UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

MAGISTRSKO DELO

PRIMERNOST KONCEPTA "PRINESI SVOJO NAPRAVO" ZA POSLOVANJE PODJETIJ

Ljubljana, junij 2016

SLAVKO KOREN

IZJAVA O AVTORSTVU

Podpisani Slavko Koren, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Primernost koncepta »prinesi svojo napravo« za poslovanje podjetij, pripravljenega v sodelovanju s svetovalcem prof.dr. Tomažem Turkom.

IZJAVLJAM

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študenta:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

V zadnjih letih je tehnološki razvoj z vidika uporabnikov najbolj zaznamoval porast mobilnih naprav nove generacije. To so pametni mobilni telefoni in tablični računalniki – tablice, ki so dejansko postale tehnološko napredne naprave.

Mobilni telefoni so opremljeni s prilagojenimi operacijskimi sistemi, ki omogočajo uporabnikom, da sami prilagajajo in izbirajo programsko opremo, ki si jo želijo naložiti. Programska oprema, ki je na voljo, je razvita po enotnih načelih, medsebojno združljiva, uporabniki pa jo lahko za plačilo ali pa tudi brezplačno dobijo v okviru posebnih zbirk – tržnic programskih rešitev (Hmelak & Žust, 2012).

Tablični računalniki oz. mobilne tablice so računalniki priročnega formata, ki nimajo tradicionalnih vhodnih naprav, kot so tipkovnica ali miška in nimajo izhodnih naprav, kot je npr. ločen monitor. Enako kot pametni telefoni delujejo na podlagi operacijskih sistemov, ki uporabnikom omogočajo poljubno nastavitev naložene programske opreme, ki je prav tako na voljo na tržnicah programskih rešitev (Hmelak & Žust, 2012).

Kdo so delavci prihodnosti, se v poročilu o povezanem svetu sprašuje družba Cisco (2014a), ki iz spletne ankete, ki jo je izpolnilo 2.912 zaposlenih iz različnih okolij in podjetij, ugotavlja, da že večina vprašanih uporablja 2 do 3 mobilne naprave dnevno in ima na svojih mobilnih napravah naloženih več kot 20 aplikacij. Skoraj 70 odstotkov vprašanih uporablja te aplikacije tudi v službene namene. Večina novodobnih delavcev prihodnosti ima rada neobičajne delovnike z mobilnim delovnim časom in delom od doma ter pripravljenostjo 24 ur na dan, 7 dni v tednu, tako preko telefona kot tudi preko elektronske pošte. To pomeni, da dostopajo do podatkov podjetja kadarkoli in od koderkoli. Dve tretjini vprašanih verjame, da imajo podjetja, ki dovolijo delavcem mobilnost, tudi z delom od doma, konkurenčno prednost pred tradicionalnimi podjetji s fizično prisotnostjo.

Kar je s stališča varnosti najbolj zaskrbljujoče v tem poročilu (Cisco, 2014a) pa je, da je 40 odstotkov vprašanih pripravljenih v zameno za brezplačni mobilni telefon z neomejenim prenosom podatkov dovoliti operaterjem dostop do vseh podatkov shranjenih na telefonu. S stališča podjetij je tako dejanje lahko zelo zaskrbljujoče, kajti ogroženi so njihovi podatki, ki jih imajo njihovi zaposleni shranjene na svojih mobilnih napravah, s katerimi dostopajo do vseh virov podjetja.

Nadalje, Ciscovo poročilo (2014b) ugotavlja, da mnogo uporabnikov dnevno prenaša mobilne aplikacije iz tržnic programske opreme, ne da bi sploh pomislili na varnost.

Družba Ericsson (2015) v svojem letnem poročilu ugotavlja, da se bodo nakupi novih mobilnih naprav več kot podvojili do leta 2020, iz 2,8 mrd nakupov v letu 2014 na 6,5 mrd

nakupov leta 2012, kar pomeni 15 odstotkov skupne letne stopnje rasti (angl. *Compound Annual Growth Rate*, v nadaljevanju CAGR). Z njihovo rastjo, kot tudi z rastjo mobilne tehnologije in z večjo dostopnostjo in razpoložljivostjo storitev mobilne tehnologije tretje in četrte generacije, v nadaljevanju 3G/4G, se je v poslovnem okolju ustvaril nov pojav »prinesi svojo napravo« (angl. *Bring Your Own Device – BYOD*, v nadaljevanju PSN) (Prashant et al., 2013), ki zaposlenim omogoča uporabo lastnih mobilnih naprav v službene namene in dostop do vseh virov podjetja (Keyes, 2013).

Uporaba mobilnih naprav hkrati za osebno kot tudi za profesionalno delo z dostopom do virov podjetja pa prinaša podjetjem tudi tveganja in grožnje, ki jih je za samo varnost podjetja potrebno identificirati in po potrebi zmanjšati. Poleg popolne prepovedi PSN v okolju podjetja je eden od načinov zmanjšanja tveganja in groženj predpis osnovnih varnostnih standardov, ki jih morajo mobilne naprave podpirati, preden jih zaposleni smejo uporabiti v poslovnem okolju. Ti varnostni standardi morajo vključevati minimalne zahteve glede dolžine in kompleksnosti gesel, prisotnost protivirusne zaščite, kriptiran oddaljen dostop ter možnosti za oddaljeno upravljanje naprav. Potrebno je dodatno šolanje uporabnikov, z vsakim zaposlenim je potrebno skleniti dodatek k pogodbi o uporabi svoje mobilne naprave za dostop do podatkov podjetja (Hmelak & Žust, 2012).

PSN je tu, v porastu in prinaša podjetjem prednosti ter nove izzive. Prinaša pa tudi grožnje in s tem povezana tveganja. Vedno več podjetij se srečuje s tem novim izzivom, zato morajo sprejeti strategijo in se opredeliti do politike PSN. Izziv podjetja je, da vse mobilne naprave, še zlasti osebne naprave zaposlenih, vključi v enotno shemo informacijske varnosti z izbiro strategije in razvojem svoje lastne politike PSN (Hmelak & Žust, 2012; Prashant et al., 2013; Manmeet et al., 2014).

Kot ugotavljata Hmelak in Žust (2012) popolna prepoved uporabe lastnih osebnih naprav na delovnem mestu dolgoročno ne bo mogoča, hkrati pa bodo uporabniki zavračali številne tradicionalne varnostne mehanizme, ker jih bodo omejevali pri uporabi njihovih naprav. Z vidika produktivnosti je uporaba mobilnih naprav na delovnem mestu dokaj smiselna, kajti nove naprave omogočajo delo kadarkoli in skoraj kjerkoli, kar pa prinaša tudi številne potencialne prednosti, kot so večja produktivnost, večja fleksibilnost, zmanjšanje stroškov podjetja in večja učinkovitost informacijske tehnologije.

Splošno razširjena in znana rešitev za PSN je uporaba centraliziranega orodja za upravljanje mobilnih naprav (angl. *Mobile Device Management*, v nadaljevanju MDM), ki ga priporoča Nacionalni inštitut za standarde in tehnologijo Združenih držav Amerike (angl. *National Institute of Standards and Technology,* v nadaljevanju NIST), v svojem dokumentu Smernice za upravljanje in varovanje mobilnih naprav v podjetju (angl. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*) (NIST, 2013). Med drugim ugotavlja, da je ročno upravljanje mobilnih naprav zelo zahtevna naloga, saj le te pogosto

nimajo kakovostnih varnostnih mehanizmov in ustrezne programske opreme za upravljanje preko oddaljenega dostopa. Poleg nadzora nad mobilnimi napravami in njihovim upravljanjem, MDM zagotavlja tudi varen dostop do internih podatkov podjetja.

Zadnje leto se na tržišču veliko govori o virtualizaciji mobilnih naprav (angl. *Virtual Mobile Infrastructure,* v nadaljevanju VMI). VMI funkcionalno prekine tok podatkov med podjetjem in PSN uporabnikom ne da bi mu preprečil dostop do njih. Strežniška infrastruktura v podjetju implementira virtualno mobilno napravo, uporabnik pa dostopa do nje s pomočjo odjemalca na svoji mobilni napravi. Med njima pa ni pretoka podatkov, temveč samo dotikanje zaslona in slik podatkov. Podatki podjetja, do katerih zaposleni dostopajo, niso več shranjeni lokalno na mobilni napravi (Hazelton, 2015).

Predstavitev problema. Zadnja leta so podjetja sledila NIST smernicam in implementirale MDM orodje za centralizirano upravljanje mobilnih naprav. Po nekaj letih ugotavljamo, da se to orodje zaradi vedno večjih zahtev trga le še dopolnjuje, postaja čedalje bolj okorno, težko se ga upravlja, sama implementacija pa zahteva veliko časa, denarja in znanja. MDM prav tako ne rešuje vseh problemov, ki obstajajo; npr. s stališča uporabnikov je uporaba MDM lahko zakonsko vprašljiva in posega v varstvo osebnih podatkov zaposlenih (npr. problematično zbiranje informacij o naloženih aplikacijah ter izbris na daljavo v primeru kraje, izgube, odhoda zaposlenega v drugo podjetje ali zaradi večkratnega napačno vnesenega PINa, ipd.). S stališča podjetja pa je problematično predvsem uhajanje in kraja podatkov, shranjenih na osebnih mobilnih napravah zaposlenih.

S hitro rastjo mobilne tehnologije, z vedno višjimi omrežnimi hitrostmi in z večjimi zmogljivostmi mobilnih naprav, zaposleni zelo hitro menjajo mobilne naprave in to hitreje, kot jim lahko to zagotovi podjetje. Zato podjetja spodbujajo zaposlene, da kupijo svoje mobilne naprave in s tem povečujejo zadovoljstvo in produktivnost zaposlenih. Zaposleni pa se lahko sami odločijo, katero napravo bodo kupili in namesto dveh uporabljali samo eno mobilno napravo. Hkrati pa jim morajo podjetja dovoliti dostop do korporativnih podatkov.

Z rastjo različnih tipov mobilnih naprav in različnih vrst operacijskih sistemov PSN politika ustvarja negotovo in v večji meri nezaščiteno okolje, ki se preko različnih dostopov razširja in postaja težko obvladljivo pred različnimi napadi iz omrežja. Za podjetja postaja vedno težje uveljaviti varnostno politiko nad mobilnimi napravami, vedno težje je slediti uhajanju korporativnih informacij, zaposleni pa so vedno bolj in bolj zaskrbljeni za svojo zasebnost.

Namen in cilji dela. Namen in cilj magistrskega dela je najti koncept PSN okolja, ki bo varno in hkrati sprejemljivo, tako za podjetje kot tudi za zaposlene. V ta namen bomo prikazali kakšni so izzivi in priložnosti, ki jih PSN koncept prinaša in kako ga vključiti v podjetje z različnimi pristopi. Identificirali bomo grožnje informacijske varnosti pri rabi mobilnih naprav v podjetju, podali zahteve informacijske varnosti in ukrepe za zmanjšanje

tveganj. Identificirali bomo cilje za varno PSN okolje ter pregledali, analizirali in ocenili trenutno stanje tržišča z orodji za upravljanje mobilnih naprav, med njimi tudi virtualne rešitve oz. VMI. Na koncu bomo s primerjalno študijo ugotovili, kako komercialne implementacije rešujejo probleme in funkcionalnosti, ki jih ima klasično centralizirano orodje za upravljanje mobilnih naprav ter izdelali analizo, podali smernice za nadaljnje korake in odgovorili na vprašanje magistrske naloge:

»Ali lahko z virtualizacijo mobilnih naprav VMI ustvarimo varno PSN okolje za podjetje in zaposlene?«

Metode dela. Magistrsko delo je sestavljeno iz teoretičnega in raziskovalnega dela. Pri izdelavi teoretičnega dela smo uporabili deskriptivno metodo ter analizo primarnih in sekundarnih virov. Sklicevali smo se predvsem na tujo strokovno literaturo in vire, pridobljene z interneta, saj je obravnavano področje dokaj novo v znanstvenih krogih. Oprli smo se tudi na smernice največjih svetovnih proizvajalcev strojne in programske opreme, na smernice vodilnih svetovnih neodvisnih ponudnikov raziskav in analiz na področju informacijske tehnologije ter na splošne trende, ki veljajo na tem področju.

Empirični del magistrskega dela temelji na metodi kompilacije in komparacije. Iz analize rešitev, ki so na tržišču, smo izluščili ključne skupne in razlikujoče elemente. Za izbrane rešitve smo preverili uporabniško izkušnjo na relaciji uporabnik – uporabniški vmesnik – strežnik – korporativno podatkovno okolje in kritično presodili, ali predstavljajo izvedljivo in zadovoljivo rešitev.

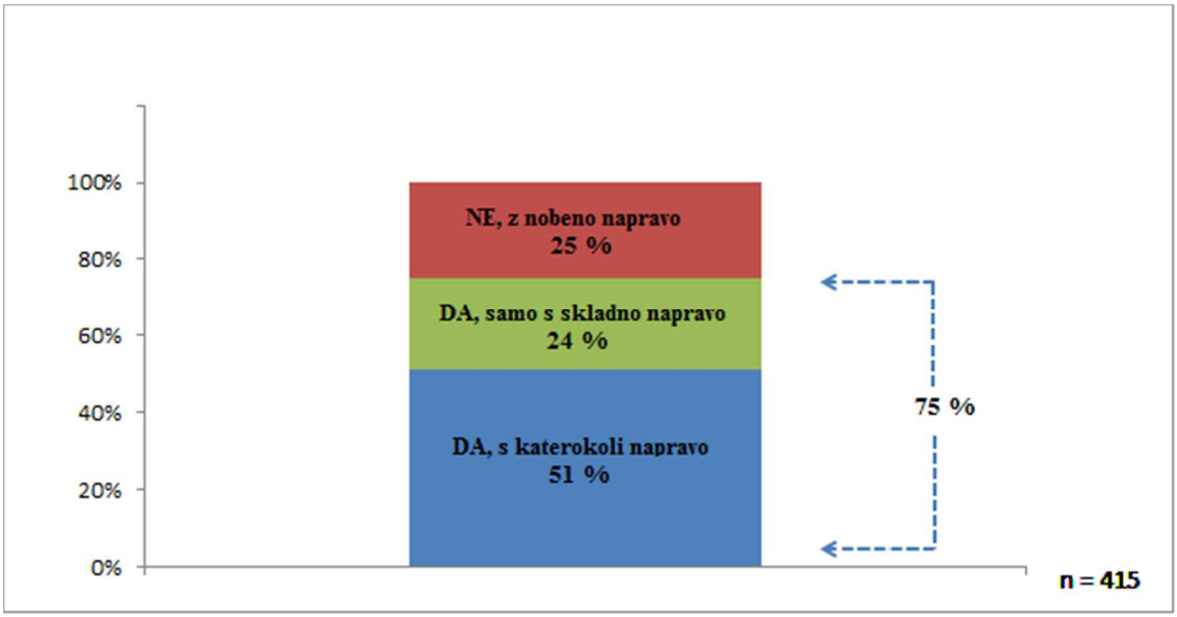
Magistrsko delo je sestavljeno iz štirih glavnih poglavij, tematika je še dodatno razdelana v podpoglavjih. V uvodnem poglavju je predstavljena obravnavana problematika z opredeljenim načrtom raziskave. V prvem poglavju smo opisali kaj je koncept PSN, njegove začetke, prednosti, slabosti, priložnosti ter izzive tako za podjetja kot tudi za zaposlene. Opisali smo korake, ki jih morajo podjetja slediti pri vpeljavi PSN koncepta v podjetje, od merjenja uspešnosti do priprave strategije in modela PSN. V drugem poglavju smo preverili, kakšne so zahteve informacijske varnosti, ki so potrebne za izvajanje politike PSN. Podali smo model varnostne politike PSN okolja, opisali vsa tveganja informacijske varnosti, ki jih mobilne naprave vnašajo v poslovno okolje ter podali ukrepe za zmanjšanje teh tveganj. Poiskali smo tudi cilje za varno PSN okolje. V tretjem poglavju smo navedli ter raziskali, katera orodja za nadzor nad mobilnimi napravami obstajajo in jih primerjali s cilji po varnem PSN okolju. V četrtem poglavju smo raziskali trg virtualizacije mobilnih naprav – VMI. Med izbranimi ponudniki smo naredili testiranje in na koncu na podlagi ciljev, ki smo si jih zadali, naredili analizo, odgovorili na raziskovalno vprašanje in podali napotke za nadaljnje delo.

1 KONCEPT »PRINESI SVOJO NAPRAVO« V PODJETJIH

1.1 Zgodovina in podatki

Pojem PSN se je prvič pojavil leta 2009, ko je podjetje Intel spoznalo vse večjo težnjo svojih zaposlenih po uporabi lastnih mobilnih naprav v njihovem delovnem okolju, ter povezovanjem v njihovo omrežje (Garner, 2013). Vendar je šele v letu 2010 dokončno zaživelo, ko je podjetje Apple predstavilo svojo mobilno tablico iPad (Apple Launches iPad, 2016) in podjetje Google svoj mobilni telefon Nexus One s svojim odprtokodnim operacijskim sistemom Android (Google Through the Years, 2016). Ti dve napravi sta bili ključni za razvoj trga mobilnih naprav in razvoj koncepta PSN v podjetjih v naslednjih letih (Laird, 2014). V poročilu Aberdeen Group (2011), enega izmed vodilnih svetovnih neodvisnih ponudnikov raziskav in analiz na področju informacijske tehnologije, je v letu 2011 že 75 odstotkov podjetij od 415 vprašanih dovoljevalo koncept PSN v svojih okoljih (Slika 1) in s tem že imelo izdelano strategijo do PSN.

Slika 1: Osebne mobilne naprave za poslovno uporabo; Ali je PSN dovoljen?



Vir: Aberdeen Group, Enterprise-Grade BYOD Strategies: Flexible, Compliant, Secure, 2011, str. 1.

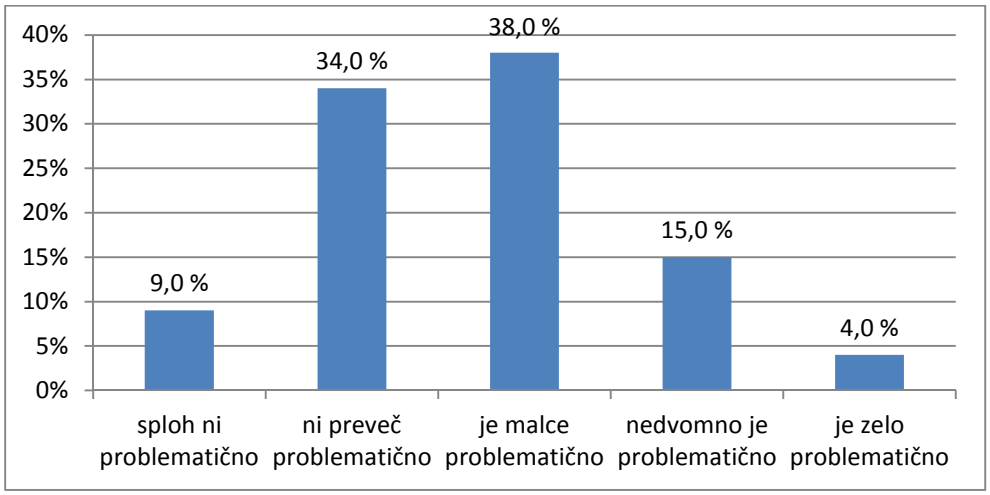
Uporaba lastnih mobilnih naprav v poslovnih okoljih je od takrat le še naraščala, s tem pa je bilo v prvi meri potrebno izboljšati povezljivost in dostopnost. Zaposleni se lahko z mobilnimi napravami povežejo z omrežjem podjetja kadarkoli in kjerkoli (preko WiFi – brezžičnih omrežij, 3G/4G omrežij) in tako dostopajo do vseh poslovnih virov podjetja.

Na Sliki 2 je prikazano tipično PSN okolje, kjer zaposleni uporabljajo osebne mobilne naprave tako za osebne namene, kot tudi za službene.

Slika 2: Tipično PSN okolje

Kot je omenjeno v raziskavi Osterman Research-a (2012) že v 82 odstotkih podjetij zaposleni uporabljajo svoje mobilne naprave za dostop do podatkov podjetij. 3 od 5 podjetij tudi verjame, da PSN predstavlja velik problem in da bo ta problem v naslednjih letih za podjetja postal še bolj resen (Slika 3).

Slika 3: Resnost problematičnosti PSN



Vir: Osterman Research, The need for IT to get in front of the BYOD problem, 2012, str. 1.

Zrela podjetja so že zdavnaj spoznala, da se je s prihodom PSN vloga njihovega IT oddelka zelo spremenila in da večkrat ko rečejo svojim zaposlenim »NE«, manj učinkovita je njihova varnostna politika. Zaposleni bodo vedno našli način, kako se povezati z omrežjem podjetja, kljub temu ali je to dovoljeno ali ne (iPass, b.l.).

1.2 Izzivi in priložnosti

Glavni izziv, s katerim se sooča podjetje pri sprejetju PSN politike in samega koncepta, so pomanjkanje smernic o PSN uporabi, neustrezna varnost podatkov, kot tudi neustrezna zaupnost informacij, do katerih lahko pridemo s PSN (Mwenemeru, 2013).

Podjetja se soočajo s pomembnimi izzivi, ki so bistvenega pomena za oceno prednosti in slabosti PSN. Te izzive lahko temeljito preverimo in potrdimo s pomočjo jasnih usmeritev in poslovnih procesov, kot je opisano spodaj (Chellakari, b.l.):

- **varnost**: razviti ustrezno politiko in postopke za zaposlene, razviti podporo informacijski tehnologiji o sprejemljivi uporabi te politike in poročanja o pomembnih dogodkih;
- **lastništvo nad napravami**: razviti obrazec, nekakšno soglasje za zaposlene o dogovoru in upoštevanju pravil za dostopanje do poslovnih sistemov in podatkov;
- **upravljanje naprav**: upravljanje naprav z orodjem za centralizirano upravljanje mobilnih naprav ter uveljavitev varnostnih mehanizmov kot so gesla, kriptiranje podatkov, omejitev aplikacij;
- **segmentacija podatkov**: ločeni osebni podatki od poslovnih podatkov na mobilnih napravah;
- **podpora informacijski tehnologiji**: potrebno je dodatno usposabljanje za podporo večjemu številu raznovrstnih osebnih mobilnih naprav z raznovrstnimi operacijskimi sistemi, večje število klicev v klicni center podpore;
- **sporazum**: razviti PSN politiko v podjetju, uvesti postopke in podporo prek usposabljanja za ozaveščanje o varnosti in grožnjah za končne uporabnike;
- **naročnine in deljeni stroški**: spremljanje stroškov porabe posameznika in pomanjkanje nadzora nad temi stroški, ugotovitev kateri stroški nastanejo v službene namene in kateri v osebne namene.

Wang et al. (2014) identificirajo tri izzive, ki so od vseh najbolj pomembni:

- **Uhajanje podatkov**: upoštevati je potrebno vse možne nevarnosti, ki vplivajo na mobilne naprave, s katerimi zaposleni dostopajo do podatkov in virov podjetja, potrebno je zavarovati podatke z uvedbo ali razvojem orodij za zavarovanje poslovnih podatkov, ki so shranjeni na mobilni napravi.
- **Nepooblaščena delitev prostorov**: v PSN okoljih lahko definiramo dva prostora, eden je osebni, drugi je poslovni. Osebni prostor vključuje vse aplikacije in podatke (fotografije, osebni stiki, igre za prosti čas), ki so v lasti zaposlenega. Prostor, ki je v lasti podjetja, pa vsebuje vse aplikacije in podatke, ki jih zaposleni potrebuje za delo v podjetju (elektronska pošta, stiki podjetja in njihovih strank, urejevalnih besedil in preglednic). Za podjetja je ohranitev teh dveh prostorov, izoliranih drug od drugega,

velik izziv. Zagotoviti je potrebno mehanizme za preprečevanje dostopa v posamezen prostor.

- **Pomanjkanje varnostne ustreznosti**: za podjetja je težko uveljavljati svojo varnostno politiko, ko je mobilna naprava v lasti zaposlenega. Na primer, če politika podjetja določa, da mora vsaka mobilna naprava imeti protivirusno zaščito, mora vse naprave, ki dostopajo do njenega omrežja, preveriti ali so v skladu s to zahtevo. Testiranje vsake naprave pa ne pride v poštev, ker je zamudno in ne rešuje problema.

Miller et al. (2012) zgornjim trem izzivom dodajajo **zasebnost zaposlenih**. S strani zaposlenih vedno obstaja skrb povezana z zasebnostjo, da lahko podjetja spremljajo njihove osebne dejavnosti in analizirajo njihove osebne podatke. Posledica vodi v nelagodje uporabe PSN naprav, kar pa negativno vpliva na učinkovitost in produktivnost ter zadovoljstvo zaposlenih, kar pa ni namen politike PSN.

Intel (2012) je v svoji raziskavi vprašal 4.300 podjetij in posameznikov »Katere so glavne prednosti vašega podjetja pri uvedbi PSN politike?« in ugotovil, da PSN koncept prinaša:

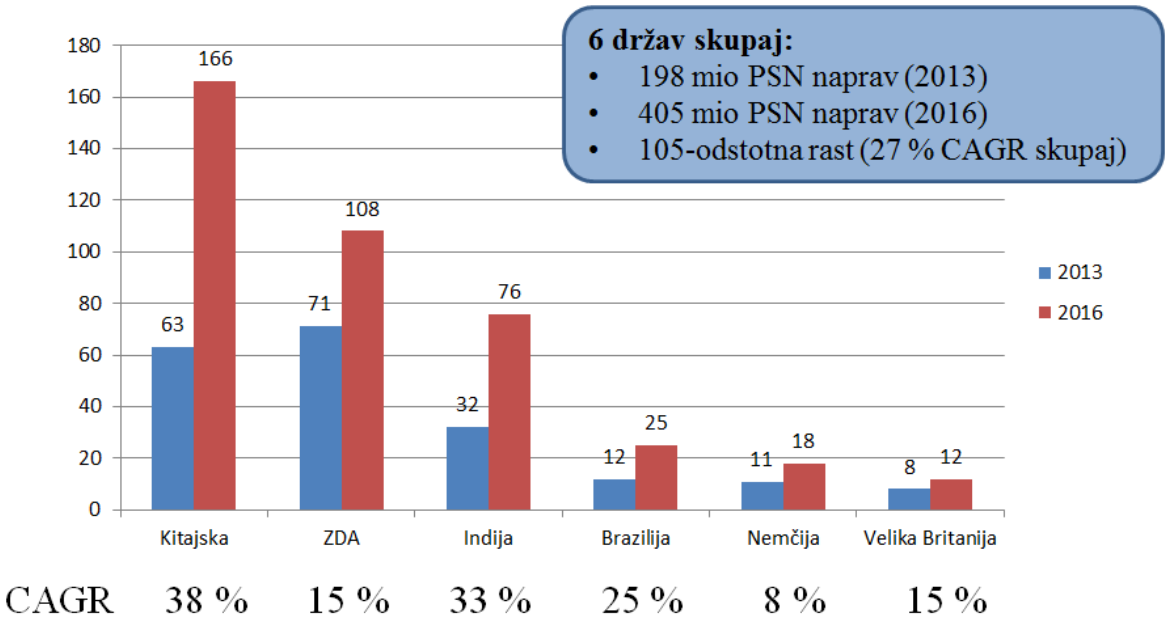
- 28-odstotno izboljšano učinkovitost in produktivnost;
- 22-odstotno izboljšano mobilnost zaposlenega;
- 17-odstotni prihranek pri nakupu novih naprav;
- 9-odstotno izboljšano zadovoljstvo in udobnost;
- 6-odstotno zmanjšanje stroškov podpore informacijske tehnologije.

PSN koncept je torej prinesel novo idejo poslovanja. Omogočil je zaposlenim večjo produktivnost in mobilnost, tako da so poslovni viri podjetja**,** katere potrebujejo za delo, ves čas na voljo. Zaposleni so bolj zadovoljni, učinkoviti, uporabljajo naprave, ki jih poznajo, z njimi se počutijo bolj udobno, z njimi ravnajo tudi bolj pazljivo, kar podjetju posledično znižuje stroške samega vzdrževanja naprav. S PSN poslovanje poteka praktično brez uporabe papirja, s stališča prodaje pa je pomemben tudi hiter odziv na kupce (Mwenemeru, 2013).

Ker imajo zaposleni na mobilnih napravah, poleg podatkov podjetja, tudi osebne podatke, v večini primerov z njimi ravnajo bolj previdno in še bolj poskrbijo za njihovo varnost pred grožnjami iz omrežja. Zavest zaposlenih o varovanju podatkov se s tem povečuje. S PSN konceptom se število nakupov mobilnih naprav s strani podjetij zmanjšuje, kar nakazuje tudi Microsoftova raziskava (Rains, 2013) iz leta 2013, 31 odstotkov podjetij od 2.234 vprašanih ne subvencionira zaposlenih pri nakupu mobilnih naprav, kar je 2 odstotka manj kot leto poprej (Jones, 2012). Posledično je zaradi tega tudi število naročnin manjše, kar še dodatno znižuje stroške podjetja in povečuje prihranek. Nadalje, raziskava ugotavlja tudi prednosti PSN s stališča uporabnikov. Več kot 40 odstotkov jih meni, da je uporaba lastnih mobilnih naprav na delu zelo pomembna. Cisco (Loucks et al., 2013) z raziskavo iz šestih držav

ugotavlja, da bo leta 2016 število PSN naprav doseglo skoraj 405 mio, kar je 27-odstotna stopnja rasti od leta 2013 (Slika 4).

Slika 4: Ocena števila PSN naprav na delovnem mestu po državah



Vir: J. Loucks et al., The financial impact of BYOD, 2013, str. 4.

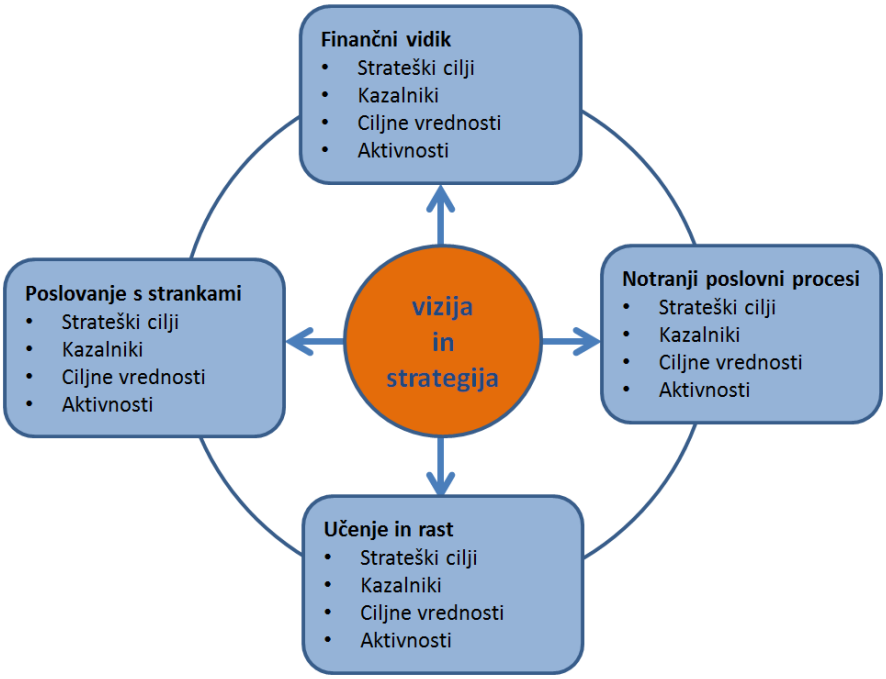
PSN je tu v porastu in prinaša podjetjem veliko novih izzivov. Vedno več podjetij se srečuje s tem novim izzivom, zato morajo sprejeti strategijo in se opredeliti do politike PSN (NIST, 2013). Za upravičenost PSN je za podjetja potrebna jasna slika uspešnosti PSN koncepta, tako kot za vsako drugo tehnologijo. Upoštevati je potrebno veliko dejavnikov, med njimi stroške, ki jih je potrebno preučiti, tudi skrite stroške, stroške za dodatno usposabljanje, strošek podpore informacijske tehnologije, stroške, ki nastanejo ob nedelovanju sistema, itd. Ko je slika uspešnosti jasna, mora podjetje razviti svoj nabor smernic, ki bodo urejale upravljanje in varovanje mobilnih naprav. To vključuje uporabo MDM, implementacije v oblaku, virtualne rešitve, itd.

1.3 Merjenje uspešnosti PSN

V zadnjih desetletjih je pri poslovanju podjetij zaslediti nov vzorec obnašanja, namreč poudarjanje nujnosti povezovanja informatike s poslovanjem podjetja in to ne le na mikronivoju, temveč tudi na višji ravni, z vključevanjem managementa. Ti trendi odnosov so vsekakor pozitivni, saj naj bi managementu omogočili boljše razumevanje strateške vloge informatike, po drugi strani pa naj bi tudi informatikom postalo jasno, da informatika ni sama sebi namen, ter da je potrebno o naložbah temeljito razmisliti in jih tudi upravičiti (Turk, 2005).

Ne glede na velikost podjetja je pomembno, da se natančno izmeri PSN vpliv na uspešnost podjetja. Pri merjenju uspešnosti gre za proces presoje napredka v smeri doseganja vnaprej določenih ciljev, vključno z informacijami o učinkovitosti, s katerimi se sredstva pretvorijo v blago in storitve (izložki), v smeri kakovosti teh izložkov (kako dobro so dostavljene strankam in v kolikšni meri so zadovoljni odjemalci), v smeri rezultatov (rezultati dejavnosti programa v primerjavi z njegovim namenom) ter v smeri učinkovitosti operacij glede na njihove posebne prispevke k programskim ciljem. Namen merjenja uspešnosti podjetja je vsekakor ključni dejavnik pri uresničevanju poslanstva, vizije in strategije podjetja. V primeru, da ni dosežen, bi verjetno povzročil znatno zmanjšanje zadovoljstva strank, zmanjšanje učinkovitosti sistema, zadovoljstva zaposlenih in učinkovitega finančnega upravljanja. Samo upravljanje uspešnosti je proces, ki vpliva na pozitivne spremembe v organizacijski kulturi, sistemov in procesov, s pomočjo nastavitev dogovorjenih ciljev uspešnosti, dodeljevanja in prednostnega obravnavanja virov, obveščanja upravljavcev o potrditvi ali spremembi trenutne politike ali o usmeritvi programa za dosego ciljev ter izmenjave rezultatov uspešnosti pri doseganju teh ciljev. Uporaba PSN mora biti usklajena s strategijo podjetja in mora dokazati, da bo pomagala doseči zastavljene cilje (Keyes, 2013).

Slika 5: Uravnoteženi kazalnik s svojimi štirimi pogledi



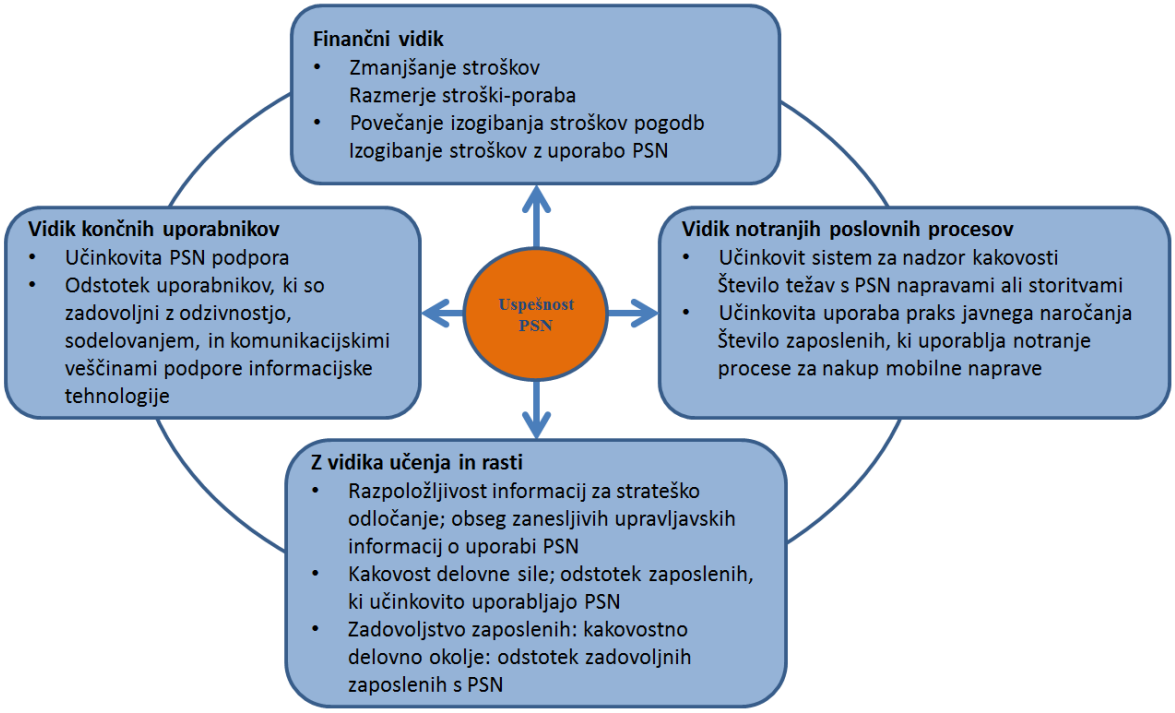
Vir: R. S. Kaplan, Conceptual Foundations of the Balanced Scorecard, 2010, str. 4.

Podjetje z uravnoteženim kazalnikom svoje poslovne cilje priredi v vseh štirih pogledih, s financami, kupci, notranjimi procesi ter učenjem oziroma z rastjo. Nato določi vzroke in posledice med temi povezavami, npr. zadovoljni kupci kupujejo več blaga, kar povečuje

prihodke podjetja. Podjetje nato izpostavi cilje, našteje ukrepe posameznega cilja, identificira projekte in druge pobude za pomoč pri doseganju teh ciljev. Ta pristop je več kot le način za identifikacijo in spremljanje meritev. Je tudi način za upravljanje sprememb in povečanje učinkovitosti, produktivnosti in konkurenčne prednosti podjetja. Podjetje, ki uporablja uravnotežene kazalnike za identifikacijo strateških ciljev in posledično uresničitev le-teh, je strateško usmerjena organizacija (Keyes, 2013).

Za upravljavce informacijske tehnologije je uravnotežen kazalnik neprecenljivo orodje, ki mu dovoljuje povezavo s poslovno stranjo organizacije. Nekateri ga enačijo kot nov jezik, ki omogoča skupno povezovanje med oddelkom informacijske tehnologije in poslovnimi vodji, ter njihovo skupno razmišljanje o tem, kaj lahko skupaj naredimo za podporo uspešnosti poslovanja. Koristen stranski učinek uporabe uravnoteženih kazalnikov je možnost izračuna moči odnosov med različnimi gonilniki vrednosti po tem, ko so vsi ukrepi identificirani in znani. Primer: z razmerjem med PSN uporabo in stopnjami stroškov lahko sklepamo, da uporaba PSN ni dovolj prispevala k rezultatu, kot je bila izražena z drugimi npr. finančnimi meritvami uspešnosti (Keyes, 2013). Slika 6 kaže pristop z uravnoteženim kazalnikom k merjenju uporabe PSN.

Slika 6: Primer PSN uravnoteženega kazalnika



Vir: J. Keyes, Bring your own devices (BYOD) survival guide, 2013, str. 61.

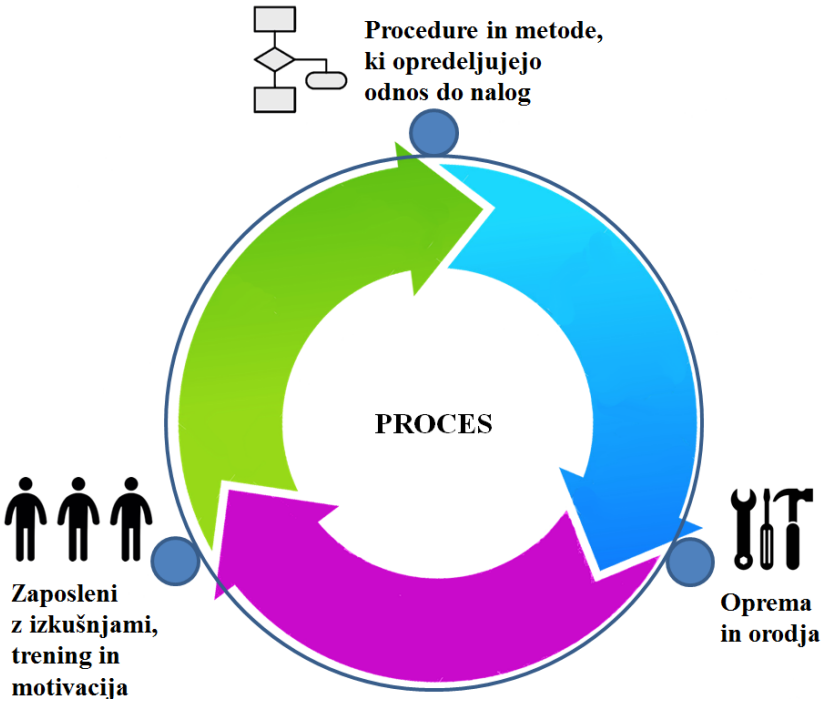
Na koncu merjenja uspešnosti PSN sta zelo pomembna procesa validacije in verifikacije.

Validacija oziroma vrednotenje je proces določanja stopnje natančnosti in zaključenosti merilnih tehnik in posledičnih podatkov. Ocenjevanje prakse in rezultatov je potrebno redno vrednotiti. Uspeh samoocenjevanja je odvisen predvsem od obojestranskih dogovorjenih in razumljenih ciljev uspešnosti, ukrepov in pričakovanj, prav tako tudi od obsega, globine, učinkovitosti in integritete samoocenjevanja (Keyes, 2013).

Verifikacija je postopek utemeljitve niza dobljenih podatkov, kot je preverjanje navedenih dejstev, citatov, meritev ali spremljajočih okoliščin. Preverjanje podatkov, ki npr. izhajajo iz samoocenjevanja in drugih dejavnosti operativnega ozaveščanja, bodo delno oblikovali podlago za odobritev poslovnega sistema. Podatke je potrebno analizirati z namenom določitve njihove natančnosti in primerjave, ter preveriti ali merila uspešnosti veljajo (Keyes, 2013).

Če podjetja ne izvajajo meritev, ne bodo nikoli izvedela, kako uspešen je njihov PSN program.

Slika 7: Tri kritične dimenzije izboljšanja poslovanja podjetij



Vir: SEICMU, Improving processes for providing better services, 2010, str. 4.

1.4 Vključitev PSN koncepta v podjetje

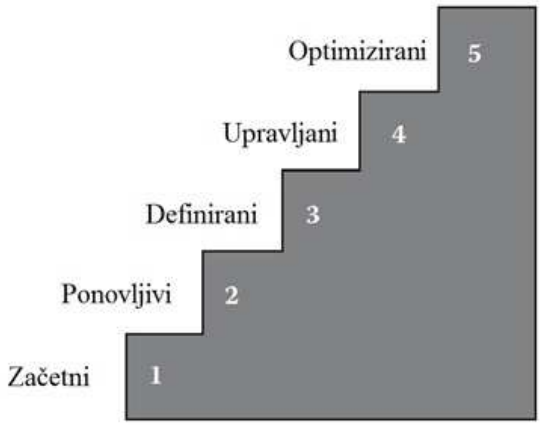
V nadaljevanju bomo govorili o tem, kako vključiti PSN koncept v podjetje. Dostop za vse ali ad-hoc pristop je recept za katastrofo in predstavlja veliko tveganje za podjetje. Podjetja

morajo izvesti podrobnejši pregled ocene tveganj in njihovo ublažitev v PSN okolju. Software Engineering Institute of Carnegie Mellon University, v nadaljevanju SEICMU (2010), našteje tri kritične dimenzije, v katere se običajno podjetja usmerjajo z namenom izboljšanja poslovanja: ljudje, postopki in metode ter orodja in oprema (Slika 7). Vsi skupaj tvorijo proces, ki omogoča usklajen način poslovanja, kako vključiti znanje in kako narediti stvari bolje. Le zrela podjetja so sposobna notranje uskladitve za dosego ciljev poslovnega procesa podjetja.

1.4.1 CMM model

Za zgoraj omenjen namen so na SEICMU razvili t.i. zmožnostno-zrelostni model (angl. *Capability Maturity Model*, v nadaljevanju CMM). Podjetjem, ki uporabljajo CMM, pomaga ugotoviti in povečati stopnjo zrelosti razvoja programske opreme, storitev in procesov.

Slika 8: Skrajšani petstopenjski CMM model zrelosti



Vir: SEICMU, Capability Maturity Model for Software, Version 1.1, 1993, str. 8.

Model, kot je prikazan na Sliki 8, je skrajšani petstopenjski CMM model zrelosti, skozi katere mora iti vsak IT oddelek podjetja, da postane popolnoma optimiziran in produktiven (SEICMU, 1993):

- Na **začetnem** nivoju (1. stopnja) je proces ustvarjanja in uporabe programske opreme označen in se izvaja kot ad-hoc. Podjetje ne zagotavlja stabilnega okolja za podporo procesom. Definirano je le nekaj procesov, uspeh pa je odvisen od prizadevanj posameznika.
- Na **ponovljivem** nivoju (2. stopnja) so osnovni procesi projektnega vodenja vzpostavljeni za spremljanje stroškov, načrtov in same uporabnosti. Z disciplino se lahko ponovi uspeh prejšnjih projektov s podobnimi aplikacijami. Za to stopnjo je značilno doseganje stabilnega procesa, s ponovljivo stopnjo statistične kontrole.

- Na **definiranem** nivoju (3. stopnja) so procesi upravljanja in tehničnega projektiranja dokumentirani, standardizirani in vključeni v proces izdelave za podjetje. Vsi projekti uporabljajo odobreno in prilagojeno različico programske opreme.
- Za **upravljani** nivo (4. stopnja) je značilno natančno merjenje kakovosti, vidne so bistvene izboljšave v kakovosti, procesi so kvantitativno sprejeti in nadzorovani.
- Za **optimizirani** nivo (5. stopnja) je značilno, da v podjetju neprestano izboljšujejo procese, kar je omogočeno s povratno informacijo o procesu in poskusnim izvajanjem inovativnih idej ter tehnologij. Cilji kvalitete in izvajanja procesov so vzpostavljeni, redno nadzorovani in so uporabljeni kot kriterij pri upravljanju procesa izboljšav.

Večina podjetij se giblje med 2. in 4. stopnjo, čeprav naj bi si vsa prizadevala doseči 5. stopnjo. Za uspešno integracijo koncepta PSN v podjetja je potreben napor v smeri izboljšanja kakovosti, nadzorovanih procesov in natančnih meritev. Z vidika informacijske tehnologije to pomeni spreminjanje standardnih postopkov, ki vodijo v sprejem koncepta PSN v podjetjih (Keyes, 2013). Ti postopki vključujejo upravljanje virov, ki vsebujejo orodje za centralizirano upravljanje mobilnih naprav, upravljanje vsebine, upravljanje konfiguracije in upravljanje zmogljivosti. Vse te postopke bomo srečali v nadaljevanju.

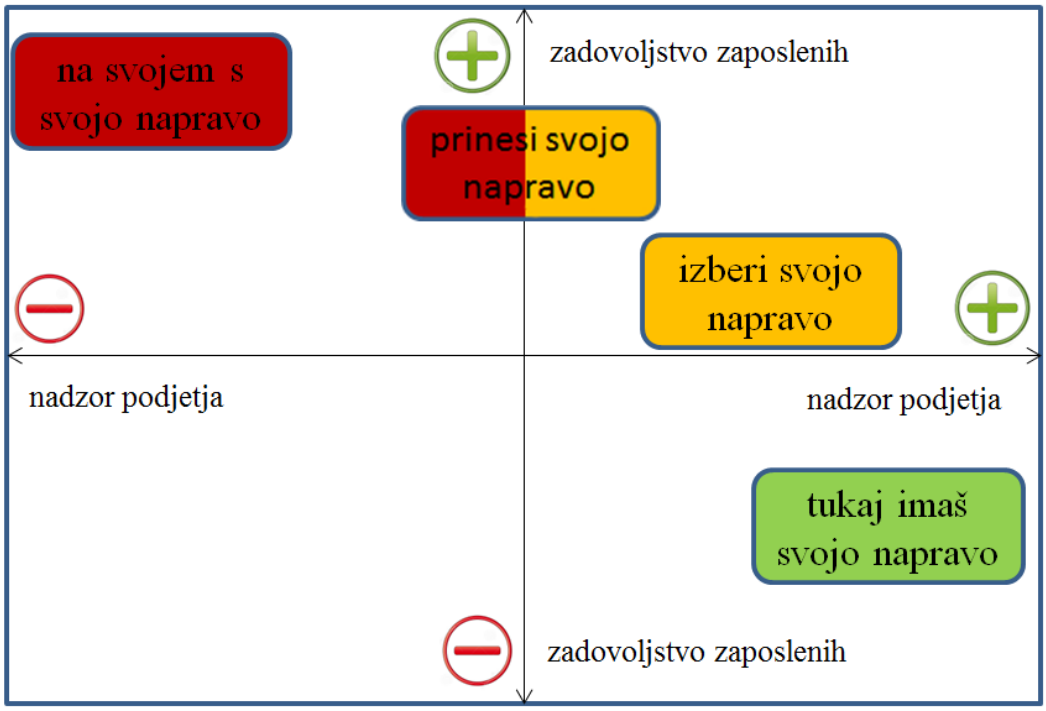
1.4.2 PSN koncept

Kljub temu, da se koncept PSN širi, je za podjetja zelo pomembno, da glede na njihovo specifiko poslovanja izberejo pravo strategijo in ugotovijo, ali je PSN koncept za njih sploh sprejemljiv. Kot pomoč za lažjo opredelitev varnostne strategije za izvajanje PSN koncepta, lahko podjetja uporabljajo naslednji okvir oz. nabor gradnikov. Ti koncepti so opisani v nadaljevanju (Prashant et al., 2013):

- **tukaj imaš svojo napravo** (angl. *Here is Your Own Device – HYOD*). Pri tem konceptu zaposlenim mobilno napravo zagotovi podjetje. Nad napravo ima popoln nadzor, pomoč uporabnikom je zagotovljena v celoti, od montaže do konfiguracije in nastavitev. Pravila so zelo stroga, uporabniki ne smejo oziroma ne morejo nameščati aplikacij;
- **izberi svojo napravo** (angl. *Choose Your Own Device – CYOD*). Pri tem konceptu podjetje zagotovi določeno število sprejemljivih mobilnih naprav za njihovo okolje, izmed katerih se zaposleni lahko odločajo. Pravila niso tako stroga kot pri prejšnjemu konceptu, pomoč uporabnikom za te naprave je zagotovljena v celoti, uporabnik ima celo pooblastila za namestitev določenih aplikacij in programske opreme;
- **prinesi svojo napravo**. Pri konceptu PSN zaposleni kupi svojo napravo ali pa mu jo v celoti ali delno kupi podjetje, v primeru strategije subvencije. Pravila pri tem konceptu so zelo ohlapna, podjetje ima manj nadzora nad napravo. Uporabnik lahko namešča katerokoli aplikacijo, le če je v skladu z varnostno politiko podjetja. Pomoč uporabnikom je delno zagotovljena;

- **na svojem s svojo napravo** (angl. *On Your Own Device – OYOD*). Pri tem konceptu lahko zaposleni v okolje podjetja prinese katerokoli napravo. Uporabnik je odgovoren za upravljanje svoje naprave. Pravil, ki bi jih bilo potrebno upoštevati ni, prav tako ni pomoči uporabnikom.

Slika 9: PSN koncepti



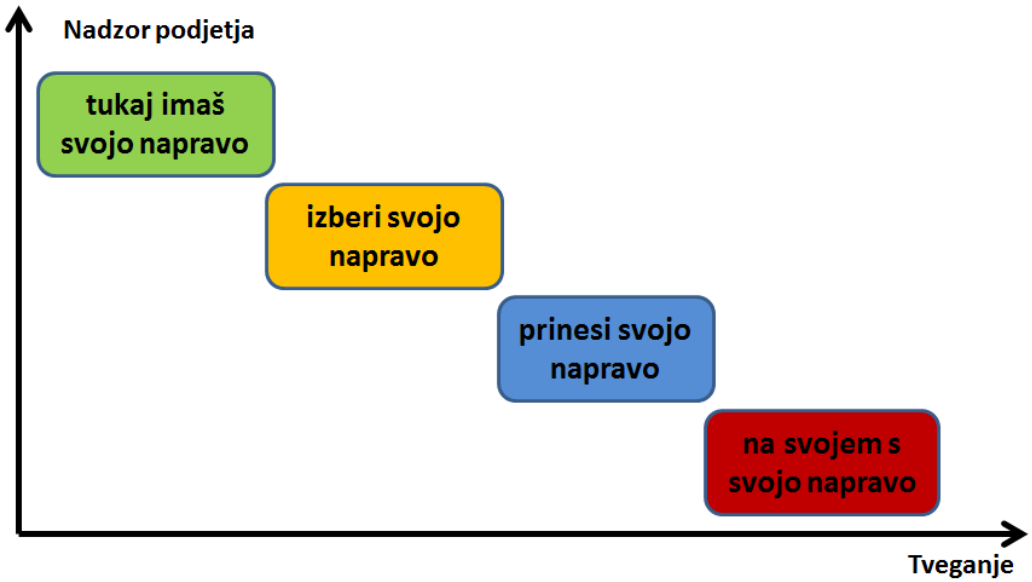
Vir: K. G. Prashant et al., Bring your own device (BYOD): Security risks and mitigating strategies, 2013, str. 64.

Na Sliki 9 so prikazani zgoraj opisani koncepti na relaciji nadzora podjetij v primerjavi z zadovoljstvom zaposlenih. Ugotovitve kažejo, da je koncept »tukaj imaš svojo napravo« zelo primeren za podjetja, ker omogoča popoln nadzor, vendar pa se s tem zelo zmanjša zadovoljstvo zaposlenih. Podobno se odraža tudi pri konceptu »na svojem s svojo napravo«, kjer je zadovoljstvo zaposlenih največje, vendar pa je nadzor podjetij zelo majhen.

Pri izbiri je potrebno upoštevati tudi tveganja, ki jih prinašajo različni koncepti. To je razvidno na Sliki 10, kjer so prikazani omenjeni koncepti v razmerju nadzora podjetij nad mobilnimi napravami v odvisnosti od tveganj.

Najboljši kompromis med zaposlenimi in podjetjem je v konceptu PSN, s katerim je doseženo najboljše razmerje med zadovoljstvom zaposlenih, nadzorom podjetij in tveganji.

Slika 10: PSN koncepti v razmerju nadzora v odvisnosti od tveganj



Vir: K. G. Prashant et al., Bring your own device (BYOD): Security risks and mitigating strategies 2013, str. 65.

1.5 Priprava strategije in modela PSN

Pri pripravi strategije PSN je potrebno (Gilmore & Beardmore, 2013):

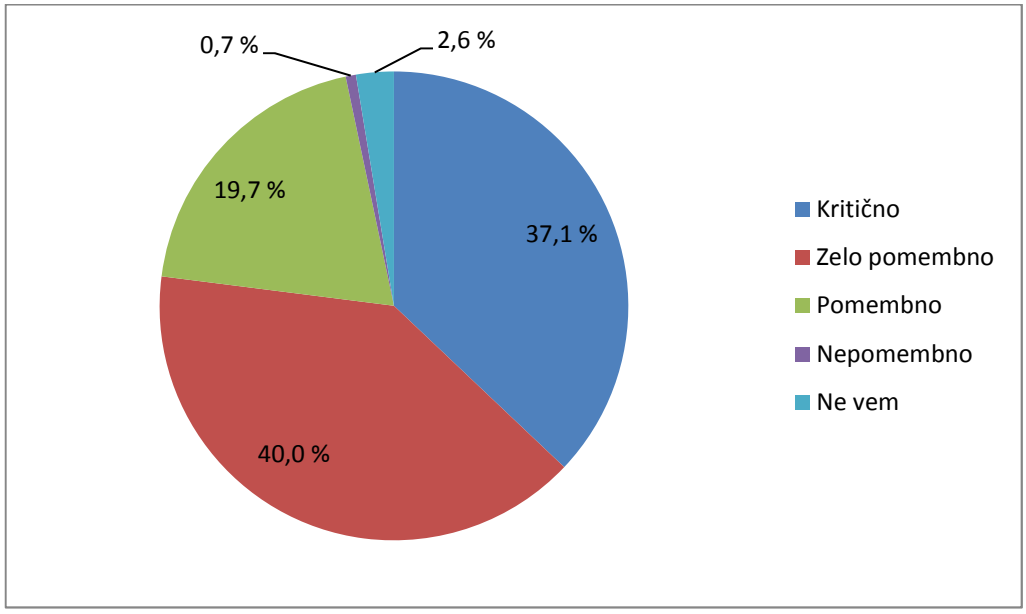
- opredeliti do katerih aplikacij in do katerih podatkov podjetja lahko dostopajo zaposleni iz oddaljenih dostopov oziroma ko so na terenu;
- zagotoviti skladnost oziroma ustreznost s pravnega vidika;
- zagotoviti pomoč pri razvoju novih postopkov usposabljanj za zaposlene;
- pripraviti spremembe oziroma anekse k pogodbi o zaposlitvi;
- zagotoviti varnost informacijskega sistema in same tehnologije. Opravka imamo z različnimi tehnologijami, zaposleni uporabljajo veliko različnih vrst mobilnih naprav, ki imajo različne operacijske sisteme. Ti operacijski sistemi pa imajo veliko število različic programske opreme. To znanje je ključnega pomena pri uvedbi novega koncepta v okolje podjetja.

V pripravo strategije PSN okolja mora biti vključen vsaj en predstavnik iz vseh pomembnejših interesnih skupin v podjetju, in sicer od pravne, kadrovske službe, službe za informacijsko tehnologijo do vodstvenih delavcev na različnih nivojih (Gilmore & Beardmore, 2013).

Vsaka interesna skupina ima drugačen pogled. Z združitvijo različnih pogledov bo pripravljena strategija bolj učinkovita. Pri pripravi PSN strategije oziroma varnostne

politike za mobilne uporabnike je za podjetje pomembna predvsem varnost informacijskega sistema in varnost podatkov, ki jih poseduje. Nedavna raziskava SANS inštituta (Johnson & DeLaGrange, 2012) ugotavlja, kako nujna je za podjetja PSN politika. O kritičnosti varnostne politike 96,7 odstotka podjetij meni, da je PSN politika pomembna, od tega jih 37 odstotkov meni, da je ključnega pomena (Slika 11).

Slika 11: Pomembnost politike mobilne varnosti za podjetja (v %)



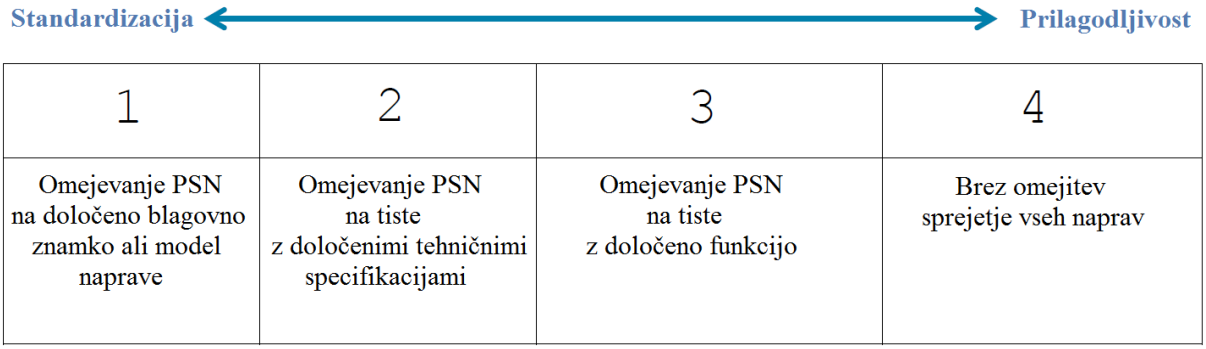
Vir: K. Johnson & T. DeLaGrange, SANS survey on mobility/BYOD security policies and practices, 2012, str. 4.

Po navedbah ustanove Alberta Education (2012) obstaja več vrst modelov PSN, ki se razlikujejo med seboj. Na Sliki 12 je prikazan integrirani model, ki temelji na širokem spektru sprejemljivih mobilnih naprav, v razponu od visoke standardizacije do visoke prilagodljivosti in združuje štiri vidike (Alberta Education, 2012):

- omejevanje naprav v osebni lasti na določeno blagovno znamko ali model naprave;
- omejevanje naprav v osebni lasti na tiste, ki izpolnjujejo določene tehnične specifikacije:
  - določeni operacijski sistem,
  - določene različice operacijskih sistemov,
  - zahteve glede minimalnega pomnilnika;
- omejevanje naprav v osebni lasti na tiste z določeno funkcijo:
  - združljivost s programsko opremo,
  - združljivost z zahtevami spletnega testiranja;
- sprejetje vseh naprav v osebni lasti.

Obstaja še peti vidik, ki pa je hibridni model in združuje kombinacijo vseh zgoraj naštetih vidikov.

Slika 12: Integrirani PSN model v štirih vidikih



Vir: Alberta Education, Bring your own device: A guide for schools, 2012, str. 11.

Za uspešno sprejetje PSN koncepta, mora podjetje identificirati vse posamezne komponente PSN. Komponente, ki sestavljajo PSN model (Slika 13) in jih je potrebno upoštevati pri učinkovitem povezovanju koncepta PSN z infrastrukturo podjetja, so navedene v nadaljevanju (Mwenemeru, 2013).

Komponenta **zasebnost uporabnika** se dotika različnih vprašanj v zvezi z varnostjo podatkov, ki so lahko v napravah zaposlenih ali pa v sami infrastrukturi podjetja. Predvsem opredeljuje aktivnosti in podatke, ki jih bo spremljal oddelek informacijske tehnologije, natančneje opredeli ukrepe, ki jih bo izvedel oddelek informacijske tehnologije, okoliščine ter politiko zasebnosti PSN. Poleg tega tudi obravnava varnostno politiko.

Komponenta **izbira naprave** je sestavljena iz različnih elementov kot so; analiziranje preferenc zaposlenih, razumevanje odločitev že kupljenih naprav, razumevanje operacijskega sistema in strojne opreme, razvoj načrta za prihodnje certificiranje, vzpostavitev jasne komunikacije z zaposlenimi in jasna opredelitev, katere naprave so dovoljene in katere ne.

Z vidika **cenovne dostopnosti** so upoštevani naslednji parametri; preusmeritev stroškov strojne opreme oziroma mobilne naprave na zaposlenega, uveljavitev subvencioniranega modela, nadzor mesečnih stroškov z bolj odgovorno uporabo, vzpostavitev in izbira ustreznih paketov storitev.

Sestavni deli komponente **odgovornosti** so; opredelitev vseh elementov zaščite podatkov podjetja na PSN napravah zaposlenih, presoja odgovornosti uporabe spleta in aplikacije za

osebno rabo, presoja odgovornosti dela v podjetju in zunaj njega, presoja odgovornosti dela znotraj delovnega časa in izven.

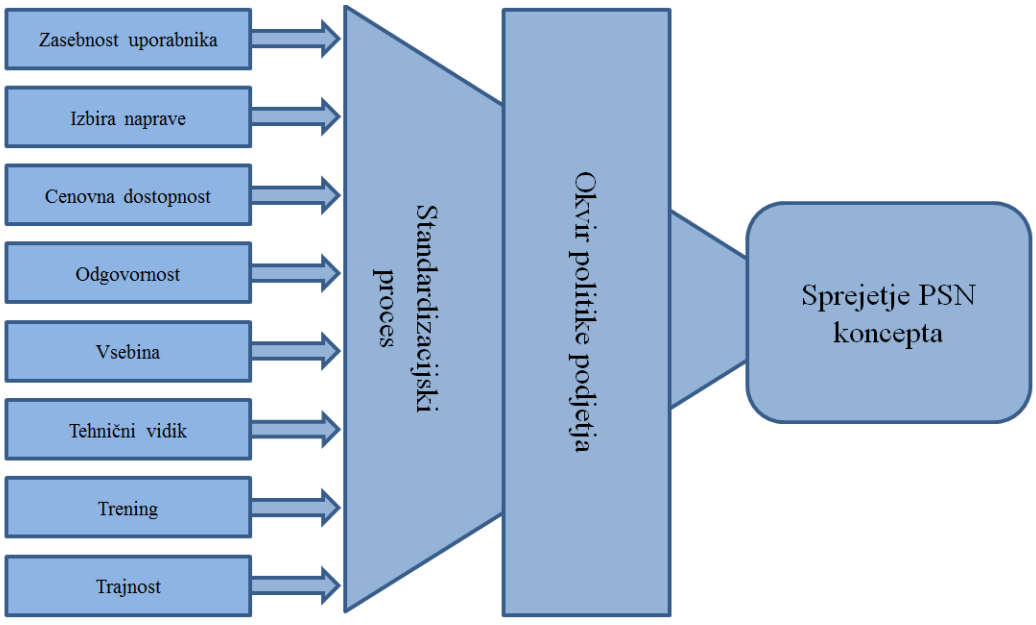
Komponenta **vsebina** je lahko prepoznana preko različnih sklopov aplikacij kot sta zaščita pred virusi ali poštni odjemalec, torej aplikacij in opcijsko tudi licenc, ki so na napravah in jih je potrebno plačati.

Tehnični vidik obravnava zmožnost in sestavo obstoječe infrastrukture vključno z brezžičnim omrežjem podjetja, da lahko sprejme toliko novih PSN uporabnikov, vključno z določili kaj, kdo in kako lahko dostopa do omrežja podjetja.

Trening je ključni element celotne pobude PSN, saj daje uporabnikom, vodstvu in oddelku informacijske tehnologije priložnost obravnave in učenja elementov varnosti in politike podjetja. Prav tako pa omogoča odprt dialog med zaposlenimi in upravljavci ter tako prispeva k uspehu koncepta.

Komponenta **trajnost** v PSN modelu obravnava področja zagotavljanja poslovnih podatkov, zmanjšanje stroškov samega izvajanja, ohranitev uporabniške izkušnje, ter kako ostati na tekočem s preferencami zaposlenih in tehnoloških inovacij.

Slika 13: Integracija PSN z okoljem podjetja



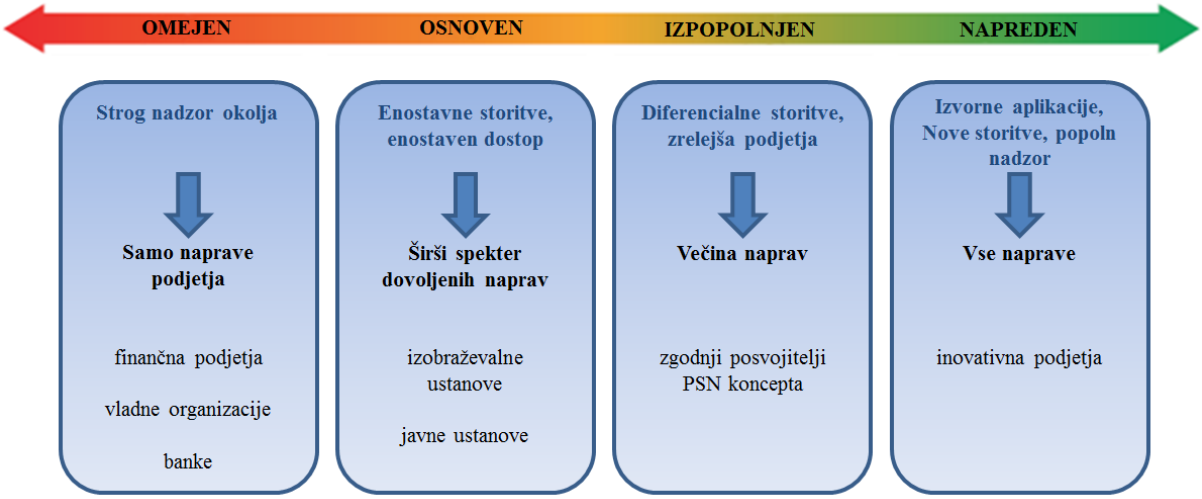
Vir: H. K. Mwenemeru, A model to guide in the adoption of bring your own device concept in an organization, 2013, str. 19.

Različni poslovni subjekti imajo do PSN različne pristope, različne poglede in pričakovanja. Vsako podjetje potrebuje strategijo PSN, tudi pri namenu omejevanja naprav v osebni lasti

na določeno blagovno znamko ali model naprave, ki jih odobri oddelek informacijske tehnologije. Podjetja iz sektorjev z visoko stopnjo regulacije, kot so finance ali vladne agencije, praviloma morajo sprejeti bolj restriktiven pristop do PSN, predvsem z namenom zaščite občutljivih podatkov. Naprave je potrebno pri takem pristopu zelo dobro nadzorovati in upravljati. Za ostala podjetja pa velja, da lahko izbirajo med širokim izborom pristopov, od najbolj restriktivnega dostopa do aplikacij podjetja do sprejetja PSN v celoti, kar pomeni, spodbujanje široke uporabe vseh vrst naprav. V vseh primerih pa je potrebno uvesti varnostne ukrepe pri dostopu do širokega nabora poslovnih aplikacij in podatkov podjetja. Možni scenariji sprejetja PSN (Slika 14), katera večina podjetij tudi sprejme, so po Ciscu (2012) naslednja:

- **Omejen** scenarij: okolje zahteva strog nadzor, dovoljene so le naprave v lasti podjetja, gre za okolja z občutljivimi podatki kot so banke, finančna podjetja, vladne organizacije.
- **Osnoven** scenarij: osredotočenost okolja le na osnovne storitve, z enostavnim dostopom, dovoljen je nabor naprav le z dostopom do spleta, gre za okolja kot so izobraževalne ustanove in javne ustanove.
- **Izpopolnjen** scenarij: osredotočenost na zrelejša okolja, ki omogočajo diferencialne storitve in imajo izdelano varnostno politiko dostopa do podatkov podjetja, tudi preko oddaljenega dostopa, gre za zgodnje posvojitelje PSN koncepta, zrelejša podjetja.
- **Napreden** scenarij: osredotočenost na okolja, kjer je omogočen popoln nadzor nad novimi storitvami, omogočen dostop do vseh aplikacij podjetja, dovoljena uporaba vseh mobilnih naprav, neodvisno od lastništva, gre za okolja kjer prevladujejo inovativna podjetja.

Slika 14: Možni scenariji sprejetja PSN

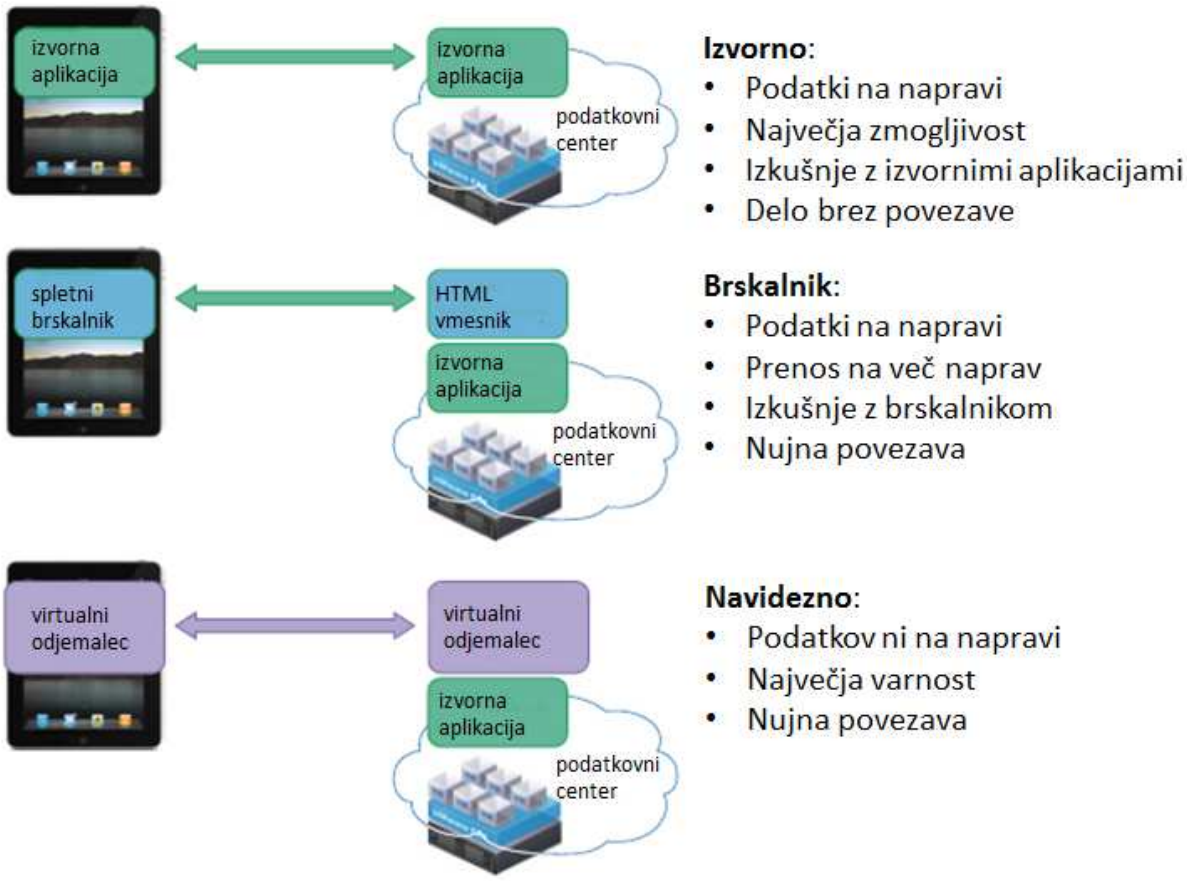


Vir: Cisco, Cisco Bring Your Own Device, Device Freedom Without Compromising the IT Network, 2012, str. 13.

1.5.1 Aplikacijski pristop

Zagotavljanje varnosti in preprečevanje izgube podatkov je glavna skrb pri uveljavljanju PSN politike. Pomembno je razumeti tri možne aplikacijske pristope: izvorne, spletne in navidezne. Vsi trije pristopi imajo dobre in slabe lastnosti. Pri odločanju je potrebno sklepati kompromise. Možne aplikacijske arhitekture so prikazane na Sliki 15.

Slika 15: Aplikacijske arhitekture PSN



Vir: Cisco, Cisco Bring Your Own Device, Device Freedom Without Compromising the IT Network, 2012, str. 14.

V **izvornem** načinu aplikacije, ki tečejo na mobilni napravi, neposredno komunicirajo z aplikacijskim strežnikom v podatkovnem centru ali oblaku. Podatki se lahko izmenjujejo in shranjujejo neposredno na PSN napravi. S stališča uporabniške izkušnje, poslovna aplikacija deluje podobno kot katera koli druga aplikacija na mobilni napravi. Zmogljivost in obnašanje mobilne naprave se s tem ne spremeni, produktivnost zaposlenih je ohranjena, s prilagojenimi aplikacijami je mogoče tudi izboljšati uporabniško izkušnjo.

Spletni pristop z brskalnikom je čedalje bolj sprejet za dostop do aplikacij zaradi lažje prenosljivosti med mobilnimi napravami in operacijskimi sistemi. V bistvu lahko z vsako napravo, ki ima naložen standardiziran HTML brskalnik, dostopamo do aplikacij. Podatki se izmenjujejo in shranjujejo neposredno na PSN napravi, kar je neke vrste varnostni izziv in vodi v zaskrbljenost glede morebitne izgube podatkov. Zaradi tega se lahko zmanjša uporabniška izkušnja.

V **virtualnem** pristopu aplikacije, ki so na aplikacijskem strežniku v podatkovnem centru ali oblaku, poganja virtualni odjemalec na mobilni napravi. Aplikacije več ne tečejo na mobilni napravi, podatki med aplikacijskim strežnikom in mobilno napravo se prenašajo le preko dotikov zaslona in slik podatkov. Ne shranjujejo se več neposredno na njej. V tem načinu je zagotovljena največja varnost glede morebitne izgube podatkov podjetja in varnosti osebnih podatkov s strani zaposlenih.

Za podjetje je zelo pomembno, kateri model aplikacijskih pristopov izbrati za infrastrukturo, izvorni ali virtualni. Mnoga podjetja se odločijo za hibridni model med njima, za dostop do izvornih aplikacij uporabljajo izvorni način, za uporabo aplikacij z zaupnimi in občutljivimi podatki pa virtualni način.

1.5.2 PSN arhitektura

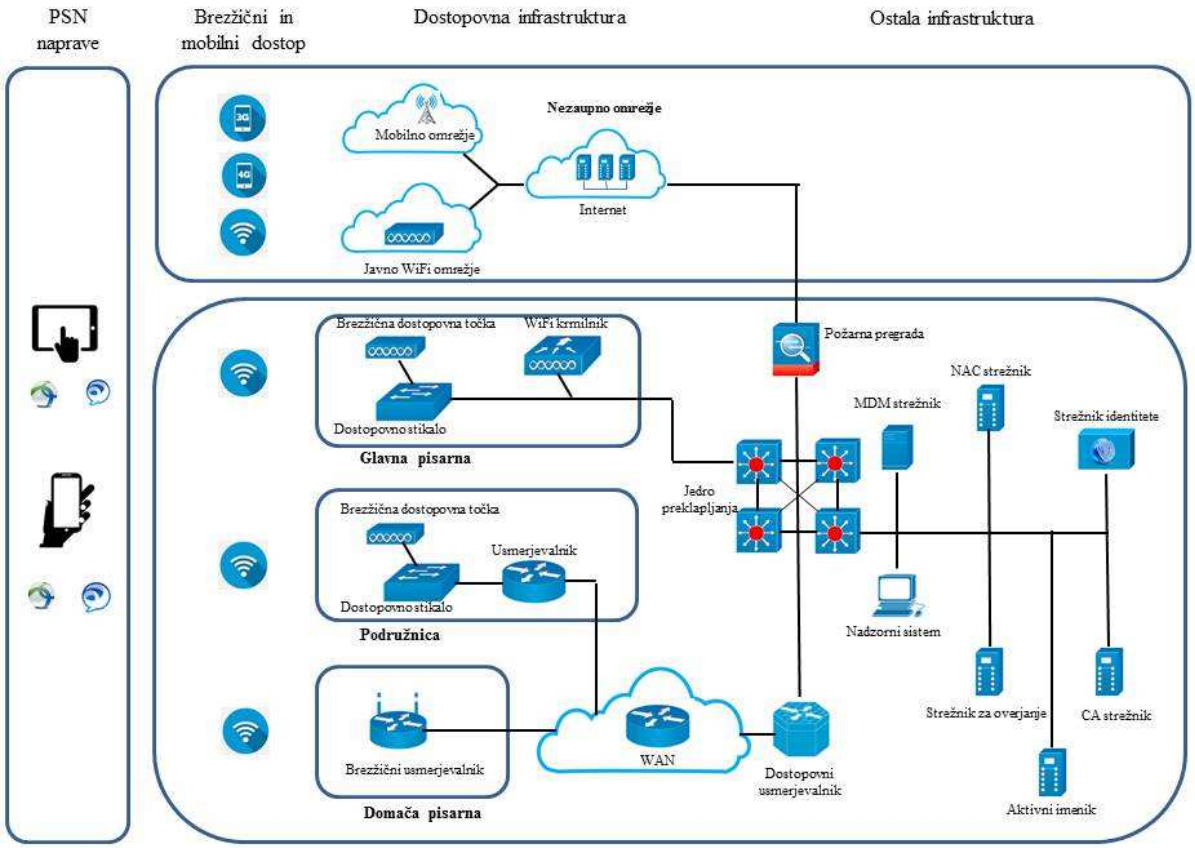
Razumeti moramo, da PSN ni samo izdelek, ki ga lahko samo vključimo v neko infrastrukturo podjetja. Za PSN rešitev je potrebna inteligentna arhitektura, ki bo zagotovila celovito rešitev za PSN arhitekturo. Združevati mora elemente celotnega omrežja podjetja, ki bodo z enotnim pristopom omogočali napravam varen dostop do podjetja, samo prepoznavnost naprav in nadzor nad varnostno politiko podjetja.

Celovita rešitev mora zagotoviti varen dostop do podjetja preko brezžičnih WiFi zasebnih in javnih omrežij, kot tudi javnih nezaupljivih mobilnih omrežij tretje in četrte generacije, podpirati mora številne znamke in modele mobilnih naprav, sposobna mora biti uveljaviti varnostne politike na različnih delih omrežja. Poleg tega mora podpirati tudi neprekinjeno preklapljanje med različnimi omrežji (WiFi, 3G/4G) medtem, ko se mobilni zaposleni premikajo iz enega dela omrežja v drugo, na primer iz WiFi omrežja podjetja na javno mobilno omrežje. Pri tem pa je zaposlenim potrebno zagotoviti še vedno varen dostop in neprekinjeno, nemoteno delo. Vsaka zasnova omrežja, ki ne upošteva različnih, možnih kontekstov dostopa, ne bo zagotovila obvladljivo, upravljano in prilagodljivo rešitev za podjetje.

Predlagani model inteligentnega omrežja podpira vse koncepte, modele, scenarije podpore in aplikacijske strategije PSN (Slika 16) in ga lahko povzamejo tako podjetja z visoko

stopnjo varovanja podatkov, kot tudi tista z manjšo stopnjo. V nadaljevanju so predstavljene posamezne komponente inteligentnega omrežja in njihova vloga pri podpori PSN.

Slika 16: PSN arhitektura



Vir: Povzeto in prirejeno po Cisco, Cisco Enterprise Mobility Solution, Device Freedom Without Compromising the IT Network, 2014c., str. 18.

Stikala omogočajo priključitev brezžičnih dostopovnih točk na eternet vrata, ki so napajana (angl. *Power Over Ethernet – PoE*). Poleg tega morajo podpirati in znati prenašati zahteve za overitev v omrežju z 802.1x protokolom (Wired 802.1x Security, 2016), ki ga je predpisalo svetovno združenje inženirjev elektronike in elektrotehnike (angl. *Institute of Electrical and Electronic Engineers – IEEE*) in je namenjen za zagotavljanje na ravni vrat, z zasnovanim avtoriziranim dostopom v omrežje.

Brezžične dostopovne točke (angl. *Wireless Access Points*) omogočajo brezžični dostop mobilnim napravam in njihovo povezljivost z omrežjem podjetja. Poleg tega morajo tudi brezžične dostopovne točke podpirati in znati prenašati protokol 802.1x (Cisco, 2012).

WiFi krmilniki omogočajo zaključevanje brezžičnih dostopovnih točk in zagotavljajo preglednost, upravljanje in nadzor nad brezžičnim lokalnim omrežjem. Krmilniki morajo biti sposobni sodelovati s strežnikom krmiljenja omrežnega dostopa (angl. *Network Access Control*, v nadaljevanju NAC), ki omogoča overjanje in avtorizacijo dostopa mobilnim napravam ter z ostalimi strežniki v arhitekturi PSN (strežniki za overjanje, izdajatelji digitalnih potrdil). Podpirati mora protokol za zaščito brezžičnega dostopa (angl. *WiFi Protected Access II – WPA2*), imeti zmožnost zaznavanja vdorov (angl. *Wireless Intrusion Detection System – WIDS*), odkrivati goljufive dostopovne točke, imeti možnost vzpostavitve varne zasebne povezave (angl. *Virtual Private Network*, v nadaljevanju VPN) in imeti na voljo funkcije spletnega filtriranja, antivirusne zaščite ter nadzor nad aplikacijami (Cisco, 2012; Fortinet, 2015a). Vse našteto mora veljati tudi za brezžične usmerjevalnike v domačem okolju.

Usmerjevalniki omogočajo povezljivost prostranega omrežja s podružnicami in domačimi pisarnami. V podružnicah omogočajo povezljivost brezžičnega lokalnega omrežja, neposredno povezljivost z medmrežjem in storitvami v oblaku, optimizacijo omrežja, lahko pa služijo mobilnim napravam kot priključna točka za zaključitev VPN tunelov. Pri nekaterih proizvajalcih omrežne opreme so ti usmerjevalniki lahko hkrati požarne pregrade in WiFi krmilniki (Fortinet, 2014).

Požarne pregrade naslednje generacije (angl. *Next Generation Firewall – NGFW*) omogočajo poleg tradicionalnih varnostnih funkcij na robu omrežja tudi funkcije sistema za preprečevanje vdorov (angl. *Intrusion Prevention System – IPS*), nadzor nad aplikacijami, filtriranje paketov, antivirusno zaščito, zaščito pred izgubo podatkov (angl. *Data Loss Protection*, v nadaljevanju DLP) zaščito pred nezaželeno elektronsko pošto, zaključitev VPN tunelov, prevajanje omrežnih naslovov (angl. *Network Address Translation – NAT*), nadzor nad varno lupino (angl. *Secure Shell – SSH*) in slojem varnih vtičnic (angl. *Secure Socket Layer*, v nadaljevanju SSL), podroben pregled paketov (angl. *Deep Packet Inspection – DPI*), zaznavanje škodljivih programov in funkcijo kakovost storitve (Fortinet, 2012; Cisco, 2015a; Skybakmoen, 2014).

NAC strežnik je bistvena komponenta omrežja za PSN koncept in vsebuje skupek protokolov, s katerimi se zagotavlja varen dostop do omrežnih končnih točk. Strežnik lahko nudi naslednje storitve (Cisco, 2012; Bradford Networks, 2012; ForeScout, 2015; PulseSecure, 2016; Orans, 2013):

- portal za vpis in registracija naprave z ene same lokacije;
- overjanje dostopa;
- avtorizacija dostopa;
- profiliranje naprav;
- vpis certifikata;

- definicija politike;
- vmesnik do trgovin(e) identitete (angl. *Identity Store*):
  – Microsoft Active Directory,
  – dostop do imenikov (angl. Lightweight Directory Access Protocol, v nadaljevanju LDAP),
  – RADIUS,
  – Kerberos;
- nadzor dostopa z določenimi dejanji za skladne in neskladne mobilne naprave (npr. blokirati, dovoliti delni ali polni dostop);
- sposobnost za presojo skladnosti politike (npr. ali imajo naprave nameščene zadnje popravke operacijskega sistema in ali imajo nameščenega MDM odjemalca);
- poročanje in uvrščanje na črno listo izgubljene in ukradene mobilne naprave.

Ko se zaposleni preko PSN naprave prvič poveže z omrežjem, je zelo pomembno, da ga NAC strežnik preusmeri na portal za vpis, kjer se lahko sam vpiše in registrira svojo napravo, hkrati pa mu strežnik avtomatsko dodeli politiko dostopa. S to avtomatizacijo se zelo zniža obremenitve oddelka za informacijsko tehnologijo. Spodaj je nekaj primerov izvajanja PSN politike, ki jih podjetja lahko uporabijo (Cisco, 2012):

- omogočiti zaposlenim, ki imajo v lasti Applove tablice, dostop do omrežja, a le za HTTP promet;
- zavrniti dostop do omrežja, če so naprave modificirane; jail-broken ali rooted;
- dovoliti poln dostop do omrežja, če je naprava v lasti podjetja.

Odjemalec mora podpirati protokol 802.1x in omogočati varen VPN (IPSec ali SSL VPN) dostop do omrežja podjetja, predvsem iz nezaupljivih javnih brezžičnih dostopovnih in 3G/4G omrežij (Cisco, 2014d; Fortinet, 2015b).

Nadzorni sistem omogoča upravljanje in nadzor omrežja. Poenostavlja omrežne operacije z intuitivnim vmesnikom in prilagodljivo nadzorno ploščo, zagotavlja izjemno vidljivost preko celotnega omrežja, zmanjšuje stroške z avtomatizacijo nalog preko življenjskega cikla omrežnih operacij, maksimira vrednost naložbe v informacijsko tehnologijo (Cisco, 2014e; Brocade, 2015).

Strežnik za overjanje se uporablja za dvostopenjsko overjanje (angl. *Two-Factor Authentification – TFA*) z osebno številko za istovetenje (angl. *Personal Identification Number – PIN*) in enkratnim geslom za varen dostop do omrežja podjetja preko VPN tunela (RSA, 2014).

MDM strežnik omogoča centralizirano upravljanje mobilnih naprav različnih vrst, ki imajo različne operacijske sisteme. Funkcionalnost in podpora se razlikuje med različnimi

ponudniki, vsekakor pa mora vključevati funkcije konfiguracije naprav, upravljanja aplikacij, šifriranja na sami napravi, sinhronizacijo in izmenjavo datotek in podporo za mobilne naprave (Rouse, 2013). Podrobno bomo o MDM govorili v 3. poglavju.

Izdajatelj digitalnih potrdil (angl. *Certifiacate Authority*, v nadaljevanju CA) izdaja digitalna potrdila mobilnim napravam za vzpostavitev varnega dostopa do omrežja podjetja z uporabo infrastrukture javnih ključev (angl. *Public Key Infrastructure – PKI*). V Sloveniji deluje več izdajateljev digitalnih potrdil; Ministrstvo za javno upravo v okviru storitve SIGEN-CA, Nova Ljubljanska banka, Pošta Slovenije v okviru storitve POŠTARCA in Halcom v okviru storitve Halcom CA FO (Digitalna potrdila, 2016).

Strežnik identitete (angl. *Identity Server***)** nudi osrednjo bazo podatkov identitet in skupin, ki ga podjetja uporabljajo kot centralizirano orodje za upravljanje z identitetami (Hybrid identity management, 2016).

Aktivni imenik (angl. *Active Directory*) je strežnik z imenikom storitev, ki shranjuje podatke o vseh objektih v omrežju in nudi te informacije na voljo uporabnikom in skrbnikom omrežja (Active Directory, 2016).

V prvem poglavju smo prikazali kakšni so izzivi in priložnosti PSN koncepta, kakšen vpliv ima na uspešnost podjetja, kako pripravimo strategijo in kako ga vključimo v podjetje. Kot smo že omenili v uvodu je namen in cilj magistrskega dela najti koncept PSN okolja, ki bo varen in hkrati sprejemljiv tako za podjetje kot tudi za zaposlene. Poleg ciljev za varno PSN okolje so pomembni tudi ostali vidiki podjetja in zaposlenih, in sicer cena, enostavnost namestitve strežnikov in odjemalca, podpora ponudnika rešitve, upravljanje sistema, združljivost z ostalimi orodji za nadzor mobilnih naprav, podpora mobilnim operacijskim sistemom, podpora aplikacijam, uporabniška izkušnja, prijaznost uporabniškega vmesnika in odzivnost aplikacij. Pri iskanju primernega PSN koncepta za podjetja in zaposlene bodo zgoraj omenjeni kriteriji, poleg ciljev varnega PSN okolja, zagotovo vplivali na končno odločitev.

2 GROŽNJE INFORMACIJSKE VARNOSTI PRI UPORABI MOBILNIH NAPRAV

2.1 Zahteve informacijske varnosti

Informacijska varnost, kot je opredeljena v standardu ISO 27001, se vrti okoli naslednjih petih temeljnih načel: zaupnost, celovitost, razpoložljivost, nadzor dostopa in nezatajljivost (NIST, 2002; Brenner, 2007).

Zaupnost se nanaša na varstvo podatkov iz namernega ali nenamernega razkritja podatkov tretjim osebam.

Celovitost podatkov pomeni, da morajo biti podatki točni in skladni v njihovem celotnem življenjskem ciklu. To pomeni, da podatkov ne sme spreminjati nepooblaščen uporabnik ali jih uporabljati na neodkrit način.

Razpoložljivost podatkov zahteva, da vsi računalniški sistemi, ki obdelujejo, shranjujejo in ščitijo podatke in komunikacijske poti med različnimi sistemi, delujejo pravilno in brezhibno. Podatek mora biti na voljo kadarkoli je to potrebno.

Nadzor dostopa je izveden z overitvijo in avtorizacijo in je opredeljen kot preprečitev nepooblaščene uporabe virov podjetja.

Nezatajljivost pomeni, da med prenosom podatkov med stranko, ki prejema in stranko, ki pošilja, nobena od strank ne more zanikati prejema ali pošiljanja podatkov.

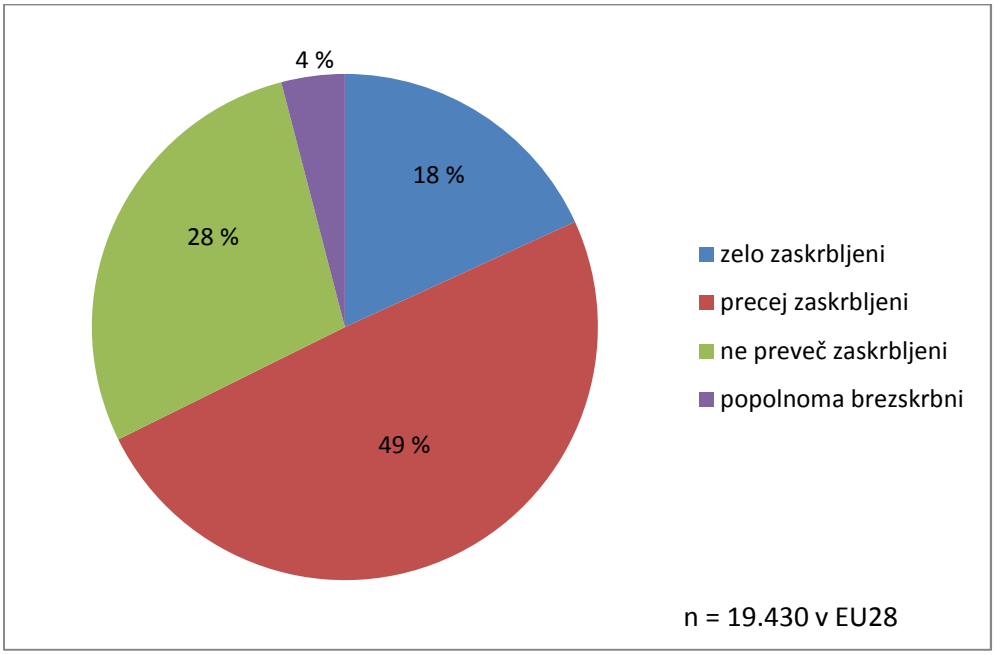
Zgornje zahteve so potrebne za podjetja, ki izvajajo PSN politiko in uporabljajo tehnologije računalništva v oblaku, kjer je izpostavljenost naprav v lasti zaposlenih še večja. Natančneje zaradi dejstva, da en sam oblak lahko gosti več uporabnikov z vrsto različnih podatkov in je zato zelo pomembno, da je zaupnost in celovitost podatkov podjetja zaščitena pred zlonamernimi osebami, med samim prenosom podatkov, obdelavo in shranjevanjem. Zato je nujno potreben mehanizem za nadzor dostopa, s katerim se zagotovi, da podatke lahko bere ali spreminja le pooblaščeno osebje v skladu s svojimi dovoljenji. Podatki morajo biti na voljo kadarkoli jih zaposleni zahtevajo, lokalno ali z oddaljenim dostopom, medtem ko mora obstajati dokaz o nezatajljivosti oziroma dokaz, da je do tega dogodka prišlo. Nadalje, zgornje varnostne zahteve so nujne tudi zaradi uporabe mobilnih naprav, tako za službene namene kot tudi osebne. Zaupnost in celovitost podatkov podjetja je potrebno zaščititi pred osebnimi aplikacijami, ki lahko vsebujejo zlonamerno kodo in pred dostopom do podatkov podjetja preko tretjih oseb (npr. družinskih članov zaposlenih ali prijateljev) (Samaras, 2013).

Glavna ovira za podjetja, ki sprejemajo PSN politiko, se nanaša na zasebnost podatkov na mobilnih napravah, ki so v lasti tako podjetja kot tudi zaposlenega. V podjetjih, ki dovoljujejo uporabo osebnih mobilnih naprav za dostop do podatkov podjetja, večinoma uporabljajo sklop pravil z namenom zaščite podjetja pred uničenjem ali uhajanjem zaupnih podatkov. V tem primeru s politiko zagotovijo, da osebne naprave spremljajo in da so vse aktivnosti zaposlenih in dostop do podatkov podjetja v skladu s poslovnimi pravili. S tem pa lahko podjetje prekorači svoja pooblastila do zasebnosti podatkov svojih zaposlenih, kar pa lahko pripelje do zmanjšanega zadovoljstva zaposlenih in celo tožb zoper podjetje (ICO, b.l.).

Pravno okolje glede zasebnosti podatkov v Evropski uniji ureja Splošna uredba o varstvu podatkov (angl. *general data protection regulation – GDPR*). Po več kot treh letih razprav na mnogih ravneh so Evropski parlament, Svet Evropske unije in Evropska komisija 15. decembra 2015 končno dosegle dogovor o novih pravilih o varstvu podatkov ter vzpostavitve sodobnega in usklajenega okvirja za varstvo podatkov v Evropski uniji. Kljub temu, da še ne bo začel takoj veljati (to bo šele v prvi polovici leta 2018), vsebuje nekatere zelo pomembne obveznosti, ki bodo imele takojšen učinek. Dogovor prinaša temeljne pravice vsem državljanom Evropske unije in jim omogoča ponovno pridobiti nadzor nad svojimi osebnimi podatki, podjetjem pa prinaša jasne sodobne predpise in koristi (European Commision, 2015a).

Nedavna raziskava Eurobarometra (European Commision, 2015b) navaja, da je dve tretjini (67 odstotkov) Evropejcev zaskrbljenih, ker nimajo popolnega nadzora nad informacijami, ki jih sami objavljajo na spletu (Slika 17). 89 odstotkov Evropejcev si tudi želi enake pravice varstva podatkov po vsej Evropski uniji, ne glede na to, kje se njihovi podatki nahajajo in obdelujejo.

Slika 17: Zaskrbljenost Evropejcev zaradi nadzora nad informacijami



Vir: European Commision, Data protection, 2015b, str .9.

Navajamo nekaj temeljnih pravic za posameznike, ki jih novi dogovor prinaša (European Commision, 2015a):

- lažji dostop do lastnih podatkov: posamezniki bodo imeli več informacij o tem, kako se njihovi podatki obdelujejo in da morajo biti le-ti na voljo na jasen in razumljiv način;

- pravica do prenosljivosti podatkov: lažji prenos osebnih podatkov med ponudniki storitev;
- razjasnjen pojem »pravica biti pozabljen«, ko ne želite več, da bi vaše podatke še naprej obdelovali in pod pogojem, da ne obstajajo utemeljeni razlogi za njihovo ohranitev, takrat bodo podatki izbrisani;
- pravica vedeti, kdaj je prišlo do vdora v vaše podatke, podjetja morajo obvestiti nacionalni nadzorni organ o resnih kršitvah podatkov čim prej, da lahko posamezniki sprejmejo ustrezne ukrepe.

Tudi podjetja bodo z novim zakonom pridobila (European Commision, 2015a):

- uredba določa en sam sklop pravil, ki bo omogočal enostavnejše in cenejše poslovanje podjetij znotraj EU;
- uredba določa znotraj EU en sam nadzorni organ;
- podjetja s sedežem izven Evrope bodo morala pri ponujanju storitev uporabljati ista pravila kot veljajo v EU;
- uredba bo zagotovila, da so ukrepi za varstvo podatkov vgrajeni v proizvode in storitve že v najzgodnejši fazi razvoja (varstvo podatkov v zasnovi).

Vsaka evropska država ima svoj nabor predpisov za podjetja, ki izvajajo politiko mobilnosti. Zasebnost podatkov v Sloveniji je urejena z Zakonom o varstvu osebnih podatkov (Ur.l. RS, št. 94/07, v nadaljevanju ZVOP-1(UPB1)).

Čeprav zaposleni uporabljajo svoje osebne naprave za opravljanje poslovnih nalog, je podjetje še vedno tisto, ki igra vlogo upravljavca podatkov (WP29, 2014). V primeru izgube, kraje ali zlorabe občutljivih in zaupnih osebnih podatkov ali podatkov podjetja, je podjetje tisto, ki je odgovorno v skladu z zakonom. Posledično bi morala podjetja zato izvajati varnostno kontrolo z namenom zaščite občutljivih podatkov, ki se obdelujejo na osebnih mobilnih napravah in so tako dostopni zaposlenim (Absalom, 2012). To pomeni varovanje shranjenih podatkov in tistih, ki se prenašajo iz in na naprave, z uporabo tehničnega nadzora samih mobilnih naprav in komunikacijskega kanala z omrežjem podjetja. Zagotoviti je potrebno skladnost zaposlenih z usmeritvami in predpisi podjetja glede zasebnosti podatkov (ICO, b.l.). Pri izgubi podatkov bi morala podjetja v strategijo poslovanja vključiti in tudi izvajati organizacijski ukrep s formalnim mehanizmom poročanja za vse podobne incidente (Absalom, 2012).

Z vidika zaposlenih je početje podjetij z dostopom in nadzorom njihovih naprav z namenom zavarovanja podatkov lahko zelo problematično, ker vdira v individualne pravice do zasebnosti. Zato vsa zakonodaja v Evropi narekuje, da mora biti vsak zaposleni o vsem popolnoma obveščen in dati nedvoumno soglasje preden lahko podjetje dostopa do njegovih osebnih podatkov in jih obdeluje. Podjetja so zakonsko obvezana tudi obveščati zaposlene o

natančnih dejavnostih spremljanja, katere podatke bo zbiralo v namen obdelave in kdo vse ima dostop do teh podatkov (Absalom, 2012; WP29, 2013). To pa ne pomeni, da lahko podjetja po pridobitvi soglasja, zbirajo vse podatke. Vsako zbiranje in obdelava podatkov mora biti v skladu z zakonom o varstvu poslovnih podatkov in politiko podjetja ter v skladu z načelom zmanjšanja količine podatkov, kar pomeni, da je potrebno zbiranje omejiti na neposredno pomembne in potrebne podatke in da se podatki lahko shranjujejo le za določen čas (WP29, 2014). Na novo sprejeta Splošna uredba o varstvu podatkov v Evropski uniji zahteva od podjetij, da imenuje pooblaščenca za varstvo osebnih podatkov (angl. *Data Protection Officer – DPO*), ki bo spremljal podatke ter sledil in poročal o vseh incidentih o izgubi osebnih podatkov in drugih kršitvah zasebnosti (European Commision, 2015a). To je še predvsem pomembno za podjetja, ki imajo politiko PSN.

Samaras (2013) predlaga naslednji pregled zahtev, ki jo mora varnostna arhitektura izpolnjevati:

- na organizacijski, pravni strani:
  - vzpostavitev soglasja zaposlenih za spremljanje osebnih mobilnih naprav,
  - omogočiti natančen zapis o kršitvah varnosti osebnih podatkov pri spremljanju mobilnih naprav,
  - določiti nabor dovoljenih funkcij na mobilni napravi,
  - določiti nabor storitev, do katerih lahko zaposleni dostopajo,
  - poskrbeti za minimalno varnostno raven na mobilnih napravah, predno se jim dovoli opravljati poslov in dostopati do omrežja podjetja,
  - določiti raven dostopa do podatkov podjetja, ki so shranjeni na strežnikih podjetja, v zasebnem ali javnem oblaku;
- na strani informacijske tehnologije:
  - zaščititi poslovne podatke podjetja, tako na strežnikih kot tudi na mobilnih napravah,
  - zaščititi njihovo zaupnost, celovitost in razpoložljivost,
  - zagotoviti nadzor dostopa do strežnikov, baz podatkov in aplikacij znotraj podjetja, kot tudi v javnem oblaku,
  - zagotoviti nezatajljivost dostopa do vseh poslovnih podatkov in aplikacij.

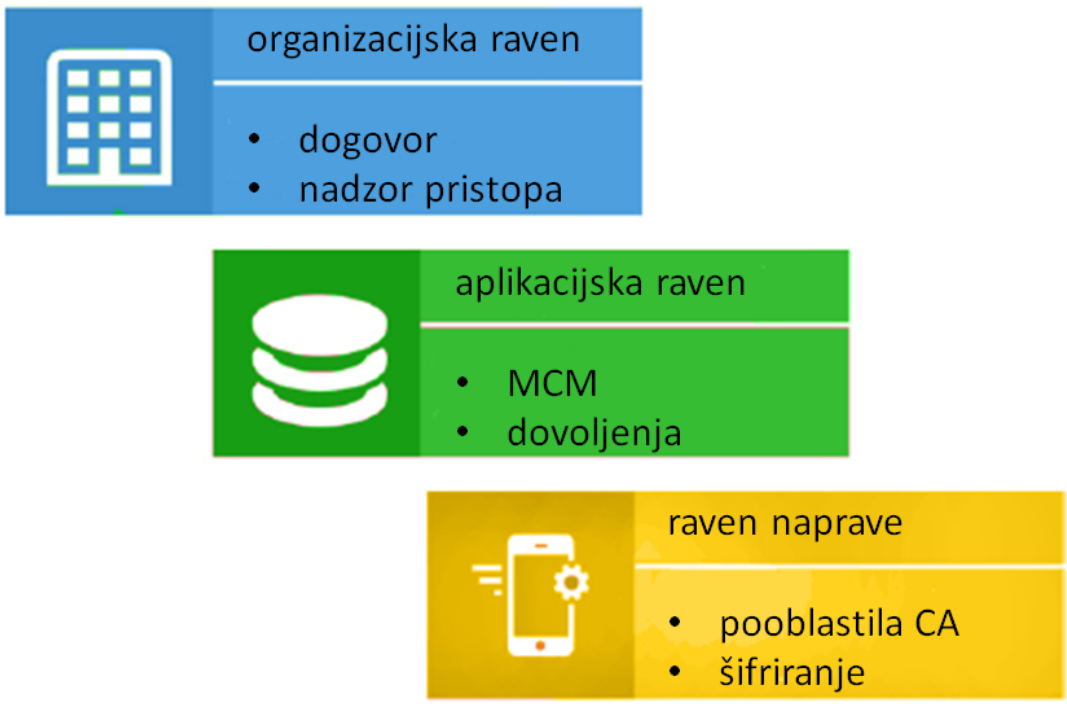
2.2 Model varnostne politike

Obstajajo različne varnostne rešitve za koncept PSN. V številnih podjetjih so nejasne in neorganizirane. Vignesh in Asha (2015) predlagata več nivojski model varnostne politike. Model je zasnovan tako, da vključuje ves potreben nabor pravil in strategij, ki so nujno potrebni za izvajanje učinkovitega PSN okolja, ne da bi kakorkoli ogrozili samo produktivnost podjetja. Slika 18 prikazuje več nivojsko varnostno politiko za PSN, ki je sestavljena iz politik na treh ravneh – organizacijski, aplikativni ravni in ravni naprav.

Organizacijska raven. Politika na organizacijski ravni vsebuje kontrolni seznam, ki ga je potrebno izdelati pred uvedbo PSN v okolje podjetja. Predlagani seznam je sledeč (Vignesh & Asha, 2015):

- razjasniti odgovornost za podporo mobilnim napravam, kdo krije stroške naročnine in klicev ter kdo krije stroške vzdrževanja mobilne naprave;
- poskrbeti, da so zaposleni odgovorni za varnostno kopiranje svojih osebnih podatkov, ki so shranjeni na mobilni napravi in da to delajo periodično;
- zaposleni morajo na zahtevo podjetja odstraniti nezaželene aplikacije;
- zaposleni ne smejo uporabljati naprave, ki ima modificirane operacijske sisteme. Modificirane Googlove Android naprave imenujemo »**rooted«** naprave, Applove iOS pa »**jail-broken«** naprave**;**
- razložiti zaposlenemu posledice pri morebitnih kršitvah.

Slika 18: Več nivojska varnostna politika za PSN



Vir: U. Vignesh & S. Asha, Modifying security policies towards BYOD, 2015, str. 513.

Vsako podjetje mora to raven upoštevati pred vključitvijo posameznega zaposlenega v PSN okolje. Dostope ni nujno dodeliti vsem zaposlenim. Omejimo jih lahko glede na nivo odgovornosti posameznega zaposlenega v podjetju. Predlagani nivoji so lahko (Vignesh & Asha, 2015):

- **standardni uporabnik** lahko uporablja PSN napravo le v omrežju podjetja, oddaljen dostop mu ni dovoljen;
- **napreden uporabnik** lahko s svojo PSN napravo dostopa v omrežje podjetja kjerkoli, dostop do občutljivih podatkov podjetja mu ni dovoljen;
- **profesionalni uporabnik** je zaupanja vreden zaposleni in ima napredno znanje o varnosti. V ta nivo spadajo sistemski administratorji in vodstvo. Imajo dostop do vseh podatkov podjetja, tudi zelo občutljivih, zaradi česar je njihove naprave potrebno skrbno spremljati;
- **gost** je nov uporabnik, ki lahko dostopa do določenih podatkov podjetja, le če je njegova naprava pred tem verificirana in preverjena s strani oddelka informacijske tehnologije. Po navadi se gostu dodeli dostop le za brskanje po spletu.

Aplikativna raven. Politika na tem nivoju zagotavlja varnost mobilnih aplikacij. Za ta namen se, kot sem že uvodoma omenil, uporablja MDM, centralizirano orodje za upravljanje mobilnih naprav. MDM podpira popoln nadzor mobilnih naprav, njihovo spremljanje in zaščito. Del MDM je tudi orodje za upravljanje mobilnih aplikacij (angl. *Mobile Application Management,* v nadaljevanju MAM), ki se za razliko od MDM uporablja le za specifične, določene aplikacije na mobilni napravi (Madden, 2012). Ta varuje aplikacije na mobilnih napravah za zaposlene in jih loči od osebnih aplikacij (MobileIron, 2015). Ker MAM ne zagotavlja popolne zaščite za mobilne naprave, mora MDM vsebovati tudi orodje za upravljanje mobilnih vsebin (angl. *Mobile Content Management,* v nadaljevanju MCM). MCM orodje vsebuje skupek tehnologij, ki zagotavljajo varen dostop do občutljivih podatkov podjetja na mobilnih napravah in se uporablja za zavarovanje vseh podatkov, ki se nahajajo na mobilni napravi (Rouse, 2014). Če hočemo zagotoviti varnost na aplikativni ravni, morajo orodja za nadzor mobilnih naprav vsebovati vsa tri zgoraj omenjena orodja. Skupek teh orodij proizvajalci na trgu imenujejo upravljanje mobilnosti v podjetju (angl. *Enterprise Mobility Management,* v nadaljevanju EMM), kar bom podrobneje opisal v tretjem poglavju.

Raven naprav. Večina podjetij politiko na ravni naprav pogosto spusti, ker predvidevajo, da je ta odvisna od lastnika in proizvajalca mobilne naprave. Kljub temu je na tej ravni potrebno opozoriti in upoštevati naslednje politike; izdajatelj digitalnih potrdil, šifriranje podatkov in modificiranje mobilnih operacijskih sistemov. Najnovejše mobilne naprave omogočajo uporabnikom upravljanje s certifikati, dodajanje in brskanje, kar pa lahko privede do zlorabe podatkov. Mobilna naprava mora spremljati overiteljeve prijavne podatke. Najnovejše mobilne naprave imajo že vgrajene aplikacije za šifriranje podatkov, kot na primer računov, nastavitev in aplikacij. Ker šifriranje lahko traja dalj časa, uporabniki tega ne uporabljajo. Z modificiranimi mobilnimi napravami uporabniki lahko namestijo katerokoli nedovoljeno aplikacijo, ki lahko omogoči spreminjanje in uhajanje občutljivih podatkov. Podjetja morajo v sklopu PSN politike preprečiti uporabo modificiranih naprav (Vignesh & Asha, 2015).

Z upoštevanjem in sprejetjem vseh treh ravni modela varnostne politike se bo v podjetju pri uporabi koncepta PSN zagotovo dvignila raven varnosti (Vignesh & Asha, 2015).

2.3 Tveganja

Po mnenju varnostnih inženirjev so bila do sedaj največja tveganja, kar zadeva elektronske naprave, povezana s prenosnimi računalniki in mobilnimi telefoni, z dostopi do elektronske pošte. Kljub tveganju kraje in izgube teh naprav, pa so imele te naprave z vidika varnosti pomembno dobro lastnost, večinoma so bile v lasti organizacije, kar je odgovornim za informacijsko varnost omogočilo vsaj to, da so jih zaščitili z enotnimi in razmeroma kakovostnimi varovalnimi mehanizmi (Hmelak & Žust, 2012).

S prihodom mobilnih naprav nove generacije, ki so dejansko postale samostojne naprave, pa se je mnenje spremenilo. Z njihovim porastom so se povečala tudi tveganja za podjetja. Mobilne naprave običajno potrebujejo podpirati več varnostnih ciljev: zaupnost, celovitost in razpoložljivost. To pomeni, da samo uporabniki z ustreznimi pooblastili lahko berejo, spremljajo in dostopajo do zasebnih podatkov v vsakem trenutku. Za dosego teh ciljev bi morale biti mobilne naprave zavarovane pred različnimi grožnjami in nevarnostmi (NIST, 2013). Grožnje, ki jih mobilne naprave, še posebej PSN naprave, prinašajo podjetjem, so navedene v nadaljevanju.

2.3.1 Izguba ali odtujitev mobilne naprave

Mobilno napravo je zaradi njegove priročnosti lažje ukrasti ali izgubiti in v prihodnje ne bo nič drugače. Večina uporabnikov na njih shranjuje vse več osebnih podatkov, in če jih uporabljajo za dostop do podjetja, tudi vse več zelo občutljivih podatkov podjetja. Če pogledamo nekaj dejstev v zvezi z izgubo ali krajo mobilnih naprav; samo v Združenem kraljestvu vsako leto ukradejo okoli 1,3 mio mobilnih naprav (Sybase, 2011), neko veliko podjetje v ZDA poroča o izgubi ali kraji okoli 1.700 mobilnih naprav na teden (Lennartsson, 2010), 120.000 pametnih telefonov se vsako leto pozabi v taksijih (Sybase, 2011), če pogledamo globalno skoraj 5 odstotkov pametnih telefonov ukradejo vsako leto (Siciliano, 2012), samo v ZDA se izgubi 113 pametnih telefonov vsako minuto (Sybase, 2011). Izguba ali odtujitev mobilnih naprav predstavlja veliko količino izgubljenih podatkov, s tem pa lahko tudi veliko tveganje za podjetja. Po poročilu Ponemon Inštituta (2014a) 37 odstotkov mobilnih naprav, ki jih zaposleni uporabljajo za dostop do podatkov podjetja, vsebujejo za podjetja občutljivo vsebino in podatke. Stroški povezani z nezavarovanimi mobilnimi napravami na delovnem mestu se gibljejo okoli 3.44 mio dolarjev na leto (Ponemon Institute, 2014a).

2.3.2 Potencialno nezaželena aplikacija

Potencialno nezaželena aplikacija (angl. *Potential Unwanted Application – PUA*) je izraz, ki opisuje aplikacije, ki po naravi niso zlonamerne, vendar pa so neprimerne za poslovna omrežja (Overview: What is Potentially Unwanted Application (PUA), 2016). Gre za del programske opreme, ki se lahko šteje za nezaželeno ali vsiljivo s strani uporabnika in predstavlja varnostna tveganja. Uporabnik je tisti, ki se mora zavedati teh tveganj, preden se odloči za namestitev aplikacije (Manmeet et al., 2014). Potencialno nezaželene aplikacije delimo na:

- Vohunska programska oprema (angl. *Spyware*). Spyware je programska oprema, ki omogoča nepooblaščeno in pritajeno spremljanje stanja informacijskega sistema, kakor tudi aktivnosti pooblaščenih uporabnikov. Pridobljene informacije napadalec shrani za prihodnjo analizo (Ocano, 2015).
- Programska oprema sledi (angl. *Trackware*). Trackware je programska oprema, ki zbira podatke s strani tretje osebe in jih je mogoče uporabiti za identifikacijo in lociranje uporabnika ali naprave (Trackware, 2016; Trackware definition, 2016).
- Oglaševalska programska oprema (angl. *Adware*). Adware je programska oprema, ki se pri uporabi interneta samodejno namesti v napravo uporabnika in omogoči sprejemanje reklamnih sporočil (Hogben & Dekker, 2010). Programska oprema prikazuje informacijo oglasa na nezaželen način, ki lahko uporabnika izpostavi tveganjem zasebnosti in varnosti (Ocano, 2015).
- Izbirnik (angl. *Dialer*). Dialer je programska oprema, ki omogoča klice ali storitev dostopa brez uporabnikovega vedenja in vodi do nepričakovanih visokih stroškov klicev ali pa povzroči dostop do nenamerne in nezaželene vsebine (Overview: What is Potentially Unwanted Application (PUA), 2016; Malware from A to Z, 2016).
- Orodja za oddaljeno skrbništvo (angl. *Remote Administration Tools*, v nadaljevanju RAT). RAT je programska oprema za nadzor sistema iz oddaljene lokacije. Napadalci jih lahko uporabijo zlonamerno z namestitvijo ali odstranitvijo programske opreme, z zagonom ali končanjem aplikacij ali pa z izvajanjem drugih nedovoljenih dejanj (Overview: What is Potentially Unwanted Application (PUA), 2016; Malware from A to Z, 2016).
- Orodja za hekanje (angl. *Hacking Tools*). Orodje za hekanje je vsak program, ki ga uporabnik uporablja za analizo ali pa za zaobitev varnostne zaščite. Uporablja se za raziskovanje, analiziranje in ogrožanje varnosti sistemov (Overview: What is Potentially Unwanted Application (PUA), 2016; Malware from A to Z, 2016).

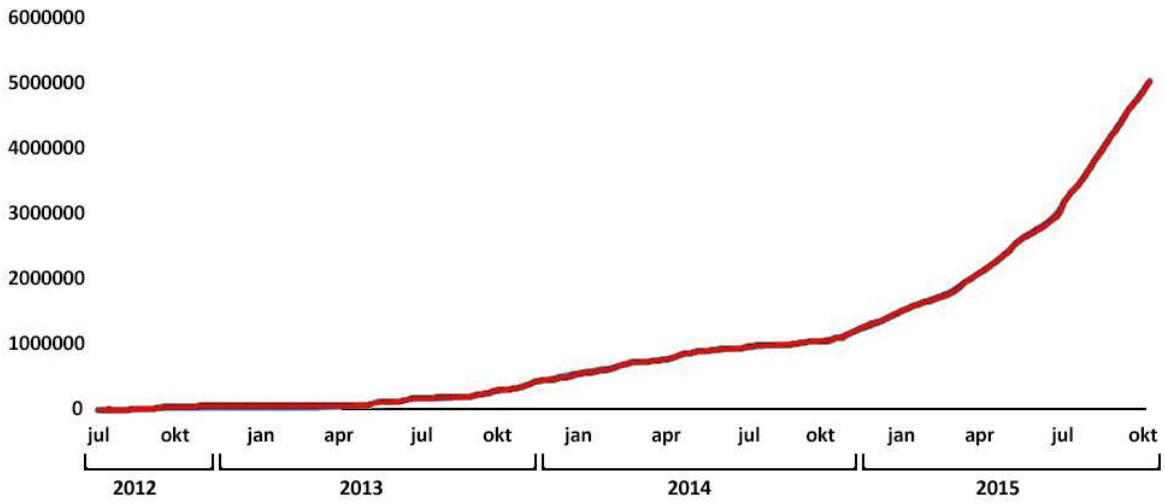
2.3.3 Zlonamerna programska oprema

Zlonamerna programska oprema (angl. *Malware*, v nadaljevanju malware) je programska oprema, katere namen je škodljivo vplivati na delovanje informacijskega sistema. Rast

malwara je v zadnjih dveh letih strmo naraslo predvsem na mobilnih napravah in zagotovo postalo ena največjih nevarnosti za podjetja, ki izvajajo PSN (Manmeet et al., 2014). Najbolj napadajo Androidov ekosistem, ker omogoča namestitev aplikacij iz aplikacijskih trgovin tretjih oseb in tudi zaradi ohlapnega nadzora nad aplikacijami. 99 odstotkov vsega zlonamernega programja je bilo v letu 2013 usmerjenega v Android (Cisco, 2014b). Malware je pogosto vgrajen v brezplačne aplikacije in v ukradene različice poslovnih aplikacij, ki so na voljo v trgovinah tretjih oseb (Motive, 2015). Nokia v svojem poročilu Threat Intelligence Report (Nokia Threat Intelligence Report – H2 2015, 2016) ugotavlja trend rasti malwara na Androidu zaradi povečanja vzorcev v njihovi podatkovni bazi. Število vzorcev se je več kot podvojilo v drugi polovici leta 2015. Skupna rast v letu 2015 je bila 342-odstotna. Na Sliki 19 je prikazan trend rasti malwara na mobilnih napravah od leta 2012.

Eden izmed prvih usmerjenih napadov zlonamernega programja na mobilne naprave je bil Red October, ki so ga prvi identificirali v Kasperski Labu. Mobilne naprave bodo v prihodnje še bolj deležne ciljanih napadov, predvsem tiste, ki lahko dostopajo do podatkov podjetij in ki vsebujejo zaupne občutljive dokumente ter imajo dostop do baz in kontaktnih podatkov podjetja. Mobilne naprave bodo verjetno postale rutinski element napadov kibernetskega vohunstva na podjetja (Gilmore & Beardmore, 2013).

Slika 19: Trend rasti zlonamerne programske opreme na mobilnih napravah od leta 2012



Vir: Nokia Threat Intelligence Report – H2 2015, 2016, str. 7.

Malware lahko razdelimo v naslednje kategorije:

- Trojanski konj (angl. *Trojan Horse*) je zlonamerni program z navidezno koristno funkcijo. Program, ki naj bi naredil eno, dejansko pa naredi drugo, v večji meri negativno vpliva na uporabnikov sistem in njegove podatke (Ocano, 2015).

- Črv (angl. *Worm*) je zlonamerni program, ki se razširja v sistemih in se pri tem samodejno razmnožuje. Njegov cilj je reprodukcija sebe. Poznamo omrežne črve, črve elektronske pošte, P2P črve in črve takojšnjega poročanja.
- Virus (angl. *Virus*) ima tako kot črv sposobnost samodejnega razmnoževanja. Za razliko od črvov, je virus pritrjen na izvedljive (exe) datoteke. Poznamo viruse zagonskega sektorja, datotečne, večstranske, polimorfne viruse, makroviruse in viruse elektronske pošte (Malware Categories, 2016).
- Stranska vrata (angl. *Backdoor*) je program, ki omogoča nepooblaščen dostop do informacij, pri tem pa se izogiba mehanizmom za preverjanje pristnosti. Pri mobilnih napravah gre za nepooblaščen dostop na daljavo (Ocano, 2015). Pod to kategorijo spadajo vsi botneti.
- Lažno sporočilo (angl. *Hoax*) ali potegavščina je lažno svarilo pred računalniškim virusom, ki se navadno širi z elektronsko pošto in spodbuja prejemnika, da sporočilo razširja dalje (Malware Categories, 2016).
- Neželena elektronska pošta (angl. *Spam*) je nadležna kuga pošiljanja neželenih sporočil oglaševanja preko elektronske pošte. Sodobni antispam programi uporabljajo kombinacijo metod za filtriranje neželene pošte, tako statično z analizo besedila ali seznami poštnih strežnikov kot tudi statistično na podlagi klasifikacijskega modela naive Bayes (Malware Categories, 2016). Po Cisco poročilu (2015b) se je obseg neželene elektronske pošte povečal za 250 odstotkov samo od januarja do novembra 2014. Vse večja grožnja današnjega časa je neželena elektronska pošta imenovana Krplje (angl. *Snowshoe*), ki pošilja manjše količine pošte iz velikega nabora IP naslovov (Cisco, 2015b).
- Zvabljanje (angl. *Phishing*) je poskus pridobitve osebnih podatkov kot so imena, gesla, številke kreditnih in bančnih kartic, podatkov za dostop do bančnega računa, itd. preko lažne spletne strani ali preko elektronske pošte (Malware Categories, 2016).
- Modificiranje mobilnih naprav (jail-braking ali rooting) je prav tako mogoče obravnavati kot zlonamerno. Naprava je tako bolj ranljiva pred zlonamernimi aplikacijami. Podjetja bi morala odklenjene naprave prepovedati v podjetju (Svensk, 2013).
- Vohunjenje (angl. *Snooping*) se nanaša na poslušanje prometa v omrežju in spremljanje podatkov, ki se izmenjujejo. Cilj je pridobiti uporabniška imena, gesla in druge vrste podatkov, ki so za napadalce zanimivi. Pri vohunjenju napadalci uporabljajo aplikacijo omrežni analizator protokolov (npr. Wireshark) in če podatki niso pravilno šifrirani oziroma uporabniki ne uporabljajo šifrirne mehanizme, z lahkoto zajamejo vse datagrame znotraj omrežja in s tem pridobijo za njih koristne podatke (Svensk, 2013).
- Izsiljevalska programska oprema (angl. *Ransomware*) je zlonamerna programska oprema, ki omogoča uporabo sistema ali storitve, za ponovno vzpostavitev uporabe zahteva plačilo.

2.3.4 Prisluškovanje

Prisluškovanje (angl. *Eavesdropping*) je metoda nepooblaščenega prestrezanja komunikacije na mobilnih napravah brez vednosti udeležencev (iSlovar, b.l.). Gre za klasično vohljanje tako v WiFi omrežjih kot tudi na 3G/4G omrežjih.

2.3.5 Organizirana trajna grožnja

Organizirana trajna grožnja (angl. *Advanced Persistant Threat*, v nadaljevanju APT) je trajno ogrožanje varnosti informacijskega sistema, ki ga izvaja neka organizirana skupina. V večini primerov so tarča podjetja. Za razliko od drugih napadov APT procesi zahtevajo visoko stopnjo prikritosti v daljšem časovnem obdobju. APT je sestavljen iz treh pomembnih komponent (C5, 2011):

- **Organizirano**. Heker ima sposobnost, da ostane neodkrit in ima možnost trajnega dostopa do dobro varovanih omrežij in občutljivih informacij. Heker je na splošno prilagodljiv in dobro opremljen.
- **Trajno**. Trajna narava grožnje otežuje preprečevanje dostopa do omrežja podjetja in ko dostop dobi, ga je težko odstraniti.
- **Grožnja**. Heker ima namen in sposobnost dostopati vseh občutljivih informacij v elektronski obliki.

2.3.6 SQL-vrinjenje

SQL-vrinjenje (angl. *SQL Injection*) je napad, pri katerem se zlonamerna koda vstavi v SQL ukazni niz, ki se posreduje podatkovni bazi kot legitimna poizvedba. PSN omogoča težje razumevanje temeljnih vzrokov napada. V raziskavi Ponemon inštituta 56 odstotkov vprašanih meni, da je zaradi naraščajočega PSN trenda vedno težje določiti temeljne vzroke za SQL-vrinjenje in da je že 42 odstotkov vseh kršitev zaradi SQL-vrinjenja (Ponemon Institute, 2014b).

2.3.7 Zasebnost podatkov za podjetje in odjemalca

Spremljanje in dostop do podatkov in aplikacij na PSN napravi sproža pravna vprašanja glede zasebnosti podatkov. V PSN okolju ima zaposleni svojo napravo, ki jo sam upravlja in vzdržuje. Podjetje se zelo težko prepriča, da ne pride do uhajanja podatkov, da občutljive informacije podjetja ne pridejo v tretje roke, recimo družinske člane, ki tudi uporabljajo PSN napravo. Zato je zasebnost podatkov pomemben napad, ko zaposleni uporablja PSN napravo za poslovne namene, bodisi v ali izven delovnega časa (Manmeet et al., 2014).

2.3.8 Socialni inženiring

Socialni inženiring je nagovarjanje uporabnikov, da izdajo informacije, ki nepooblaščenim osebam omogoči dostop do informacijskega sistema oziroma informacijskega vira. Cilj socialnega inženiringa je pridobitev občutljivih in zaupnih podatkov. Ko je uporabljen kot napad na mobilne naprave, ki vsebujejo občutljive aplikacije podjetja, kot je elektronska pošta, lahko socialni inženiring predstavlja veliko grožnjo za varnost. Tehnike socialnega inženiringa v PSN okolju so na primer zvabljanje, lažno virusno sporočilo, zlonamerna povezava in nepooblaščena mobilna aplikacija (Manmeet et al., 2014; Government Business Council, 2013).

2.3.9 Napadi SSL

Napadi SSL so vrsta napada, ki se osredotoča na kršitev ranljivih točk omrežnega protokola. Napadalec uporablja za to vrsto napada enoten protokol SSL in TLS (angl. *Transport Layer Security*). Najboljši primer takega napada je programska napaka imenovana Heartbleed, ki je bila odkrita aprila 2014 in povzroča ranljivost v kriptografski knjižnici OpenSSL (OpenSSL »Hartbleed« vulnerability (CVE-2014-0160), 2016). Posledica Heartbleeda je bila pridobitev eno tretjino vseh uporabniških imen in gesel, ki so bile shranjene na različnih strežnikih po svetu. V PSN okolju ta napad prinaša več tveganja za nezaščitene mobilne naprave, ki vsebujejo poslovne podatke (Manmeet et al., 2014).

2.3.10 Mobilni napadalec

Mobilni napadalec (angl. *Man-In-The-Mobile*) je nedaven izraz za mobilno verzijo vrinjenega napadalca (angl. *Man-In-The-Middle – MITM*). Zlonamerna programa »beležnik tipkanja« (angl. *Keylogger*) in »vohunjenje« se lahko namestita na vse nezaščitene mobilne naprave, tako da se mobilni napadalec lahko izvede brez težav. Trojanec Zitmo (Zeus in the mobile) bere in prestreza SMS na mobilni Android napravi. Z mobilnim napadalcem je enostavno pridobiti tudi zelo občutljiv podatek, kot npr. mobilno transakcijsko avtentikacijsko številko (angl. *Mobile Transaction Authentication Number,* v nadaljevanju mTan). mTan se uporablja kot enkratno geslo za bančne transakcije z mobilnimi napravami (Manmeet et al., 2014).

2.3.11 Zloraba Bluetooth

Mobilne naprave z vmesnikom Bluetooth so ranljive za aktivne (neposredne napade na modul Bluetooth) in pasivne napade (napadalec čaka na vzpostavitev povezave in prestreza podatke) (Markelj, 2012). Tveganje je večje, ko je naprava povezana preko javnih dostopovnih WiFi točk ali mobilnega omrežja. Napadalci lahko izkoristijo slabo varovane

ali celo nezavarovane povezave Bluetooth in se s svojo napravo povežejo z uporabnikovo, nato pa preko WiFi povezave v okolje podjetij.

2.3.12 Brezžična Wifi omrežja

Brezžična omrežja so zelo občutljiva in izpostavljena napadom zaradi svoje brezmejne narave. Zelo enostavno je vdreti v vsako lokalno žično omrežje preko WiFi dostopovnih točk, ki povezujejo lokalna žična omrežja in brezžična omrežja, če ta niso zavarovana z gesli in enkripcijskimi algoritmi. Rast WiFi vstopnih točk ali t.i. hotspotov izpostavlja mobilne naprave hekerjem, ki izvajajo monitoring na teh omrežjih. Trajne grožnje brezžičnim WiFi omrežjem so: vrinjeni napadalec, vohljanje – prestrezanje podatkovnih paketov pri prenosu v omrežju, goljufive dostopovne točke (angl. *Rogue Access Points*), ohromitev storitve (angl. *Denial of Service – DoS*), prestrezanje radiofrekvenčnega prepoznavanja (angl. *Radio Frequency Identification – RFID*) in napadi socialnega inženiringa (Noor & Hassan, 2013).

2.3.13 Ranljivost programske opreme

Ranljivost programske opreme predstavlja za katerokoli aplikacijo stalno varnostno tveganje. Največje tveganje za aplikacije predstavlja čas med odkritjem ranljivosti in programskim popravkom. Spletni brskalnik je tipični primer in je na voljo praktično na vsaki mobilni napravi. Ko avtorji zlonamerne kode odkrijejo razpoko v programski opremi, lahko potem z lahkoto vbrizgajo zlonamerno kodo, ki (lahko) potem vpliva na milijone naprav do trenutka, ko je ranljivost odkrita in s popravkom odstranjena (Svensk, 2013). Neprofitna organizacija Open Web Application Security Project – OWASP objavlja seznam deset najpogostejših ranljivosti in med njimi je večina povezanih s spletnim brskalnikom (The Ten Most Critical Web Application Security Risks, 2016). Spletni brskalnik je opredeljen kot sistemska aplikacija, to pa pomeni, da je del operacijskega sistema in ima zato dostop do sistemski virov na mobilni napravi.

2.3.14 Napad notranje osebe

Napad notranje osebe najbolj opišejo avtorji Salem et al. (2008) v svoji raziskavi, kjer ugotavljajo, da napadi notranje osebe postajajo večja grožnja podjetjem kot zlonamerna programska oprema. Ker so varnostni ukrepi v podjetjih osredotočeni na protiukrepe nedovoljenega in nezakonitega dostopa do njihovega omrežja, predstavljajo grožnje, ki izhajajo iz zlorabe naprav znotraj omrežja, največji vir škodljivih zlonamernih aktivnosti. Raziskava deli napade notranje osebe na dva dela: izdajalce in zamaskirance. Izdajalec je opisan kot zaposleni, ki ima dovoljenje in lahko dostopa do virov podjetja, medtem ko je zamaskiranec označen kot zaposleni, ki krade identiteto in privilegije drugega za izvršitev zlonamerne aktivnosti. V kontekstu PSN okolja je zelo pomembno zagotoviti varnost

omrežja pred napadi notranjih oseb, v prvi meri z avtorizacijo dostopa v omrežje podjetja (Salem et al., 2008).

2.4 Ukrepi za zmanjšanje tveganj

Kot smo že uvodoma ugotovili, popolna prepoved uporabe lastnih osebnih naprav na delovnem mestu dolgoročno ne bo mogoča, hkrati pa bodo uporabniki zavračali številne tradicionalne varnostne mehanizme, ker jih bodo omejevali pri uporabi njihovih naprav. Z vidika produktivnosti je uporaba mobilnih naprav na delovnem mestu dokaj smiselna, kajti nove naprave omogočajo delo kadarkoli in skoraj kjerkoli, kar pa prinaša tudi številne potencialne prednosti, kot so večja produktivnost, večja fleksibilnost, zmanjšanje stroškov podjetja in večja učinkovitost informacijske tehnologije (Hmelak & Žust, 2012).

Podjetja morajo izvesti podrobnejši pregled ocene tveganj in njihovo ublažitev v PSN okolju. Same morajo preučiti modele za vključitev PSN koncepta, kot smo jih opisali v prvem poglavju in na podlagi ocene tveganj same preučiti, kakšen dostop bodo dovolile mobilnim napravam, zlasti napravam v osebni lasti uporabnikov (PSN) ter pri tej oceni tveganj upoštevati najmanj naslednje dejavnike (Hmelak & Žust, 2012; Manmeet et al., 2014; Chellakari, 2012):

- občutljivost dela, zlasti dostop do občutljivih (osebnih) podatkov;
- zanesljivost skladnosti s politikami varovanja informacij: številne varnostne zahteve je mogoče izpolniti le na napravah z nameščenim odjemalcem za oddaljeno upravljanje mobilne naprave oz. njene varnosti;
- nadzor nad aplikacijami: nepreverjene, nenadzorovane in nezavarovane aplikacije, ki so nameščene na mobilnih napravah zaposlenega;
- nadzor nad podatki: jasna razmejitev kdo je lastnik katerih podatkov na mobilni napravi, obnovitev in brisanje teh podatkov v primeru izgube in kraje naprav ali pa v primeru ko zaposleni zapusti podjetje;
- stroški mobilnih naprav in odjemalcev za njihovo upravljanje (preko centralnega orodja za upravljanje mobilnih naprav);
- dostop do omrežja podjetja; večinoma so povezave, s katerimi zaposleni dostopajo do elektronske pošte, datotečnih sistemov in drugih internih virov podjetja, nezaščitene in nekriptirane in jih je mogoče prestreči;
- lokacija dela: uporaba mobilnih naprav je bolj tvegana pri oddaljenih dostopih do omrežja podjetja, torej zunaj prostorov podjetja;
- veliko število različnih mobilnih operacijskih sistemov: Googlov Android, Applov iOS, Nokiin Symbian, Microsoftov Windows, BlackBerrijev OS, Samsungov BADA;
- tehnične omejitve naprav: problem pri kompatibilnosti z nadzornim orodjem, ker ni nujno, da vsaka mobilna naprava podpira njihovega odjemalca;

- morebitna izguba podatkov: pri tem je pomembno popolnoma odpraviti ali vsaj zmanjšati izpostavljenost občutljivih in kritičnih podatkov;
- izguba in kraja mobilnih naprav: takojšnje poročanje zaposlenih, ki z mobilnimi napravami dostopajo do virov podjetja;
- skladnost z zakoni in drugimi predpisi: lokalna zakonodaja, zakonodaja o varstvu osebnih podatkov.

Kot eden od ukrepov za zmanjšanje tveganj, NIST predlaga podjetjem v implementacijo in izvajanje za izboljšanje varnosti njihovih mobilnih naprav spodaj navedene smernice. Vsako podjetje bi moralo imeti mobilno varnostno politiko. Varnostna politika mora določiti, katere dele omrežja in do katerih virov podjetja lahko dostopajo zaposleni z mobilnimi napravami, s katero vrsto naprav in katero stopnjo dostopa jim dovoliti. Nadalje, mobilna varnostna politika mora zajemati tudi vprašanja v zvezi s centraliziranim orodjem za nadzor, kdo in kako jih bo upravljal, kako se bodo strežniki in mobilna politika posodabljala. Mobilna varnostna politika mora biti dokumentirana v varnostnem načrtu podjetja ter skladna in hkrati dopolnjena s celotno varnostno politiko podjetja (NIST, 2013).

Podjetja morajo razviti model sistemskih groženj za mobilne naprave in za vse vire, ki so dostopni prek mobilnih naprav. Model vključuje (NIST, 2013):

- opredelitev virov možnih groženj;
- varnostni nadzor nad temi viri;
- opredelitev ranljivosti organizacije;
- količinska ocena verjetnosti uspešnih napadov in njihovih vplivov;
- analiza teh podatkov s smernicami za izboljšavo.

Podjetja naj preučijo možnost uporabe naslednjih kategorij varnostnih mehanizmov, ki jih zagotavlja centralno orodje za upravljanje mobilnih naprav (NIST, 2013):

- **Splošna politika**: Uveljavitev varnostne politike organizacije na mobilne naprave, kot so omejitev dostopa do strojne in programske opreme:
  - digitalna kamera,
  - sistem za pozicioniranje (angl. *Global Positioning System,* v nadaljevanju GPS),
  - Bluetooth,
  - USB vmesnik in spominske kartice,
  - upravljanje z dostopi do brezžičnih omrežij (WiFi),
  - nadzor in poročanje kršitev varnostne politike.
- **Podatkovne komunikacije in hramba podatkov**: Podpora močne enkripcije podatkovne povezave med mobilno napravo in hrambo podatkov (uporaba VPN povezave) in podatkov na vgrajenih spominskih medijih, kot tudi na spominskih karticah in oddaljeno brisanje podatkov na napravi v primeru kraje ali izgube.

- **Overjanje uporabnika in naprave**: Zahteva po uporabi kakovostnih gesel in drugih varnih mehanizmov overjanja, možnost oddaljenega dostopa do mobilnih naprav, oddaljen ponovni zagon in nastavljanje gesel, avtomatično zaklepanje naprave po določenem obdobju neaktivnosti oziroma neuporabe ter brisanje vseh podatkov na napravi po določenem številu neuspelih poskusov dostopa oziroma overjanja do internih virov organizacije.
- **Aplikacije**: Omejitev nameščanja, posodabljanja in odstranjevanja aplikacij, digitalnega podpisovanja in omejitev dostopa do informacijskih virov organizacije za samo določene različice programskih rešitev.

Podjetja bi morala izvesti pilotno postavitev svoje rešitve pred samim zagonom. Rešitev je potrebno oceniti za vsak tip mobilne naprave, njihovo povezljivost v okolje, zaščito, overjanje, funkcionalnost aplikacij, upravljanje, beleženje, poročanje in zmogljivost rešitve. Nadalje, omogočiti se mora posodabljanje z najnovejšimi programskimi popravki, avtomatsko zaznavanje jail-broken in rooted naprav ter onemogočena nepričakovana ponastavitev naprav na privzete nastavitve. Podjetja bi morala v celoti preprečiti izgubo podatkov podjetja in širitve virusnih programov. To predvsem velja za mobilne podatke v lasti podjetja (NIST, 2013).

Podjetja morajo redno vzdrževati svojo mobilno varnostno politiko z naslednjimi operativnimi postopki: preverjanje za nadgradnje in popravke, odkrivanje in dokumentiranje nepravilnosti, vključno z nepooblaščenimi vstopi in spremembami v konfiguraciji mobilne naprave, aktivno vodenje mobilnih naprav, njihov dostop, preklic dostopa ali brisanje aplikacij, ki so ocenjene kot tvegane (NIST, 2013).

2.5 Operacijski sistemi mobilnih naprav

Za podjetja je eden od ukrepov za zmanjšanje tveganj tudi pravilna izbira operacijskega sistema na mobilnih napravah, ki jih nameravajo podpirati. Ko gre za mobilnost podjetij, je zagotavljanje varnosti mobilnih naprav in aplikacij postala prednostna naloga. Ker se vedno več podjetij odloča za mobilnost, je učinkovito upravljanje teh naprav in izvajanje ustreznih varnostnih politik zelo pomembna naloga oddelkov informacijske tehnologije. Proizvajalci mobilnih naprav vsako leto dodajajo vse več varnostnih mehanizmov v mobilne naprave. Napredek, ki sta ga zadnja leta Google in Apple naredila na tem področju, je izbiro le še olajšalo.

Izbira, katere operacijske sisteme podpirati, vključuje tudi ključno odločitev o tem, kakšen je najboljši pristop k upravljanju naprav in aplikacij, problem zasebnosti, sporazumi z zaposlenimi in še veliko več (Klein, 2015).

Applov iOS in Googlov Android prevladujeta na trgu operacijskih sistemov mobilnih naprav. Iz Tabele 1, ki jo je predstavil IDC v svoji raziskavi avgusta 2015, je razviden že skoraj 97-odstotni svetovni tržni delež v letu 2015 (Smartphone OS Market Share, 2015 Q2, 2016).

Tabela 1: Svetovni tržni delež mobilnih operacijskih sistemov v letih 2012–2015 (v %)

Obdobje	Android	iOS	Windows	BlackBerry OS	Ostali
2015Q2	**82,8**	**13,9**	**2,6**	**0,3**	**0,4**
2014Q2	**84,8**	**11,6**	**2,5**	**0,5**	**0,7**
2013Q2	**79,8**	**12,9**	**3,4**	**2,8**	**1,2**
2012Q2	**69,3**	**16,6**	**3,1**	**4,9**	**6,1**

Vir: Smartphone OS Market Share, 2015 Q2, 2016, str. 1.

2.5.1 Apple iOS

Applova iOS platforma ima trdne, večplastne varnostne elemente v svojem jedru brez ogrožanja uporabniške izkušnje. Na ravni strojne opreme Apple uporablja AES-256 (angl. *Advanced Encryption Standard*) kriptografijo za šifriranje celega diska. Omogoča tudi zmogljivost oddaljenega brisanja naprave in funkcijo peskovnika (angl. *Sandbox*), nadzorovanega okolja za preizkus aplikacij. Vsaka aplikacija na mobilni napravi je omejena v zapisovanju podatkov in ne more kar tako dostopati do podatkov drugih aplikacij ali same kode. Za izmenjavo informacij med aplikacijami skrbi programski vmesnik (angl. *Application Program Interface*, v nadaljevanju API). Particija jedra operacijskega sistema je samo za branje (angl. *Read Only*), kar še dodatno varuje napravo pred zlonamerno programsko opremo. Nova različica iOSa 9 temelji na funkcijah, ki so v večini namenjena podjetjem, vključujoč šifriranje pomnilnika, zmogljivost oddaljenega brisanja. Njihov API zagotavlja Touch ID biometrične varnostne funkcije razvijalcem tretjih oseb. Prav tako je Apple implementiral zmogljivosti z gesli na številnih izvornih aplikacijah (Klein, 2015).

Z nenehnimi izboljšavami na področju varnosti bo Applov operacijski sistem iOS za podjetja zagotovo ostal na vrhu seznama izbire.

2.5.2 Google Android

Prav tako kot Apple je tudi Google veliko naredil na področju varnosti. Najnovejše različice Androida na primer že vključujejo sposobnost preverjanja pristnosti prstnih odtisov za vstop v aplikacije, prav tako vsebujejo tudi nekakšno požarno pregrado za vse aplikacije na napravi

in s tem oblikujejo sistem za nadzor dostopa, ki prenesene aplikacije osami, da malware ne more dostopati do samega operacijskega sistema. Ker Android ostaja odprtokodni operacijski sistem, bo še vedno zelo dovzeten za malware, vendar pa je Google uspel prepričati podjetja in jim ponuditi funkcije večje zaščite in večjega nadzora nad napravo (Klein, 2015). S tem Android ostaja prva izbira podjetij.

2.5.3 Microsoft Windows

Tudi Microsoft s svojim Windows operacijskim sistemom za mobilne naprave v varnosti ne zaostaja za tekmeci. S funkcijo Windows Hello je Microsoft močno izboljšal varnost, ki omogoča uporabnikom dostop do Windows naprav preko svojih prstnih odtisov, očesne šarenice ali detekcije obraza. S funkcijo Passport uporabniki lahko dostopajo do aplikacij, spletnih strani in omrežja brez dodatnih gesel po preverjanju. Z zmanjšanjem potrebe po geslih, katere lahko uporabniki nehote ali namenoma delijo z drugimi, se zmanjša verjetnost vdora v uporabnikove informacije in napravo. Najnovejši operacijski sistem Windows 10 Mobile pa vsebuje funkcijo Device Guard, varnostno izboljšavo, ki ščiti pred zlonamerno programsko opremo z blokiranjem neodobrenih aplikacij (Klein, 2015).

2.5.4 BlackBerry

Med poslovnimi uporabniki je BlackBerry zagotovo številka ena. Moč blagovne znamke si je utrdil s svojimi varnostnimi zmogljivostmi ter elektronsko pošto in sporočanjem znotraj podjetij. Počasen premik k zaslonom na dotik in pomanjkanje notranjega sodelovanja med razvijalci je zelo škodilo družbi in znatno zmanjšalo njen tržni delež. V zadnjih letih so se postavili na noge in pokazali napredek z inovativnimi funkcijami. BlackBerry blesti v panogah s strogimi varnostnimi zahtevami in pooblastili ustreznosti, kot so finančne storitve in zdravstveno varstvo (Klein, 2015). Zagotovo bo v prihodnosti BlackBerry resen tekmec.

2.6 Cilji varnega PSN okolja

Za podjetja je zelo pomembno imeti varno PSN okolje. Izdelati morajo ne samo trdno mobilno varnostno politiko, temveč tudi celovito varnostno politiko podjetja. Vse koncepte in modele, ki smo jih predstavili v prejšnjih poglavjih, je potrebno vključiti v enotno rešitev in jo lahko kot tako prikažemo skozi celotni življenjski cikel rešitve.

V nadaljevanju je prikazan pet fazni model življenjskega cikla PSN rešitve (Slika 20), ki pomaga podjetjem določiti, v kateri fazi se neko varnostno priporočilo nahaja. Podjetja lahko sledijo metodologiji projektnega vodenja ali metodi življenjskega cikla, ki nujno ne sledi petim fazam, vendar so vrste nalog v skladu z metodologijo in njihovim zaporedjem verjetno podobne (Keyes, 2013).

Faze življenjskega cikla so (NIST, 2013):

- **Faza 1: Uvajanje**. Ta faza vključuje naloge, ki jih mora podjetje izvesti predno začne oblikovati rešitev za mobilne naprave. Te vključujejo: ugotavljanje potreb za mobilne naprave, zagotavljanje celovite vizije, kako naj rešitev podpira poslanstvo podjetja, ustvarjanje strategije na visoki ravni za implementacijo, razvijanje mobilne varnostne politike in navajanje poslovnih ter funkcionalnih zahtev za rešitev.
- **Faza 2: Razvoj**. V tej fazi osebje podjetja določi tehnične karakteristike mobilnih naprav in povezanih komponent. Ta vključuje tudi načine overjanja in šifrirne mehanizme za zaščito komunikacij in shranjenih podatkov, oblikovanje arhitekture, zahteve nastavitev, oskrbovanje naprav, uporabo varnostnega preverjanja in zahteve glede certificiranja. Upoštevati je potrebno veliko število različnih vrst mobilnih naprav različnih znamk in z različnimi vrstami operacijskih sistemov. Tu je potrebno biti zelo pazljiv, da se mobilna varnostna politika lahko implementira in uporabi ter izvaja z vsemi pooblaščenimi zaposlenimi. Na koncu te faze se dobavlja komponente rešitve.
- **Faza 3: Implementacija**. V tej fazi se opremo nastavi tako, da izpolnjuje operativne in varnostne zahteve, vključno z dokumentiranjem mobilne varnostne politike v sistemski varnostni načrt. Oprema mora biti montirana in preizkušena kot pilotna postavitev ter šele nato spuščena v produkcijo oziroma uradno potrjeno delovanje. Faza implementacije vključuje tudi integracijo z drugimi varnostnimi nadzori in tehnologijami, med drugim tudi z varnostnim beleženjem dogodkov in strežniki za overjanje.
- **Faza 4: Izvajanje in vzdrževanje**. Ta faza vključuje naloge povezane z varnostjo, ki bi jo moralo podjetje opravljati sproti od trenutka, ko je mobilna naprava spuščena v obratovanje, vključno z nameščanjem popravkov, sinhronizacijo ure na posameznih mobilnih napravah, pregledov zapisanih dogodkov, zagotavljanjem šolanja in ozaveščenje uporabnikov, preklic dostopa, brisanje aplikacij, odkrivanje in dokumentiranje napadov.
- **Faza 5: Odstranitev**. Ta faza obsega vse naloge, ki se pojavijo, ko celotno rešitev ali njenih sestavnih delov ne potrebujemo več. Te naloge vključujejo tudi ohranjanje podatkov z izpolnjevanjem zakonskih zahtev, sanacijo medijev in pravilno odstranjevanje opreme.

Na podlagi izzivov, s katerimi se podjetja soočajo pri PSN konceptu, od katerih so najbolj pomembni uhajanje podatkov, nepooblaščena delitev prostorov, pomanjkanje varnostne ustreznosti in zasebnost zaposlenih. Poleg ostalih ukrepov za zmanjšanje tveganj, ki so bila predstavljena, lahko identificiramo glavne cilje za varno PSN okolje. Avtorji Wang et al. (2014) so identificirali cilje, ki jih navajamo v nadaljevanju.

Slika 20: Pet fazni model življenjskega cikla PSN rešitve

2.6.1 Izolacija prostora

Ta cilj obravnava nedovoljeno izmenjavo prostorov. Ta se doseže z izolacijo osebnega prostora od prostora podjetja na način, da med omenjenima prostoroma ni nobene izmenjave podatkov. Vendar pa izvajanje izolacije prostora ne preprečuje situacij, v katerih podjetje izvede povrnitev na privzeto tovarniško nastavitev z namenom izbrisa vseh zaupnih podatkov, ki se nahajajo na mobilni napravi. S stališča zaposlenih to seveda ni zaželeno, ker bi v tem primeru tudi zaposleni izgubili vse podatke shranjene v njihovem osebnem prostoru (Wang et al., 2014).

2.6.2 Varovanje podatkov podjetja

Zaupne informacije o podjetju morajo ostati skrivnost tudi po tem, ko je mobilna naprava prodana, ukradena ali izgubljena. Pri tem načinu se uporablja kriptografske algoritme za šifriranje podatkov podjetja. Na ta način imajo dostop do informacij le pooblaščene osebe podjetja, ki imajo ključ za dostop (Wang et al., 2014).

2.6.3 Izvrševanje varnostne politike

S stališča podjetja je izvrševanje varnostne politike za mobilne naprave zelo težko. Eden izmed ciljev je s programsko opremo zagotoviti avtomatizirano izvrševanje politike. Programska oprema mora izvrševati politiko z avtomatiziranimi pregledi še posebej zato, ker je nerealistično preverjati vsako mobilno napravo posebej. Poleg tega mora rešitev vključevati tudi mehanizme za prevajanje pravil programske opreme (Wang et al., 2014).

Prvi trije identificirani cilji so zelo pomembni za dosego varnega PSN okolja, vendar pa ugotavljam, da so nezadostni za popolno dosego varnega PSN okolja. Zadani cilj magistrskega dela je najti koncept PSN okolja, ki bo varno in hkrati sprejemljivo tako za

podjetje kot tudi za zaposlene. Zgornji cilji po našem mnenju niso dovolj varni in sprejemljivi za obe strani, ker ne upoštevajo varnost podatkov podjetja in zasebnosti zaposlenih v celoti. Tudi avtor Ocano (2015) ocenjuje, da je potrebno za popolno dosego varnega PSN okolja identificirati dodatne cilje, ki jih navajamo v nadaljevanju.

2.6.4 Popolna izolacija prostora

Čeprav je sama izolacija prostora dovolj za preprečitev izmenjave podatkov med osebnim prostorom in prostorom podjetja, za popolno varnost podatki podjetja ne bi smeli biti nikoli shranjeni v mobilnih napravah. Popolna izolacija prostora obravnava shranjevanje podatkov podjetja le na strežnike podjetja, hkrati pa preprečuje pošiljanje osebnih podatkov zaposlenih na strežnike podjetja. Na ta način podatki podjetja ostanejo varni tudi ob morebitni izgubi ali kraji mobilne naprave ali odhodu zaposlenega. Ta način rešuje tudi problem, ko podjetje izvede na mobilni napravi obnovitev na tovarniške privzete nastavitve in so s tem izgubljeni tudi vsi osebni podatki zaposlenih, kar pa z njihove strani nikakor ni zaželeno (Ocano, 2015).

2.6.5 Nevsiljivost

Z vidika zaposlenih PSN rešitev nikakor ne sme vplivati na zasebnost posameznega zaposlenega. Rešitev ne sme zahtevati nobenih privilegiranih dovoljenj na mobilnih napravah, prav tako tudi nameščeni agenti ali aplikacije, ki na zahtevo te rešitve iščejo, zbirajo in obdelujejo podatke v ozadju, ne smejo vdirati v osebni prostor zaposlenega. Nadalje, rešitev ne sme spreminjati operacijskega sistema in bralnega pomnilnika, ki bi kakorkoli vplivala na osnovno, začetno konfiguracijo mobilne naprave. Taka modifikacija lahko privede do razveljavitve garancije proizvajalca (Ocano, 2015).

2.6.6 Nizka poraba virov

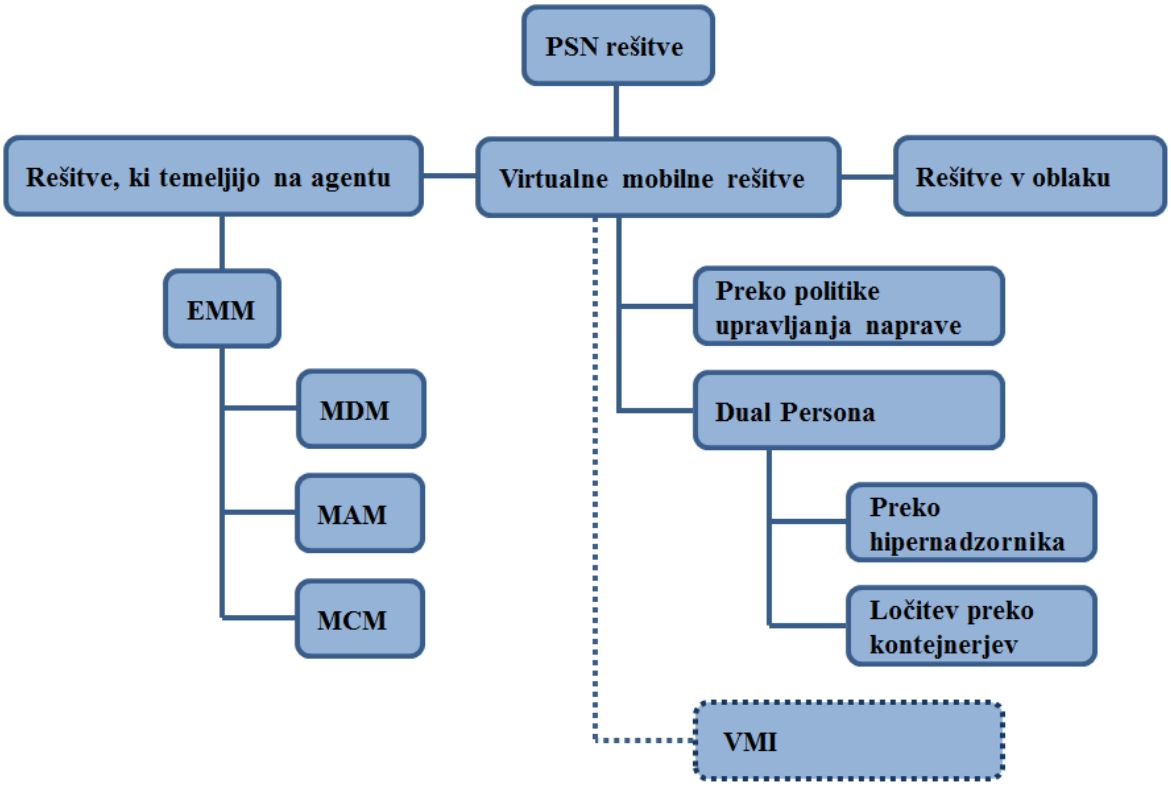
Vsaka rešitev mora upoštevati omejitve virov na mobilni napravi, ki jih glede hitrosti obdelave podatkov lahko zmorejo. Rešitve, ki zahtevajo veliko procesno moč in veliko bralno-pisalnega pomnilnika oz. RAM-a, lahko vplivajo na običajno obnašanje in delovanje mobilne naprave, kar bi lahko pripeljalo do upada sprejetja rešitve s strani zaposlenih. Poraba virov mobilne naprave mora biti zelo nizka (Ocano, 2015).

V tem poglavju smo navedli zahteve informacijske varnosti, kaj vse je opredeljeno v standardu ISO 27001, nakazali smo primer varnostne politike, navedli smo vsa tveganja, ki jih prinašajo mobilne naprave in ukrepe za zmanjšanje le teh ter identificirali najpomembnejše cilje za varno PSN okolje. V naslednjem poglavju bomo razpravljali o rešitvah, ki so na voljo za PSN, razvrstili jih bomo glede na tip rešitve in razpravljali o ciljih, ki jih dosegajo.

3 REŠITVE ZA NADZOR MOBILNIH NAPRAV

Pri pregledu literature in skozi raziskovalno delo ugotavljamo, da je na trgu več rešitev za nadzor mobilnih naprav. Kot smo že uvodoma ugotovili, je ena od rešitev za nadzor mobilnih naprav v PSN okolju, uporaba centraliziranega orodja za upravljanje z mobilnimi napravami, ki ga tudi priporoča NIST v svojem dokumentu Smernice za upravljanje in varovanje mobilnih naprav v podjetju iz leta 2013. Zadnja leta smo priča velikim spremembam na tem področju in za učinkovit nadzor mobilnih naprav ugotavljamo, da MDM potrebuje MAM in MCM, ki jih vse skupaj združujemo v EMM. Možne rešitve nadzora mobilnih naprav prikazuje Slika 21. Poleg rešitev EMM, ki temeljijo na agentu, so tu še virtualne mobilne rešitve in rešitve v oblaku. Vsaka od teh rešitev ima svoje značilnosti, ki jih bomo tudi podrobneje predstavili v nadaljevanju.

Slika 21: Taksonomija PSN rešitev



3.1 Rešitve, ki temeljijo na agentu

Rešitve, ki temeljijo na agentu zagotavljajo varnostno politiko in ostale značilnosti z namestitvijo mobilne aplikacije na PSN napravo. V omrežju oziroma v infrastrukturi podjetja je nameščena programska oprema, ki je pristojna za vzpostavitev in izvajanje nabora pravil in različnih profilov, ki jih bodo imele različne mobilne naprave. Mobilna aplikacija nameščena na mobilni napravi potrebuje posebne privilegije, saj se uporablja za uveljavitev

konfiguracije in profilov na podlagi pravil, ki so jih skrbno določili skrbniki omrežja in je del varnostne politike podjetja. Te rešitve so s stališča zaposlenih zelo moteče, kajti agent potrebuje posebne privilegije za spremljanje in uveljavljanje varnostnih politik na mobilni napravi. Zlasti je tu problem pri mobilnih napravah v lasti zaposlenih. Te rešitve ne zagotavljajo nobene oblike izolacije prostora, ker so vsi podatki, osebni in od podjetja, shranjeni na mobilni napravi. Prav tako tudi ne izpolnjujejo cilja nevsiljivosti, ker nekako vplivajo na zasebnost zaposlenega. V osnovi te rešitve niso potratne po virih mobilne naprave in lahko zagotavljajo varnost podatkov podjetja z uporabo kriptografije.

3.1.1 Upravljanje mobilnosti v podjetju – EMM

EMM pomaga podjetjem pri integraciji mobilnih naprav v svoj varnostni okvir ter življenjski cikel sistemov in informacijske tehnologije. Podjetja uporabljajo EMM orodja za opravljanje naslednjih funkcij za svoje uporabnike (Cosgrove et al., 2015):

- **Oskrbovanje**. Konfiguracija naprav za uporabo v poslovnem okolju.
- **Revizija, spremljanje in poročanje**. Ta orodja revidirajo mobilne naprave in aplikacije za spremljanje skladnosti s politiko podjetja. Prav tako so sposobna slediti uporabi storitev in aplikacij ter so sposobna vzdrževati evidenco stroškov.
- **Varovanje podatkov podjetja**. EMM orodja uporabljajo tehnologijo za šifriranje podatkov, nadzorujejo pretok podatkov in na daljavo prekličejo zaposlenemu dostop do mobilnih aplikacij in podatkov v primeru, da njegova naprava predstavlja grožnjo podjetju (npr. zaradi izgube ali kraje mobilne naprave, nepooblaščene konfiguracije naprave ali pa prenehanja zaposlitve).
- **Podpora**. EMM pomaga oddelku informacijske tehnologije pri odpravljanju težav na mobilnih napravah s pomočjo vodenja inventarja, analitike in uveljavljanjem ukrepov na daljavo.

EMM orodja pomagajo zagotoviti le zaupanja vrednim napravam in uporabnikom dostop do poslovnih aplikacij in podatkov z uporabo ene ali več tehnologij: z uporabniškimi certifikati, s certifikati ustreznosti naprave, s kodo izvedljivosti podpisane aplikacije, z mehanizmi overjanja in enotno prijavo v sistem. EMM orodja vse bolj uporabljajo informacije o lokaciji in času za pomoč pri obveščanju o dostopu (Cosgrove et al., 2015).

Obstaja več temeljnih tehničnih skupin EMM, ki pomagajo podjetjem in njihovim oddelkom informacijske tehnologije opravljati vse zgoraj omenjene funkcije. Ta so MDM, MAM in MCM. Med temi kategorijami obstajajo prekrivajoče zmogljivosti, ki jih podjetja glede na njihove zahteve lahko uporabijo v celoti ali delno.

3.1.1.1 Upravljanje mobilnih naprav - MDM

Glavni cilj MDM rešitve je spremljanje mobilne naprave, prenašanje aplikacijskih in uporabniških podatkov na enega ali več strežnikov in uveljavljanje politike z varnostnimi mehanizmi kot je npr. daljinsko brisanje podatkov na napravi. Agenta za delovanje uporabnik namesti iz tržnic programskih rešitev, ki so na voljo na javnih strežnikih ali pa strežnikih v lasti podjetja. S pomočjo agenta nameščenega na mobilni napravi lahko MDM strežnik izvaja ukaze na mobilni napravi v smislu nadzora, zaklepanja, šifriranja podatkov, preprečevanja uporabe senzorjev, preprečevanje uhajanja podatkov podjetja in uveljavljanje mobilne varnostne politike. Poleg tega MDM omogoča tudi distribucijo programske opreme na mobilne naprave. Če povzamemo, mora MDM rešitev imeti naslednje zmogljivosti in funkcije (Fortinet, b.l.; Gilmore & Beardmore, 2013; Svensk, 2013; Redman, 2013; Madden, 2014; Phifer, 2013):

- **Izvrševanje politike in skladnosti**:
  - odkrivanje in uveljavitev operacijskih sistemov in različic,
  - odkrivanje jail-broken iOS naprav in rooted Android naprav,
  - filtriranje oziroma omejitev dostopa z naprav, ki niso skladne, do strežnikov podjetja (npr. strežnika elektronske pošte),
  - omejevanje števila naprav na posameznega zaposlenega,
  - omejevanje nalaganja aplikacij preko belih in črnih seznamov,
  - spremljanje dostopa do trgovin z aplikacijami in prenosa aplikacij, dajanje prepovedanih aplikacij v karanteno, spremljanje dostopa do spletnih storitev, socialnih omrežij,
  - spletno filtriranje vsebin,
  - prepoznavanje kršitev politike podjetja in pošiljanje sporočil upravljavcem in zaposlenim o teh kršitvah,
  - upravljanje aplikacij podjetja na PSN napravah in upravljanje osebnih aplikacij na napravah podjetja,
  - označevanje vsebine z zastavicami kot osebne ali od podjetja,
  - omejevanje ali prepoved dostopa do strežnikov podjetja v primeru kršitev politike podjetja.
- **Upravljanje mobilne varnosti**. To je niz mehanizmov za zaščito poslovnih podatkov na napravah in sistemu za ohranitev skladnosti s predpisi:
  - izvrševanje dostopa z geslom,
  - zaklepanje naprave po npr. določenem času neaktivnosti,
  - daljinsko brisanje podatkov na napravi, selektivno ali popolnoma,
  - šifriranje podatkov na napravi,
  - overjanje s certifikati,
  - preprečevanje uhajanja občutljivih podatkov podjetja,
  - spremljanje naprav in manipulacija s podatki na napravah,

  - funkcije požarne pregrade,
  - proti virusna zaščita,
  - zaščita proti zlonamerni programski opremi,
  - možnost vzpostavitve varnih zasebnih povezav preko mobilnih naprav,
  - lociranje mobilnih naprav s sistemi za pozicioniranje,
  - arhiviranje sporočil in podatkov,
  - zaščita pred goljufivimi aplikacijami in v takem primeru možnost karantene.
- **Upravljanje mobilne programske opreme:**
  - mehanizmi za nadgradnje programske opreme preko omrežja (angl. *Over The Air – OTA*),
  - podpora operacijskim sistemom in različicam,
  - posodobitve programske opreme za aplikacije in operacijske sisteme,
  - sposobnost trgovine z aplikacijami,
  - izdelava varnostnih kopij,
  - ponovna vzpostavitev stanja iz varnostnih kopij,
  - sinhronizacija ure v okolja.
- **Razširljivost**:
  - visoka razpoložljivost (angl. *High Availability – HA*),
  - tehnike ponovne vzpostavitve sistema (angl. *Disaster Recovery*).
- **Implementacija**:
  - v podatkovnem centru podjetja z namensko napravo ali virtualno napravo,
  - programska oprema kot storitev (angl. S*oftware as a Service*, v nadaljevanju SaaS), kot gostovanje ali lasten oblak,
  - enostavnost izvedbe,
  - cenovna politika usmerjena na uporabnika, na napravo ali na trajno licenciranje.
- **Analitika**. Pristopi, ki se uporabljajo za podporo potrebe po podatkih podjetja:
  - poročanje,
  - nadzorna plošča (angl. *Dashboard*),
  - analiza,
  - raba programske opreme in raba omrežja.

MDM zagotavlja nadzor in upravljanje mobilnih naprav na varen način, ki je v glavnem v interesu podjetja. Večina podjetij je zainteresirana za uporabo MDM orodij za nadzor velikega števila mobilnih naprav, ki se pojavljajo v njihovem omrežju ter svojih mobilnih delavcev. Ker zaposleni lahko uporabljajo tudi svoje PSN naprave za dostop do elektronske pošte in do ključnih poslovnih aplikacij ter podatkov, ki so potrebni za njihovo delo, so bolj produktivni in bolj učinkoviti.

Kadarkoli uporabnik namesti katerokoli aplikacijo na svojo mobilno napravo preko tržnic programskih rešitev, lahko aplikacija zahteva dovoljenje za dostop do naslednjih funkcij (Vignesh & Asha, 2015):

- podrobnosti računa uporabnika;
- informacije o aplikaciji;
- telefonskih klicev;
- omrežne komunikacije;
- nastavitev sinhronizacije;
- sistemska orodja;
- lokacije;
- fotoaparata;
- zaznamkov ter zgodovine brskanja po spletu;
- pomnilnika.

Zgornji podatki o uporabniku, ki omogočajo dostop do storitve oziroma omogočajo delovanje aplikacije, so za uporabnike lahko zelo občutljivi, zaradi česar je mobilna naprava izpostavljena napadom in občutljivi podatki o napravi lahko uidejo brez njihove vednosti. MDM mora zato znati preprečiti ali omejiti namestitev problematičnih aplikacij na mobilne naprave. Uporabnika mora pred namestitvijo opozoriti (Vignesh & Asha, 2015).

Avtorji Wang et al. (2014) navajajo vrsto pomanjkljivosti MDM rešitev. Prvič, uporabniki imajo lahko več vlog v podjetju in tu je MDM pokazal, da ima težave s tovrstnimi scenariji. Drugič, podjetja imajo lahko sprejeto politiko, ki jo ni mogoče izvajati z MDM. In tretjič, ker izolacija prostora z MDM ni možna, je nemogoče izvajati različne varnostne politike za uporabniške podatke in aplikacije kar pa vodi v izgubo prožnosti v osebnem prostoru mobilne naprave zaposlenega.

Mnogi zaposleni imajo tudi občutek, da jih podjetje z uvedbo MDM orodij nenehno nadzoruje v smislu »veliki brat te opazuje« (angl. *big brother is watching you*), besedne zveze iz knjige *1984* Georga Orwella. Poleg zaklepanja naprave, daljinskega brisanja vseh podatkov na napravi, nadzora vseh aplikacij na napravi, tudi osebnih, je eden od glavnih vprašanj o zasebnosti sledenje njihovih lokacij s sistemi za pozicioniranje. Zaposleni seveda lahko izključijo lokacijske storitve in s tem onemogočijo lociranje, vendar je tu lahko problem v tem, da uporabniki tega ne znajo narediti ali pa da je politika MDM ustvarjena tako, da za delovanje zahteva lokacijske storitve (Madden, 2014).

S stališča ZVOP-1(UPB1) in Zakona o delovnih razmerjih (Ur.l. RS, št. 21/13, v nadaljevanju ZDR-1) je glede zgornjih vprašanj zasebnosti, še posebej kadar gre za PSN naprave, predvsem lahko problematično zbiranje informacij o naloženih aplikacijah. Imena mnogih aplikacij lahko kažejo na popolnoma zasebno sfero zaposlenega in celo na občutljive osebne podatke (npr. na spolno usmerjenost, na zdravstvene težave, na zasebne aktivnosti, itd.). Zbiranje takih informacij s strani delodajalca ni potrebno in primerno za izvajanje pogodbe o zaposlitvi, kot to določa ZDR-1. Prav tako je lahko na PSN napravah problematičen tudi izbris podatkov na daljavo, ki prav tako pomeni obdelavo osebnih

podatkov, ki se nahajajo na napravi (njihov izbris), zadeva pa vse osebne podatke, ki jih hrani uporabnik (fotografije, dokumente, video posnetke, ostale osebne podatke) in ne samo tiste, ki so na napravi in so v zvezi z delovnim razmerjem. Tudi pri službenih napravah je nerealno pričakovati, da bodo zaposleni te naprave uporabljali izključno za službene namene, kar pomeni, da se bodo neizogibno na napravah nahajali tudi osebni podatki zaposlenega. Pravne podlage za tako obdelavo osebnih podatkov tudi po mnenju Informacijskega pooblaščenca delodajalec nima (Uporaba sistema za upravljanje mobilnih naprav, 2016).

Ob hitro razvijajoči se tehnologiji postaja vprašanje zasebnosti na delovnem mestu vse bolj problematično. Na področju varstva osebnih podatkov v primeru dvoma razmerja pristojnosti delodajalca in svobode delavca, si razlagamo v prid zasebnosti. Primeri, ko bi bil delodajalčev poseg v zasebnost delavca na delovnem mestu dopusten, bi bili resnično izjemni in redki, predvsem pa odvisni od dejanskih okoliščin. Delodajalec je dolžan cilj, ki ga zasleduje (čim bolj racionalno izrabo delovnega časa in delovnih sredstev za doseganje poslovnih rezultatov), v našem primeru z uvedbo MDM orodij za nadzor mobilnih naprav, podpreti s čim manj invazivnimi in represivnimi ukrepi (Uporaba sistema za upravljanje mobilnih naprav, 2016).

3.1.1.2 Upravljanje mobilnih aplikacij - MAM

Glavni cilj orodja za upravljanje mobilnih aplikacij je obvladovanje in omejevanje mobilnih aplikacij na PSN napravah. MAM dovoljuje le pooblaščenim aplikacijam dostop do podatkov podjetja ter varuje aplikacije podjetja na mobilni napravi zaposlenega in jih hkrati ločuje od osebnih aplikacij (Ocano, 2015). MAM uporablja funkcijo upravljanja in nadzora politike posameznih aplikacij, ki so nato dostavljene preko trgovin z aplikacijami in upravljane lokalno na mobilni napravi preko EMM konzole. Ta zmožnost je potrebna, kadar operacijski sistem ne zagotavlja ustreznega upravljanja, varnostne zmogljivosti ali pa ko se podjetje odloči, da se ne namesti MDM agenta na mobilno napravo. MAM lahko zagotovi tudi anane zmogljivosti, s pomočjo katerih lahko administratorji in lastniki aplikacij razumejo vzorce uporabe. Obstajata dve osnovni obliki MAM (Cosgrove et al., 2015):

- **prednastavljena aplikacija**; EMM proizvajalci ponujajo lastniške mobilne aplikacije ali pa jih integrirajo z določenimi aplikacijami tretjih oseb za zagotavljanje izboljšanja ravni upravljanja. Te najpogosteje vključujejo produktivnost in sodelovanje aplikacij kot je varen brskalnik in varno upravljanje zasebnih podatkov (angl. *Personal Information Manager – PIM*) za elektronsko pošto, koledar in upravljanje stikov;
- **aplikacijske razširitve**; te uporabljajo politike do aplikacij preko uporabe paketa za razvoj programske opreme (angl. *Software Development Kit – SDK*) ali preko oblivanja (angl. *Wrapping*).

Razlika med MDM in MAM rešitvami je v tem, da prva opravlja nadzor na ravni strojne opreme, slednja pa nadzoruje programsko opremo na mobilni napravi. Posledično se lahko politiko podjetja izvrši le na aplikacije v zvezi s podjetjem. MDM in MAM sta komplementarni rešitvi, to je tudi razlog, da so MAM rešitve del MDM rešitev. Ker MAM ne zagotavlja popolne zaščite za mobilne naprave, mora MDM vsebovati tudi orodje za upravljanje mobilnih vsebin – MCM.

3.1.1.3 Upravljanje mobilnih vsebin - MCM

Orodje za upravljanje mobilnih vsebin obsega skupek tehnologij, ki zagotavljajo varen dostop do občutljivih podatkov podjetja na mobilnih napravah in se uporablja za zavarovanje vseh podatkov, ki se nahajajo na mobilni napravi (Rouse, 2014).

MCM vsebuje niz mehanizmov za podporo sinhronizacije, souporabe in distribucije datotek. Osredotoča se na varno upravljanje dokumentov z overjanjem, avtorizacijo in dostopom. Uporabniki pridobijo dostop do vsebin z uporabniškimi imeni, gesli, naslovi IP in overjanjem pristnosti mobilne naprave. MCM rešitve običajno uporabljajo metode večstopenjskega overjanja za odobritev in upravljanje dostopa do odlagališč in dokumentov. MCM znotraj EMM ima štiri temeljne naloge (Cosgrove et al., 2015):

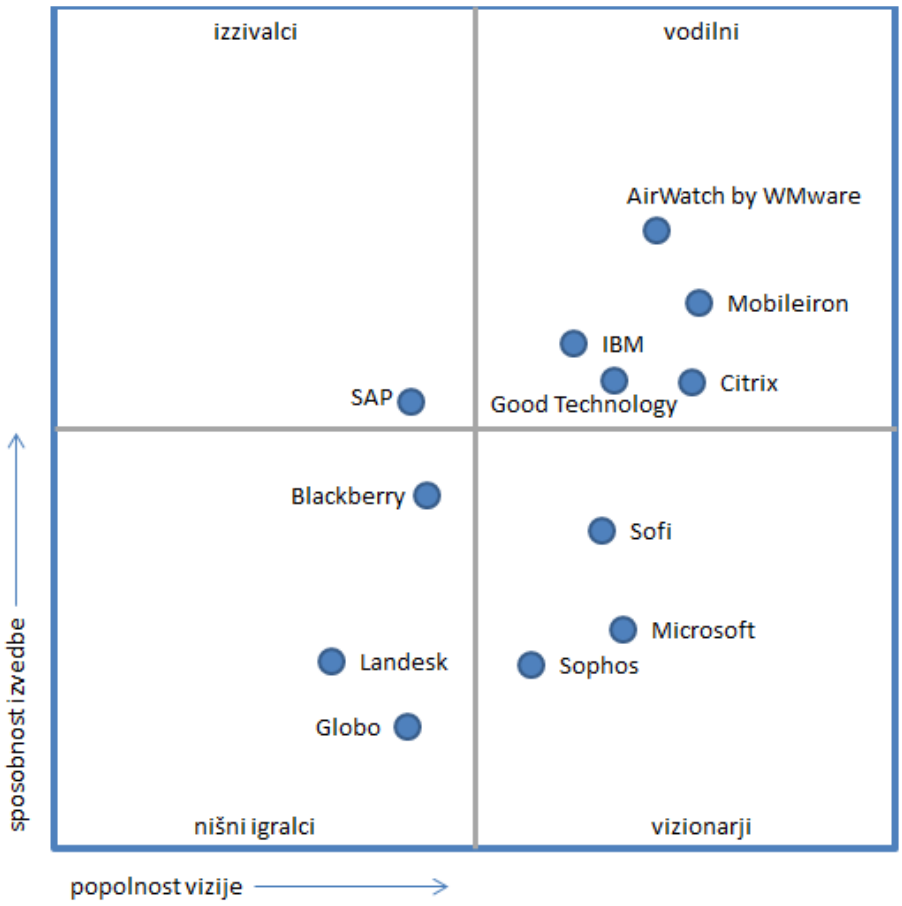
- Aplikacija na strani odjemalca omogoča uporabniku varno shranjevanje vsebin na mobilno napravo. EMM lahko izvršuje politiko kot je overjanje, izmenjava podatkov in omejevanje funkcije kopiraj-prilepi. Vsebina prihaja iz virov kot so priloge elektronski pošti, podatki iz zalednega dela sistema ali podatki iz oblaka.
- Dostop do vsebine. To je povezava z zalednim delom odlagališča, kjer uporabniki potegnejo vsebino na njihove naprave.
- Potisni vsebino. Te zmogljivosti vključujejo distribucijo datotek, njihovo zamenjavo in izbris na funkciji potisni.
- Zaščita na ravni datoteke. EMM orodja ne zagotavljajo popolno zaščito pred izgubo podatkov in niso popolni produkti upravljanja informacijskih pravic (angl. *Information Rights Management – IRM*), vendar pa se lahko uporabljajo kot zaščita na ravni datotek v nekaterih mobilnih okoljih in jih tako lahko vključimo v večji okvir.

Pri pregledu trga rešitev EMM smo si pomagali z analizo Gartnerja, ki je eden od vodilnih svetovnih neodvisnih ponudnikov raziskav in analiz na področju informacijske tehnologije. V svojih analizah predstavlja čarobni kvadrant ponudnikov na različnih področjih, ki prednjačijo pred drugimi. V svoji klasifikaciji upošteva privlačnost produkta, tržni delež proizvajalca, njegovo strategijo, inovacije, poslovni model in podporo, tržne aktivnosti, kot tudi tržne aktivnosti konkurence. Upošteva tudi pretekle in trenutne aktivnosti ponudnika na tem področju. Analiza nam lahko olajša pomoč pri izbiri oziroma ožji selekciji rešitev pri nakupu. Na sliki 22 je prikazan čarobni kvadrant EMM rešitev.

Po Gartnerju na področju EMM prednjačijo rešitve VMware Airwatch (Mobile Device Management, 2016), MobileIron (MobileIron Product Overview, 2016), Citrix XenMobile (XenMobile, 2016) in IBM MobileFirst (MobileFirst, 2016). Po pregledu njihove uporabniške dokumentacije in podatkov s spletnih strani lahko zaključimo, da vse zgoraj omenjene EMM rešitve v večini izpolnjujejo zmogljivosti in funkcije, ki jih mora imeti vsako dobro orodje za nadzor mobilnih naprav. Zagotavljajo podobne funkcije v smislu:

- oblikovanja konfiguracij;
- ukrepov, ki jih je mogoče sprejeti na mobilnih napravah;
- različnih vrst podprtih mobilnih operacijskih sistemov na njihovih platformah (podpora za android, iOS in drugih);
- odkrivanja jail-broken iOS naprav in rooted Android naprav;
- integracija z AD in LDAP;
- daljinskega brisanja podatkov na napravi;
- šifriranja podatkov.

Slika 22: Gartnerjev čarobni kvadrant EMM rešitev



Vir: T. Cosgrove et al., Magic Quadrant for Enterprise Mobility Management Suites, 2015, str. 2.

Vendar pa obstajajo tudi razlike v smislu, kje je implementacija izvedena, glede na to, da nekateri omogočajo le implementacijo v oblaku. Nadalje, možnosti zaznavanja zlonamerne kode, možnosti požarne pregrade in lociranja mobilnih naprav, ki podjetjem omogoča uveljavljanje politike temelječe na lokaciji, kje se mobilna naprava nahaja.

3.2 Rešitve v oblaku

Rešitve v oblaku temeljijo na pomnilniškem prostoru v oblaku (angl. *Cloud Storage*), ki uporabnikom omogoča mobilni dostop do podatkov, shranjevanje in uporabo le teh, kot tudi uporabo aplikacij v oblaku. Te rešitve zagotavljajo izolacijo prostora, saj so lahko osebni podatki zaposlenega shranjeni na mobilni naprave, medtem ko so podatki podjetja shranjeni v oblaku. Osebni podatki zaposlenih se lahko tudi shranijo v oblaku, v drugo odlagališče. Popolna izolacija prostora je pri rešitvah v oblaku prav tako zagotovljena, ko podatki podjetja nikoli ne gostujejo na mobilnih napravah zaposlenih. V primeru, da so podatki preneseni na mobilno napravo, popolna izolacija prostora ni več zagotovljena. Nadalje, dostop do podatkov podjetja v oblaku mora biti pravilno nastavljen in upravljan, bodisi s strani sistemskega upravljavca ali uporabnika (Leavitt, 2013).

Poleg vsega omenjenega te rešitve zagotavljajo tudi zaščito poslovnih podatkov, ker rešitve v oblaku nudijo tudi algoritme šifriranja. Rešitve v oblaku tudi niso moteče za zaposlene, saj ni potrebe po namestitvi dodatne programske opreme na njihovo mobilno napravo za dostop do podatkov v oblaku. Do podatkov lahko dostopajo preko privzetega spletnega brskalnika. Mnogo ponudnikov pa že ponuja namenske mobilne aplikacije za dostop do skladišč podatkov. Rešitve v oblaku od mobilnih naprav tudi ne zahtevajo prav visoke porabe virov, samo mrežno povezljivost (Ocano, 2015).

Za večino podjetij rešitve v oblaku ne izpolnjujejo njihovih potreb in zahtev glede varnostne politike podjetja. Da bi zadostili svojim potrebam, se podjetja večkrat zaradi tega obrnejo na rešitve tretjih oseb, kar pa lahko pomeni s stališča varnosti določeno stopnjo tveganja zaradi izgube stopnje zaupanja do ponudnika rešitev v oblaku in nadzora nad svojimi podatki. V vsakem primeru bi morala podjetja imeti določeno stopnjo zaupanja v ponudnike rešitev v oblaku v smislu zagotavljanja varnostnih ukrepov, ki jih izvajajo in v smislu upravljanja storitev.

Kljub temu, da večina proizvajalcev EMM rešitev danes ponuja implementacije v oblaku za nadzor mobilnih naprav, se bomo v nadaljevanju osredotočili le na ponudnike SaaS. Programska oprema, kot storitev, pomeni zagotavljanje celotne infrastrukture skupaj s programsko opremo in nastavitvami za njeno delovanje (Informacijski pooblaščenec RS, 2012). Je model rešitve v oblaku, ki ponuja aplikacije na zahtevo, jih upravlja ponudnik teh storitev in so običajno plačljive na podlagi naročnine. Pred rešitvami, ki jih podjetja implementirajo lokalno, imajo več prednosti: minimalno upravljanje in vzdrževanje, dostop

kjerkoli in kadarkoli, izboljšana komunikacija in sodelovanje. V mnogih primerih so te rešitve tudi cenejše (Sullivan, 2014).

Po pregledu trga rešitev v oblaku smo ugotovili, da je rešitev za podjetja za nadzor mobilnih naprav več. Med njimi najbolj prednjačijo Googlova storitev Google Apps (Google, b.l.), Microsoftova storitev Office 365 Enterprise (Office 365 Enterprise E5, 2016), Dropbox (Dropbox Business User Guide, 2016) in Box (Top Five Ways Any Business Can Benefit from Box, 2016). Po pregledu njihove uporabniške dokumentacije in podatkov s spletnih strani lahko zaključimo, da zagotavljajo in izpolnjujejo vse lastnosti, primerne za podjetja, vključno s podporo PSN.

3.3 Virtualne mobilne rešitve

Da bi dosegli sprejetje PSN koncepta v podjetjih, postajajo virtualne mobilne rešitve zelo privlačna izbira, saj zagotavljajo tako zaposlenim kot podjetjem prilagodljivost ob obravnavi pomislekov glede zasebnosti zaposlenih in izpolnjevanje varnostnih zahtev podjetja. Dopuščanje PSN naprav v podjetja zahteva politiko, ki določa, kako se bodo naprave uporabljale in na kakšen način se bodo upravljale ob ohranitvi prilagodljivosti zaposlenega. V zadnjih nekaj letih je bilo razvitih kar nekaj tehnologij za mobilno virtualizacijo, ki segajo od politike upravljanja naprave (angl. *Device Management Policy – DMP*) do rešitev z dvojno osebnostjo (angl. *Dual Persona*, v nadaljevanju dual persona), virtualizacijo preko hipernadzornika (angl. *Hypervisor*, v nadaljevanju hipernadzornik) do členitve na osnovi kontejnerjev (angl. *Container Based Separation*) (Jaramillo et al., 2014).

3.3.1 Mobilna virtualizacija preko politike upravljanja naprave

Mobilno členitev je mogoče doseči z uporabo varnostne politike informacijske tehnologije, ki jih MDM sistem upravlja. Ta oblika pristopa se izvede s pristopom upravljanja na osnovi strežnika, ki omogoča upravljavcem informacijske tehnologije uveljavljanje politike po vsej uporabniški bazi. Uporablja se lahko za celotno skupnost ali pa za posamezno skupino uporabnikov, ki jo je mogoče prilagoditi stopnji varnosti na skupino. Na primer, vodilni v podjetju imajo lahko strožji niz pravil, ki vključuje šifriranje naprave (Jaramillo et al., 2014). Predstavnika te virtualizacije sta MobileIron Virtual Smartphone Platform (MobileIron, 2010) in Good Technologies, ki ga je konec leta 2015 kupil BlackBerry (Blackberry completes Good Technology Acquisition, 2016).

3.3.2 Dual persona

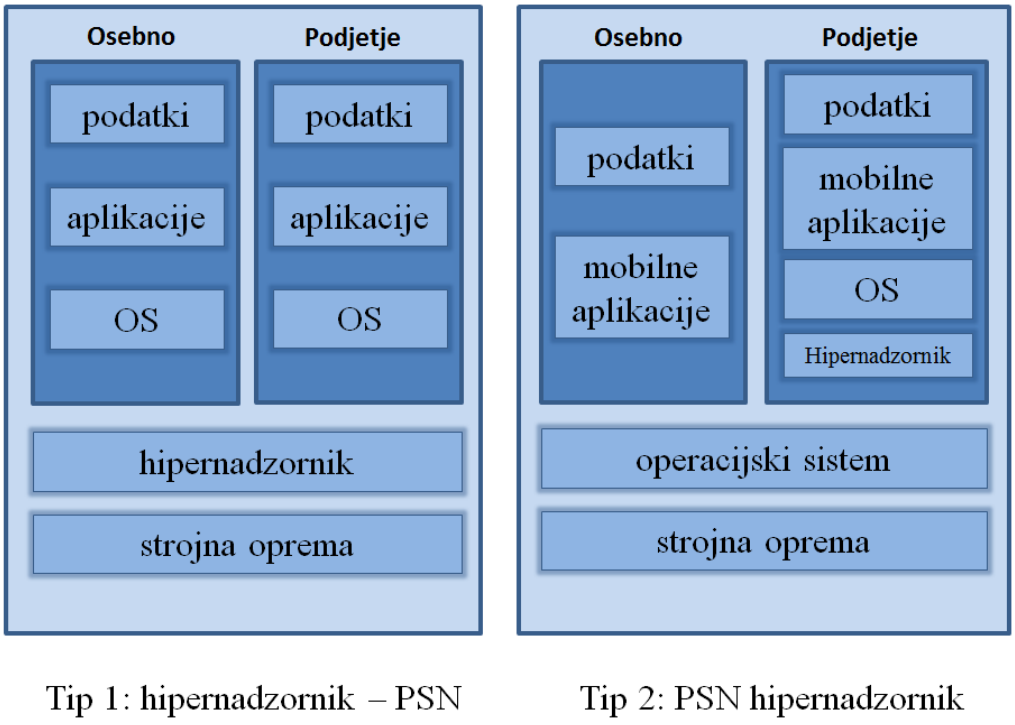
Dual persona spremeni mobilno napravo na dve osebnosti, ki delujeta kot dve izolirani napravi, ena za poslovna opravila in druga za osebno uporabo. Zaposleni tako dobijo popoln nadzor nad osebno »persono«, kjer vse aplikacije, podatki in aktivnosti ostanejo nevidni

delodajalcu. Hkrati pa podjetje dobi popoln nadzor nad delovno »persono«, vključno s sposobnostjo zagotavljanja celovitosti operacijskega sistema, uveljavljanje varnostne politike in daljinsko namestitvijo s strani podjetja odobrenih aplikacij. Dual persona tudi preprečuje, da poslovne aplikacije ne ogrožajo uporabnikove neodobrene osebne aplikacije (Phifer, 2014). Cilj dual persone je zagotoviti podjetju, da so njihove aplikacije in pripadajoči podatki ločeni in zaščiteni na mobilni napravi zaposlenega. Hkrati pa za zaščito zasebnosti zaposlenega poskrbi, da podjetje lahko upravlja in vidi le aplikacije in podatke v poslovni »personi«. V primeru brisanja podatkov podjetja na napravi, ostanejo aplikacije in osebni podatki zaposlenega nedotaknjeni. Pri vpeljavi koncepta PSN, tehnologija dual persona nekako uresničuje nadzor nad osebnimi napravami zaposlenih, ne da bi pri tem podjetje kršilo pravico do zasebnosti zaposlenih (Rouse, 2012). Obstajata dva pristopa k dual personi, mobilna virtualizacija preko hipernadzornika in mobilna ločitev preko kontejnerjev.

3.3.2.1 Mobilna virtualizacija preko hipernadzornika

Virtualizacija preko hipernadzornika daje možnost dvema ali več instancam operacijskega sistema, da tečejo na isti mobilni napravi. S tem je omogočeno, da lahko osebne aplikacije tečejo na enem operacijskem sistemu, poslovne pa na drugem.

Slika 23: Virtualizacija preko hipernadzornika



Tip 1: hipernadzornik – PSN Tip 2: PSN hipernadzornik

Vir: D. Jaramillo et al., Virtualization techniques for mobile systems, 2014, str. 7.

Obstajata dva tipa virtualizacije (Slika 23) (Jaramillo et al., 2014):

- **Tip 1: virtualizacija gole kovine** (angl. *Bare Metal Virtualization*), ki teče na ravni strojne opreme mobilne naprave, ima neposreden dostop do virov strojne opreme in lahko gosti več operacijskih sistemov. Ker imamo neposreden nadzor nad strojno opremo, lahko zmogljivost operacijskega sistema prilagajamo.
- **Tip 2: gostujoča virtualizacija** (angl. *Hosted Virtualization*), ki teče znotraj gostujočega okolja mobilnega operacijskega sistema. Namestitev hipernadzornika se izvede na vrhu gostujočega operacijskega sistema kot vsaka druga aplikacija. Zmogljivost gostujočega operacijskega sistema pa je močno odvisna od zmogljivosti operacijskega sistema gostitelja.

Predstavniki virtualizacije preko hipernadzornika so Linux KVM/ARM (Dall & Nieh, 2014), Cells (Andrus et al., 2011), Xen on ARM (Wafaa, 2014), Cellrox (Thinvisor, 2016), VMWare (VMware to Bring Virtualization to Mobile Phones, Enabling a Host of Benefits for Handset Vendors, Corporations and Mobile Phone Users, 2016) in Google (b.l.).

3.3.2.2 Mobilna ločitev preko kontejnerjev

Ta pristop zagotavlja ločitev na mobilni napravi preko aplikacijskih kontejnerjev, doseže se z uporabo rešitve podobne Unix metodi večkratnih uporabnikov, kjer je več uporabnikov hkrati prijavljenih na eno napravo in vsak ima svojo izkušnjo. Vse uporabniške seje tečejo vzporedno, z enim jedrom in enim operacijskim sistemom (Jaramillo et al., 2014). Predstavnika te tehnologije sta TrustDroid (Zhao & Osorio, 2012) in Samsung Knox (Knox Workspace, 2016).

3.4 Primerjava rešitev za nadzor mobilnih naprav s cilji varnega PSN okolja

V Tabeli 2 smo povzeli vse rešitve za nadzor mobilnih naprav in jih primerjali s postavljenimi cilji za varno PSN okolje. Namen primerjave ni bil primerjati rešitve med seboj v smislu funkcionalnosti in značilnosti, ampak primerjati s cilji, ki smo jih identificirali v drugem poglavju. Ugotavljamo, da nobena od rešitev za nadzor mobilnih naprav iz tega poglavja ne dosega želenega cilja, to je varnega PSN okolja.

V tem poglavju smo identificirali možne rešitve za nadzor mobilnih naprav in jih podrobneje predstavili ter jih na koncu primerjali s cilji za varno PSN okolje in ugotovili, da z nobeno rešitvijo ne moremo doseči popolnoma varnega PSN okolja.

V nadaljevanju se bomo posvetili virtualizaciji mobilnih naprav, ki naj bi dosegala cilje varnega PSN okolja.

Tabela 2: Primerjava rešitev za nadzor mobilnih naprav s cilji varnega PSN okolja

	Rešitve za nadzor mobilnih naprav		
Želeni cilji	**EMM**	**Rešitve v oblaku**	**Virtualne rešitve**
Izolacija prostora		✓	✓
Varovanje podatkov podjetja	✓	✓	✓
Izvrševanje varnostne politike	✓		
Popolna izolacija prostora			
Nevsiljivost			
Nizka poraba virov	✓		

4 VIRTUALIZACIJA MOBILNIH NAPRAV – VMI

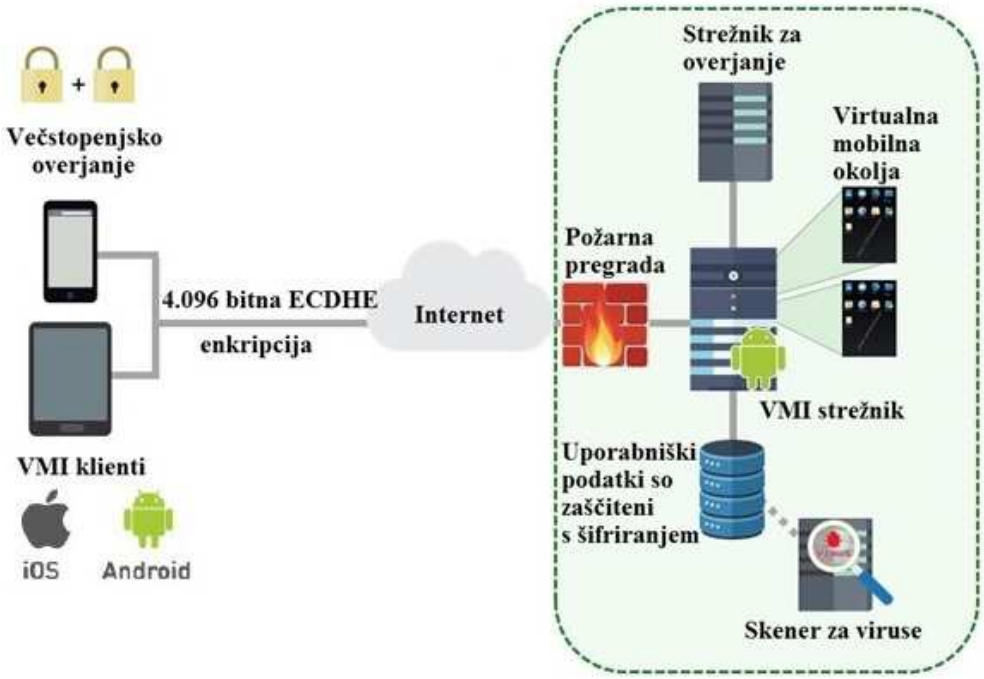
VMI je namestitev po meri izdelanega mobilnega operacijskega sistema na navidezno napravo (angl. v*irtual machine*, v nadaljevanju VM) na oddaljenem strežniku v javnem ali zasebnem oblaku. Vsaka navidezna naprava omogoča več uporabniških sej. Vsaka seja ponuja virtualno mobilno okolje, kjer uporabniki dostopajo do mobilnih aplikacij, ki so nato prikazane na posamezni mobilni napravi. Te aplikacije so lahko celoten spekter mobilnih aplikacij za potrebe zaposlenih, od aplikacij za elektronsko pošto do specifičnih poslovnih aplikacij, ki jih podjetje uporablja. Glede na to, da se te aplikacije nahajajo na enem mestu v podatkovnem centru, ni potrebno, da jih posamezno zavarujemo. Že sama povezava med mobilno in navidezno napravo, kjer se te aplikacije nahajajo, je šifrirana. Za povezavo se uporablja protokol oddaljenega prikazovalnika (angl. *Remote Display Protocol*, v nadaljevanju RDP), ki podpira dotik ekrana. Večina RDP temelji na kompresijskem formatu H.264 ali Motion JPEG. Gre torej za strežniško infrastrukturo v javnem ali zasebnem oblaku podjetja, na katerem teče mobilni operacijski sistem, implementacija virtualnih mobilnih naprav, uporabnik pa do nje dostopa s pomočjo odjemalca na svoji mobilni napravi. Ti odjemalci lahko tečejo na kateremkoli mobilnem operacijskem sistemu. Virtualizirani operacijski sistem strežniškega okolja mora biti mobilni operacijski sistem Android, ker je odprtokodne narave in edina platforma, ki jo VMI ponudniki potrebujejo. To pa ne pomeni, da VMI ne deluje z drugimi platformami.

Podjetja se morajo le zavedati, da pri razvoju delovnih aplikacij uporabljajo Android platformo, ker ima Apple stroge omejitve glede strojne opreme, na kateri lahko teče njihov iOS. Je pa potrebno tudi omeniti, da je za delovanje VMI potrebno razviti le eno Android verzijo aplikacije. Glede same varnosti se tako lahko zanašamo na celoten sistem VMI. To pomeni, da je breme razvijanja in varovanja te aplikacije nižje, kajti VMI kot tak poskrbi za varnost in razpršeno oddajanje (angl. *Broadcastin*g) na več naprav hkrati.

Na Sliki 24 je prikazana tipična namestitev VMI okolja za mala podjetja z vsemi potrebnimi komponentami, kjer mobilne naprave dostopajo do VMI strežnika, ki gostuje na mobilnih aplikacijah. VMI strežnik zaključuje SSL povezave, overja uporabnike in usmerja povezave z enim ali več Androidovim virtualnim mobilnim okoljem. Pri podjetjih z manj kot 100 uporabniki lahko VMI strežnik enostavno implementiramo kar na osebni računalnik z najmanj naslednjimi predlaganimi karakteristikami:

- Core-i7-6700 centralno procesno enoto (angl. *Central Processing Unit*, v nadaljevanju CPU) s štirimi jedri;
- 8GB RAMa;
- 128GB SSD diska;
- e-SATA RAID1 za shranjevanje varnostnih kopij.

Slika 24: Primer VMI okolja za mala podjetja



Vir: Sierraware, Mobile Security Checklist: An Easy, Achievable Plan for Security and Compliance, 2016, str. 5.

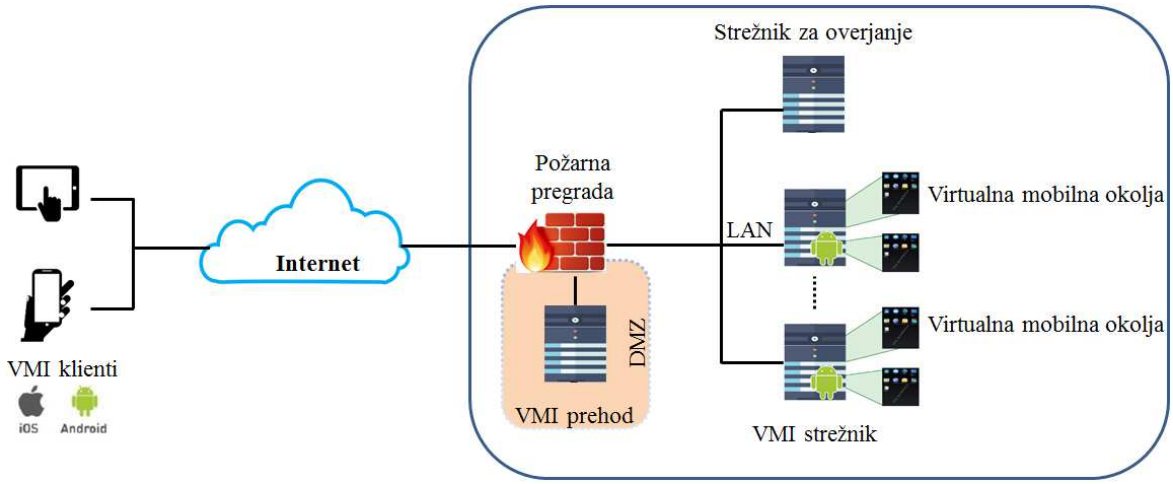
Zgoraj navedena priporočila so namenjena za osnovne poslovne aplikacije, kot so urejevalniki besedil, e-poštni odjemalci in spletni brskalniki. Za podjetja nad sto uporabniki in poslovnimi aplikacijami, ki zahtevajo večjo procesno moč, pa je potrebno v okolje poleg VMI strežnika postaviti tudi VMI prehod (angl. *Gateway*) v demilitarizirano okolje zaradi izolacije pred notranjim omrežjem (Slika 25). Podjetja, ki imajo še več uporabnikov, lahko

uporabijo več VMI strežnikov za porazdelitev bremena. VMI strežnik in VMI prehod za srednja in večja podjetja morata imeti najmanj naslednje predlagane karakteristike:

- CPU Xeon 2640v3 x2 z osmimi jedri, 2.6Ghz;
- 128GB RAMa;
- 750+ napajalnik,;
- 6T trdega diska za VMI strežnik in 512GB SSD diska za VMI prehod;
- omrežno kartico 4x10G Intel X710 NIC;
- e-SATA RAID5 za shranjevanje varnostnih kopij.

VMI strežnik mora opraviti večino zahtev gostovanja aplikacij in kodiranja. Zato mora biti strojna oprema VMI strežnika pogosto močnejša in zmogljivejša od VMI prehoda. Pri dimenzioniranju strežnikov je potrebno upoštevati število sočasnih uporabnikovih sej, ki jih namerava podjetje v svojem oblaku zaključevati, in zahteve po grafično intenzivnih aplikacijah, ki zahtevajo bolj zmogljive procesorje in grafične procesne enote (angl. G*raphics Processing Unit*, v nadaljevanju GPU). Podjetja morajo upoštevati, da uporaba mobilnih aplikacij narašča in da je potrebno razmisliti o dodelitvi dodatnih zmogljivosti za obvladovanje te rasti že sedaj. S tem bo zagotovljena podpora VMI zahtevam danes in v prihodnosti.

Slika 25: Primer VMI okolja za srednja in večja podjetja



Pri vpeljavi VMI okolja morajo podjetja vključiti naslednje komponente in ukrepe za zmanjšanje tveganj (Sierraware, 2016):

- Močno overjanje. Da bi preprečili nepooblaščene dostope in napade z ugibanji gesel, morajo podjetja uveljaviti močno overjanje, najbolje večstopenjsko. Glavni trije dejavniki za preverjanje pristnosti so; nekaj, kar uporabnik ve (geslo ali PIN), nekaj, kar

uporabnik ima (mobilno napravo) in nekaj, kar uporabnik je (prstni odtis). Preverjanje pristnosti z geslom lahko združimo s certifikatom odjemalca ali ID napravo, ali pa z enkratnim geslom, kar bistveno zmanjša nevarnost nepooblaščenega dostopa. Podjetja lahko izvajajo tudi časovne in lokacijske omejitve za preprečevanje goljufij.

- Močno šifriranje mobilnih komunikacij. Podjetja morajo zagotoviti šifriranje komunikacije med mobilnimi aplikacijami in strežniki aplikacij. Močno šifriranje, ki temelji na 4.096 bitnem SSL ključu in sejni izmenjavi ključev, lahko prepreči tudi zelo usposobljenim hekerjem dešifriranje komunikacije. Poleg šifriranja prometa je pomembno tudi šifriranje podatkov na mobilnih napravah. Podjetja bi morda želela v celoti preprečiti prenos občutljivih podatkov podjetja na napravo zaposlenega.
- Nadzor in spremljanje okolja ter spremljanje aktivnosti uporabnika. Ohranjanje podrobne revizijske sledi je pomemben način za ugotavljanje internih zlorab, naključnega uhajanja podatkov in celo zlonamerne programske opreme. Če mobilni uporabniki lahko pregledujejo in urejajo zaupne informacije podjetja, potem bi moralo podjetje spremljati njihove aktivnosti. Prijavna sporočila določajo kdaj uporabniki dostopajo do poslovnih aplikacij, sledijo uporabnikovo lokacijo in ID naprave. Podatke o neuspešnih prijavah in ostalih napakah je ravno tako potrebno zapisati. Pri zelo občutljivih aplikacijah lahko podjetje tudi snema mobilne uporabniške seje in s tem ugotovi kdo je naredil kaj in videl rezultate z uporabniškega vidika. Snemanje mobilnega zaslona prinaša popolno sliko uporabnikove dejavnosti. Pri spremljanju aktivnosti morajo biti zaposleni obveščeni in dati soglasje za spremljanje. Nadzorna komponenta poskrbi tudi za aktivacijo uporabnikov, vzpostavljanje sej, prijavo in odjavo uporabnikov, porazdeljevanje bremen med uporabniškimi virtualnimi napravami, sinhronizacijo z datotečnimi sistemi, sinhronizacijo med uporabnikom in prehodom omrežja (angl. *Gateway*).
- Preprečiti uhajanje podatkov. Ustvarjanje varnih mobilnih okolij preprečuje zlonamerni programski opremi dostop do aplikacij podjetja in onemogoči uporabnikom kopiranje, shranjevanje ali distribucijo občutljivih podatkov. Nadalje, podjetja morajo pri preprečitvi uhajanju podatkov preprečiti prenos občutljivih podatkov na mobilne naprave, blokirati posnetke zaslona in funkcijo odložišča, uvesti vodni žig na vseh zaupnih datotekah in video posnetkih (Mason, 2016).
- Skeniranje mobilnih aplikacij za malwareom in virusi. Odpravljanje malware in oglaševalskega programja s testiranji aplikacije za zlonamerna vedenja. Malware je mogoče odkriti z uporabo virtualnega peskovnika ali z orodji za skeniranje, ki temeljijo na podpisih. Skeniranje naj se opravlja na strežniku.
- Izobraževanje uporabnikov o mobilnih varnostnih tveganjih.

VMI prinaša podjetjem veliko koristi (Madden, 2015):

- nobenega podatka ni shranjenega na napravi zaposlenih, kar je zagotovo dobro v smislu uhajanja podatkov podjetja;

- vse poslovne aplikacije tečejo na strežnikih v podatkovnih centrih podjetja;
- aplikacije podjetja so ločene od osebnih aplikacij in hkrati zavarovane, zato ni potrebe po daljinskem brisanju podatkov na napravi ali omejevanju uporabniške izkušnje za osebne aplikacije, kar je zagotovo dobro v smislu zasebnosti zaposlenih;
- ni zaskrbljenosti glede varnosti samih mobilnih naprav;
- VMI zagotavlja ustrezen in sprejemljiv uporabniški vmesnik;
- VMI daje popoln nadzor nad mobilnim operacijskim sistemom, ki se ga z lahkoto prilagaja, nadzoruje nadgradnjo, določi dovoljenja in se ga lahko zaklene, kakor koli hočemo.

Prve implementacije VMI so se pojavile v Ministrstvu za obrambo in vojski Združenih držav Amerike, ki vlagajo v mobilno virtualizacijo že vrsto let. Veliko pozornosti pa VMI privablja tudi v ostalih sektorjih, kjer se osredotoča predvsem na reševanje težav novih potrošniških tehnologij v podjetjih (Sheldon, 2015).

Pri VMI je nujno potrebno upoštevati kontekst celotnega mobilnega prostora v podjetju, vključno z vsemi najnovejšimi zmožnostmi različnih oblik upravljanja mobilnih naprav, mobilnega upravljanja z aplikacijami, mobilne varnosti in mobilnih naprav (Madden, 2015). Za popoln nadzor mobilnih naprav, njihovo spremljanje in zaščito potrebujemo skupek orodij, ki jih zagotavljajo MDM, MAM in MCM hkrati. Kot smo že uvodoma ugotovili, se ta orodja zaradi vedno večjih zahtev mobilnega trga le še dopolnjujejo, postajajo čedalje bolj okorna, težko se jih upravlja, sama implementacija pa zahteva veliko časa, denarja in znanja.

Predvidevamo, da če je VMI dovolj varen za mobilne aplikacije vojske in Ministrstva za obrambo Združenih držav Amerike, potem je zagotovo primeren tudi za ostala podjetja v drugih sektorjih delovanja, ki so varnostno osveščena.

4.1 Pregled trga VMI rešitev

Pri temeljitem pregledu trga komercialnih VMI rešitev smo ugotovili, da se trenutno z virtualizacijo mobilnih naprav ukvarja šest podjetij, in sicer Remotium/Avast Software, Sierraware, Nubo Software, Hypori, Raytheon in Trend Micro. Odzvalo se je pet podjetij, razen Hyporija. Raytheon in Trend Micro trenutno še razvijata svojo VMI rešitev za potrebe področja farmacevtske industrije in še nimata dokončne rešitve.

V nadaljevanju bomo podrobno opisali vsako rešitev posebej. Preverili bomo ali zadostujejo ciljem in kriterijem z vidika podjetja in zaposlenih po varnem in sprejemljivem PSN okolju. Prva dva krovna kriterija, ki nas zanimata v smislu primernosti PSN koncepta, sta cena in podpora ponudnika. Ponudniki VMI rešitev imajo poslovni model s prodajo kupcem preko partnerjev. Za pridobitev partnerskega statusa se morajo partnerji ustrezno izobraziti. Podpora podjetjem je tako zagotovljena preko partnerjev. Cenik je pri vseh treh ponudnikih

sestavljen na podlagi licenciranja s ceno na uporabnika. Glede na to, da je tehnologija relativno nova, ponudniki VMI rešitev za našo regijo še nimajo izdelanih cen. Zagotavljajo pa, da je lahko cena na uporabnika za več kot polovico nižja, kot pri ostalih EMM rešitvah za nadzor mobilnih naprav. Ostali kriteriji, s katerimi bomo primerjali rešitve med seboj, so naslednji:

- namestitev strežniškega okolja v podjetje. Zanima nas kompleksnost izvedbe, kdo je izvajalec postavitve in kakšne kadrovske vire potrebujemo;
- v kakšnem virtualnem okolju lahko poganjamo rešitev VMI v podjetju. Parameter je pomemben za vedenje ali lahko VMI implementiramo na obstoječi virtualizirani infrastrukturi podjetja ali moramo postaviti alternativno;
- katero ciljno virtualizirano okolje VMI je implementirano v strežniku. Vprašanje se nanaša predvsem na operacijska sistema Android in iOS;
- kdo lahko namesti odjemalca na mobilno napravo in kompleksnost namestitve;
- ali rešitev uporablja standardizirani ali lastniški protokol komuniciranja med odjemalcem in strežnikom ter kako je zagotovljena varnost;
- ali rešitev s stališča dodatne varnosti podpira dvostopenjsko overjanje;
- narava povezave (trajnost) in potreba po ponovnem overjanju;
- kakšne vrste aplikacij podpira okolje VMI;
- komunikacijski medij za dostop odjemalca do strežnika (WiFi ali 3G/4G); ta kriterij je pomemben zaradi komunikacijskih stroškov uporabnika;
- zaščitna sredstva za preprečitev uhajanja podatkov, npr. blokiranje posnetka ekrana (angl. *Screen Snapshot*), vodni žig (angl. *Watermark*) za morebitno fotografiranje zaslona;
- združljivost z ostalimi orodji za nadzor mobilnih naprav;
- način upravljanja sistema;
- za katere mobilne operacijske sisteme obstaja odjemalec;
- prijaznost do uporabnika, odzivnost aplikacij; predvsem glede celostne uporabniške izkušnje.

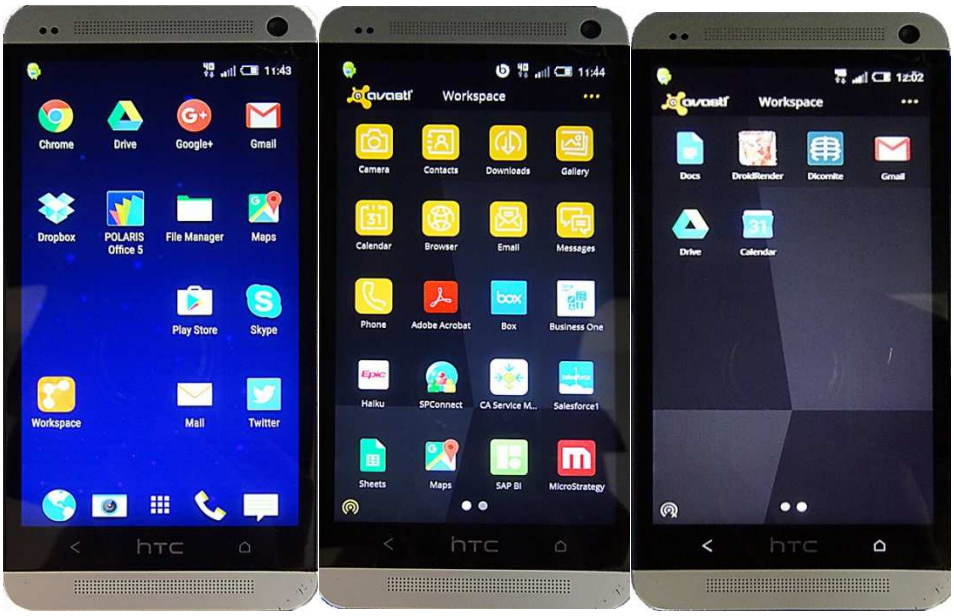
Pri iskanju primernega PSN koncepta za podjetja in zaposlene bodo zgoraj omenjeni kriteriji, poleg ciljev varnega PSN okolja, zagotovo vplivali na končno odločitev. Med tremi komercialno dostopnimi ponudniki bomo naredili primerjalno analizo in jo prikazali v tabeli v nadaljevanju.

Za potrebe testiranj smo uporabili pametni telefon HTC One M8 z verzijo Androida 5.0.2 Lollipop.

4.1.1 Remotium / Avast Software

Remotium VMI rešitev je Virtual Mobile Platform (v nadaljevanju VMP) in temelji na njihovem lastnem sistemu, na osnovi kontejnerjev s skupnim jedrom in ARM emulacijo na strežnikih. VMP je razvit kot VM, ki deluje na zaupanja vrednih strežnikih in kot odjemalec, ki deluje na mobilnih napravah. Vse aplikacije v virtualnem mobilnem prostoru so pretočene iz VMP virtualne naprave. Z uporabo patentirane virtualne tehnologije nad operacijskim sistemom, virtualna naprava gosti več primerkov virtualnih aplikacij in jih pretoči v mobilne delovne prostore z uporabo naprednih in prilagodljivih protokolov za pretakanje, ki so jih prvotno razvili za potrebe igralništva v oblaku. Vsa komunikacija med virtualnimi napravami in odjemalci je zaščitena z 256-bitnim AES šifriranjem ter s politikami za nadzor dostopa in beleženja. VMP v celoti omogoča centralizirano upravljanje mobilnosti v podjetju. Kot zagotavljajo v podjetju, ima njihova rešitev zelo nizek TCO in temelji na modelu preprostega uvajanja, enega prodajalca, enotne licence in manj računalniških virov. Občutljivi podatki se nikoli ne shranijo na končni napravi. Izgubljene ali ukradene mobilne naprave ne bodo nikoli izpostavile podatke podjetja. Podatki zaposlenih in poslovni podatki so shranjeni ločeno, kar zmanjšuje odpor zaposlenih do PSN programov. VMP prekine VM in zagotavlja zunajpasovnega agenta za zbiranje obvestil. Neobstojne virtualne instance zmanjšujejo tveganja pred zlonamerno programsko opremo in omogočajo celovite varnostne preglede za aplikacije tretjih oseb. Napredni protokoli za pretakanje vsebin, ki so prilagojeni na omrežne pogoje, zagotavljajo visoko odzivnost. Njihov RDP temelji na kompresijskem formatu H.264 (Avast Virtual Mobile Platform, 2016).

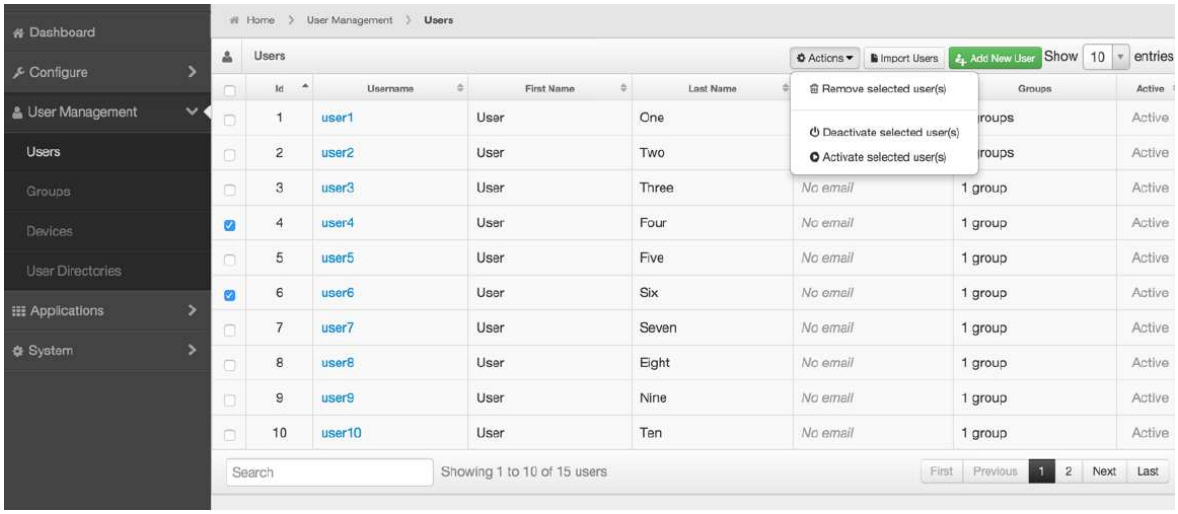
Slika 26: Remotium/Avast Virtual Mobile Platform



Za nadzor in spremljanje uporabnikov, kje in kako dostopajo do virov podjetja, skrbi zelo napredna in pregledna nadzorna plošča. S stališča aplikacij si prizadevajo, da bi njihova aplikacija lahko vsebovala tudi Google Mobile Services, v nadaljevanju GMS (aplikacije kot so mail, maps, play store, itd.), vendar gradijo svoj alternativni programski vmesnik ali API. Trenutno še noben VMI ponudnik nima pridobljene licence za GMS. Avast VMP teče na VMWare ESXi in KVM hipernadzorniku. Lahko pa podpira tudi kateregakoli drugega hipernadzornika, ki podpira OVF format (Microsoft Hyper-V, XenServer,OpenStack, VirtualBox). Podpira dvostopenjsko overjanje (LDAP, Google OAuth2, Exchange ActiveSync). Deluje na različicah od verzije iOS 6 naprej ter Android različicah od verzije 4.0 naprej (Avast Virtual Mobile Platform, 2016).

Julija leta 2015 je Remotium kupilo podjetje Avast Software, češko podjetje z varnostno programsko opremo in tako razširilo svojo ponudbo varnosti mobilnih aplikacij v okolje podjetij (Avast Software Acquires Mobile Virtualization Company Remotium, 2016).

Slika 27: Avast nadzorna plošča



Vir: Avast Virtual Mobile Platform, 2016.

Slika 26 prikazuje demo okolje Avastove VMI rešitve VMP. Na levi sliki je prikazano domače okolje z osebnimi aplikacijami na našem pametnem telefonu HTC One M8 in VMI odjemalcem Workspace, s katerim dostopamo do virtualnega Android okolja v oblaku. Na srednji in desni sliki pa je prikazano virtualno okolje VMP rešitve z razpoložljivimi aplikacijami, med njimi tudi GMS. Namestitev strežniškega okolja je zelo enostavna, z enostavnimi navodili in jo lahko izvede administrator podjetja, ki ima znanja iz tega področja. Odjemalca za VMP rešitev je enostavno prenesti iz tržnic programskih rešitev in ga namestiti na mobilno napravo. Aplikacija od uporabnika zahteva dovoljenje za dostop do naslednjih funkcij na mobilni napravi:

- lokacije;
- telefona;
- fotografij, predstavnosti in datotek;
- fotoaparata;
- mikrofona;
- podatkeov o WiFi povezavi;
- ID naprave in informacije klicev.

Povezava med podatkovnim centrom in odjemalcem se vzpostavi po pritisku na želeno aplikacijo in prekine po petih minutah nedejavnosti. Dostop z mobilnimi napravami deluje tako preko WiFi kot tudi 3G/4G omrežij. Podatki podjetja niso shranjeni na mobilni napravi.

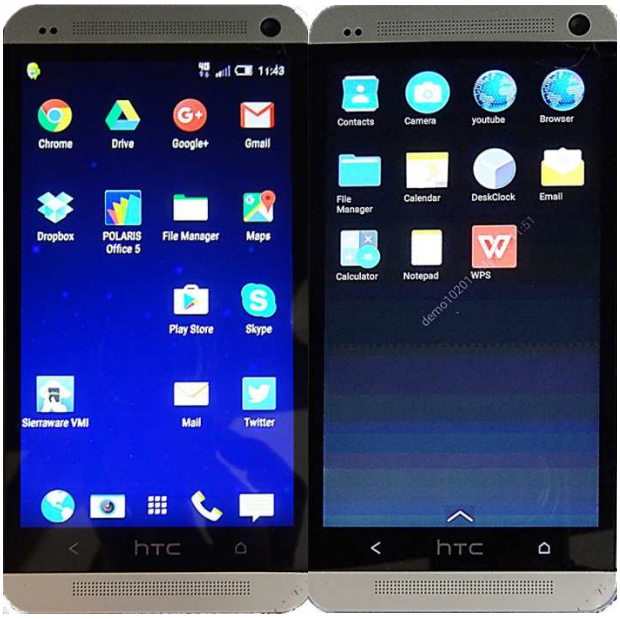
4.1.2 Sierraware

Sierraware z rešitvijo SierraVMI ponuja zmogljivo VMI platformo za Androidove aplikacije. Platforma kombinira pristop virtualizacije preko kontejnerjev in virtualizacije gole kovine, ki omogoča podjetjem, da streže tisočim uporabnikom iz enega, velikega VM oblaka. Hkrati tudi odpravlja potrebo po zapletenih sistemih v oblaku. Platforma je zgrajena na ARM strežniški strojni opremi, vendar podpira tudi Intelovo x86 arhitekturo. Zaradi svoje arhitekture z visoko stopnjo zapisa, lahko podjetja zagotavljajo dostop do 10.000 uporabnikom iz 12-ih strežnikov. Njihova namestitev je zelo enostavna in zahteva malo časa. SierraVMI omogoča nižje stroške razvoja aplikacij in zagotavlja podporo za več različnih platform. Pristop pri grafiki je nekoliko drugačen od ostalih, lahko se ga razširi in prilagodi, uporablja GPU za kodiranje, gonilniki pa so direktno v VM in ne v hipernadzorniku, GMS ima pri Sierraware nižjo prioriteto. Podjetja lahko razvijajo svoje aplikacije za Android in hkrati poskrbijo, da aplikacije podpirajo oddaljen dostop iz katerekoli mobilne naprave (Androida, Apple-a, Microsofta ali BlackBerry-a).

Ni jim potrebno več skrbeti za združljivost in različice operacijskega sistema. Podjetjem je preko nadzornega sistema omogočeno tudi spremljanje aktivnosti uporabnikov. Platforma prepoznava kibernetske napade s pregledovanjem datotek za škodljivimi vsebinami in uporabnikom preprečuje distribucijo zaupnih podatkov. Gosti mobilne aplikacije centralno in odpravlja potrebo za namestitev in nadgradnjo več aplikacij na posamezni napravi. Podpira dvostopenjsko overjanje. Z enkratno prijavo in s kombinacijo gesla ter biometričnih podatkov za overjanje uporabnikov omogoča podjetjem uporabo varne in enotne politike prijavljanja na vseh mobilnih aplikacijah. SierraVMI ponuja polno Android ponudbo, uporabnikovi podatki so shranjeni ločeno. Deluje na različicah od verzije iOS 7.1 naprej ter različicah od verzije Android 3.0 naprej. Podpira tudi uporabnike Microsoftovih in Blackberry-jevih mobilnih naprav (Sierraware, 2015).

Slika 28 prikazuje demo okolje SierraVMI platforme. Na levi sliki je prikazano domače okolje z osebnimi aplikacijami na našem pametnem telefonu HTC One M8 in VMI odjemalcem Sierraware VMI, s katerim dostopamo do virtualnega Android okolja v oblaku. Na desni sliki je prikazano virtualno okolje SierraVMI – rešitve z razpoložljivimi aplikacijami.

Slika 28: Sierraware SierraVMI rešitev

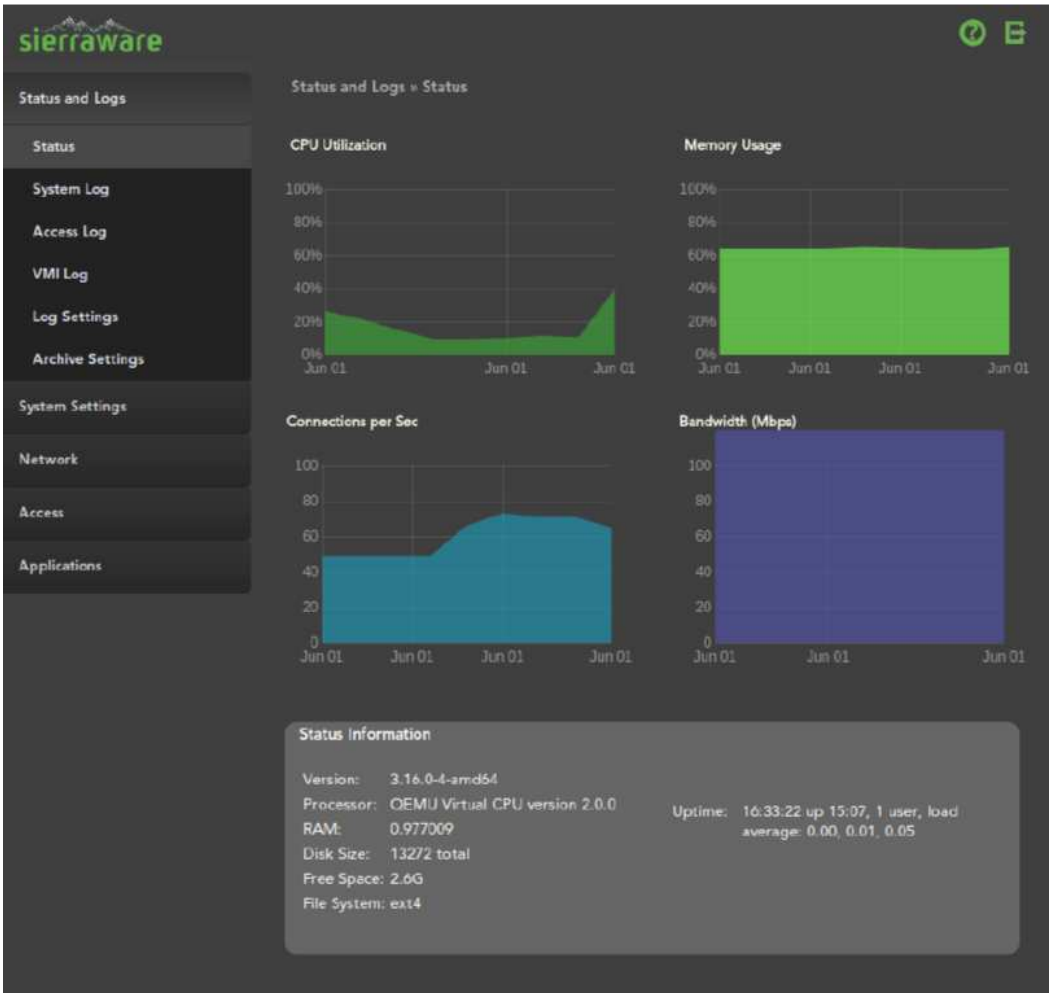


Namestitev strežniškega okolja je zelo enostavna, z enostavnimi navodili in jo lahko izvede administrator podjetja, ki ima znanja iz tega področja. Odjemalca za SierraVMI rešitev je enostavno prenesti iz tržnic programskih rešitev in ga enostavno namestiti na mobilno napravo. Aplikacija od uporabnika zahteva dovoljenje za dostop do naslednjih funkcij na mobilni napravi:

- lokacije;
- fotografij, predstavnosti in datotek;
- fotoaparata;
- mikrofona.

Povezava med podatkovnim centrom in odjemalcem je neobstojna in se vzpostavi po pritisku na VMI odjemalca. Dostop z mobilnimi napravami deluje tako preko WiFi, kot tudi 3G/4G omrežij. Podatki podjetja niso shranjeni na mobilni napravi. Aplikacija omogoča blokado posnetkov zaslona in ima možnost vključitve vodnega žiga. Spletni nadzorni sistem (Slika 29) je enostaven in pregleden. Aplikacije, ki so na voljo, delujejo. Ugotavljamo, da je tudi pri Sierraware uporabniška izkušnja za delo z aplikacijami zelo dobra in enaka kot pri izvornih aplikacijah, ima prijazen uporabniški vmesnik s hitro odzivnostjo.

Slika 29: Sierraware SierraVMI nadzorna plošča



Vir: Sierraware, 7 Things You Need to Know about Virtual Mobile Infrastructure, 2015.

4.1.3 Nubo Software

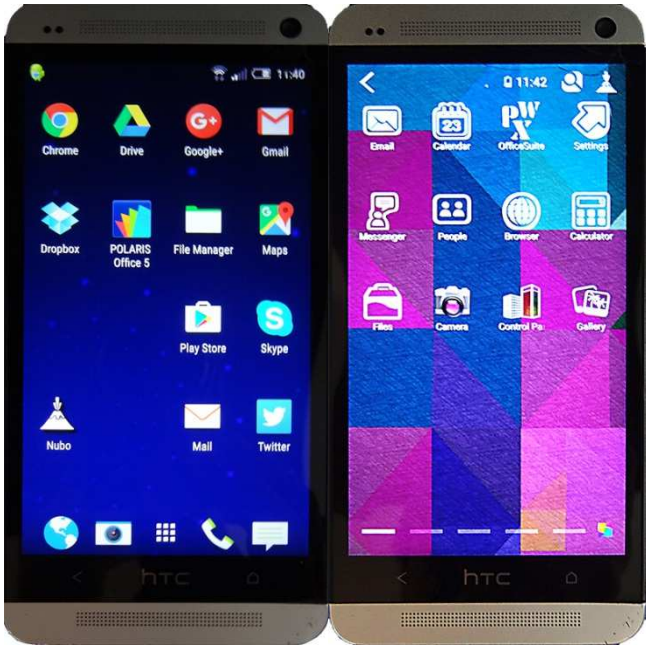
Nubo je ustvaril prilagojeno Android platformo, ki poteka v podatkovnem centru na VM. Na vsakem VM lahko teče več uporabniških sej. To omogoča Nubovi VMI rešitvi, da lahko dela na vseh priljubljenih virtualizacijskih orodjih, vključno z VMWare in Citrixom. Platforma podpira x86 Android arhitekturo vključno z VMWare ESXi, Microsoft Hyper-V, Citrix XenServer, KVM in Amazon Web Services. Rešitev podpira dvostopenjsko overjanje, uporabnikovi podatki so shranjeni ločeno in šifrirani ter hkrati ločeni od VM.

Nubo je za potrebe povezave med podatkovnim centrom in tankim odjemalcem na mobilni napravi razvil lasten, varen komunikacijski protokol UX-over-IP, ki temelji na TLS verziji 1.2 (angl. *Transport Layer Security*) in podpira funkcije samodejnega prilagajanja velikosti zaslona, delovanje zaslona na dotik, komunikacijo z mobilnimi senzorji (vrtenje, lokacija), učinkovito uporabo pasovne širine in je oblikovan za brezžična omrežja. Dostop do aplikacij

in podatkov v oblaku je lažji in varen. Implementacija platforme je lahko bodisi na lokaciji podjetja ali v oblaku. Nadzorni sistem je odgovoren za usklajevanje uporabniškega overjanja in avtorizacije, ustvarjanje sej in izenačevanje obremenitev. Nubo platforma zagotavlja hitro povezavo kadarkoli in kjerkoli na svetu. Uporabljajo neobstojne virtualne instance. Vsakič, ko se uporabnik prijavi v svoje delovno okolje, je ustvarjena nova seja in dodeljena na najbližjo razpoložljivo platformo. Ko se uporabnik odjavi, se vsi novi podatki s te seje samodejno sinhronizirajo med vsemi regijami. Deluje na različicah od verzije iOS 5.1.1 dalje ter različicah od verzije Android 4.0 dalje (Virtual Mobile Infrastructure, 2016).

Slika 30 prikazuje demo okolje Nubo VMI platforme. Na levi sliki je prikazano domače okolje z osebnimi aplikacijami na našem pametnem telefonu HTC One M8 in Nubo VMI odjemalcem, s katerim dostopamo do virtualnega Android okolja v oblaku. Na desni sliki je prikazano virtualno okolje Nubove rešitve z razpoložljivimi aplikacijami. Namestitev strežniškega okolja je možna le ob pomoči proizvajalca proti plačilu storitve.

Slika 30: Nubo Software VMI rešitev



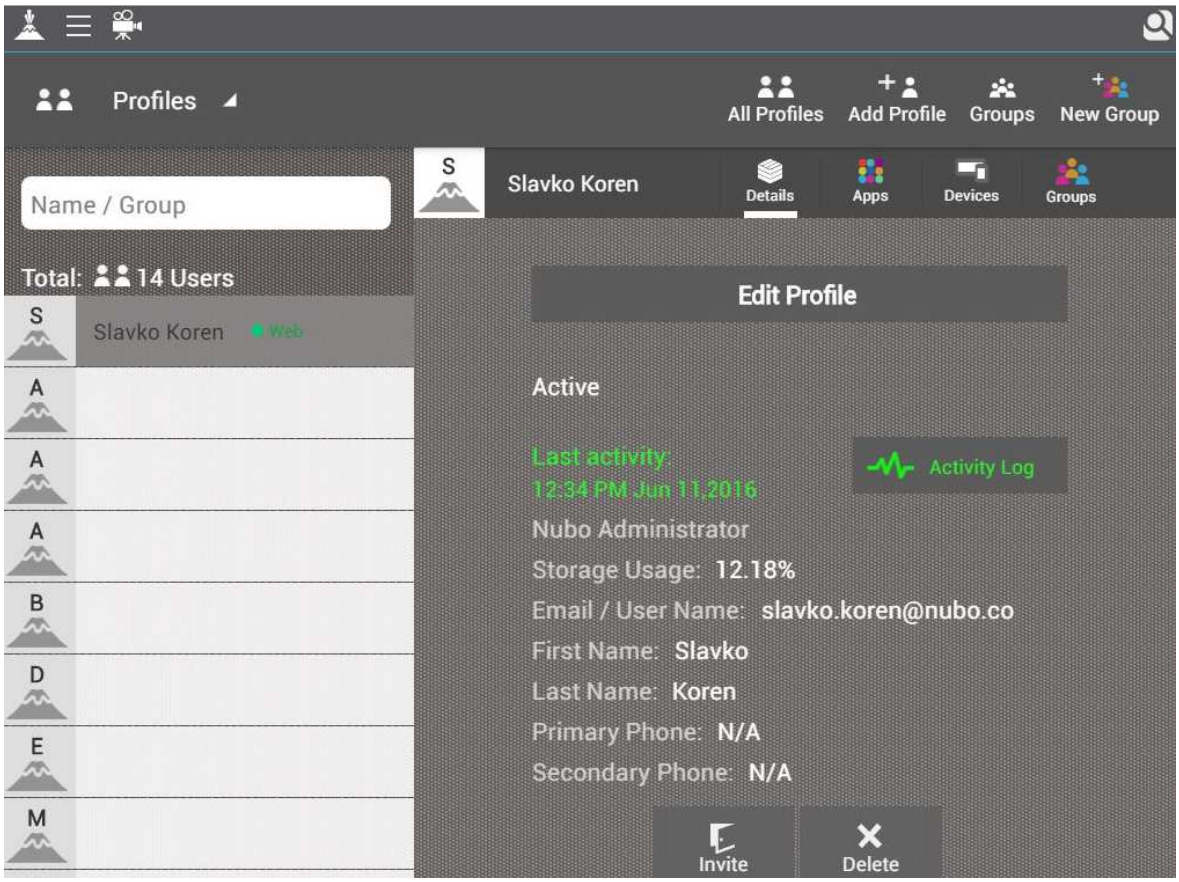
Odjemalca za Nubo VMI rešitev je enostavno prenesti iz tržnic programskih rešitev in se ga enostavno namesti na mobilno napravo. Aplikacija od uporabnika zahteva dovoljenje za dostop do naslednjih funkcij na mobilni napravi:

- zgodovine naprave in aplikacij;
- identitete;
- stikov;
- lokacije;

- telefona;
- fotografij, predstavnosti in datotek;
- fotoaparata;
- podatke o WiFi povezavi;
- ID naprave.

Povezava med podatkovnim centrom in odjemalcem je neobstojna in se vzpostavi po pritisku na VMI odjemalca. Dostop z mobilnimi napravami deluje le preko 3G/4G omrežij. Z dostopom preko WiFi omrežij je bilo precej težav. Podatki podjetja niso shranjeni na mobilni napravi. Aplikacija omogoča blokado posnetkov zaslona in ima možnost vključitve vodnega žiga. Spletni nadzorni sistem (Slika 31) je enostaven in pregleden. Aplikacije, ki so na voljo, delujejo. Ugotavljamo, da je pri Nubu uporabniška izkušnja za delo z aplikacijami zelo dobra in enaka kot pri izvornih aplikacijah, ima prijazen uporabniški vmesnik s hitro odzivnostjo.

Slika 31: Nubo Software nadzorna plošča



4.1.4 Hypori

Hypori ACE rešitev omogoča oddaljen dostop mobilnim napravam na operacijskem sistemu Android, ki deluje kot virtualna mobilna naprava na strežniku in zagotavlja uporabnikom mobilno izkušnjo, ki je optimizirana za pametne telefone in tablice. Platforma nudi popolno integracijo z vodilnimi EMM (MDM in MAM) rešitvami. Overjanje in avtorizacija temelji na AD in LDAP, upravljanje temelji na politiki, centralni reviziji in beleženju aktivnosti vseh uporabnikov. Na mobilnih napravah ni shranjenega nobenega občutljivega podatka podjetja.

Aplikacije in podatki so na varnem in ločeni od uporabnikovih aplikacij, ki lahko vsebujejo zlonamerno programsko opremo. Z upravljanjem in uporabo enotne centralizirane slike operacijskega sistema podjetja povečajo varnost in zmanjšajo stroške. Dostop do Android aplikacij je omogočen iz različnih vrst naprav; Android, Apple in Windows mobilnih naprav. Hypori stremi h konceptu popolne virtualizacije mobilnih naprav, kar omogoča uporabnikom zelo dobro uporabniško izkušnjo. Podpirajo obstojne oziroma trajne virtualne instance in si s stališča aplikacij prizadevajo vključiti GMS aplikacije.

Slika 32: Hypori ACE rešitev

Vir: C. Hazelton, Virtual mobile infrastructure: What it's about, and why it's important to the enterprise, 2015.

Platforma uporablja KVM in QEMU za ARM Android emulacijo na Intelovih strežnikih. Njihov RDP temelji na kompresijskem formatu H.264 s po meri narejenimi kodeki. Deluje

na različicah od verzije iOS 8.0 dalje ter različicah od verzije Android 4.1 dalje (Hazelton, 2015).

4.1.5 Raytheon

Raytheonova VMI rešitev je Trusted Access Mobile, v nadaljevanju TAM, ki omogoča varen dostop in interakcijo s podatki in aplikacijami iz katerekoli mobilne naprave. Za razliko od klasičnih MDM rešitev, ki varujejo podatke podjetja z uporabo mobilnega kontejnerja na mobilni napravi in na varnostnih tehnologijah, ki temeljijo na MDM, TAM ter ponujajo virtualizacijo lastnih mobilnih aplikacij v varnem VMI okolju. Blaži skrbi zaradi izgube podatkov, kraje ali ogrožanja, zaradi česar je TAM rešitev idealna za PSN okolja. Uporabljajo lastno VMI platformo z ARM Android emulacijo. Uporabljajo RDP, ki temelji na kompresijskem formatu H.264 in neobstojne virtualne instance zaradi lestvičenja (angl. *Scaling*). Funkcije TAM so usmerjene v varnostno zavedne organizacije, ki so pri PSN politiki bolj konzervativne. Deluje na različicah od verzije iOS 7.1 dalje ter različicah od verzije Android 3.0 dalje (Raytheon, 2014).

Slika 33: Raytheon TAM rešitev

Vir: Raytheon, Trusted Access: Mobile, 2014.

4.1.6 Trend Micro

Pri Trend Micro rešitvi Safe Mobile Workforce lahko skrbniki VMI okolja nastavljajo in uvajajo več mobilnih delovnih prostorov za vse svoje poslovne uporabnike preko centralne

pregledne plošče. Posredovanje za posodobitev ni več potrebno, zaposleni lahko snamejo odjemalca za VMI rešitev preko tržnic programskih rešitev in ga namestijo na svoje mobilne naprave. Odjemalec je podprt za Android, iOS in Windows operacijske sisteme. Preprečuje uhajanje ali izgubo podatkov podjetja, ker so podatki shranjeni na varnih strežnikih in ne na napravah zaposlenih. Zadovoljstvo in produktivnost zaposlenih je izboljšana, ker omogoča varen oddaljen dostop do vseh virov podjetja, ne da bi s tem kakorkoli vplivalo ali omejevalo osebno uporabo. Zmanjšuje potrebo po internih virih podpore za več mobilnih platform. Oddelku informacijske tehnologije omogoča preko centralne konzole posodobitev nameščene aplikacije in upravljanje profilov brez posredovanja uporabnikov. Deluje z obstoječimi EMM rešitvami za upravljanje mobilnih naprav (Trend Micro, 2014).

4.2 Primerjava VMI rešitev

V poglavju 4.1 smo razvili in opredelili kriterije, ki se nam zdijo pomembni za verificiranje sprejemljivosti rešitve in jih uporabili pri primerjavi v Tabeli 3.

Tabela 3: Povzetek testiranja VMI rešitev za nadzor mobilnih naprav

	VMI rešitve za nadzor mobilnih naprav		
Kriteriji primerjave	**Remotium/Avast**	**Sierraware**	**Nubo Software**
Namestitev strežnika	IT administrator podjetja, enostavna namestitev	IT administrator podjetja, enostavna namestitev	IT administrator podjetja, enostavna namestitev
Podprte različice virtualnih okolij	VMWare ESXi, KVM in OVF format Hyper-V, XenServer,OpenStack, VirtualBox	KVM, VMWare ESXi	VMWare ESXi, Hyper-V, XEN in KVM
Vgrajena emulacija	Android	Android	Android
Namestitev odjemalca	Uporabnik sam, enostavna namestitev	Uporabnik sam, enostavna namestitev	Uporabnik sam, enostavna namestitev
Komunikacijski protokol med podatkovnim centrom in odjemalcem	RDP (SSL)	RDP (SSL)	Lastni, UX-over-IP (TLS/SSL)
Dvostopenjsko overjanje	Da	Da	Da
Obstojnost povezave med podatkovnim centrom in odjemalcem	Neobstojna, povezava se po potrebi vzpostavi po pritisku na želeno aplikacijo, sistem uporabnika odjavi po 10 minutah neaktivnosti	Neobstojna, povezava se vzpostavi po potrebi in prekine po 15 minutah neaktivnosti	Neobstojna, povezava se vzpostavi po potrebi in prekine po 1 minuti neaktivnosti
Podprte aplikacije	Lasten API, GMS in ostale aplikacije	Lasten API, nižja prioriteta za GMS, ostale aplikacije	Lasten API in ostale aplikacije
Dostop	Wifi, 3G/4G	Wifi, 3G/4G	3G/4G

se nadaljuje

Tabela 3: Povzetek testiranja VMI rešitev za nadzor mobilnih naprav (nad.)

	VMI rešitve za nadzor mobilnih naprav		
Kriteriji primerjave	**Remotium/Avast**	**Sierraware**	**Nubo Software**
Preprečitev uhajanja podatkov	Da, podatki podjetja niso shranjeni na mobilni napravi	Da, podatki podjetja niso shranjeni na mobilni napravi	Da, podatki podjetja niso shranjeni na mobilni napravi
Blokada posnetkov zaslona	Da	Da	Da
Možnost vodnega žiga	Da	Da	Da
Združljivost z ostalimi MDM	Da	Da	Da
Nadzorni sistem za upravljavca sistema	Da	Da	Da
Odjemalec za naprave z Android OS	Da, od različice 4.0 naprej	Da, od različice 3.0 naprej	Da, od različice 4.0 naprej
Odjemalec za naprave z iOS	Da, od različice 6.0 naprej	Da, od različice 7.1 naprej	Da, od različice 5.1.1 naprej
Uporabniška izkušnja, prijaznost uporabniškega vmesnika in odzivnost aplikacij	Zelo dobra izkušnja, prijazen uporabniški vmesnik, hitra odzivnost	Zelo dobra izkušnja, prijazen uporabniški vmesnik, hitra odzivnost	Zelo dobra izkušnja, prijazen uporabniški vmesnik, hitra odzivnost

V Tabeli 4 smo VMI rešitve primerjali s postavljenimi cilji za varno PSN okolje, ki smo jih identificirali v drugem poglavju.

Tabela 4: Primerjava VMI rešitev za nadzor mobilnih naprav s cilji varnega PSN okolja

	VMI rešitve za nadzor mobilnih naprav		
Želeni cilji	**Remotium/Avast**	**Sierraware**	**Nubo Software**
Izolacija prostora	✓	✓	✓
Varovanje podatkov podjetja	✓	✓	✓
Izvrševanje varnostne politike	✓	✓	✓
Popolna izolacija prostora	✓	✓	✓
Nevsiljivost	✓	✓	✓
Nizka poraba virov	✓	✓	✓

Skozi raziskovalno delo smo ugotovili, da za podjetja postaja vedno težje uveljaviti varnostno politiko nad mobilnimi napravami, vedno težje sledijo uhajanju svojih občutljivih podatkov, njihovi zaposleni pa so vedno bolj zaskrbljeni za svojo zasebnost. Ugotavljamo, da vse tri pregledane VMI rešitve zagotavljajo varno in sprejemljivo PSN okolje tako za podjetja kot tudi zaposlene in v celoti rešujejo opisane probleme in dosegajo zastavljene cilje.

Na vprašanje magistrske naloge »Ali lahko z virtualizacijo mobilnih naprav – VMI ustvarimo varno PSN okolje za podjetje in zaposlene?« je odgovor »**da, lahko**«.

SKLEP

Dejstvo je, da mobilne naprave v podjetjih izpodrivajo klasične računalnike. Kar pa je malo manj jasno je, kako bo mobilno računalništvo implementirano v okolja podjetij. Prodaja osebnih računalnikov je prvič v zgodovini računalništva v upadu. V letu 2015 je prodaja po analitski hiši IDC padla za 10,6 odstotka v primerjavi z letom poprej (PC Market Finishes 2015 As Expected, Hopefully Setting the Stage for a More Stable Future, According to IDC, 2016). Po analitski hiši Gartner pa za 8,3 odstotka v primerjavi z letom poprej (Gartner Says Worldwide PC shipments declined 8.3 Percent in Fourth Quarter of 2015, 2016). Ti podatki so zaskrbljujoči za prihodnost klasičnih računalnikov. Mobilnost postaja vedno bolj in bolj pomembna platforma tudi v poslovnem svetu, kjer podjetja z zelo občutljivimi in tajnimi podatki iščejo rešitve za varno PSN okolje. Predvsem gre za zaskrbljenost glede podatkov podjetja, ki so shranjeni na mobilnih napravah ali pa se prenašajo iz in na mobilne naprave zaposlenih. Vedno večja kompleksnost mobilnih okolij zahteva zelo prilagodljiv nabor orodij za upravljanje mobilnih uporabnikov. Da bi zadostili zahtevam po varnem dostopu, so podjetja kupovala in uporabljala drago namensko strojno in programsko opremo. Do sedaj so bile EMM z MDM, MAM in MCM orodja tiste najbolj obsežne ter vsestransko prilagodljive rešitve za upravljanje naprav, aplikacij in podatkov za potrebe mobilno usmerjenega podjetja. V naslednjih nekaj letih se bodo EMM implementacije drastično znižale, kajti podjetja se usmerjajo iz samega upravljanja naprav in sredstev k pristopu za upravljanje podatkov in uporabnikov. Ta pristop vodi k VMI, ki ponuja virtualno okolje, kjer ni korporativnih podatkov na končnih mobilnih napravah. Kjerkoli so mobilni podatki, tam bo podjetje vedno potrebovalo nekakšen nadzor nad njimi, če je to na ravni naprave, na ravni aplikacije ali pa na ravni hipernadzornika. Ideja VMI ni v znižanju stroškov strojne opreme in preusmeritvi teh stroškov na zaposlenega, ampak prehod in prenos podatkov v oblak. Do danes je bilo le nekaj varnostnih poudarkov na preprečevanju uhajanja podatkov podjetja in poudarkov glede zasebnosti zaposlenih. Glavno gonilo podjetij mora zato biti v rešitvi, ki ustreza vsaki platformi in ščiti podatke podjetja brez kršenja zasebnosti zaposlenih (Hazelton, 2015).

Tematika v magistrskem delu je podrobno razdelana in je napisana kot usmeritev za podjetja s smernicami, ki jim morajo podjetja slediti, ko uvajajo PSN koncept v podjetje. Za upravičenost PSN je za podjetja najprej potrebna jasna slika uspešnosti PSN koncepta, upoštevati mora veliko dejavnikov. Ko je slika jasna in so meritve uspešnosti PSN opravljene, lahko podjetja pripravijo strategijo in model vključitve PSN koncepta v podjetje. Na podlagi zahtev in modelov informacijske varnosti ter upoštevanj morebitnih tveganj pri uporabi mobilni naprav, mora podjetje razviti svoj nabor smernic, ki bodo blažile tveganja ter urejale upravljanje in varovanje mobilnih naprav. To pa vključuje uporabo rešitev za nadzor mobilnih naprav, ki jih je na tržišču veliko.

Uvedba politike PSN je koristna tako za podjetja kot tudi za zaposlene, saj povečuje zadovoljstvo pri delu, zaposleni pa postanejo bolj učinkoviti in produktivni. Vendar pa politika PSN in sama mobilnost PSN naprav predstavlja varnostno grožnjo občutljivim podatkom podjetja, kot tudi zasebnosti zaposlenih. To ustvarja izzive pri uhajanju podatkov, nepooblaščene delitve prostorov, pomanjkanju varnosti, skladnosti in zasebnosti zaposlenih. Odgovor na te izzive je varno PSN okolje, ki izpolnjuje cilje izolacije prostora, varovanja podatkov podjetja, izvrševanje varnostne politike, popolno izolacijo prostora, nevsiljivost in nizko porabo virov.

Ugotovili smo, da rešitev z virtualizacijo mobilnih naprav – VMI, zagotavlja in izpolnjuje vse cilje za varno PSN okolje za podjetja in zaposlene in ga zato priporočamo.

Nadaljnji koraki. VMI je relativno nova tehnologija, ki se je na tržišču šele pojavila. Obstajajo tehnični in logistični izzivi, ki jih bo še potrebno rešiti. Z enim ali več proizvajalci bomo nadaljevali delo, postavili lastni oblak z rešitvijo VMI in jo ponudili tržišču. Kaj se bo zgodilo in ali bodo podjetja našla v VMI pravo rešitev za njih, bo pokazal čas.

Nadaljnje raziskave. Pri raziskovanju za magistrsko delo smo naleteli na kar nekaj potencialnih rešitev, ki bi lahko ustrezala opisu za varno PSN okolje. Ena takih rešitev je tehnologija HTML5. Kadarkoli govorimo o prihodnosti spletnih aplikacij ali novih spletnih aplikacij, pridemo na HTML5. HTML5 lahko reši veliko vprašanj, ki jih imajo tradicionalne spletne aplikacije na mobilnih napravah. Gartner (Gartner Identifies Top 10 Mobile Technologies and Capabilities for 2015 and 2016, 2016) je za leti 2015 in 2016 HTML5 identificiral kot vrhunsko mobilno tehnologijo. HTML5 ima funkcije, ki se z lahkoto prilagajajo. Obstajajo API-ji, ki se ukvarjajo z dogodki na dotik, orientacijo zaslona in geolokacijo. Medtem, ko tradicionalne spletne aplikacije ne delujejo nepovezano, HTML5 lahko. HTML5 je zelo razširjen standard, implementiran v veliko število vtičnikov različnih brskalnikov in lahko z lahkoto trdimo, da bodo te aplikacije delovale kjerkoli na katerikoli napravi. S stališča podjetij je HTML5 odličen pripomoček za dostavo svojih aplikacij na mobilne naprave. HTML5 omogoča izolacijo prostora med podatki podjetja in osebnimi podatki zaposlenih. Ta aplikacija je neodvisna od platforme in je zelo primerna za mobilne naprave. Aplikacija bo delovala tako na iOS kot tudi na Android napravah (Madden, 2014).

LITERATURA IN VIRI

1. Aberdeen Group. (2011). *Enterprise-Grade BYOD Strategies: Flexible, Compliant, Secure*. Najdeno 20. marca 2016 na spletnem naslovu http://fm.sap.com/data/UPLOAD/files/Enterprise_Grade_BYOD_Strategies__2012.4.11-18.52.49.pdf
2. Absalom, R. (2012, 17. maj). International Data Privacy Legislation Review: A Guide for BYOD Policies. *Ovum.* Najdeno 20. marca 2016 na spletnem naslovu http://www.webtorials.com/main/resource/papers/mobileiron/paper5/Guide_for_BYOD_Policies.pdf
3. *Active Directory*. Najdeno 20. marca 2016 na spletnem naslovu https://technet.microsoft.com/en-us/library/cc782657(v=ws.10).aspx
4. Alberta Education. (2012). *Bring your own device: A guide for schools*. Najdeno 20. marca 2016 na spletnem naslovu https://archive.education.alberta.ca/media/6749210/byod%20guide%20revised%202012-09-05.pdf
5. Andrus, J., Dall, C., Van`t Hof, A., Laandan, O., & Nieh, J. (2011). Cells: a virtual mobile smartphone architecture. *SOSP '11 Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles* (str. 173-187). New York: ACM.
6. *Apple Launches iPad*. Najdeno 20. marca 2016 na spletnem naslovu http://www.apple.com/pr/library/2010/01/27Apple-Launches-iPad.html
7. Article 29 Working Party – WP29. (2013, 27. februar). *Opinion 02/2013 on apps on smart devices*. Najdeno 20. marca 2016 na spletnem naslovu http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
8. Article 29 Working Party – WP29. (2014, 16. september). *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*. Najdeno 20. marca 2016 na spletnem naslovu http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf
9. *Avast Software Acquires Mobile Virtualization Company Remotium.* Najdeno 20. marca 2016 na spletnem naslovu https://press.avast.com/avast-software-acquires-mobile-virtualization-company-remotium
10. *Avast Virtual Mobile Platform*. Najdeno 20. marca 2016 na spletnem naslovu https://www.avast.com/virtual-mobile-platform
11. *Blackberry completes Good Technology Acquisition*. Najdeno 20. marca 2016 na spletnem naslovu http://press.blackberry.com/en/press/2015/blackberry-completes-good-technology-acquisition.html
12. Bradford Networks. (2012). *Network sentry*. Najdeno 20. marca 2016 na spletnem naslovu http://infosightsol.com/wordpress/wp-content/uploads/2013/03/Datasheet-Network-Sentry-10-17-2012.pdf

13. Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk Management, 54*(1), 24-29.
14. Brocade. (2015). *Brocade Network Advisor*. Najdeno 20. marca 2016 na spletnem naslovu https://www.brocade.com/content/dam/common/documents/content-types/datasheet/brocade-network-advisor-ds.pdf
15. Chellakari, K. (2012). Developing a BYOD strategy: Weigh the Risks, Challenges and Benefits. *TechTarget*. Najdeno 6. februarja 2016 na spletnem naslovu http://searchsecurity.techtarget.com/feature/Developing-a-BYOD-Strategy-Weigh-the-Risks-Challenges-and-Benefits
16. Cisco. (2012). *Cisco Bring Your Own Device, Device Freedom Without Compromising the IT Network.* Najdeno 20. marca 2016 na spletnem naslovu http://www.cisco.com/c/dam/en_us/solutions/trends/byod_smart_solution/docs/BYOD_Whitepaper.pdf
17. Cisco. (2014a). *2014 Connected World Technology Final Report*. Najdeno 6. februarja 2016 na spletnem naslovu http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/connected-world-technology-report/cisco-2014-connected-world-technology-report.pdf
18. Cisco. (2014b). *Cisco 2014 Annual Security Report*. Najdeno 6. februarja 2016 na spletnem naslovu http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
19. Cisco. (2014c). *Cisco Enterprise Mobility Solution, Device Freedom Without Compromising the IT Network.* Najdeno 20. marca 2016 na spletnem naslovu http://www.cisco.com/c/dam/en_us/solutions/trends/byod_smart_solution/docs/BYOD_Whitepaper.pdf
20. Cisco. (2014d). *Cisco Anyconnect Secure Mobility Client Administrator Guide, Release 3.1*. Najdeno 20. marca 2016 na spletnem naslovu http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect31/administration/guide/anyconnectadmin31.pdf
21. Cisco. (2014e). *Cisco Prime for IT*. Najdeno 20. marca 2016 na spletnem naslovu http://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/prime-collaboration-manager/at_a_glance_c45-714537.pdf
22. Cisco. (2015a). *Cisco ASA Next-Generation Firewall Services*. Najdeno 20. marca 2016 na spletnem naslovu http://www.cisco.com/c/en/us/products/collateral/security/ asa-5500-series-next-generation-firewalls/data_sheet_c78-701659.pdf
23. Cisco. (2015b). *Annual Security Report 2015*. Najdeno 20. marca 2016 na spletnem http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf
24. *XenMobile*. Najdeno 20. marca 2016 na spletnem naslovu https://www.citrix.com/products/xenmobile
25. Command Five – C5. (2011). *Advanced Peersistent Threats: A Decade in Review*. Najdeno 20. marca 2016 na spletnem http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

26. Cosgrove, T., Smith, R., Silva, C., Girard, J., & Taylor, B. (2015, 8. junij). Magic Quadrant for Enterprise Mobility Management Suites. *Gartner*. Najdeno 20. marca 2016 na spletnem naslovu http://s.nsit.com/content/dam/insight/EMEA/uk/insightcloud/Airwatch/Magic_Quadrant_for_Enterprise_Mobility_Management_Suites.pdf
27. Dall, C., & Nieh, J. (2014). KVM/ARM: the design and implementation of the linux ARM hypervisor. *ACM SIGARCH Computer Architecture News – ASPLOS `14, 42*(1), 333-348.
28. *Digitalna potrdila*. Najdeno 20. marca 2016 na spletnem naslovu http://evem.gov.si/info/zacenjam/digitalna-potrdila
29. *Dropbox Business User Guide*. Najdeno 20. marca 2016 na spletnem naslovu https://www.dropbox.com/static/docs/guide/dropbox_for_business_user_guide.pdf
30. *Enterprise Mobility Management*. Najdeno 20. marca 2016 na spletnem naslovu https://www.citrix.com/enterprise-mobility-management
31. Ericsson. (2015). *Ericsson Mobility Report*. Najdeno 6. februarja 2016 na spletnem naslovu http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf
32. European Commission. (2015a, 15. december). *Agreement on Commission`s data protection reform will boost Digital Single Market*. Najdeno 20. marca 2016 na spletnem naslovu http://europa.eu/rapid/press-release_IP-15-6321_en.pdf
33. European Commission. (2015b). *Data protection*. Najdeno 20. marca 2016 na spletnem naslovu http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf
34. ForeScout. (2015). *Network Access Control*. Najdeno 20. marca 2016 na spletnem naslovu http://www.forescout.com/wp-content/media/ForeScout-NAC-Datasheet.pdf
35. Fortinet. (b.l.). *Enabling secure BYOD*. Najdeno 6. februarja 2016 na spletnem naslovu http://www.fortinet.com/sites/default/files/solutionbrief/Enabling%20Secure%20BYOD.pdf
36. Fortinet. (2012). *Solution Brief – The World`s Most Intelligent and Powerful NGFW*. Najdeno 20. marca 2016 na spletnem naslovu http://www.fortinet.com/sites/default/files/solutionbrief/NGFW_Solution_Brief.pdf
37. Fortinet. (2014). *FortiOS Handbook – Advanced Routing for FortiOS 5.0*. Najdeno 20. marca 2016 na spletnem naslovu http://docs.fortinet.com/uploaded/files/1093/advanced-routing.pdf
38. Fortinet. (2015a). *Secure Wireless LAN Solutions Guide: Complete Wi-Fi Security for Any Network Topology*. Najdeno 20. marca 2016 na spletnem naslovu https://www.fortinet.com/sites/default/files/solutionbrief/Fortinet-Secure-Wireless-LAN-Solutions-Guide.pdf
39. Fortinet. (2015b). *FortiClient*. Najdeno 20. marca 2016 na spletnem naslovu http://www.fortinet.com/sites/default/files/productdatasheets/FortiClient.pdf

40. Garner, J. (2013, 13. marec). Everything you need to know about BYOD. *iMeetCentral.* Najdeno 20. marca 2016 na spletnem naslovu https://www.imeetcentral.com/everything-you-need-to-know-about-byod/
41. *Gartner Identifies Top 10 Mobile Technologies and Capabilities for 2015 and 2016*. Najdeno 20. marca 2016 na spletnem naslovu http://www.gartner.com/newsroom/id/2669915
42. *Gartner Says Worldwide PC shipments declined 8.3 Percent in Fourth Quarter of 2015*. Najdeno 20. marca 2016 na spletnem naslovu http://www.gartner.com/newsroom/id/3185224
43. Gilmore, G., & Beardmore, P. (2013). *Mobile security & BYOD for dummies, Kaspersky lab limited edition*. Chichester: John Wiley & Sons Ltd.
44. Google. (b.l.). *Google for Work Security and Compliance Whitepaper*. Najdeno 20. marca 2016 na spletnem naslovu http://www.teamcomputers.com/wp-content/white-paper/google-apps-security-and-compliance-whitepaper.pdf
45. *Google Through the Years*. Najdeno 20. marca 2016 na spletnem naslovu https://www.google.com/about/company/timeline/
46. Government Business Council. (2013). *3 Mobile Security Threats a BYOD Strategy Should Prepare For*. Najdeno 20. marca 2016 na spletnem naslovu https://www.f5.com/pdf/analyst-reports/mobility-issue-brief.pdf
47. Hazelton, C. (2015, 7. april). Virtual mobile infrastructure: What it's about, and why it's important to the enterprise. *451 Research*. Najdeno 6. februarja 2016 na spletnem naslovu http://www.hypori.com/sites/default/files/pdf/451research.pdf
48. Hmelak, M., & Žust, U. (2012). Tveganja v zvezi z uporabo lastnih osebnih naprav na delovnem mestu. *Revizor: revija o reviziji, 23*(5), 56-65.
49. Hogben, G., & Dekker, M. (2010). Smartphones: Information security risks, opportunities and recommendations for users. *ENISA.* Najdeno 20. marca 2016 na spletnem naslovu https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport
50. *Hybrid identity management*. Najdeno 20. marca 2016 na spletnem naslovu https://www.microsoft.com/en/server-cloud/solutions/identity-management.aspx
51. *MobileFirst*. Najdeno 20. marca 2016 na spletnem naslovu http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS215-078
52. Informacijski pooblaščenec RS. (2012, 15. junija). *Varstvo osebnih podatkov & računalništvo v oblaku*. Najdeno 6. februarja 2016 na spletnem naslovu https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf
53. Information Commisioner's Office UK. – ICO. (b.l.). Bring your own device (BYOD). *Data Protection Act 1998*. Najdeno 6. februarja 2016 na spletnem naslovu https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

54. *Institute of electrical and electronic engineers – IEEE*. Najdeno 20. marca 2016 na spletnem naslovu http://www.ieee.org/index.html
55. Intel. (2012). *Insights on the current state of BYOD*. Najdeno 6. Februarja 2016 na spletnem naslovu http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf
56. iPass. (b.l.). *Why BYOD needs BYON to be succesful*. Najdeno 6. februarja 2016 na spletnem naslovu https://www.ipass.com/wp-content/uploads/2015/07/iPass-White-Paper-Why-BYOD-needs-BYON.pdf
57. Jaramillo, D., Furht, B., & Agarwal, A. (2014). *Virtualization techniques for mobile systems*. Cham Heidelberg New York Dordreht London: Springer.
58. Johnson, K., & DeLaGrange, T. (2012). SANS survey on mobility/BYOD security policies and practices. *SANS Institute*. Najdeno 6. februarja 2016 na spletnem naslovu https://www.sans.org/reading-room/whitepapers/analyst/survey-mobility-byod-security-policies-practices-35175
59. Jones, J. (2012, 2. avgust). BYOD: Organizations question risk vs benefit. *Microsoft.* Najdeno 6. februarja 2016 na spletnem naslovu http://blogs.microsoft.com/cybertrust/2012/08/02/byod-organizations-question-risk-vs-benefit/
60. Kaplan, R. S., & Norton, D. P. (1992). *The Balanced Scorecard: Measures that Drive Performance*. Najdeno 20. marca 2016 na spletnem naslovu www.alnap.org/pool/files/balanced-scorecard.pdf
61. Kaplan, R. S. (2010). *Conceptual Foundations of the Balanced Scorecard*. Najdeno 20. marca 2016 na spletnem naslovu http://www.hbs.edu/faculty/Publication%20Files/10-074.pdf
62. Keyes, J. (2013). *Bring your own devices (BYOD) survival guide*. Boca Raton: CRC Press.
63. Klein, E. (2015). A mobile OS market comparison: Security is paramount. *TechTarget*. Najdeno 20. marca 2016 na spletnem naslovu http://searchmobilecomputing.techtarget.com/opinion/A-mobile-OS-market-comparison-Security-is-paramount?utm_medium=EM&asrc=EM_ERU_52717353&utm_campaign=20160126_ERU%20Transmission%20for%2001/26/2016%20(UserUniverse:%201917043)_myka-reports@techtarget.com&utm
64. *Knox Workspace*. Najdeno 20. marca 2016 na spletnem naslovu https://www.samsungknox.com/en/products/knox-workspace
65. Laird, J. (2014, 7. november). A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. *Lifehacker*. Najdeno 20. marca 2016 na spletnem naslovu http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore
66. Leavitt, N. (2013). Today`s mobile security requires a new approach. *Computer*, *46*(11), 16-19.
67. Lennartsson, K. (2010, 14. januar). How to Use Data Encryption to Secure Mobile Business Data. *eWeek.* Najdeno 20. marca 2016 na spletnem naslovu

http://www.eweek.com/c/a/Security/How-to-Use-Data-Encryption-to-Secure-Mobile-Business-Data

68. Loucks, J., Medcalf, R., Buckalew, L., & Faria, F. (2013). The financial impact of BYOD. *Cisco*. Najdeno 6. februarja 2016 na spletnem naslovu http://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD-Economics_Econ_Analysis.pdf
69. Madden, B. (2012, 29. maj). What is MDM, MAM, and MIM? (And what`s the difference). *BrianMadden.com.* Najdeno 20. marca 2016 na spletnem naslovu http://www.brianmadden.com/opinion/What-is-MDM-MAM-and-MIM-And-whats-the-difference
70. Madden, J. (2014). *Enterprise Mobility Management: Everything you need to know about MDM, MAM, & BYOD.* San Francisco: Jack Madden.
71. Madden, J. (2015, 13. avgust). Digging into virtual mobile infrastructure: What are the right use cases for VMI?. *BrianMadden.com*. Najdeno 20. marca 2016 na spletnem naslovu http://www.brianmadden.com/opinion/Digging-into-virtual-mobile-infrastructure-What-are-the-right-use-cases-for-VMI
72. *Malware Categories*. Najdeno 20. marca 2016 na spletnem https://www.gdata-software.com/security-labs/information/malware-categories
73. *Malware from A to Z*. Najdeno 20. marca 2016 na spletnem naslovu http://www.lavasoft.com/mylavasoft/securitycenter/spyware-glossary
74. Manmeet, M. S., Soh, S. S., Oh, Y. S., Nurul, H. A. H. M., & Azizul, R. M. S. (2014). Security attacks taxonomy on bring your own devices (BYOD) model. *International Journal of Mobile Network Communications & Telematics (IJMNCT), 4*(5), 1-17.
75. Markelj, B. (2012). *Grožnje informacijski varnosti pri rabi mobilnih naprav* (doktorska disertacija). Ljubljana: Fakulteta za varnostne vede.
76. Mason, M. (2016, 28. april). Data Loss Prevention in a Mobile World. *Sierraware*. Najdeno 20. marca 2016 na spletnem naslovu https://sierraware.com/blog/?p=212
77. Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and Privacy Considerations. *IT Professional*, *14*(5), 53-55.
78. *MobileIron Product Overview*. Najdeno 20. marca 2016 na spletnem naslovu https://www.mobileiron.com/en/products/product-overview
79. MobileIron. (2010). *MobileIron Virtual Smartphone Platform.* Najdeno 20. marca 2016 na spletnem naslovu http://www.brightpoint.co.uk/sites/default/files/ mobileiron_ product_datasheet.pdf
80. MobileIron. (2015). *MobileIron Cloud*. Najdeno 20. marca 2016 na spletnem naslovu https://www.mobileiron.com/sites/default/files/datasheets/files/MobileIron-Cloud-2015-Datasheet_v2.1_EN.pdf
81. *Mobile Device Management.* Najdeno 20. marca 2016 na spletnem naslovu http://www.air-watch.com/solutions/mobile-device-management/

82. Motive. (2015). *Mobile malware: A network view*. Najdeno 20. marca 2016 na spletnem https://www.blackhat.com/docs/ldn-15/materials/london-15-McNamee-Mobile-Malware-A-Network-View-wp.pdf
83. Mwenemeru, H. K. (2013). *A model to guide in the adoption of bring your own device concept in an organization* (Master Thesis). Nairobi: Strathmore University.
84. National Institute of Standards and Technology – NIST. (2002). *Risk Management Guide for Information Technology Systems*. Gaithersburg: National Institute of Standards and Technology.
85. National Institute of Standards and Technology – NIST. (2013). *Guidelines for managing the security of mobile devices in the enterprise*. Gaithersburg: National Institute of Standards and Technology.
86. *Nokia Threat Intelligence Report – H2 2015*. Najdeno 20. marca 2016 na spletnem http://resources.alcatel-lucent.com/asset/193174
87. Noor, M. M., & Hassan, W. H. (2013). Wireless Networks: Developments, Threats and Countermeasures. *International Journal of Digital Information and Wireless Communicatons (IJDIWC), 3*(1), 125-140.
88. Ocano, S. G. (2015). *Remote mobile screen (RMS): An approach for secure BYOD environments* (Master Thesis). Lincoln: University of Nebraska.
89. *Office 365 Enterprise E5*. Najdeno 20. marca 2016 na spletnem naslovu https://products.office.com/en/business/office-365-enterprise-e5-business-software
90. *OpenSSL »Hartbleed« vulnerability (CVE-2014-0160).* Najdeno 20. marca 2016 na spletnem naslovu https://www.us-cert.gov/ncas/alerts/TA14-098A
91. Orans, L. (2013). Magic Quadrant for Network Access Control. *Gartner*. Najdeno 20. marca 2016 na spletnem naslovu http://emailing.aquastar-consulting.com/2013/Infra/Newsletters/2014/Janvier/Magic-Quadrant-for-Network-Access-Control.pdf
92. Osterman Research. (2012). *The need for IT to get in front of the BYOD problem*. Najdeno 6. februarja 2016 na spletnem naslovu http://resources.idgenterprise.com/original/AST-0077420_The_Need_for_IT_to_Get_in_Front_of_the_BYOD_Problem_pdf.pdf
93. *Overview: What is Potentially Unwanted Application (PUA).* Najdeno 20. marca 2016 na spletnem naslovu https://www.sophos.com/en-us/support/knowledgebase/14887.aspx
94. *PC Market Finishes 2015 As Expected, Hopefully Setting the Stage for a More Stable Future, According to IDC*. Najdeno 20. marca 2016 na spletnem naslovu http://www.idc.com/getdoc.jsp?containerId=prUS40909316
95. Phifer, L. (2013). Mobile device management checklist. *TechTarget*. Najdeno 20. marca 2016 na spletnem naslovu http://searchmobilecomputing.techtarget.com/tip/ Mobile-device-management-checklist

96. Phifer, L. (2014). Dual persona tackles Android device security concerns. TechTarget. Najdeno 6. februarja 2016 na spletnem naslovu http://searchmobilecomputing.techtarget.com/tip/Dual-persona-tackles-Android-device -security-concerns
97. Phillips, J. J. (2003). *Return on investment in training and performance improvement programs*. Amsterdam: Butterworth-Heinemann.
98. Ponemon Institute. (2014a). *The Cost of Insecure Mobile Devices in the Workplace*. Najdeno 20. marca 2016 na spletnem naslovu http://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf
99. Ponemon Institute. (2014b). *The SQL Injection Threat Study*. Najdeno 20. marca 2016 na spletnem naslovu http://www.dbnetworks.com/pdf/ponemon-the-SQL-injection-threat-study.pdf
100. Poslovna aplikacija. (b.l.). V *iSlovarju.* Najdeno 20. marca 2016 na spletnem naslovu http://www.islovar.org/izpisclanka.asp?id=7234
101. Prashant, K. G., Arnab, G., & Shashikant, R. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4*(4), 62-70.
102. PulseSecure. (2016). *Pulse Policy Secure*. Najdeno 20. marca 2016 na spletnem naslovu https://www.pulsesecure.net/.../1474/Pulse-Policy-Secure-DataSheet.pdf
103. Rains, T. (2013, 10. julij). Trust in Computing Survey, Part I: Consumerization of IT Goes Mainstream. *Microsoft.* Najdeno 6. februarja 2016 na spletnem naslovu https://blogs.microsoft.com/cybertrust/2013/07/10/trust-in-computing-survey-part-i-consumerization-of-it-goes-mainstream/
104. Raytheon. (2014). *Trusted Access: Mobile*. Najdeno 20. marca 2016 na spletnem naslovu http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_215849.pdf
105. Redman, P. (2013, 23. maj). Critical Capabilities for Mobile Device Management Software. *Gartner*. Najdeno 20. marca 2016 na spletnem naslovu https://www.business.att.com/content/whitepaper/Gartner-Crit_Caps_for_MDM.pdf
106. Rouse, M. (2012). Dual persona (mobile device management). *TechTarget*. Najdeno 20. marca 2016 na spletnem naslovu http://searchmobilecomputing.techtarget.com/definition/dual-persona-mobile-device-management
107. Rouse, M. (2013). Mobile Device Management. *TechTarget.* Najdeno 20. marca 2016 na spletnem naslovu http://searchmobilecomputing.techtarget.com/definition/mobile-device-management
108. Rouse, M. (2014). Mobile content management. *TechTarget.* Najdeno 20. marca 2016 na spletnem naslovu http://searchmobilecomputing.techtarget.com/definition/mobile-content-management

109. RSA. (2014). *RSA SecurID: Management Console*. Najdeno 20. marca 2016 na spletnem naslovu https://www.rsa.com/content/dam/rsa/PDF/h13822-ds-rsa-securid-management-console.pdf
110. Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey if insider attack detection research. *Iniside Attack and Cyber Security, 3*, 69-90.
111. Samaras, V. (2013). *A BYOD enterprise security architecture for accessing SaaS cloud services* (Master Thesis). Delft: University of Technology.
112. Sheldon, R. (2015). Why the U.S. military uses virtual mobile infrastructure. *TechTarget*. Najdeno 20. marca 2016 na spletnem naslovu http://searchvirtualdesktop.techtarget.com/tip/Why-the-US-military-uses-virtual-mobile-infrastructure
113. Siciliano, R. (2012, 15. februar). Almost 5% of Smartphones Lost Every Year. *McAfee.* Najdeno 20. marca 2016 na spletnem naslovu https://blogs.mcafee.com/consumer/almost-5-of-smartphones-lost-every-year/
114. Sierraware. (2015). *7 Things You Need to Know about Virtual Mobile Infrastructure*. Najdeno 20. marca 2016 na spletnem naslovu https://www.sierraware.com/7_Things_to_Know_about_Virtual_Mobile_Infrastructure.pdf
115. Sierraware. (2016). *Mobile Security Checklist: An Easy, Achievable Plan for Security and Compliance*. Najdeno 20. marca 2016 na spletnem naslovu https://sierraware.com/MobileSecurityChecklistWP.pdf
116. Skybakmoen, T. (2014). Next Generation Firewall Comparative Analisys. *NSS Labs.* Najdeno 20. marca 2016 na spletnem naslovu http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-701659.pdf
117. *Smartphone OS Market Share, 2015 Q2*. Najdeno 20. marca 2016 na spletnem naslovu http://www.idc.com/prodserv/smartphone-os-market-share.jsp
118. Software Engineering Institute of Carnegie Mellon University - SEICMU. (1993). *Capability Maturity Model for Software, Version 1.1*. Najdeno 20. marca 2016 na spletnem naslovu http://www.sei.cmu.edu/reports/93tr024.pdf
119. Software Engineering Institute of Carnegie Mellon University - SEICMU. (2010). *Improving processes for providing better services*. Najdeno 20. marca 2016 na spletnem naslovu www.sei.cmu.edu/reports/10tr034.pdf
120. Sullivan, D. (2014, 28. februarja). SaaS Providers List: Comparison And Guide. *Tom`sIT PRO*. Najdeno 20. marca 2016 na spletnem naslovu http://www.tomsitpro.com/articles/saas-providers,1-1554.html
121. Svensk, K. (2013). *Exploring the possibilities and limitations with Bring Your Own Device (BYOD)* (Master Thesis). Stockholm: KTH School of Electrical Engineering.
122. Sybase. (2011). *Mobility Advantage: Why Secure Your Mobile Devices?* Najdeno 20. marca 2016 na spletnem naslovu http://hosteddocs.ittoolbox.com/whysecuritywhitepaper.pdf

123. *The Ten Most Critical Web Application Security Risks*. Najdeno 20. marca 2016 na spletnem naslovu https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
124. *Thinvisor*. Najdeno 20. marca 2016 na spletnem naslovu http://www.cellrox.com/product/#product-thinvisor
125. *Top Five Ways Any Business Can Benefit from Box*. Najdeno 20. marca 2016 na spletnem naslovu http://www.eurekasolutions.co.uk/wp-content/uploads/ 2015/11/ Top-5-Ways-Businesses-Benefit-Box-DataSheet.pdf
126. *Trackware*. Najdeno 20. marca 2016 na spletnem naslovu https://www.f-secure.com/v-descs/trackware_w32_trackware.shtml
127. *Trackware definition*. Najdeno 20. marca 2016 na spletnem naslovu http://www.trendmicro.com/vinfo/us/security/definition/trackware
128. Trend Micro. (2014). *Safe Mobile Workforce*. Najdeno 20. marca 2016 na spletnem naslovu http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ virtual-security-mobile.pdf
129. Turk, T. (2005). Analiza stroškov in koristi naložb v informatiko. *Uporabna informatika, 13*(3), 153-169.
130. *Uporaba sistema za upravljanje mobilnih naprav*. Najdeno 20. marca na spletnem naslovu https://www.ip-rs.si/vop/uporaba-sistema-za-upravljanje-mobilnih-naprav-2568/
131. Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science, 50*, 511-516.
132. *Virtual Mobile Infrastructure*. Najdeno 20. marca 2016 na spletnem naslovu https://nubosoftware.com/vmi.html
133. *VMware to Bring Virtualization to Mobile Phones, Enabling a Host of Benefits for Handset Vendors, Corporations and Mobile Phone Users.* Najdeno 20. marca 2016 na spletnem naslovu https://www.vmware.com/company/news/releases/mvp
134. Wafaa, A. (2014, 28. marec). Virtualization on ARM with Xen. *ARMConnected Community*. Najdeno 20. marca 2016 na spletnem naslovu https://community.arm.com/groups/processors/blog/2014/03/28/virtualization-on-arm-with-xen
135. Wang, Y., Wei, J., & Vangury, K. (2014). Bring Your Own Device security issues and challenges. *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)* (str. 80-85). Las Vegas: IEEE.
136. *Wired 802.1x Security*. Najdeno 20. marca 2016 na spletnem naslovu https://www.sans.org/reading-room/whitepapers/networkdevs/wired-8021x-security-1654
137. Zakon o delovnih razmerjih (ZDR-1). *Uradni list RS* št. 21/2013.
138. Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1). *Uradni list RS* št. 94/2007.
139. Zhao, Z., & Osorio, F. C. (2012). TrustDroid: Preventing the use of SmartPhones for information leaking in corporate networks through the used of static analysis taint

tracking. *Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on* (str. 135-143). Fajardo, PR: IEEE.