Komparativna analiza koncepta BYOD na različitim platformama

Mihovljanec, Goran

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Goran Mihovljanec

KOMPARATIVNA ANALIZA KONCEPTA BYOD NA RAZLIČITIM PLATFORMAMA

ZAVRŠNI RAD

Zagreb, 2020.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

KOMPARATIVNA ANALIZA KONCEPTA BYOD NA RAZLIČITIM PLATFORMAMA
COMPARATIVE ANALYSIS OF THE BYOD CONCEPT ON DIFFERENT PLATFORMS

Mentor: prof. dr. sc. Dragan Peraković

Student: Goran Mihovljanec
JMBAG: 0135249822

Zagreb, rujan 2020.

SAŽETAK

Bring Your Own Device (BYOD) rastući je trend i termin koji se danas sve više koristi, a predstavlja mogućnost korištenja osobnog terminalnog uređaja u poslovne svrhe. Značajnije se upotrebljava od 2009. godine, a 2011. godine doživio je značajan porast broja radnih mjesta na kojima se koristi. BYOD obuhvaća slične termine poput Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP) i Bring Your Own PC (BYOPC). Svi oni razvili su se kako bi takozvanom 'potrošačkom informatikom' osnažili radnu snagu. Kao dio toga BYOD zaposlenike u tvrtki potiče da rade na vlastitom terminalnom uređaju – primjerice, na vlastitom uređaju zaposlenici imaju pristup korporativnoj e-pošti, pregledavaju poslovne dokumente, mogu raditi od kuće, koristiti korporativne aplikacije i sl. BYOD je odlično rješenje za mala i srednja poduzeća jer se povećava produktivnost i smanjuju se troškovi. BYOD ima i negativnu stranu. Ako se regulira i ne razumije u potpunosti, može se ugroziti informatička sigurnost i osjetljivi poslovni sustavi korporacije.

ključne riječi: BYOD, TVRTKA, TERMINALNI UREĐAJ, ZAPOSLENIK, POSLODAVAC, SUSTAV

SUMMARY

Bring Your Own Device (BYOD) is a growing trend and term that is increasingly used today, and refers to being allowed to use a personal terminal device for business purposes.BYOD has been used significantly since 2009, and in 2011 it experienced a significant increase in the number of workplaces where it is used. BYOD includes similar terms like Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP) and Bring Your Own PC (BYOPC). All of them were developed to empower the workforce with so-called ‘consumerisation of IT’. As part of this consumerisation, BYOD encourages company employees to work on their own terminal device - for example, on their own device, employees have access to corporate email, view business documents, can work from home, use corporate applications, and more. BYOD is a great solution for small and medium enterprises because it increases productivity and reduces costs. BYOD also has disadvantages. If regulated and not fully understood, the information security and sensitive business systems of a corporation can very easily be compromised.

keywords: BYOD, BUSINESS, TERMINAL DEVICE, EMPLOYEE, EMPLOYER, SYSTEM

Sadržaj

1. UVOD

Život bez pametnih terminalnih uređaja danas je nezamisliv. Svatko ima minimalno jedan osobni pametni terminalni uređaj. Oni se još uvijek razvijaju i svakim danom pružaju neke nove mogućnosti i aplikacije. BYOD je mogućnost pametnog terminalnog uređaja koja omogućuje korisnicima i poslodavcima korištenje privatnog terminalnog uređaja za posao. BYOD se može koristiti na različitim platformama, a vodeće su iOS i Android platforme. Svaka od njih ima svoje prednosti i neke nedostatke i tvrtke često biraju između te dvije platforme.

Obradom ove teme predstavlja se BYOD koncept i ulazi se u njegovu problematiku te se pobliže predstavlja BYOD koncept kao takav na iOS i Android platformama.

Naslov teme završnog rada je *„Komparativna analiza BYOD koncepta na različitim platformama“,* a cilj rada je dati općeniti prikaz o osnovama BYOD koncepta te detaljnije prikazati BYOD koncept na: Android platformi te iOS platformi. Rad je podijeljen u 7 poglavlja:

1. Uvod
2. Općenito o BYOD konceptu
3. Arhitektura BYOD koncepta
4. Prednosti i nedostaci BYOD koncepta
5. Metode za odvajanje privatnih i poslovnih podataka
6. BYOD koncept na iOS i Android platformama
7. Zaključak

Poglavlje „Općenito o BYOD konceptu“ pobliže opisuje termin BYOD, njegovu povijest i zašto se koristi te kako se koristi u poslovnom okruženju. Treće poglavlje govori o arhitekturi BYOD koncepta, koji uređaji se koriste, mrežna arhitektura, proxy arhitektura. Četvrto poglavlje predstavlja prednosti i nedostatke koje sadrži BYOD. Sljedeće poglavlje opisuje metode za odvajanje privatnih i poslovnih podataka što je vrlo bitno vlasnicima terminalnih uređaja kako bi zaštitili svoju privatnost. U šestom poglavlju opisuje se korištenje BYOD koncepta na platformama iOS i Android te koje su karakteristike tih platforme i koje su im mogućnosti.

2. OPĆENITO O BYOD KONCEPTU

Bring your own device (BYOD) odnosi se na trend zaposlenika određene tvrtke koja preferira korištenje osobnog uređaja za povezivanje sa svojim organizacijskim mrežama i pristup sustavima povezanim sa njihovim poslom i potencijalno osjetljivim ili povjerljivim podacima. [1] BYOD je IT politika koja zaposlenicima omogućava, a ponekad i potiče pristup podacima i sustavima poduzeća pomoću osobnih terminalnih uređaja (pametni telefoni, osobna računala, tableti ili USB pogoni).

BYOD se također izražava i drugim terminima kao npr. **bring your own technology (BYOT), bring your own phone (BYOP),** and **bring your own personal computer (BYOPC).** [1]

Veliki broj organizacija dopušta upotrebu privatnih uređaja, svojih zaposlenika i suradnika, u poslovne svrhe, poput vođenja poslovnih poziva, slanja i primanja poslovne e-pošte i obavljanja drugih poslovnih aktivnosti. [20]

Dva su osnovna konteksta gdje se pojam **BYOD** koristi. Jedan je **u mobilnoj industriji**, gdje se odnosi na operatere koji omogućavaju kupcima da aktiviraju svoj postojeći telefon (ili drugi mobilni uređaj) za spajanje na mrežu, umjesto da budu prisiljeni kupiti novi uređaj od mobilnog operatera.

Drugi, i glavni fokus ovog pojma je korištenje BYOD-a **na radnom mjestu**, gdje se odnosi na politiku dopuštanja zaposlenicima da na posao nose uređaje u osobnom vlasništvu (prijenosna računala, tablete, pametne telefone itd.) i da ih koriste za pristup privilegiranim informacijama o tvrtki i aplikacijama. Taj se fenomen obično naziva **IT consumerization**. [2]

2.1. Povijest BYOD

Izraz **„Bring your own device“** je u početku koristio pružatelj VoIP usluga BroadVoicein 2004.g. s uslugom koja je tvrtkama omogućila da donesu svoj uređaj za otvoreniji model davatelja usluga. [1]

Pojam BYOD tada je ušao u uobičajenu upotrebu 2009. godine zahvaljujući Intelu, kada je prepoznao sve veću sklonost među svojim zaposlenicima da svoje pametne telefone, tablete i prijenosna računala dovode u rad i povezuju s korporativnom mrežom. Međutim, taj termin postao je istaknut početkom 2011. godine, kada su pružatelj IT usluga Unisys i dobavljač softvera Citrix Systems počeli dijeliti svoje viđenje ovog novonastalog trenda. BYOD je okarakteriziran kao značajka "potrošačkog društva" u kojem se poduzeća stapaju s potrošačima. [2] Također 2011. godine BYOD software i službena podrška značajno su se počeli razvijati na radnim mjestima. Rukovoditelji tvrtki počeli su se osjećati ugodno tipkajući po tipkovnicama zaslona osjetljivim na dodir, a tržište mobilnosti poduzeća također se počelo znatnije razvijati.

2012. godine „Američka komisija za jednake mogućnosti pri zapošljavanju“ usvojila je BYOD politiku, ali mnogi su zaposlenici nastavili koristiti BlackBerry-je koje je izdala država zbog zabrinutosti oko naplate i nedostatka alternativnih uređaja. [1]

2.2. Zašto BYOD?

Za današnje zaposlenike sposobnost rada s bilo kojeg uređaja više nije privilegija - to je očekivanje. Donijeti svoj uređaj (BYOD) postalo je uobičajeno za sve industrije, pružajući zaposlenicima slobodu rada s uređaja po njihovom izboru, istovremeno smanjujući troškove i poboljšavajući organizacijsku produktivnost. [6] BYOD politika važna je jer pomaže organizacijama da uspostave ravnotežu između poboljšane produktivnosti i upravljanog rizika. [5]

BYOD koncept **povećava produktivnost i inovativnost**: zaposlenicima je ugodniji osobni uređaj i postaju stručni za njegovo korištenje, što ih čini produktivnijima. Osobni uređaji obično su najmoderniji, tako da poduzeće koristi najnovije značajke. Također korisnici češće kupuju nove osobne uređaje nego same korporacije.

Zadovoljstvo zaposlenika: zaposlenici koriste uređaje koje su odabrali sami i u koje su uložili vlastiti novac - umjesto onoga što je odabrala tvrtka, odnosno njezin IT odjel. Dopuštanje zaposlenicima da koriste osobne uređaje također im pomaže da izbjegnu nošenje više uređaja. [1]

Ušteda troškova: BYOD programi ponekad štede proračun prebacujući troškove na zaposlenike koji plaćaju mobilne uređaje i podatkovne usluge. Međutim, to često rezultira sa malo ili nimalo uštede, stoga odluka se ne temelji prvenstveno na očekivanoj uštedi. [1]

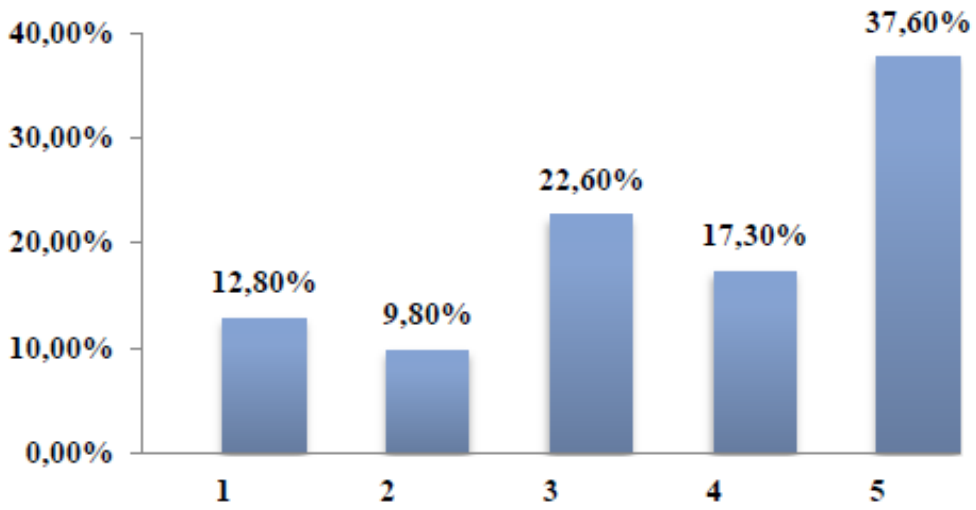
2.3. BYOD u poslovnom okruženju

Provedena je anketa pojma upotrebe terminalnih uređaja u poslovnom okruženju (BYOD) u Republici Hrvatskoj. Osim postotaka korištenja terminalnih uređaja, anketa je također pokazala rezultate o svijest zaposlenika o sigurnosnim problemima koji nastaju kao rezultat korištenja osobnih uređaja na radnom mjestu.

Ciljni korisnici ovog istraživanja bili su isključivo zaposlene osobe. Istraživanje je obuhvatilo 133 ispitanika od čega 67 žena i 66 muškaraca. Ispitanici su uglavnom mlađi, između 18 i 35 godina.

Prema istraživanju koje je provedeno može se zaključiti da zaposlenici u Hrvatskoj često koriste svoje terminalni uređaje na radnom mjestu, ali BYOD trendovi nisu razvijeni kao što su razvijeni u Sjedinjenim Američkim Državama ili nekim drugim zemlje Europske unije. 12,8% ispitanika nikada ne koriste svoje osobne terminalne uređaje na radnom mjestu, 9,8% od njih rijetko koriste svoje osobne terminalne uređaje, 22,6% koriste ih povremeno, a često ih koristi 17,3%.

Čak 37,6% ispitanika koriste svoj osobni terminalni uređaj na radnom mjestu vrlo često. Ti su rezultati prikazani na slici 1. [21]



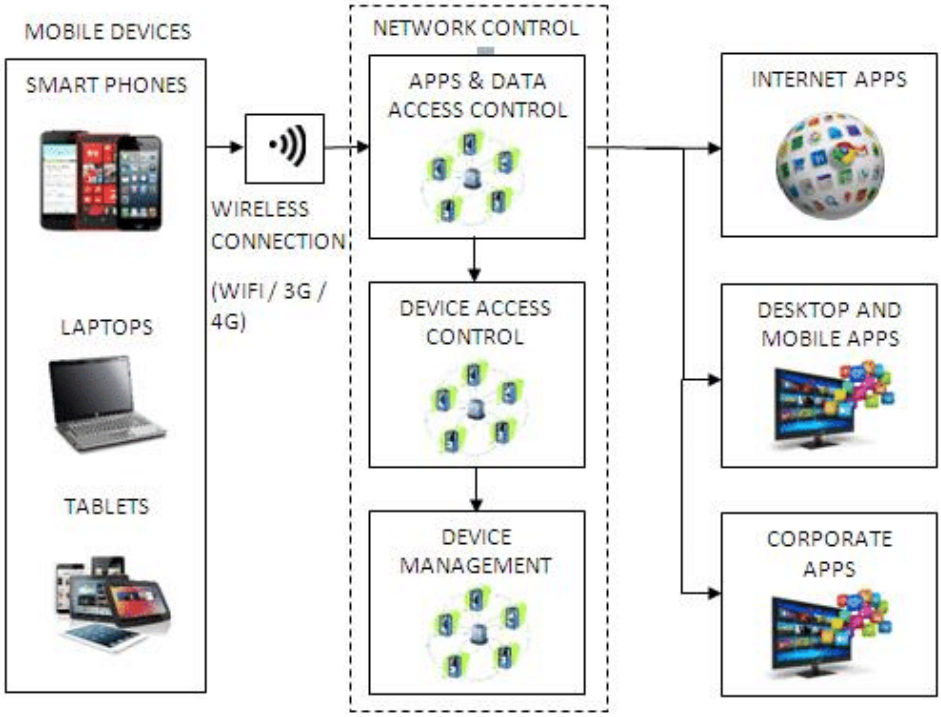
Slika 1. Korištenje terminalnih uređaja na radnom mjestu[21]

3. ARHITEKTURA BYOD KONCEPTA

Korisnici sve više žele pristupiti korporativnim aplikacijama, podacima i uslugama sa svojih mobilnih telefona i tableta. Ovi uređaji najčešće pokreću platformu Apple iOS ili Google Android. BYOD uređaji obično su povezani s javnim Internetom (npr. putem kućnog WiFi-a ili podatkovnim paketom mobilnog operatera), a manje često s poslovnom mrežom. To znači da se trebaju poduzeti posebni koraci kako bi se osiguralo povezivanje uređaja za pristup aplikacijama instaliranim na privatnoj korporativnoj mreži. Osnovni problem u davanja pristupa uređajima privatnim korporativnim sustavima i aplikacijama je kako osigurati sigurnu povezanost. [4]

BYOD uređaji, baš kao i javna mreža na koju je uređaj spojen su jednako nepouzdani. To predstavlja veliki problem za sigurnost same korporacije jer uvijek postoji netko tko želi pristupi neovlaštenom sadržaju. Korporacijama koje imaju važne podatke i informacije u svojem sustavu povećava se rizik od neovlaštenog upada u isti. Zbog toga većina organizacija upravlja sigurnom, privatnom mrežom s vatrozidima koji štite sve točke povezivanja između ove mreže i javnog Interneta. Često postoje posredne mreže između privatne, korporativne mreže i nepouzdanog, javnog Interneta gdje su instalirani web poslužitelji, poslužitelji pošte i drugi sustavi koji moraju biti javno dostupni.

Osnovna arhitektura BYOD koncepta prikazana na slici 2. je vrlo jednostavna. Uređaji su spojeni na neku od mreža (Wi-FI, mobilna mreža, LAN kabel). Spajanje na mrežu dopušta im pristup internetskim aplikacijama, mobilnim i računalnim aplikacijama i aplikacijama koje su pod „pečatom“ njihove korporacije.



Slika 2. Osnovna arhitektura BYOD koncepta, [5]

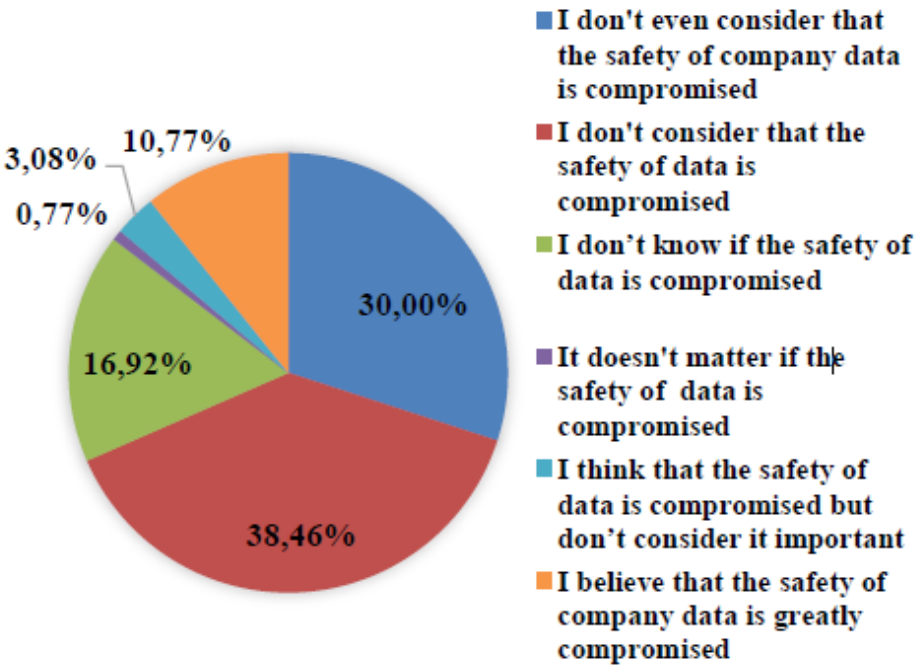
3.1. Sigurnost organizacije

Uvođenje BYOD modela u organizacijsku strukturu dovelo je do redefiniranja načina na koji korisnici izvršavaju svoje svakodnevne zadatke, ali je također dalo jasan uvid u način na koji organizacija upravlja svojom računalnom mrežom, mobilnim terminalnim uređajima i ljudskim resursima. [20]

Sigurnost svake organizacije je bitno za njihovo poslovanje i očuvanje podataka i privatnosti. Rezultati istraživanja o svijesti korisnika o sigurnosnim problemima povezivanja osobnog terminalnog uređaja s poslovnom mrežom (slika 3.) pomalo su uznemiravajući.

Istraživanje je pokazalo da 30,00% ispitanika čak i ne smatra (s većim uvjerenjem) da je sigurnost podataka tvrtke ugrožena, dok 38,46% ne smatra (s manje uvjerenja) da je sigurnost podataka ugrožena. 68,46% ispitanika nije svjesno sigurnosnih problema korištenja svojih osobnih terminalnih uređaja u korporacijskom okruženju. 16,92% ispitanika ne zna je li sigurnost podataka ugrožena, a 0,77%

navodi da nije važno je li sigurnost podataka ugrožena. Da je sigurnost podataka ugrožena smatra tek 3,08%, ali to ne smatraju važnim, dok samo 10,77% ispitanika vjeruje da je sigurnost podataka tvrtke jako ugrožena.

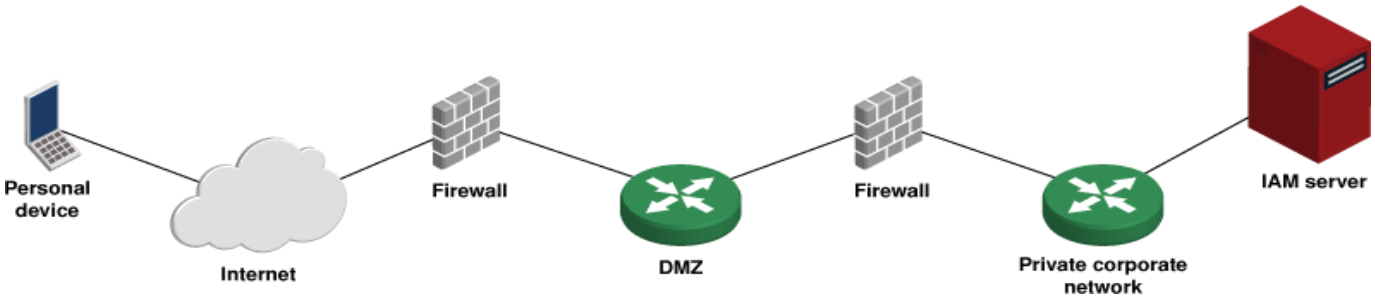


Slika 3. Svijest o ugrožavanju sigurnosti podataka tvrtke [21]

3.2. Sigurnosni ciljevi

Kao i svaki segment informacijskih i komunikacijskih struktura, mobilni terminalni uređaji također moraju podržavati tri glavna cilja sigurnosti, povjerljivosti, dostupnosti i integriteta. Ti se ciljevi mogu postići kombiniranom primjenom sigurnosnih mehanizama, ugrađenih u mobilne uređaje, kao i provedbom dodatnih sigurnosnih kontrola na različitim razinama informacijskih i komunikacijskih struktura.[24]

Sigurnosno osjetljivi sustavi i aplikacije, poput sustava identiteta i pristupa (IAM), najčešće su raspoređeni na privatnoj korporativnoj mreži. Ovo postavljanje namjerno otežava pristup IAM sustavima s javnog Interneta.[6] Odnos između BYOD-a, IAM sustava, privatne mreže, javnog Interneta (DMZ) prikazan je na slici 4.



Slika 4. Odnos BYOD-a, privatne mreže, javnog Interneta i IAM sustava, [6]

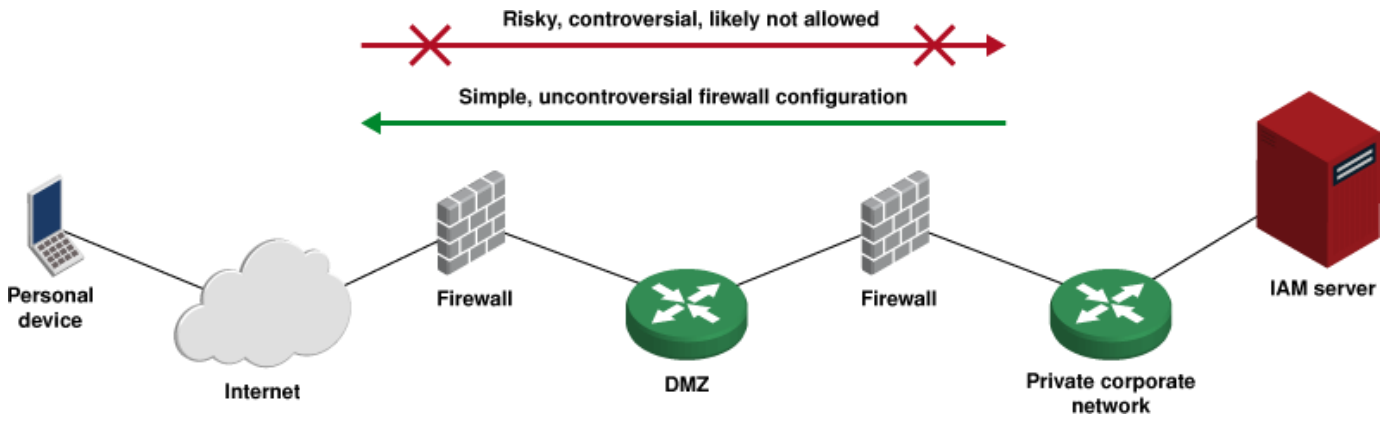
Kako bi se ponudilo adekvatno rješenje koje će omogućiti BYOD uređaju pristup lokalnoj aplikaciji, moraju se osigurati sljedeće sigurnosne karakteristike:

1. Prema zadanim postavkama potrebno je blokirati pristup bilo kojoj javnoj IP adresi te bilo kojem lokalnom sustavu - samo ovlašteni uređaji trebaju imati mogućnost povezivanja s IAM sustavom.
2. Preporučeno je blokirati i ovlaštene uređaje da pristupe bilo čemu u korporacijskoj mreži, osim IAM sustava.
3. Sustave i aplikacije na privatnoj, korporativnoj mreži potrebno je zaštititi od (mogućih) napada uskraćivanja usluge.
4. Korisničke ID-ove nije poželjno objavljivati na javnom Internetu.
5. Ovlaštene uređaje potrebno je povezati s poznatim korisničkim identitetima. Korisnicima se dopušta pristup IAM sustavu samo s vlastitog uređaja, nikako sa uređaja koji nije u njegovom vlasništvu.
6. Uređaje za pristup potrebno je aktivirati s mogućnošću deaktiviranja tih uređaja ako ih korisnik izgubi, ako uređaj ukradu ili ako dotični korisnik ode iz korporacije.[6]

3.3. Mrežna arhitektura i vatrozid

Na slici 3. jasno je da, bez prolaska veze kroz vatrozid mreže, ne postoji način da se korisnički uređaj poveže s lokalnim IAM sustavom.

Administratori vatrozida opravdano ne žele dopustiti bilo kakve uzlazne veze koje potječu s javnog Interneta i završavaju na mrežnim adresama na privatnoj mreži. S druge strane, mnogi sustavi u privatnoj mreži zahtijevaju mogućnost povezivanja s javnim internetskim adresama. Drugim riječima, smjer veze je važan - odlazne veze s korporativne mreže su rutina, dok su dolazne veze rizične, složene i nepoželjne.[6] To je također ilustrirano na slici 5.



Slika 5. Veza između BYOD uređaja i IAM sustava, [6]

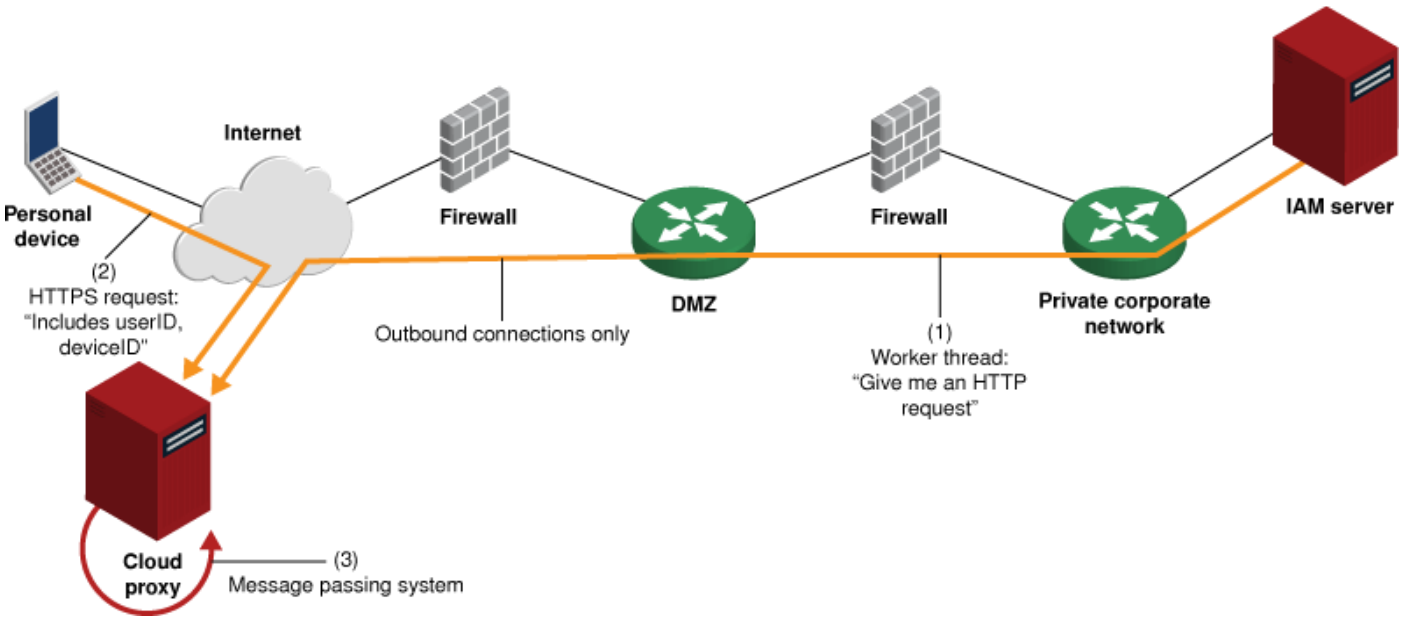
3.4. Proxy arhitektura

Kako bi udovoljio potrebnim zahtjevima (npr. HTTPS zahtjev), a da se pritom ne krše propisana ograničenja preko vatrozida, uvedena je proxy arhitektura, kao što je prikazano na slici 6.[7]

U ovoj su arhitekturi zapravo dva zasebna proxyja:

- Na svakom lokalnom poslužitelju nalazi se proxy usluga koja kontinuirano stvara radničke niti i šalje zahtjeve drugom proxyju temeljenom u oblaku (Cloud Proxy) tražeći posao.

- Postoji novi proxy u oblaku, instaliran na javno dostupnom VM-u na Internetu, koji implementira arhitekturu za prosljeđivanje poruka. Prihvaća zahtjeve BYOD uređaja i - ako potječu s valjanog, aktiviranog uređaja, prosljeđuje te zahtjeve nekoj od radnih niti da ih dovrši. Zatim čeka odgovor i prosljeđuje odgovor natrag na BYOD uređaj.[7]



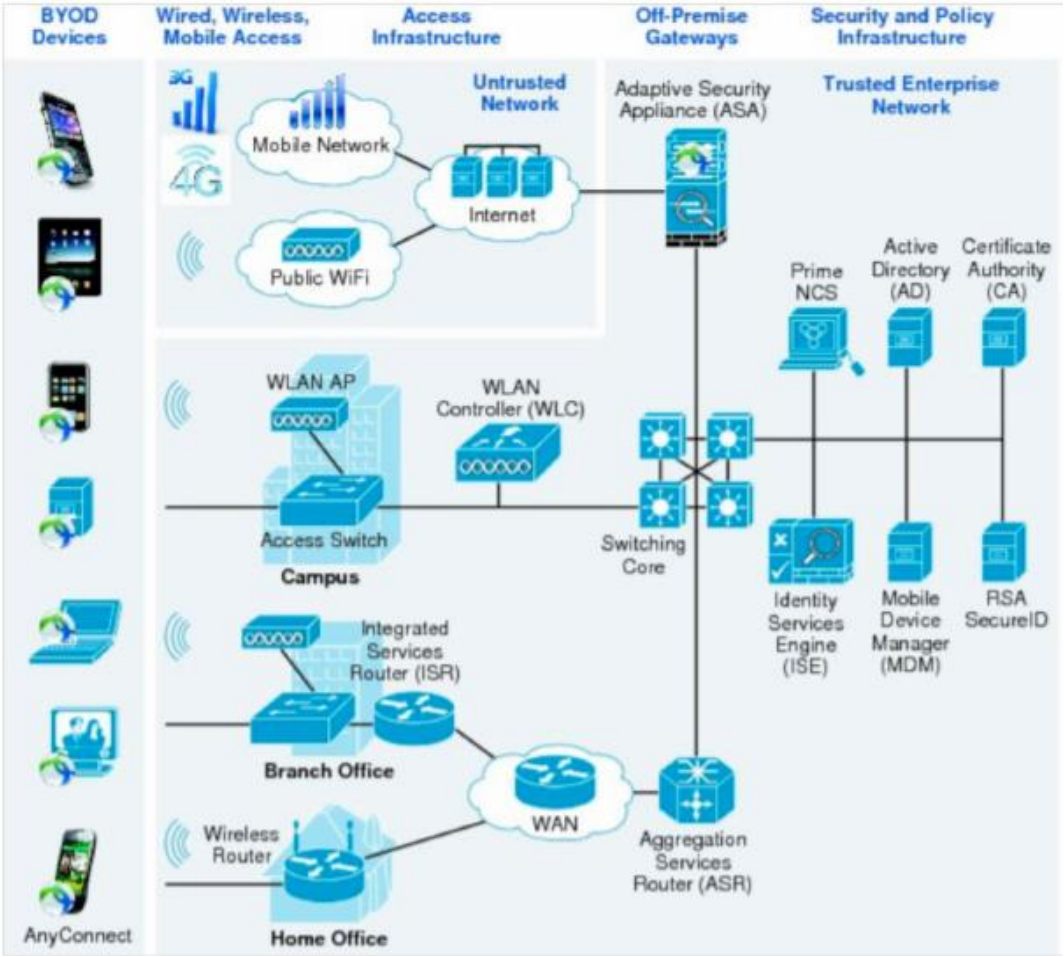
Slika 6. Proxy arhitektura, [7]

3.5. Rješenje BYOD na visokoj razini

BYOD KONCEPT mora osigurati žičani, bežični ili mobilni pristup mreži. Mora biti podržan na različitim vrstama uređaja i mora biti sposoban za provođenje različitih zadataka sa strane korisnika i uređaja. Uz to, kako se uređaji premještaju iz jedne mreže u drugu, na primjer iz školske WiFi mreže u javnu 3G/4G mobilnu mrežu, BYOD rješenje mora biti u mogućnosti pružati siguran pristup, a istovremeno očuvati korisničko iskustvo bez problema.[8]

Za bilo koju BYOD strategiju potrebno je razmotriti sveobuhvatan pristup javnoj mreži, a bilo koji dizajn koji ne podržava širok raspon pristupa mreži neće uspjeti pružiti traženo i potrebno upravljačko rješenje za IT.

Tvrtke koje se bave BYOD konceptom, implementiraju ga i razvijaju imaju svoja vlastita rješenja. Primjerice, tvrtka Cisco razvila je svoj vlastiti koncept koji je prikazan na slici 7. Komponente koje su koristili za usavršavanje navedene arhitekture su: Cisco Catalyst Switches, Cisco Integrated Services Routers, Cisco Wireless LAN Access Points, Cisco Wireless LAN Controller, Cisco Adaptive Security Appliance, Cisco AnyConnect Client, Cisco Identity Services Engine, Cisco Prime, Third-Party Solution Components, RSA SecurID, Mobile Device Manager, Certificate Authority, Microsoft Active Directory, Supported Devices.



Slika 7. Arhitektura visoke razine (Cisco), [8]

3.5.1. Catalyst Switches

Omogućuju žičani pristup mreži i obrađuju zahtjeve za provjeru autentičnosti za pristup mreži s 802.1x. U odjeljku Omogućuju PoE za uređaje kojima je potrebna snaga, uključujući VDI radne stanice, IP telefone i WLAN pristupne točke (AP).[8]

3.5.2. Usmjerivači integriranih usluga (ISR)

Usmjerivači integriranih usluga (ISR) nude ožičeni WAN i osim toga, ISR-ovi mogu pružiti izravnu povezanost s Internetom i uslugama u oblaku, uslugama optimizacije aplikacija i WAN-a, a mogu poslužiti i kao završne točke za VPN veze

putem mobilnih uređaja. Pomoću funkcije Secure Device Provisioning (SDP) u ISR-u također se može koristiti kao tijelo za izdavanje certifikata (CA), što je korisno za relativno manje implementacije.[8]

3.5.3. Pristupne točke bežičnog LAN-a (AP)

Bežična pristupna točka (bežična pristupna točka) mrežni je uređaj koji prenosi i prima podatke putem bežične lokalne mreže (WLAN). Bežična pristupna točka služi kao točka povezivanja između WLAN-a i fiksne žičane mreže. Kada se bežični uređaj pomakne izvan dosega jedne AP, on se predaje sljedećoj AP.[32]

3.5.4. LAN kontroler (bežični)

Glavna funkcija tradicionalnog bežičnog LAN kontrolora (WLC) je konfiguriranje bežičnih pristupnih točaka (AP) koje se na njega povezuju lokalno. [33]

3.5.5. Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) pruža tradicionalne sigurnosne funkcije na rubnim dijelovima mreže, uključujući vatrozid i sustav za sprječavanje neovlaštenog upada (IPS), kao i kritičnu sigurnosnu točku VPN (npr. Cisco AnyConnect) za mobilne uređaje koji se spajaju putem Interneta, uključujući javne WiFi žarišne točke i 3G / 4G mobilne mreže. [8]

3.5.6. Virtualna privatna mreža (VPN)

Virtualna privatna mreža (VPN) pruža vam internetsku privatnost i anonimnost stvaranjem privatne mreže od javne internetske veze. VPN-ovi maskiraju vašu adresu internetskog protokola (IP), tako da vaše mrežne radnje gotovo nije moguće pratiti. Najvažnije je da VPN usluge uspostavljaju sigurne i šifrirane veze kako bi pružile veću privatnost nego čak i zaštićena Wi-Fi žarišna točka.[31]

3.5.7. Identity Services Engine (ISE)

Identity Services Engine (ISE) temeljna je komponenta rješenja BYOD arhitekture tvrtke Cisco i pruža niz usluga, uključujući:

- Autorizacija
- Autentifikacija
- Upis certifikata
- Provođenje politike
- Sučelje za pohranu identiteta (npr. RSA) [8]

3.5.8. RSA SecurID

RSA SecurID token i Authentication Server koriste se za pružanje dvofaktorske (tajni PIN i jednokratni kod lozinke) autentifikacije zbog jake sigurnosti prilikom povezivanja putem VPN-a. [8]

3.5.9. Mobile Device Managment (MDM)

Upravitelj mobilnih uređaja (MDM) pruža centralizirano upravljanje krajnjim točkama za više operativnih sustava BYOD uređaja. Funkcionalnost i podrška variraju kod različitih dobavljača MDM-a. Međutim, tipična funkcionalnost uključuje konfiguraciju uređaja, enkripciju na uređaju, provedbu lozinke i pružanje samoposluživanja.

Uz gore navedene funkcije usmjerene na pristup mreži, MDM može poslužiti i kao važna sigurnosna usluga na krajnjem uređaju koja pruža usluge provjere autentičnosti aplikacija. [8]

3.5.10. Tijelo za izdavanje certifikata (CA)

Tijelo za izdavanje certifikata (CA), koje se ponekad naziva i tijelom za ovjeravanje, je tvrtka ili organizacija koja djeluje kako bi provjerila identitet entiteta (poput web stranica, adresa e-pošte, tvrtki ili pojedinačnih osoba) i povezala ih s kriptografskim ključevima putem izdavanje elektroničkih dokumenata poznatih kao digitalni certifikati.[34]

4. PREDNOSTI I NEDOSTACI BYOD KONCEPTA

Želi li se u neku organizaciju uvesti BYOD politika potrebno je znati koje su joj prednosti a koji nedostaci. Potrebno je upoznati se sa konceptom BYOD- a te kako on funkcionira i koje su mu mogućnosti kako bi se mogla ugovoriti pravila organizacije i njihovih zaposlenika. Primjena BYOD modela pruža konkretne koristi zaposlenicima, ali i organizaciji, poput povećanog zadovoljstva zaposlenika, povećane produktivnosti i financijske uštede [22].

4.1. Prednosti BYOD koncepta

Prednosti BYOD-a:

- **Zadržavanje zaposlenika zadovoljnima**: zadržavanje jakih terenskih tehničara izuzetno je važno, ali i teško. Kad tehničari koriste uređaje koje već poznaju i vole, bit će sretniji radeći za vašu tvrtku, a ujedno i produktivniji. Studije su pokazale da zaposlenici uživaju u korištenju svojih osobnih uređaja više nego u korištenju uređaja izdanih od strane IT odjela, unatoč tome što su sami odgovorni za svoje troškove. [9]

- **Smanjenje tehnoloških troškova-** tehnologija na radnom mjestu povezana je s porastom troškova, ali BYOD zapravo pomaže uštedjeti novac na hardveru i podršci. Omogućavanje zaposlenicima da koriste vlastite uređaje smanjuje troškove kupnje i zamjene tehnologije za osoblje na prvom mjestu.[35]

- **Poboljšavanje rada korisnika**: prosječni korisnik BYOD-a uštedi 58 minuta dnevno koristeći svoje osobne uređaje na poslu, što im daje više vremena za učenje, rast i izvršavanje velikog korisničkog iskustva. Pristup informacijama o proizvodima i promocijama u stvarnom vremenu, kao i digitalni rasporedi i programi obuke, pomažu suradnicima u prvoj liniji da budu produktivniji, angažiraniji i posvećeniji zadovoljstvu kupaca.[35]

- **Povećanje fleksibilnosti-** BYOD je dio fleksibilnosti na radnom mjestu, što posebno milenijalci cijene kao jednog od ključnih čimbenika koji dovodi do zadovoljstva poslom. Fleksibilnost radnog mjesta općenito povećava vjernosti, moral i angažman zaposlenika. Osoblje kojem je dozvoljeno da odluči o alatima koje koriste i odabere gdje će ih koristiti, ima veću ravnotežu između poslovnog i privatnog života i kao rezultat toga, ne samo da će biti produktivnije nego i manje vjerojatno da će trebati bolesne dane ili napustiti tvrtku.[36]

- **Prednost novijih uređaja** i Cutting Edge značajki: pojedinačni korisnici obično preferiraju najnovije uređaje koji su brži, elegantniji i sposobniji. Noviji uređaji sa značajkama kao što su Siri i 4G LTE koriste se za terenske radne zadatke te nadogradnju brzine, pohrane, fotografije, video zapisa, naplate i još mnogo toga[9]

- **Pružanje jednostavnijeg pristupa informacijama:** brzo vrijeme obrade znači sretne kupce i veći prihod. Tehničari terenske službe trebaju informacije dostupne u bilo koje vrijeme i na mjestu kako bi dobro obavljali svoj posao. Stari uređaji polako dolaze do podataka, što dovodi do sporijeg vremena obrade. Implementacijom ažuriranih fleksibilnih platformi sa podacima pruža zaposlenicima pristup podacima na zahtjev, što povećava produktivnost. [9]

4.2. Nedostaci BYOD koncepta

- **Pitanja vezana uz sigurnost**: sigurnost je bila jedna od najvećih briga oko donošenja vlastitih pravila o uređajima. IT stručnjaci teže nadziru i rješavaju viruse, hakiranje i druge probleme s kibernetskom sigurnošću s osobnim uređajima. Međutim, neki zaposlenici možda ne odobravaju da njihovi šefovi imaju pristup njihovim osobnim podacima. Zaposlenici također mogu smatrati nezgodnim kad ne mogu preuzeti podatke o tvrtki na osobne uređaje. [9]

- **Nema jedinstvene podrške krajnjem korisniku**: važno je potražiti mogućnosti podrške za svaku od glavnih platformi. Na taj način može se pomoći zaposleniku ako se i kada se pojave problemi.
- **Lokalne poteškoće sa softverom**: ako tvrtka kupi program bez ugovora o podršci, uz ostale skupe troškove možda će morati angažirati informatičku obuku za internu podršku softvera. Jednostavno rješenje je kupnja softvera kao usluge (SaaS) tako da davatelj usluge automatski brine o podršci
- **Pravni troškovi** [9]
- Zaposlenici možda na svojim uređajima nemaju instaliran učinkovit antivirusni softver, vatrozid ili drugi specijalizirani sigurnosni softver.
- Uređaji koje zaposlenici koriste osjetljivi su na krađu, gubitak ili oštećenje.
- Zaposlenici često rade na Wi-Fi lokacijama koje nisu sigurne i podložne su napadima drugih. [10]
- Zaposlenici možda iz sigurnosnih razloga neće dopustiti tvrtki pristup njihovom osobnom uređaju, jer brisanjem osobnog uređaja zaposlenika mogu se izbrisati svi podaci na uređaju, kako poslovni tako i osobni.
- Neki zaposlenici možda koriste određene softverske sustave koji nisu kompatibilni.[10]
- Zaposlenik koristi svoj uređaj iz osobnih razloga dok je u tvrtki, smanjujući produktivnost.
- Zaposlenici mogu fotografirati ili snimati informacije koje mogu biti vlasništvo tvrtke, bez obzira je li uređaj povezan s mrežom tvrtke.

Također zbog velike pokretljivosti, male veličine i mogućnosti povezivanja putem nekoliko dostupnih tehnologija, mobilni terminalni uređaji ranjiviji su na sigurnosne prijetnje, navedene u nastavku. Osim njih ranjivi su i ostali klijentski terminalni uređaji (poput računala i prijenosnih računala), [23] [24] :

- krađa ili gubitak mobilnog terminalnog uređaja,
- napadi na uređaje namijenjene recikliranju,
- napadi kroz zlonamjerni sadržaj (virusi, crvi, špijunski softver, adware i trojanski konji)
- praćenje podataka implementiranih napadima na senzore (GPS, akcelerometar, mikrofon, kamera)

- napadi krađe identiteta,
- iskorištavanje ranjivosti u web preglednicima,
- automatsko preuzimanje aplikacija,
- napadi putem lažnih mrežnih podataka,
- iskorištavanje mrežnih previda,
- socijalni inženjering.[20]

5. METODE ZA ODVAJANJE PRIVATNIH I POSLOVNIH PODATAKA

Problem za organizaciju, ali i za korisnike u BYOD modelu, predstavlja obrada, upotreba i pohrana privatnih i poslovnih podataka unutar istog uređaja bez ikakvih sigurnosnih ograničenja među njima. To znači da neovlašteni pristup korisničkom uređaju znači i pristup svim podacima koje korisnik posjeduje na uređaju, privatnim i poslovnim.

Problem za korisnike predstavlja, na primjer, upravljanje i konfiguracija uređaja od strane organizacije jer organizacija tada ima uvid u podatke, ne samo u poslovne, već i u privatne podatke zaposlenika ili vlasnika uređaja. Stoga je dobra strategija odvajanja podataka presudna za sigurnost podataka, ali i za očuvanje privatnosti korisnika unutar BYOD okruženja.

U svrhu razdvajanja privatnih i poslovnih podataka unutar uređaja razvijene su određene metode. Te su metode pokrivene jednim pojmom, sustav za upravljanje mobilnim sadržajem (eng. Mobile Content Managment- MCM). Sustav upravljanja mobilnim sadržajem gotovo je uvijek dio većeg organizacijskog sustava upravljanja mobilnošću (eng. Enterprise Mobility Management- EMM). Ovaj sustav, zajedno s MCM-om, kombinira nekoliko metoda koje pokrivaju aspekte upravljanja i sigurnosti organizacija, mobilnih uređaja, podataka i aplikacija, kao što je [26]:

- Mobile Email Management (MEM),
- Mobile Device Management (MDM),
- Mobile Application Management (MAM),
- Mobile Information Management (MIM).

Iako sve metode razdvajanja privatnih i poslovnih podataka imaju isti cilj, da štite aplikacije i podatke organizacije, pristupi definiranom problemu znatno se razlikuju. Postoji nekoliko pristupa:[25]

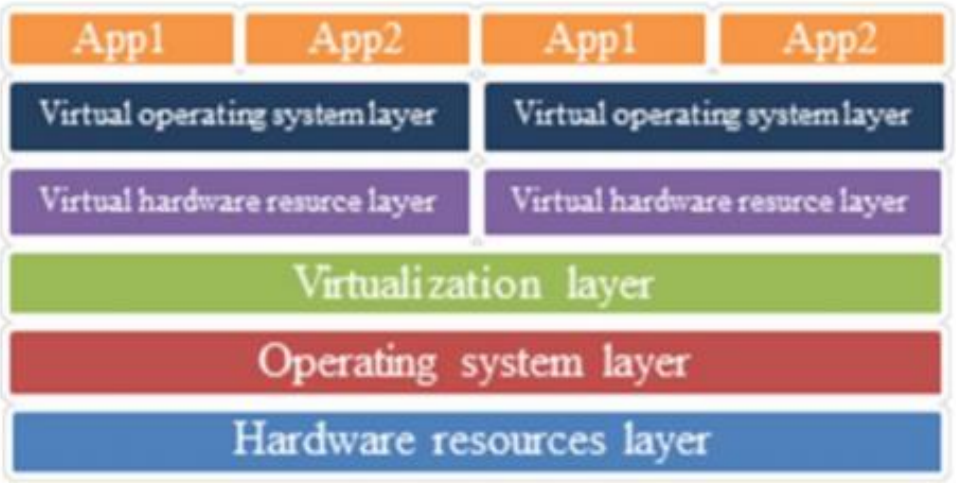
- **Virtualizacija**
  - Mobilna virtualna desktop infrastruktura (mobile VDI),
  - Virtualizacija mobilnog operativnog sustava (mobilna OS virtualizacija).

- **Kontejnerizacija**
  - Application specific containers
  - Application neutral containers
  - Integrated containers

5.1. Virtualizacija

Virtualizacija je metoda emulacije softverskog i / ili hardverskog okruženja koja se izvodi iznad drugog softvera. Ovo simulirano okruženje naziva se virtualni stroj [27].

Virtualni stroj logično je ekvivalentan fizičkom stroju, a razlog široke primjene virtualizacije je mogućnost pokretanja više virtualnih strojeva na jednom fizičkom stroju. Slika 8. prikazuje generalizirani prikaz principa rada virtualnih strojeva. Sloj virtualizacije omogućuje istovremeno izvršavanje više različitih operativnih sustava na jednom računalu, dinamički dijeleći dostupne hardverske resurse (CPU, RAM, HDD, I / O uređaji) [20].



Slika 8. Općenit prikaz rada virtualne mašine[20]

5.1.1. Mobilni pristup virtualnoj radnoj površini

Mobilni VDI odnosi se na infrastrukturu koja omogućuje pristup virtualnoj radnoj površini putem različitih mobilnih uređaja. Općenito, podržava dvije osnovne arhitekture klijenta [28]:

- VDI baziran na klijentu - VDI klijentska aplikacija instalirana je na mobilnom terminalnom uređaju i koristi se za stvaranje sesije između uređaja i računalne infrastrukture unutar organizacije. Stvorena sesija omogućuje mobilnom terminalnom uređaju pristup aplikacijama i podacima organizacije putem virtualiziranih sučelja.
- VDI na temelju web pregledniku - ova alternativna arhitektura koristi web preglednik s podrškom za HTML 5 za pristup web-baziranom VDI klijentu. Korištenje ove arhitekture eliminira potrebu za instalacijom pojedinih klijentskih aplikacija na uređaj.

Nedostatak mobilnog pristupa virtualnoj radnoj površini leži u činjenici da danas mobilni terminalni uređaj nema fizičke ulazne jedinice (miš i tipkovnica), već se oslanja na primjenu virtualnih alternativa.

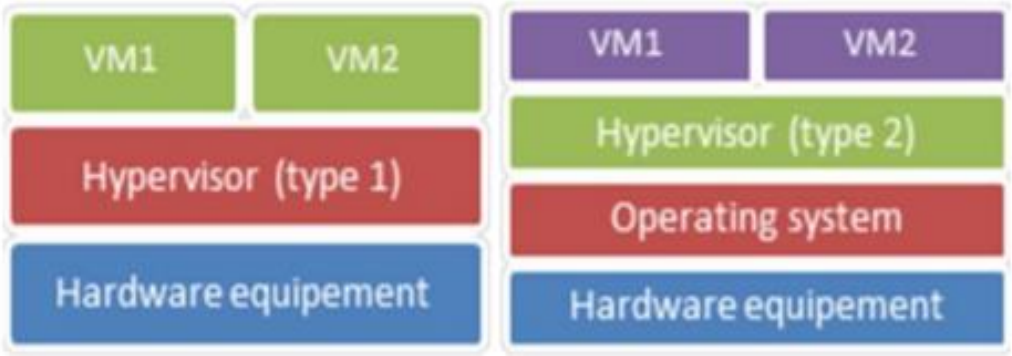
Bez klasičnih ulaznih jedinica teško je, a ponekad je i nemoguće koristiti određene aplikacije putem rješenja koja se temelje na mobilnom VDI pristupu. Također, zbog malih dimenzija uređaja, korisnici ne mogu uvijek vidjeti cijelu virtualnu radnu površinu; na primjer, padajući izbornici određenih aplikacija neće biti vidljivi. Stoga je potrebno testirati aplikacije prije nego što postanu dostupne korisnicima [20].

5.1.2. Virtualizacija mobilnog operativnog sustava

Zbog ograničenih hardverskih mogućnosti mobilnih terminalnih uređaja, implementacija rješenja za virtualizaciju mobilnih operativnih sustava najteža je održiva metoda razdvajanja privatnih i poslovnih podataka. Postoje dvije vrste hipervizora za virtualizaciju:

- **Tip 1** je hardverski zasnovan i implementiran u uređaj koji stvara novu inačicu postojećeg operativnog sustava. Obje inačice operativnog sustava rade na dvije odvojene procesorske regije
- Tip 2 nalazi se na vrhu operacijskog sustava za koji ga nije potrebno implementirati tijekom proizvodnog procesa, ali ga je moguće instalirati kasnije. Smatra se manje sigurnim od Tipa 1 zbog mogućnosti ugrožavanja operativnog sustava i stvaranja puta za postizanje napada na virtualni stroj.

Razlika između gore spomenute arhitekture hipervizora prikazana je na slici 9.



Slika 9. Razlika arhitektura hipervizora Tipa 1 i Tipa 2 [20]

Problemi upotrebljivosti mogu se povezati s izvedbom dvaju primjeraka operativnog sustava koji se istodobno izvršavaju na jednom uređaju. Također, ova metoda zahtijeva prelazak s privatnog na poslovni način, što za korisnika može biti nepraktično.[29]

5.2. Kontenjerizacija

Kontejnerizacija pruža administratorima mogućnost stvaranja sigurnih spremnika na uređaju unutar kojih se nalaze sve aplikacije i podaci organizacije. Tijekom primjene ove metode podaci se mogu dijeliti isključivo između aplikacija koje se nalaze u sigurnom spremniku.

Ova metoda omogućuje provedbu sigurnosne politike organizacije nad unaprijed određenim sigurnim spremnicima, bez utjecaja na funkcionalnost i podatke privatnog dijela uređaja.[20]

Kontejnerizacija omogućuje provedbu različitih sigurnosnih mehanizama, poput [30]:

- Guranje ažuriranja sadržaja izravno u sigurni spremnik,
- Ograničenje pristupa na temelju vremena i mjesta mobilnog uređaja,
- Šifriranje sadržaja pohranjenog u sigurnom spremniku pomoću 256-bitne SSL enkripcije,
- Uklanjanje pohranjenog sadržaja odmah nakon napuštanja aplikacije.

5.2.1. Kontejneri specifični za aplikaciju (Application specific containers)

Kontejneri specifični za aplikaciju zahtijevaju poseban razvoj aplikacije zbog potrebe prilagodbe sučelja za programiranje aplikacija (API) radi zaštite podataka. Poznati su i pod nazivom SDK (Software Development Kit).

Zbog potrebe prilagodbe aplikacija izvornog koda, ova vrsta standardiziranih kontejnera uzrokuje promjene u izgledu korisničkog sučelja, što često dovodi do nezadovoljstva kupaca. [20]

5.2.2. Neutralni aplikacijski kontejneri (Application neutral containers)

Aplikacijski neutralni kontejneri koristili su postupak koji se naziva omatanje aplikacija za pružanje sigurnosnih mehanizama koji nisu dio izvornog koda aplikacije. Na njih je moguće utjecati daljinski, putem aplikacija za upravljanje. Omotavanje aplikacija može se implementirati u vrlo kratkom vremenskom razdoblju, jer aplikacijski neutralni spremnici ne zahtijevaju promjene izvornog programskog koda.

Ovaj pristup razdvajanja podataka, u smislu iskoristivosti, pruža korisnicima izvorni raspored i dosljednost aplikacija u načinima korištenja privatnog i poslovnog prostora. [20]

5.2.3. Integrirani kontejneri (Integrated containers)

Zbog duboke integracije u operativni sustav, pristup zasnovan na integriranom kontejneru pruža visoku razinu sigurnosti, značajno smanjujući ranjivosti povezane s performansama sigurnih kontejnera koji nisu integrirani u operativni sustav.

Centralizirani pristup pri dizajniranju integriranog spremnika omogućuje optimizaciju sigurnosti i poslovne produktivnosti iskorištavanjem mogućnosti grupiranja alata i aplikacija namijenjenih u tu svrhu [20].

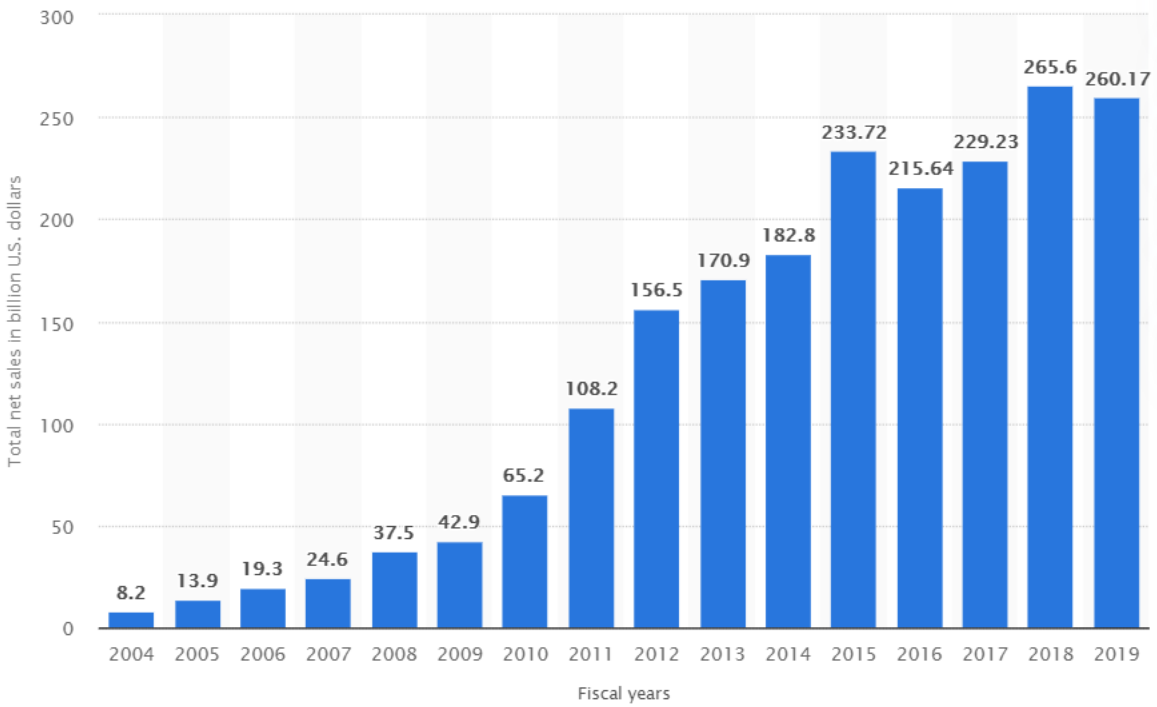
6. BYOD KONCEPT NA IOS I ANDROID PLATFORMAMA

Sve više poduzeća ulaže u mobilne aplikacije na platformama, najčešće su to iOS i Android platforme. Izvješće o mobilnim aplikacijama za 2017. godinu za tvrtke koje je objavio Adobe pojačava rastuću potrebu poduzeća za ulaganjem u mobilne aplikacije. Budući da Apple čini glavni udio na svjetskom tržištu pametnih telefona, iOS je najpoželjnija platforma u razvoju poslovnih aplikacija.[11]

Kao što je prikazano na slici 10., Appleova globalna prodaja iPhonea nastavlja rasti iza vodećih konglomerata mobilne komunikacije.

Stalna popularnost i pouzdanost Appleove linije pametnih telefona učinili su je preferiranim izborom za poduzeća u osiguranju poslovne produktivnosti. iOS je kao mobilna platforma uvijek bio u prvom planu u pogledu robusnosti i sigurnosti.

No stvar je u tome što na trenutnom tržištu postoje jači konkurenti koji se izravno natječu s iOS-om. Android u vlasništvu Googlea izuzetno se dobro snašao na tržištu mobilnih uređaja, ponajviše zahvaljujući brzoj integraciji s Googleovim opsežnim uslugama, fleksibilnosti i podršci.[11]



Slika 10. Globalna prodaja Appleovih mobilni telefona, [37]

6.1. Sigurnost kao prioritet u poslovnim aplikacijama

Podaci kojima tvrtka rukuje ne uključuju samo vlastite podatke, već i podatke njihovih kupaca. Na primjer, banka koja koristi mobilne aplikacije mora imati iznimne sigurnosne značajke jer se koriste za obradu, pohranu i prijenos osjetljivih podataka njihovih klijenata, poput podataka o bankovnom računu.

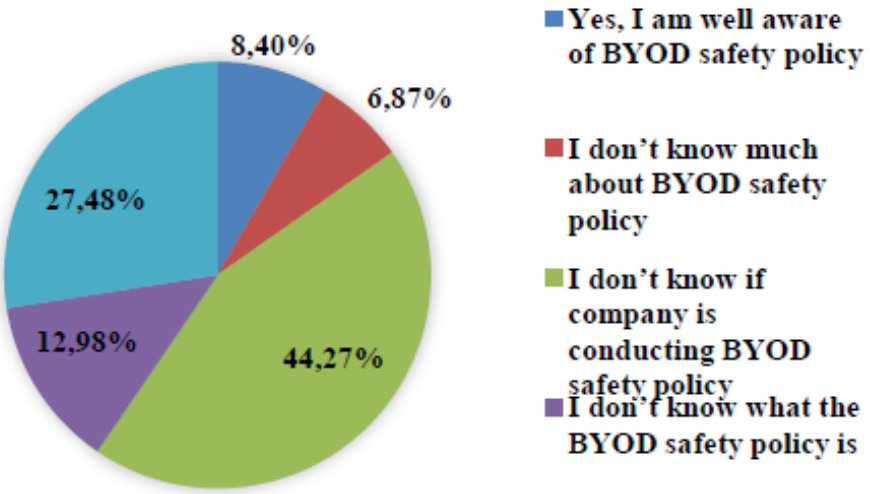
Sigurnost poslovne aplikacije je važna jer:

- Štiti osjetljive podatke i osigurava privatnost podataka
- Podržava reputaciju tvrtke štiteći je od cyber napada

Prema provedenom istraživanju prikazanom na slici 11. može se zaključiti da zaposlenici nisu dovoljno educirani ili nisu svjesni sigurnosne politike tvrtke i načina osiguranja sigurnosti podataka tvrtke.

Čak 44,27% ispitanika ne zna ima li tvrtka u kojoj rade BYOD sigurnosnu politiku. 27,48% ispitanika tvrdi da tvrtka u kojoj rade ne provodi BYOD sigurnosnu politiku, a

12,98% kaže da ne zna što je BYOD sigurnosna politika. 6,87% ispitanika tvrdi da tvrtka ima BYOD sigurnosnu politiku, ali zaposlenik s njom nije upoznat, dok samo 8,40% kaže da tvrtka provodi BYOD sigurnosnu politiku i zaposlenik je s njom dobro upoznat. [21]



Slika 11. Informiranost korisnika o BYOD sigurnosnoj politici, [21]

Globalno, sigurnost je uvijek zauzimala ključnu poziciju u poduzećima zbog strogih normi vezanih uz podatke i komunikacije. Svi mogući nedostaci u sigurnosti mogu ugroziti čitav niz povjerljivih podataka koje tvrtka posjeduje.

Učinak takvih narušavanja sigurnosti u tvrtki je katastrofalan. To može dovesti do ogromnih financijskih gubitaka, izgubiti ili promijeniti osjetljive podatke, pa čak i naštetiti ugledu tvrtke.[11]

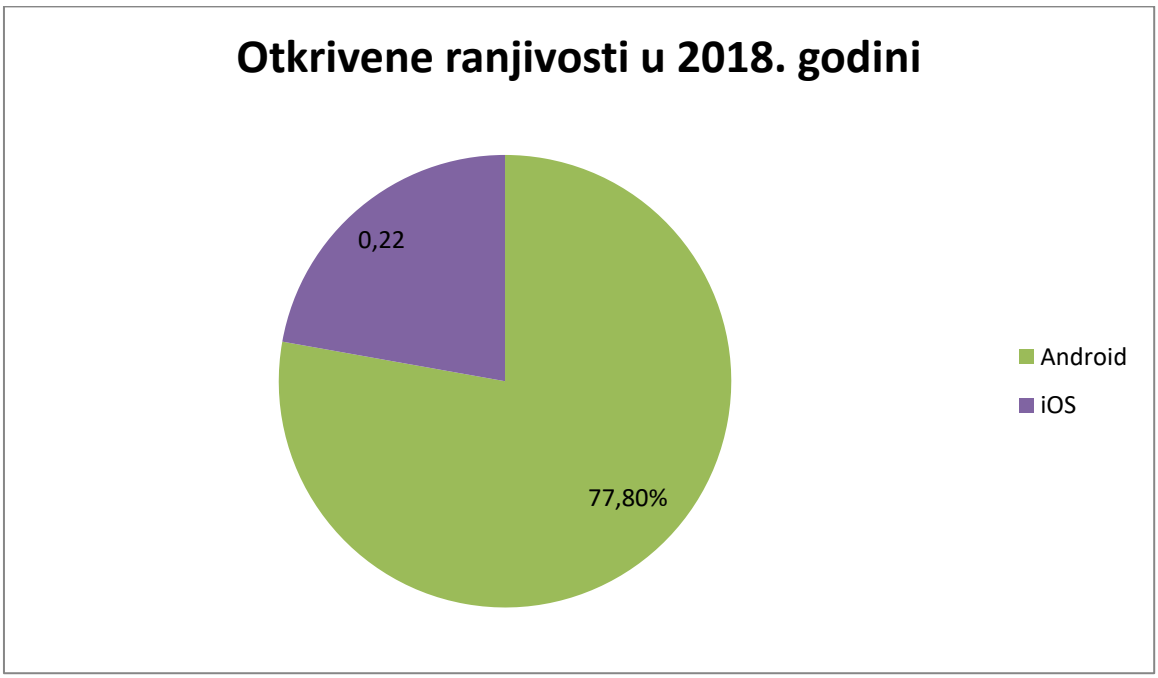
6.2. Rješavanje sigurnosnih ranjivosti u iOS-u i Androidu

Prema Nortonu, globalnom dobavljaču kibernetske sigurnosti, i iOS i Android suočavaju se s nizom sigurnosnih prijetnji i ranjivosti. Dvije mobilne platforme još uvijek pate od nekog oblika ranjivosti usprkos nedavnim nadogradnjama i poboljšanjima.

Do sada iOS ima 1457 ranjivosti prema izvješću objavljenom u detaljima CVE baze podataka o procjeni sigurnosne ranjivosti. Android se skalira s oko 1834 otkrivenih sigurnosnih ranjivosti kako je spomenuto u izvješću. Na grafikonu 1. prikazane su otkrivene ranjivosti na android i iOS platformama u 2018. godini.

Pri procjeni izvješća postaje jasno da iOS ima manje ranjivosti u odnosu na Android. Štoviše, u 2018. godini i iOS-u je pronađeno samo 86 ranjivosti što je velika razlika u odnosu na prethodnu godinu gdje je otkriveno 387 ranjivosti.

Appleova brza primjena najnovijih ažuriranja i ispravci programskih pogrešaka na platformi većinom su riješili mnoge njihove ranjivosti. Android, međutim, ne uspijeva suzbiti ranjivosti koje su još uvijek značajno utjecale na platformu u 2018. godini. [11]



Grafikon 1. Otkrivene ranjivosti na iOS i Android platformama u 2018. godini

Izvor: [11]

6.3. Android i ios sa stajališta sigurnosti

Aplikacije razvijene za poduzeće razlikuju se od onih napravljenih za privatne korisnike. Poduzetnička aplikacija, bilo iOS ili Android, napravljena je za pomoć u različitim poslovnim procesima. Kao dodatna značajka, u poslovne su aplikacije ugrađene određene sigurnosne značajke koje štite podatke i sprečavaju ih od zlouporabe.

Programeri aplikacija uzeli su u obzir nekoliko ključnih sigurnosnih problema prilikom izrade aplikacija za poduzeća. Korištenje jake enkripcije, potpore certifikata i prebacivanje na model oblaka neke su od tehnika koje se koriste za poboljšanje sigurnosti aplikacija.

6.3.1. Razine prijetnji

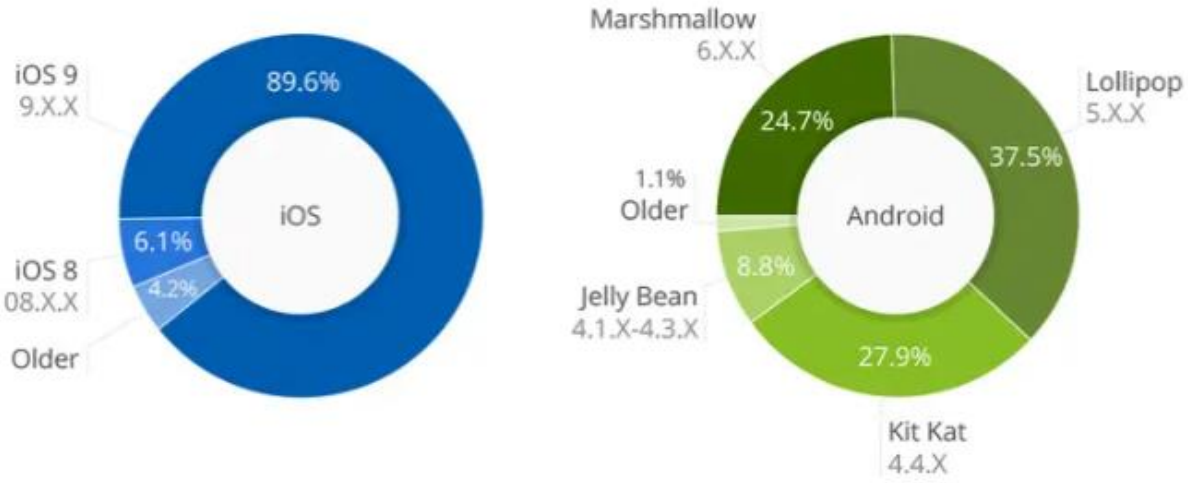
Android OS bazira se na platformi otvorenog koda (eng. open source) posebno je ranjiva na viruse jer omogućuje pokretanje aplikacija trećih strana. Izvješća navode da je 97 posto zlonamjernog softvera na Android platformi. Jasno je da sve veće sigurnosne ranjivosti Androida znače je manje sposoban i manje poželjan za uporabu u poduzeću u odnosu na iOS platformu [11]

Budući da podržava programe trećih strana, Android je uvijek rizičniji za korištenje u poslovne svrhe. iOS nudi određenu razinu zaštite od zlonamjernog softvera i drugih prijetnji zbog svoje zatvorenosti. Tvrtka za razvoj softvera može raditi s iOS-om za izgradnju aplikacija s jasno definiranim sigurnosnim mjerama za poduzeća.

Iako iOS još uvijek ima brojne sigurnosne ranjivosti, njihov se rizik smanjuje nadogradnjama. Štoviše, iOS kao zatvoreni izvor (eng. closed source) ne podržava programe trećih strana, što ratificira sigurnost koju pruža za poslovne programe. [11]

6.3.2. Fragmentacija uređaja

Fragmentacija uređaja jedna je ključna značajka koja određuje razinu sigurnosti koja se nudi u aplikaciji platforme. Veća fragmentacija rezultirat će povećanim rizikom od povrede podataka.



Slika 12. Fragmentacija raznih verzija Andriod i iOS uređaja u 2014.g. [15]

6.3.3. Sigurnost softvera

I iOS i Android sigurnosti imaju presudan prioritet. Kao dio toga, obje platforme izbacuju česta ažuriranja kako bi poboljšale zaštitu uređaja od novih oblika prijetnji. iOS povremeno izdaje ažuriranja koja se obavezno instaliraju na uređaj.

Android također objavljuje nova ažuriranja kako bi poboljšao funkcionalnost i sigurnost svog OS-a. Ali to nije obvezno jer korisnici mogu odrediti hoće li ažurirati svoje uređaje. Izostanak ažuriranja može učiniti uređaj i aplikacije ranjivim na razne prijetnje. [11]

6.4. Potrebe za poslovnim upravljanjem

Što se tiče upravljanja raznim operacijama povezanim s poduzećem, i iOS i Android imaju ugrađeni skup značajki i funkcionalnosti. To će pomoći upravljanju mobilnim uređajima da pomogne poduzećima da povećaju sigurnost i učinkovitost u svom poslovanju.

iOS platforma pruža:

- BYOD kompatibilan zbog boljih alata za upravljanje mobilnim uređajima.
- Jednostavna centralizirana administracija za kontrolu svih povezanih iOS uređaja.
- Poboljšano korisničko iskustvo koje pokreće rast i poboljšava učinkovitost

U slučaju Androida, upravljanje mobilnim uređajima ne uspijeva postići onu razinu fleksibilnosti koju nudi iOS. Budući da različiti proizvođači različito upravljaju mobilnim uređajima, to sprječava centralizirano upravljanje uređajima, što je preduvjet mobilnosti poduzeća.

6.5. Android radni profil (work profile)

Radni profil odvaja radne aplikacije i podatke na Android uređaju od osobnih aplikacija i podataka. Prema zadanim postavkama, obavijesti i ikone radnog profila za aplikacije instalirane na radnom profilu označene su radnom značkom (ikona aktovke) kako biste ih mogli razlikovati od osobnih aplikacija što je prikazano na slici 13.[12]

Slika 13. Sučelje Android uređaja sa aktivnim radnim profilom, [14]

Radni profili IT odjelu omogućuju sigurno upravljanje radnim okruženjem bez ograničavanja korisnika da koriste svoj uređaj za osobne aplikacije i podatke. Ako vaša organizacija to podržava, vaš IT odjel trebao bi pružiti upute za dodavanje radnog profila na vaš Android 5.0 Lollipop ili noviji uređaj. Preporučeno je imati što višu verziju Android softvera jer svaka nova nadogradnja može onemogućiti neke zastarjele opcije radnog profila ili pak uvesti neke nove.[12]

Kada se radni profil postavi na uređaju u osobnom vlasništvu, aplikacija koja upravlja pravilima uređaja predstavit će uvjete korištenja i detaljno prikazati podatke na vašem uređaju koji su zabilježeni i snimljeni. Zaposlenik ima obvezu pregledati uvjete korištenja i prihvatiti ugovor o korisničkoj licenci da bi se radni profil mogao implementirati.

Pomoću radnih profila administratori mogu izvršiti neke ili sve sljedeće radnje:

- mijenjanje postavki i stavljanje ograničenja aplikacijama
- zapisivanje, promjena i brisanje podatke u radnom profilu
- instalacija i brisanje aplikacija i certifikata
- stvaranje popisa aplikacija koje imaju pristup podacima na radnom profilu

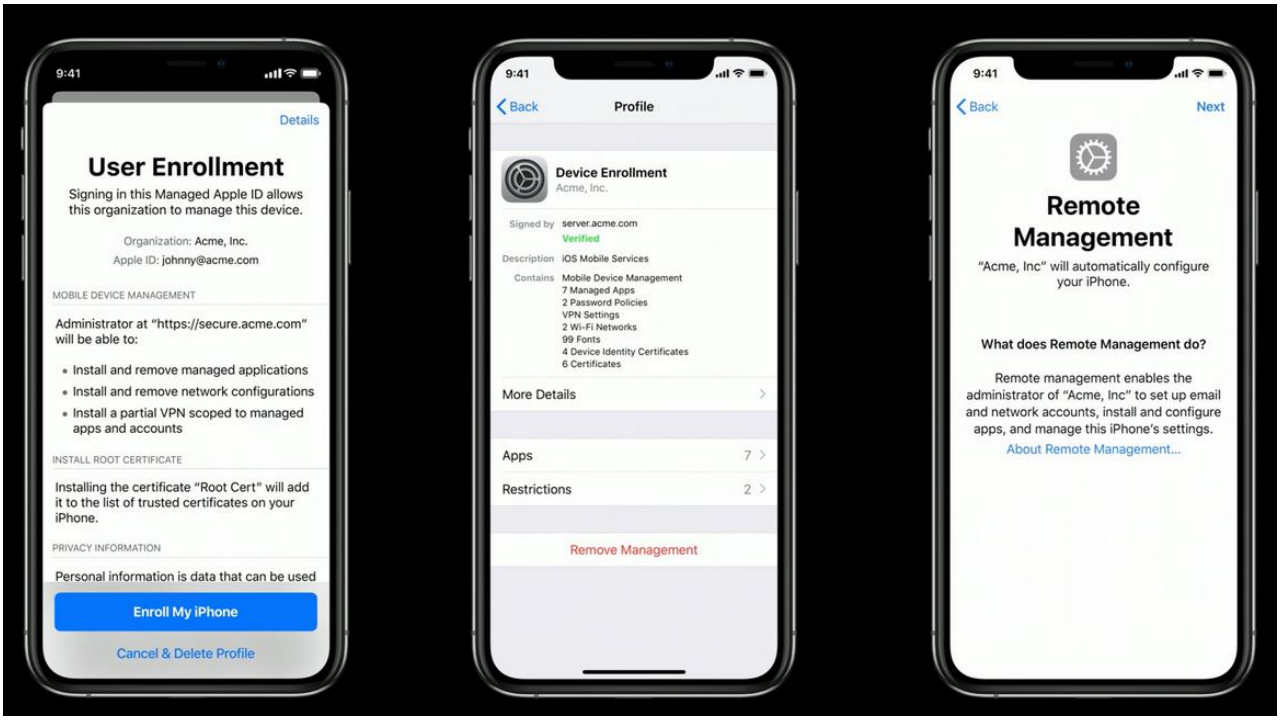
- daljinsko brisanje podatke radnog profila
- ograničavanje dijeljenja između osobnog i radnog profila
- blokiranje snimanja zaslona na radnom profilu
- pregledavanje statističkih podatke o upravljanom računu
- upravljanje korporativnim pristupom poslužitelju pošte i internim podacima
- mijenjanje lozinke računa
- nadgledanje mrežne aktivnosti i informacije o lokaciji [12]

Na primjer, prije nego što se dovrši postavljanje radnog profila, administrator može odrediti da uređaj ima lozinku s najmanje 4 znaka i da se koriste najnovija pravila uređaja. Kasnije mogu postojati različita pravila za zaštitu uređaja, poput mogućnosti brisanja računa s uređaja nakon 30 dana bez sinkronizacije odnosno 30 dana neaktivnosti radnog profila.

6.6. iOS User Enrollment

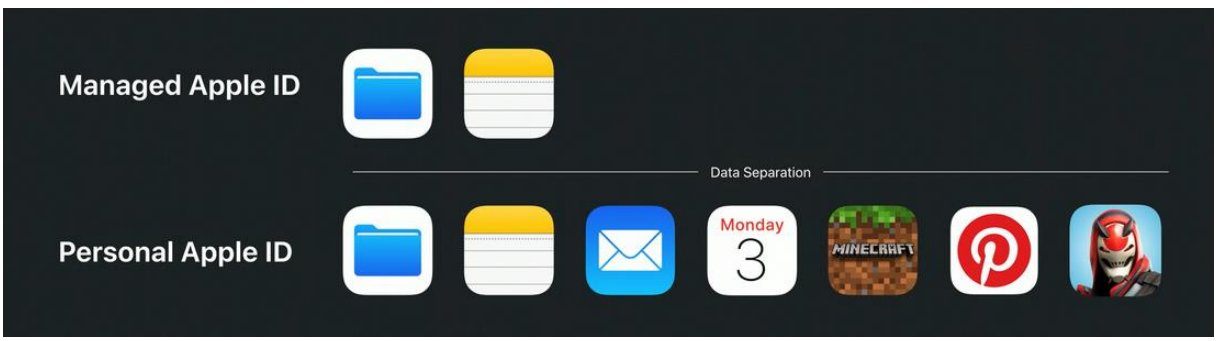
BYOD je trenutno MDM aktivacija, što znači da je MDM profil instaliran i da administratori imaju velika ovlaštenja na uređaju. Ili možete koristiti aktivaciju samo za MAM (eng. Mobile Application Management – only).

Za BYOD Apple sada provodi aktivaciju User Enrollment-a. Koraci njegove aktivacije prikazani su na slici 14. Tehnički, ovo nije pristup više korisnika, već više računa. Korisnik se na svoj uređaj prijavljuje svojim poslovnim Apple ID-om uz svoj privatni. Kao rezultat toga, administratori moraju registrirati vlastitu domenu kod Apple Business Managera (ABM) ili nadograditi svoj DEP račun na ABM. Ako je uređaj deaktiviran, Managed Apple ID automatski se briše s uređaja. [13]



Slika 14. Aktivacija User Enrollment-a, [13]

Aplikacije su vezane uz Apple ID i mogu se koristiti samo s tim ID-om. Slikom 15. prikazano je sučelje uređaja kada je aktiviran odnosno koje značajke se koriste u poslovne svrhe, a koje u privatne. Izuzete su aplikacije koje pristupaju računima. Oni zatim podatke dobivaju iz upravljanih i neupravljanih izvora putem računa.[13]



Slika 15. Sučelje aktiviranog BYOD uređaja, [13]

Tijekom aktivacije stvara se upravljani APFS disk s vlastitim ključevima. Upravljani izvori zapisuju podatke samo na ovaj disk: „kontejneri“ s aplikacijama, bilješke, iCloud datoteke, privjesak za ključeve, elektronička pošta, prilozi kalendara. Ako se uređaj deaktivira podaci sa navedenih izvora ce se izbrisati.

MDM protokol ne pruža trajne podatke kao što su UDID, IMEI i slično tijekom aktivacije upisa korisnika. ID za registraciju korisnika koristi se za identifikaciju i s njime se prijavljuje na MDM poslužitelje. Ako se uređaj deaktivira ID korisnika se briše, a uređaj dobiva nove ID-ove ako se ponovno aktivira.

6.7. iOS user enrollment vs. Android work profile

iOS User Enrollment s obzirom na Android Enterprise Work Profile ima ozbiljnu razliku, a to je da se ne temelji se na više korisnika. To vam daje neka ograničenja na iOS uređajima koja nemate na Androidu:

- Android aplikacija može se istovremeno koristiti i kao privatna i kao poslovna aplikacija.
- Uz Google PlayStore za posao imate vlastitu trgovinu za poslovne aplikacije na uređaju bez potrebe da EMM mora implementirati trgovinu s aplikacijama na svoj način.
- Profil rada može implementirati globalne postavke poput VPN-a. Dakle, svaka poslovna aplikacija koristi VPN vezu (sve dok nisu definirane iznimke).
- Android ne ograničava pristup uređaju kao što to čini iOS (samo 6-znamenkasti pin ili složeni).
- Na Androidu ne postoji ovisnost o VPN-u i domeni.
- Profil rada može se deaktivirati u smislu pristupačnosti. Tako korisnik može isključiti cijelo poslovno područje na kraju dana i ponovo ga uključiti sljedeći dan. [13]

7. ZAKLJUČAK

Sve više se razvija BYOD trend. Tvrtke puno više cijene prednosti korištenja vlastitog uređaja nego nedostatke, kojih je dosta. BYOD se razvija i smanjuju se sigurnosne prijetnje razvijanjem novih sigurnosnih aplikacija i nadograđivanjem postojećeg softvera i hardvera. Najviše se koriste iOS (User Enrollment) i Android (Work profile) platforme i svaka od njih ima svoje prednosti i svoje mane. I Android i Apple mogu se pohvaliti snažnim sigurnosnim mjerama za svoje uređaje zbog kojih je teško birati između njih. iOS kao sustav je puno zatvoreniji i nema toliko manevarskog prostora koliko ima na Android platformi. Razlike BYOD koncepta na ovim platformama su velike, i to je možda u nekim situacijama i velika prednost.

Da bi se mogao koristiti BYOD, prije svega potrebno je uključiti značajku sustava koja se u iOS okruženju naziva User Enrollment (UE), a u Androidu Work profile. Dok je Work profile značajka za više korisnika, UE nije. Ona je značajka za više računa. Korisnik iOS uređaja dobiva korporativni račun koji ima sadrži aplikacije za traženu BYOD uslugu i konfiguriran je prema dogovoru. Radni profili Androida IT odjelu omogućuju sigurno upravljanje radnim okruženjem bez ograničavanja korisnika da koriste svoj uređaj za osobne aplikacije i podatke. Kod Androida jedna aplikacija se može koristiti i za javne i za poslovne svrhe, dok su u iOS- u to dvije zasebne aplikacije.

Činjenica je da je BYOD koncept na obje platforme na odličnoj razini. I sa strane sigurnosti i sa strane upravljanja i da obje platforme odlično obavljaju i implementaciju i podršku za BYOD uslugu. Puno je mjesta za napredak i za još veći razvoj ovog koncepta Razvijanjem novih mogućnosti i razvijanjem sigurnosti „Bring your own device“ ima sigurnu budućnost u poslovnom svijetu.

LITERATURA

[1] „Bring Your Own Device (BYOD)“ Dostupno: https://cio-wiki.org/wiki/Bring_Your_Own_Device_(BYOD) (Zadnje pristupano: 3.8. 2020.)

[2] „Bring your own device“ Dostupno: https://wikivisually.com/wiki/Bring_your_own_device (Zadnje pristupano: 5.8.2020.g.)

[3] „What is Bring Your Own Device (BYOD)?“ Dostupno: https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod (Zadnje pristupano: 20.8.2020.g.)

[4] „Secure Architecture for BYOD Access to On-Premises Applications“ Dostupno: https://hitachi-id.com/documents/secure-architecture-for-mobile-device-access-to-on-premises-applications.php?page=1 (Zadnje pristupano: 17.8.2020.g.)

[5] Macaraeg, T.: BRING-YOUR-OWN-DEVICE (BYOD): ISSUES AND IMPLEMENTATION IN LOCAL COLLEGES AND UNIVERSITIES IN THE PHILIPPINES Dostupno: https://www.researchgate.net/figure/Basic-BYOD-Architecture_fig1_313649980 (Zadnje pristupano: 15.8.2020.)

[6] „Secure Architecture for BYOD Access to On-Premises Applications“ Dostupno: https://hitachi-id.com/documents/secure-architecture-for-mobile-device-access-to-on-premises-applications.php?page=2 (Zadnje pristupano: 17.8.2020.g.)

[7] „Secure Architecture for BYOD Access to On-Premises Applications“ Dostupno: https://hitachi-id.com/documents/secure-architecture-for-mobile-device-access-to-on-premises-applications.php?page=3 (Zadnje pristupano: 17.8.2020.g.)

[8] „HIGH LEVEL BRING YOUR OWN DEVICE (BYOD) ARCHITECTURE“ Dostupno:https://images01.insight.com/media/pdf/0412IPSHighLevelBYODArchitectureDatasheet.pdf?cm_mmc=EDM-_-partnerAdHoc-_-ET1234-_-sideLink5 (Zadnje pristupano: 12.8.2020.g.)

[9] Matteucci, G.: The Pros and Cons of Bring-Your-Own-Device (BYOD) for Your Mobile Field Workforce – Field Force Friday Dostupno: https://www.msidata.com/pros-and-cons-of-byod-in-mobile-field-workforce/ (Zadnje pristupano: 12.8.2020.g.)

[10] Russell, W., Gilmore, Cissp, Cism, Ence: BENEFITS AND DISADVANTAGES OF BYOD https://protus3.com/benefits-and-disadvantages-of-byod/ (Zadnje pristupano: 26.8.2020.g.)

[11] Dass, R.: Enterprise Android vs IOS : Which is more secure? Dostupno: https://medium.com/@ritidass29/enterprise-android-vs-ios-which-is-more-secure-3ccf90ff81f1 (Zadnje pristupano: 10.8.2020.g.)

[12] „What is a work profile?“ Dostupno: https://support.google.com/work/android/answer/6191949?hl=en] (Zadnje pristupano: 10.8.2020.)

[13] „Presentation of iOS BYOD and comparison to Android“ Dostupno: https://9to5mdm.com/2019/06/presentation-of-ios-byod-and-comparison-to-android/ (Zadnje pristupano: 7.8.2020.g.)

[14] Knox Developer Documentation: „What happens to existing Work Profiles?“ Dostupno: https://docs.samsungknox.com/dev/knox-sdk/existing-android-profiles.htm (Zadnje pristupano: 23.8.2020.g.)

[15] Rosoff, M: Why Google would want to build its own phone Dostupno: https://www.businessinsider.com/chart-android-vs-ios-fragmentation-2016-6 (Zadnje pristupano 5.9.2020.)

[16] IBM: „What is Bring Your Own Device (BYOD)? Dostupno: https://www.ibm.com/services/digital-workplace/byod (Zadnje pristupano: 21.8.2020.g.)

[18] „What is BYOD?“ Dostupno https://one.comodo.com/byod-bring-your-own-device/ (Zadnje pristupano: 25.8.2020.)

[19] „Secure Bring Your Own Device (BYOD) for iOS, macOS, Android and Windows“ Dostupno: https://mediacenter.ibm.com/media/0_o9c56key (Zadnje pristupano: 2.9.2020.g.)

[20] Peraković, D., Husnjak S., Cvitić I. Comparative Analysis of Enterprise Mobility Management Systems in BYOD Environment // RCITD 2014 (Zadnje pristupano: 5.9.2020.g.)

[21] Peraković, D., Husnjak S., Mišić V., Kuljanić T. M.: Employee's awareness on security aspects of use bring your own device paradigm in Republic of Croatia // RCITD 2016 (Zadnje pristupano: 5.9.2020.g.)

[22] Slottow, T.: Action learning project : Bring your own device (BYOD), Business Finance Leadership Academy, 2012 (Zadnje pristupano: 29.8.2020.g.)

[23] Peraković, D., Husnjak, S., Remenar, V.: Research of security threats in the use of modern terminal devices, 23td International DAAAM Symposium, vol. 23, 2012, pp. 545–548 (Zadnje pristupano: 29.8.2020.g.)

[24] Murugiah, S., Scarfone, K.: Guidelines for managing and securing mobile devices in the enterprise (Draft), NIST, National Institute of Standards and Technology, USA, 2013 (Zadnje pristupano: 29.8.2020.g.)

[25] BlackBerry: Finding the right mobile device containerization solution, BlackBerry, 2014 (Zadnje pristupano: 5.9.2020.g.)

[26] TechTarget: Enterprise mobility management : choosing the right approach and considering costs, Techtarget, USA, 2014 (Zadnje pristupano: 30.8.2020.g.)

[27]] Scarfone, K., Souppaya, Hoffman, P.: Guide to security for full virtualization technologies, NIST, National Institute of Standards and Technology, USA, 2011 (Zadnje pristupano: 25.8.2020.g.)

[28]] CDW Government LLC: Virtual desktop infrastructure goes mobile (White paper), CDW Government LLC, 2013 (Zadnje pristupano: 19.8.2020.g.)

[29] Mobile virtualization: Hypervisors go small. (2014. Jun 23) Online Document. Dostupno: http://mobilecomputingtrek.wordpress.com/2012/04/04/mobilevirtualization-hypervisors-go-small/ (Zadnje pristupano: 20.8.2020.g.)

[30] Mobile device management technologies. (2014, Jun 23) Online Document. Dostupno:: http://ukblog.immobility.com/book/export/html/7. (Zadnje pristupano: 1.9.2020.g.)

[31] Dostupno: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html (Zadnje pristupano: 7.9.2020.g.)

[32] Dostupno: https://searchmobilecomputing.techtarget.com/definition/access-point (Zadnje pristupano: 2.9.2020.g.)

[33] Dostupno: https://www.teldat.com/blog/en/what-is-a-wireless-lan-controller-and-who-has-taken-it-to-the-cloud/ (Zadnje pristupano: 2.9.2020.g.)

[34] Dostupno: https://www.ssl.com/faqs/what-is-a-certificate-authority/ (Zadnje pristupano: 2.9.2020.g.)

[35] Dostupno: https://www.retailcustomerexperience.com/blogs/8-byod-benefits-for-organizations-with-frontline-staff/ (Zadnje pristupano: 20.8.2020.g.)

[36] Dostupno: https://staffbase.com/blog/six-advantages-byod-bring-your-own-device/ (Zadnje pristupano: 20.8.2020.g.)

[37] Dostupno: https://www.statista.com/statistics/265125/total-net-sales-of-apple-since-2004/ (Zadnje pristupano: 7.9.2020.g.)

POPIS KRATICA

IAM- sustav identiteta i pristupa (Identity and Access Management)

DMZ- fizička je ili logična podmreža koja sadrži i izlaže vanjske usluge organizacije nepouzdanoj, obično većoj mreži kao što je Internet (Demilitarized zone)

VM- virtualna mašina (Virtual Machine)

VDI- softverska tehnologija koja razdvaja okruženje radne površine i pripadajući softver od fizičkog uređaja klijenta koji se koristi za pristup njemu (Virtual Desktop Infrastructure)

PoE- napajanje preko Ethernet kabela (Power over Ethernet)

ISR- usmjerivač integrirane usluge (Integrated Services Routers)

AP- Pristupna točka (Access Point)

WLC- bežični LAN kontrolor (Wireless LAN Controller)

ISE- Identity Services Engine

RSA- Sučelje za pohranu identiteta (Rivest–Shamir–Adleman)

CA- certifikat (Certificate authority)

POPIS SLIKA

POPIS GRAFIKONA