Celovit pristop obvladovanja mobilnih naprav

Tadej Prešeren
Krka, d. d., Novo mesto
tadej.preseren@krka.biz

Marko Bajec
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
marko.bajec@fri.uni-lj.si

Izvleček

Namen članka je predstaviti smernice, ki jih je smiselno upoštevati pri vzpostavljanju sistema obvladovanja mobilnih naprav. V članku so predstavljena izhodišča, kako se lotiti upravljanja mobilnih naprav, saj se to področje v zadnjem času izredno hitro razvija. Članek zajema vse ključne korake, ki jih je treba upoštevati. Izdelan je bil pregled standardov ter priporočil na področju varnosti na mobilnih napravah. Podane so smernice, ki jih je smiselno upoštevati pri izdelavi varnostne politike, izdelana pa je tudi analiza tveganj za farmacevtsko podjetje. Podrobno je predstavljen model za upravljanje mobilnih naprav.

Abstract

AN APPROACH TO MANAGEMENT OF MOBILE DEVICES

The field of mobile device management is developing very fast. The purpose of this article is to introduce all key directives that should be considered when implementing mobile device management. A survey of standards and recommendations on the mobile device security has been elaborated. Relevant guidelines for security policy definition are presented with the risk analysis for mobile device usage. Furthermore, the models for managing mobile devices and tool analysis are explained in detail.

1 UVOD

Vloga sodobne informacijske tehnologije (v nadaljevanju IT) se je od omejene uporabe osnovne IT razvila do razširjene in za poslovanje podjetja pomembne infrastrukture. Investicije v tako infrastrukturo so preveč pomembne, še posebno glede vpliva te infrastrukture na poslovanje in stroške ter tveganja napačnih odločitev, da bi jih prepustili svojemu toku [1]. Do tega pojava je prišlo zaradi dejstva, da so sredstva IT za današnje uspešno poslovanje tako pomembna in draga, da jih je treba upravljati, vzdrževati ter nadzorovati. Podjetja, ki se zavedajo pomembnosti kakovostnega upravljanja sredstev IT, vedo, da ta sredstva predstavljajo temelj za realizacijo poslovne strategije organizacije. Prav tako se zavedajo, da brez učinkovite infrastrukture z visoko razpoložljivostjo ter stalnim zagotavljanjem ustrezne ravni storitev danes ni moč uspešno poslovati.

Pogosto zasledimo, da je področje mobilnih naprav v podjetjih neurejeno. V podjetju, ki ga obravnavamo v prispevku, je v uporabi prek tisoč pametnih mobilnih naprav (npr. pametni mobilni telefoni, dlančniki, zmogljivejši mobilni telefoni ipd.), število pa strmo narašča.

Mobilne naprave delujejo na različnih platformah in zagotavljajo različne funkcionalnosti. V obravnavanem farmacevtskem podjetju je na mobilnih napravah trenutno zagotavljena le storitev elektronske pošte, vendar je lahko kljub temu na mobilnih napravah velika količina zaupnih ali strogo zaupnih podatkov.

Področja obvladovanja mobilnih naprav ter procesa upravljanja konfiguracij na mobilnih napravah trenutno ni mogoče izvajati, pojavljajo se težave predvsem pri uvajanju novih storitev, ker je treba vpoklicati v storitveni center (angl. Service Desk) vse mobilne naprave, na katerih bi želeli uporabljati novo storitev. To zahteva velike stroške, nered, nezadovoljstvo uporabnikov, slabo fleksibilnost, nizko odzivnost, ni poročil ter statistik o uporabi ter težavah na mobilnih napravah. V podjetju tudi ni celovitega sistema za varovanje in zaščito informacij v primeru izgube ali kraje mobilne naprave, ki bi ga potrebovali.

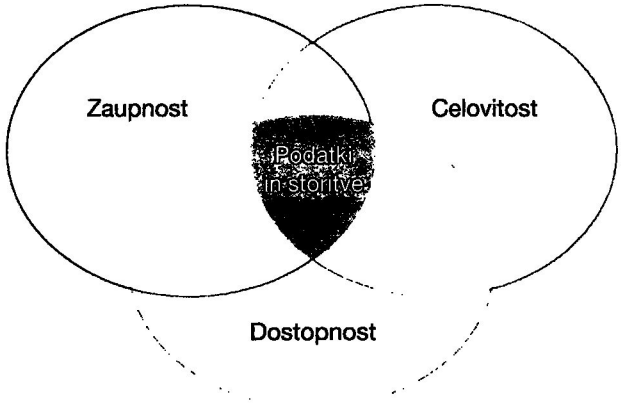
Tako mobilne naprave kot tudi njihovo obvladovanje je novo področje v znanosti, ki se intenzivno

razvija v zadnjih dveh desetletjih. Problem obvladovanja večjega števila mobilnih naprav je zanimiv ne samo v farmacevtskem podjetju, temveč v vseh združbah, v katerih jih uporabljajo. Še večji poudarek je pri organizacijah, ki na mobilnih napravah zagotavljajo storitve, povezane z dejavnostjo podjetja (npr. elektronska pošta, mobilne aplikacije – CRM idr.), in imajo informacije na mobilnih napravah še večjo vrednost.

2 INFORMACIJSKA VARNOST NA MOBILNIH NAPRAVAH

Informacijska varnost je področje, ki se ukvarja z varovanjem podatkov pred nepooblaščenim dostopom, uporabo, razkritjem, uničenjem, spremembo ali razpoložljivostjo. Termini informacijska varnost, računalniška varnost ter varnost informacijskih sistemov (angl. Information assurance) se pogosto uporabljajo izmenično. Čeprav vsa tri področja delijo mnoge skupne lastnosti oz. imajo vsa skupen cilj v varovanju zaupnosti, celovitosti ter razpoložljivosti informacij, obstajajo med njimi razlike glede vidika, s katerega pristopajo k tem ciljem in načinov zagotavljanja le-teh.

Definicija varnosti po ISO 17799:2005 se glasi [2]: Informacijska varnost zagotavlja ohranitev zaupnosti, celovitosti in razpoložljivosti informacij; dodatno so lahko vpletene tudi druge lastnosti, kot so istovetnost, odgovornost, preprečevanja nepriznavanja in zanesljivost.



Slika 1: **Trije glavni cilji informacijske varnosti [3]**

Varnost informacijskih sistemov pristopa nekoliko drugače, tako da upošteva predvsem varovanje sistemov, ki omogočajo hrambo, procesiranje, predstavitev ali prenos informacij. Dodatno daje poudarek zasebnosti, upoštevanju zakonskih in drugih določil, neprekinjenemu poslovanju ter okrevanju po katastrofi. Računalniška varnost se osredinja na zagotavljanje varne uporabe računalnikov. Osnovni pristop je izdelava računalniških platform, jezikov in programov z vgrajenimi omejitvami, tako da agenti lahko izvedejo le določene akcije. Danes pa vse bolj uveljavlja varnost mobilnih naprav.

2.1 COBIT in varnost mobilnih naprav

V delovnem okviru COBIT področje mobilnih naprav ni obravnavano eksplicitno. Podani so splošni kontrolni cilji. Ker se v nalogi v prvi vrsti osredinjamo na varnost mobilnih naprav, bomo v nadaljevanju podrobneje predstavili proces DS5, ki se ukvarja s kontrolnimi cilji, povezanimi z informacijsko varnostjo.

Sama informacijska varnost je prek kontrolnih ciljev zajeta v posameznih procesih, proces DS5 – zagotovitev varnosti sistemov (angl. Ensure Systems Security) pa varnost obravnava v celoti.

Proces DS5 je sestavljen iz naslednjih področij:

- DS5.1 – upravljanje varnosti sistemov (angl. Management of IT Security),
- DS5.2 – načrt varovanja IT (angl. IT Security Plan),
- DS5.3 – upravljanje identitete (angl. Identity Management),
- DS5.4 – upravljanje uporabniškega računa (angl. User Account Management),
- DS5.5 – testiranje, nadzor in spremljanja varovanja (angl. Security Testing, Surveilliance and Monitoring),
- DS5.6 – opredelitev varnostnega incidenta (angl. Security Incident Definition),
- DS5.7 – zaščita varnostne tehnologije (angl. Protection of Security Technology),
- DS5.8 – upravljanje kriptografskih ključev (angl. Cryptographic Key Management),
- DS5.9 – preprečevanje in odkrivanje zlonamernih programov in popravljanje (angl. Malicious Software Prevention, Detection and Correction),
- DS5.10 – omrežna varnost (angl. Network Security),
- DS5.11 – izmenjava občutljivih podatkov (angl. Exchange of Sensitive Data).

Ker je vsako področje zelo obširno in je tesno povezano z mobilnimi napravami, je za vsako podan predlog, kaj storiti v primeru mobilnih naprav. Pri vseh predlogih izhajamo iz predpostavke, da je v

organizaciji že vzpostavljen sistem varovanja informacij, da so izdelane varnostne politike itn.

V upravljanje informacijske varnosti je treba vključiti tudi mobilne naprave. V večini primerov se na mobilne naprave pozabi ter jih ne obravnavamo glede na njihove funkcionalnosti in podatke, ki jih lahko vsebujejo.

V krovni varnostni politiki je treba pokriti tudi področje mobilnih naprav ter ga podrobneje definirati z varnostno politiko.

Zagotoviti je treba identifikacijo uporabnikov na mobilnih napravah na enak način, kot se uporablja pri drugih IT-sistemih, s pomočjo centralnega repozitorija. Postopki dodeljevanja pravic morajo biti enaki kot za vse druge sisteme.

Procesov za področje mobilnih naprav ni treba spreminjati, če so v organizaciji definirani. Če v organizaciji procesi niso definirani, jih je priporočljivo definirati in nato dosledno izvajati ter neprestano izboljševati.

Na mobilnih napravah je treba zagotoviti mehanizme, ki bodo omogočali takšno vrsto nadzora. To so tako imenovana menedžment orodja, ki jih je danes na trgu že veliko.

Varnostne incidente je treba definirati tudi za mobilne naprave.

Zagotoviti je treba pravočasno ter ažurno posodabljanje mobilnih naprav z zaščito pred zlonamerno kodo in varnostne mehanizme na mobilni napravi, ki bodo omogočali varen način prenosa in dostopa do zaupnih informacij.

2.2 ISO/IEC 27001:2005 in mobilne naprave

Standard ISO/IEC 27001:2005 pokriva tudi področje mobilnih naprav ter dela na daljavo, priporočila pa so predstavljena v nadaljevanju.

Glavni cilj področja je zagotavljati informacijsko varnost pri uporabi mobilnih naprav ter pri delu na daljavo.

Definirati je treba ustrezno varnostno politiko ter primerne varnostne indikatorje za zaščito pred grožnjami pri uporabi mobilnih naprav ter komunikacij.

Priporočila za implementacijo

Pri uporabi mobilnih naprav se je treba zavedati groženj pri delu v nenadzorovanih okoljih ter temu primerno definirati varnostne politike.

Varnostna politika za mobilne naprave mora vsebovati priporočila za fizično zaščito, dostopno kontrolo, kriptografske tehnike, varnostne kopije, protivirusno zaščito. Politika naj tudi vsebuje pravila in nasvete pri povezavi mobilnih pripomočkov v omrežje ter priporočila uporabe teh pripomočkov na javnih krajih.

Posebno skrb je treba posvetiti uporabi mobilnih naprav na javnih krajih, sejnih sobah ali drugih prostorih zunaj organizacije. Implementirana mora biti zaščita, da ne pride do nepooblaščenega dostopa ali razkritja informacij, shranjenih in obdelanih na mobilnih napravah (kriptografske tehnike ipd.).

Uporabniki mobilnih naprav na javnih krajih morajo tudi paziti na nepooblaščen prevzem nadzora. Zagotoviti je treba zaščito pred zlonamerno kodo, ki mora biti vedno posodobljena.

Varnostno kopiranje kritičnih poslovnih informacij mora biti narejeno pogosto. Oprema mora zagotavljati hitro in varno izvajanje varnostnih kopij. Varnostne kopije morajo biti ustrezno varovane.

Vzpostavljeni morajo biti primerni mehanizmi varovanja mobilnih naprav pri povezavi na internet. Za oddaljen dostop do poslovnih informacij prek javnih omrežij je treba zagotoviti pravilno identifikacijo ter primerne mehanizme za nadzor dostopa.

Mobilne naprave je treba tudi ustrezno fizično zaščititi pred krajo, še posebno v avtomobilu, hotelskih sobah, konferenčnih centrih ipd. V organizaciji je treba vzpostaviti procese za primere kraje mobilnih naprav. Oprema, ki vsebuje pomembne poslovne informacije, mora biti ustrezno varovana in je ni dovoljeno nenadzorovano puščati na javnih krajih.

Priporočljivo je izvesti usposabljanje za uporabnike mobilnih naprav. Predvsem jih je treba seznaniti z nevarnostmi ter možnimi posledicami, da se bodo tudi sami zavedali pomena vgrajenih varnostnih mehanizmov pri uporabi mobilnih naprav.

2.3 Povzetek

Delovni okvir COBIT se ne spušča konkretno na področje mobilnih naprav, definira generične kontrolne cilje za področje informacijske varnosti, ki jih je mogoče uporabiti oz. aplicirati na katerem koli področju. Standard ISO vsebuje tudi poglavje, ki se ukvarja specifično z mobilnimi napravami.

Pri oblikovanju in izvajanju varnostne politike pri mobilnih napravah izredno pomembno vlogo igrata COBIT ter ISO. Definirata osnove in izhodišča, iz katerih je nato definirana varnostna politika, ki je primerna za posamezno organizacijo. Pri definiranju

varnostne politike mobilnih naprav se ni primerno zanašati samo na COBIT ter ISO, pogledati je treba tudi na druge karakteristike družbe (storitve, velikost organizacije, zaupnost informacij na mobilnih napravah, funkcionalnosti mobilnih naprav itn.).

3 VARNOSTNA POLITIKA

Varnostna politika definira odgovore na dejavnike, ki ogrožajo informacijski sistem od zunaj, kot tudi na dejavnike, ki ogrožajo sistem od znotraj. Varnostna politika je program varnosti in je v pristojnosti vodstva. V tem programu so definirani cilji, pravila in odgovornosti v zvezi z varnostjo informacijskih virov podjetja, razni postopki in pravila. Program obsega pravila o fizičnem in tehničnem varovanju ter pravila, s katerimi je določeno, kakšni bodo načini varovanja. Dobra varnostna politika ima dovolj informacij, virov ter ljudi v podjetju. Sestavljena je iz skupka varnostnih pravil, s katerimi morajo biti seznanjeni vsi zaposleni. Ta pravila opredeljujejo način obnašanja, odgovornosti, naloge in splošna pravila za delo zaposlenih [4].

3.1 Analiza tveganj

3.1.1 Osnovni pojmi

Varnostna analiza tveganj je osnovna zahteva standarda ISO 27000, ki je mednarodno priznan kot generični standard za varnost informacijskih sistemov. Analiza tveganj je izdelana na podlagi glavnih aspektov informacijske varnosti – zaupnosti, celovitosti ter dostopnosti. Kriterij sprejetosti grožnje je definiran z varnostno politiko organizacije [5].

Obstaja veliko metod ter priporočil za pripravo analiz tveganj, vse pa vključujejo glavna tri področja:

- identifikacija groženj ali možnih neželenih incidentov,
- analiziranje vpliva ter verjetnosti groženj,
- ovrednotenje grožnje glede na kriterije odobritve.

Postopek izdelave analize tveganja vključuje naslednje korake:

- identifikacija vsebine analize: opis sistema, ki ga bomo obravnavali v analizi;
- identifikacija groženj: identifikacija možnih scenarijev, ki se lahko zgodijo;
- analiza vpliva ter verjetnosti pojavitve posamezne grožnje;
- ocena tveganja: v povezavi z ocenjenim tveganjem ter kriterijem sprejemljivosti;[1]
- grožnje tveganj: identifikacija in ugotavljanje možnosti groženj.

Analiza tveganj predstavlja formalni pristop za oceno izpostavljenosti. Ugotoviti je treba, katere grožnje pretijo ter kako lahko vplivajo na poslovanje. V nadaljevanju je prikazana analiza tveganja za mobilne naprave. Analiza tveganj je podlaga za izdelavo varnostne politike.

Grožnja je dogodek ali okoliščina, ki bi lahko šla v sistemu narobe (požar, poplava, vdor napadalca, okvara opreme itd.) in bi povzročila izpad informacijskih virov ter škodo pri poslovanju. Grožnje so navzoče v vsakem informacijskem sistemu [6].

Z analizo tveganj sistematično opredelimo informacijske vire in grožnje, ki jim pretijo, ter tako podrobno spoznamo naravo in strukturo tveganj. Izvedba analize tveganj in poznavanje metodologije ocenjevanja prispevata k razumevanju izpostavljenosti in bistveno pripomoreta h kakovostnim odločitvam poslovodstva o načinu in obsegu obvladovanja tveganj. Ocenjevanje in analiza tveganj je eden od glavnih in prvih korakov, ko ugotavljamo skladnost varovanja podatkov in informacij s skupino standardov ISO 27000. Največkrat se odločimo podrobneje analizirati le zelo velika tveganja, manjša pa sprejmemo [7].

3.1.2 Rezultati analize tveganja

Tabela 2 prikazuje grožnje, ki so bile identificirane med analiziranjem tveganja. Tabela za vsako grožnjo prikazuje ocenjeno verjetnost uresničitve grožnje ter posledice.

Veliko identificiranih groženj je splošnih, predvsem so povezane z mobilnimi napravami ter zaupnimi podatki, seveda pa so v tabeli navedene tudi grožnje, ki so vezane na specifičnost obravnave storitve na mobilni napravi.

V izdelani analizi tveganj smo našli tri grožnje, ki imajo nesprejemljivo raven tveganja, kot je lahko tudi razvidno iz matrike tveganj (tabela 1). Dve izmed teh groženj (8 ter 17) se nanašata na verjetnost pojavitve tveganja, ko je mobilna naprava sočasno povezana iz ene možne povezave v varno, nadzorovano omrežje, z drugo možno povezavo pa sočasno na javni internet in je tako izpostavljena tveganjem z interneta. Ta grožnja predstavlja zelo veliko tveganje, kajti na ta način je potencialnemu napadalcu odprta prosta pot do internega omrežja podjetja.

[1] Kriterij sprejemljivosti pomeni stopnjo grožnje, katere se zavedamo, vendar jo sprejmemo in za njo stojimo.

Tabela 1: **Matrika tveganj za storitev elektronske pošte, v kateri so prikazane tudi različne ravni tveganj (brezpredmetno, majhno, zmerno, visoko)**

Verjetnost \ Posledice	Zelo majhne	Majhne	Srednje	Velike	Zelo velike
Zelo majhna				7	
Majhna	16		18, 19	9	4
Srednja	11		14	1, 3, 12, 15	
Velika	13		2, 6	5, 8	
Zelo velika				17	

Pri identifikaciji možnih groženj je treba upoštevati predvsem to, da so mobilne naprave vse bolj zmogljive ter da na njih narašča količina poslovno kritičnih informacij. Zavedati se je treba groženj in začeti izvajati aktivnosti. Sprememb ni mogoče narediti v trenutku, temveč je za to potreben čas [8].

Slika 2: **Grožnje na mobilnih napravah**

Zap. št.	Grožnja
1	Mobilna naprava z aktivnim klientom se lahko izgubi ali pa jo ukrade tretja oseba, ki lahko v imenu uporabnika pridobi določene informacije ter pošilja/prejema elektronsko pošto v imenu uporabnika.
2	Ugasnjeno mobilno napravo lahko nepooblaščena oseba najde ali ukrade – uporabnik ostane brez mobilne naprave.
3	Ugasnjeno mobilno napravo lahko najde ali ukrade nepooblaščena oseba. Nepooblaščena oseba lahko poskuša resetirati PIN-kodo ali kako drugače priti do podatkov, shranjenih na mobilni napravi.
4	Ugasnjeno mobilno napravo lahko najde ali ukrade nepooblaščena oseba. Nepooblaščena oseba lahko poskuša priti do klientovega gesla. Pri tej grožnji predpostavljamo, da je nepooblaščeni osebi že uspelo ugotoviti PIN-kodo.
5	Izguba zunanje spominske kartice, na kateri so shranjeni zaupni podatki. Podatki so lahko razkriti nepooblaščenim osebam – kršenje zaupnosti podatkov.
6	Izguba zunanje spominske kartice, na kateri so shranjeni zaupni podatki. Podatki so izgubljeni in nedostopni.
7	Prejem virusa na mobilno napravo pri sinhronizaciji podatkov s PC.
8	Povezave prek bluetootha ali druge storitve oz. omrežja, ki dostavljajo podatke od zunaj (SMS, MMS, infrared), lahko dajo poln dostop do storitev na mobilni napravi. Metode napada so lahko prepis podatkov, zloraba slabosti protokolov idr. storitve, ki lahko spremenijo konfiguracijo naprave (SMS).
9	Nepooblaščeni uporabniki lahko mobilno napravo najdejo oz. jo za kratek čas ukradejo ter spremenijo konfiguracijo naprave, npr. vklopijo bluetooth. To lahko nepooblaščenim osebam omogoči dostop do storitev ali izrabo pomanjkljivosti protokolov (gl. grožnjo 8).
10	Kršenje interne varnostne politike ter nenamerno povezovanje internega omrežja (npr. prek WiFi) ter zunanjega omrežja (npr. prek GSM/GPRS). S tem se celotno interno omrežje odpre za zunanje napadalce in omogoči nekontroliran prenos podatkov iz internega omrežja v zunanje omrežje.
11	Mobilna naprava je ves čas povezana na internet (npr. prek GPRS) ter tako izpostavljena vsem mogočim grožnjam z interneta, npr. prenehanje delovanja storitve.
12	Mobilna naprava je ves čas povezana na internet (npr. prek GPRS) ter tako izpostavljena vsem mogočim grožnjam z interneta, npr. nepooblaščene osebe lahko pošiljajo elektronsko pošto v imenu uporabnika, jo berejo, odgovarjajo. To predstavlja kršitev zaupnosti, integritete ter dostopnosti.
13	ISA-strežnik, prek katerega je objavljena storitev elektronske pošte, je lahko zlorabljen s strani nepooblaščenih oseb, ker se nahaja v DMZ. Storitev ni dostopna oz. ne deluje.
14	ISA-strežnik, prek katerega je objavljena storitev elektronske pošte, je lahko zlorabljen s strani nepooblaščenih oseb, ker se nahaja v DMZ. Sporočila niso poslana naprej oz. niso poslana ob pravem času.
15	Obstajajo občutljivi podatki, shranjeni na mobilni napravi. Podatki so zlorabljeni, s tem je povzročena kršitev zaupnosti, če mobilno napravo uporabi nepooblaščena oseba.
16	Zloraba strežnika LDAP. Nepooblaščena oseba lahko spremeni uporabniško ime in geslo, storitev uporabniku ne deluje več.
17	Mobilni uporabnik se lahko premika iz nadzorovane cone v nenadzorovano (uporaba brezžičnega omrežja). Mobilna uporaba je lahko uporabljena kot mehanizem za komunikacijo oz. prenos podatkov med nadzorovano in nenadzorovano cono. Poleg prenosa podatkov se v nadzorovano okolje lahko prenese tudi neželena programska oprema ali virus, ki lahko okuži nadzorovano okolje oz. okolje podjetja.
18	Storitve niso dostopne, ker se uporabnik giblje zunaj dosega GSM/GPRS-omrežja.
19	Storitve niso dostopne, ker se uporabnik giblje na območjih, kjer je uporaba mobilnih naprav prepovedana (bolnišnice, letala idr.).

Grožnja 10 ni bila upoštevana v analizi tveganj, kajti ni bilo mogoče objektivno oceniti verjetnosti pojavitve.

4 MODEL UPRAVLJANJA MOBILNIH NAPRAV

4.1 Uvod

Natančno definiran koncept termina upravljanje z napravami – »device management« – pomaga pri razvoju mehanizmov za upravljanje oz. je ključen zanj. Upravljanje naprav lahko obravnavamo kot storitev, ki omogoča uporabniku, da upravlja z vsemi mobilnimi napravami kot celoto [9]. Zajema vse vrste komunikacijskih naprav kot velik virtualni terminal z mnogimi vhodnimi in izhodnimi zmogljivostmi in predstavlja, kako neprestano vzdrževati, opazovati in posodabljati konfiguracijo virtualnih terminalov, kako poteka distribucija podatkov, nastavitev ter konfiguracij na ciljne naprave.

V nadaljevanju predstavljamo pregled obstoječih tehnik in sistemov implementacije za upravljanje z napravami. Združen je v celoto in predstavlja splošni model.

4.2 Arhitektura splošnega sistema za upravljanje mobilnih naprav

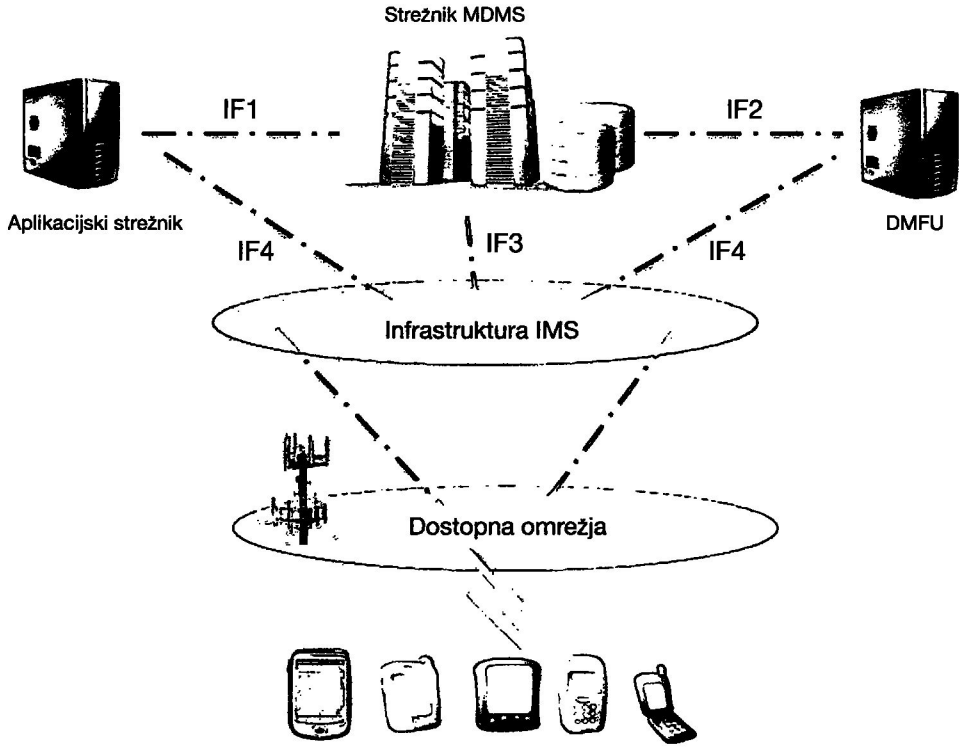
Za zadostitev vseh zahtev, predstavljenih v predhodnem poglavju, je tu predstavljen koncept arhitekture sistema za upravljanje z mobilnimi napravami. V predstavitvi so ločene upravljavske ter izvajalske funkcionalnosti. Arhitektura zajema tudi funkcionalnosti za aplikacijski strežnik za upravljanje nekaterih zmožnosti IMS.

Pregled arhitekture

Kot prikazuje slika 3, je sistem sestavljen iz Master Device Management Serverja (MDMS), Device Management Execution Unit (DMEU), aplikacijskega strežnika (AS) ter pripadajoče infrastrukture IMS (IP multimedia subsystem). MDMS je komponenta arhitekture, ki je glavna za definiranje globalnih upravljavskih politik v obravnavanem okolju. MDMS tudi sodeluje z aplikacijskim strežnikom in drugimi zunanjimi entitetami.

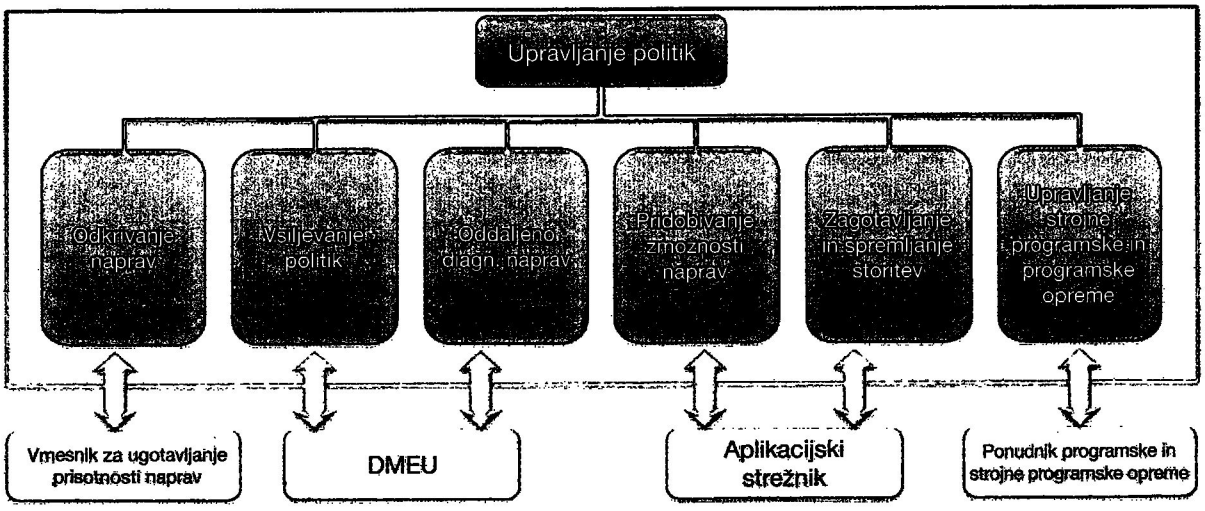
Master Device Management Server – MDMS

Sistem je mogoče definirati tako, da operaterji definirajo domene upravljanja. Lahko se upravlja več domen (grupirane različne mobilne naprave, različni tipi uporabnikov itn.), vendar pa je treba za vsako domeno zagotoviti po en sistem MDMS.



Slika 3: **Arhitektura sistema za upravljanje z mobilnimi napravami [10]**

Na spodnji sliki so predstavljene funkcionalnosti sistema MDMS.



Slika 4: **Funkcionalnosti MDMS**

Sistem MDMS vsebuje naslednje funkcionalnosti:

1. Odkrivanje naprav
2. Upravljanje s politikami
3. Diagnosticiranje oddaljenih naprav
4. Pridobivanje zmožnosti mobilnih naprav
5. Zagotavljanje storitev ter opazovanje pravilnosti delovanja storitev
6. Upravljanje strojnih programskih/programskih komponent

Device Management Execution Unit – DMEU

DMEU je vmesni med celotno arhitekturo za upravljanje in mobilno napravo. Zaradi heterogenosti mobilnih naprav ter podprtih upravljavskih protokolov, mora DMEU podpirati veliko vmesnikov. SNMP je široko podprt pri stacionarnih napravah, kot so PC, OMA DM pa se osredinja na mobilne naprave. Podprti so tudi nekateri drugi upravljavski protokoli, kot je WBEM. DMEU je lahko postavljen tako, da skrbi samo za individualno vrsto naprave. Vsak DMEU lahko uporablja protokol, ki kar najbolje ustreza tipu naprav, ki jih podpira (npr. ena enota DMEU je namenjena obvladovanju mobilnih naprav, druga je za prenosne računalnike). Ena DMEU enota lahko podpira tudi več protokolov.

Aplikacijski strežnik – AS

AS ni neposredno povezan z operacijami upravljanja naprav. AS predstavlja upravljavske zahteve ter jih sporoča sistemu MDMS, vse upravljavske operacije so izvršene s pomočjo MDMS ter DMEU. AS ne potrebuje znanja o posameznih protokolih upravljanja, temveč skrbi le za zagotavljanje storitve (posredovanje zahtev).

Infrastruktura IMS

Z vidika upravljanja mobilnih naprav je IMS osnova za zagotavljanje določenih zmogljivosti (kontrola SIP), kot so polnjenje, avtentikacija, kompresija, preusmerjanje. IMS zagotavlja komunikacijo med upravljalskim strežnikom ter napravo in zagotavlja funkcionalnost odkrivanje naprav ter drugih podprtih kompetenc.

Vmesniki

Kot je prikazano na sliki 4, sta IF1 – vmesnik med MDMS in AS – ter vmesnik IF2 – vmesnik med MDMS in DMEU – lahko implementirana kot spletna storitev [11] ter opisana z Web Service Description Language (WSDL) [12].

Operacije vmesnika IF1 so namenjene zagotavljanju boljših storitev. AS potrebuje informacije o napravi vključno s konfiguracijo naprave ter zmogljivostmi naprave (verzija programske opreme, podprtih storitev idr.) prek IF1. AS konfigurira naprave, povezane z informacijami o napravi, vključno z nastavitvami parametrov ter nameščanjem potrebnih posodobitev. AS sledi tudi statusu storitev in vrača poročila, ko se uporablja storitev. Operacije IF2 se servisirajo z namenom sodelovanja med MDMD ter DMEU, ki vključuje poizvedovanje po politikah, poročila izvajanja ter asinhrono obveščanje. Poizvedovanje po politikah omogoča dostavo upravljavske politike iz

MDMS v DMEU. Poročilo izvedbe politike je posredovano nazaj v sistem MDMS. Asinhrone notifikacije prenašajo asinhrone dogodke, npr. pomembna informacija iz naprave je posredovana v sistem MDMS.

Vmesniki med infrastrukturo IMS ter drugimi elementi – IF3 ter IF4 – se prilagajajo specifikacijam IMS glede na scenarije implementacije.

Možnosti integracije več funkcionalnosti IMS v upravljanje naprav

Prednost IMS je integracija funkcionalnosti SIP skupaj v celoto ter servisiranje multimedijske storitve. Nobeden od SNMP, WBEM ali OMA DM ne vpliva na SIP neposredno in tudi ne more neposredno uporabljati funkcionalnosti IMS. Možen pristop je, da se razvije nov protokol za upravljanje, ki je osnovan na protokolu SIP z razširjanjem nekaj metod ter glav [13]. Vendar ni eksplicitnih tehničnih razlogov za razvijanje novega protokola. Naslednji mogoči pristop je dodajanje mehanizmov SIP v obstoječe rešitve za izboljšanje performans.

4.3 Primerjava produktov na trgu

V predhodnem poglavju je predstavljen splošen sistem – idealen sistem, v nadaljevanju pa so predstavljeni štirje produkti, ki jih je mogoče kupiti na trgu.

Tabela 2: **Primerjalna tabela prednosti in slabosti produktov na trgu**

Fukcionalnosti produktov za upravljanje mobilnih naprav	**Sybase iAnywhere Afaria 6.0**	**Nokia Intellisync Device Management**	**System Center Mobile Device Management**	**Exchange Server 2007**
Podpora končnim uporabnikom 32-bit Windows kompatibilni				
Windows PPC 2000/2002/2003	D	D	D	D
Windows Mobile 5/6/6.1	D	D	D	D
Sony Ericsson M600i/P1i	D	D	N	D
Nokia E & N Series	D	D	N	D
Integracija s SCCM-jem	D	D	D	N
Funkcionalosti, podprte na podprtih platformah Windows Mobile/Symbian				
Nameščanje agenta po zraku	D	D	D	N
Zbiranje vseh podatkov o napravah	D	D	D	N
Distribucija programske opreme	D	D	D	N
Distribucija dokumentov	D	D	N	N
Konfiguriranje mobilnih naprav	D	D	D	N
Vsiljevanje varnostnih politik na mobilne naprave	D	D	D	D
Kriptiranje datoteke ali mape na napravi	D	D	D	N
Oddaljeno zaklepanje mobilne naprave	D	D	D	D
Oddaljeno resetiranje naprave na tovarniške nastavitve	D	D	D	D
Izdelovanje varnostnih kopij mobilne naprave	D	D	D	N
Izdelovanje skript za mobilne naprave	D	D	D	N
Podpora ob neuspešni sinhronizaciji	D	D	D	N
Kompresija	D	D	D	N
Ponastavljanje točke povrnitve stanja na mobilni napravi	D	D	D	N
Sinhronizacija samo spremenjenih podatkov	D	D	N	N
Konfiguracija pasovne širine na posamezni mobilni napravi	D	D	N	N
Granualna enkripcija podatkov pri sinhronizaciji: control channel/package/file	D	D	D	N
Dinamična podpora skupinam glede na hardware/software	D	N	D	N
Push distribucija	SMS, IP	SMS, IP	SMS	N
Podpora za upravljanje osebnih podatkov (personal information manager-PIM)	N	D	N	N
Podpora integraciji z aktivnim imenikom podjetja	LDAP, AD	LDAP, AD	LDAP, AD	N
Generiranje poročil	D	D	D	N
Beleženje dogodkov, ki se izvajajo na napravah	D	N	D	N
Zunanje in PDA sinhroniziranje podatkovne baze	D	D	N	N

Produkti so si v splošnem med sabo zelo podobni, izstopa le upravljanje mobilnih naprav z orodjem Microsoft Exchange 2007. Omogoča predvsem vsiljevanje politik na naprave ter oddaljeno brisanje podatkov na mobilni napravi, medtem ko ne podpira drugih funkcionalnosti. Vse zgoraj navedene funkcionalnosti podpira na ključnih platformah mobilnih naprav (Windows Mobile, Symbian).

5 VPELJAVA CELOVITEGA PRISTOPA OBVLADOVANJA MOBILNIH NAPRAV

Poglavje prikazuje vse aktivnosti, ki jih je treba upoštevati pri uvajanju sistema obvladovanja (upravljanja) mobilnih naprav. Slika 5 prikazuje diagram poteka aktivnosti. Potek aktivnosti ni pravilo, ki se ga je treba nujno držati, so le priporočila in usmeritve za druga podjetja oz. organizacije, ki se bodo srečevali s podobnim problemom.

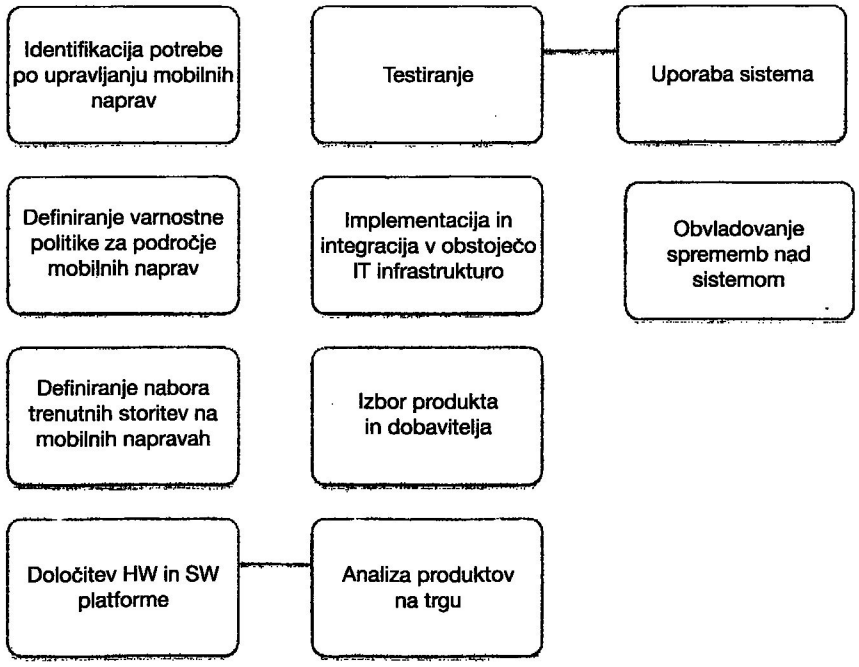
Proces se začne izvajati takrat, ko se pojavi dovolj velika potreba po upravljanju obilnih naprav. To se ne more zgoditi v kratkem časovnem intervalu, potreben je določen čas, da potrebe dozorijo.

Ko potrebe dozorijo, je treba definirati temelje uspešnega upravljanja mobilnih naprav, in sicer je to varnostna politika, nato trenutni podprti nabor storitev na mobilnih napravah ter trendi na področju storitev na mobilnih napravah. Definirati je treba tudi platformo strojne opreme in programske opreme (operacijski sistemi), ki jih bomo uporabljali v podjetju. Platforma mora biti zastavljena tako, da predvideva zamenjavo modela mobilne naprave z novejšim.

Ko so definirani temelji in okvirna pričakovanja (cilji) orodja za upravljanje mobilnih naprav, je priporočljivo izvesti analizo produktov na trgu ter izbrati najugodnejšega oz. tistega, ki najbolje pokriva vse zahteve.

Ko je produkt izbran, je treba zagotoviti uspešno implementacijo orodja v obstoječo infrastrukturo podjetja in po možnosti zagotoviti integracijo orodja z drugimi orodji za upravljanje (npr. orodje za upravljanje delovnih postaj, strežnikov itn.).

Na koncu seveda sledi testiranje sistema ter uporaba v produkciji. Ko se sistem nekaj časa uporablja, se pojavijo tudi problemi oz. stvari, ki jih je treba popraviti ali izboljšati. Za to poskrbi aktivnost obvladovanja sprememb nad sistemom, s katero zagotovimo sledljivost vseh sprememb nad sistemom. Proces se ne sme nikoli končati, neprestano je treba spremljati delovanje sistema ter ustrezno ukrepati pri odstopanjih od pričakovanj.



Slika 5: **Prikaz poteka aktivnosti pri uvajanju sistema v organizacijo**

6 SKLEP

Problem lahko rešimo šele takrat, ko se zavedamo, da obstaja. Pogledati je treba po organizaciji in prešteti, koliko različnih modelov mobilnih naprav uporabljamo. Brez pravega pristopa in brez pravega sistema upravljanja mobilnih naprav bodo podjetja težko preprečila odtekanje oz. krajo zaupnih informacij iz mobilnih naprav.

Podjetja se bodo morala soočiti z velikim naborom različnih platform mobilnih naprav. Za začetek uspešnega obvladovanja mobilnih naprav bodo morala podjetja definirati standarde, kot je napisal Gold v enem od svojih zaključkov: »Standardizacija platforme bo pomagala – vendar ne popolnoma izolirala organizacijo pred raznolikostjo mobilnih naprav. Organizacije bodo morale posodabljati mobilno strategijo prihodnja leta, da bodo zmožne uporabljati tehnologije za izboljšanje produktivnosti, varnosti itn. [14].

Obvladovanje mobilnih naprav v podjetju bo uspešno in bo imelo pozitivne učinke za podjetje, če se bomo pri samem pristopu definirali dobre temelje, na katerih bomo gradili celoten pristop. Dober temelj je dobro definiran in fleksibilen standard mobilnih naprav, ki ga je treba dosledno upoštevati.

Članek prikazuje pristop obvladovanja mobilnih naprav v podjetju, ki mu bo prinesel nižje stroške upravljanja z mobilnimi napravami, zmanjšale se bodo varnostne grožnje, povečala se bo produktivnost uporabnikov. Cilj pa je bil tudi zagotoviti povečanje ravni varnosti, ne da bi se poslabšala uporabniška izkušnja. Delo prikazuje predvsem probleme ter nakazuje možne rešitve.

Z varnostjo se je treba spoprijeti na vseh ravneh poslovanja in se ji dnevno posvečati. Ključnega pomena so stalni pregledi sistema in njegovo izboljševanje, saj lahko le tako zagotavljamo varnost informacijskega sistema v vsakem trenutku, ne glede na spremembe, ki nastajajo v procesih in sredstvih. Ključni dejavnik vpeljave sistema za upravljanje informacijske varnosti so zaposleni, vključno z upravo in vodstvom, ki morajo sprejeti varnostno politiko.

Ker se mobilne tehnologije izredno hitro spreminjajo, je treba biti pri definiranju celovitih pristopov previden. V članku predstavljeni pristop bi bilo treba v praksi čim večkrat preizkusiti in ga dopolniti ter spremeniti glede na novo pridobljene izkušnje.

7 LITERATURA

[1] Renkema, Theo J. W.: The IT value quest: how to capture the business value of IT-based infrastructure. Chichester, England: John Wiley & Sons Ltd, 2000.

[2] ISO 17799:2005 Information technology – Security techniques – Code of practice for information security management. Geneva: ISO/IEC, 2005, 115 str.

[3] ISO 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO/IEC, 2005, 34 str.

[4] Petrović, Damjan: 'Analiza informacijske varnostne politike v Agenciji RS za kmetijske trge in razvoj podeželja. Diplomsko delo. Univerza v Ljubljani, Ekonomska fakulteta, 2007.

[5] Bŕnes, Erlend et al.: Risk analysis of information security in a mobile instant messaging and presence system for healthcare, International Journal of Medical Informatics (2006), doi:10.1016/j.ijmedinf. (2. 6. 2006)

[6] Calder, Alan, Watkins, Steve: 'International IT Governance: An Executive Guide to ISO 17799/ISO 27001', Kogan Page Limited, 2006.

[7] Potočnik, Marko: Analiza tveganja za odločanje o ravni varovanja informacij. Varnostni forum. Ljubljana, 2006. Str. 12.

[8] Schultz, E. Eugene: 'Mobile computing: The Next Pandora's Box', Computers & Security. Letnik 2007, vol. 26, št. 3, str. 187.

[9] Van Thanh, D., Jonvik, T., Vanem, E., Van Tran, D., Audestad, J. A.: The device management service. In: Proceedings of IEEE Intelligent Network Workshop, Boston, US, 2001.

[10] Jun Ma, Jianxin Liao, Xiaomin Zhu: Device management in the IMS, Journal of Network and Systems Management, Springer Netherlands, Vol. 16, št. 1, str 46–62, marec 2008.

[11] Karl, G., Stephen, G., Heather, K., James, S.: Introduction to Web services architecture. IBM Syst. J. 41 (2), 170–177, 2002.

[12] W3C, Web Services Description Language (WSDL), http://www.w3.org.

[13] State, R., Frestor, O.: Management of wireless dynamic infrastructures. In: proceedings of the Eighth IEEE International Symposium on Computer and Communications, Kemer-Antalya, Turkey, 2003.

[14] R. Hickey, Mobile device trends: Security, consolidation and more, SearchMobileComputing.com, Maj 2006.

Tadej Prešeren je leta 2006 diplomiral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani in tam leta 2008 tudi magistriral na programu Informacijski sistemi in odločanje. Leta 2007 se je zaposlil v podjetju Krka, d. d., Novo mesto v sektorju za informacijske tehnologije in telekomunikacije, kjer skrbi za delovne postaje, mobilne naprave in vodi številne projekte na področju zaščite podatkov, uvedbe orodja za upravljanja mobilnih naprav, virtualizacije aplikacij ter uvedbe poenotenih komunikacij. S svojimi prispevki sodeluje na srečanjih in posvetovanjih.

Marko Bajec je zaposlen kot docent na Fakulteti za računalništvo in informatiko Univerza v Ljubljani, kjer predava predmete s področja informacijskih sistemov. Raziskovalno in v praksi se ukvarja predvsem s področji, kot so načrtovanje in uvajanje metodologij razvoja informacijskih sistemov (poudarek na uporabi sodobnih pristopov ter najboljših praks), strateško planiranje informatike, poslovno modeliranje, elektronsko poslovanje ter v zadnjem času analiza podatkov in odkrivanje anomalij. Je član več strokovnih in znanstvenih združenj. Svoje delo objavlja v domačem in mednarodnem prostoru.