Wi-Fi mrežu tvrtke narušavate sigurnost njenih podataka?**
Označite samo jedan oval.

- ◯ Ne, uopće ne smatram da je narušena sigurnost podataka tvrtke
- ◯ Ne smatram da je narušena sigurnost podataka tvrtke
- ◯ Ne znam da li je narušena sigurnost podataka tvrtke
- ◯ Nije mi važno da li je narušena sigurnost podataka tvrtke
- ◯ Smatram da je narušena sigurnost podataka tvrtke, ali ne smatram to važnim
- ◯ Da, smatram da je sigurnost podataka tvrtke uvelike narušena

15. **15. Smatrate li da pristupanjem na Wi-Fi mrežu tvrtke narušavate privatnost vlastitih podataka?**
Označite samo jedan oval.

- ◯ Ne, uopće ne smatram da je narušena privatnost vlastitih podataka
- ◯ Ne smatram da je narušena privatnost vlastitih podataka
- ◯ Ne znam da li je narušena privatnost vlastitih podataka
- ◯ Nije mi važno da li je narušena privatnost vlastitih podataka
- ◯ Smatram da je narušena privatnost vlastitih podataka, ali ne smatram to važnim
- ◯ Da, smatram da je privatnost vlastitih podataka uvelike narušena

16. **16. Koliko često koristite vlastiti terminalni uređaj za slanje službenih e-mailova?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

17. **17. Koliko često koristite vlastiti terminalni uređaj za službenu komunikaciju s ostalim zaposlenicima tvrtke?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

18. **18. Koliko često koristite vlastiti terminalni uređaj za službenu komunikaciju s osobama izvan korporativnog okruženja/klijentima?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

19. **19. Koliko često preuzimate datoteke vezane uz posao na vlastiti terminalni uređaj?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

20. **20. Zaključavate li vlastiti terminalni uređaj?**
Označite samo jedan oval.

	1	2	3	4	5	
Nikada	◯	◯	◯	◯	◯	Vrlo često

21. **21. Na koji način zaključavate vlastiti terminalni uređaj?**
Odaberite sve točne odgovore.

- [ ] PIN-om
- [ ] Lozinkom
- [ ] Uzorkom
- [ ] Konck Code-om
- [ ] Prepoznavanjem lica
- [ ] Otiskom prsta
- [ ] Ne zaključavam vlastiti terminalni uređaj
- [ ] Ostalo: _____

22. **22. Preuzimate li sigurnosna ažuriranja na vlastiti terminalni uređaj?**
Označite samo jedan oval.

- Da, odmah kada su dostupna
- Da, s vremenom
- Ažuriranja se preuzimaju automatski
- Ne, nisam znao/znala da ona postoje
- Ne, ne smatram to važnim
- Ne znam

23. **23. Da li ste ikada izgubili ili Vam je ukraden vlastiti terminalni uređaj?**
Označite samo jedan oval.

- Nikada
- Jednom
- Dva puta
- Tri puta
- Tri i više puta

24. **24. Da li ste ikada izgubili ili Vam je ukraden terminalni uređaj u vlasništvu tvrtke?**
Označite samo jedan oval.

- Nikada
- Jednom
- Dva puta
- Tri puta
- Tri i više puta

25. **25. Što ste poduzeli kada ste izgubili ili kada Vam je ukraden terminalni uređaj?**
Odaberite sve točne odgovore.

- [ ] Nisam ništa poduzeo/la po tom pitanju
- [ ] Zvao/la sam taj broj
- [ ] Tražio/la sam uređaj pomoću neke aplikacije
- [ ] Objavio/la sam oglas da se traži uređaj
- [ ] Vratio/la sam se na mjesta gdje sam se kretao/la da ga pronađem
- [ ] Prijavio/la sam gubitak/nestanak policiji
- [ ] Nikada nisam izgubio/la niti mi je ukraden terminalni uređaj
- [ ] Ostalo: _____

26. **26. Koji model vlasništva terminalnih uređaja koristi tvrtka u kojoj ste zaposleni?**
Označite samo jedan oval.

- Uređaji bez korporativnog upravljanja (uređaji u vlasništvu zaposlenika)
- Djelomično upravljani uređaji (u vlasništvu zaposlenika, djeomično upravljani od strane kompanije)
- Korporativno vlasništvo, osobno omogućeni uređaji (uređaji u vlasništvu tvrtke, zaposlenici ih koriste prema određenim pravilima)
- Potpuno upravljani uređaji (uređaji u potpunom vlasništvu tvrtke, zaposlenici ih koriste prema određenim pravilima)

27. **27. Jeste li upoznati sa terminom BYOD (eng. Bring Your Own Device)**
Označite samo jedan oval.

- Nisam nikada čuo/la za BYOD termin
- Čuo/la sam za BYOD termin, ali nisam upoznat/a s njime
- Malo sam upoznat/a s BYOD terminom
- Dosta sam upoznat/a s BYOD terminom
- U potpunosti sam upoznat/a s BYOD terminom

28. **28. Prema Vašim dosadašnjim saznanjima, što biste rekli da je BYOD?**
Označite samo jedan oval.

- Zaposlenici donose vlastite terminalne uređaje (smartphone, tablete, prijenosna računala) na radno mjesto za pristupanje aplikacijama i podacima tvrtke
- Zaposlenici koriste vlastite terminalne uređaje (smartphone, tablete, prijenosna računala) za pristupanje aplikacijama i podacima tvrtke izvan radnog mjesta (kod kuće)
- Zaposlenici donose vlastita osobna računala na radno mjesto za pristupanje aplikacijama i podacima tvrtke
- Zaposlenici koriste vlastita osobna računala za pristupanje aplikacijama i podacima tvrtke izvan radnog mjesta (kod kuće)
- Ostalo:

29. **29. Ima li tvrtka u kojoj ste zaposleni BYOD sigurnosnu politiku?**
Označite samo jedan oval.

- Da, dobro sam upoznat/upoznata s njome
- Da, ali ne znam mnogo o tome
- Ne znam da li tvrtka ima BYOD sigurnosnu politiku
- Ne znam što je BYOD sigurnosna politika
- Ne, tvrtka nema BYOD sigurnosnu politiku

30. **30. Smatrate li da bi tvrtka u kojoj ste zaposleni trebala imati BYOD sigurnosnu politiku?**
Označite samo jedan oval.

- Da, smatram da je to od ključne važnosti
- Da, smatram da bi to bilo korisno
- Ne znam da li bi tvrtka trebala BYOD sigurnosnu politiku
- Ne, ne smatram da bi to bilo korisno
- Ne, ne smatram to nimalo važnim

31. **31. Koristi li tvrtka u kojoj ste zaposleni određene aplikacije za suzbijanje zlonamjernih programa (malware-a)?**
Označite samo jedan oval.

- Da, smatram da je to od ključne važnosti
- Da, smatram da je to korisno
- Ne znam da li tvrtka koristi određene aplikacije za suzbijanje zlonamjernih programa (malware-a)
- Ne, ne smatram da je to korisno
- Ne, ne smatram to nimalo važnim

32. **32. Koristi li tvrtka u kojoj ste zaposleni određene aplikacije za zaštitu privatnosti podataka?**
Označite samo jedan oval.

- Da, smatram da je to od ključne važnosti
- Da, smatram da je to korisno
- Ne znam da li tvrtka koristi određene aplikacije za zaštitu privatnosti podataka
- Ne, ne smatram da je to korisno
- Ne, ne smatram to nimalo važnim

33. **33. Koliko često koristite uređaj u vlasništvu tvrtke ili u djelomičnom vlasništvu tvrtke za privatu komunikaciju?**
Označite samo jedan oval.

- Nikada
- Rijetko
- Povremeno
- Često
- Vrlo često
- Ne koristim uređaj u vlasništvu tvrtke ili u djelomičnom vlasništvu tvrtke

34. **34. Koliko često koristite uređaj u vlasništvu tvrtke ili u djelomičnom vlasništvu tvrtke za lociranje?**
Označite samo jedan oval.

- Nikada
- Rijetko
- Povremeno
- Često
- Vrlo često
- Ne koristim uređaj u vlasništvu tvrtke ili u djelomičnom vlasništvu tvrtke

35. **35. Koliko često koristite uređaj u vlasništvu tvrtke ili u djelomičnom vlasništvu tvrtke za fotografiranje privatnih fotografija?**
Označite samo jedan oval.

- Nikada
- Rijetko
- Povremeno
- Često
- Vrlo često
- Ne koristim uređaj u vlasništvu tvrtke ili u djelomičnom vlasništvu tvrtke

36. **36. Razumijete li razliku između privatnih podataka i podataka tvrtke?**
Označite samo jedan oval.

- Uopće ne razumijem razliku između privatnih podataka i podataka tvrtke
- Ne razumijem razliku između privatnih podataka i podataka tvrtke
- Djelomično razumijem razliku između privatnih podataka i podataka tvrtke
- Razumijem razliku između privatnih podataka i podataka tvrtke
- U potpunosti razumijem razliku između privatnih podataka i podataka tvrtke

37. **37. Odvajate li privatne podatke i podatke tvrtke?**
Označite samo jedan oval.

- Ne odvajam ih i ne smatram to važnim
- Ne odvajam ih, ali razumijem važnost odvajanja podataka
- Ponekad ih odvajam ali ne smatram to previše važnim
- Ponekad ih odvajam i razumijem važnost odvajanja podataka
- Odvajam ih ali ne smatram to previše važnim
- Odvajam ih i pridajem tome veliku važnost

Omogućuje
Google Forms

METAPODACI

Naslov rada: Istraživanje sigurnosnih aspekata primjene vlastitih terminalnih uređaja u korporativnom okruženju

Studentica: Vlatka Mišić

Mentor: izv. prof. dr. sc. Dragan Peraković

Naslov na drugom jeziku (engleski): The Study of Security Aspects of the BYOD trends in the Corporate Environment

Povjerenstvo za obranu:

- doc. dr. sc. Marko Periša, predsjednik
- izv. prof. dr. sc. Dragan Peraković, mentor
- Siniša Husnjak, mag. ing. traff., član
- izv. prof. dr. sc. Štefica Mrvelj, zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko-komunikacijski promet

Vrsta studija: diplomski

Studij: Promet

Datum obrane diplomskog rada: 27.9.2016.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako 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 diplomskog rada pod naslovom **Istraživanje sigurnosnih aspekata primjene vlastitih uređaja u korporativnom okruženju** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 9/20/2016

(potpis)