Univerza v Mariboru

Fakulteta za organizacijske vede

Magistrsko delo
Management informacijskih sistemov
Kakovost in varnost informacijskih sistemov

MODEL UPRAVLJANJA MOBILNIH NAPRAV IN ZASEBNOSTI Z REŠITVIJO MOBILEIRON

Mentor: red. prof. dr. Robert Leskovar

Kandidat: Andrej Vovk

Kranj, april 2016

ZAHVALA

Zahvaljujem se mentorju prof. dr. Robertu Leskovarju za pomoč in usmeritve pri izdelavi magistrske naloge.

Hvala sodelavcem iz Zavoda za zdravstveno zavarovanje Slovenije za pomoč, spodbudo, nasvete in sodelovanje.

Posebna zahvala moji družini, ki me je vse čas študija in priprave magistrske naloge spodbujala in mi stala ob strani.

POVZETEK

Raziskava obravnava razvoj modela upravljanja mobilnih naprav in zasebnosti z rešitvijo MobileIron. Analiziran je informacijski sistem Zavoda za zdravstveno zavarovanje Slovenije. Predstavljeni so posamezni segmenti, ki se nanašajo na varovanje zasebnosti: video nadzor, snemanje telefonskih pogovorov, preverjanje telefonskih pogovorov na stacionarnih in mobilnih telefonih, elektronska pošta, spremljanje nameščene programske opreme na mobilnih napravah, spremljanje lokacije mobilne naprave, spremljanje obiskanosti spletnih strani in shranjevanje podatkov mobilne naprave na centralni strežnik. Opisana je programska rešitev MobileIron ter politika upravljanja mobilnih naprav. Razvit je model upravljanja mobilnih naprav in zasebnosti za konkretno organizacijo z rešitvijo MobileIron. Model obsega človeške vire, tehnološke elemente, organizacijske elemente ter integracijo elementov. Vpeljan je bil tudi v uporabo. Empirična raziskava med zaposlenimi je pokazala, da so uporabniki zadovoljni z vpeljanim modelom, imajo pa večja pričakovanja o obdobnih usposabljanjih za varno uporabo mobilnih naprav.

KLJUČNE BESEDE:

- mobilnost
- zasebnost
- varnost
- usposabljanje
- upravljanje

ABSTRACT

This research addresses the development of the model of mobile device management and privacy with the MobileIron. The information system of the Health Insurance Institute of Slovenia is analyzed. Particular segments, related to privacy is presented: video monitoring, recording of telephone conversations, checking phone calls on stationary and mobile phones, e-mail, monitoring software installed on mobile devices, location tracking for mobile devices, tracking website visits and backup of mobile device data on central server. MobileIron software and management policy for mobile devices are presented. The developed model include human resources, technological elements, organizational elements and the integration of elements. The model was introduced in use. Empirical research among employees showed that users are satisfied with the model-established, but they have higher expectations for periodic training on the safe use of mobile devices.

KEYWORDS:

- mobility
- privacy
- safety
- training
- management

KAZALO

1. UVOD

Uporaba mobilne tehnologije raste z neverjetno hitrostjo v smeri akronima MAGIC - *Mobile Anytime Globally Integrated Customized* (NTTDoCoMo). Mobilne naprave nam omogočajo preprosto povezovanje v svetovni splet, izmenjavo ter dostop do različnih informacij, katere lahko uporabnik shrani na svoji mobilni napravi za kasnejšo uporabo. Dinamičen razvoj tehnologije, ozaveščenost, zahteve uporabnikov, hitre spremembe na pravnem področju in kompleksnost sistemov zahtevajo ustrezno znanje. Zaradi kompleksnosti in neobvladljivosti mobilne tehnologije se stalno pojavlja potreba po zaščiti in zagotavljanju varnosti z namenom zagotavljanja zaupnosti, integritete in dostopnosti vseh komponent informacijskega sistema (v nadaljevanju: IS) in naprav, ki se vanj povezujejo.

Magistrska naloga bo pripomogla k boljšemu razumevanju uvajanja mobilne tehnologije v organizacijah in oblikovanju strategije upravljanja mobilnih naprav. Predstavljeni modeli upravljanja bodo zagotavljali preglednost, enostavnost in učinkovitost upravljanje varnostnih politik na mobilnih napravah. Hkrati pa bo upoštevana zahteva po zakonitosti upravljanja podatkov, ki se zbirajo za potrebe upravljanja mobilnih naprav.

Z upravljanjem mobilnosti, poskušajo zaradi zelo velike izpostavljenosti varnostnim grožnjam, podjetja zagotoviti celovit dostop do zalednih sistemov in zmanjševanje stroškov mobilne tehnologije. Tehnološke rešitve, ki jih pri tem uporabljajo, imajo zelo napredne funkcije upravljanja, ki so vgrajene v mobilne naprave. Prav tu pa se pojavi navzkrižje interesov podjetja in posameznika. V magistrski nalogi bodo predstavljene pravne podlage in prakse v svetu, predvsem iz Evropske unije ter Slovenije na področju varovanja zasebnosti.

Tehnologija ne vključuje »neizogiben« kompromis z zasebnostjo. Le neizogibnost mora biti zahteva, da je zasebnost vrednota, ki je vgrajena v našo tehnologijo (Fakhoury, 2012).

V raziskavi bomo obravnavali Zavod za zdravstveno zavarovanje Slovenije (v nadaljevanju: Zavod), ki je bil ustanovljen marca 1992 na podlagi Zakona o zdravstvenem varstvu in zdravstvenem zavarovanju. Danes deluje kot javni zavod za izvajanje obveznega zdravstvenega zavarovanja v Republiki Sloveniji.

Osnovna funkcija Zavoda je izvajanje obveznega zdravstvenega zavarovanja, zagotavljanje učinkovitega zbiranja in razdeljevanja javnih sredstev za kakovostno uresničevanje pravic iz tega naslova. Pravice iz obveznega zdravstvenega zavarovanja zajemajo pravice do zdravstvenih storitev in do nekaterih denarnih nadomestil (boleznine, potni stroški, pogrebnine in posmrtnine).

Za izvajanje obveznega zdravstvenega zavarovanja je Zavod v letu 2014 porabil skupno nekaj več kot 2,35 milijarde evrov. Gre za porabo javnih sredstev, ki se pretežni del zbirajo na podlagi plačanih prispevkov za obvezno zdravstveno zavarovanje s strani delodajalcev in delojemalcev (ZZZS; 2015).

Zavod posluje prek svojih območnih enot z izpostavami po Sloveniji. Področje informacijske dejavnosti pokriva samostojna področna enota Informacijski center, organizacijske, vodstvene, razvojne in usklajevalne naloge pa Direkcija. Takšna poslovna mreža zagotavlja, da je zavarovalna storitev v največji meri približana zavarovancem. Ob koncu leta 2014 je bilo na Zavodu za nedoločen čas zaposlenih 865 delavcev (ZZZS; 2015).

Zavod povezuje vse lokacije poslovanja z navideznim zasebnim omrežjem, ki omogoča distribuirano delo s centralno bazo podatkov, interno komuniciranje in predstavlja komunikacijsko hrbtenico (Kapus; 2013).

Organizacijska struktura Zavoda je prikazana na sliki 1. Enote Zavoda so Direkcija, Poslovna enota Informacijski center in območne enote.

Direkcija
Na sedežu Zavoda opravljajo predvsem organizacijske, vodstvene, razvojne in usklajevalne naloge. Glede na naravo dejavnosti, so večinoma visoko izobraženi specializirani strokovnjaki ekonomskih, pravnih, medicinskih, naravoslovnih in drugih ved, ki koordinirajo delo v Zavodu (Kapus; 2013).

Poslovna enota Informacijski center
V področni enoti Informacijski center delavci skrbijo za izdelavo in vzdrževanje baz podatkov, informacijskih rešitev ter informacijsko-komunikacijsko opremo (Kapus; 2013).

Poslovna mreža Zavoda
Zavod ima 10 območnih enot s 45 izpostavami. Vsaka območna enota s svojim delovanjem pokriva določeno območje. V njenem okviru pa obstaja mreža izpostav, ki poslujejo v posameznih občinah (Kapus; 2013).

V okviru poslovne mreže Zavoda delujejo naslednje območne enote (v nadaljevanju: OE):

- OE Celje (Laško, Šmarje pri Jelšah, Slovenske Konjice, Žalec, Šentjur pri Celju);
- OE Koper (Ilirska Bistrica Izola, Piran, Postojna Sežana);
- OE Krško (Brežice, Sevnica);
- OE Kranj (Jesenice, Škofja Loka, Radovljica, Tržič),
- OE Ljubljana (Cerknica, Domžale, Grosuplje, Hrastnik, Idrija, Kamnik, Litija, Logatec, Ribnica, Trbovlje, Vrhnika, Zagorje);
- OE Maribor (Ormož, Lenart, Ptuj, Slovenska Bistrica);
- OE Murska Sobota (Gornja Radgona, Lendava, Ljutomer);
- OE Nova Gorica (Ajdovščina, Tolmin);
- OE Novo mesto (Črnomelj, Metlika, Trebnje);
- OE Ravne na Koroškem (Mozirje. Slovenj Gradec, Radlje ob Dravi, Velenje).

Slika 1: Makro organizacijska struktura Zavoda (Vir: ZZZS)

Na območnih enotah oziroma v njihovih izpostavah poteka delo z zavezanci za izpolnjevanje ter vlaganje in sprejemanje obrazcev. Sedanji sistem temelji pretežno še na papirni dokumentaciji. Za lažje poslovanje Zavoda in poenostavitev postopkov Zavod pospešeno izvaja dejavnosti za informatizacijo poslovanja in približevanje storitev uporabnikom (zavarovancem, izvajalcem – dobaviteljem in zavezancem za plačevanje prispevkov (Kapus; 2013).

V raziskavi bo uporabljena rešitev MobileIron, ki je bila v letu 2014 uvrščena med vodilne produkte v Gartnerjevem magičnem kvadrantu za upravljanje mobilnih naprav v podjetju (Gartner, 2014).

2. METODOLOGIJA DELA

2.1. DEFINICIJA PROBLEMA

Po desetletjih nenehnih sprememb je razvoj tehnologije na področju mobilne telefonije vse bolj intenziven. Ob tem se veča število uporabnikov in širi se nabor funkcionalnosti mobilnega aparata. Vse to rojeva burne poslovne aktivnosti, od širitve trgov in vzpona blagovnih znamk do globalnih prevzemov in zavezništev. Tehnološko, uporabniško in poslovno ekspanzijo mobilne telefonije spremljata tudi nenehna oglaševalska prisotnost in medijska izpostavljenost, predvsem pa številni izzivi na področju potrošnje, izobraževanja, prava, zdravja, politike, poslovanja, zabave, organiziranosti, medosebnih odnosov itd. (Vehovar, 2007)

Mobilne naprave so še posebej primerne za zagotavljanje dostopnosti informacij. Najprej je treba ugotoviti, katere informacije se lahko dajo na voljo in ali je smiselno, da so na voljo mobilno. Mobilnost je v tem primeru elastična beseda: začne se s zaposlenim, ki sedi za svojo mizo ter s pomočjo pametnega telefona dostopa do podatkov, saj je le ta dostop hitrejši in bolj priročen. To lahko pomeni, da zaposleni lahko preverijo svoje dogovorjene sestanke za naslednji dan tudi po vrnitvi domov ter delujejo popolnoma mobilno (Majchrzak in Heitkőtter, 2013).

S povečanjem števila uporabljenih mobilnih naprav, le te postajajo primarne naprave številnim zaposlenim, saj lahko nadomeščajo tako namizne kot tudi prenosne računalnike. Mobilne naprave tako zamenjujejo namizne telefone kot glavno ikono komunikacijska orodja za zaposlene v pisarniškem okolju (Osterman Research, 2011).

Nakup pametnega telefona vsakemu zaposlenemu, je zelo draga naložba za podjetje, ki ga lahko obravnavamo tudi kot negospodarna naložba, saj zaposleni že ima svoj privatni pametni telefon, kateri je več kot sposoben opraviti zahtevano funkcijo. S tem bi podjetja prihranila znatno količino denarja (Majdi, 2013).

Na pametnem telefonu bo uporabnik moral narediti praktično vse, kar danes opravi z osebnim računalnikom: komunicira, išče, nakupuje, plačuje, igra, bere, se zabava itd. Za izvajanje teh opravil, uporabniki uporabljajo posebej razvito programsko opremo, ki se izvaja na njihovih mobilnih napravah. Glavna značilnost večine te opreme je izjemna uporabniška izkušnja, izkoriščanje vseh zmožnosti naprave, ki še dodatno poveča enostavnost in uporabnost mobilnih naprav. Uporabniki mobilnih naprav pričakujejo, da imajo orodje za hiter in enostaven dostop do informacij ali produktov. Le-te pa morajo imeti sposobnost upoštevati preference uporabnika, lokacijo, čas, pretekle izkušnje ter na tej osnovi uporabniku pomagati, svetovati ali ponuditi pravi odgovor (InfoSRC, 2012).

Pametni telefoni lahko vsebujejo velike količine podatkov pravnih oseb, ki so občutljive narave in lahko škodijo v primeru nepooblaščenega vpogleda v podatke.

Hkrati pa tudi dostopajo do informacijskih virov podjetji, kot so sistemi za elektronsko pošto, podatkovne baze, arhive in druga sredstva. Dostop do teh virov pa lahko povzroči okužbo z zlonamerno programsko opremo, ki povzroča škodo na informacijskih virih, saj večina uporabnikov ne uporablja nikakršne obrambe na svoji pametni napravi (Majdi, 2013).

Slabo ali nesprejemljivo vedenje končnih uporabnikov glede varnosti, je velik problem za organizacijo ter povzročitelj velikega števila informacijskih incidentov (Leach, 2003).

Ovire pri ozaveščanju o informacijski varnosti v organizacijah se pojavljajo kot: splošna ozaveščenost o varnosti, računalniško znanje zaposlenih in proračun organizacije. Možnosti za boj proti temu je sprejetje ustrezne usmeritve usposabljanja za vse uporabnike v vladnih informacijskih okoljih. Za programe usposabljanja je potrebno preveriti kako lahko vplivajo na obnašanje končnega uporabnika in s tem upravičenost časa in stroškov (Charest, 2013).

Pristop uvedbe strategije upravljanja pametnih mobilnih naprav temelji na približevanju produktivnost zaposlenih in hkrati ustrezni zaščiti na način, ki upravlja naprave, aplikativne rešitve in podatke na pametnih mobilnih napravah. Vsako podjetje potrebuje v mobilni strategiji predvideti ustrezne rešitve za upravljanje mobilnih naprav, ki bi lahko zagotavljale varnost ter zasebnost tako zaposlenim kot podjetju (Majdi, 2013).

Smotrno je poiskati takšno rešitev, s katero lahko podjetje obvladuje vse naprave v poslovnem okolju in ne le omejen nabor platform. V nasprotnem primeru je potrebno namestiti več različnih rešitev za upravljanje, kar močno poveča kompleksnost, otežuje doslednost nastavitev ter zagotavljanje skladnosti na napravah različnih proizvajalcev (InfoSRC, 2013).

Z vedno večjo razširjenostjo mobilnih naprav se na strani podjetij kaže tudi vedno večja potreba po njihovem obvladovanju. Pozitiven učinek povečanja produktivnosti spremlja določena mera tveganja, vendar je to tveganje s pametnim in premišljenim pristopom obvladljivo. Namen obvladovanja mobilnih naprav je predvsem varovanje podatkov podjetja. Skrbniki IS potrebujejo nadzor, kako in na kakšen način mobilne naprave dostopajo do virov podjetja. S pravo mero zagotavljanja integritete in varnosti ter obenem zagotavljanje preprostega dostopa do poslovnih aplikacij omogoča organizacijam konkurenčno prednost v prihodnosti (InfoSRC, 2013).

Mobilna varnost je zelo pomembna tema. Varnostni sistem je treba obravnavati v začetnem procesu načrtovanja, saj ga je izredno težko oblikovati po že uvedenem sistemu (Jansen in Scarfone, 2008). Strokovnjaki za varnost se močno zavedajo, da je pri napadalcih veliko zanimanja, da bi izkoristili napake mobilnih naprav za napade na podoben način, kot jih lahko opravijo na tradicionalnem računalniku (Viega in Michael, 2010).

Mobilna varnost zaobjema varnost podatkov in aplikacij na mobilnih napravah, ki se uporabljajo v okviru podjetja. Le to je izjemnega pomena, zaradi občutljivih informacij shranjenih na napravah. Varnost je treba upoštevati tako pri upravljanju naprav, zaposlenih in pri razvoju aplikacije za notranjo ali zunanjo

uporabo. Na eni strani, standardni varnostni pomisleki znani tudi iz namiznih in prenosnih računalnikov, na primer v povezavi z brezžično komunikacijo in pooblastili za uporabo aplikacij. Po drugi strani, pa zahtevajo posebne varnostne ukrepe zaradi njihove mobilnosti, na primer, varstvo podatkov v primeru kraje ali izgube. Resne izzive predstavlja edinstvena kombinacija varnostnih tveganj, skupaj z nivojem ozaveščenosti uporabnikov zaradi igrive uporabe mobilnih naprav. Poleg tega uporabniki pogosto uporabljajo mobilne naprave v zasebni in poslovni rabi do točke, kjer zaposleni uporabi svojo privatno mobilno napravo za delo v službi – Bring Your Own Device (v nadaljevanju: BYOD).

Strokovnjaki za varnost opažajo, da so na mobilnih napravah napadi v vzponu v primerjavi s tradicionalnim računalnikom (Rose, 2012). Po Jansen in Scarfone (2008), v kolikor mobilne naprave niso ustrezno obravnavane v varnostnih načrtih podjetji, bo večja verjetnost za ogrožanje varnosti informacijske infrastrukture.

Mobilna naprava je lahko kjer koli po svetu in ima možnost, da se poveže v informacijsko infrastrukturo organizacije za potrebe povezovanja, kar predstavlja izziv za proces upravljanja (Jansen, idr., 2004). Uporabnikom, ki delujejo izven običajnega delovnega okolja, jim morajo zaupati, da izvajajo pozitivni nadzor nad svojimi mobilnimi napravami v vsakem trenutku.

Težava pri zagotavljanju varnosti mobilnih naprav, zvišuje stroške ocene varnosti glede na kratek življenjski cikel mobilnih naprav v primerjavi s tradicionalnimi omrežnimi napravami (Viega in Michael, 2010).

Varnostne politike na mobilnih napravah, je treba izvajati in nadzirati, da dosežemo učinkovit varnostni nivo na nivoju celotnega podjetja (Liu, idr., 2010). Centralizirano upravljanje varnosti poenostavlja nadzor, upravljanje in spoštovanje politike mobilnih naprav v podjetju (Jansen in Scarfone, 2008). Varnost mobilnih naprav in razširljivost le teh, sta ključnega pomena za uspeh podjetja pri izvajanju rešitev za mobilnost v podjetju (Liu, idr., 2010).

Avtomatizirana orodja zmanjšujejo izpostavljenost tveganju zaradi napačne konfiguracije s katerimi se srečujejo pri podeljevanju in odvzemanju pooblastil v informacijskem okolju (Mont in Brown, 2011). Podeljevanje in odvzemanje pooblastil v informacijskem okolju so pomembni pri upravljanju računov in pravicah za dostop do sistema. Napake lahko povzroči izkoriščanje sistema, vključno z nepooblaščenim dostopom informacij in virov, ter zloraba poverilnic za nezakonite namene (Mont in Brown, 2011).

Rešitve za upravljanje mobilnih naprav omogočajo upravljanje varnostnih politik ter zagotavljajo sredstva za odziv na izgubo naprave. Ponudniki platforme za mobilne naprave, kot so Google in Apple, sta pripravila smernice za razvijanje varnih aplikacij. Kljub temu, celovit varnostni pristop še vedno zahteva veliko truda in znanja (Majchrzak in Heitkőtter, 2013).

Potreben napor in trud za uvedbo varnosti za mobilne naprave je odvisen tudi od upoštevanja ravni kritičnosti informacij. Priporočljivo je, da je programska oprema pripravljena na način, ki omogoča uporabnikom širok spekter različnih nastavitev, kar bo pripomoglo k učinkovitejši uporabi nameščene rešitve.

Upravljanje mobilnih naprav predstavlja množico medsebojno povezanih funkcij, ki jih je potrebno obravnavati celovito. Zagotoviti je potreben konsistenten in vsestranski pristop pri upravljanju mobilnih naprav od programske, strojne opreme, varnosti in večkrat pozabljeno področje zakonodaje glede zasebnosti. Pravica do zasebnosti ni trdno in univerzalno definirana, saj je dojemanje zasebnosti izrazito subjektivno. Poleg tega v pravu prevladuje pristop varstva in s tem definiranja pravice do zasebnosti prek poseganja vanjo (da torej pravo predvsem prepoveduje določene posege v zasebnost) (Orehar-Ivanc, 2002). Zato in zaradi pritiskov širjenja družbenega na območje zasebne sfere, gre pri pravnem varstvu pravice do zasebnosti, večinoma le za reakcijo na pritiske, ne pa toliko za vnaprejšnje postavljanje omejitev ali varstva. Literatura sicer kot poglavitni dejavnik, ki je povzročil zahteve po prilagajanju načel varstva zasebnosti v pravu, izpostavlja tehnološke spremembe (Gellman, 2001, v Kovačič, 2006).

Tehnološke rešitve na področju upravljanja mobilnosti, poskušajo zaradi zelo velike izpostavljenosti varnostnim grožnjam, zagotavljanju celovitega dostopa do zalednih sistemov in zmanjševanju stroškov mobilne tehnologije, uporabljati zelo napredne funkcije upravljanja, ki so vgrajene v mobilne naprave. Prav tu pa se pojavi navzkrižje interesov podjetja in posameznika. Podjetje ima pravico in dolžnost do varovanja zaupnih poslovnih ali osebnih podatkov, zmanjševanja stroškov in povečanja učinkovitosti poslovanja.

Zaposleni želi ali pa je celo zahtevano s strani delodajalca, da je le ta vključen v delovni proces tudi preko mobilne naprave. Le to pa zaposlenemu omogoči večjo vpetost v delovni proces in učinkovitejše opravljanje dela. Pri delu z mobilno tehnologijo se mora upoštevati zaposlenemu pravico do zasebnosti in uporabo svoje mobilne naprave v polni funkcionalnosti.

2.2. DEFINICIJA CILJEV

Namen magistrske naloge je predstaviti upravljanja mobilnih odjemalcev in zasebnosti v konkretni organizaciji z rešitvijo MobileIron. Glavni cilji naloge so:

- Izvesti študij aktualne literature s področja upravljanja mobilnih naprav in zasebnosti.
- Analizirati stanje upravljanja mobilnih odjemalcev in zasebnosti v konkretni organizaciji;
- Razviti celovit model upravljanja mobilnih odjemalcev in zasebnosti za konkretno organizacijo;
- Testirati in uvesti model celovitega upravljanja mobilnih odjemalcev in zasebnosti v konkretni organizaciji;
- Evalvirati učinke uvedbe modela upravljanja mobilnih odjemalcev in zasebnosti v konkretni organizaciji ter predlagati izboljšave.

Razviti model in pridobljene izkušnje bosta lahko strokovnjakom na področju informacijske tehnologije (v nadaljevanju: IT) pomagale pri vpeljavi učinkovitih pristopov in tako povečala verjetnost uspeha takih projektov.

2.3. UPORABLJENE METODE, TEHNIKE IN PROGRAMSKE REŠITVE

V teoretičnem delu magistrske naloge bom proučil strokovno literaturo domačih ter tujih avtorjev s področja upravljanja mobilne tehnologije, zbiranje ter obdelovanje osebnih podatkov na mobilnih napravah ter s tem povezane kršitve do zasebnosti. Uporabljene bodo deskriptivne metode za pregled domače in tuje literature s področja obravnavane tematike (analiza objavljenih člankov, strokovnih knjig in druge literature).

Empirični del magistrske naloge bo temeljil na študiju literature, programske opreme MobileIron in pametnih mobilnih naprav z nameščenim operacijskim sistemom Android. Na osnovi teh okolji se bodo pripravili modeli upravljanja mobilne tehnologije v organizaciji tipa javne uprave. Evalvacijo modela bom izvedel pri zaposlenih, ki imajo v uporabi službene mobilne naprave in bo vključevala zadovoljstvo pri uporabi pametnih mobilnih naprav z nastavljenimi nivoji varnostnih mehanizmov.

Priprava modelov upravljanja se bo izvajala na produktu MobileIron, ki je bil v letu 2014 s strani analitskega podjetja Gartner, uvrščen med vodilne produkte v magičnem kvadrantu za upravljanje mobilnih naprav v podjetju (Gartner, 2014).

2.4. POMEMBNE PREDHODNE RAZISKAVE

Industrija pametnih mobilnih telefonov in tabličnih računalnikov je zadnje čase ena najbolj rastočih industrij na svetu. Število prodanih pametnih mobilnih naprav je preseglo število prodanih osebnih računalnikov in po napovedih analitikov, bo to razmerje še drastično naraslo. Ogromni potencial, ki ga imajo mobilne naprave, bo za uporabnike najbolj vidna sprememba v načinu uporabe svoje mobilne naprave. To ne bo več samo naprava za pogovarjanje in pisanje kratkih sporočil, to bo pri mnogih edini računalnik, ki bo v stalni uporabi. Mobilnost je začetek trenda prehoda k sistemom vključenosti, ki podjetjem omogočajo, da uporabnike vključijo ter ponudijo vsebinsko bogate aplikacije in pametne rešitve, ki jim pomagajo pri takojšnjih poslovnih odločitvah. Osnova novega sistema so ljudje in ne procesi. Temelji na mobilnosti, družbenosti in računalništvu v oblaku ter na tej osnovi prinaša aplikacije in pametne rešitve naravnost v uporabnikov kontekst uporabe.

2.4.1. MOBILNOST

BYOD

BYOD je pojem, ki se je v zadnjih letih pojavil kot odgovor na nastanek velikega števila pametnih mobilnih naprav v poslovnem okolju, katerih lastniki so zaposleni. Podjetja na področju IT varnosti v zadnjih letih poskušajo nadomestiti vrzel, ki se je pojavila pri zaščiti pametnih mobilnih naprav, programske opreme in podatkov shranjenih na njih.

Zadnje desetletje so pametne mobilne naprave bistveno spremenile poslovna okolja in prosti čas uporabnikov. Število teh naprav (mobilni telefoni, tablice in

prenosni računalniki) se naglo povečuje, s tem pa tudi število programskih in tehnoloških rešitev, načinov uporabe ter podatkov na njih. Poleg teh rešitev, pa so se pojavile tudi sodobne storitve v oblaku (Facebook, Google, Dropbox, iTunes itd.), ki so sestavni del mobilnega sveta in uporabnike vežejo z napravo čez ves dan.

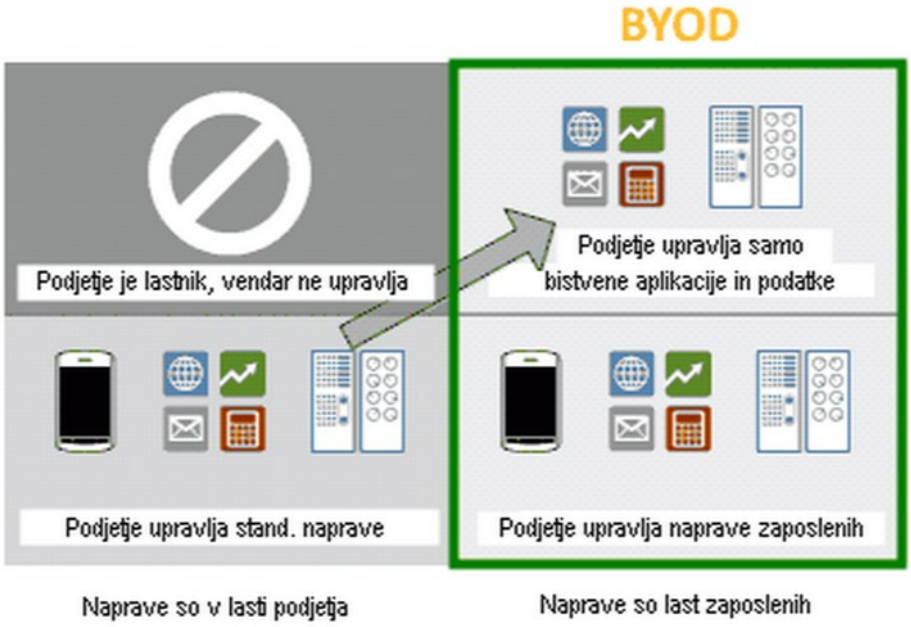
V podjetjih, na vodilnih položajih ter v storitvenih službah, so pametne mobilne naprave skoraj nujno potrebno »orodje« za opravljanje svojega dela. Mobilnost in dostop do podatkov v/in izven delovnega časa je za skoraj vse zaposlene zaželena. Zaposleni zahtevajo svobodo, zasebnost in produktivnosti na način, da imajo enostaven dostop do podatkov, tehničnih rešitev, elektronske pošte, itd, hkrati pa imajo možnost uporabe najnovejše tehnologije, ki je na trgu (mobilne telefone, tablične računalnike in programske opreme). Pomembno je, da ostanejo njihovi osebni podatki in programska oprema varno shranjeni.

Trendi in želje, da bi povečali produktivnost, fleksibilnost delovnega časa in mest, zaposleni želijo, da pri svojem delu uporabljajo naprave, ki so v njihovi lasti oz. oblikuje se koncept BYOD, kar pomeni »prinesi svojo lastno napravo«. Prednosti BYOD je tako za zaposlene kot tudi za podjetje, vendar je treba, te naprave ustrezno nadzorovati, zagotoviti ustrezni nivo varnosti naprave, programske opreme in podatkov.

Zagotavljanje ustreznega upravljanja pametnih mobilnih naprav lahko zagotovimo s tehnološko rešitvijo - upravljanje mobilnih naprav oz. *Mobile Data Management* (v nadaljevanju: MDM). Rešitev mora zagotavljati prikaz nivoja varnosti programske opreme ter spremljanje, upravljanje in široko podporo mobilnim napravam. Funkcionalnosti MDM sistemov zajemajo distribucijo programske opreme, podatkov in varnostnih politik za različne vrste pametnih mobilnih naprav, kot so mobilni telefoni, tablični računalniki itd. na različnih sistemskih platformah Android, iOS, Windows Phone itd.

Strategija BYOD

Na sliki 2 so prikazane štiri faze sprejemanja strategije BYOD. Spodnji levi kvadrat je tradicionalni model, v katerem so pametne mobilne naprave v lasti družbe in jih tudi družba v celoti upravlja. Desna stran predstavlja naprave, ki so v lasti zaposlenih. Spodnji desni kvadrat je scenarij, v katerem podjetje kljub temu, da je lastnik pametne mobilne naprave zaposleni, v celoti upravlja z napravo. V tem primeru lahko govorimo, da je na neki način naprava »ukradena« lastniku, saj mu lahko zelo omeji uporabnost naprave. Desno zgornja stran, je področje, na katerem želimo, da uveljavljamo strategijo BYOD. V tem področju se uporabljajo manj pomembne naprave na katerih je nameščenih več programske opreme in podatkov do katerih se dostopa, vendar le te niso v lasti podjetja.



Slika 2: Štiri faze sprejemanja strategije BYOD (vir: https://www.symantec.com)

Vsako podjetje oblikuje svojo strategijo BYOD, ki je odvisna od poslovnih potreb. Strategija se začne z oceno glede na to kdo je lastnik naprave in kakšen bo nivo upravljanja oz. nadzora, je prikazan na sliki 2. Večina podjetji se bo zaradi poslovnih potreb in pritiskov zaposlenih pozicioniralo v več kot v enem kvadratu (Symantec, 2013).

V nadaljevanju podajam razlago posameznih kvadrantov (Symantec, 2013):

1. V zgornjem levem kvadrantu matrike, so podjetja, ki imajo v lasti napravo, vendar jih ne nadzirajo, spremljajo in pogosto jih tudi nimajo v evidenci. Ti primeri so, ko lahko zaposleni kupijo pametno mobilno napravo na račun podjetja, vendar o nakupu niso bili obveščeni v oddelku informacije tehnologije. Pogosto so nastavitve za vstop v pametno mobilno napravo s šibkim geslom ali pa celo brez uporabniškega gesla. Na napravi so shranjeni uporabniški podatki ali pa celo podatki podjetja z različnimi nivoji zaupnosti. Varnostna tveganja so v teh primerih precej očitna. Naprave v tem kvadrantu je treba čim prej preseliti v obvladljiv kvadrant.

2. Kvadrant v levem spodnjem delu predstavlja tradicionalni pristop, v katerem ima podjetje omejen nabor mobilnih naprav. Pri tem imajo popoln nadzor z nameščanjem, nastavitvami, upravljanju varnosti programske opreme na pametnih mobilnih napravah. Ta pristop je enak kot pri običajnih osebnih in prenosnih računalnikih, kjer ima podjetje v lasti napravo in je odgovorno za njegovo celovito upravljanje.

3. Spodnji desni kvadrant prikazuje naprave za dostop, ki so v lasti zaposlenih oz. tako imenovane »BYOD« mobilne naprave. V tem primeru podjetje vzpostavi

nadzor nad pametno mobilno napravo, tako, da so podatki na napravi ustrezno zaščiteni in dostop do zalednih sistemov podjetja ustrezno varovani. Vendar pa obstaja velika razlika v pričakovanjih glede zasebnosti. Tak način upravljanja pametnih mobilnih naprav je primeren, ko nadzor in omejitve niso prestroge. V primeru, da mora podjetje zaradi svoje panoge, kot so zdravstveno varstvo, finančni in vladni resorji, zvišati nivo zahtevane varnosti. Zaposlenim se zaradi uvedbe restriktivne politike na pametnih mobilnih napravah, ki so jih sami kupili, ne zdi ustrezen. To se imenuje napravam usmerjen model - *device-centric*.

4. Zgornji desni kvadrant je primer kompromisa med zaposlenim, ki je kupil pametno mobilno napravo in podjetjem, ki omogoča dostop do zalednih sistemov podjetja. Tukaj ni namen uveljavljanja restriktivne varnostne politike ali nadzora nad celotno napravo. Namesto tega so podatki do katerih dostopa zaposleni ustrezno zaščiteni s specifično programsko opremo, v katerih ti podatki tudi ostanejo. To se imenuje aplikacijam usmerjen model - *application-centric*. Potreba po uvedbi zaščitnih ukrepov nadzora pri ključnih specifičnih aplikativnih rešitvah se bistveno zmanjša. Ta pristop je dober za podjetje, ki želi uvesti model upravljanja pametnih mobilnih naprav, ki je v lasti zaposlenih, vendar nima potrebe po popolnem nadzoru nad mobilno napravo.

Strategija in rešitve za obvladovanje mobilnih naprav v podjetju

Pristop uvedbe strategije upravljanja pametnih mobilnih naprav temelji na približevanju produktivnosti zaposlenih in hkrati ustrezni zaščiti na način, ki upravlja naprave, aplikativne rešitve in podatke na pametnih mobilnih napravah. Smotrno je poiskati takšno rešitev, s katero lahko podjetje obvladuje vse naprave v poslovnem okolju in ne le omejen nabor platform. V nasprotnem primeru je treba namestiti več različnih rešitev za upravljanje, kar močno poveča kompleksnost, otežuje doslednost nastavitev ter zagotavljanje skladnosti na napravah različnih proizvajalcev.

Izzivi s katerimi se srečujejo oddelki IT glede mobilnih naprav so:

- Prehod iz uniformiranega, po navadi Windows okolja, v okolje z več operacijski sistemi;
- Varnostna vprašanja glede mobilnih naprav: naprave vsebujejo občutljive podatke, izgubljene/ukradene naprave, zaščita pred ne zaželeno kodo;
- Celovita podpora varnostnim zahtevam za dostop do podatkov v omrežju podjetja;
- Priprava strategije za mobilno programsko opremo: namestitve iz različnih virov, razvoj in tipi lastne programske opreme za dostop do podatkov podjetja za zaposlene, stranke in partnerje;
- Manj kontrole, več naprav, enaka odgovornost;
- Obvladovanje stroškov povezanih z mobilno tehnologijo, gostovanje pri tujih mobilnih operaterjih;
- Uporabniki zahtevajo sodobne in zmogljive naprave z več mobilnimi storitvami.

Podjetja morajo zagotoviti izvedbo petih ciljev, ki so podlaga za mobilno strategijo. Pričakovano je, da izvedejo vseh pet ciljev na vseh kontrolnih točkah (naprave, programska oprema, podatki):

1. Dostop uporabnika in programske opreme
Vsaka oseba, programska oprema in naprava, ki se povezuje z zalednim sistemom podjetja se mora predstaviti kot poslovni subjekt podjetja. Preverjanje pristnosti je še posebej pomembno na področju mobilnosti, saj dostop do pametnih mobilnih naprav in virov v oblaku ni pod nadzorom, kot je to urejeno na namiznih delovnih napravah v omrežje podjetja. Postopki preverjanja pristnosti morajo biti pregledni za zaposlene.

2. Varstvo podatkov in programske opreme
Poslovni podatki morajo biti vedno zaščiteni. Več kot mobilna programska oprema dostopa, zbira, hrani in pošilja poslovne podatke, bolj občutljivi so podatki, ki so shranjeni ali potujejo do mobilnih naprav. Ravno v takih primerih je treba programsko opremo in podatke ustrezno opremiti z zaščito, ki ustreza varnostni politiki podjetja.

3. Upravljanje s pametno mobilno napravo
Naprave, ki imajo dostop do poslovnih informacijskih virov in omrežij, morajo imeti možnost upravljanja in uveljavljanja varnostnih nastavitev tako, da so v skladu z varnostno politiko podjetij. Podjetja v svojih aktih varnostne politike opredelijo strategijo upravljanja in nadziranja za pametne mobilne naprave, enako, kot so opredeljena za namizne in prenosne računalnike.

4. Zaščita pred grožnjami
Število pametnih mobilnih naprav je v zelo velikem porastu. Zaradi tega pa so pametne mobilne naprave postale tarča napadalcev iz interneta. Različne platforme imajo različna tveganja, zato je pomembno razumeti, ranljivosti in potrebne ukrepe za njihovo obvladovanje. Pametne mobilne naprave morajo biti ustrezno zaščitene pred zunanjimi napadi zlonamerne programske kode, nevarno brskanje po internetu, odtujitvi ali zlorabi.

5. Varna izmenjava podatkov
Čeprav souporaba, dostop in shranjevanje datotek ni samo izziv za pametne mobilne naprave, če upoštevamo, da je pametnih mobilnih naprav več kot drugih, so storitve v oblaku očitno enostavna rešitev za souporabo in sinhronizacijo podatkov med pametnimi mobilnimi napravami. Podjetja morajo imeti popoln nadzor nad storitvami izmenjave in dostopov do poslovnih dokumentov v omrežju, še posebej v oblaku.

Ne glede na tip rešitve upravljanja naprav (kot nadgradnja ali samostojna rešitev) mora rešitev zagotavljati upravljanje naslednjih funkcionalnosti:

- Celovito upravljanje sredstev, popis strojne in programske opreme z namenom upravljanja celotnega življenjskega cikla mobilne naprave in s tem zmanjševanje stroškov lastništva.
- Samodejno in centralizirano upravljanje mobilne programske opreme:
    - Namestitev;
    - Odstranitev;
    - Nameščanje popravkov;

    - Konfiguracija;
    - Virtualizacija.
- Avtomatizacija uvedbe varnostnih politik iz namiznih računalnikov na mobilne naprave:
    - Centralno zaklepanje/odklepanje mobilne naprave;
    - Upravljanje politike gesel;
    - Šifriranje podatkov;
    - Kontrola skladnosti mobilne naprave.
- Operativne naloge IT:
    - Varnostno kopiranje vsebin mobilnih naprav;
    - Pomoč uporabnikom preko oddaljenega dostopa;
    - Spremljanje statusa naprave;
    - Spremljanje stroškov tako za govor, SMS in prenos podatkov ter alarmiranje ob prekoračitvi mejnih vrednosti.

Razvoj funkcij upravljanja mobilnih naprav na Android OS

Sprva jedro različice Android, ni imelo potrebnih programskih vmesnikov (v nadaljevanju: API) za upravljanje, saj se je pričakovalo, da jih bodo pripravili sami proizvajalci mobilnih naprav. Različica Android jedra 2.2 je imela vgrajene osnovne funkcije za upravljanje mobilne naprave, v katero je bilo vključeno upravljanje s politiko gesla, daljinsko zaklepanje ter oddaljeno brisanje mobilne naprave. Različici jedra Android 3.0 je bila dodana funkcionalnost šifriranja naprave, v verziji jedra 4.0 pa možnost onemogočanja uporabe vgrajenega fotoaparata. Android 4.3 Jellybean je predstavil možnost centralnega nadzora nastavitev Wifi. Deljene uporabe mobilnih naprav, so v podjetju pogost pojav, saj si zaradi poslovnih potreb zaposleni delijo mobilno napravo. Z nadgradnjo na posodobitev Android 4.4 KitKat se lahko različnim uporabnikom iste mobilne naprave omogoči, da uporabljajo napravo tako, da ne vplivajo na druge uporabnike na napravi. Upravljanje z vsebinami, pregledovanje in shranjevanje dokumentov, slik in drugih vrst datotek je za posameznega uporabnika na napravi omogočeno ločeno shranjevanje. Zadnja objavljena verzija Android 5.0 Lollipop uvaja nov model upravljanja mobilnih naprav *Android for Work*. Tehnologija je bila razvita s strani proizvajalca Google in temelji na ločevanju osebnih in delovnih podatkov na mobilni napravi. Upravljanje okolja mobilne naprave pa se izvaja preko vgrajenih API funkcij. Uporabnik je do sedaj uporabljal dodatne varnostne načine za dostop do mobilne naprave s PIN kodo ali vzorcem, z verzijo Android 5.0 pa je mogoče, da uporabnik svojo napravo uporabi tudi v primeru, da je v bližini zaupanja vredna naprava Bluetooth ali pa NFC (*Near Field Communication*) oznaka.

Različni proizvajalci kot so Samsung, Motorola, HTC in drugi, imajo v svojih mobilnih napravah nekoliko različne zmogljivosti upravljanja mobilnih naprav kljub dejstvu, da vse mobilne naprave delujejo na istem jedru sistemske platforme. To pa pomeni razdrobljenost na področju upravljanja mobilnih naprav ter zelo velik izziv proizvajalcem produktov MDM, da svoje produkte pripravijo za čim bolj dosledno upravljanje v vseh teh različnih mobilnih napravah.

2.4.2. UPRAVLJANJE POLITIKE ZASEBNOSTI

Zasebnost je v zadnjem času pogosto uporabljen pojem, saj sodobne tehnologije, ki omogočajo učinkovit elektronski nadzor, shranjevanje in obdelovanje informacij, omogočajo enostaven nadzor nad posamezniki, kar sproža pomisleke glede upravičenosti takih posegov. Kljub vsesplošni uporabi pojma zasebnost, dobimo od vsakega posameznika nekoliko drugačen odgovor na vprašanje, kaj mu pomeni zasebnost. Med prve, ki so uvedli koncept zasebnosti in ločevali javno ter zasebno sfero, je bil Aristotel. Razlikoval je sferi v grški družbi - *oikos*, sfero v okviru doma, in *polis*, javno sfero (Vukelič B., 2007).

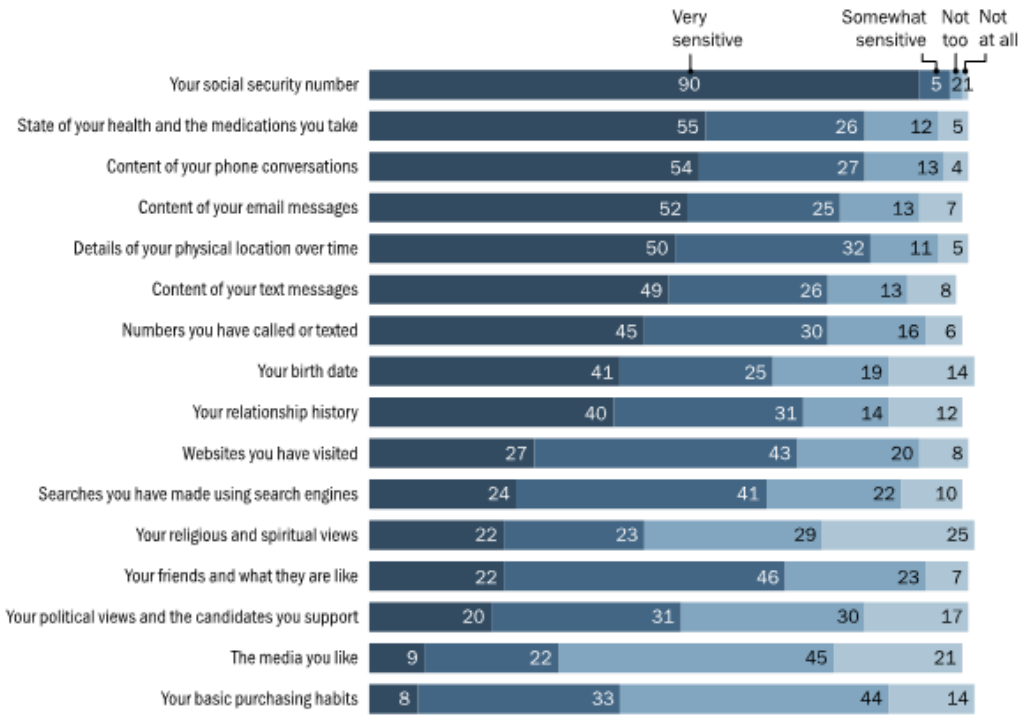
Zasebnost v splošnem kontekstu je definirana kot »meja, do katere lahko družba posega v posameznikove zadeve« (Davies v Laurant, 2003 v Pestotnik, 2007).

Robert Ellis Smith (1964) je zasebnosti definiral, kot »želja vsakega izmed nas za fizičen prostor, v katerem nas nihče ne moti, ne nadleguje, ne spravlja v zadrego, v katerem nimamo odgovornosti in imamo možnost in priložnost sami nadzorovati čas in način razkrivanja privatnih informacij o nas« (Laurant 2003, v Pestotnik, 2007).

Zasebnost je temelj človekovega dostojanstva in ostalih vrednot, kot so svoboda združevanja in svoboda govora. V današnjem svetu pa je postala zasebnost celo ena izmed najpomembnejših človekovih pravic. Poznajo jo povsod po svetu, v najrazličnejših regijah in kulturah (Laurant 2003, v Pestotnik, 2007).

Prihod mobilnega telefona, njegovo vsidranje v naš vsakdanjik in njegova mobilnost pa so odprli mnoga nova vprašanja in nove pomisleke, kot so vdor javnega v zasebno sfero in obratno, zbiranje podatkov o lokaciji in prometu uporabnika mobilnega telefona, ipd. (Vukelič B., 2007).

Na slike 3 so prikazani rezultati ankete glede zasebnosti v ZDA v letu 2014. Anketiranci so za občutljive osebne podatke opredelili medicinske in zavarovalniške podatke ter vsebino telefonskih pogovorov.



*Slika 3: Razumevanje javnosti glede zasebnosti in varnosti v post-Snowden dobi (vir:*http://www.pewinternet.org*)*

ZVOP-1 opredeljuje osebni podatek kot katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, pri čemer je posameznik določena ali določljiva fizična oseba, na katero se nanaša osebni podatek (ZVOP-1-UPB1; 3. člen).

Splošna opredelitev obdelave osebnih podatkov določa, da se osebni podatki lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. Namen obdelave osebnih podatkov mora biti določen v zakonu. V primeru obdelave osebnih podatkov na podlagi osebne privolitve posameznika, mora posameznik biti predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov. Le ta pa mora biti ustavno in zakonsko dopustna, obdelovati pa se smejo le tisti osebni podatki, ki so primerni in nujno potrebni za uresničitev opredeljenega namena in ne pomenijo neupravičenega posega v zasebnost in dostojanstvo posameznika (Kovačič, 2006).

Pri obdelavi osebnih podatkov je treba upoštevati načelo sorazmernosti, ki je kot temeljno načelo, opredeljeno v 3. členu ZVOP-1, in določa, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni, glede na namene, za katere se zbirajo in nadalje obdelujejo.

Pravica do zasebnosti ni trdno in univerzalno definirana, saj je dojemanje zasebnosti izrazito subjektivno. Poleg tega v pravu prevladuje pristop varstva in s tem definiranja pravice do zasebnosti prek poseganja vanjo (da torej pravo predvsem prepoveduje določene posege v zasebnost) (Orehar-Ivanc, 2002). Zato in zaradi pritiskov širjenja družbenega na območje zasebne sfere gre pri pravnem

varstvu pravice do zasebnosti večinoma le za reakcijo na pritiske, ne pa toliko za vnaprejšnje postavljanje omejitev ali varstva. Literatura sicer kot poglavitni dejavnik, ki je povzročil zahteve po prilagajanju načel varstva zasebnosti v pravu, izpostavlja tehnološke spremembe (Gellman, 2001, v Kovačič, 2006).

Zasebnost ima več dimenzij, ki pa so med seboj prepletene:

- Informacijska zasebnost (varstvo osebnih podatkov);
- Komunikacijska zasebnost;
- Prostorska zasebnost ter
- Zasebnost telesa.

Filozofija vodenja temelji na postavljanju strateških ciljev in strategij, planskih nalog ter aktivnosti sektorjev, oddelkov, posameznih zaposlenih, ki so potrebni za njihovo uresničevanje. Ciljno vodenje lahko zahteve varstva osebnih podatkov doživlja kot zavoro ter oviro za hitro in stroškovno ugodno doseganje pričakovanih rezultatov.

Oblike nadzora nad zaposlenimi

Vzroki za povečan nadzor zaposlenih so zaostrene gospodarske razmere, zahteve po večji učinkovitosti posameznika, zmanjševanja stroškov itd. Pri tem podjetja poskušajo reševati upravljavske (organizacijske, finančne, kadrovske itd.) težave s tehnološkimi rešitvami, ki olajšujejo nadzor. To pa predstavlja še dodatne izzive za ločevanje službenega in zasebnega.

Podatki, ki lahko privedejo do nepooblaščene uporabe ali zlorabe podatkov za druge namene:

- Osebnostno in psihološko testiranje, raziskovanje osebnostnih lastnosti, religioznih in drugih prepričanj;
- Nadzor nad prihodom in odhodom z delovnega mesta (evidenčne kartice, biometrija ipd.);
- Splošni video nadzor nad delom in gibanjem delavca;
- Nadzor nad telefonskimi klici in drug avdio nadzor (npr. snemanje sestankov);
- Nadzor nad uporabo interneta (angl. *cyberslacking*);
- Nadzor nad elektronsko pošto;
- Nadzor nad uporabo vhodno-izhodnih naprav (tipkovnica, tiskalnik, miška, zaslon itd.);
- Nadzor nad lokacijo oziroma gibanjem delavca znotraj službenih prostorov;
- Nadzor nad gibanjem delavca pri uporabi službenih vozil (npr. GPS);
- Nadzor nad delavčevo prehrano in morebitnimi odvisnostmi (npr. testiranje glede uživanja drog, alkohola itd.);
- Nadzor nad oblačenjem, obnašanjem in druženjem delavcev.

Koncept varstva osebnih podatkov v ZDA

V ameriški ustavi pravica do zasebnosti ni nikjer izrecno navedena (pravica do zasebnosti je sicer izrecno omenjena v ustavah vsaj osmih zveznih držav (Cate, 1997, v Kovačič, 2006). Izkazalo se je, da ameriška pravna praksa zasebnosti ne

dojema zgolj kot komunikacijsko zasebnost in pravico biti sam, temveč jo povezuje tudi z avtonomijo posameznika (Kovačič, 2006).

Priznanje obstoja pravice do zasebnosti v ameriški ustavi je sicer izzvalo številke kritike in polemike o pravnem »izumljanju«, med drugim tudi zato, ker je sodišče našlo pravico v obliki »sence« (ang. *penumbra*), torej kot pravico, ki ni izrecno definirana, temveč je zagotovljena le v konceptu; številne kritike pa so šle tudi v smeri očitkov o vsiljevanju skrajne individualistične filozofije in moralnega relativizma (Sykes, 1999, v Kovačič, 2006).

Ameriška ustava ustvarja prostor posameznikove svobode pri razvoju varstva zasebnosti, ki pa ima za posledico širjenje avtonomije posameznika. Vendar pa ravno od tu in iz pravice do zasebnosti, ki je na nekaterih področjih še vedno lastninsko koncipirana, izvira tudi poglavitna pomanjkljivost varstva zasebnosti v ZDA, ki preprečuje učinkovito varovanje informacijske zasebnosti. Ravno pri varovanju informacijske zasebnosti v zasebnem sektorju pa je nujno potrebna dejavna vloga države pri ščitenju pravic posameznika; tu so se ZDA skoraj popolnoma odpovedale regulaciji in zadeve prepustile trgu (Kovačič, 2006).

Lastninsko razumevanje zasebnosti v ZDA pomeni, da je zasebnost (tudi informacijska) last posameznika s katero lahko prosto razpolaga oz. lahko tudi proda. Škodovanje npr. posameznikovemu ugledu ni enako posegu v zasebnost, ampak je poškodba nečesa kar posameznik poseduje, kar privede do zmanjšanja vrednosti stvari. Varstvo osebnih podatkov sodi v domeno FTC (*Federal Trade Commission* – kot varstvo pravic potrošnikov) (Kovačič, 2006).

Delodajalci v ZDA večinoma nasprotujejo državni regulaciji zaščite zasebnosti na delovnem mestu in menijo, da zadostuje samoregulacija s strani podjetij. Podobno menijo podjetja tudi glede zaščite zasebnosti potrošnikov, čeprav je v 70. letih prejšnjega stoletja ameriški Kongres ustanovil *Federal Privacy Comission*, ta pa je v svoji raziskavi ugotovila, da je samoregulacija v zasebnem sektorju popolna napaka (Sykes, 1999, v Kovačič, 2006).

Podobno stanje, kot velja na področju zasebnosti na delovnem mestu, v ZDA velja tudi na področju informacijske zasebnosti (in zasebnosti nasploh) v zasebnem sektorju, v katerem je še vedno zelo razširjen lastninski koncept pravice do zasebnosti. Ravno tako kot za delodajalca velja, da lahko posega v zasebnost svojih zaposlenih bistveno bolj, kot vlada lahko posega v zasebnost svojih državljanov (Sykes, 1999, v Kovačič, 2006), velja za upravljavce osebnih podatkov, da lahko osebne podatke posameznikov zbirajo skoraj brez vsakršnih omejitev (Kovačič, 2006).

Načeloma namreč v ZDA na zvezni ravni za zasebni sektor ne veljajo skoraj nikakršne omejitve pri zbiranju in obdelavi osebnih podatkov (Kovačič, s. a.). V ameriški ustavi zasebnost ni omenjena kot pozitivna pravica (RIS, 2008).

Ko nekdo zbere osebne podatke, so ti njegova last in lahko z njimi počne praktično karkoli; to pomeni, da ni nikakršnih omejitev za njihovo nadaljnjo prodajo. Nekaj omejitev velja le za nekatere vrste osebnih podatkov, in sicer za finančne zapise, zdravstvene informacije, kreditna poročila, podatke o izposoji video kaset, kabelski TV, internetnih dejavnostih otrok, mlajših od 13 let, podatke o šolanju in

izobrazbi, podatke o lastnikih motornih vozil ter podatke, ki jih uporablja telemarketing (Laurant, 2003, v Pestotnik, 2007).

Vprašanje obdelave osebnih podatkov v zasebnem sektorju v ZDA torej ni predvsem vprašanje (informacijske) zasebnosti, temveč svobode trgovanja in svobode komercialnega govora. Namesto poseganja v pravice se postavlja zgolj vprašanje trgovanja med posameznikom in organizacijo, ki zbira osebne podatke. Posameznik ima načeloma sicer možnost, da svojih podatkov ne proda, toda v praksi te možnosti največkrat dejansko nima, če se ne želi izključiti iz družbe. Sistemska ne regulacija tega področja v zasebnem sektorju s strani ZDA tako posameznike glede informacijske zasebnosti sili v položaj, ko se svoji informacijski zasebnosti odrekajo na videz prostovoljno (Kovačič, 2006).

V ZDA je prostorska, komunikacijska in informacijska zasebnost zunaj doma slabo varovana. Iz ameriške sodne prakse izhaja, da lahko kot pogoj za zaposlitev delodajalci zahtevajo soglasje za nadzor v kakršnemkoli obsegu in v tem primeru je nadzor zaposlenega povsem zakonit. Delodajalci v ZDA redno posegajo v zasebnost svojih zaposlenih, to pravico pa jim domnevno daje lastništvo nad delovno opremo (Kovačič, 2006).

Koncept varstva osebnih podatkov v Evropi

V Evropi je večina držav podpisala in ratificirala mednarodne akte, ki urejajo varstvo zasebnosti. Najpomembnejši med njimi so Splošna deklaracija človekovih pravic, Mednarodni pakt o državljanskih in političnih pravicah ter Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (v nadaljevanju: EKČP) (Kovačič, 2006).

Splošna deklaracija človekovih pravic v 12. členu določa, da »nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takim vmešavanjem ali takimi napadi.«

EKČP v 8. členu opredeljuje, da ima »vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi«.

Evropske države, članice Sveta Evrope, razen San Marina, so sprejele Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov. To pomeni, da imajo večinoma tudi poseben zakon o varstvu osebnih podatkov in vzpostavljen nadzorni organ, ki bdi nad varstvom informacijske zasebnosti (Kovačič, 2006).

Zasebnost (tudi informacijska) je človekova pravica, ki je v Sloveniji urejena v Ustavi RS v 35. in 38. členu. Človekova pravica je zavarovana tako na upravnem kot tudi na sodnem področju. Poseg vanjo je lahko prekršek, kaznivo dejanje ali predmet varstva v civilnem sodnem postopku.

Varstvo informacijske zasebnosti v Evropi

V Evropi je prvi zakon za zaščito informacijske zasebnosti na svetu, ki je bil sprejet leta 1970 v Nemčiji (v zvezni državi Hesse), postavil enotna merila za javni in zasebni sektor. Razlogi za sprejem take zakonodaje so bile obsežne družbene reforme, do katerih je v Evropi prišlo po drugi svetovni vojni (Kovačič, 2006).

Z razvojem mikroprocesorskih tehnologij uporaba velikih računalniških sistemov ni bila več ekonomsko upravičena. Nastanek množice majhnih, poceni, a zmogljivih računalnikov je razpravo o zaščiti informacijske zasebnosti obrnil v povsem drugo smer, saj je bilo novo, razpršeno tehnologijo veliko teže nadzirati kot omejeno število kompleksnih in dragih sistemov (katerih upravljanje je povrh vsega za razliko od nove generacije računalnikov zahtevalo večje število visoko specializiranih ljudi). Zaradi nove tehnologije so se v Evropi odločili, da je treba zaščitno zakonodajo razširiti tudi na zasebni sektor, z majhnimi podjetji vred (Mayer-Schönberger, 2001, v Kovačič, 2006).

Postopoma je postajalo jasno, da niso podatki tisti, ki potrebujejo zaščito, temveč da zaščito potrebuje posameznik. Zato so uvedli nekatere nove pravice: zbiranje podatkov je bilo mogoče le na podlagi zakona ali soglasja posameznika (na Norveškem so npr. v zakon izrecno zapisali, da ima posameznik pravico zavrniti oddajo osebnih podatkov, ki bodo uporabljeni v namene neposrednega trženja ali tržnih raziskav), posamezniki so morali biti obveščeni o namenu zbiranja, imeli so pravico zahtevati spremembo ali celo izbris netočnih podatkov (Mayer-Schönberger, 2001, v Kovačič, 2006).

Komunikacijska zasebnost v Evropi

8. člen EKČP vsakomur priznava tajnost pisem in drugih občil, ki se razlagajo zelo široko, torej kot telefonske komunikacije, elektronska pošta, kratka sporočila SMS itd., saj oblika in vsebina sporazumevanja ni pomembna. Kljub temu imajo v nekaterih državah še težave s prilagajanjem zakonodaje razvoju tehnologije.

Seveda pa pravica do komunikacijske zasebnosti ni absolutna, saj je Evropsko sodišče za človekove pravice v primeru Klaas in drugih proti Nemčiji leta 1978 zapisalo, da je tajni nadzor telekomunikacij nujno potreben element zagotavljanja nacionalne varnosti (Klemenčič, 2002, v Kovačič, 2006).

Zakon o elektronskih komunikacijah (v nadaljevanju: ZeKOM) in Zakon o varstvu potrošnikov (ZVPot-A), določa, da komunikacij in z njimi povezanih prometnih podatkov ni dovoljeno shranjevati brez soglasja uporabnika, razen za potrebe prenosa ali upravljanja prometa ter zaračunavanja storitev. Izjema je shranjevanje komunikacij za potrebe dokazovanja komercialnih transakcij, pri čemer pa morajo biti uporabniki predhodno obveščeni o shranjevanju, namenu shranjevanja in trajanju hranjenja. 5. točka 6. člena pa pravi, da smejo prometne podatke obdelovati samo tisti, ki delujejo pod oblastjo ponudnikov storitev; to je posebej pomembno pri oddaji del zunanjim izvajalcem (Kovačič, 2006).

Direktiva o zasebnosti in elektronskih komunikacijah 2002/58/EC opredeljuje evropski pristop pri varovanju informacijske zasebnosti. V 30. točki izpostavlja

načelo čim manjšega obsega zbiranja osebnih podatkov, pri čemer je v direktivi zapisano, da morajo biti sistemi za zagotavljanje storitev zasnovani tako, da zbiranje osebnih podatkov zmanjšajo na minimum; z drugimi besedami, sistemi morajo biti zasnovani za ščitenje zasebnosti (Kovačič, 2006).

Zasebnost na delovnem mestu

Glede pravice do zasebnosti na delovnem mestu v evropski pravni ureditvi sicer vlada še nekaj nejasnosti (predvsem manjka določitev najnižje zahtevane stopnje varstva zasebnosti, podobno kot pri informacijski zasebnosti). Vsekakor pa je zasebnost na delovnem mestu v razvitih evropskih državah precej bolje zaščitena kot v ZDA, saj načeloma velja obveznost delodajalca, da zaposlene vsaj obvesti o možnosti nadzora na delovnem mestu, poleg tega je v primeru nadzora komunikacij dovoljen samo tisti nadzor, ki se nanaša na delo (Kovačič, 2006).

Poleg tega bi nadzor s strani delodajalca lahko kršil tudi interes tretjih oseb, ki komunicirajo z zaposlenim in morda niti ne vedo, da gre za službeno komunikacijsko sredstvo in da delodajalec nadzoruje komunikacije zaposlenega, s katerim so v stiku (Klemenčič, 2001). Ta problem je zelo očiten pri morebitnem nadzorovanju službenih mobilnih telefonov, kjer je možnosti za razlikovanje med službenim in zasebnim komunikacijskim sredstvom še manj. Tudi tu se je slovenska sodna praksa postavila na stran posameznika, saj je Upravno sodišče RS sprejelo odločitev U 702/99, s katero je zaposlenemu priznalo pravico do varstva zasebnosti pri uporabi službenih mobilnih telefonov (Klemenčič, 2003, v Kovačič, 2006).

»Delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema prek službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen EKČP. To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene. Podjetje ali druge ustanove ne smejo biti mesta, na katerih bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, v katerih temeljne človekove pravice nimajo veljave. Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.« (Klemenčič, 2002, v Kovačič, 2006)

Osebna privolitev delavca je dopustna le izjemoma in le v tistih primerih obdelave osebnih podatkov, ki niso vezani na uresničevanje pravic in obveznosti iz delovnega razmerja oz. niso v zvezi z delovnim razmerjem posameznika (npr. posredovanje podatkov za novoletno obdarovanje otrok delavcev) in kadar delavec v primeru, da osebnih podatkov ne posreduje, ne more utrpeti kakršnihkoli delovnopravnih sankcij (IP-RS, 2008).

2.5. OMEJITVE RAZISKAVE

Glavne predpostavke so:

- Industrija pametnih mobilnih telefonov in tabličnih računalnikov je zadnje čase ena najbolj rastočih industrij na svetu;
- Mobilnost je začetek trenda prehoda k sistemom vključenosti, ki podjetjem omogočajo, da uporabnike vključijo ter ponudijo vsebinsko bogate

aplikacije in pametne rešitve, ki jim pomagajo pri takojšnjih poslovnih odločitvah;
- Slabo ali nesprejemljivo vedenje končnih uporabnikov glede varnosti, je velik problem za organizacijo ter povzročitelj velikega števila informacijskih incidentov;
- Pristop uvedbe strategije upravljanja pametnih mobilnih naprav temelji na približevanju produktivnosti zaposlenih in hkrati ustrezni zaščiti na način, ki upravlja naprave, programske rešitve in podatke na pametnih mobilnih napravah;
- Podjetja poskušajo zaradi zelo velike izpostavljenosti varnostnim grožnjam uporabljati zelo napredne funkcije upravljanja mobilnih naprav. Pri tem se pojavijo navzkrižje interesov podjetja in posameznika.

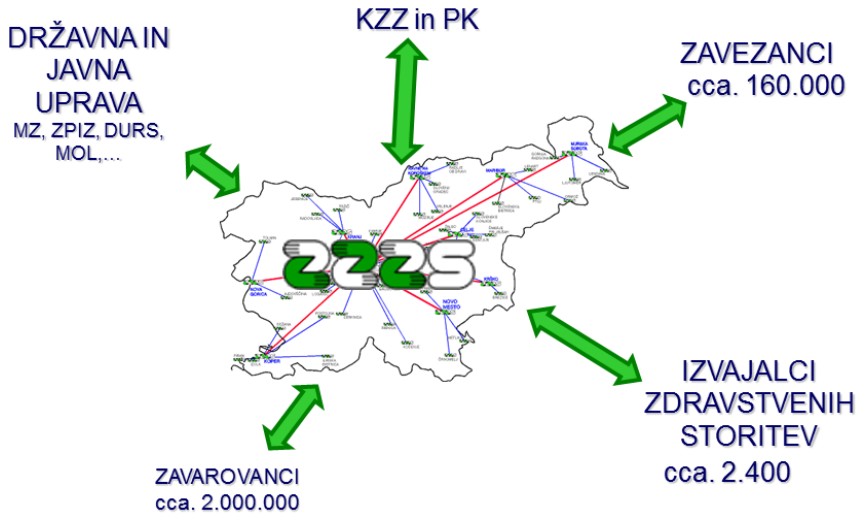
Omejitve so:
- Zaradi zahtev tržišča se hitro spreminjajo funkcionalnosti okolja MobileIron na področju upravljanja. Pri tem se spreminjajo delovanje vgrajenih funkcij upravljanja, grafičnega vmesnika in pomanjkanje ustreznega znanja z upravljanjem nastavitev v MobileIron okolju;
- Proizvajalci mobilnih naprav sprotno posodabljajo varnostne nastavitve na napravah, zato se priprava modelov upravljanja hitro spreminja;
- Modela upravljanja bo pripravljen na osnovi dveh modelov mobilnih naprav: pametni mobilni telefon in tablični računalnik enega;
- Pomanjkanje poglobljenega znanja o delovanju operacijskega sistema Android na mobilnih napravah.

3. ANALIZA STANJA

3.1. PREDSTAVITEV INFORMACIJSKEGA SISTEMA ZZZS

V letu 2013 je Zavod realiziral številne dopolnitve obstoječih računalniških rešitev in razvoja novih. S številnimi aplikacijami informacijski sistem Zavoda ne služi samo podpori notranjim procesom Zavoda, temveč zagotavlja informacijsko podporo tudi drugim deležnikom v zdravstvenem sistemu (izvajalcem zdravstvenih storitev, zavarovanim osebam, zavezancem za prijavo v zavarovanje) in zunaj njega (Zavod za pokojninsko in invalidsko zavarovanje, Finančna uprava Republike Slovenije, ministrstva, sodišča itd.).

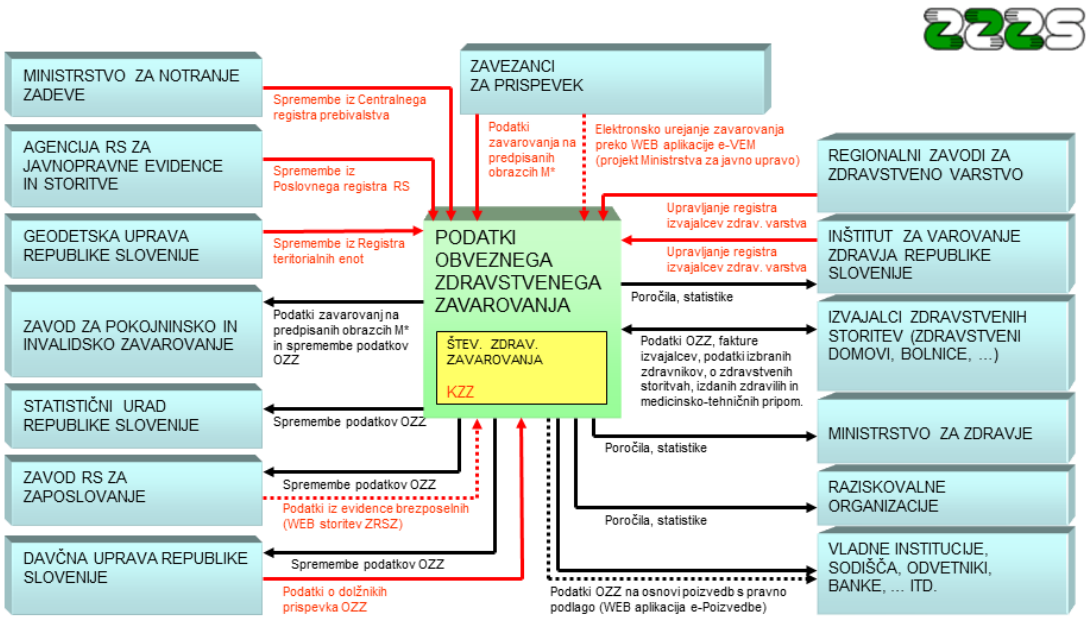
Zavod izvaja politiko aktivnega vključevanja v različne nacionalne projekte (slika 4), s katerimi širi ponudbo e-storitev v zdravstvenem sistemu, kot tudi za ostale uporabnike baz podatkov, s katerimi upravlja Zavod. Za potrebe računalniško podprtega poslovanja in komuniciranja z zunanjimi subjekti in zavarovanci, je Zavod z uvedbo spletnih storitev vzpostavil varno informacijsko infrastrukturo, ki omogoča tehnološke nadgradnje oziroma nove generacije informacijskih storitev.



Slika 4: Povezave informacijskega sistema Zavoda (vir: ZZZS)

V skladu z zakonskimi podlagami in medsebojnimi pogodbami Zavod elektronsko posluje z nekaterimi javnimi zavodi in institucijami (slika 5). Zavod v elektronski obliki zagotavlja podatke iz prijav v obvezno zdravstveno, pokojninsko in invalidsko zavarovanje Zavodu za pokojninsko in invalidsko zavarovanje, Zavodu za zaposlovanje, Statističnemu uradu in drugim zakonsko določenim upravičencem do podatkov na osnovi poizvedb. S strani Ministrstva za notranje zadeve in Statističnega urada RS pridobiva Zavod podatke iz nacionalnih registrov, iz Finančna uprava Republike Slovenije pa pridobiva podatke o izterjavi prispevkov

obveznega zdravstvenega zavarovanja. Zelo dejavno je elektronsko posredovanje podatkov tudi z Ministrstvom za zdravje in Inštitutom za varovanje zdravja na različnih področjih. Vse komponente IS Zavoda se stalno nadgrajujejo in s stalnim spremljanjem novih tehnoloških in organizacijskih možnosti, informacijski center zagotavlja tudi v prihodnje varno in sodobno elektronsko poslovanje (M. Nussdorfer; 2009).



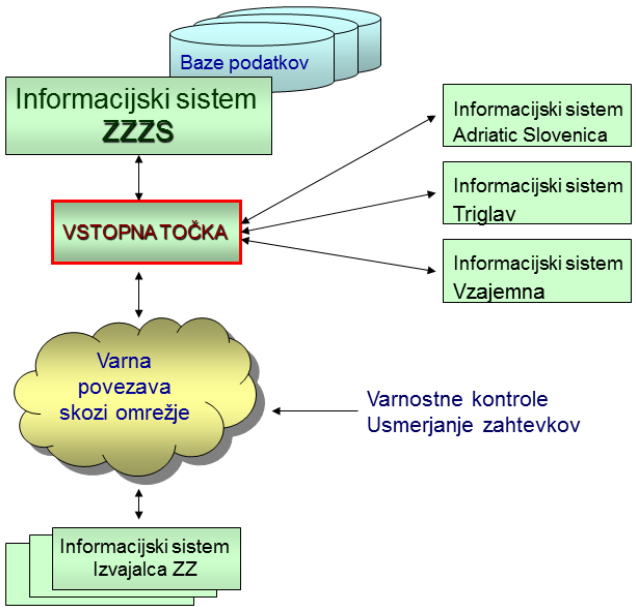
Slika 5: Povezovanje informacijskega sistema Zavoda z zunanjimi subjekti (Vir: ZZZS)

Evropske strateške usmeritve na področju e-Zdravja priporočajo pospešeno izgradnjo varne zdravstvene informacijske mreže, razširitve uporabe kartic v zdravstvu ter postopno vzpostavitev on-line dostopov do podatkov (M. Nussdorfer; 2009).

Zavod je vzpostavil on-line sistem, ki omogoča takojšnje, neposredno in varno izmenjevanje podatkov. Dostop do podatkov zdravstvenega zavarovanja (slika 6) je namenjen zdravstvenim delavcem, ki navedene podatke potrebujejo v postopkih nudenja zdravstvenih storitev. Administrativne funkcije (preverjanje zavarovanj in pravic iz teh zavarovanj) so na voljo medicinskim sestram in administrativnemu osebju, funkcije z medicinskimi podatki pa uporabljajo zdravniki in farmacevti. Za vse dostope do podatkov je točno opredeljena shema pooblastil (Nussdorfer; 2009).

Sistem on-line zdravstvenega zavarovanja je zasnovan na osnovi naslednjih ključnih komponent:

- Programske knjižnice, ki jih uporabljajo izvajalci zdravstvenih storitev v svojih programskih rešitvah za komuniciranje z on-line sistemom;
- Vstopna točka kot centralni varnostno-komunikacijski strežni servis in
- Zaledni sistemi upravljavcev zbirk podatkov, od koder izvajalci zdravstvenih storitev podatke pridobijo ali jih tja sproti pošiljajo.



Slika 6: On-line zdravstvenega zavarovanja (vir: ZZZS)

Zaposleni na Zavodu iz organizacijskega vidika opravljajo eno ali več organizacijskih vlog, ki v skladu s svojimi pooblastili sodelujejo v več poslovnih procesih. Pri tem so imeli potrebo po uporabi mobilne tehnologije, ki bi jim omogočala vez s svojim delovnim okoljem in njegovim IS. Kontekst potreb so izražale uporabnikove potrebe, ki so bodisi njegove potrebe ali pa potrebe organizacije.

Najpomembnejši dejavnik pri odločitvi sprejema mobilnih sistemov, je uporabnikovo dojemanje vrednosti mobilnosti. Koristi mobilnih sistemov je treba oceniti glede na vsebinsko potrebo uporabnikov, ki zagotavljajo zmanjševanje odvisnosti od časa in potreb za zagotavljanje storitev v vsakem trenutku in kraju.

Potrebe IS po eni strani določajo potrebe uporabnika, po drugi strani pa uporabnik svoje potrebe v stanju mobilnosti izrazi tako, da zažene mobilno programsko rešitev.

IS mora zagotavljati možnost, da mobilnega uporabnika preko mobilne aplikacije vključi v poslovne procese.

V kontekstu mobilnih aplikacij

Uporabljajo se rešitve, ki omogočajo zaposlenim dostop do IS organizacije ter hitro in nemoteno izmenjavo informacij.

V ta namen uporabljajo zaposleni na svojih pametnih napravah poštni odjemalec proizvajalca elektronske pošte, ki se uporablja kot interna pošta organizacije.

Za organizacijo svojega časa, sklicevanje sestankov ali opomnikov uporabljajo koledar, ki je integriran v internem poštnem sistemu.

Pomemben del aplikativne podpore na mobilnih napravah so stiki. Zaposleni lahko na mobilni napravi uporabljajo svoje privatne stike, imenik zaposlenih ter stike zunanjih partnerjev in drugih javnosti.

Zasebni stiki so del poštnega predala zaposlenega in ga lahko ureja na delovni postaji ali mobilni napravi. V primeru izgube ali okvare mobilne naprave se le ti prenesejo na novo vzpostavljeno mobilno napravo.

Imenik zaposlenih vsebuje podrobne službene informacije, ki so ključnega pomena za hitro vzpostavitev komunikacije z zaposlenim. Podatki so pridobljeni v uradnih internih evidencah zaposlenih in so javnega značaja. Podrobni službeni podatki vključujejo interni elektronski naslov, službeno stacionarno telefonsko številko, naziv delovnega mesta, naziv in naslov organizacijske enote ter lokacijo pisarne zaposlenega.

Poleg podrobnih službenih kontaktnih podatkov, pa so lahko vključeni tudi nekateri osebni podatki, ki vključujejo domači naslov in domačo telefonsko številko zaposlenega. Vpisovanje osebnih podatkov je omogočeno in prepuščeno zgolj zaposlenemu.

Zavod za potrebe komuniciranja z nekaterimi svojimi zunanjimi partnerji uporablja tudi centralni imenik, v katerem so shranjeni podatki o osebi, nazivu, podjetju, elektronskem naslovu ter telefonski številki.

Dostop do internih dokumentov in izmenjava dokumentov med zaposlenimi

Zaposleni se pogosto udeležujejo sestankov in različnih drugih dogodkov zunaj naše organizacije. Za udeležbo potrebujejo različne oblike gradiv, ki so v elektronski obliki varno shranjeni na centralnem IS Zavoda.

V kontekstu organizacijskih potreb

Razširjenost uporabe mobilnih naprav na Zavodu je predvsem med vodstvenim kadrom: generalni direktor, direktorji sektorjev in področji, svetovalci, višji strokovni sodelavci. Ti profili uporabljajo mobilne rešitve znotraj in zunaj Zavoda na sestankih, drugi dogodki itd.

Za potrebe izvajanja vzdrževanja in skrbništva ključni informacijskih rešitev so potrebe po uporabi mobilnih rešitev tudi skrbniške in dežurne ekipe Informacijskega centra Zavoda.

V kontekstu tipov mobilnih naprav

Na Zavodu smo se odločili za uporabo dveh tipov mobilnih naprav: pametne mobilne telefone in tablične računalnike. Izbor mobilnih naprav je bil na osnovi spodnjih kriterijev:

- Velikosti zaslonov;

- Procesorske zmogljivosti,
- Spominske sposobnosti;
- Povezljivosti v internet:
    - Povezujejo se preko brezžične povezave in pri tem uporablja enega od standardnih protokolov: Wifi, Bluetooth in mobilno omrežje;
    - Povezovanje preko USB.

Podpora in izbira izvajalnega okolja na pametnih mobilnih napravah je temeljila na osnovi podprtosti mobilnih rešitev za dostop do potisne pošte, podpori okolja s stališča varnostnih rešitev in tehnične podpore, razširjenosti in ponudbe mobilnih rešitev ter cenovna dostopnost. Glede na tržne deleže izvajalskih okolji smo se odločili, da primarno podpremo izvajalno okolje Android, ostale okolja, kot so iOS, Windows Phone in BlackBerry pa po najboljših močeh.

3.2. VAROVANJE ZASEBNOSTI V ZZZS

Zakon o delovnih razmerjih varuje delavca kot šibkejšo stranko v delovnem razmerju z delodajalcem, zato tudi omejuje delodajalca, da zbira zgolj tiste podatke, ki jih nujno potrebuje. Nadzor je torej popolnoma legalna in legitimna pravica delodajalca vendar z vnaprej pripravljenimi in objavljenimi pravili.

Pravica delavca do zasebnosti na delovnem mestu je na Zavodu zagotovljena z internimi akti in pravilniki, ki določajo, da je za vsako obliko nadzora ali spremljanja njegovih aktivnosti, zaposleni vnaprej opozorjen ter mu je razloženo, za kateri namen in v katerih primerih se ukrep lahko uporablja.

Varnostna politika Zavoda opredeljuje zasebnost zaposlenega kot temeljno človekovo pravico in ustavno normo, ki se jo spoštuje ter upošteva pri pripravi informacijskih rešitev.

3.2.1. VIDEO NADZOR

Za namene varovanja ljudi, premoženja ter reda v prostorih Zavoda se v nekaterih prostorih centralne lokacije izvaja video nadzor vstopa ali izstopa.

V prostorih, kjer se izvaja video nadzor, so vidno in razločno objavljena obvestila, ki omogočajo posamezniku seznanitev izvajanja video nadzora. Video nadzorni sistem je zavarovan pred dostopom nepooblaščenih oseb. Posnetki se shranjujejo omejeni čas sedmih dni.

3.2.2. SNEMANJE TELEFONSKIH POGOVOROV

Zavod ne poseduje tehničnih možnosti za izvajanje snemanja telefonskim pogovorom.

3.2.3. PREVERJANJE TELEFONSKIH POGOVOROV NA STACIONARNIH IN MOBILNIH NAPRAVAH

Z vzpostavitvijo IP telefonije so se možnosti upravljanja okolja bistveno povečale. Okolje omogoča spremljanje telefonskih klicev posamezne telefonske številke, ki

pripada zaposlenemu. Vpogled je strogo nadzorovan ter omejen zgolj na skrbnika sistema za potrebe odprave napak in nadzora napak.

Na mobilnih napravah je prav tako onemogočeno zbiranje statističnih podatkov o poslanih in prejetih SMS sporočilih.

3.2.4. ELEKTRONSKA POŠTA

Elektronska pošta je ena bistvenih komunikacijskih kanalov za medsebojno izmenjavo informacij ter poslovanja z zunanjimi partnerji. Glede na varnostne grožnje in morebitne zlorabe, ki obstajajo pri izmenjavi elektronske pošte, je bilo treba uvesti varnostne mehanizme za preprečevanje le teh. Pravila uporabe elektronske pošte se izvajajo z omejevanjem na sistemu z različnimi pravili: velikost elektronske pošte, sprejem elektronske pošte, ki ne vsebuje morebitne škodljive kode ali nenaročene in nezaželene vsebine (*spam*).

Z uvedbo varnostnih mehanizmov, pa se z obravnavo elektronskega sporočila, pojavljajo sledi v sistemskih dnevnikih in na uporabniških vmesnikih skrbniških modulov. Nivo sledenja elektronskim sporočilom je omejeno le na spremljanje pošiljatelja, datum in zadeva sporočila.

Z obravnavo elektronskega sporočila se na IS elektronsko zapisujejo sledi v sistemskih dnevnikih in kot povzetki na uporabniških vmesnikih skrbniških modulov. Nivo sledenja elektronskim sporočilom je omejeno le na spremljanje pošiljatelja, datum in zadeva elektronskega sporočila.

Varnostna politika opredeljuje tudi sistemsko upravljanje poštnih predalov zaposlenih. Vpogled v poštne predale zaposlenih je zagotovljen le zaposlenemu. Obstaja pa tudi možnost sistemskega vpogleda v poštni predal zaposlenega vendar le s osebno ali pisno privolitvijo zaposlenega. Po zaključku delovnega razmerja zaposlenega, se v postopku odvzema pooblastil na IS izvede tudi celovito brisanje poštnega predala.

3.2.5. SPREMLJANJE NAMEŠČENE PROGRAMSKE OPREME NA MOBILNIH NAPRAVAH

Spremljanje seznama nameščene programske opreme pokaže pri uporabnikih različne potrebe. Pridobljeni podatki so lahko v določeni meri tudi zasebni, saj izkazujejo osebnostne značilnosti uporabnika mobilne naprave. Le ti podatki se lahko v določenih primerih uporabijo proti uporabniku oz. zaposlenemu.
Nameščena programska oprema MobileIron za upravljanje pametnih mobilnih naprav ima vgrajeno funkcionalnost, ki omogoča pridobivanje podatkov o nameščeni programski opremi vključno z verzijo. Podatki o posamezni programski opremi vsebuje naziv programa ter verzijo.

Upravljanje mobilne programske opreme na napravi se izvaja z omejevanjem nameščanja dostopne programske opreme na internetu. Dovoljeno je nameščanje programske opreme le iz javno dostopnega portala proizvajalca Google. Pri vključitvi uporabnika v centralni sistem upravljanja mobilne tehnologije, se na njegovo mobilno napravo namesti pred pripravljeno standardno programsko

opremo. Z vzpostavitvijo internega portala za mobilne programske rešitve, si zaposleni tudi lahko namesti dodatno preverjeno programsko opremo, ki ni v standardnem naboru nameščene opreme.

3.2.6. SPREMLJANJE LOKACIJE MOBILNE NAPRAVE

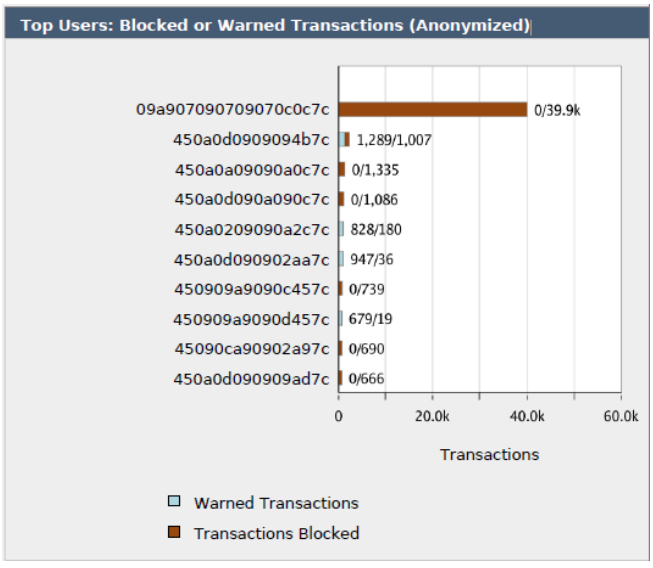
Delovni proces v organizaciji ni vezan na trenutno lokacijo zaposlenega, na osnovi katere bi se učinkoviteje organiziral delovni proces. Spremljanje lokacije mobilne naprave je privzeto izključeno.

Vklop funkcije trenutne lokacije mobilne naprave je predviden le v izjemnem primeru, če je mobilna naprava zaposlenemu odtujena. V tem primeru zaposleni posreduje informacijo o odtujitvi mobilne naprave skrbniku sistema za upravljanje mobilnih naprav, kateri na osnovi odobritve svetovalca za varnost, lahko začne postopke pridobitve informacije trenutne lokacije mobilne naprave.

3.2.7. SPREMLJANJE OBISKANOSTI SPLETNIH STRANI

Za uveljavljenje varnostne politike dostopa do interneta, se uporablja namenska programska oprema IronPort. Politika dostopa do internih strani temelji na pravilih omejevanja. Zagotavlja uveljavljanje dostopa z omejitvami dostopa do neprimernih in škodljivih spletnih vsebin ter pregledovanje vsebine na morebitno vsebovano škodljivo programsko kodo.

Pri izvajanju varnostne politike dostopa do interneta se beležijo tudi podatki o zaposlenem. Zbrani in obdelani podatki izkazujejo osebnostne značilnosti zaposlenega, zato so le ti v končnih poročilih (slika 7) za izvajanje nadzora in poročil za vodstvo anonimizirani.



Slika 7: Anonimizirano poročilo o dostopu na Internet (Vir: ZZZS)

3.2.8. SHRANJEVANJE PODATKOV MOBILNIH NAPRAV NA CENTRALNI STREŽNIK

Zaposleni na svojih mobilnih napravah lahko shranjujejo različne oblike podatkov oz. datotek:

- Dokumentne datoteke;
- Digitalne slike;
- Video datoteke;
- Glasbene datoteke.

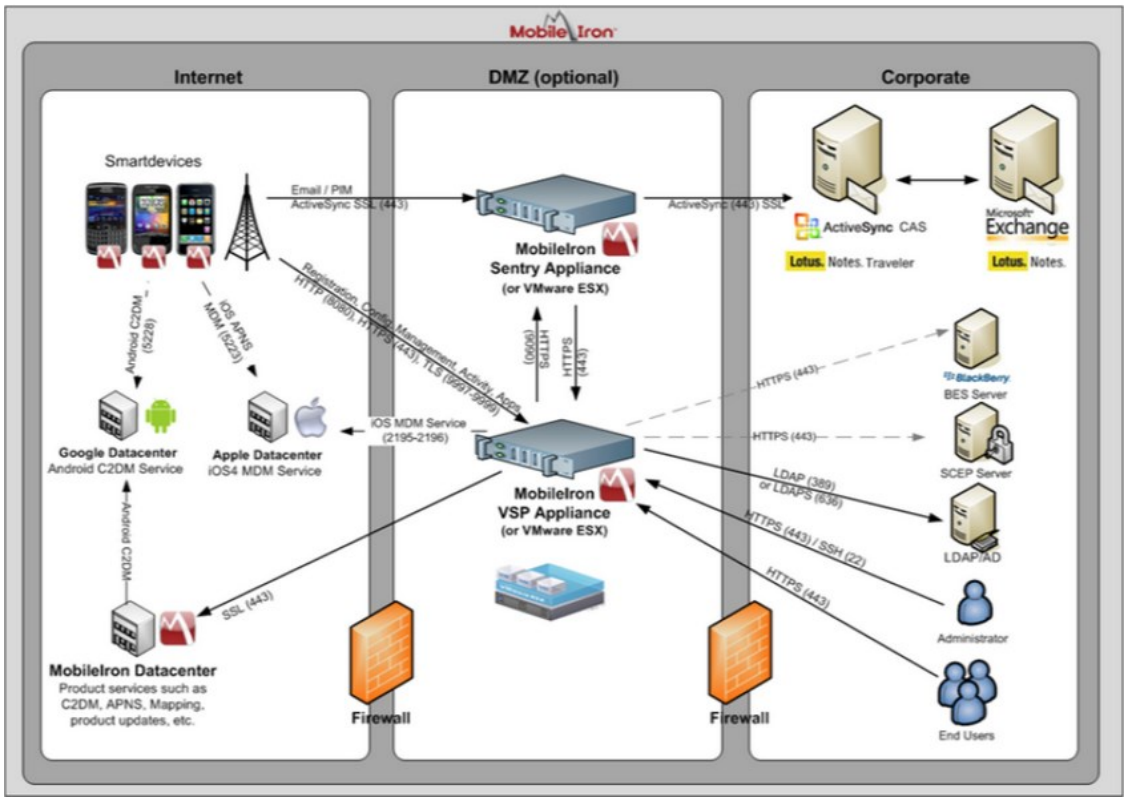
Zaradi občutljivosti vsebin v zgoraj naštetih datotekah, se le te varnostno ne shranjujejo na centralnem strežniku MobileIron. Za izvajanje varnostnih kopij datotek na mobilnih napravah uporabniki poskrbijo sami.

4. PREDSTAVITEV REŠITVE MOBILEIRON

Pri testiranju programske rešitve MobileIron za upravljanje mobilnih naprav, bomo preverili zanesljivost trditve proizvajalca, da rešitev deluje v skladu s specifikacijami proizvajalca za področje sledenja podatkov mobilne naprave zaposlenega, ki je opredeljeno z zakonom o zasebnosti.

Arhitektura postavitve MobileIron Sentry v podjetju, ki je prikazana na sliki 8, je odvisna od varnostnih ciljev podjetja, topologije omrežja in zaledne infrastrukture elektronske poštne.

MobileIron Sentry samostojno deluje, kot posrednik med aplikacijo na mobilni napravi ter zalednim sistemom infrastrukture elektronske poštne, pri čemer se uporablja protokol ActiveSync. Ta podpira različne poštne sisteme: Microsoft Exchange, Lotus Notes z uporabo IBM Notes Traveler ali pa gostujoče internetne servise (Google Gmail ali Microsoft Office 365).



Slika 8: Arhitektura MobileIron okolja (Vir: ZZZS)

4.1. NAMESTITEV

Virtual Smartphone (VSP)

MobileIron je strežnik v vlogi centralne sistemske komponente za integracijo med mobilnimi napravami in zalednim IS organizacije ter upravljanje varnosti, aplikacij in podatkov na mobilnih napravah.

MobileIron Sentry

MobileIron Sentry zagotavlja izvajanje varnostne politike za dostop mobilnih naprav do zalednih IS na ravni omrežja. Za dostop zaposlenega do mobilne storitve elektronske pošte, se mora mobilna naprava s pomočjo ActiveSync protokola povezati s strežnikom MobileIron Sentry, ki je v vlogi centralne sistemske komponente za integracijo z zalednim IS. Preverjanje pooblastil, ki jih ima mobilna naprava v omrežju podjetja, se preverja v centralnem nadzornem-upravljavskem sistemu MobileIron VSP.

Na osnovi posredovanih podatkov iz mobilne naprave in opredeljenih varnostnih politik se sistem VPS odloča ali je mobilna naprava v skladu z varnostnimi politikami ter je vredna zaupanja za komunikacijo z zalednim IS organizacije. Posredovani podatki vključujejo vrsto odjemalca, stanje varnosti, različico operacijskega sistema in druge potrebne podatke. Če mobilna naprava ne izpolnjuje vseh vnaprej določenih kriterijev, se le tej ne omogoči nadaljnja komunikacija z zalednim IS.

MobileIron na mobilnih napravah zagotovi:

- Samo pooblaščenim mobilnim napravam, da se lahko povežejo na ActiveSync strežnik;
- Izvajanje ukazov upravljanja na mobilnih napravah, kot je oddaljeno brisanje podatkov, v primeru odtujitve;
- Dostop do službene elektronske pošte, koledarja in stikov v podjetju brez posredovanja lastnika mobilne naprave;
- Samodejni dostop do Wifi in VPN omrežij podjetja;
- Namestitev in nastavitev mobilne programske opreme, ki je povezana z delom zaposlenega;
- Omogoča preverjanje skladnosti mobilnih naprav z varnostnimi politikami podjetja;
- Iskanje izgubljenih ali odtujenih mobilnih naprav.

V zameno za dostop do zalednega IS organizacije, se zaposleni strinjajo, da organizacija upravlja z njihovo mobilno napravo.

Upravljanje mobilne naprave vključuje sledeče nadzorne funkcije:

- Brisanje vsebine na mobilni napravi. Brisanje se lahko izvaja na vsebini v lasti podjetja, v primeru, da je mobilna naprava odtujena, se lahko izbriše tudi vsebina, ki je last uporabnika;
- Iskanje mobilne naprave. Če je bila mobilna naprava izgubljena ali odtujena, lahko skrbnik sistema za upravljanje mobilnih naprav MobileIron, preko spletnega grafičnega vmesnika locira napravo. Lokacija naprave se

določi s pomočjo vgrajenega GPS modula v mobilni napravi ali preko mobilnega signala operaterja;
- Upravljanje mobilne programske opreme. Politika upravljanja opredeljuje seznam mobilne programske opreme, ki se lahko uporablja za dostop do zalednega IS organizacije. Za zmanjšanje varnostnega tveganja, se pripravi seznam tveganih programskih rešitev, ki se jim omeji delovanje ali avtomatično od namesti iz mobilne naprave;
- Določitev minimalnih varnostnih standardov za uporabo mobilne naprave:
    - Šifriranje vsebine mobilne naprave. Vsebina, ki je last organizacije se privzeto šifrira, lahko pa se izvede tudi šifriranje celotne vsebine na mobilni napravi;
    - Zahteve za minimalno različico sistemske in mobilne programske opreme;
    - Vstopno geslo za vstop v mobilno napravo in dostop do zalednega IS organizacije;
    - Uporaba mobilne naprave s skrbniškimi pooblastili, ki omogoča spreminjanje funkcionalnosti in nivo varnostnih nastavitev sistemske programske opreme (*rooting* na Android ali *jailbreaking* na iOS).

Web@Work

Web@Work programska rešitev ponuja vse funkcionalnosti brskalnika, vendar z dodano AppConnect in AppTunnel funkcionalnostjo. Primerna je predvsem za dostop do spletnih poslovnih aplikacij, ki niso na voljo iz javnega interneta. Tako lahko promet do notranjih aplikacijskih strežnikov tuneliramo z uporabo AppTunnel preko Sentry strežnika. Tunelira se lahko ves ali samo vnaprej opredeljen omrežni promet med mobilno programsko rešitvijo in strežnikom v zalednem IS organizacije. Programska rešitev za shranjevanje podatkov uporablja AppConnect zabojnik, ki zagotavlja, da so preneseni podatki varni pred ostalimi aplikacijami.

AppConnect in AppTunnel

Delovanje programskih rešitev znotraj MobileIron okolja ponujajo dodatne funkcionalnosti upravljanja in varnosti preko AppConnect in AppTunnel funkcionalnosti. Funkcionalnost AppConnect, programsko rešitev na mobilni napravi ovije v varni zabojnik. Le ta zagotavlja ločevanje programske rešitve in njenih podatkov od ostalih programskih rešitev. S tem zagotovimo, da podatki ne prehajajo iz varnega okolja v manj varno okolje in obratno. Za dodani nivo varnosti pri prenosu podatkov med programsko rešitvijo na mobilni napravi in aplikacijskim strežnikom v zalednem IS organizacije, se uporabi funkcionalnost AppTunnel. S tem programska rešitev nikoli neposredno ne dostopa do aplikacijskih strežnikov, ampak le do Sentry strežnika, ki izvede preverjanje identitete uporabnika ter na osnovi tega uporabniku dodeli zadostne pravice za dostop do notranjih virov zalednega IS. MobileIron zagotavlja neposredno upravljanje nastavitev mobilnih programskih rešitev preko AppTunnel funkcionalnosti.

Integracija z imeniškim sistemom LDAP

Integracija z obstoječim imenskim strežnikom poslovnih uporabnikov poenostavi prijavo uporabnikov ter upravljanje le teh iz centralnega mesta.

4.2. POLITIKA UPRAVLJANJA MOBILNIH NAPRAV

Pri namestitvi rešitev za upravljanje z mobilnimi napravami, moramo veliko pozornost posvetiti nastavitvam, ki lahko posegajo v zasebnost zaposlenega.

Glede na opredelitve potreb za mobilne naprave, ki bodo zagotavljale skupno vizijo ter podpirale poslanstvo organizacije, se oblikuje strategija za uvajanje mobilnih rešitev, pripravi se varnostna politika za uporabo mobilnih naprav in opredelijo se poslovne in funkcijske zahteve mobilnih rešitev.

Rešitev MobileIron ponuja veliko možnosti nastavitev zaščite za podjetje in zaposlenega, vendar do te mere, da se ne razkrijejo osebni podatki zaposlenega. Iz tega razloga na MobileIron ni možno nastaviti sledeče funkcionalnosti:

- Pregledovanje fotografij, ki so shranjene na mobilni napravi;
- Spremljanje elektronskih sporočil;
- Omejiti dostop do določenih dostopnih brezžičnih točk, spletnih strani ali lokacij;
- Slediti uporabi interneta;
- Snemanje telefonskih klicev.

4.2.1. UPRAVLJANJE POLITIKE ZASEBNOSTI

Politika zasebnosti določa, katere datoteke se sinhronizacijo z MobileIron VSP in ali je za vsako vrsto podatkov treba sinhronizirati aktivnosti ali vsebine. Pravilnik o zasebnosti prav tako določajo, katere informacije MobileIron odjemalec mora vključiti v svoj dnevnik sledenja na mobilni napravi.

Nastavitev politike zasebnost, ki je prikazana na sliki 9:

Naziv (Name)
Opisno ime za politiko, ki mora biti unikatno znotraj te vrste politike.

Status (Status)
Vklop ali izklop politike.

Prioriteta (Priority)
Določa prioriteto politike glede na druge politike v isti vrsti politike oz. katera politika se uporablja, če je opredeljena več kot ena politika, povezana z mobilno napravo. Možnosti so »Višje kot« ali »Manj kot« glede na izbrano politiko.

Opis (Description)
Kratek opis pravilnika o zasebnosti oz. kratko pojasnilo politike.

Klici (Calls)
Zbiranje statističnih podatkov o dohodnih in odhodnih klicih.

SMS (SMS)
Zbiranje statistike poslanih in prejetih SMS sporočil. Vsebina SMS sporočil se shrani na MobileIron Server.

Podatki o prometu (Data Traffic)
Zbiranje statističnih podatkov o podatkovnem prenosu na mobilni napravi.

Imenik (Contacts)
Sinhronizirane vsebine kontaktov med mobilno napravo in MobileIron strežnikom.

Aplikacije (Apps)
Pridobivanja identifikacijskih podatkov (npr. metapodatki) programskih rešitev nameščenih na mobilni napravi. Informacije se zbirajo in hranijo na MobileIron strežniku.

Dokumenti (Documents)
Sinhronizirane datoteke med mobilno napravo in MobileIron strežnikom so naslednje končnice: doc, docx, docm, dotx, dotm, xls, xlsx, xlsm, xltx, xltm, xlsb, xlam, ppt, pptx, pptm, potx, potm, ppam, ppsx, ppsm.

Digitalne slike (Picture Files)
Sinhronizirane digitalnih slik med mobilno napravo in MobileIron strežnikom so naslednje končnice: bmp, gif, jpeg, jpg, png, psd, psp, tif, 3dm, 3df.

Video (Video Files)
Sinhronizirane video datotek med mobilno napravo in MobileIron strežnikom so naslednje končnice: 3gp, asf, asx, avi, mov, mp4, mpg, qt, rm, swf, wmv.

Glasbene datoteke (Music Files)
Sinhronizirane vsebine glasbenih med mobilno napravo in MobileIron strežnikom so naslednje končnice: aac, aif, iff, m3u, v sredini, midi, mp3, mpa, ra, ram, wav, wma.

MobileIron iOS večopravilne aplikacije (MobileIron iOS App Multitasking)
Funkcija omogoča podelitev pravice sistemski platformi mobilne naprave za občasno izvajanje mobilne aplikacije MobileIron v spominu mobilne naprave. Primer take aplikacije je sporočanje lokacije mobilne naprave v primeru na silo prekinjenega klica.

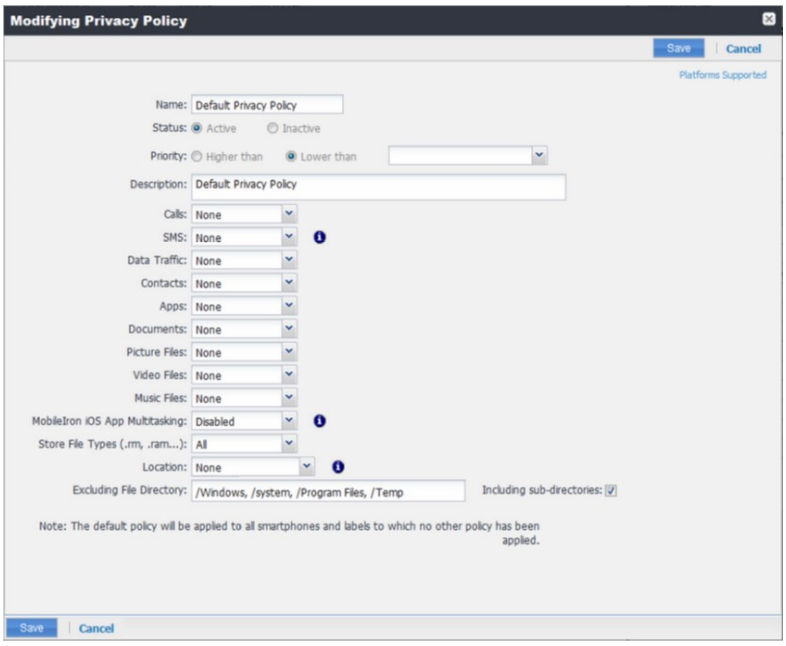
Druge oblike datotek (Store File Types)
Kopiranje vseh ostalih vrst datotek, ki niso opredeljene v zgoraj navedenih oblikah na MobileIron strežniku.

Lokacija (Location)
Opredelitev načina pridobivanja podatkov o lokaciji mobilne naprave, ki se hranijo na MobileIron strežnik. Lokacijski podatki mobilne naprave so:

- Mobilna naprava ima 2G/3G modul za priklop na operaterja mobilne telefonije na osnovi katerega se lahko določi lokacija mobilne naprave;

- Mobilna naprava ima GPS modul, ki sporoča lokacijo mobilne naprave;

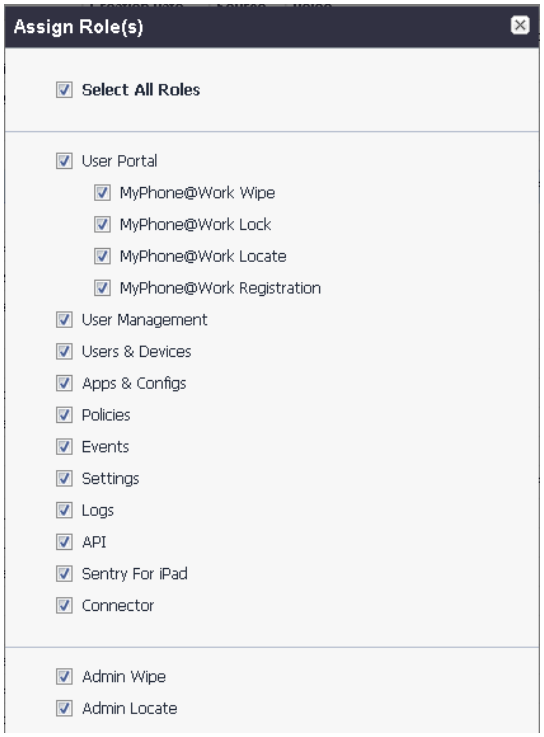
Izvzeti datotečni imeniki (Excluding File Directory)
Opredelitev poljubnega datotečnega imenika, ki ne bo vključen v sinhronizacijo med mobilno napravo in MobileIron strežnikom.



Slika 9: Nivo dostopa v Access Control Listi (Vir: ZZZS)

4.2.2. POOBLASTILA NA SISTEMU

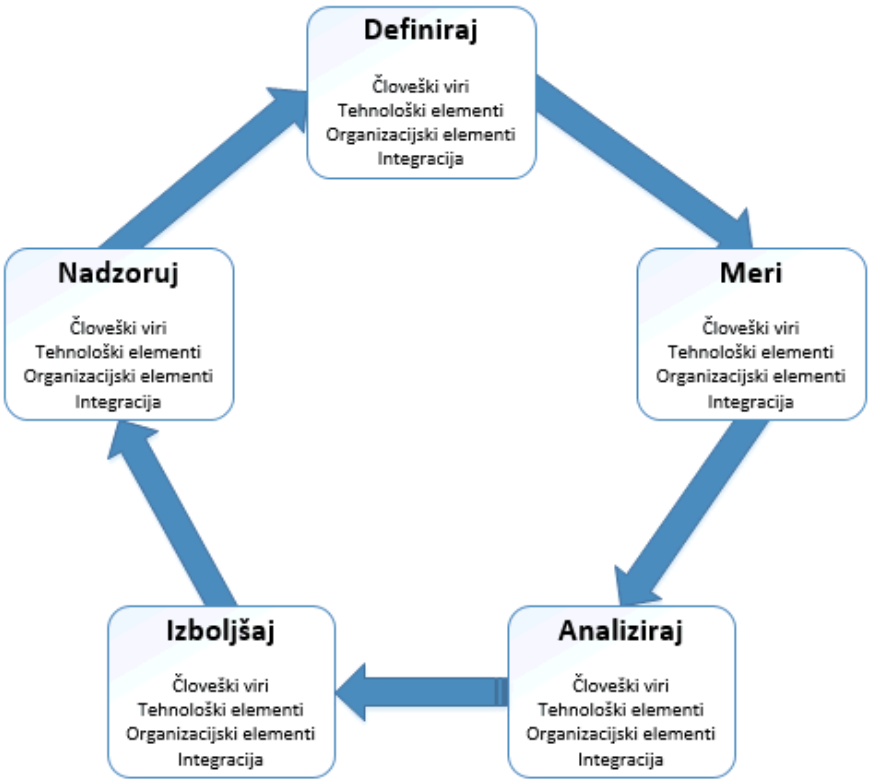
Za potrebe testiranja politike zasebnosti v MobileIron okolju je potrebno imeti podeljena ustrezna pooblastila, ki so prikazana na sliki 10.



Slika 10: Nivo pooblastil za upravljanje mobilnih naprav (Vir: ZZZS)

5. RAZVOJ MODELA UPRAVLJANJA MOBILNIH NAPRAV IN ZASEBNOSTI

Model upravljanja mobilnih naprav in zasebnosti bo temeljil na metodologiji DMAIC, ki vključuje izpeljavo petih zaporednih faz: *Define* (Definiraj), *Measure* (Meri), *Analayse* (Analiziraj), *Improve* (Izboljšaj) in *Control* (Nadzoruj). Komponente predlaganega modela so človeški viri, tehnološki element, organizacijski elementi in integracija. Na sliki 11 je prikazan predlog modela upravljanja.



Slika 11: Model upravljanja mobilnih naprav in zasebnosti (vir: ZZZS)

5.1. ČLOVEŠKI VIRI

Organizacija za uspešno izvajanje varovanja zaupnosti, celovitosti in razpoložljivosti informacij v današnjih informacijskih rešitvah zahteva vključevanje vseh zaposlenih pri uporabi in upravljanju IT rešitev:

- Zavedati se morajo svoje vloge in odgovornosti, povezane s poslanstvom organizacije;
- Razumeti IT varnostno politiko organizacije, postopkov in praks;

- Posedovati ustrezno znanje o upravljanju ter zahtevanih operativnih in tehničnih nadzornih funkcijah pri zaščiti IT virov za katere so odgovorni.

Končni uporabniki

Uporaba mobilne tehnologije je za končne uporabnike s stališča varnosti zahtevna in iz tega razloga občutljiva, saj se zelo velika večina uporabnikov ne zaveda varnostnih tveganj z nepravilno uporabo le te.

Pogosto je v revizijskih poročilih in strokovnih srečanjih za varnost navedeno, da je človek najšibkejši člen pri izvajanju varovanja sistemov in omrežji. Tako lahko sklepamo, da je »človeški faktor« ključnega pomena za zagotavljanje zadostne in ustrezne ravni varnosti. Glede na to, je treba uporabnikom posvetiti dovolj pozornosti.

Celovit in dovolj razširjen program ozaveščanja in usposabljanja je bistvenega pomena, saj le s tem lahko ljudje razumejo svoje varnostne odgovornosti pri uporabi IS, organizacijske politike ter, kako se pravilno uporablja in varuje informacijske vire, ki so jim zaupani. Ozaveščenost na področju varnosti in usposabljanje bi morala biti usmerjena na celotno populacijo uporabnikov organizacije, vključno z vodstvenimi in vodilnimi menedžerji. Le ti pa naj bi bili tudi zgled pravilne in varne uporabe IT in s tem povezana ter upoštevana varnostna pravila uporabe le te v organizaciji.

Kontinuirano ozaveščanje s posodobljenimi interaktivnimi vsebinami glede uporabe in novosti mobilne tehnologije, novimi varnostnimi grožnjami ter priporočili uporabe, zagotovimo večje zadovoljstvo in zaupanje v tehnološke rešitve pri uporabnikih. Ozaveščenost uporabnikov tako prispeva k zmanjševanju varnostnih incidentov.

Z uvajanjem usposabljanja prilagojenega potrebi mobilne tehnologije, se uporabnike praktično usposablja za delo z mobilno tehnologijo. Na usposabljanju se preverijo razumevanje delovanja, postopke uporabe in upravljanje mobilnih naprav ter osnovne postopke za zmanjšanje varnostnih incidentov.

Razvijalci – uvajalci tehničnih rešitev

Uvajalci na osnovi strategije upravljanja mobilnih naprav ter opredeljenih poslovnih in funkcijskih zahtev, implementirajo – razvijejo programske rešitve in s tem povezane komponente. V implementaciji vgradijo operativne in varnostne zahteve, z vključeno mobilno varnostno politiko naprav, dokumentirajo načrt varnostnega sistema ter pripravijo in preizkusijo prototip.

Pri preizkušanju prototipa uvajalci tudi preverjajo uporabniško izkušnjo. S tem se zagotavlja, da bo uporabniška izkušnja z vključenimi varnostnih mehanizmi in politikami uporabe čim boljša, saj je namen, da z mobilno napravo uporabniku zagotovimo varno in enostavno vključenost v poslovni proces ter opravljanje poslanstva organizacije.

Služba za pomoč uporabnikom - HelpDesk

Služba za tehnično podporo uporabnikom – HelpDesk je enotna in glavna vstopna točka za vse uporabnike mobilne tehnologije v organizaciji. Njeno delo je sprejemanje prijav incidentov, poizvedb in zahtev uporabnikov ter vseh ostalih procesov podpore uporabnikom.

5.2. TEHNOLOŠKI ELEMENTI

Tehnološko okolje za mobilno tehnologijo je lahko v celoti nameščeno na obstoječi infrastrukturi organizacije ali pa se nekateri elementi upravljanja lahko uporabljajo kot oblačna storitev pri zunanjem – internetnem ponudniku.

Glavne značilnosti tehnološke infrastrukture:
- Infrastruktura je postavljena v luči zagotavljanja visoke razpoložljivosti, dodajanje novih informacijskih sredstev za povečanje zmogljivosti sistema ter prenosljivosti na različno strojno opremo;
- Temelji na okoljih, ki so neodvisne od sistemov strežnikov;
- Uporabljena je strojna oprema za porazdelitev bremen, za večje obremenitve so predvideni ločeni sklopi po več instanc strežnikov.

Arhitektura za upravljanje mobilne tehnologije podjetja vsebuje štiri področja:
- Zaledni IS organizacije;
- Varnost;
- Internet;
- Uporabniške mobilne naprave.

V vsakem posameznem področju mora biti zagotovljeno pravilno delovanje za uspešno vsakodnevno uporabo mobilnih naprav, saj okvara enega od elementov v posameznem področju, lahko povzroči odpoved delovanja mobilnih naprav in s tem težave pri opravljanju vsakodnevnih dejavnosti v organizaciji.

Zaledni IS organizacije

V primeru mobilnega dostopa, zaledni IS organizacije predstavljajo namenski strežniki, do katerih dostopajo programske rešitve na mobilni napravi. Tipične mobilne programske rešitve so dostop do elektronske pošte, koledarja in stikov.

Za vzpostavitev infrastrukture prikazane na sliki 12 za mobilni dostop, so uporabljeni naslednji strežniki:
- Interni poštni strežnik;
- Strežnik za mobilni dostop do elektronskih sporočil;
- Strežnik za upravljanje mobilnih naprav;
- Aktivni imenik za preverjanje pristnosti uporabnikov;
- Podatkovna baza, ki vsebuje vse podatke o mobilnih uporabnikih in napravah.

Slika 12: Zaledni IS organizacije (Vir: ZZZS)

Poštni strežnik

Poštni strežnik je srce sistema za mobilni dostop. Tu so shranjeni vsi podatki elektronske pošte, koledarja in imenika, do katerih uporabniki dostopajo z mobilnimi napravami. V primeru, da je strežnik dlje časa nedostopen zaradi izgube povezave ali funkcionalne napake, infrastruktura ne more dostavljati podatkov do mobilnih naprav, zato uporabniki zaradi zahtev v poslovnem procesu čutijo veliko motnjo pri opravljanju svojega dela. V ta namen je potrebno pri načrtovanju izgradnje poštnega sistema elektronske pošte, upoštevati poslovne potrebe na osnovi katerih se pripravi ustrezna tehnološka okolica.

Nadzorni strežnik za mobilni dostop do sistema elektronske pošte

Strežnik za nadzor mobilnega dostopa do sistema elektronske pošte je sistemska programska oprema, ki zagotavlja mobilnim napravam stalno in takojšnjo povezavo do zalednega poštnega sistema organizacije. Povezava med strežnikom in mobilnimi napravami temelji na brezžični omrežni tehnologiji. Osnova za izmenjavo je potisni mehanizem oz. protokol, ki zagotavlja dostavo dokumentov iz zalednega poštnega sistema na mobilno napravo in obratno. Potisni mehanizem omogoča izmenjavo osebne elektronske pošte, opravil, osebnega koledarja in imenika.

Strežnik za upravljanje mobilnih naprav

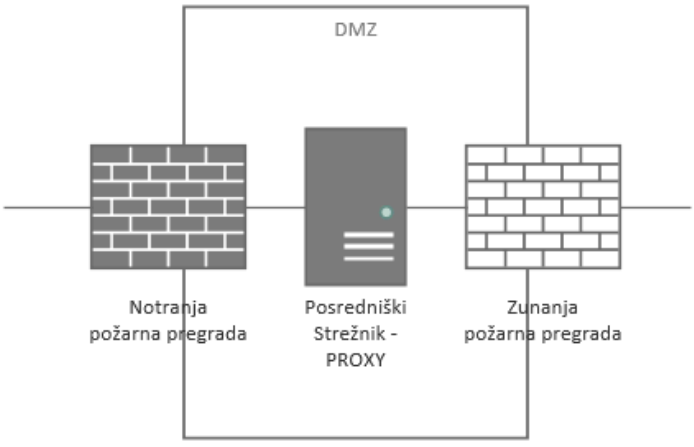
Strežnik s funkcijo upravljanja mobilnih naprav, zagotavlja pregleden seznam uporabnikov in mobilnih naprav, katerim organizacija zagotavlja uporabo servisov v zalednem IS organizacije. Na strežniku je pripravljeno standardno okolje mobilne naprave, ki zagotavlja nabor in nastavitve mobilne programske opreme ter varnostne nastavitve, za uporabo in dostop do zalednih sistemov. Zelo pomembna funkcionalnost sistema za upravljanje mobilnih narav je sprotno spremljanje stanja mobilne naprave: verzije sistemske programske opreme, seznam in verzije nameščene programske opreme, zadnja izmenjava informacij med mobilno napravo in strežnikom za upravljanje. V nekaterih primerih strežnik zagotavlja tudi varno povezavo, ki jo vzpostavlja mobilna naprava do zalednega sistema *Virtual Private Network* (v nadaljevanju: VPN).

Aktivni imenik za preverjanje pristnosti uporabnikov

Aktivi imenik je strežnik, ki je bistven element infrastrukture mobilne tehnologije. Strežnik vsebuje seznam vseh uporabnikov organizacije. To je ključna varnostna komponenta v organizaciji, saj se z njim upravljajo uporabniška imena, gesla in dovoljenja za uporabo mobilnih naprav in dostopov do zalednih sistemov organizacije.

Varnostno področje

Varnostno področje organizacije prikazano na sliki 13, je ključnega pomena in zaradi svoje sestave izredno kompleksno. Upravljanje in nadzor izvajajo interni strokovnjaki za omrežje in omrežno varnost. Običajno je to področje sestavljeno iz mrežne požarne pregrade, ki je neposredno priključena na interno mrežno infrastrukturo podjetja in internet. Običajno vključuje tudi drugi požarni zid, ki skupaj tvorita dvojno požarno pregrado, imenovano demilitarizirana cona (DMZ).



Slika 13: Varnostno področje (Vir: ZZZS)

Notranja požarna pregrada zagotavlja iz pooblaščenih omrežnih naslovov, dostopov preko VPN in strežnikov v demilitarizirani coni, dostop do strežnikov v

zalednem IS organizacije. Zunanja požarna pregrada omejuje ves promet iz interneta v omrežje organizacije kot tudi vzpostavljanje povezave v internet s strani naprav v internem in zalednem informacijskem okolju organizacije. Obojestranska komunikacija poteka zgolj po vnaprej določenih pravilih.

Odvisno od tehnične zasnove rešitve za upravljanje mobilnih naprav, je v področju med dvema požarnima pregradama, strežnik za zaključevanje VPN povezav in posredniški strežnik. VPN omogoča varno upravljanje, brskanje in dostopnost do podatkov v zalednem sistemu organizacije. Posredniški strežnik posreduje zahtevke, ki so zahtevane s strani mobilnih naprav organizacije ali drugih naprav v internetu, tako da le ti nikoli direktno ne dostopajo do strežnika infrastrukture v zalednem IS organizacije.

Internet

To je območje, kjer organizacija nima nikakršnega nadzora in je na poti med mobilno napravo uporabnika in organizacijo. Uporabnik za potrebe povezave z zalednim IS uporablja dva najbolj pogosta načina dostopa: mobilni prenos podatkov ponudnikov mobilnega omrežja in brezžično omrežje v domačem okolju ali kot javno dostopna omrežja v trgovinah, letališčih, kavarnah, hotelih itd. Javno dostopna brezžična omrežja so enostavno dostopna in ne zahtevajo posebne usposobljenosti uporabnika. Z uporabo le teh, pa se bistveno poveča možnost zlorab brez vednosti lastnika.

Uporabniško okolje

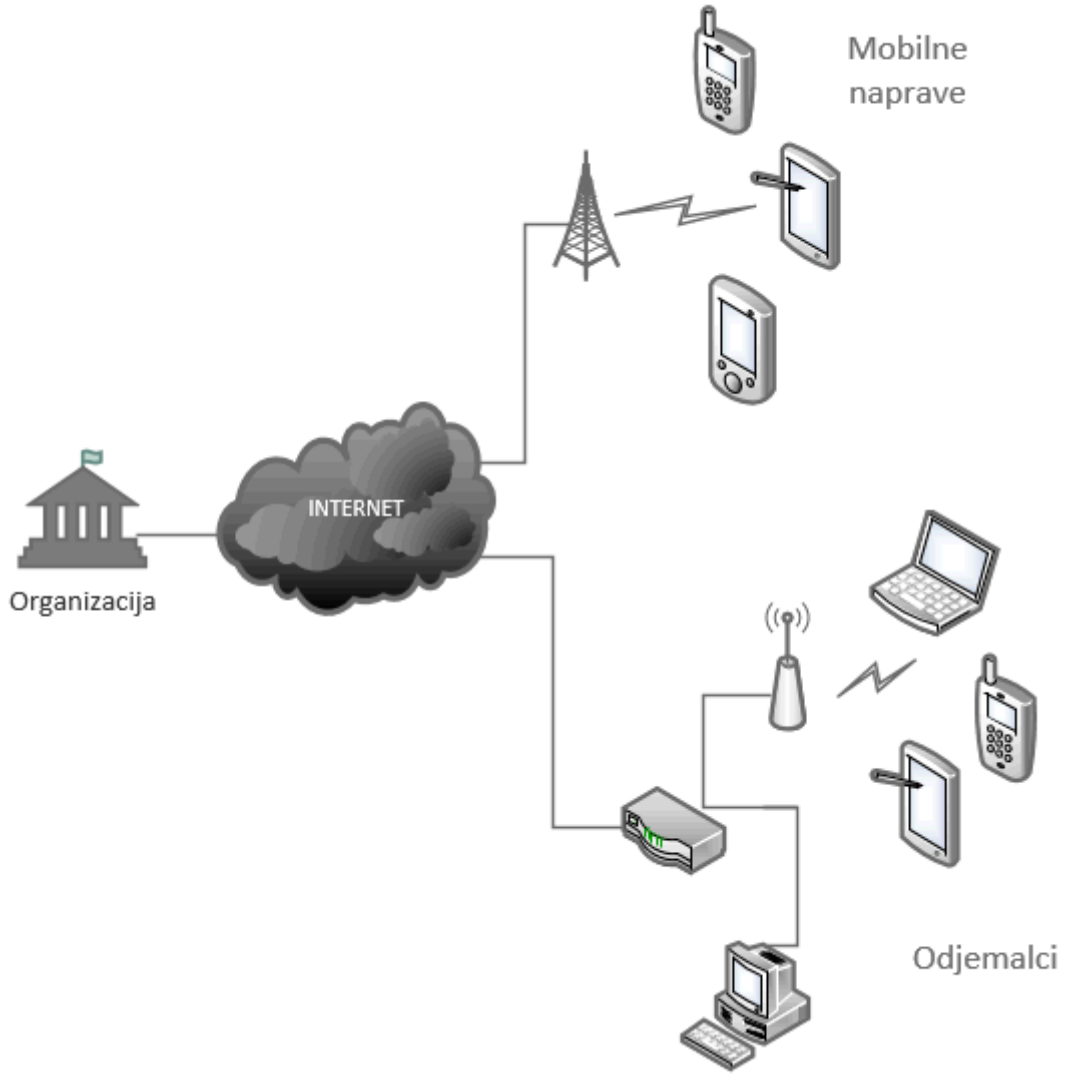
Uporabniško okolje je sestavljeno iz uporabnika, mobilne naprave, mobilne programske opreme in ponudnika brezžične komunikacije.

Mobilna naprava

Je majhna računalniška naprava, običajno dovolj majhna, da jo držimo v roki ter ima zaslon z možnostjo dotika ali tipkovnice. Od velikosti zaslona naprave je odvisno, ali jo uporabljamo kot pametni mobilni telefon ali kot tablični računalnik. Naprava ima operacijski sistem, na katerem se izvajajo različne vrste mobilne programske opreme ter so opremljeni z vmesniki za prenos podatkov (Wifi ali Bluetooth), sistem za bližnjo komunikacijo (NFC) in globalni navigacijski sistem (GPS).

Mobilna programska oprema

Mobilna programska oprema je prilagojena za delovanje na mobilni napravi, ki so lahko nameščene privzeto, preko osebnega računalnika, običajno pa se jih namesti s prenosom z internetnih strani ponudnikov nameščene sistemske programske opreme t.i. operacijski sistem na napravi. Mobilna programska oprema je razvita za potrebe večje produktivnosti, pridobivanja informacij (borza, vreme, elektronska pošta, koledar itd.) in zabavi. Z razvojem sodobnih razvojnih orodij in zahtev uporabnikov, se funkcionalnost približuje programski opremi na namiznih računalnikih.



Slika 14: Internet in uporabniško okolje (Vir: ZZZS)

5.3. ORGANIZACIJSKI ELEMENTI

Celovito upravljanje z mobilno tehnologijo, mora biti urejeno z notranjimi pravili, politikami in navodili, ki opredeljujejo način in organizacijo dela v posamezni organizacijski enoti, postopke ter tehnološke ukrepe, s katerimi se zagotavlja skladnost z načeli, normami in standardi organizacije.

Nenehno posodabljanje tehnološkega okolja, usposabljanje zaposlenih na področju varnosti in uporabe mobilne tehnologije, varovanju informacij, upravljanje tveganj in potrebnih ukrepov za dvig zavesti na tem področju je nujno potrebno.

Interni nadzor z vnaprej pripravljenimi načrti občasnih pregledov, izvaja pregled nad izvajanjem upravljanja z mobilno tehnologijo. S tem organizacija zagotavlja stalno ustreznost in učinkovitost izvajanja ter izpolnjevanja veljavnih notranjih

pravil, predpisov, standardov in zastavljenih ciljev na področju uvajanja mobilne tehnologije. Ugotovitve notranjih nadzorov so podlaga za potrebne morebitne spremembe in dopolnitve sistema in s tem možnosti za izboljšave.

Celovito upravljanje pomeni stalen proces spremljanja, izvajanja, nadzora in ukrepanja, s katerim nenehno dvigujemo raven storitve mobilne tehnologije. S tem se zagotavlja stalno odkrivanje novih potreb uporabnikov in posledično prilaganje poslovnim potrebam, zaznavanje varnostnih dogodkov, zahtevam internih predpisov in zakonodaji.

5.3.1. ZADOLŽITVE POSAMEZNIKOV V ORGANIZACIJSKI STRUKTURI

Direktor IS

Direktor je odgovoren za izpolnjevanje zahtev informacijske in komunikacijske tehnologije pri uporabi mobilne tehnologije. Zato mora biti seznanjen in usposobljen s področja uporabe in varnostnih tveganj mobilne tehnologije. V sodelovanju s strokovnimi sodelavci mora pripraviti ustrezne predpogoje za izvajanje aktivnosti uvajanja mobilne tehnologije. Za celovito upravljanje in uvajanje mobilne tehnologije mora:

- Imenovati koordinatorja za mobilno tehnologijo;
- Zagotoviti pogoje za usposabljanje zaposlenih pri uporabi, uvajanju in upravljanju mobilne tehnologije;
- Pripraviti smernice razvoja mobilne tehnologije;
- Izvajati nadzor oseb s pomembnimi odgovornostmi pri izvajanju politik in postopkov mobilne tehnologije;
- Spodbujati strokovni razvoj strokovnih sodelavcev za mobilno tehnologijo;
- Potrjevati program razvoja mobilne tehnologije;
- Zagotoviti, da zaposleni razumejo pravila uporabe mobilne tehnologije;
- Pripraviti postopke za odvzem pooblastil zaposlenim zaradi pomanjkanja ozaveščenosti ali usposobljenosti;
- Pripraviti kriterije za podelitev mobilnih naprav zaposlenim, ki temelji na zadolžitvah zaposlenega;
- Opredeliti finančna sredstva za uvedbo storitve za mobilne naprave;
- Podeliti pooblastila za lokalnega koordinatorja mobilne tehnologije.

Svetovalec direktorja za varnost

Svetovalec direktorja za varnost je odgovoren za razvoj, strategijo in vizijo upravljanja varnosti v organizaciji:

- Usmerja oblikovanje in izvajanje politik in postopkov, povezanih z varnostjo IS;
- Pripravlja (upravljanje razvoj) in izvaja globalno varnostno politiko, standarde, smernice in postopke za zagotavljanje stalnega vzdrževanja varnosti;
- Usmerja zaposlene za prepoznavanje, razvijanje, izvajanje in vzdrževanje varnostnih procesov v organizaciji za zmanjšanje varnostnih tveganj, odzivanje na incidente;
- Vzdržuje odnose z organi pregona in drugimi sorodnimi vladnimi organi;

- Sodeluje z zunanjimi svetovalnimi podjetji za potrebe neodvisne varnostne presoje;
- Obdobno ovrednoti varnostna tveganja, ki so rezultati presoj, pregledov in testiranj. Na osnovi teh pripraviti načrt ukrepov za izboljšanje stanja informacijske varnosti.

Lokalni koordinator za mobilno tehnologijo

Lokalni koordinator za mobilno tehnologijo je operativno zadolžen za spremljanje in vodenje evidenc nabave mobilne tehnologije. Izvaja sledeče postopke:

- Vodi evidenco imetnikov mobilnih naprav in podatkov o mobilni napravi:
  - Podrobne podatke o zaposlenem;
  - Telefonska številka, ki jo uporablja mobilna naprava;
  - Podatki o odobritvi mobilne naprave;
  - Datum izdaje mobilne naprave;
  - PIN in PUK koda;
  - Kontaktne podatke;
  - Datum nadgradnje ali servisnih posegov;
  - Dodatna oprema (baterija, polnilci itd.);
  - Podrobnosti o omejitvah.
- Naročanje tehnološke opreme mobilne tehnologije;
- Prijave in odjava mobilnih številk pri mobilnem operaterju;
- Spremlja mesečno porabo stroškov po uporabniku;
- Od uporabnika pridobiva potrditve za upravičenost porabe v tekočem mesecu;
- Pripravi podatke za računovodstvo o vsoti, ki se uporabniku zaračuna zaradi neupravičene uporabe klicev ali drugih plačljivih storitev na mobilni napravi.

Skrbniki IS

Skrbniki IS upravljajo strojno in programsko opremo, ki zagotavlja nemoteno delovanje mobilne tehnologije. Naloge, ki jih izvajajo:

- Nadziranje in spremljanje informacijsko komunikacijske opreme;
- Podeljujejo pooblastila uporabnikom za dostop do storitev mobilne tehnologije;
- Poročajo o varnostnih incidentih pri uporabi mobilne tehnologije svetovalcu za varnost;
- Pripravljajo predloge v primeru novih ranljivosti ali varnostnih incidentih;
- Obveščajo uporabnike o morebitnih varnostnih incidentih in jih ozaveščajo o varni rabi mobilne tehnologije;
- Svetuje pri uporabi in nadgradnji IS.

Finančni vodja

Finančne vodje so odgovorne osebe v posamezni organizacijski enoti, ki izvajajo postopke za spremljanje izdatkov mobilne tehnologije za posameznega zaposlenega. V primeru prekoračitve opredeljene višine računa ter dejstvom, da

je bila le ta uporabljena za osebne namene, se zahteva povračilo prekoračenega zneska.

Služba za pomoč uporabnikov - HelpDesk

Naloge službe za pomoč uporabnikom v okviru izvajanja podpore uporabnikom:

- Identificirajo težave in jih sistematično beležijo;
- Raziskujejo prijavljene probleme;
- Beležijo vse ustrezne začasne rešitve in hitre popravke;
- Uvajajo spremembe za izvajanje trajnih strukturnih rešitev;
- Analizirajo in ugotavljajo trende pojavljanja incidentov in problemov ter proaktivno preprečujejo njihovo nastajanje;
- Proaktivno preprečujejo težave s tehnikami, kot je analiza trendov.

Cilj zgoraj navedenih nalog je obnova normalnega delovanja storitve ali mobilne naprave v čim krajšem času in s čim manjšimi motnjami pri uporabi.

Izhajajoč iz prakse bi končne uporabnike, glede na njihovo usposobljenost za samostojno delo z računalnikom, lahko razdelili v tri skupine (povzeto po Cotman, 2003):

- **Napredni uporabnik:** samostojno uporablja strojno in programsko opremo. Znajde se v omrežju in na svetovnem spletu. Sam si nameša popravke, nadgradnje, gonilnike za strojno opremo, skrbi za zaščito in arhiviranje. Razume delovanje osebnega računalnika in si ga sam prilagaja svojim potrebam;
- **Aktivni uporabnik:** samostojno uporablja strojno in programsko opremo. Znajde se v omrežju in na svetovnem spletu, načeloma razume delovanje osebnega računalnika, vendar občasno potrebuje pomoč pri nameščanju popravkov, nadgradenj ali gonilnikov strojne opreme. Površno skrbi za zaščito in arhiviranje. Potrebuje pomoč pri zahtevnejših in nestandardnih opravilih;
- **Pasivni uporabnik:** je usmerjen izključno v ozko uporabo aplikacij, ki jih potrebuje pri svojem delu. Ni ozaveščen glede zaščite in arhiviranja, ne razume delovanja osebnega računalnika, ne znajde se pri delu z datotekami, z internetnimi storitvami ali s strojno opremo.

Uporabniki se na HelpDesk obračajo z različnimi vrstami zahtev:

- **Zahteve po pojasnjevanju in razlagi,** je najpogostejši razlog, ki je posledica slabega poznavanja sistemske ali programske opreme na mobilni napravi. Uporabniku je v tem primeru hitreje in enostavneje poklicati HelpDesk, kot pa samostojno raziskovati okolje mobilne naprave;
- **Odpravljanje napak uporabnika**, je posledica nepoznavanja delovanja sistemske ali programske opreme. Skrbniki sistemske in programske opreme HelpDesku pripravijo ustrezna navodila za odpravo napake ali ponovno namestitev;
- **Sistemske in programske napake**, predstavljajo najmanjši delež zahtev uporabnikov. Pred uvedbo v produkcijo, se rešitve temeljito preverijo. Te zahteve predvidoma zahtevajo posredovanje incidenta na višji nivo podpore;
- **Dopolnitev sistemskih in programskih nastavitev ali funkcionalnosti.** Uporabniki s pridobljenimi izkušnjami pri uporabi izrazijo željo po

spremembi, nadgraditvi ali namestitvi novih programskih rešitev na mobilni napravi.

Upravljanje konfiguracij je osnova za uspešno upravljanje mobilne tehnologije. Posamezni elementi upravljavskih sistemov za mobilno tehnologijo morajo zagotoviti pregleden seznam obstoječih konfiguracij. Na ta način je omogočeno celovito izvajanje analize scenarijev nadgradnje, izvajanje pomoči uporabnikom. HelpDesk pri upravljanju s spremembami strojne in programske opreme zagotavlja celostno obravnavo sprememb na mobilnih napravah, pri čemer upošteva tako tehnične kot tudi pravne in pogodbene obveznosti (Zabukovec, 2008).

Uporabnike morajo o predvidenih spremembah pravočasno obveščati, saj vzdrževanje lahko zahteva tudi prekinitev delovanja uporabljeni spletnih ali internih mobilnih servisov ter mobilnih naprav. Pravočasno in celovito napovedovanje vzdrževalnih postopkov tako lahko prepreči slabo voljo pri uporabnikih.

HelpDesk poleg odpravljanja težav in incidentov, izvaja tudi usposabljanje uporabnikov. V ta namen morajo zaposlenemu biti zagotovljene neformalne oblike usposabljanja. Usposabljanje služi pridobivanju, obnavljanju, razširjanju, posodabljanju in poglabljanju znanja. Področja usposabljanja morajo obsegati tako tehnično usposabljanje za uporabo orodij (sistemska in aplikativna programska oprema), usposabljanje glede postopkov, urjenje v nameščanju, uporabi in izboljševanju delovanja programskih rešitev za avtomatizirano podporo, kot tudi osebnostnem usposabljanju: urjenje v komunikacijskih sposobnostih, hitrem iskanju odgovorov itd (Zabukovec, 2008).

Usposabljanje končnih uporabnikov je namenjeno učinkovitejši uporabi strojne in programske opreme, ki jo poseduje. Usposabljanje vseh uporabnikov pa je naložba v celostno poslovanje organizacije. Za delovno mesto podpore uporabnikom to posledično pomeni manjša poraba časa za nezahtevnejše intervencije in več časa za centralni nadzor in upravljanje sistema (Zabukovec, 2008).

5.3.2. PRAVILA, POLITIKE IN NAVODILA

Politike varovanja zasebnosti

Upravljanje z mobilno tehnologijo mora vključevati skladnost z notranjimi pravili in politikami z veljavno zakonodajo in predpisi. Nadzor mobilnih naprav mora upoštevati pravno ravnovesje med zasebnostjo in organizacijsko varnostjo. Sistemski skrbniki, lokalni koordinatorji in drugi, ki upravljajo mobilne naprave, morajo ves čas spoštovati zasebnost podatkov, kar pomeni, da ne izvajajo sistematičnega spremljanja aktivnost na mobilnih napravah za posameznega uporabnika.

Če obstaja sum kršitve notranjih pravil in politik ali nezakonite dejavnosti zaposlenega pri uporabi mobilne naprave, je za spremljanje aktivnosti, treba pridobiti soglasje s strani vodje posamezne organizacijske enote, svetovalca direktorja za varnost in zaposlenega. Podrobni podatki spremljanja se morajo

varno shraniti in so dostopni osebam, ki imajo dovoljenje za dostop do teh informacij.

Opredelitev celovitih postopkov oddaljenega brisanja podatkov v primeru zlorabe mobilne naprave, zagotavlja spoštovanje zasebnosti in celovitosti osebnih podatkov zaposlenega.

Dostop do podatkov na mobilni napravi, ki so last uporabnika, lahko podeli zgolj uporabnik sam. Podatki so: klici mobilne telefonske naprave, kratka besedilna sporočila, glasovna pošta, fotografije ali kakršne koli druge informacije, na mobilni napravi, ki so last uporabnika mobilne naprave.

Pravilnik o varovanju osebnih in občutljivih podatkov

Zaradi varstva osebnih podatkov morajo zaposleni in zunanji sodelavci pri obdelavi osebnih podatkov izvajati splošne varnostne ukrepe, tako da:

- Osebne podatke obdelujejo le v okviru svojih pooblastil in delovnih potreb, pristojnosti ali dela izključno v dovoljene namene in v dogovorjenem obsegu ter da jih ne obdelujejo za osebne namene ali za nepooblaščeno tretjo osebo;
- Delovno okolje in delovna sredstva zavarujejo pred nepooblaščenim dostopom in vpogledom do osebnih podatkov;
- Zavarujejo pred odtujitvijo iz delovnega okolja in iz delovnih sredstev osebne podatke kot tudi delovna sredstva;
- Po končani obdelavi osebnih podatkov uničijo pomožno gradivo, ki so ga uporabili oziroma je nastalo pri obdelavi;
- O aktivnosti, ki je usmerjena v nepooblaščeno, nepravilno ali zlonamerno obdelavo osebnih podatkov nemudoma obvestijo nadrejenega delavca, sami pa poskušajo te aktivnosti preprečiti;
- Upoštevajo vse zakonske in interne predpise, ki urejajo ravnanje z osebnimi podatki.

Za zagotovitev varstva osebnih podatkov zaposleni pri obdelavi:

- Ne odlagajo nosilcev osebnih podatkov, svojega delovnega področja in informacijske opreme, ki jo uporabljajo, nenadzorovane (zaklepanje prostorov, omar, pisalnih miz ipd.) ali v prisotnosti oseb, ki nimajo pravice dostopa in vpogleda vanj;
- Osebne podatke posredujejo le fizičnim in pravnim osebam, ki izkažejo zakonsko upravičenost do pridobitve teh podatkov;
- Uporabljajo gesla na način, ki nepooblaščenim osebam onemogoča seznanitev z njimi;
- Ne »posojajo« svojega gesla sodelavcem, tudi v primerih, ko ima sodelavec enak obseg pooblastil;
- Ob koncu dela s predpisanim postopkom zaključijo uporabo opreme (izklopijo računalnike in drugo strojno opremo ali so kako drugače fizično ali programsko zaklenjeni) in zaklenejo prostore, omare, pisalne mize ipd., kjer so nosilci osebnih podatkov;
- Ne posredujejo osebnih podatkov po telefonu;
- Praviloma ne sprejemajo strank v pisarnah oziroma izven prostorov, namenjenih obiskovalcem, ter izven časa, določenega za delo s strankami;

- Upravičenim uporabnikom posredujejo le podatke s svojega delovnega področja, o zadevah drugih delavcev pa le z njihovim predhodnim dovoljenjem;
- Iz uradnih prostorov ne odnašajo dokumentacije in drugega materiala, ki vsebuje osebne podatke;
- Ne mečejo odpadnih nosilcev podatkov z osebnimi podatki v koše za smeti;
- Ne nameščajo in ne odnašajo programske opreme brez vednosti in odobritve pooblaščene osebe, zadolžene za delovanje računalniškega IS iz delovnega okolja;
- V primeru izginotja osebnih podatkov o tem nemudoma obvestijo nadrejenega delavca.

Prenos osebnih podatkov

Prenos osebnih podatkov z informacijskimi - telekomunikacijskimi in drugimi sredstvi, je dovoljen le na način, ki nepooblaščenim osebam onemogoča neupravičeno seznanjanje z vsebino teh podatkov, njihovo spreminjanje, prilaščanje ali uničenje.

Pri prenosu občutljivih osebnih podatkov preko teh sredstev, morajo biti ti podatki ustrezno zavarovani s primernimi metodami šifriranja tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Uničenje osebnih podatkov

Osebni podatki se izbrišejo oziroma uničijo:
- Po izpolnitvi namena, zaradi katerega so bili zbrani, vodeni in obdelovani;
- Po preteku rokov za hrambo dokumentacijskega gradiva, določenih z zakonom ali internim aktom organizacije.

Za izbris oziroma uničenje osebnih podatkov iz računalniških medijev se uporabijo metode in postopki, ki popolnoma onemogočajo restavracijo izbrisanih osebnih podatkov (formatiranje medija). Delavca za izbris oziroma uničenje osebnih podatkov na računalniških medijih določi direktor.

V primeru, da uničenje osebnih podatkov izvede pogodbeni partner, mora pri uničenju sodelovati pooblaščeni delavec organizacije, ki ga določi direktor.

Odhod zaposlenega iz organizacije

Zaposleni mora vrniti svoje mobilno napravo in vso pripadajočo opremo lokalnemu koordinatorju za mobilno tehnologijo, preden zapusti organizacijo.

V primeru, da se izvede prerazporeditev zaposlenega znotraj organizacije, se mora zagotoviti, da so o tem obveščeni lokalni koordinatorji za mobilno tehnologijo v obeh organizacijah, ki opravijo popravke v internih evidencah mobilnih naprav.

Zaposleni, ki se upokoji ali sporazumno zapusti organizacijo, lahko klicno številko obdrži, mobilno napravo in vso pripadajočo opremo pa odkupi.

Zaupnost in zasebnost

Glede na potrebo po spoštovanju zaupnosti, morajo biti uporabniki v vsakem trenutku pazljivi pri uporabi svoje mobilne naprave na javnih mestih. S tem preprečijo nenamerno razkritje občutljivih, zaupnih osebnih informacij in informacij partnerjev organizacije.

Uporabniki ne smejo uporabljati mobilne naprave za pošiljanje besedilnih sporočil, ki vsebujejo zaupne in/ali osebne podatke v povezavi z organizacijo, njenih zaposlenih in poslovnih strank.

Vsa poslana elektronska sporočila z mobilne naprave prejemnikom v internet, ki vsebujejo zaupne in/ali osebne podatke, je potrebno šifrirati v skladu s pravilnikom o varovanju osebnih in občutljivih podatkov.

Uporaba storitev interneta in elektronske pošte

Uporabo storitev internetna in/ali elektronske pošte je omogočena vsem zaposlenim v organizaciji in je praviloma namenjena službeni uporabi z namenom, da se zagotovi učinkovito opravljanje delovnih nalog. Uporaba za osebne namene je dopustna le, če to ni v nasprotju z interesi organizacije, ne ovira njenih delovnih procesov in ne ogroža varnosti informacij.

Cilja organizacijskega predpisa glede omejevanja uporabe interneta sta:

- Preprečiti:
  - Izgubo, spremembo ali zlorabo informacij in podatkov;
  - Nepooblaščen dostop, spremembo ali zavrnitev storitev;
  - Zmanjšati dovzetnost za napake;
  - Posledice, ki jih ima objava javno dosegljivega seznama elektronskih poštnih seznamov zaposlenih v organizaciji;
  - Nenamensko uporabo storitev interneta in elektronske pošte;
- Zagotoviti:
  - Večjo zanesljivost in dostopnost storitev interneta in elektronske pošte;
  - Možnost morebitnega dokazovanja izvora, odpošiljanja, dostave in prejema informacij in podatkov;
  - Seznanjenost vseh uporabnikov z njihovimi pravicami in odgovornostmi v povezavi s storitvami interneta in elektronske pošte.

Z organizacijskim predpisom o uporabi interneta in/ali elektronske pošte je opredeljen namen, postopki, pravice in obveznosti uporabnikov storitev interneta in elektronske pošte, kot dela IS organizacije. Namenjen je vsem zaposlenim, ki uporabljajo storitve interneta in/ali elektronske pošte.

S prekinitvijo delovnega razmerja v organizaciji, prenehajo tudi vse pravice do uporabe storitev interneta in/ali elektronske pošte.

Zaposleni, ki uporabljajo storitve interneta in/ali elektronske pošte, ne smejo uporabljati lažnih ali zavajajočih osebnih podatkov. Za nedopustno ravnanje se štejejo aktivnosti, ki so v nasprotju z veljavno zakonodajo, predpisi in pravili dobre prakse, ter škodujejo ugledu in poslovanju organizacije.

Zaposleni pri uporabi internetnih storitev ne smejo:

- Pošiljati prispevkov za nestrokovne ali osebne polemike, oglasov, verižnih sporočil;
- Objavljati ali pošiljati podatkov z žaljivo ali pornografsko vsebino, tajnih podatkov ali podatkov, ki so zaščiteni z avtorskimi pravicami ali so v lasti drugih uporabnikov. To velja tako za uporabo elektronske pošte kot sodelovanje v raznih forumih;
- Uničevati ali spreminjati podatkov, ki so last drugih uporabnikov;
- Uporabljati programov ali postopkov, ki ovirajo normalno delovanje računalniških naprav, ki sestavljajo omrežje;
- Omogočati dostop do informacijskega okolja organizacije tretjim osebam;
- Poskušati pridobiti in uporabiti dostop, ki je bil dodeljen drugemu zaposlenemu;
- Uporabljati dostop do omrežja za pridobitne dejavnosti;
- Uporabiti dostop za napad na katerokoli postajo v svetovnem spletu;
- Uporabiti servise, ki niso namenjeni javni uporabi;
- Izmenjevati škodljivo in zlonamerno programsko opremo;
- Izmenjevati avtorsko ali patentno zaščiteno programsko opremo, orodja in dokumente brez pisne privolitve lastnika;
- Nameščati programsko opremo brez pisne odobritve avtorja ali odgovorne osebe.

Zaposlenim ni dovoljeno:

- Širjenje ali pregledovanje nemoralnih, žaljivih in nezakonitih vsebin;
- Prenos oz. nalaganje podatkov v zasebne namene;
- Prenos oz. nalaganje datotek iz nezanesljivih oziroma sumljivih virov;
- Prenos oz. nalaganje in uporaba programske opreme v nasprotju z licenčnimi pogoji;
- Nezakonito kopiranje in izraba avtorske glasbe, filmov in programske opreme.

Pregledovanje določenih spletnih (URL) naslovov ali določenih vsebin na spletu, se lahko onemogoči. Odgovorna oseba odobri spletne naslove ali vsebine, do katerih se bo tehnično omejil dostop.

Organizacijski predpis o uporabi interneta se v praksi izvaja z ustreznimi nastavitvami na tehničnih elementih za dostop do interneta. Pravilni način izvajanja pravilnika je politika preprečevanja na osnovi vnaprej določenih spletnih vsebinskih sklopih (pornografija, igralništvo, nasilje, igralništvo, posredniški strežnik (Proxy), omrežje vsak z vsakim (P2P) itd.). Svetovalec direktorja za varnost v sodelovanju s skrbnikom tehničnega sistema pripravi spletne naslove ali vsebinske sklope, do katerih se bo tehnično omejil ali preprečil dostop na internetu.

Nadzor uporabe storitev interneta in elektronske pošte

IS organizacije beleži dogodke, povezane z uporabo in upravljanjem storitev interneta in/ali elektronske pošte s strani zaposlenih. Nadzor nad uporabo se izvaja v primeru zaznanih varnostnih incidentov v skladu s politiko upravljanja varnostnih dogodkov.

Organizacija ima pravico spremljati, nadzorovati in zapisovati dostope do interneta, elektronske pošte in njegovega omrežja. Za potrebe zakonitega in neodvisnega nadzora se mora zagotoviti sledljivost aktivnosti izvajanja nadzora iz revizijskih sledi.

Odgovorna oseba za informacijsko varnost in skrbniki posameznih sistemov za storitve interneta in/ali elektronske pošte so odgovorni za vzpostavitev nadzora dostopa do storitev, za obveščanje uporabnikov o možnih nevarnostih pri uporabi storitev interneta ter za njihovo ozaveščanje in usposabljanje pri ugotavljanju in preprečevanju varnostnih incidentov v organizaciji.

Skrbnik sistema sebi ali komu drugemu ne sme pridobivati informacij o vsebini, dejstvih ali okoliščinah uporabe storitev interneta in/ali elektronske pošte ter brez vednosti uporabnika posegati v vsebino in sporočila elektronskega poštnega predala uporabnika.

Skrbnik uporabi namensko programsko orodje za omejevanje in preprečevanje dostopa zaposlenih iz lokalnega omrežja organizacije, če je to potrebno za zagotavljanje večje razpoložljivosti komunikacijskih poti, zmanjševanje stroškov in obrambo pred zlonamerno programsko opremo, s katero je ogrožen IS organizacije.

Pravila uporabe mobilnih naprav

Mobilne naprave se predvsem uporabljajo za namene, ki so povezane s službenim delom, dovoljeno pa je tudi za občasno in omejeno osebno uporabo, vendar omejeno z določenim skupnim zneskom mesečne porabe pri operaterju, s katero je sklenjena pogodba o zagotavljanju storitev mobilne telefonije.

Mobilno napravo lahko uporablja samo zaposleni, ki je zadolžil dotično napravo in si je ne sme deliti z drugimi zaposlenimi v organizaciji ali dati v uporabo katerikoli tretji osebi izven organizacije, razen s predhodnim dovoljenjem lokalnega koordinatorja za mobilno tehnologijo.

Zaposleni morajo zagotoviti, da ves čas uporabljajo mobilno napravo na način, ki je zakonit, etični in učinkovit. Organizacija lahko zaposlenemu odvzame mobilno napravo, če presodi, da uporaba ni v skladu z notranjimi pravili, ali zaposleni zlorablja mobilno napravo na kakršenkoli način.
Zaposleni se mora po svojih najboljših močeh potruditi, da se zagotovi varno hranjenje mobilne naprave oz., da je pod nenehnim nadzorom zaposlenega. Med delovnim časom, dežurstvi in stalno pripravljenostjo morajo biti mobilne naprave

napolnjene, vklopljene ter dosegljive za klic. To velja za mobilne naprave, ki imajo omogočeno sprejemanje in klicanje preko operaterja mobilne telefonije.

Na mobilno napravo je lahko nameščena samo programska oprema, ki je pravilno in ustrezno licenčno kupljena ali s strani organizacije odobrena. Podlaga za to je pripravljen sezname potrebnih in dovoljenih mobilnih aplikacij ter kriteriji za prepovedane mobilne aplikacije.

Celovito in učinkovito upravljanje mobilnih naprav lahko zagotovimo le s pripravljenim seznamom podprtih mobilnih naprav, kar zagotavlja ustrezen nivo podpore, obvladovanje upravljanja mobilnih naprav ter zmanjševanje možnosti varnostnega incidenta.

Pogost način shranjevanja mobilnih podatkov so oblačne storitve, ki predstavljajo navidezna spletna sredstva z enostavno uporabo preko vmesnikov. Navidezna spletna sredstva so zelo razširjena med uporabniki, saj zagotavljajo visoko zmogljivost, prilagodljivost, zanesljivost, predvsem pa cenovno ugodno ponudbo, ki je pogosto pri osnovni uporabi brezplačna. V ta namen se pripravijo priporočila za shranjevanje vsebin v oblaku ali pa se uporabnikom zagotovi podobna storitev shranjevanja podatkov v zalednem sistemu organizacije.

Klici iz mobilne naprave se lahko izvajajo le znotraj telefonskih številk nacionalnih operaterjev. Uporaba mobilnih naprav za mednarodne klice se uporablja le v izjemnih okoliščinah, kot so na primer:

- Zaposleni je na poslovnem potovanju v tujini;
- Zaposleni dela izven kraja zaposlitve ali rednega delovnega časa ter mora vzpostaviti kontakt z zunanjim partnerjem ali ponudnikom storitev v tujini;
- V primeru izrednega dogodka;
- Po presoji nadrejenega ali direktorja organizacije.

Mobilna naprava se ne sme uporabljati za klicanje premijskih telefonskih številk 090 ali plačljivih SMS sporočil.

Uporaba elektronske pošte in dostop do interneta na mobilni napravi se ureja po pogojih pravilnika o uporabi elektronske pošte in interneta.

Uporaba mobilnih naprav v vozilu mora biti zaradi pravnih razlogov, interesa javnosti in osebne varnosti, v skladu z veljavno zakonodajo.

Nesprejemljiva uporaba mobilne naprave

Mobilna naprava se ne sme uporabljati:

- Pretirana osebna uporaba, oglaševanje ali opravljanje dela za osebno korist ali dobiček;
- Posredovanje zaupnih ali osebnih podatkov zunaj organizacije, razen če so bili podatki šifrirani in izmenjava odobrena s strani lastnika podatkov;
- Pošiljanje besedilnih sporočil, ki vsebujejo zaupne in/ali osebne podatke v zvezi z organizacijo, njenimi zaposlenimi ali zunanjimi partnerji;

- Ogled, ustvarjanje ali prenos pornografskega, žaljivega ali obscenega gradiva (v obliki informacije, digitalne slike, avdio-video posnetka itd.), ki bi lahko povzročila kaznivo dejanje;
- Dejavnost, ki bi kršile pravice intelektualne lastnine (npr.: ne licencirana namestitev, distribucija ali kopiranje avtorsko zaščitenega materiala);
- Vsaka dejavnost, ki bi ogrožala zasebnost drugih;
- Vsaka dejavnost, ki bi namerno povzročila motnje na IS organizacije ali drugih subjektov mobilne tehnologije;
- Vsaka dejavnost, ki bi namerno ogrozila varnost virov IS organizacije, vključno z zaupnostjo in celovitostjo podatkov in razpoložljivostjo informacijskih virov (npr.: namerno ali malomarno povzroči okužbo in širitev računalniškega virusa ali zlonamerne programske opreme);
- Z namestitvijo in uporabo programske ali strojne opreme, ki bi onemogočala prekinitev varnostnih mehanizmov in centralnega upravljanja na mobilni napravi;
- Za ustvarjanje ali prenos nezaželenih *spam* elektronskih sporočil v komercialne ali oglaševalske namene;
- Vsako dejavnost, ki bi pomenila kaznivo dejanje in s tem povzročila civilno odgovornost ali kakršno drugo kršitev zakona.

Varnost pri uporabi mobilne naprave

Zaposleni morajo zagotoviti, da je njihova mobilna naprava ob vsakem času zaščitena pred nepooblaščeno uporabo. Vsi modeli mobilnih naprav morajo za dostop v napravo imeti vklopljeno možnost gesla z uporabo PIN (*Personal Identification Number*), geslo, vzorec ali biometrični znak (prsni odtis ali slika obraza).

Pri uporabi morajo zaposleni sprejeti vse razumne ukrepe za preprečitev škode ali izgube/odtujitve zadolžene mobilne naprave. Mobilne naprave ne smejo pustiti nenadzorovane in ko le ta ni v uporabi, jo varno shranijo. Zaposleni prevzame odgovornost za izgubo ali morebitno škodo na mobilni napravi, če je ugotovljeno, da le ta ni ustrezno izvajal ukrepov za preprečitev.

V primeru suma varnostnega incidenta, katerega posledica je sprememba varnostnih nastavitev mobilne naprave in s tem povezana izguba, sprememba ali zloraba informacij in podatkov, nepooblaščen dostop, spremembo ali zavrnitev uporabniških mobilnih storitev organizacije, so uporabniki dolžni preprečiti tako, da ugasnejo mobilno napravo in o tem takoj obvestijo odgovorno osebo v organizaciji.

Občutljivih in osebnih podatkov ne smejo shraniti na mobilni napravi brez predhodnega dovoljenja predpostavljenega vodje in v soglasju s svetovalcem direktorja za varnost. Kadar so občutljivi in osebni podatki shranjeni na mobilni napravi, morajo biti informacije šifrirane v skladu s pravilnikom o varovanju osebnih in občutljivih podatkih.

Izgubljene ali odtujene mobilne naprave

Zaposleni mora takoj prijaviti izgubo ali odtujitev mobilne naprave lokalnemu koordinatorju za mobilno tehnologijo in skrbniku za upravljanje mobilnih naprav. Zaposleni odtujitev mobilne naprave prijavijo tudi na policijo.

Skrbniki mobilnih naprav glede na prijavo o izgubi ali odtujitvi naprave, izvedejo postopke oddaljenega brisanja podatkov elektronske pošte in morebitne shranjene zaupne ali občutljive podatke organizacije ali njenih partnerjev na mobilni napravi. Skrbniki sistema za upravljanje mobilnih naprav, lahko izbrišejo zasebne podatke na mobilni napravi le s privolitvijo lastnika naprave. Po izvedbi brisanja se izvede blokada dostopa mobilne naprave do vseh virov zalednega IS organizacije.

Lokalni koordinator za mobilne naprave mora o dogodku obvestiti direktorja enote in ponudnika mobilne telefonije, ki izvede vse potrebne aktivnosti za blokado telefonske številke ter mobilne naprave.

Servisiranje mobilne naprave

Okvarjene mobilne naprave se na popravilo predajo le zunanjim pooblaščenim servisom. Koordinator za mobilno tehnologijo, okvarjeno mobilno napravo evidentira v centralni evidenci, v kateri navede opis napake ter pripravi servisni zahtevek ter izbriše vse uporabniške podatke in sistemske nastavitve s pomočjo vgrajene sistemske funkcije za celovito brisanje – povrnitev na tovarniške nastavitve.

Odpis mobilnih naprav

Zastarele in okvarjene mobilne naprave, ki jih ni moč popraviti, jim je potrebno izbrisati vse podatke na napravi ter jih ustrezno uničiti v skladu z Uredbo o ravnanju z odpadno električno in elektronsko opremo.

Usposabljanje zaposlenih

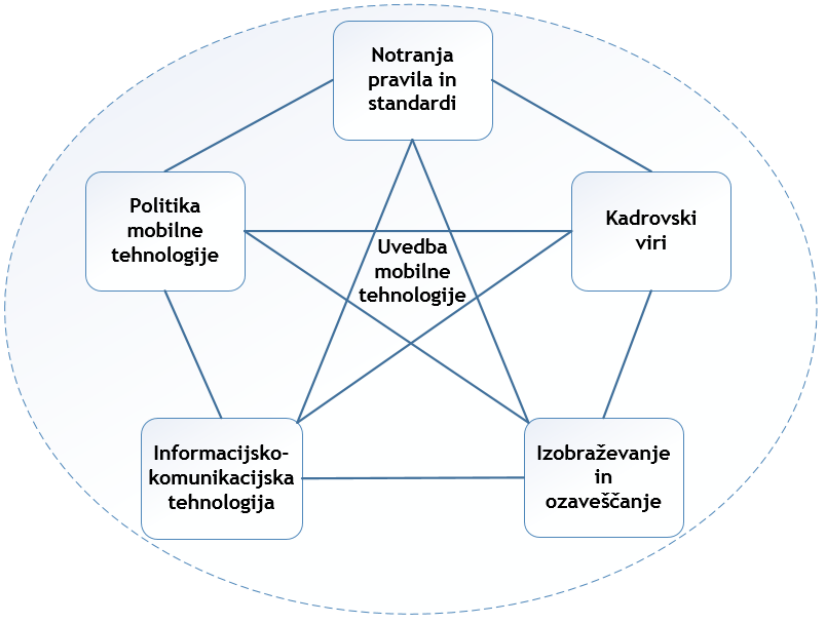
Program usposabljanja zaposlenih na področju uporabe mobilne tehnologije je ključnega pomena. Uporabniki bi morali pred uporabo mobilnih naprav z dostopom do zalednih sistemov organizacije biti obveščeni o njihovih pričakovanjih, saj le dobro usposobljen in ozaveščen zaposleni lahko izpolni pričakovanja glede odgovorne uporabe mobilne naprave. Cilj usposabljanja je ozaveščen uporabnik, ki premišljeno in odgovorno uporablja mobilno napravo in varno dostopa v internetni prostor brez strahu pred zlorabo. Prizadevanja za ozaveščanje so predvsem namenjena preprostemu osnovnemu spoznavanju mobilne tehnologije, spremembi vedenja in okrepitev dobrih varnostnih praks.

Zaposlenim program usposabljanja zagotavlja pridobivanje ključnih informacij o pravilih uporabe ter tehničnih lastnostih mobilne tehnologije, varnostnih grožnjah in razpoložljivi pomoči pri uporabi. S pridobljenimi informacijami bodo zaposleni tako lahko izpolnili odgovornosti za varno uporabo mobilne naprave.

Ravnanje v skladu s pravili uporabe sistema in obdobno usposabljanja za obnovitev znanja in pridobitev novih informacij, je pogoj za nadaljnjo uporabo mobilne naprave in dostop do mobilnih storitev.

5.4. INTEGRACIJA ELEMENTOV

Učinkovita in varna uvedba mobilne tehnologije temelji na medsebojni povezanosti ključnih elementov, ki so prikazani na sliki 15. Povezanost elementov ima namen ponuditi kakovostne mobilne storitve, ki zadovoljijo potrebe in pričakovanja zaposlenih, hkrati pa dosegati poslovne in varnostne zahteve organizacije.



Slika 15: Povezava elementov pri uvedbi mobilne tehnologije (Vir: ZZZS)

Postopki vključitve zaposlenega v sistem uporabe mobilne tehnologije, so sestavljeni iz posameznih korakov in odločitev. Organizacija s pomočjo tehnoloških rešitev, notranjih predpisov, standardov, politikami ter internimi človeškimi viri, zagotovijo učinkovito in enotno uvajanje mobilne tehnologije. Postopki vključujejo obstoječe tehnološke rešitve, ki zagotavljajo čim bolj avtomatiziran način izvajanja posameznih postopkov.

Za potrebe anketiranja zaposlenih sem pripravil spletno anketo. Anketa je bila razposlana vsem zaposlenim v organizaciji, ki imajo zadolžene pametne mobilne naprave in jih uporabljajo za dostop do zalednega IS.

V spletni anketi so bili zaposleni vprašani glede zadovoljstva pri uporabi naprav in programske opreme na mobilnih napravah, zavedanju glede varnosti pri uporabi pametnih mobilnih naprav ter zasebnosti pri uporabi mobilne tehnologije, interneta in programskih rešitev.

Zadovoljstvo uporabnikov sem preveril v povezavi z zadolženo mobilno napravo:

- Tehničnih značilnosti narave (velikost zaslona, hitrost izvajanja, povezljivost, vgrajena kamera, avtonomija);
- Nameščena programska oprema, možnosti za nadgradnjo in nameščanje nove programske opreme.

V anketi so bili zaposleni vprašani, tudi glede postopkov zadolžitve mobilne naprave, usposabljanja in vgrajenih funkcionalnosti mobilne naprave ter postopkov prenosa podatkov pri zamenjavi mobilne naprave.

Z vedno večjo razširjenostjo pametnih mobilnih naprav in dejstvom, da se uporabniki ne zavedajo nevarnosti, ki prežijo z uporabo le teh, bom preveril, kako upoštevajo navodila in priporočila varne uporabe pametnih mobilnih naprav.

Z analizo pridobljenih podatkov sem pripravil predloge za izboljšave na področju zadovoljstva uporabnikov pri uporabi mobilne tehnologije, zmanjševanju varnostnih incidentov in obvladovanju zaupnosti podatkov pri upravljanju z nadzornimi sistemi.

6. PREIZKUS IN EVALVACIJA RAZVITEGA MODELA

Za potrebe raziskave zadovoljstva zaposlenih z upravljanjem mobilne tehnologije je bila izvedena spletna anketa.

Anketa je bila posredovana 102 zaposlenim v Zavodu, ki imajo službeno napravo in hkrati uporabljajo tudi možnosti oddaljenega dostopa do zalednega IS. Popolno oddanih je bilo 59 anket, 8 anket pa je bilo nepopolno izpolnjenih.

Podatki v tabeli 1 prikazujejo vrste in način uporabe mobilnih naprav. Velika večina uporabnikov uporablja mobilne naprave v službene in privatne namene. Iz ankete je bilo ugotovljeno, da so uporabniki, ki nimajo službenih tabličnih računalnikov le te kupili sami.

Vrste in način uporabe mobilne naprave	Službena uporaba (N)	Privatna uporaba (N)
Pametni mobilni telefon	59	50
Tablični računalnik	27	33

Tabela 1: Vrste in način uporabe mobilne naprave

Način dostopa do interneta je prikazan v tabeli 2, kjer je razvidno, da 10 % uporabnikov ne uporablja mobilnega prenosa podatkov, ki je del naročnine.

Za upravljanje mobilne tehnologije je pomemben podatek, da 75 % uporabnikov uporablja javna brezžična omrežja. Javno objavljene odkrite grožnje in zlorabe mobilne tehnologije na internetu potrjujejo, da je potrebno pripraviti celovit načrt varnostnega utrjevanja mobilne naprave ter usposobiti in ozavestiti uporabnike o nevarnostih in grožnjah pri uporabi nezavarovanih javnih brezžičnih omrežjih. Ozaveščanje je toliko bolj pomembno za uporabnike, ki v 49 % gostujejo pri operaterjih v tujini.

Način dostopa do interneta	N	%
Mobilni prenos podatkov, ki je del naročnine	53	90
Mobilni prenos podatkov tujega operaterja na gostovanju v tujini	29	49
Brezžično službeno omrežje	54	92
Brezžično domače omrežje	56	95
Javna brezžična omrežja (hoteli, restavracije, knjižnice, odprta omrežja itd.)	44	75

Tabela 2: Način dostopa do interneta

Podatki o zadovoljstvu uporabnikov glede tehničnih značilnosti mobilne naprave ter nameščene programske opreme so predstavljeni v tabeli 3. Primerjava zadovoljstva med pametnim mobilnim telefonom in tabličnim računalnikom je pokazala, da so uporabniki bistveno bolje zadovoljni s tabličnim računalnikom. Nakup pametnih mobilnih naprav je odvisna od seznama, ki ga pripravi in sprotno osvežuje ponudnik mobilne telefonije za celotno državno upravo Republike Slovenije. Na tem seznamu ni zmogljivejših modelov pametnih mobilnih telefonov. Nezadovoljstvo s pametnim mobilnim telefonom se pokaže v povezavi s tehnološko opremo, ki zagotavlja hitrost delovanja (procesorska enota in velikost delovnega pomnilnika). Kapaciteta baterije glede na vgrajene elemente (mobilni signal 3G in LTE/4G, ločljivost in velikost zaslona) ni dovolj zmogljiva ter tako ne zagotavlja daljše avtonomije mobilnega telefona.

V Zavodu smo pred uvedbo mobilnih naprav Android imeli BlackBerry mobilne telefone, kateri so imeli Qwerty tipkovnico. Pisanje besedila s Qwerty tipkovnico je enostavneje in hitrejše kot v primerjavi z virtualno tipkovnico. Z Android virtualno tipkovnico na mobilnih napravah je 69 % zaposlenih zadovoljnih, 11 % zaposlenih ima še težave pri pisanju besedila ter 20 % je neopredeljenih. 93 % zaposlenih je mnenja, da pametni mobilni telefon vsebuje vse potrebne funkcije, ki jih uporabnik potrebuje za komuniciranje in delo na spletu. 22 % zaposlenih je izrazilo nezadovoljstvo z odzivnostjo pametnega mobilnega telefona, saj so modeli s povprečnimi tehničnimi karakteristikami.

1 - zelo nezadovoljen; 2 – nezadovoljen; 3 - niti zadovoljen niti nezadovoljen; 4 - zadovoljen; 5 - zelo zadovoljen

N(59)

Zadovoljstvo s svojim pametnim mobilnim telefonom	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Velikost zaslona	2	3	8	58	29
Zaslon za dotik	0	3	14	49	34
Virtualna tipkovnica	4	7	20	54	15
Hitrost delovanja	5	17	15	49	14
Kvaliteta vgrajenega fotoaparata	0	9	15	54	22
Teža aparata	0	3	10	70	17
Vsebuje vse potrebne funkcije	0	2	5	64	29
Avtonomija delovanja (baterija)	3	27	17	43	10
Zanesljivost delovanja pametnega mobilnega telefona (pogosta neodzivnost, samodejni ponovni zagon itd.)	3	14	31	42	10
Zmogljivost zagotavljanja mobilnega signala in Wifi signal	0	14	17	59	10

Tabela 3: Zadovoljstvo s svojim pametnim mobilnim telefonom

V tabeli 4 je prikazano zadovoljstvo zaposlenih pri uporabi s tabličnim računalnikom. Vsi zaposleni nimajo službenega tabličnega računalnika. Zaposleni, ki imajo tablični računalnik, pa so ocenili, da so s tehničnimi značilnostmi bolj

zadovoljni kot s pametnim mobilnim telefonom. Nezadovoljstvo pri tabličnem računalniku je bilo z vgrajenim fotoaparatom in težo naprave.

1 - zelo nezadovoljen; 2 – nezadovoljen; 3 - niti zadovoljen niti nezadovoljen; 4 - zadovoljen; 5 - zelo zadovoljen

N(27)

Zadovoljstvo s svojim tabličnim računalnikom	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Velikost zaslona	0	0	4	44	52
Zaslon za dotik	0	0	4	48	48
Virtualna tipkovnica	0	0	4	55	41
Hitrost delovanja	0	4	11	59	26
Kvaliteta vgrajenega fotoaparata	4	4	22	48	22
Teža aparata	4	4	7	59	26
Vsebuje vse potrebne funkcije	0	0	15	55	30
Avtonomija delovanja (baterija)	0	4	11	48	37
Zanesljivost delovanja tabličnega računalnika	0	4	15	44	37

Tabela 4: Zadovoljstvo s svojim tabličnim računalnikom

V tabeli 5 so podatki o zadovoljstvu zaposlenih s prednameščeno programsko opremo, ki jo namesti proizvajalec pametne mobilne naprave, ponudnik mobilne telefonije ter Zavod za potrebe oddaljenega upravljanja mobilne naprave. Z naborom, uporabnostjo in zanesljivostjo prednameščene programske opreme so zaposleni zadovoljni. S priporočenim naborom dodatne programske opreme na portalu za mobilno tehnologijo Zavoda pa je 60 % zaposlenih zadovoljnih.

1 - zelo nezadovoljen; 2 – nezadovoljen; 3 - niti zadovoljen niti nezadovoljen; 4 - zadovoljen; 5 - zelo zadovoljen

N(59)

Programska oprema na službenem pametnem mobilnem telefonu	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Nabor nameščenih programov	0	3	15	65	17
Uporabnost nameščenih programov	0	2	20	61	17
Zanesljivost nameščenih programov	0	2	29	49	20
Izbira priporočenih programov na portalu organizacije	2	3	34	51	10
Izbira na Google Play portalu (spletna trgovina Google za Android naprave)	0	2	22	54	22
Splošno o uporabnosti programov za mobilne naprave	0	0	19	68	13
Prilagoditev mojim potrebam in željam	0	2	24	54	20

Tabela 5: Programska oprema na službenem pametnem mobilnem telefonu

Zadovoljstvo zaposlenih s prednameščeno programsko opremo na tabličnem računalniku je prikazano v tabeli 6. Okoli 75 % zaposlenih je zadovoljnih z naborom in uporabnostjo prednameščene programske opreme, 78 % pa jih meni, da le ta tudi zanesljivo deluje.

1 - zelo nezadovoljen; 2 – nezadovoljen; 3 - niti zadovoljen niti nezadovoljen; 4 - zadovoljen; 5 - zelo zadovoljen

N(28)

Programska oprema na službenem tabličnem računalniku	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Nabor nameščenih programov	0	0	25	46	29
Uporabnost nameščenih programov	0	0	25	46	29
Zanesljivost nameščenih programov	0	0	22	46	32

Tabela 6: Programska oprema na službenem tabličnem računalniku

V tabeli 7 so predstavljeni podatki o zadovoljstvu z upravljanjem mobilnih naprav v Zavodu. 76 % zaposlenih je zadovoljnih z varnostnimi nastavitvami in omejitvami, ki so privzeto nastavljene pri prevzemu mobilne naprave. S privzetimi nastavitvami mobilnih naprav je 73 % zaposlenih zadovoljnih, 81 % jih je zadovoljnih z ažurnostjo novih verzij programske opreme ter 76 % s samodejnimi nastavitvami, ki se izvajajo preko nadzornih orodij. Zaposleni so z nudenjem podpore pri uporabi mobilne naprave s strani službe za pomoč uporabnikom zadovoljni v 83 %.

S postopki zamenjave mobilne naprave, ki se izvaja v primeru tehnične okvare mobilne naprave ali pri zamenjavi z BlackBerry mobilnim telefonom, je zadovoljnih 61 % zaposlenih. 50 % zaposlenih je ocenilo z najmanjšo stopnjo zadovoljstva nabor podprtih modelov mobilnih naprav. To je posledica dejstva, da uporabnikom organizacija ne more ponuditi velike izbire različnih modelov mobilnih naprav, ki so trenutno na trgu, ampak zgolj modele, ki jih pripravi ponudnik mobilne telefonije za državno upravo Republike Slovenije.

1 - zelo nezadovoljen; 2 – nezadovoljen; 3 - niti zadovoljen niti nezadovoljen; 4 - zadovoljen; 5 - zelo zadovoljen

N(59)

Zadovoljstvo z upravljanjem mobilnih naprav s strani organizacije	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Varnostne nastavitve/omejitve funkcionalnosti mobilne naprave	0	5	19	57	19
Ažurnost novih verzij programov na mobilni napravi	0	2	17	64	17
Privzete nastavitve mobilne naprave	0	3	24	64	9
Samodejna nastavitev mobilnih naprav	0	5	19	66	10
Postopki zamenjave mobilne naprave	3	5	31	42	19
Nabor podprtih modelov in proizvajalcev mobilnih naprav	12	13	32	36	7
Podpora pri uporabi mobilnih naprav in programov	0	2	15	63	20

Tabela 7: Zadovoljstvo z upravljanjem mobilnih naprav s strani organizacije

V tabeli 8 so predstavljeni podatki o pridobivanju podatkov o varni rabi interneta in mobilnih naprav. Pridobivanje znanja o varni rabi interneta in mobilne tehnologije je 63 % zaposlenih samoiniciativno pridobilo na internetu, 73 % zaposlenih je potrdilo, da so bili o tem seznanjeni s strani službe za pomoč uporabnikov. Pred izvedbo postopka prevzema mobilne naprave ter vklopom storitev za dostop do zalednega IS, si mora zaposleni ogledati predstavitev o varni rabi interneta in mobilne tehnologije na internem portalu eUčenje. Ogled teh vsebin je potrdilo le 70 % zaposlenih.

N(59)

Seznanjenost o varni rabi interneta in mobilne naprave	N	%
Podatke sem pridobil na internetu	37	63
Pri prevzemu so me seznanili v Službi za pomoč uporabnikom	43	73
Ogledal sem si e-Gradivo »Mobilni dostop« na portalu eUčenje	41	70

Tabela 8: Seznanjenost o varni rabi interneta in mobilne naprave

V tabeli 9 so prikazani podatki o zadovoljstvu zaposlenih s pridobivanjem informacij in pomoči pri varni rabi mobilne naprave, ki jo pridobijo s strani službe za pomoč uporabnikov v organizaciji. Zaposleni so v 83 % zadovoljni s pridobljenimi podatki o varovanju mobilne naprave, v 75 % pa so zadovoljni z načini in priporočili glede podatkovnega prenosa. Pri obnovitvenih tečajih glede varne rabe mobilnih naprav in interneta 50 % zaposlenih meni, da niso pridobili zadostnih informacij. Zaposleni v 44 % menijo, da sprotno obveščanje o aktualnih nevarnostih pri uporabi mobilne naprave ni zadostno. Enaka stopnja nezadovoljstva (44 %) je tudi v primeru seznanitve s postopki v primeru zlorabe in odtujitve mobilne naprave.

1 - zelo nezadovoljen; 2 – nezadovoljen; 3 - niti zadovoljen niti nezadovoljen; 4 - zadovoljen; 5 - zelo zadovoljen

N(59)

Seznanjenost o varni rabi mobilne naprave s strani organizacije	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Varnostna priporočila glede varovanja mobilne naprave	0	2	15	66	17
Načini in priporočila podatkovnega prenosa	0	0	25	61	14
Obnovitveni tečaji o nevarnostih pri uporabi mobilne naprave	0	9	47	32	12
Obveščanje o aktualnih nevarnostih pri uporabi mobilnih naprav	0	5	39	44	12
Seznanitev s postopki v primeru zlorabe ali odtujitve mobilne naprave	0	3	41	44	12

Tabela 9: Seznanjenost o varni rabi mobilne naprave s strani organizacije

V tabeli 10 so prikazani podatki o načinu uporabe mobilne naprave v kontekstu varnosti s strani zaposlenega. Zaposleni le v 12 % uporabljajo namensko programsko opremo, ki zagotavlja, da na varen način shranijo občutljive podatke v šifrirani obliki ter s tem preprečijo nepooblaščen dostop v primeru zlorabe ali odtujitve mobilne naprave. Zaposleni so v 50 % ocenili, da svojo mobilno napravo ustrezno varujejo, v 12 % zaposleni dovoljujejo uporabo svoje mobilne naprave tudi svojim bližnjim. Vsebino mobilne naprave 39 % zaposlenih obdobno kopira na druge medije za potrebe zaščite podatkov v primeru okvare ali odtujitve. 2 % zaposlenih svoje podatke shranjuje nezavarovano. Pri uporabi storitev na internetu 5 % zaposlenih objavlja osebne slike na socialnih omrežjih, nihče ne objavlja svoje trenutne lokacije ali osebne podatke na spletu. Zaposleni v 39 % primerih uporabljajo trenutno lokacijo (GPS) v nameščeni programski opremi (Google, zemljevidi, fotoaparat itd.).

Ocenjujem, da zaposleni niso dovolj informirani o uporabi, delovanju in povezovanju funkcionalnosti trenutne lokacije GPS na mobilni napravi in nameščene programske opreme. Lastnik mobilne naprave zavestno ne objavlja svoje trenutno lokacije na npr.: na socialnih omrežjih, portalih, forumih, ampak to izvaja mobilna naprava z vklopljenim GPS v povezavi z nameščeno programsko opremo.

Z zbiranjem in posredovanjem trenutne lokacije s strani programske opreme, se strinja uporabnik sam pred namestitvijo le te na mobilno napravo. Postopek namestitve programske opreme namreč zahteva, da se uporabnik pred namestitvijo strinja z dovoljenji programske opreme za dostop do podatkov, storitev in funkcionalnosti na mobilni napravi. Zaposleni v 53 % pozorno preberejo zahtevana dovoljenja programske opreme, ki opredeljuje dostope do podatkov, storitev in funkcionalnosti na mobilni napravi.

V 7 % imajo zaposleni stalno vklopljeno Bluetooth povezavo, ki je varnostno tvegana, saj le ta omogoča nenadzorovano povezovanje z drugimi napravami v bližini. Varnostno tveganje za organizacijo predstavljajo tudi 3 % zaposlenih, ki nameščajo programsko opremo iz neznanih spletnih mest.

N(59)

Način uporabe uporaba mobilne naprave v kontekstu varnosti	N	%
Zaklepanje mobilne naprave (PIN, vzorec, geslo)	59	100,00
Uporabljam program za varno shranjevanje pomembnih podatkov (PIN kode bančnih kartic, št. potnega lista, gesla za dostop do spleta itd.)	7	11,86
Podatke o dostopu do mobilne naprave zaupam tudi drugim osebam	2	3,39
Obdobno varnostno kopiram podatke	23	38,98
Občutljive osebne podatke in multimedijske datoteke shranjujem nezavarovano	1	1,69
Dovoljujem uporabo svoje mobilne naprave drugi osebi (otrok, prijatelj, sodelavec)	7	11,86
Dovoljujem nameščanje zabavnih programov iz neznanih spletnih mest	2	3,39
Skrbno varujem mobilno napravo in je ne puščam brez nadzora	50	84,75
Imam vklopljen Bluetooth tudi, ko ga ne uporabljam	4	6,78
Redno posodabljam programe	43	72,88
Objavljam osebne slike na socialnih omrežjih	3	5,08
Objavljam trenutno lokacijo na socialnih omrežjih	0	0,00
Uporabljam trenutno lokacijo (GPS) v programih na mobilni napravi (Google, zemljevidi, fotoaparat itd.)	23	38,98
Objavljam osebne podatke na spletu	0	0,00
Pozorno preberem zahtevana dovoljenja novega programa za dostop do podatkov na mobilni napravi	31	52,54

Tabela 10: Način uporabe mobilne naprave v kontekstu varnosti

V tabeli 11 so prikazani podatki o mnenju zaposlenih o prednostih rabe mobilnih naprav. Iz podatkov je razvidno, da so zaposleni sprejeli mobilno tehnologijo in prepoznali njene prednosti pri vsakdanjih opravilih. Zaposleni se v 95 % strinjajo, da so mobilne naprave priročne in jim omogočijo ne glede na čas in lokacijo dostop do virov na internetu. 86 % zaposlenih se strinja, da mobilna tehnologija pripomore k vključenosti zaposlenega v poslovni proces in hkrati tudi omogoči hitrejše izvajanje delovnih nalog. 49 % zaposlenih se strinja, da se z mobilno

tehnologijo poenostavi dostop do virov in opravljenih storitev na internet-u, 51 % pa se strinja, da se jim s tem tudi izboljša kakovost in organiziranost njihovega življenja. Glede na priljubljenost in sprejetost mobilne tehnologije 51 % zaposlenih uporablja le to tudi za zabavo.

1 - sploh se ne strinjam; 2 – ne strinjam se; 3 - niti se strinjam, niti ne strinjam; 4 - strinjam se; 5 - v celoti se strinjam

N(59)

Prednosti rabe mobilnih naprav	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Vključenost v poslovni proces	2	2	10	47	39
Hitrejše izvajanje delovnih nalog	2	2	12	49	35
Dostop do virov na internetu (službeni podatki, vreme, promet, borza itd.) ne glede na čas in lokacijo	0	0	5	53	42
Zabava	5	8	36	37	14
Poenostavitev postopkov (nakup letalske karte, rezervacija hotela, navigacija, pisanje dokumentov itd.)	0	12	39	37	12
Izboljšuje kakovost mojega življenja	0	12	37	36	15
Večja organiziranost	0	4	25	47	24
Priročnost	0	0	5	54	41

Tabela 11: Prednosti rabe mobilnih naprav

V tabeli 12 so prikazani podatki o mnenju zaposlenih o slabostih uporabe mobilnih naprav. Slabost je bila prepoznana v manj zasebnosti pri 78 % in s tem povezana »stalna« dosegljivost pri 83 % zaposlenih. To pa povzroči pri 70 % zaposlenih večjo skrb ter posledično večjo obremenjenost. Z uporabo mobilne tehnologije 65 % zaposlenih vidi možnosti zlorabe pri vsakdanji uporabi mobilnih naprav na internetu, 54 % se strinja, da se zmanjša anonimnost uporabnika, saj vgrajene funkcionalnosti (GPS, Bluetooth, Wifi itd.) omogočajo sledenje uporabniku na poti, v službi, v trgovini itd.

Zasvojenosti in s tem povezano odtujenost zaradi mobilne tehnologije zaposleni ne vidijo kot težavo. Uradne raziskave o škodljivosti uporabe mobilne tehnologije še niso pokazale direktnega vpliva na zdravje človeka, zato je tudi mnenje o škodljivosti le pri 19 % zaposlenih in 47 % neopredeljenih. 61 % zaposlenih meni, da je uporaba mobilne tehnologije pri vožnji z motornimi vozili vzrok za zmanjšanje pozornosti.

1 - sploh se ne strinjam; 2 – ne strinjam se; 3 - niti se strinjam, niti ne strinjam; 4 - strinjam se; 5 - v celoti se strinjam

N(59)

Slabosti uporabe mobilnih naprav	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)
Manj zasebnosti	0	12	10	54	24
Vedno dosegljiv	2	5	10	56	27
Večja skrb zaradi obveznosti	2	8	20	53	17
Možne zlorabe	0	5	29	41	25
Ni anonimnosti	0	10	36	34	20
Zasvojenost	10	29	26	25	10
Škodljivo zdravju (sevanje, nepravilna drža, ipd.)	5	14	47	29	5
Odtujenost	5	25	32	29	9
Zmanjšana pozornost pri vožnji z motornim vozilom	2	17	20	34	27

Tabela 12: Slabosti uporabe mobilnih naprav

Demografski podatki anketirancev

V tabeli 13 je prikazano, da je največji odstotek zaposlenih, ki je odgovarjalo na anketo, zaposleno v področni enoti Informacijskega centra; teh je bilo 47 %, 31 % na območnih enotah in izpostavah ter 22 % na Direkciji.

N(59)

Lokacija zaposlitve	N	%
Območna enota in izpostava	18	31
Informacijski center	28	47
Direkcija	13	22

Tabela 13: Lokacija zaposlitve

V tabeli 14 je prikazana izobrazbena struktura anketiranih. Največji delež, 70 % anketiranih je z višjo ali univerzitetno izobrazbo, sledi jim magisterij in doktorat z 20 %. Najmanj je bilo anketirancev s srednješolsko izobrazbo 10 %.

N(59)

Stopnja izobrazbe	N	%
Srednja šola	6	10
Višja, univerzitetna izobrazba	41	70
Magisterij, doktorat	12	20

Tabela 14: Stopnja izobrazbe

V tabeli 15 je prikazan seznam programske opreme, ki je na internem portalu za mobilne naprave. Najpogosteje nameščena programska oprema z internega

portala je oprema, ki je namenjena oddaljenemu upravljanju mobilnih naprav in dostopu do elektronske pošte. Ostali programi so nameščeni v zelo majhnem številu.

N(140)

Naziv aplikacije	Število mobilnih naprav N	%
TeamViewer QuickSupport	103	73,57
IBM Verse	83	59,29
MobileIron	70	50,00
QuickSupport Add-On Samsung	68	48,57
Chrome	16	11,43
Web@Work	15	10,71
Enterprise Alert®	14	10,00
Secure Apps Manager	9	6,43
Access	7	5,00
Barcode Scanner+	4	2,86
Docs@Work	4	2,86
Firefox	4	2,86
IBM Connections	4	2,86
ThinkFree Office Viewer	4	2,86
Wifi Inspector	4	2,86
Heart Rate	3	2,14
WiFi File Explorer PRO	3	2,14
Canesten	2	1,43
Fing - Network Tools	2	1,43
Opera	2	1,43
Pedometer	2	1,43
QuickSupport Add-On HTC	2	1,43
Runtastic	2	1,43
TeamViewer Manager	2	1,43
AirDroid	1	0,71
AnyConnect	1	0,71
Headspace	1	0,71
Nutri Explorer	1	0,71
Smart Switch Mobile	1	0,71
Sworkit Lite	1	0,71
Veš kaj ješ	1	0,71

Tabela 15: Seznam programske opreme na internem portalu organizacije

Analiza pogostosti nameščene programske opreme na mobilnih napravah je v tabeli 16. Na mobilnih napravah je nameščeno 998 različnih programov. Tako veliko število je pričakovano glede na ponudbo, ki je na portalu pri proizvajalcu Android operacijskega sistema Google ter dejstvo, da politika nameščanja nove programske opreme v Zavodu ne omejuje nameščanja.

Pri razvrstitvi v razrede glede na množičnost pojava določene programske opreme na mobilni napravi je razvidno, da je število enkratno nameščenih programov zelo veliko.

N(998)

Število mobilnih naprav, ki imajo nameščen isti program	Število primerov programske opreme (N)	%
71 – 125	29	2,91
51 – 70	10	1,00
11- 50	41	4,11
2 -10	313	31,36
1	642	64,33

Tabela 16: Nameščena programska oprema na mobilnih napravah

V razredu z največ namestitvami programske opreme na mobilnih napravah je oprema, ki je prednameščena s strani proizvajalca mobilne naprave, mobilnega operaterja ter standardna programska oprema organizacije.

Raznolikost nameščene programske opreme je s stališča standardizacije ter s tem učinkovitega upravljanja, podpore uporabnikom ter zanesljivosti delovanja mobilnih naprav vprašljiva.

Pregled seznama programske opreme je pokazal, da je od 998 verzij, kar 170 oz. 17 % programske opreme take, ki ne obstaja na portalu Google Play. Če je bila ta programska oprema nameščena s portala Google Play, pomeni, da le ta ni posodobljena in zastarela. Obstajajo možna tveganja, da so v njih skrite varnostne ranljivosti ali pa nekompatibilnost z novejšo sistemsko programsko opremo mobilne naprave. Varnostno tveganje je lahko bistveno večje, če je bila programska oprema nameščena iz neznanih spletnih virov.

7. ZAKLJUČEK

S širjenjem pametnih mobilnih naprav in drugih prenosnih tehnologij postajata zasebnost in varnost vse bolj pomembni področji raziskovanja, upravljanja in omejevanja. Varnost se v tem predstavlja ne le kot nerešljiv izziv za mobilno tehnologijo, ampak tudi za celotno IT. Neprestano vznikajo nove varnostne grožnje in v kompleksnosti današnjih informacijskih sistemov prav tako tudi druge potencialne ranljivosti.

IT strokovnjaki imajo na voljo učinkovite tehnološke rešitve za reševanje varnostnih izzivov, vključno s šifriranjem podatkov, avtentikacijo in avtorizacijo ter upravljanjem mobilnih naprav. Z uporabo analitičnih orodij lahko zaznajo morebitne varnostne grožnje, še preden se le-te pojavijo. Stalna budnost organizacije je cena, ki jo morajo plačati za uspeh na varnostnem področju.

Organizacija mora pri celovitem upravljanju mobilne tehnologije gojiti kulturo zasebnosti dopolnjeno z obstoječo varnostno politiko. Opredeljene smernice obvladovanja zasebnosti, morajo biti zapisane v notranjih pravilih in aktih organizacije, ki se nanašajo na pravice zaposlenega povezanega z le-to.

Analiza varovanja zasebnosti v organizaciji je pokazala, da sprejemanje organizacijskih aktov in tehnoloških rešitev zagotavlja spoštovanje informacijske zasebnosti – torej omogoča posamezniku možnost zadržanja osebnih informacij ne da bi bili o njih seznanjeni drugi. Politika zasebnosti opredeljuje zbiranje informacij za potrebe upravljanja mobilne tehnologije in zagotavlja le nujno potreben nabor podatkov, ki pa so zaščiteni kot katerikoli drugi občutljivi podatki.

Zaposleni so z uporabo mobilnih naprav pri uporabi spletnih storitev v internetu izpostavljeni tudi kršenju zasebnosti. Vse večja vloga mobilne tehnologije ustvarja novo gospodarstvo, v katerem so zbrani podatki o navadah, dejavnosti in interesih ljudi. V vzponu so sodobne tehnološke rešitve za sledenje uporabnikom mobilne tehnologije, z namenom vseprisotnega nadzora dejavnosti uporabnika. Zbiranje podatkov se izvaja pod pretvezo učinkovitejšega delovanja mobilnih naprav ali programske opreme, brezplačne uporabe internetnih storitev ali nameščene programske opreme. Uporabniki interneta se morajo zavedati, da v dobi Facebooka, kjer vsi z vsemi delimo različne oblike (tudi osebnih) podatkov, ne moremo več govoriti o varstvu zasebnosti, saj gre namreč za preživete norme. Vsak posameznik sam odloča s kom bo delil svoje podatke. Z zbranimi in obdelanimi informacijami pa se pogosto trguje tudi brez vednosti uporabnika. Zbrani podatki o posamezniku omogočajo profiliranje, avtomatizirano odločanje, prilagajanje storitev in oglaševanja, kar predstavlja velik izziv za varstvo informacijske zasebnosti (Tomšič, 2014).

Obdobno izvajanje usposabljanja in sprotno obveščanje o novo odkritih nevarnostih pri uporabi mobilne tehnologije in interneta lahko bistveno zmanjša pojav zlorab, ki so povezane s kršenjem zasebnosti. V raziskavi se je ugotovilo (tabela 9), da so zaposlenim s trenutnim obveščanjem zadovoljni, vendar imajo večja pričakovanja glede obdobnih usposabljanj o uporabi mobilne tehnologije. V

raziskavi (tabela 8) se je pokazalo, da zaposleni tudi sami pridobivajo informacije o pravilni uporabi mobilne tehnologije in interneta. Raziskava o načinih uporabe mobilnih naprav v kontekstu varnosti (tabela 10) je pokazala, da uporabniki tudi v praksi upoštevajo priporočila o varni uporabi mobilnih naprav.

Raziskava zadovoljstva uporabe mobilne tehnologije na Zavodu je pokazala, da so s trenutnim modelom upravljanja mobilnih naprav zaposleni zadovoljni. To je rezultat sprotnega prilagajanja in sledenja uporabniškim zahtevam ter sodelovanje zaposlenih pri preizkušanju politike upravljanja mobilnih naprav. Trenutni model upravljanja zagotavlja uravnoteženo upravljanje, uporabnost in varnost mobilnih naprav v organizaciji.

Mobilna tehnologija lahko omogoča hiter in varen dostop do poslovnih podatkov v zalednem informacijskem sistemu organizacije ter enostaven dostop do virov informacij in storitev na internetu. Raziskava je pokazala, da je mobilnost uporabna in zelo priljubljena, saj zagotavlja zaposlenim večjo vključenost v poslovni proces in hitrejše izvajanje delovnih nalog, večjo organiziranost ter poenostavitev vsakodnevnih postopkov, kar posledično vodi v izboljšanje kakovosti njihovega življenja.

Predlog izboljšav

Izboljšave bodo usmerjenje v celovitejše usposabljanje uporabnikov na področju uporabe mobilne naprave, interneta in aplikacij. Uporabniki imajo vse večjo moč odločanja pri izbiri naprave, programske rešitve in oblačnih storitev v internetu. Komunikacija z uporabniki bo morala biti odkrita in obojestranska. Odgovorni v informacijskih centrih se morajo zavedati, da z odkrito komunikacijo in prilagajanjem uporabniškim potrebam privedejo mobilno tehnologijo na nivo, kjer rešitve niso zgolj varne, ampak tudi uporabne. V nasprotnem primeru lahko to privede do omejevanja ustvarjalnosti, storilnosti in na koncu do nevključenosti v poslovni proces zaposlenega. To pa ima za posledico bistveno višje stroške upravljanja mobilnih naprav.

Zaposleni lahko zaradi nezadovoljstva pri uporabi mobilne tehnologije, aktivno ne sodelujejo. Ustvarijo se pogoji za prikrito uporabo ne varne programske rešitve na mobilnih napravah kljub temu, da zaposleni kršijo varnostna pravila organizacije, kar privede do varnostnih incidentov.

Vzpostavitev in ohranjanje zadovoljivega nivoja varnosti in celovitosti IS, je posledično povzročena škoda do zasebnosti. Zavedanje potrebe po povečevanju individualne zaščite pri uporabi mobilne tehnologije, bo treba ustrezno opredeliti v internih aktih organizacije.

Portal za izmenjavo izkušenj bi pokrival področje mobilne tehnologije za zaposlene in bi bil usmerjen za zbiranje informacij o novostih in navodilih za uporabo pametnih mobilnih naprav, programskih rešitev, internetnih storitev, varnostnih groženj, priporočil za varno uporabo mobilne tehnologije in obvestil o tehničnih posegih in razpoložljivosti na mobilnih storitvah organizacije. Pripravljene vsebine bi bile prilagojene uporabnikom s splošnim znanjem kot tudi naprednim uporabnikom mobilne tehnologije.

Vsebine na portalu bi bile pripravljene in objavljene s strani skrbnikov posameznih področij mobilne tehnologije, službe za pomoč uporabnikov na osnovi zaznanih potreb uporabnikov ter seveda prispevki posameznih uporabnikov mobilne tehnologije, ki bi bili pripravljeni deliti svoje znanje in izkušnje z ostalimi zaposlenimi. Portal bi poleg objavljenih prispevkov, omogočal tudi komentiranje in ocenjevanje prispevkov ter možnost statističnega vpogleda v obiskanosti posameznih področij portala ali branosti prispevka.

Statistični podatki o obiskanosti portala, branosti prispevkov in komentarji obiskovalcev, bi skrbnikom internega »socialnega omrežja« pomagala pri pripravi novih prispevkov oz. novih področij na portalu. Zaposlene, ki prostovoljno soustvarjajo nove prispevke, pišejo konstruktivne kritike za izboljšanje vsebin in mobilne tehnologije se povabijo k aktivnemu sodelovanju pri pripravi novih prispevkov.

Integracija novih orodij v IS zahteva celovito obvladovanje in upravljanje varnostnih komponent, kar predstavlja velik izziv skrbnikom sistemov.

Dinamika nastajanja varnostnih groženj in odkrivanje ranljivosti vgrajenih rešitev, zahteva nenehne tehnične prilagoditve in izpopolnitve varnostnih sistemov ter usposabljanje skrbnikov sistemov. Za učinkovitejše odkrivanje varnostnih groženj ter pravočasno ravnanje ob zaznavi varnostno kritičnih dogodkov, se v procesu integracije dopolnijo z dvema dodanima elementoma: SIEM (*Security information and event management*) orodje in požarni zidovi nove generacije (NGFW - *Next-Generation Firewalls*).

Orodja SIEM omogočajo centralno zbiranje in združevanje podatkov o dogodkih, ki jih beležijo varnostne omrežne naprave in aplikacije v kontekstu uporabnika. S pridobljenimi podatki okolje v realnem času izvaja primerjave in korelacije med različnimi viri, varnostnimi incidenti ter primerljivimi primeri in aktivnosti iz preteklosti. V primeru zaznave varnostne grožnje omogoča avtomatizirano opozarjanje po elektronski pošti ali namizju SIEM orodja.

Požarni zidovi nove generacije združujejo funkcije tradicionalne požarne pregrade, preprečevanje vdorov v IS (IPS - *Intrusion Prevention Systems*), prepoznavanje in podroben nadzor aplikacij glede na varnostno politiko organizacije, dešifriranje protokolov SSL (*Secure Sockets Layer*), prepoznavo uporabnikov ter na osnovi varnostne politike dodeljevanje pooblastil za uporabo mrežnih storitev.

V sistemu za upravljanje mobilnih naprav se omogočijo funkcionalnosti za zaznavanje napačnih sistemskih nastavitev mobilne naprave, zaznavanje ranljivosti na nivoju sistemske programske opreme mobilne naprave, upravljanje službene vsebine na mobilni napravi z izoliranjem in šifriranjem ter zagotavljanje zaščite na mobilni napravi proti grožnjam z zlonamerno programsko opremo.
Zasebnost podatkov na mobilni napravi zaposlenega se z nepravilnim in nenamenskim upravljanjem mobilne naprave lahko krši. Predvideti je potrebno celovit sistem nastavitev, ki onemogoča zbiranje ali pogledovanje podatkov na napravi, ki so potrebni za zagotavljanje učinkovitega upravljanja mobilne naprave. Spremljanje vsebine mobilne naprave, ki predstavljajo osebne zaupne podatke, kot so npr.: lokacija mobilne naprave, spremljanje poslanih in prejetih

SMS in MMS sporočil, nameščena programska oprema, osebni imenik, shranjene slike in podobno, je treba omejiti na minimalno možno raven. Za spremljanje nekaterih zgoraj naštetih podatkov mora organizacija imeti ustrezno podlago, ki daje osnovo za centralno pridobivanje in shranjevanje zasebnih podatkov.

Samopostrežne storitve za mobilne naprave v internem omrežju omogočajo uporabnikom namestitev preverjenih programskih rešitev, ki uporabnikom zagotavljajo varno, zanesljivo in učinkovito uporabo svoje naprave.

Dopolnitve organizacijskih elementov niso potrebne, saj trenutna organizacijska struktura za potrebe mobilne tehnologije že ustreza vsem zahtevam za učinkovito, varno in gospodarno upravljanje mobilnih tehnologij.

LITERATURA

Bernik, I., Prislan, K. (2012). Upravljanje varnostnih tvegan pri rabi mobilnih naprav, Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, 2012.

Boehm, B. (1986). A Spiral Model of Software Development and Enhancement. TRW Defense System Group. Dostopno na spletnem naslovu: <http://csse.usc.edu/csse/TECHRPTS/1988/usccse88-500/usccse88-500.pdf>. (1.9.2015).

Burback, R. (1998). Software engineering methodology: The watersluice, disertacija, Stanford University. Dostopno na spletnem naslovu: <*http://infolab.stanford.edu/~burback/watersluice/watersluice.pdf*>. (1.9.2015).

Charest, M. K. (2013). Factors affecting user behavior and conformance to information security practices are end users really the problem?, Capella University.

Clapsad, M. (2012). Standardizing the security of mobile app store platforms, Capstone Project, Faculty of Utica College.

Cotman, G. (2003). Informacijski sistem podjetja Dnevnik d.d., diplomsko delo, Univerza v Ljubljani, Ekonomska fakulteta.

Drev, M. (2010). Množični nadzor v sodobni družbi, magistrsko delo, Univerza v Ljubljani, Fakulteta za družbene vede.

Dutta, A. (2010). Systems Optimization for Mobility Management, Columbia University.

Frangež, E. (2013). Vpliv mobilnih aplikacij na elektronsko poslovanje, magistrsko delo, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko.

Gens, F. (2013). IDC Predictions 2014: Battles for Dominance — and Survival — on the 3rd Platform, IDC.

Gerbič, J. (2007). Predlog prenove uporabniške rešitve za sklepanje avtomobilskih zavarovanj na Zavarovalnici Triglav, d.d., diplomsko delo, Univerza v Mariboru, Fakulteta za organizacijske vede.

Goltez, P. M., Kovačič, A. (2005). Testiranje informacijskega sistema v različnih razvojnih fazah, magistrsko delo, Univerza v Ljubljani, Ekonomska fakulteta, Ljubljana.

Grajfoner, P. (2013). Spletno igralništvo, diplomsko delo. Univerza v Mariboru, EPF, Maribor.

Jansen, W., Gavrilla, S., Séveillac, C., Heute, T., Korolev, V. (2004). A unified framework for mobile device security. Dostopno na spletnem naslovu: <http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-UNIsecFramework-fin.pdf>. (1.9.2015).

Jansen, W., Scarfone, K. (2008). Guidelines on cell phone and PDA security recommendations of the National Institute of Standards and Technology (NIST SP800–124). Dostopno na spletnem naslovu: <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>. (1.9.2015).

Kapus, Ž. (2013). Digitalna potrdila in njihova uporaba v ZZZS, diplomsko delo, Univerza v Mariboru, Ekonomsko-poslovna fakulteta.

Kelley, P. G. (2013). Designing Privacy Notices Supporting User Understanding and Control, dizertacija, School of Computer Science, Carnegie Mellon University.

Klemenčič, G. (2001). Varstvo elektronske zasebnosti. Internet in pravo, Ljubljana: Pasadena.

Kovačič, M. (2003). Zasebnost na internetu, Mirovni inštitut, Inštitut za sodobne in družbene študije.

Kovačič, M. (2006). Nadzor in zasebnost v informacijski družbi: Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu. Univerza v Ljubljani, Fakulteta za družbene vede.

Leach, J. (2003). Improving user security behaviour, John Leach Information Security Ltd.

Liu, L., Moulic, R., Shea, D. (2010). Cloud service portal for mobile device management. In Proceedings of the 2010 IEEE Seventh International Conference on E-Business Engineering, str. 474–478.

Majchrzak T. A., Heitkötter H. (2013). Development of Mobile Applications in Regional Companies - Status Quo and Best Practices, WEBIST 2013, str. 341 – 346.

Majdi, E. B. (2013). Evolution of mobile device management tools and analysing integration models for mobility enterprise, Umeå University, Department of Computing Science, Jan 2013, str. 20.

Markelj, B. (2014). Grožnje informacijski varnosti pri rabi mobilnih naprav, dizertacija, Univerza v Mariboru, Fakulteta za varnostne vede.

Mont, M.C., Brown, R. (2011). Risk assessment and decision support for security policies and related enterprise operational processes, HP Laboratories, HP-2011-12.

Lobnikar, B., Prislan K., Markelj B., Banutai E. (2012). Informacijskovarnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji, Varstvoslovje, let. 14, št.3, str. 345-363.

Mirkovic, J. (2013). Usability, Security, and Mobility for Mobile Devices in Healthcare Information Systems, Faculty of Mathematics and Natural Sciences, University of Oslo.

Moškon, S. (2010). Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji, Uporabna informatika, let. 18, št. 2, str. 106-108.

Mayer-Schönberger, Viktor. (2001). Generational Development of Data Protection in Europe. V Agre E. P. in Rotenberg M., (ur.). 2001. Technology and Privacy: The New Landscape, str. 219–241. Cambridge, Massachusetts, London, England:MIT Press.

Nussdorfer M., (2009). Uvajanje elektronskih listin obveznega zdravstvenega zavarovanja, Univerza v Ljubljani, Ekonomska fakulteta.

Orehar-Ivanc, M. (2002): »35. člen (varstvo pravic zasebnosti in osebnostnih pravic)«. V Šturm, Lovro (ur.). 2002. Komentar ustave republike Slovenije, str. 370-386. Ljubljana: Fakulteta za podiplomske državne in evropske študije.

Pestotnik, A. (2007). Zasebnost in mobilni telefoni, diplomsko delo, Fakulteta za družbene vede.

Pratt, E. D., Jones, B. K., (2013). Mobile device management in the DoD enterprise network factors for risk management, integration, and it acquisition, Naval postgraduate school, Monterey.

Rupnik, R. (2003). Modeli uporabe mobilnih aplikacij v državni upravi, INDO 2003.

Rose, C. (2012). Smart phone, dumb security. Review of Business, 16(1), str.21–26.

Schadler, T. (2013). Mobile Workforce Adoption Trends, Forrester, feb. 2013.

Tomšič, A. (2014). Varstvo osebnih podatkov v dobi podatkovnega izobilja, V Smartdoc (str. 13-24), Ljubljana: Media.doc.

Vehovar, V. (2007). Mobilne refleksije, Knjižna zbirka Družboslovna informatika, Informacijska družba, Fakulteta za družbene vede.

Viega, J., Michael, B. (2010). Mobile device security. IEEE Security & Privacy

Vukelič, B. (2007). Zasebnost na delovnem mestu, diplomsko delo, Fakulteta za družbene vede.

Zabukovec, P. (2008). Vzpostavitev službe za podporo uporabnikom, Univerza v Mariboru, Fakulteta za organizacijske vede.

Poročila, interni dokumenti:

Gartner, (2014). Magic Quadrant for Enterprise Mobility Management Suites, (3.6.2014).

MobileIron, (2013). MobileIron VSP Administration Guide, ver. 5.6.

MobileIron, (2013). Getting Started with Mobile@Work for Android, ver. 5.6.

ZZZS, (2015). Poslovno poročilo za leto 2014.

Gradiva predavanj:

Ljudmila, Mehanizmi varovanja zasebnosti v informacijski družbi, Izpitna naloga pri predmetu sociologija informacijskih procesov, Dostopno na spletnem naslovu: <http://www.ljudmila.org/matej/zasebnost/zasebnost.html>. (1.9.2015).

Vir:

Enuis, (2013). Model Uporabe Mobilnih Apl., Dostopno na spletnem naslovu: <http://www2.gov.si/mju/emris.nsf/0/848EFA07C2377926C1256ED600758BEA> . (1.9.2015).

Enterprise mobility: Enabling Productivity without Sacrificing Protection, Dostopno na spletnem naslovu: <https://www.symantec.com/content/en/us/enterprise/brochures/b-enterprise-mobility-enabling-productivity.en-us.pdf>. (1.9.2015).

Havliček M., E-pošta in zasebnost na delovnem mestu, Dostopno na spletnem naslovu: <http://eudace.eu/knjiznica/clanki/2013021410315019/>. (1.9.2015).

InfoSRC, Mobilnost je prihodost (2012), Dostopno na spletnem naslovu: <https://infosrc.wordpress.com/2012/06/13/mobilno-je-prihodnost/>. (1.9.2015).

InfoSRC, Mobilno je lahko nenevarno (2013), Dostopno na spletnem naslovu: <https://infosrc.wordpress.com/2013/10/10/mobilno-je-lahko-nenevarno/>. (1.9.2015).

Hanni M. Fakhoury. (2012). Technology and Privacy Can Co-Exist., Dostopno na spletnem naslovu: <http://www.nytimes.com/roomfordebate/2012/12/11/privacy-and-the-apps-you-download/privacy-and-technology-can-and-should-co-exist>. (1.9.2015).

Kovačič M., Zasebnost in hramba prometnih podatkov v mobilni telefoniji, Dostopno na spletnem naslovu: <http://uploadi.www.ris.org/editor/1224355967kovacicZasebnostinhrambaprometnih.PDF>. (1.9.2015).

Osterman Research: Key Issues to Consider in Mobile Device Management, An Osterman Research White Paper, May 2011, Dostopno na spletnem naslovu: <http://www.smarsh.com/whitepapers/key-issues-to-consider-in-mobile-device-management/>. (1.9.2015).

RIS, (2008). Zasebnost in varnost, Dostopno na spletnem naslovu: <http://www.ris.org/db/26/12030/Novice/EU_sledenje_s_piskotki_samo_ob_soglasju_uporabnika/?&cat=707&p1=276&p2=285&p3=1318&p4=1335&p5=0&id=1335&cat=707>. (1.9.2015).

IP-RS, Smernice za varstvo osebnih podatkov v delovnih razmerjih, Dostopno na spletnem naslovu: <https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_varstvo_osebnih_podatkov_v_delovnih_razmerjih.pdf>. (1.9.2015).

IP-RS (2015). Zasebnost na delovnem mestu, Dostopno na spletnem naslovu: <https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf>. (1.9.2015).

Schulman, A. (2001). The Extent of Systematic Monitoring of Employee E-mail and Internet Use, Dostopno na spletnem naslovu: <>. (1. 9. 2015).

Pravni viri:

Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1), Stran 12707. (Uradni list RS, št. 94/2007), Dostopno na spletnem naslovu: <https://www.uradni-list.si/1/content?id=82668>.

IP-RS, (2015). Odločba, Dostopno na spletnem naslovu: <https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=2530&cHash=86d88f25676aaed5632fe21e0a5a1acb>. (1.9.2015).

KAZALO SLIK

KAZALO TABEL

POJMOVNIK

ActiveSync: Microsoft programska oprema za sinhronizacijo elektronske pošte, koledarja, stikov in ostali podatkov med strežnikom in mobilno napravo.
Bluetooth: Varna brezžična tehnologija za povezovanje različnih digitalnih elektronskih naprav.
Cyberslacking: Zaposleni, ki z iskanjem iger ali drugimi dejanji na internetu, ki niso povezane s službenim delom in se s tem izogiba delu ali drugim službenim obveznostim.
Jailbreaking: Poseg v mobilno napravo z Apple sistemsko programsko opremo, ki omogoča zaobiti omejitve pri namestitvi in uporabi neavtorizirane programske opreme s strani proizvajalca.
Proxy: Posredniški strežnik.
Rooting: Proces, ki uporabnikom mobilnih naprav z Android operacijskim sistemom omogoča privilegiran nadzor naprave.
Spam: Neželena elektronska pošta.
Spyware: Vohunski programi.
Web bugs: Spletni hrošči.
Wifi: Brezžična tehnologija, ki omogoča, da se lahko naprava poveže v računalniško omrežje.

KRATICE IN AKRONIMI

2G: druga generacija mobilnih omrežij oziroma tehnologija GSM
3G: tretja generacija mobilnih omrežij oziroma tehnologija UMTS
4G: četrta generacija mobilnih omrežij oziroma tehnologijo LTE
API: Application programming interface
BYOD: Bring your own device
BYOP: Bring your own phone
BYOPC: Bring your own PC
BYOT: Bring your own technology,
DMAIC: Define, Measure, Analayse, Improve, Control
DMZ: Demilitarizirano območje
EKČP: Evropska konvencija o varstvu človekovih pravic
FTC: Federal Trade Commission
FURS: Finančna uprava Republike Slovenije
GPS: Global Positioning System
HTC: Tajski proizvajalec pametnih telefonov in tablic
IP-RS: Informacijski pooblaščenec Republike Slovenije
IPS: Intrusion Prevention Systems
IT: Informacijska tehnologija
KZZ: Kartica zdravstvenega zavarovanja
LDAP: Lightweight Directory Access Protocol
LTE: Long Term Evolution
MAGIC: Mobile Anytime Globally Integrated Customized
MDM: Mobile Data Management
MMS: Multimedia Messaging Service
NFC: Near Field Communication
NGFW: Next-Generation Firewalls
OE: Območna enota

OS:	Operacijski sistem
P2P:	Peer-to-peer
PIN:	Personal Identification Number
PK:	Profesionalna kartica
PUK:	Personal Unlock Key
RS:	Republika Slovenija
SIEM:	Security information and event management
SMS:	Short Message Service
SSL:	Secure Sockets Layer
UMTS:	Universal Mobile Telecommunications System
URL:	Uniform Resource Locator
USB:	Universal Serial Bus
VPN:	Virtualno privatno omrežje
VSP:	Virtual Smartphone
Wifi:	Wireless internet for Frequent Interface
ZDA:	Združene države Amerike
ZDR:	Zakon o delovnih razmerjih
ZeKOM:	Zakon o elektronskih komunikacijah
ZPIZ:	Zavod za pokojninsko in invalidsko zavarovanje
ZVOP:	Zakon o varstvu osebnih podatkov