UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matjaž Cör

NAČRTOVANJE IN STRATEGIJA SISTEMA ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI

Mentorica: doc. dr. Mojca Ciglarič

DIPLOMSKO DELO
NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Ljubljana, 2009

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00454/2009
Datum: 05.04.2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MATJAŽ COER**

Naslov: **NAČRTOVANJE IN STRATEGIJA SISTEMA ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI**

DIGITAL IDENTITY MANAGEMENT SYSTEM: STRATEGY AND DESIGN CONSIDERATIONS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

Preučite področje digitalnih identitet in sistemov za upravljanje z njimi ter definirajte relevantne pojme na tem področju. Opišite administrativne naloge, ki jih je potrebno izvajati v organizaciji, ki nima vpeljanega sistema za upravljanje z digitalnimi identitetami. Nato opišite okvir strategije, ki naj jo organizacija definira, preden uvede takšen sistem – definirajte pojem strategije in opišite vsebinska področja ali vprašanja, na katera je potrebno odgovoriti, da lahko opredelimo vse lastnosti sistema za upravljanje z digitalnimi identitetami. Preglejte tržno dosegljive izvedbe sistemov za upravljanje z digitalnimi identitetami in naredite njihovo medsebojno primerjavo. Na primeru konkretne organizacije opišite izbiro sistema za upravljanje z digitalnimi identitetami in proces postavljanja strategije na tem področju. Odločitve utemeljite ter navedite njihove prednosti in slabosti.

Mentor:

M. Ciglarič

doc. dr. Mojca Ciglarič

Dekan:

prof. dr. Franc Solina

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00454/2009
Datum: 05.04.2009

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MATJAŽ COER**

Naslov: **NAČRTOVANJE IN STRATEGIJA SISTEMA ZA UPRAVLJANJE Z DIGITALNIMI IDENTITETAMI**

DIGITAL IDENTITY MANAGEMENT SYSTEM: STRATEGY AND DESIGN CONSIDERATIONS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

Preučite področje digitalnih identitet in sistemov za upravljanje z njimi ter definirajte relevantne pojme na tem področju. Opišite administrativne naloge, ki jih je potrebno izvajati v organizaciji, ki nima vpeljanega sistema za upravljanje z digitalnimi identitetami. Nato opišite okvir strategije, ki naj jo organizacija definira, preden uvede takšen sistem – definirajte pojem strategije in opišite vsebinska področja ali vprašanja, na katera je potrebno odgovoriti, da lahko opredelimo vse lastnosti sistema za upravljanje z digitalnimi identitetami. Preglejte tržno dosegljive izvedbe sistemov za upravljanje z digitalnimi identitetami in naredite njihovo medsebojno primerjavo. Na primeru konkretne organizacije opišite izbiro sistema za upravljanje z digitalnimi identitetami in proces postavljanja strategije na tem področju. Odločitve utemeljite ter navedite njihove prednosti in slabosti.

Mentor:

M. Ciglarič

doc. dr. Mojca Ciglarič

Dekan:

prof. dr. Franc Solina

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani/-a Matjaž Cör,
z vpisno številko 63980019,

sem avtor/-ica diplomskega dela z naslovom:

»Načrtovanje in strategija sistema za upravljanje z digitalnimi identitetami«

»Digital Identity Management System: Strategy And Design Considerations«

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal/-a samostojno pod mentorstvom (naziv, ime in priimek)

  doc.dr. Mojca Ciglarič

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela

- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne 15.10.2009 Podpis avtorja/-ice: _____

Kazalo

Zahvala

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za njeno potrpljenje in koristne nasvete ter napotke. Zahvalil bi se tudi sodelavcem v podjetju KPMG Slovenija, d.o.o., ki so verjeli vame in me vzpodbujali ter mi dajali napotke za pisanje diplomske naloge. Posebna zahvala gre staršema za potrpljenje in podporo.
Hvala tebi Iris, brez tebe mi ne bi uspelo!

Seznam uporabljenih kratic

Kratica	Pomen	Prevod
IAM	Identity and Access Management	Upravljanje z digitalnimi identitetami in dostopi
PKI	Public Key Infrastructure	Infrastruktura za avtentikacijo s pomočjo javnega ključa
AD	Active Directory	Aktivni imenik
SSO	Single Sign-On	Enotna prijava
HR	Human Resources	Človeški viri – kadrovanje
IM	Identity management	Upravljanje z digitalnimi identitetami
IT	Information technology	Informacijska tehnologija
LDAP	Lightweight Directory Access Protocol	Enostavni protokol za dostop do aktivnega imenika
SPML	Service Provisioning Markup Language	Ogrodje za izmenjavo in upravljanje z uporabniškimi pravicami za dostop do aplikacij in z informacijskimi viri v heterogenih okoljih
ITIL	IT Infrastructure Library	Najbolj razširjena zbirka dobrih praks za upravljanje informacijskih tehnologij
VPN	Virtual Private Network	Navidezno zasebno omrežje

Povzetek

Velika podjetja se dnevno srečujejo z novimi izzivi na vseh področjih. Mnogi izzivi prihajajo s strani informacijske tehnologije. V zadnjih časih se pogosto pojavlja vprašanje identitete uporabnikov in njihovega upravljanja. Vedno več je aplikacij in še več internetnih dostopov, uporabniki imajo svoje poštne predale in različne dostopne podatke. Uporabniška imena in gesla se kopičijo in tako zlahka pride do zmešnjave, pozabljenega uporabniškega dostopa, zlorabe, posledica vsega tega pa je slaba volja zaposlenih in administratorjev.

Rešitev navedenih problemov predstavlja sistem za upravljanje z digitalnimi identitetami. Podjetja stremijo k čim bolj enostavnim in celovitim rešitvam, zato bodo s pomočjo enotnega upravljanja zmanjšala čas, potreben za administracijo uporabnikov, zmanjšala bodo tveganje za izgubo podatkov, uporabniki in administratorji bodo zadovoljni, povrh vsega pa se bo dvignil nivo varnosti celotnega informacijskega sistema.

V pričujoči diplomski nalogi bomo preučili področje digitalnih identitet, opisali koncept sistema za upravljanje z digitalnimi identitetami, njegovo delovanje in katere so njegove komponente. Opisali bomo okvir strategije, ki ga mora podjetje definirati, preden uvede tovrsten sistem. Na kratko bomo pregledali tudi najbolj razširjene proizvajalce sistemov za upravljanje z digitalnimi identitetami in opisali njihove lastnosti ter preverili tržne deleže.

Ker sem zaposlen v podjetju, ki se dnevno ukvarja z upravljanjem identitet in dostopov, mi je področje še bolj domače, saj administratorji vedno iščemo nove rešitve za poenostavitev svojega dela. V diplomski nalogi bomo zato predstavili obstoječe stanje v izbranem podjetju, ki nima avtomatizirane rešitve, in predlagali strategijo, kako podjetje s »papirnatega« sistema za upravljanje identitet preide na avtomatiziran sistem. V nalogi bomo pregledali strateške cilje in povzeli odločitve, ki jih mora izbrano podjetje upoštevati, da v svojo infrastrukturo uvede sistem za upravljanje z digitalnimi identitetami.

Ključne besede: identiteta, upravljanje z identitetami, upravljanje z uporabniki, aktivni imenik, strategija

Abstract

Large companies are daily faced with new challenges in all areas. Many challenges come from information technology. In the recent past there is often a question of users identity and their management. There is an increasing number of applications and internet providers, users have their mailboxes and various access data. Usernames and passwords are easily accumulate which easily leads to confusion, forgotten user access, misuse and the result of all this is bad mood of employees and administrators.

A system for managing identities is a solution of those problems. Companies seek to find the simplest and complete solutions, so they are going to reduced the time required for administration of users and reduce the risk of data loss through the single management. The users and administrators will also be satisfied and on top of it, it is going to raise the security level of the entire information system.

In the present diploma thesis I am going to study the area of digital identities, describe the concept of a system for managing digital identities, its operation components. I am also going to describe the framework of the strategy defined by the company, before introducing such a system. In short, I am also going to examine the producers of the most widespread systems for managing digital identities, describe their properties and check the market shares.

Because I work in the company that is daily concerned with the management of identities and access, I am especially familiar with the problematic, since as an administrator, I always look for new solutions to simplify my work. In the graduation thesis, I am therefore going to present the current state of the selected company, which does not have the automated solution, and propose a strategy, how the company with a "paper" identity management systems to passes to the automated system. In this thesis, I am also going to review the strategic objectives and summarize the decisions which have to be taken into account by the selected firm must take into account in order to introduce the system for management with digital identities into its own infrastructure.

Keywords: identity, identity management, user management, active directory, strategy

1 Uvod

Varnost omrežja in celotne infrastrukture podjetja je poglaviten razlog za uvajanje sistema za upravljanje z digitalnimi identitetami. Podjetja rastejo in postopoma uvajajo nove storitve, kot so e-poslovanje in dostop do elektronske pošte iz celega sveta, podjetja povečujejo projekte, se povezujejo z raznoraznimi podjetji, in pri vsem tem je postal nadzor dostopa do podatkov zelo težko in obširno opravilo. Specialisti za omrežja in informacijsko varnost morajo imeti pregled in nadzor nad tem, kdo ima dostop, kje in kdaj uporabnik dostopa in na kakšen način dostopa. Vrste dostopov, ki jih lahko upravljamo, so spletni dostop (Web-Access), oddaljen telefonski dostop, VPN itd.

Načinov dostopanja do pošte je vsak dan več, poleg tega lahko do svoje pošte pridemo skorajda od kjer koli in kadar koli. Torej, kako lahko podjetje upravlja in nadzira dostope do omrežja? Odgovor je: z obsežnimi pravilniki za upravljanje z digitalnimi identitetami in s pomočjo obsežne aplikacije za upravljanje z digitalnimi identitetami.

Vse skupaj zveni enostavno, vendar pa je v realnosti le redko celotna zadeva tako enostavna. Pravilniki za upravljanje z digitalnimi identitetami morajo biti osredotočeni na to, kaj želi podjetje ustvariti, in se ne smejo prilagoditi temu, kar podjetje že počne. Nato je potrebno oceniti in primerjati obstoječe delovne procese z želenimi procedurami ter poiskati pravilne rešitve za nadzor dostopa. To so take rešitve, ki ustrezajo delovanju podjetja. Na koncu je potrebno izdelati načrt, kako celotno zadevo implementirati. Spremembe, ki jih nameravamo uvesti, lahko uvedemo v celotni infrastrukturi, lahko pa spremenimo le tiste segmente v infrastrukturi, kjer bodo spremembe najbolj vplivale na učinkovitost delovanja podjetja.

Varnost je zadnjih letih največji in najpomembnejši sestavni del delovanja velikih in majhnih podjetij. Z eksplozijo elektronskega poslovanja je število uporabnikov in aplikacij naraslo skorajda eksponentno, zato so bila podjetja z informacijsko tehnologijo prisiljena izboljšati svoje tedanje aplikacije in politike, da so lahko obvladovale tako strmo rast uporabnikov. Kot posledica tega je postala varnostna politika precejšnja ovira pri uvajanju in razvijanju novih poslovnih rešitev. Precejšnja rast uporabnikov, velika potreba po e-poslovanju in razni prehodi uporabnikov med oddelki so bili poglavitni pogoj za iskanje rešitve, ki bo spremljala celotni življenjski cikel uporabnika. Poleg tega je upravljanje in določanje ustreznih pravic uporabnikom postalo zelo pomembna odgovornost, saj se lahko upravljanje pravic neposredno odraža na to, kako dobro ima neko podjetje urejene poslovne stike.

Dandanes se podjetja vedno bolj zanašajo na svoje aplikacije, ki delujejo v zelo različnih okoljih v podjetju. Uporabniki do aplikacije ne morejo dostopati ne da bi bili registrirani oz. do podatkov ne morejo dostopati brez uporabniškega imena in gesla. V velikih podjetjih se uporabniška imena in gesla nenehno ustvarjajo in brišejo glede na prihode in odhode ljudi, se spreminjajo glede na vlogo uporabnika v sistemu oz. organizaciji.

Tipični uporabnik potrebuje uporabniško ime, s katerim bo lahko dostopal do različnih aplikacij v podjetju. Dostop do aplikacij mora biti na nekem nivoju tudi povezan s sistemom za upravljanje dostopov, zato je več kot očitno, da mora biti uporabnik registriran na vseh mestih, kjer bo dostopal do podatkov.
Razvoj dobrega in efektivnega sistema za upravljanje z digitalnimi identitetami, ki upravlja z uporabniki, njihovimi podatki in njihovimi ustreznimi pravicami, podjetju pomaga se

spoprijeti z vsemi temi izzivi. Sistemi za upravljanje z digitalnimi identitetami, ki danes že obstajajo, lahko izboljšajo delovanje samega podjetja. Ne samo da zmanjšujejo stroške, povečujejo uspešnost in zadovoljstvo uporabnikov, povrh vsega zagotavljajo visoko raven varnosti informacij.

2 Upravljanje z digitalnimi identitetami

V drugem poglavju bomo pregledali lastnosti sistema za upravljanje z digitalnimi identitetami. Pogledali in opredelili bomo pojme, kot so identiteta, identifikacija, overitev in digitalna identiteta.

2.1 Kaj je upravljanje z digitalnimi identitetami?

Glavna naloga sistema za upravljanje z digitalnimi identitetami je upravljanje celotnega t. i. življenjskega cikla uporabnika v nekem sistemu oz. z drugimi besedami upravljanje »identitete« uporabnika. Upravljanje se začne že z ustvarjanjem uporabniškega računa in se nadaljuje s postavljanjem uporabnika v različna uporabniška okolja, kjer moramo uporabniku določiti njegove pravice, s katerimi lahko dostopa do podatkov. Uporabnika vedno spremlja upravljanje sprememb, ki uporabniku ob menjavi službe oz. statusa v podjetju spet določi ustrezne pravice.

Upravljanje uporabnika se konča, ko uporabnik zapusti podjetje oz. ko se mora njegov uporabniški račun zbrisati, ali pa se mu enostavno odvzamejo pravice za dostop.
Ponavadi življenjski cikel uporabnika spremljajo bolj ali manj kompleksni delovni procesi, kot so registracija uporabnika, odobritev managerjev, določanje nivoja dostopa, potrebno pa je obvestiti tudi sistemske administratorje, da pripravijo uporabniški račun in ga opremijo z ustreznimi pravicami.

Življenjski cikel uporabnika in predvsem določanje pravic uporabniku je le majhen sestavni del sistema za upravljanje z digitalnimi identitetami. Drugi in večkrat pozabljen sestavni del je *Access management* (v nadaljevanju upravljanje z dostopi). Kako prepoznati uporabnika? Katere mehanizme uporabiti za prepoznavo uporabniškega imena in gesla? Katerega od SSO (Single Sing-On) mehanizmov uporabiti? Celota vseh sestavnih delov pa lahko skupaj deluje le, če ima podjetje pravilno postavljeno strategijo, katere se mora držati, da pride do želenega cilja.

2.2 Kaj je to identiteta?

Identifikacija v informacijskem sistemu pomeni zmožnost povezovanja nekega digitalnega identifikatorja z neko osebo ali računalniško komponento v informacijskem sistemu (npr. strežnik, računalnik ...). Ta identifikator je lahko nek PKI certifikat, lahko pa je shranjen v obliki druge informacije v računalniškem sistemu, kot npr. skrivna povezava med identiteto in geslom ali kriptirano geslo.

Zelo pomembna je odločitev, katere podatke bomo uporabljali, da bomo na podlagi le-teh ugotovili, katera oseba ali računalnik želi dostopati do določenega vira podatkov. Če izberemo samo neko ime, nam to ne zadostuje, potrebujemo še kakšen dodaten unikaten podatek, da lahko natančno določimo dostop.

Slika 1. Katere podatke bomo uporabili za opredelitev identitete?

Na spletu je dostopno ogromno literature o identitetah na splošno. Ena izmed največkrat uporabljenih definicij identitete se nahaja v dokumentu [16], ki se posodablja že skoraj deset let in je bil že mnogokrat objavljen in citiran. V tem dokumentu avtor zastavi zelo podrobno taksonomijo pojmov na področju anonimnosti uporabnika, vključno s pojmi identiteta, psevdonim in »neopazljivost« (unobservability).

Pojem identiteta osebka je v tem dokumentu tista množica atributov, ki ga identificira znotraj neke množice osebkov. Ker so lahko množice osebkov zelo različne, tudi ta množica atributov ni enaka vsaki množici osebkov. Lahko torej trdimo, da osebek nima ene unikatne identitete, temveč celo množico identitet. Vrednosti atributov in tudi sami atributi se lahko sčasoma spreminjajo, torej se nujno spreminjajo tudi identitete.

Digitalna identiteta po dokumentu [16] je množica tistih atributov, ki so shranjeni, povezani in dosegljivi s pomočjo računalniške tehnologije. S svojo digitalno identiteto se uporabnik prvič sreča ob prijavi na računalnik.

2.3 Identifikacija in overitev

Avtentikacijo oz. overitev si lahko razlagamo kot neko metodo, ki preverja digitalni identifikator in ga poveže z določeno osebo ali računalnikom, s katerim je dejansko povezan. Po procesu overitve, metoda poveže identiteto z njenimi že določenimi pravicami za dostop do podatkov.

Na svetovnem trgu ne primanjkuje tehnologij za identificiranje oseb. Nekatere izmed njih se lahko uporabljajo samostojno, nekatere je potrebno združiti z drugimi aplikacijami, da dobimo želeni rezultat. Ponavadi za identifikacijo zahtevajo ime in priimek, ali t. i. pametno kartico ali prstni odtis, skratka možnosti je neskončno mnogo.
Za identifikacijo računalnikov se največkrat uporablja unikatna identifikacijska koda (UID), ki jo največkrat določi proizvajalec računalnika oz. računalniške opreme, ali pa sistemski administrator določi neko unikatno ime za določen računalnik ali strežnik.

2.4 Kriza digitalne identitete

Problematika identitete v današnjem informacijskem okolju je še vedno aktualna. V bistvu se ta problem ne navezuje samo na poslovne procese, ampak na splošno uporabo informacijskih tehnologij na delovnem mestu, doma, v šoli in pri uporabi javnih storitev.
Univerzalna identiteta trenutno še ni mogoča. Ker je bil internet zgrajen za anonimni dostop in ker lokalna omrežja uporabljajo različne, med seboj nezdružljive identitete, uporabniki v zadnjem času ne morejo več upravljati z vsemi svojimi identitetami. To pa nekateri s pridom izkoriščajo v kriminalne namene.

Pred letom 1980 je imel uporabnik običajno eno identiteto, ali pa morda dve, na centralnem strežniku. S prihodom aplikacij odjemalec/strežnik sredi osemdesetih je začelo število identitete uporabnika drastično naraščati. Današnja praksa kaže na problem identitet enega uporabnika za dostop do različnih servisov na spletu, dostop preko mobilnih naprav, pri prijavah v različne aplikacije na delovnem mestu ali na javnih servisih, v domačem omrežju ipd.

Kako so se problemi reševali? Vsak servis ali aplikacija ima mehanizem za overjanje, avtorizacijo in identifikacijske podatke za dostop do ponujene storitve. Združevanje identitet uporabnika se je reševalo preko centralnega imenika, v katerem je bilo treba urediti povezave v sistemu za overitev med posameznimi servisi in dostopom uporabnikov do teh servisov. Zaradi vse večjega števila uporabnikov in storitev ter povezovanja med storitvami se že pojavljajo težave z upravljanjem identitet. Glavni problemi so: preveč uporabnikov in preveč zahtev za administrativne pravice, preveč gesel, predolgi časi za prijavo (zaradi overjanja), preveč »sirot« – neuporabljenih ali pozabljenih identitet in s tem omejeno upravljanje.

Iz tega po [13] sledi, da:

- povprečni uporabnik porabi na dan 16 minut za prijave (Vir: Meta Group),
- ima tipični uporabnik več kot 21 identitet (Vir: NTA Monitor Password Survey),
- je število strani s potrebno registracijo vedno več,
- IT-operator v povprečju upravlja s 73. aplikacijami in 46. dobavitelji (Vir: Gartner),
- postajajo zahteve glede pritožb in sledenja vse strožje,

- predstavljajo »osirotele identitete« velik varnostni problem.

Za reševanje tega problema obstajata dve rešitvi:

- Zgraditev globalnega, vsestranskega in skupnega metasistema identitet, kar s časovnega vidika pomeni vsaj leto dni dela (boljša rešitev).
- Zgraditev skupnega metasistema identitet na osnovi standardov za vse, ki bi uporabljali enake standarde (hitrejša rešitev).

Karakteristike metasistema identitet:

- ni sistem ali proizvod,
- je dogovor o metapodatkih in protokolih in omogoča več ponudnikov identitete,
- temelji na odprtih standardih,
- podpirajo ga vse tehnologije,
- vključuje zavedanje o zakonih, ki veljajo v okviru »identitete«,
- spoštuje zasebnost.

Vzemimo za primer Microsoftov sistem Passport oz. Windows Live ID. To je sistem, ki omogoča dostop do raznih Windows Live storitev s samo enim uporabniškim imenom. Uporabniki, ki imajo ustvarjen svoj Live ID, lahko z eno prijavo v sistem dostopajo do svoje pošte, se pogovarjajo s prijatelji ali organizirajo svoje opravke.
Izkazalo pa se je, da je kot metasistem identitete neprimeren. Vendar je MS Passport ponudnik identitet za MSN, ki vsebuje več kot 330 milijonov uporabnikov, in preko njega se izvede na dan več kot ena milijarda prijav. To pomeni, da je učinkovit. Če uporabimo Passport za javni dostop v internet, se takoj opazi težava zaradi nezaupanja do tretjih uporabnikov, sistem ni več dovolj standarden, pojavijo se problemi z upravljanjem identitet (Ali dovoliti dostop do sistema za upravljanje identitet?). Največji problem pa je predelava aplikacij, da bi sploh lahko uporabljale takšen sistem.
MS Passport ne zagotavlja ideje o metasistemu identitet v najmanj dveh zgoraj omenjenih točkah, kjer omenjamo karakteristike metasistema identitet.

Vloge v metasistemu identitet:

- Ponudniki identitete: pooblaščene organizacije, vladne organizacije ali morda tudi končni uporabniki, ki bi dajali zahtevke za identiteto (ime, starost, naslov itd.).
- Zaupanja vredni partnerji, ki bi ponujali vstopne točke, spletne storitve itd.
- Stranke (individualne osebe) ali pravni subjekti, ki bi potrebovali identiteto.

Katera koli stranka v eni izmed vlog v metasistemu, bi morala biti seznanjena z nadzorom identitete, minimalnim razkritjem identitete in omejeno uporabo ter opravičljivostjo uporabe v različne namene. Posest identitet ne bi smela predstavljati tveganja za razkritje uporabnikov, zato bi morali imeti uporabniki nadzor nad pretokom informacij o njihovih identitetah.

Predlagane rešitve naj bi zadovoljevale potrebe znotraj podjetja, spremembe pa naj bi bile potrebne šele po petih ali sedmih letih. V praksi, kjer so običajno potrebne takojšnje rešitve, bo potreba po upravljanju identitet za daljše obdobje izpolnjena z upoštevanjem karakteristik metasistema identitet.

2.5 Vprašanja s strani podjetja

Bistveni del katere koli operacije v podjetju je zmožnost identifikacije in overitve uporabnikov informacijskih sistemov do takega nivoja, da dosežemo raven, ki jo zahteva varnostna politika v podjetju, torej mora biti točno določeno, kdo dostopa do katerih podatkov s katere naprave. Seveda mora biti varnostna politika jasno določena, preden se določa, kako se bo preverjala pristnost uporabnikov in kako se bodo določali njihovi privilegiji v informacijskem sistemu.

2.6 Kakšna je realnost?

Preden se lotimo načrtovanja strategije sistema za upravljanje identitet je potrebno odgovoriti na nekatera ključna vprašanja, ki nam bodo pomagala pri samem odločanju, za kateri sistem se bomo odločali in na kakšne težave lahko naletimo:

- Koga ali kaj moramo identificirati in zakaj?
- Ali moramo vedeti ime in priimek ali nam je dovolj podatek o njegovih pooblastilih?
- Ali je poleg njegovega uporabniškega imena in gesla pomemben še kakšen podatek, ki lahko vpliva na naše poslovanje?
- Od kod bomo dobili informacijo o identiteti?
- Kaj se zgodi, če dobimo informacijo o lažni identiteti?
- Kaj se zgodi, če ne dobimo informacije o identiteti?
- Kaj se zgodi, če nas lahko nekdo zavede z lažno informacijo?

Na podlagi odgovorov na ta vprašanja se bomo lažje odločili, kakšen sistem bomo izbrali in na kakšne dodatne stroške lahko med samim poslovnim procesom naletimo.

3 Strategija podjetja pri uvedbi sistema za upravljanje z digitalnimi identitetami

V tretjem poglavju se bomo osredotočili na pojem strategija in na način, kako si podjetje zastavi svojo strategijo pri uvedbi sistema za upravljanje z digitalnimi identitetami. Pregledali bomo, katere odločitve so bistvenega pomena in zakaj je sistem za upravljanje z digitalnimi identitetami koristen. Poglavje je namenjeno tudi pregledu stanja v izbranem podjetju. Opisali bomo obstoječe postopke, ki so del sistema za upravljanje z digitalnimi identitetami.

3.1 Kaj je strategija?

»… je dobro delo organizacije in način, kako preživeti ali biti pokončan, zato ga ne smemo zanemarjati« (Sun Tzu, »Art Of War, 6. st. pr. n. št.«), je samo ena izmed mnogih definicij pojma strategija. V modernejših časih pa se strategija definira kot dolgoročen načrt dejanj, potrebnih za reševanje problemov pri doseganju določenega cilja [23]. Beseda izvira iz grških besed stratos (vojska) in ago (voditi), tudi danes se pogosto uporablja v kontekstu vojaških operacij, poleg tega pa tudi v politiki, ekonomiji in drugih dejavnostih [23].

Strategijo Henry Mintzberg v dokumentu [8] opisuje na štiri različne načine:

- strategija je nek načrt, »vodič«, ki nas pripelje iz ene točke do druge
- strategija je vzorec dogodkov skozi čas (npr. neko podjetje, ki prodaja zelo drage izdelke, uporablja strategijo »high end«)
- strategija je neka pozicija – odraža odločitve za ponudbo produktov in storitev na določeno tržišče
- strategija je neka perspektiva, vizija, smernica za naprej

Poleg naštetih definicij strategije obstaja na spletu še vrsta drugih definicij, vendar je za vsako področje specifična.

Za naše področje lahko strategijo definiramo kot skupek smernic, ki nam določajo cilje, kako bomo delali s podatki v zvezi identitetami in da bomo dosegli določene zastavljene cilje. Za načrtovanje sistema z upravljanje z identitetami torej lahko povemo, da je naša strategija:

- narediti načrt, kako izboljšati sedanje upravljanje identitet
- poenostaviti administracijo
- avtomatizirati obstoječe procese
- zmanjšati konflikte, ki nastanejo pri napačnem določanju pravic
- poskrbeti za čim boljšo dokumentacijo

Uvedba sistema vpliva na vse informacijske sisteme in postopke za dodeljevanje pravic v teh sistemih. Končni cilj je centralizirano (t. j. prek enega sistema) obvladovanje vseh pravic in dostopov do informacijskih ter drugih sredstev prek avtomatiziranih postopkov.

Podjetje, ki želi vpeljati sistem za upravljanje z digitalnimi identitetami, mora imeti jasno vizijo o tem, kako mora sistem na koncu delovati. Če je strategija podjetja že pravilno opredeljena, lahko podjetje svoje cilje sproti uresničuje in spotoma pride do želene rešitve.

Upravljanje z digitalnimi identitetami predstavlja korak naprej k povečanju varnosti in zmanjševanju tveganj v sodobnih informacijskih rešitvah. Bistvo rešitve ni le v izbranem končnem produktu, ampak v sami organizacijski strukturi podjetja, ki združuje obstoječe pravilnike, procese in informacije. Seveda pa tudi v tem, kako jasno ima podjetje določeno svojo strategijo za implementacijo rešitve v svoj informacijski sistem.

Za učinkovito implementacijo takšnega sistema je potrebno najprej določiti natančne vloge posameznikov ali pravice, potrebne za izvrševanje določene naloge v poslovnem procesu in posredno na posameznih informacijskih sistemih. Upravljanje z digitalnimi identitetami je pomembno predvsem v okoljih z veliko uporabniki ali z drugimi zakonskimi zahtevami, kjer želimo zagotoviti takojšnje ukrepanje in kjer hočemo imeti popolni nadzor nad vsemi pravicami uporabnikov. Pomanjkanje nadzora nad pravicami uporabnikov ima lahko »katastrofalne« posledice, saj so v današnjih časih informacije velikega pomena.

Ena izmed pomembnejših stvari, katere se je potrebno držati pri načrtovanju strategije, je konsistentna stopnja avtomatizacije procesov. Če si podjetje zada cilj, da bodo administratorji čim manj spreminjali pravice in dostope, bo že na pravi poti. Ravno procesi, kot so premestitve zaposlenih na druga mesta in uvajanje novo zaposlenih, nas stanejo največ časa in denarja. Z avtomatizacijo procesov bo podjetje bistveno zmanjšalo stroške in čas, porabljen za tako navidezno majhen poseg v informacijski sistem. Prav tako je pomembno pri strategiji razmišljati tudi o nadzorovanem beleženju vseh sprememb, povezanih z upravljanjem z identitetami za vse sisteme, kajti v mnogih podjetjih so med prioritetami tudi skladnost z zakonodajo, predpisi, standardi in dobro prakso. Z vpeljavo rešitve za upravljanje z digitalnimi identitetami si bo podjetje zagotovilo sledenje identitetam skozi njihov celotni življenjski cikel.

3.2 Pregled obstoječega stanja v izbranem podjetju brez sistema za upravljanje z digitalnimi identitetami

Podjetja (in posledično administratorji), ki še nimajo celovite rešitve za upravljanje z digitalnimi identitetami, imajo kar nekaj opravil ob registraciji novega uporabnika v njihov informacijski sistem. Kot primer vzemimo izbrano podjetje s približno 200 uporabniki in brez ustreznega sistema za upravljanje z digitalnimi identitetami. Že sama predstava o ročni administraciji vseh uporabnikov povzroča sive lase marsikateremu administratorju. Taka administracija obsega veliko raznih registracijskih in de-registracijskih obrazcev, ogromno obrazcev o spremembi dostopov in veliko ostalih obrazcev, ki so za vsako podjetje specifični. Kot vidimo je to velik kup papirja, katerega je potrebno urejati, ažurirati in sortirati. Upravljanje tako urejenega sistema zahteva veliko natančnosti pri delu, saj se lahko zelo hitro zgodi, da pridejo podatki v napačne roke, če je dostop do podatkov dodeljen napačni osebi. Poglejmo, kako potekajo tipične operacije v takem sistemu.

3.2.1 Registracija uporabnika

Administratorji, ki želijo novega uporabnika registrirati v svoj informacijski sistem, morajo najprej pridobiti registracijski obrazec s podatki novega uporabnika. Obrazec mora izdelati in izpolniti kadrovski oddelek, ga potrditi in poslati naprej administratorjem. Registracijski obrazec je prvi in bistveni dokument za začetek upravljanja z identitetami. Podatki, ki jih kadrovska služba vnese v registracijski obrazec, so administratorjem osnova za kreiranje identitete.

Na podlagi imena in priimka administrator ustvari unikatno uporabniško ime – identiteto uporabnika. Identiteti dodeli še svoje geslo in e-poštni naslov ter ostale atribute, kot so ime, priimek, polno ime, naslov, šifra zaposlenega itn. Množica atributov je odvisna od politike podjetja in zakonodaje države. Nekatera podjetja potrebujejo vse atribute, nekaterim so pomembni samo osnovni, kot so ime, priimek in naslov.

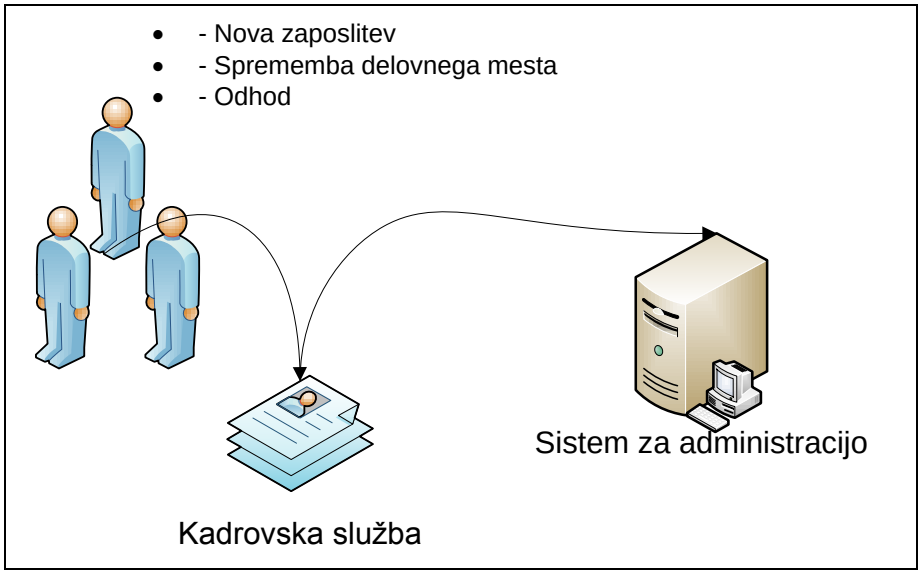
Sledi še urejanje dostopov na novo registriranemu uporabniku. Pravice in dostopi se dodajajo na podlagi izpolnjene forme. Največkrat se uporablja Windows strežniško okolje in aktivni imenik. Uporabnik je vključen v t. i. uporabniško skupino. Uporabniške skupine olajšajo sistemsko administracijo in omogočajo preprosto zagotavljanje konsistentnosti pravic in omejitev.
Če ima podjetje dobro razvito omrežje in urejen aktivni imenik, traja propagiranje pravic le nekaj trenutkov. V primeru, da je podjetje le del podjetniškega gozda, lahko traja propagiranje pravice tudi nekaj dni.
Sedaj, ko je uporabnik registriran v sistem in ima dodeljene pravice za dostop, lahko prične s svojim delom. Uporabniku se postavi delovna postaja, s katere bo dostopal do podatkov.
Administratorji ponavadi obrazec shranijo pri sebi ali pa ga pošljejo naprej v finančni oddelek. Tipični registracijski obrazec ima obliko, kot je v Prilogi 1.

3.2.2 Sprememba dostopov

Spremembe delovnih položajev v podjetjih so nekaj vsakdanjega. Zaposleni so povišani ali dobijo drugo delovno mesto znotraj podjetja. S selitvijo delovnega mesta so povezane tudi dostopne pravice, ki morajo biti spremenjene, to pa je povezano s samim upravljanjem dostopov oz. identitet.
Postopek spremembe pravic se začne v kadrovskem oddelku, ki izda odločbo za spremembo delovnega mesta in s tem poda zahtevek za spremembo dostopnih pravic v IT službo. Administrator sistema zahtevek pregleda, ga podpiše, dodeli ali odvzame ustrezne pravice in zahtevek shrani, za poznejše morebitno dokazovanje in sledenje spremembam pravic. Kot že mnogokrat poudarjeno, mora biti administrator zelo natančen pri spremembah dostopov, predvsem ne sme pozabiti odvzeti dostopnih pravic, če tako zahteva kadrovska služba.
S tem je postopek za spremembo pravic dokončan. Spremembe so opravljene, dokaz o tem, kdo je zahteval spremembo, pa je shranjen na papirju.

3.2.3 Brisanje uporabnikov oz. njihove identitete

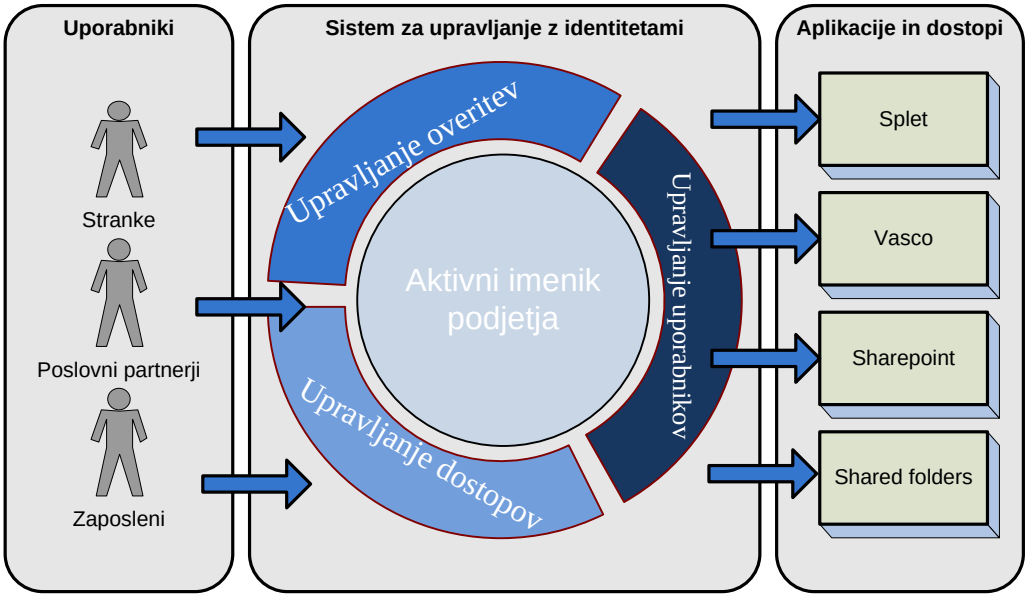
Uporabniku, ki je zapustil podjetje, mora biti onemogočen uporabniški račun, lahko se mu odvzamejo dostopne pravice ali pa je izbrisan iz sistema identitet. Ponavadi kadrovski oddelek spet izda de-registracijsko formo, na kateri so podatki o uporabniku in njegovi dostopi, katere je potrebno izbrisati. Posebej pozorni morajo biti administratorji na spletne dostope (VPN, Webmail …), saj največkrat takšen dostop ni neposredno povezan z aktivnim imenikom podjetja. Torej, administrator dostope odvzame, formo shrani ali jo pošlje naprej. Nekatera podjetja so dolžna hraniti podatke še nekaj let, druga podatke takoj zbrišejo. Hramba podatkov o neki identiteti je odvisna od politike podjetja.



Slika 2. Tipična administracija identitet v podjetju

3.3 Kako sistem za upravljanje z digitalnimi identitetami lahko pomaga?

Kot že rečeno, je sistem za upravljanje z digitalnimi identitetami proces upravljanja podatkov med uporabnikom in podjetjem. Seveda je ključnega pomena varnost e-poslovanja, da lahko podjetje posluje »zdravo« in uspešno. Brez ustreznega sistema za upravljanje identitet, se lahko pojavijo številne težave, ko želijo uporabniki (zaposleni, stranke, poslovni partnerji ali dobavitelji) dostopati do informacijskih virov podjetja. V današnjih razmerah obstaja mnogo načinov, kako lahko uporabnik dostopa do podatkov, podjetja ne smejo ogrožati odnosa s strankami, zato je nujno, da sistem deluje zanesljivo in da ne pride do administrativnih napak. Sistem za upravljanje z digitalnimi identitetami sam po sebi ni rešitev, ampak je le del strategije, da podjetje deluje učinkovito in se razvija naprej.



Slika 3. Delovanje sistema za upravljanje z digitalnimi identitetami

3.4 Poslovni razlogi za uvedbo sistema za upravljanje z digitalnimi identitetami

Veliko podjetij zavedno ali nezavedno dnevno porablja denar za upravljanje identitet, kajti stroški, povezani z administracijo, niso zanemarljivi. Zelo hiter razvoj računalniških nevarnosti, kot so računalniški vdori v sisteme (hacking), kraja elektronske dokumentacije, nezaželena pošta oz. spam, virusi in informacijski črvi, nam je zelo jasno dal vedeti, da je podatek, da vemo, kdo je pošiljal neke podatke, ključnega pomena, še bolj pa, ali je bila oseba, ki je pošiljala podatke, avtorizirana za to.

Kakšna je prava odločitev za nek produkt za upravljanje identitet? Ali se lahko zanesemo na sistem, ki ga že uporabljamo, ali je bolje kupiti kakšen tretji produkt?

Eden od tehničnih mehanizmov je PKI (The Public Key Infrastructure) in ponuja možnost overjanja in identifikacije ljudi, ki so na računalnikih, iskanje izvira iz informacij. Mehanizem sicer deluje v redu, vendar nam velikokrat ne zagotavlja celovite rešitve, saj zelo težko zadovolji vse naše potrebe, podjetja pa so zaradi tega prisiljena poiskati kakšno drugo alternativo za reševanje problematike.

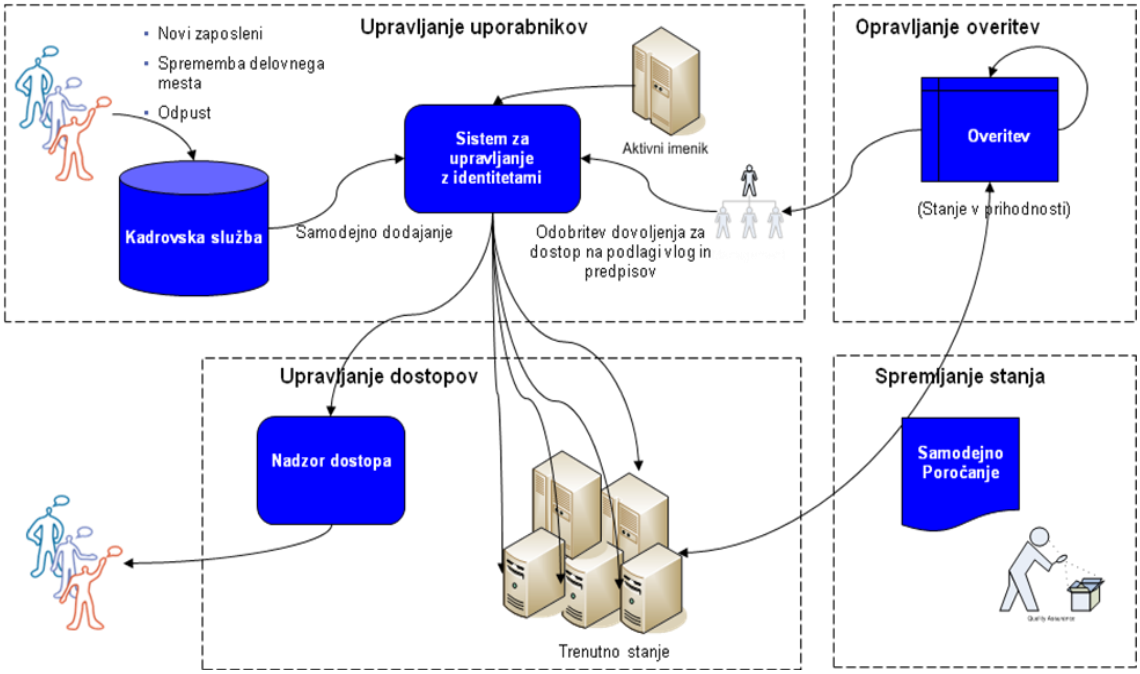
Poslovni procesi podjetjem prikažejo problematiko, povezano z upravljanjem identitet, in na podlagi skrbne analize scenarijev podjetja na lažji način določijo produkt, ki jim bo pomagal pri upravljanju.

Implementacija sistema za upravljanje identitet organizaciji zagotavlja konkurenčno prednost. Dandanes večina podjetij omogoča dostop do svojih informacijskih sistemov tudi zunanjim partnerjem ali naročnikom. Z informacijsko podprtim procesom lahko tak dostop omogočimo nemudoma in s tem zmanjšamo varnostno tveganje pri ročnih posegih ter ne izgubljamo časa. Istočasno se poveča tudi produktivnost zaposlenih, saj vse potrebne identitete za svoje delo dobijo takoj, ko nastopijo z delom, kasneje pa lahko sami upravljajo z zahtevki za spremembo dostopnih pravic in spreminjajo svoja pozabljena gesla. Upravljanje identitet bistveno zmanjšuje varnostna tveganja zaradi morebitne napačne dodelitve uporabniških pravic in zaradi neažurno odstranjenih neaktivnih identitet, hkrati pa uveljavlja dosledno in enotno varnostno politiko ter zagotavlja revizijsko sled celotnega življenjskega cikla identitet.

Upravljanje in vzdrževanje varnega informacijskega okolja je v današnjih časih zelo zahtevno, zato se mora podjetje obvarovati pred t. i. virtualnim terorizmom, pred hekerji in pred nezadovoljnimi zaposlenimi. Vzdrževanje postane še bolj zahtevno ob kaotičnih spremembah, kot so pripojitve, razne pridobitve podjetij, pri spremembah pri dobaviteljih in nenazadnje pri spremembah pozicij zaposlenih. Torej, podjetja so nenehno podvržena manjšim spremembam, ki jih je treba upravljati. Vse te zahteve pritiskajo na vodstvo podjetij, ki mora oceniti, kakšna je najboljša in ugodna rešitev za implementacijo varnega informacijskega okolja. Pri tem so najbolj izpostavljeni naslednji dejavniki:

- **Zmanjšanje stroškov –** neučinkovit sistem za upravljanje z digitalnimi identitetami povečuje stroške. Bodisi uporabniki bodisi stranke lahko čakajo predolgo na ustrezne pravice za dostop, po drugi strani pa podjetje čaka in delo stoji, čakanje na dostop in dodeljevanje pravic lahko zmanjša produktivnost. Seveda dodeljevanje pravic stane čas administratorja, poleg tega pa administrator stane podjetje. S samodejnim dodeljevanjem pravic lahko podjetje zmanjša stroške in porabljen čas za čakanje preusmeri v bolj efektivno delo.
- **Povečana varnost –** neustrezne in zastarele dostopne pravice predstavljajo nepotrebno varnostno tveganje podjetja. Z odstranitvijo neustreznih pravic, brisanjem neaktivnih uporabniških računov in rednim pregledovanjem uporabniških pravic lahko podjetje zmanjša nepotrebno tveganje.
- **Povečana skladnost s predpisi in regulativami –** s povečanjem poudarka na varovanje osebnih podatkov lahko sistem za upravljanje z digitalnimi identitetami pomaga k skladnosti podjetja z mednarodnimi standardi za varovanje osebnih podatkov. S tem lahko zmanjšamo razne zlorabe in reduciramo tveganje za neskladnost.
- **Izboljšanje kakovost storitev –** s pravočasnim dodeljevanjem pravic uporabnikom za dostop do podatkov in aplikacij imajo uporabniki možnost, da svoje delo prilagodijo na način, ki je njim najbolj domač.

- **Omogočiti enostaven razvoj novih poslovnih modelov** – razvoj lastnih aplikacij na način, da se obnovijo in dogradijo že obstoječe aplikacije, znatno pospeši nastanek novih storitev v podjetju.



Slika 4. Sistem za upravljanje z digitalnimi identitetami

3.5 Zakaj investirati v nek produkt?

Informacija o tem, kdo uporablja kateri računalnik, kateri računalnik je priklopljen v omrežje in kdo ima dostop do kakšnega vira podatkov, je v današnjih časih ključnega pomena.

V večjih omreženih sistemih je zelo težko ali skoraj nemogoče ugotoviti oz. identificirati vsakega uporabnika v sistemu. Če tehnologije, ki omogočajo identificirati uporabnika, ki je na nekem računalniku, ali poizvedeti, kdo je poslal kakšno elektronsko sporočilo ali kdo je opravil kakšen internetni nakup, ne bi bile varne, bi se virusi, lažna elektronska sporočila in internetne prevare kar vrstile, kar se v današnjih modernih časih tudi dogaja. Pomanjkanje kontrole nad temi dostopi pomeni, da bi lahko kdor koli, ki ima dostop do omrežja, pogledal, brisal in kopiral podatke, ki mu niso namenjeni. V veliko primerih gre tudi za zaupne dokumente.

Upravljanje identitet je neposredno povezano z varnostjo in produktivnostjo organizacij, ki za svoje poslovanje uporabljajo informacijske storitve. Ne samo, da si zagotovijo ustrezno varnost digitalnih vsebin, temveč lahko tudi povečajo produktivnost. Centralno upravljanje identitet zmanjšuje kompleksnost in stroške tega procesa ter hkrati dosledno uveljavlja varno politiko podjetja. Nadzorovan, jasen in pregleden proces upravljanja identitet navsezadnje

zahtevajo tudi standardi in predpisi, ki organizacijam nalagajo odgovornost nadziranja dostopov do podatkov naročnika in zaposlenih.

Preden se podjetje odloči za nakup nekega produkta za upravljanje identitet, mora vnaprej določiti, koliko denarja želi porabiti in katero področje želi pri tem izpostaviti. Na prvem mestu so seveda identifikacija in overjanje uporabnikov za računalniki in zaščita podatkov, ki krožijo po informacijskih sistemih.

4 Strateški cilji pri uvajanju sistema za upravljanje z digitalnimi identitetami

Četrto poglavje je namenjeno pregledu zadanih strateških ciljev pri uvajanju sistema za upravljanje z digitalnimi identitetami. Cilji so lahko tehnične ali organizacijske narave.

Uvedba sistema za upravljanje z digitalnimi identitetami je pravzaprav formalizacija obstoječih postopkov oziroma v večini primerov pomeni uvajanje postopkov in pravil. Prav zaradi neurejenosti okolja, v katerega uvajamo to rešitev, je običajno projekt bolj organizacijske kot tehnične narave.

Upravljanje z digitalnimi identitetami je povezano z vlogami posameznikov v podjetju. Vloge so povezane s pravilniki (politikami), ki določajo pravice na posameznih informacijskih sredstvih. Pravilniki se izvajajo po vnaprej predpisanih postopkih, ki zahtevajo v določenih primerih tudi potrditve odgovornih oseb.

Določitev vlog in pravilnikov ter vseh povezav v organizacijski strukturi organizacije je praviloma najtežji del uvedbe sistema za upravljanje z digitalnimi identitetami.

Načrtovanje sistema za upravljanje z digitalnimi identitetami poteka vedno v obstoječem stanju, kjer je treba ohraniti trenutno funkcionalnost oziroma jo le nadgraditi. Prvi korak pri uvedbi sistema za upravljanje z digitalnimi identitetami je prenos vseh uporabnikov v centralni sistem za upravljanje z digitalnimi identitetami. Prenos podatkov o uporabnikih lahko izvedemo iz katerega koli obstoječega informacijskega sistema. Običajno je najboljša rešitev prenos uporabniških podatkov iz sistema kadrovske službe (plačilne liste), saj tako zagotovimo najvišjo kakovost (točnost) prenesenih podatkov.

4.1 Tehnični cilji pri uvedbi

Glavni tehnični cilji pri uvajanju sistema za upravljanje z digitalnimi identitetami so povečanje varnosti, izboljšanje upravljanja, razpoložljivosti in možnosti integracije oziroma nadaljnje širitve uporabe tega sistema ter integracija z obstoječimi in novimi informacijskimi rešitvami.

Najpomembnejše cilje lahko predstavimo s tabelo:

Cilj	Vpliv vpeljave sistema za upravljanje z digitalnimi identitetami
Varnost	Projekt ne sme negativno vplivati na obstoječo varnostno politiko. Pred izvedbo je treba narediti oceno tveganj in uvesti dodatne kontrole ali protiukrepe za izboljšanje varnosti.
Razpoložljivost	Uporabniško okolje je treba ohraniti nespremenjeno ali uvesti novo enostavnejše okolje.
Zmanjšana administracija	Uvedba novega sistema mora biti za končnega uporabnika čim bolj nevidna. Ohraniti je treba uporabniška gesla za dostop do informacijskih sistemov. Nastavitev novih pravic mora biti enostavna in hitra.
Hitra izvedba projekta	Čim prej je potrebno zagotoviti uporabo ključnih funkcionalnosti sistema za upravljanje z digitalnimi identitetami (funkcionalnosti, zaradi katerih se uvaja upravljanje z digitalnimi identitetami).

Tabela 1. Tehnični cilji pri načrtovanju sistema za upravljanje z digitalnimi identitetami

Upravljanje z digitalnimi identitetami pomeni komunikacijo z različnimi sistemi in upravljanje s podatki na teh sistemih. Informacijski sistemi imajo različne možnosti za identifikacijo uporabnika, zato so tudi podatki v teh sistemih lahko precej različni.
Izdelki, ki jih ponujajo različni proizvajalci, zahtevajo prilagoditve, tako da hitra in enostavna rešitev ne obstaja. Programske pakete je treba ustrezno prilagoditi okolju, v katerem jih želimo uporabljati. Priporočljivo je uporabiti pomoč zunanjih partnerjev, ki že imajo izkušnje z vpeljavo sistemov za upravljanje z digitalnimi identitetami.

Pri izbiri primernega izdelka je treba pregledati celotno obstoječo infrastrukturo, vse zahteve in obstoječe veljavne postopke, ki jih je treba vgraditi v nov sistem. Izbira sistema torej ni odvisna samo od pregleda matrike izdelkov v popularnih analizah, kjer so razvidni najboljši izdelki za posamezne kategorije, ampak je treba pregledati celotno informacijsko okolje in izbrati najprimernejši izdelek.

Uvajanje rešitve za upravljanje z digitalnimi identitetami je zaradi tesne povezanosti z mnogimi procesi v organizaciji zelo občutljivo. Za zmanjšanje tveganja je v začetnih fazah vpeljave še vedno priporočljivo ohranjati star, delujoč sistem upravljanja. Najučinkovitejše je postopno uvajanje novih rešitev, ki jih ponuja sistem upravljanja z identitetami. Pred uporabo sistema v celotni organizaciji je smiselno načrtovati pilotno testiranje sistema na manjšem številu uporabnikov. S tem se izognemo pojavu začetnih napak v delovanju sistema oziroma jih pred splošnim uvajanjem rešitve pravočasno rešimo.

Izbira pilotne skupine uporabnikov mora biti premišljena, tako da lahko preverimo delovanje sistema v celotni organizaciji – zajemati mora vse postopke, ki jih želimo v določenem

trenutku predati v uporabo. Pred uvedbo novega sistema je treba načrtovati tudi ustrezno izobraževanje uporabnikov novega sistema. Predvideti moramo tudi vse potrebne procese in financiranje za vzdrževanje postavljenega sistema in širjenje njegove funkcionalnosti.

4.2 Ostali operativni cilji

Podjetje, ki bo razvijalo ali kupilo sistem za upravljanje z digitalnimi identitetami, pričakuje, da bo končna rešitev ustrezala tudi ostalim, predvsem socialnim in ekonomskim, potrebam uporabnikov sistema. Pri tem bi izpostavili nekaj najbolj ključnih problemov, ki so vzrok za nezadovoljstvo uporabnikov:

- slaba odzivnost in prilagodljivost sistema
- komplicirana uporaba
- ukradeni podatki zaradi prešibkih gesel (dokumenti, slike …)

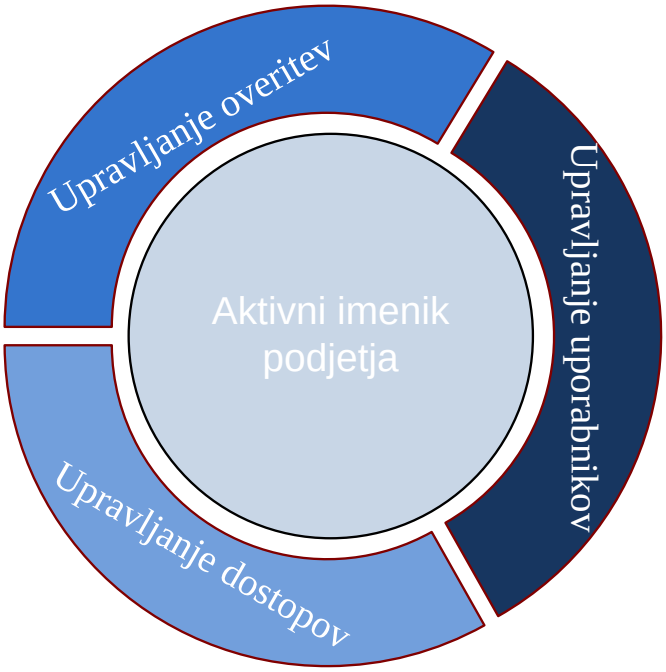
To je le nekaj stvari, na katere je potrebno biti pozoren pri uvedbi sistema za upravljanje identitet. Zlahka se zgodi, da pride do zlorabe. Zelo tipičen primer kraje podatkov se zgodi, če uporabnik zapusti svoj računalnik in se ne odjavi iz sistem. Vsakdo, ki pride mimo računalnika, ima sedaj možnost dostopa do podatkov in posledice, kot si lahko predstavljamo, so lahko zelo hude.

5 Strateške odločitve pri upravljanju z identitetami

Peto poglavje je najbolj obširno in vsebuje podroben pregled osnovnih komponent sistema za upravljanje z digitalnimi identitetami. Opisane so njihove lastnosti, njihove dobre in slabe strani. V tem poglavju najdemo bistvene značilnosti sistemov za upravljanje z digitalnimi identitetami.

5.1 Ključne komponente sistema za upravljanje z digitalnimi identitetami

Sistem za upravljanje z digitalnimi identitetami lahko razdelimo na 4 ključne komponente:



Slika 5. Komponente aktivnega imenika

Aktivni imenik podjetja sestoji iz dveh glavnih podkomponent:

- Podatkovna baza aktivnega imenika – podatkovna baza aktivnega imenika (ponavadi pravimo samo imenik) nam služi kot glavno skladišče podatkov o identiteti in o overjanju uporabnika v ogrodju sistema za upravljanje z digitalnimi identitetami.
- Povezovanje z meta imeniki – meta imenik je tehnologija, ki omogoča povezovanje in sinhronizacijo podatkov o identitetah med različnimi aktivnimi imeniki, podatkovnimi bazami in aplikacijami znotraj nekega podjetja.

V okolju, kjer je več kot pet delovnih postaj Windows, je aktivni imenik skoraj nujen, saj se administracija delovnega okolja bistveno olajša. Namesto delovne skupine (Workgroup) so delovne postaje vključene v *domeno* (domain), za katero veljajo določena pravila in ki predstavlja meje zaupanja in varnosti delovnega okolja. Tako je na primer potrebna le ena

sprememba uporabniškega gesla na eni delovni postaji v domeni in ni treba spreminjati gesla na vseh postajah v delovni skupini, če želimo izvesti prijavo v svoje delovno okolje (profil) ali imeti dostop do omrežnih sredstev (mape v skupni rabi, tiskalnik).

Bistvene prednosti aktivnega imenika so:

- kreiranje in spreminjanje uporabniških imen in gesel ter skupin uporabnikov na enem mestu – centralizirana administracija,
- varno shranjevanje uporabniških gesel,
- upravljanje s profili uporabniških računov in možnost sledenja profila (Roaming Profile),
- paleta dodatnih podatkov o uporabnikih (naslov e-pošte, telefonske številke …), po katerih lahko tudi iščemo,
- članstvo uporabnika ali skupine uporabnikov v eni ali več skupinah uporabnikov,
- lažje dodeljevanje uporabniških pravic na datotekah in tiskalnikih v skupni rabi,
- objavljanje tiskalnikov v aktivnem imeniku, ki omogoča enostavno dodajanje tiskalnikov na voljo uporabnikom na delovnih postajah,
- uporaba organizacijskih enot (Organizational Unit – OU) glede na naravo dela ali glede na lokacijo,
- nastavitev skupinskih pravilnikov (Group Policy) preko organizacijskih enot na uporabniških računih ali delovnih postajah,
- nastavitev varnostnih pravilnikov (Security policy) na delovnih postajah in uporabniških računih preko skupinskih pravilnikov,
- namestitev aplikativne programske opreme s pomočjo skupinskih pravilnikov.

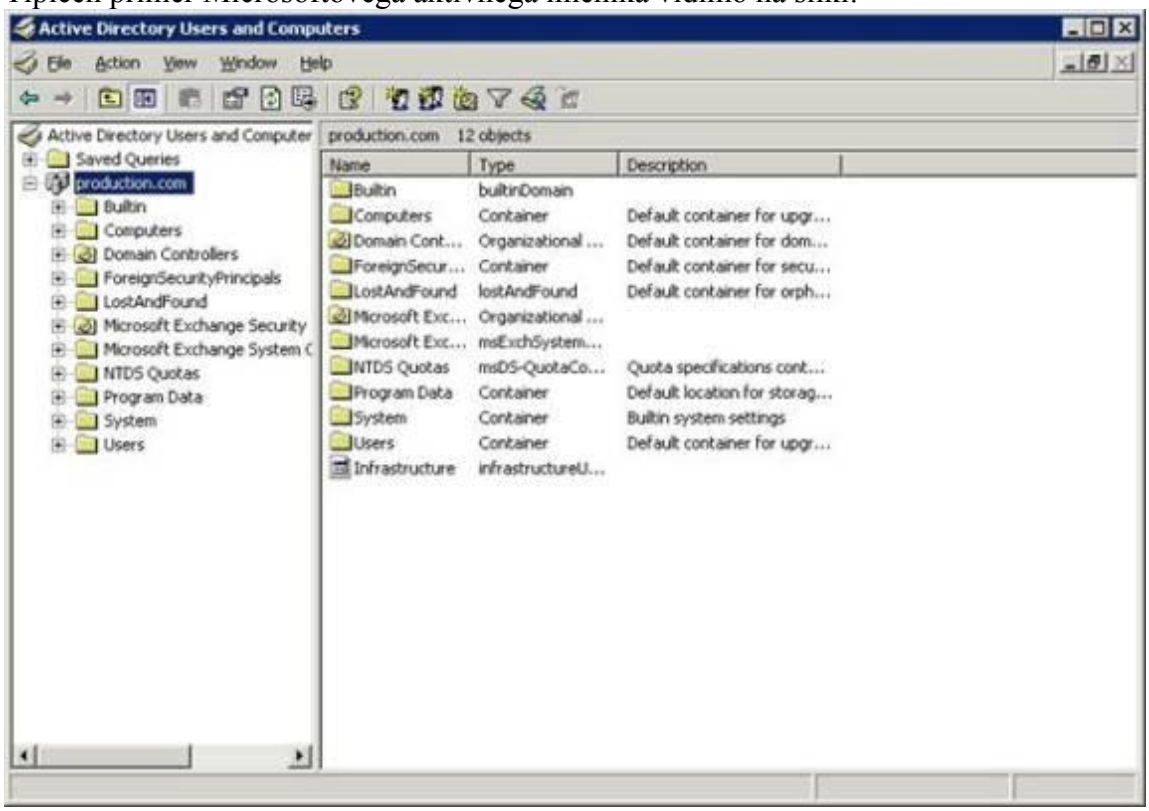
Vsaka izmed teh komponent potrebuje svojo tehnologijo, ki naslavlja različne aspekte digitalne identitete, kot so upravljanje identitet, podatki o neki identiteti, dostop do teh podatkov in sistem za shranjevanje in izmenjevanje podatkov. Te komponente lahko razvijamo ločeno, čeprav je boljše zaradi samega delovanja sistema imeti celovito rešitev.

Te komponente so ustvarjene za upravljanje celotnega življenjskega cikla identitete v nekem sistemu, od samega začetka – nastanek, do konca – brisanje.

Aktivnih imenikov je več vrst. Poleg Microsoftovega aktivnega imenika lahko omenimo še naslednje:

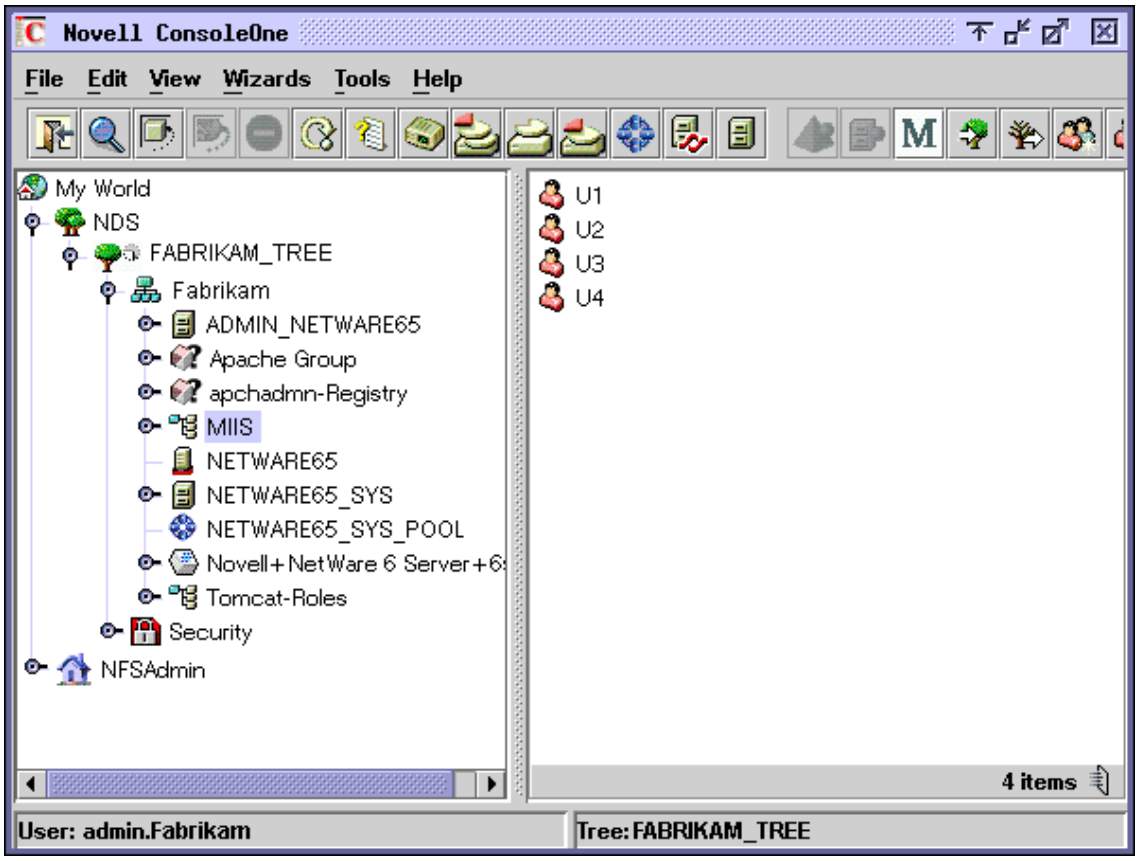
- eDirectory (Novell)
- OpenLDAP (Apple)
- RedHat Directory Server (Red Hat)
- Apache Directory Server (Apache Software Foundation)
- Oracle Internet Directory (Oracle)
- CA Directory (CA)
- Sun Java System Directory Server (Sun Microsystems)
- IBM Tivoli Directory Server (IBM)
- Siemens DirX DirectoryServer

Tipičen primer Microsoftovega aktivnega imenika vidimo na sliki:



Slika 6. Microsoft aktivni imenik

Primer imenika proizvajalca Novell (eDirectory) vidimo na spodnji sliki:



Slika 7. Novell eDirectory

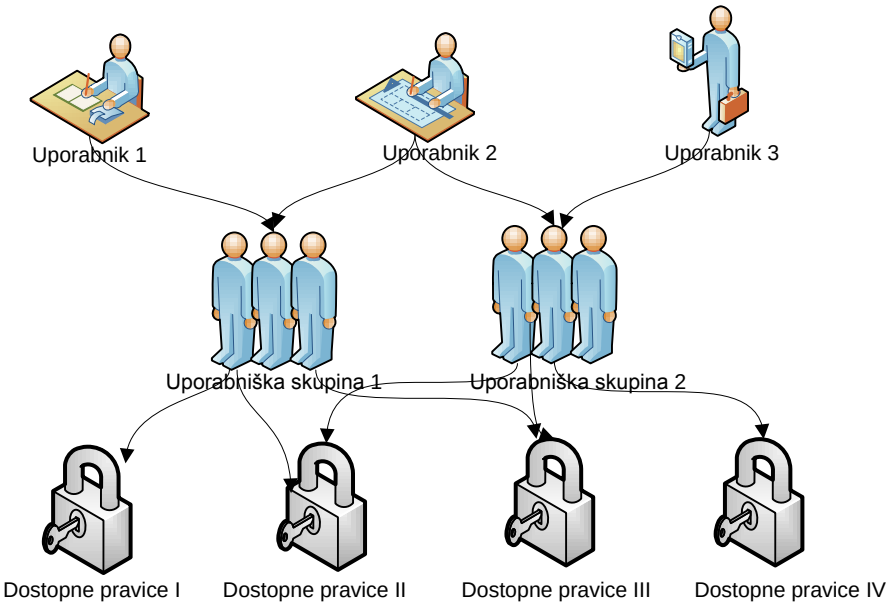
5.2 Upravljanje uporabnikov

Upravljanje uporabnikov je pojem, ki se uporablja pri opisovanju tehnologij, ki omogočajo upravljanje z velikim številom uporabnikov. Upravljanje uporabnikov omogoča določanje pravic uporabnikom v celotni infrastrukturi nekega podjetja oz. dostop do različnih aplikacij v sistemu. Kot celota upravljanje uporabnikov predstavlja ogrodje za izmenjavo podatkov iz različnih okolij in poleg tega zagotavlja njihovo doslednost, omogoča tudi t. i. Self-service in pooblaščeno upravljanje uporabnikov in podatkov.

Velika podjetja, kot so Gartner, META Group in Giga information group, so izvedla raziskave, ki so pokazale, da se podjetja soočajo z novimi izzivi, ko prehajajo na e-poslovanje in ko jim internet predstavlja medij, preko katerega poslujejo. Obseg podatkov se iz dneva v dan povečuje in tako se povečujejo tudi odgovornosti in zahteve informacijskih oddelkov v podjetjih.

Vse več podjetij poseduje različne zaupne podatke, ki pa lahko vsebujejo tudi podatke o identitetah, ki so lahko osebne narave, in ne bi smeli biti dostopni vsakomur. Zato ima vsaka skupina uporabnikov informacijskega sistema določen nivo dostopa do teh podatkov. S povečevanjem obsega podatkov in povečevanjem e-poslovanja se viša tudi zahtevana stopnja informacijske varnosti, ki pa seveda zahteva večjo pozornost in investiranje v sisteme za zagotavljanje informacijske varnosti. Vsaka nova komponenta, ki se pojavi v infrastrukturi informacijskega sistema podjetja, bodisi je to novi operacijski sistem, nova podatkovna baza, bodisi je to nov strežnik ali aplikacija, ima že vgrajene varnostne mehanizme, katere upravljamo (uporabnikom dajemo pravice za dostop) vsakega na svoj način. Vsaka komponenta doda nove atribute nekega uporabnika, nove pravice, po možnosti pa so vse dodane na svoj način.

Rezultat tega je povečana ogroženost varnosti, povečanje števila zaposlenih v informacijskih službah, cena vzdrževanja sistema zaradi tega drastično naraste, zelo pogosto se dogaja, da pride do konflikta med uporabniki in vzdrževalci zaradi netočnih informacij o uporabniku ali poteklih pravic za dostop. Navsezadnje podjetje lahko posluje z izgubo samo zaradi preveč kompliciranega administrativnega dela. Eden kritičnih faktorjev za uspešno poslovanje podjetja je ta, da podjetje identificira uporabnike hitro brez zamikov in jim na podlagi njihove identitete dodeli ustrezne pravice za dostop.



Slika 8. Upravljanje uporabnikov

Izkušnje kažejo, da je uspešnost podjetja, njegovo poslovanje s poslovnimi partnerji in njegovo povečevanje produktivnosti odvisno od nekaj predpostavk. Prvič, viri informacij morajo biti vedno na voljo in povezani, drugič, infrastruktura, ki podpira tako povezljivost, mora biti odporna in zanesljiva. Te predpostavke prevesti v realnost je šele pravi izziv za varnost informacijskega sistema.

S tega vidika obstajata dve zahtevi:

- **Zanesljivost** – zahteva, da dobijo kontroliran dostop do podatkov le ustrezni ljudje, vključno s strankami, dobavitelji, poslovnimi partnerji. S tem scenarijem ne sme priti do tega, da bi bil informacijski sistem nedostopen. Informacijska infrastruktura mora biti dostopna vedno, da lahko omogoča normalno delovanje podjetja z drugimi besedami.

- **Zagotavljanje zaščite** predstavlja obvezo podjetja, da morajo biti vsa informacijska sredstva zaščitena in s tem omogočajo zanesljivost in popolnost sistema. To pomeni, da ne smemo dovoliti prostega dostopa do informacijskega sistema za vsako poslovno sodelovanje, ampak moramo vzpostaviti varnostne mejnike, katerih se moramo držati. Največji problem tukaj je upravljanje z velikostjo (preveč informacij, preveč dogodkov) in prevelika kompleksnost sistema (različne platforme, različni protokoli …).

5.2.1 Tipični problemi, povezani z upravljanjem uporabnikov

Večina organizacij se spopada s tem, kako uporabnikom omogočiti dostop do aplikacij in virov na pravočasen in učinkovit način. Te težave so lahko naslednje:

Problemi, povezani s stroko

- Zmanjšanje produktivnosti zaradi zamud v administraciji
- Neusklajen pregled trenutnih pravic,oz. kdo ima kje dostop
- Ogrožena varnost sistemov velikih organizacij zaradi pomanjkanja celovitosti življenjskega cikla uporabnika
- Naraščajoče potrebe po poslovnem sodelovanju z drugimi podjetji
- Povečana skrb za zasebnost podatkov

Problemi, povezani s tehnologijo

- Upravljanje več »skladišč« identitet hkrati
- Večje število uporabniških imen in gesel za uporabnike in aplikacije
- Povečano število klicev v podporo uporabnikom zaradi pozabljenih gesel
- Ročno reševanje problemov v administraciji poveča možnost napak in vodi do nesprejemljivih časov za reševanje problemov
- Pomanjkanje dokumentacije o ustvarjanju ali brisanju digitalnih identitet
- Nepravilnosti in napake pri dodeljevanju uporabniških imen in pravic uporabnikov lahko pripelje do tega, da izgubimo pregled nad vsem in tako zlahka dobimo uporabniška imena v sistemu, ki nikoli ne bodo uporabljena (t. i. Osiroteli uporabniški račun)

5.2.2 Vrste sistemov za upravljanje uporabnikov

Na trgu obstaja več tipov sistemov za upravljanje uporabnikov. Osredotočili se bomo na tri najbolj pogoste:

Lastno razvit sistem

Za lastno razvit sistem se podjetje odloči takrat, ko ima na voljo zadosti programerjev, ki ga lahko programirajo. Takšen sistem je zelo specifičen, saj je narejen tako, da zadovoljuje vse potrebe uporabnikov in administratorjev. Seveda mora biti sistem dobro zasnovan, mora delovati učinkovito in mora zagotavljati visok nivo varnosti.
Pogosto se zgodi, da ravno ta sistem ne dosega svojega namena v vseh oddelkih v podjetju, ker je zasnovan premalo fleksibilno, da bi ga prilagodili vsaki potrebi podjetja. Prav tako ga ja težko spreminjati, če se podjetje odloča korenito spremeniti svoj sistem delovanja.
Samostojen sistem je velikokrat programiran tako, da ga programira več programerjev in vsak razvija svojo komponento sistema. Na koncu se komponente zložijo v celoto in tako nastane celoten sistem, vendar je prav ta »zloženost« sistema ključna za njegovo morebitno nestabilnost.

Selekcija komponent

Selekcija komponent pomeni, da podjetje odloča in kupi posamezne komponente sistemov (npr. samo aktivni imenik, sistem za nadzor dostopa …), ki jih nato zloži v celoto. Pogosto pravijo, da je to zelo smiselno, ker se lahko osredotočimo na zelo specifične dele sistema, ki ga bomo rabili, in lahko zanemarimo nepotrebne in odvečne komponente. Takšen pristop je sicer odličen, vendar pa lahko selekcioniranje postane na koncu zelo drago. Velikokrat se namreč zgodi, da prepletanje vseh komponent naredi sistem še bolj kompleksen kot je in ga ne poenostavi. Poleg tega je tudi samo sestavljanje sistema iz komponent zelo zahtevno, ker lahko pride do nekompatibilnosti.

Enotna infrastruktura

Enotna infrastruktura je najbolj pogosta vrsta sistema za upravljanje uporabnikov. Če sistem opazujemo na dolgo časovno obdobje, se izkaže, da je tudi najbolj fleksibilen sistem. Ker je izdelek celovit, ne porabimo veliko časa z njegovim sestavljanjem in ga lahko začnemo takoj uporabljati. Ko pa je sistem enkrat kompletno nastavljen in funkcionalen, nam zelo olajša vsakdanjik v podjetju. Sistem močno poenostavi IT infrastrukturo. Slabost tega je cena, ki lahko zelo drastično naraste pri podjetjih z zelo veliko uporabniki in kompleksno infrastrukturo. Poleg tega je možno, da sistem na določenih področjih ne dosega točno tistega namena kot smo si zamislili in zato ga je treba večkrat prilagoditi lastnim potrebam, kar pa je ponovno povezano z dodatnimi stroški.

5.3 Upravljanje dostopov

Splošno znano je, da je vzdrževanje varnosti velikega informacijskega sistema nujno potrebno in težko obvladljivo, saj je osebje v podpori nenehno zasedeno z raznimi servisnimi posegi, kot so ponovna nastavitev gesla in dodajanje ali odvzemanje pravic. Zelo pogosti klici v podporno službo podjetja so podobni naslednjim: »Bil sem na dopustu, pa se ne morem spomniti gesla.« ali pa »Imamo novega sodelavca na našem oddelku, rabi dostop do aplikacije, ali mu lahko to uredite?« ali pa » Napredoval sem, ali mi lahko uredite, da bom imel menedžerski dostop?«.

Tovrstni, na pogled enostavni klici, bremenijo IT osebje, saj takih klicev ni malo in si je težko na pamet zapomniti vse servisne zahteve uporabnikov. Zato se večkrat zgodi, da preprosto ne pride do sprememb pravic ali da kakšen uporabnik dobi pravice za dostop do podatkov, do katerih ne bi smel imeti dostopa. Pregled nad tem, kdo je na kakšni poziciji v podjetju, kdo ima pravice za dostop do določenega področja, postane z vsakim uporabnikom in vsakim podatkom bolj nemogoč za obvladovanje brez ustreznega upravljanja.

Upravljanje dostopov je del celovite rešitve za nadzor dostopa uporabnikov. Upravljanje dostopov se po standardih ITIL ne ukvarja z uvajanjem varnostnih standardov, ampak se ukvarja izključno in ekskluzivno z izvajanjem varnostnih pravilnikov, ki so razpoložljivi v sistemu. Po standardu ITIL izvaja upravljanje dostopov naslednje naloge:

- zahtevo za dostop,
- verifikacijo,
- dodeljevanje pravic,
- beleženje vseh dogodkov,
- sledenje spremembam oz t. i. monitoring,
- odvzemanje pravic – blokiranje dostopa.

V nadaljevanju bomo te naloge opisali malenkost bolj podrobno. S tem bomo razložili, zakaj je vsaka naloga potrebna za pravilno izvrševanje sistema za upravljanje dostopov.

Zahteva za dostop – je odlično izhodišče za definiranje procedure upravljanja dostopov, ker bi lahko različne zahteve za dostop izhajale iz že prej definiranih področij. Npr. kadrovska služba lahko naredi standardno zahtevo za dostop vedno, ko je nekdo na novo zaposlen, ali ko je nekdo prezaposlen, premeščen ali pa ko zapusti podjetje.
Torej, generalno gledano, bodo varnostni pravilniki definirali, kateri oddelki lahko zahtevajo dostop, in sistem za upravljanje dostopov bo uredil dostop in ustvaril mehanizem, kako bo dostop omogočil.

Verifikacija – glavna naloga verifikacije je preverjanje zahtev za dostop in s tem zagotavljanje, da je uporabnik, ki je zahteval dostop, res pravi in da ima uporabnik vso pravico zahtevati dostop. Obstaja več metod verifikacije, od navadnih enostavnih gesel, do biometričnih podatkov. Vendar potrebuje legitimnost zahteve še nekaj drugih verifikacijskih korakov. Na primer, zahtevamo lahko še dodatno odobritev kadrovskega oddelka in

managerja. Proces upravljanja sprememb mora vključevati tudi revizijo pravic in s tem popravljanje morebitnih napak in urejanje sprememb. Način verifikacije podjetje določi na podlagi svojih varnostnih politik, s katerimi omejuje in ureja dostop do podatkov. Samo za primer lahko navedemo, da zahteva za dostop do bančnega sistema potrebuje veliko višjo stopnjo verifikacije, kot zahteva za dodajanje novega uporabnika.

5.3.1 Dodeljevanje pravic

Ko je uporabnik preverjen, mu sistem za upravljanje dostopov dodeli ustrezne pravice, pri tem pa mora biti sam sistem seveda pozoren na morebitne konflikte. Na primer: dva različna dostopa sta bila lahko dodeljena dvema različnima uporabnikoma, vendar za samo en projekt – eden je namenjen avtorizaciji ur, porabljenih za delo na projektu, drugi za preverjanje vseh plačil za isti projekt.

Kot vidimo, imajo velika podjetja zelo veliko različnih skupin dovoljenj in pravic, zato se zlahka zgodi, da kakšen uporabnik nima ustreznih dostopnih pravic ali pa so pravice podvojene (npr. uporabnik dobi dostop kot posameznik in kot član skupine).
Sistem za upravljanje dostopov ne popravlja teh konflikto, ampak ustvarjalca zahtevka za dostop opomni na morebitne napake.

Varnostni pravilniki definirajo pravice, ki bi naj bile dostopne uporabniku, in sistem za upravljanje z dostopi te pravice dodeljuje na podlagi definicij pravic.

Ekipa, ki je zadolžena za varnost, in ekipa za upravljanje z dostopi morata tesno sodelovati in s tem vzpostaviti neko ozaveščenost znotraj dodeljevanja pravic in potencialnih navzkrižij ali vzajemnega izključevanja.

5.3.2 Nadzor dostopa - Access Control

Eden pomembnejših delov sistema za upravljanje z digitalnimi identitetami je nadzor dostopa. Nadzor dostopa je proces dodeljevanja in odvzemanja dostopa določenim osebam ali programom. Seveda je to le grobo rečeno, kajti potrebno se je osredotočiti na mnoge podrobnosti tega procesa, kot primer vzemimo:

- nekemu uporabniku želimo dodati pravice do njegovega poštnega predala, moramo pa prepovedati dostop do drugih poštnih predalov,
- banka nam dodeli dostop do našega bančnega računa, vendar nam omeji delo na njem, kot so npr. povečanje limita, limit dnevnega dviga ipd.

Kot vidimo, je možnih nešteto kombinacij dodeljevanja in odvzemanja pravic. Naš cilj pri vzpostavitvi sistema za upravljanje z digitalnimi identitetami je, da bi nadzor dostopa upravljali na nivoju identitete uporabnika.

Namen nadzora dostopa je uporabnikom zagotoviti pravilen dostop do aplikacij ali podatkov, kateri so namenjeni le njim. Včasih se srečamo tudi s pojmom Privilege Management Infrastructure ali »Permission and Policy Management, ki pravzaprav pomenita isto. To so ogrodja za varnostne rešitve, ki vključujejo nadzor dostopa, avtorizacijo uporabnika, dodajanje pravic, varnost aplikacij itd. Takšne aplikacije lahko povežejo standardne aktivne

imenike z različnimi aplikacijami širom informacijskega sistema v podjetju. Tako nam olajšajo in poenostavijo nadzor dostopa iz ene same aplikacije.

5.3.3 Skupinski pravilniki – Group Policy

Skupinski pravilnik je objekt (Group Policy Object – GPO), ki se nahaja v zbirki aktivnega imenika in vsebuje razdrobljene nastavitve obnašanja delovne postaje ali uporabnika. Vseh nastavitev je preko 700, Microsoft in drugi razvijalci opreme nenehno pripravljajo nove predloge. Pa poglejmo nekaj zanimivih nastavitev s skupinskim pravilnikom:

- preusmeritev mape Moji dokumenti (My Documents) na strežnik tako, da je uporabniku uporaba jasna in razumljiva,
- preprečitev zagona Windows Messengerja,
- nastavitev obnašanja datotek brez povezave (Offline Files),
- nastavitev omejevanja dostopa do nadzorne plošče (Control Panel),
- nastavitev omrežnih lastnosti za internetni brskalnik (Internet Explorer),
- nastavitev obnašanja Windows raziskovalca (Windows Explorer),
- nastavitev namizja in ohranjevalnika zaslona,
- nastavitev obnašanja aplikacij iz paketa Microsoft Office,
- nemotena namestitev paketa Microsoft Office in aplikacije WRQ Reflection,
- nastavitev Windowsovega požarnega zidu (Windows Service Pack 2 Firewall) itd.

Nadzor dostopa je predvsem vprašanje politike IT podjetja. Tehnologija nadzora dostopa samodejno vsiljuje politiko, ki jo IT oddelek ustvari.

Da si bomo lažje predstavljali politiko uporabe, bomo našteli nekaj primerov:

- vsi uporabniki lahko prebirajo mape in vsebine v mapah,
- vsi uporabniki, ki so se prijavili (so vnesli svoje uporabniško ime in geslo), lahko spreminjajo vsebine v mapah,
- uporabnik »Janez Novak« lahko briše določene datoteke,
- vsi uporabniki iz kadrovskega oddelka imajo pravico do vpogleda v kadrovske podatke.

Kot vidimo, se nadzor dostopa lahko stopnjuje iz osnovnega dostopa do zelo kompleksnega omejevanja. Dostop lahko dodelimo po želji, lahko ga omejimo na eno osebo, ali pa na

skupino ljudi (npr. kadrovski oddelek). Omejevanje dostopov na samo določeno osebo se v praksi izkaže kot zelo nesmiselno, saj zlahka izgubimo nadzor nad pravicami dostopov. Vsekakor se je boljše posluževati varnostnih skupin (Security Groups) in nato dostop omejevati na nivoju skupine. Na splošno je to zelo uporabno v organizacijah s frekventnim menjavanjem osebja.

5.3.4 Odgovornost

Najpomembnejše vprašanje pri nadzoru dostopa je *odgovornost.* Ponavadi delimo odgovornost na naslednje skupine:

- lastnike (owners)
- skrbnike (custodians)
- uporabnike (users)

Lastnik nekega vira je lahko oseba, ki je objekt ustvarila, lastnik objekta je lahko tudi direktor podjetja, lahko pa tudi kakšna tretja oseba, ki jo določimo, skratka lastništvo se lahko določi neki osebi ali skupini.

Skrbniki vira imenujemo tiste, ki imajo opravka s temi viri vsak dan in so odgovorni za to, da so viri vedno dostopni pravilnim ljudem. V večini primerov so lastniki virov tudi njihovi skrbniki.

Uporabnik je lahko oseba, skupina, podjetje ali program, ki ima dostop do tega vira. Njihova bistvena naloga je, da je vir zaščiten, kadar ga uporabljajo. V večini primerov so uporabniki ljudje znotraj organizacije, ki je lastnik vira.

5.3.5 Kaj obsega upravljanje dostopov?

Komponenta upravljanja dostopov, ki je del sistema za upravljanje z digitalnimi identitetami, uveljavlja varnostno politiko, ki ureja dostop do virov, kateri so zaščiteni z infrastrukturo. Vse ostale komponente – upravljanje uporabnikov, upravljanje overitev in upravljanje avtorizacij – močno vplivajo na upravljanje dostopov.

Preden se proces za implementacijo sistema za upravljanje dostopov začne, mora oddelek za upravljanje programov (PMO – Program Management Office) izdelati načrt, ki bo definiral specifične vmesne ciljne točke za implementacijo IAM v nekem podjetju. Ena izmed prvih faz vključuje razvoj projektnega načrta, ki bo obsegal vse zadane specifikacije.

Torej, predpogoja za implementacijo sistema za upravljanje dostopov sta:

- Projektni načrt in strukturna razčlenitev dela;
- Delujoč sistem za upravljanje uporabnikov in za upravljanje overitev.

Tipične konfiguracije

Upravljanje z dostopi se je v preteklosti v podjetjih implementiralo na dva načina: z razvojem svojega lastnega sistema ali pa z nabavo ustreznega že razvitega programa. Lastno razviti sistemi se pogosto ne obnesejo in niso tako efektivni kot že razviti produkti.

Kot omenjeno zgoraj, upravljanje z dostopi je stroj, ki poganja sistem za upravljanje z digitalnimi identitetami. Uveljavlja skupinske pravilnike, ki urejajo dostop do virov, ki so zaščiteni z lastno infrastrukturo. Da bi lahko upravljanje z dostopi nemoteno delovalo, rabimo naslednje komponente:

- **Vir uporabniških podatkov** – vir podatkov, ki bo infrastrukturi upravljanja z dostopi zagotavljal seznam uporabnikov, vključno z njihovimi uporabniškimi imeni in gesli, tako da lahko overitev in avtorizacija uporabnikov in dostopov avtomatsko deluje.

- **Skladišče pravilnikov** – je objekt za skladiščenje podatkov, kjer sistem za upravljanje z dostopi shranjuje svoje podatke o svojih pravilnikih.

- **Strežnik pravilnikov** – je objekt, ki izvaja overitev in avtorizacijo, ki jo zahtevajo aplikacije z varnostnega vidika. V bistvu to funkcijo izvaja skupina programskih vmesnikov in storitev na nekem strežniku.

- **Izvršilna točka** – je storitev oz. proces, ki uporabniku prepreči dostop do prepovedanih virov.

Obstajata dva glavna tipa sistemov za upravljanje z dostopi, ki se prodajajo: sistem, ki deluje s pomočjo programskih agentov (Agent-based System), in sistem brez agentov (Agentless System). Oba sistema imata svoje dobre in svoje slabe strani. Podjetje mora izbrati tak sistem, ki ne bo zahteval velikih sprememb v njegovi že obstoječi infrastrukturi.

Sistem, ki deluje s pomočjo programskih agentov, ponavadi že vključuje vir uporabniških podatkov, shrambo pravilnikov in strežnik s pravilniki. Poleg tega uporablja še majhen del procesa oz. računalniških storitev (t. i. Programski agent) za uveljavljanje pravilnikov dostopa na izvršilnih točkah (ang. enforcement points). Izvršilna točka v sistemu, ki deluje s pomočjo agentov, so ponavadi aplikacijski ali spletni strežniki znotraj omrežja.

Torej je programski agent nameščen na aplikacijskem ali spletnem strežniku.
Programski agent prestreže vso komunikacijo med uporabnikom in morebitnimi prepovedanimi viri na računalniku. S prestreženimi podatki lahko agent uveljavlja varnostno politiko in hkrati komunicira s strežnikom za pravilnike.

5.3.6 Skladiščenje pravilnikov

Sistem za upravljanje dostopov zahteva lokacijo, kjer bo shranjeval informacije, ki mu bodo omogočale pravilno odločitev za overitev in avtorizacijo. Te informacije naj bi vsebovale podatke o povezljivosti, podatke o reverse proxy nastavitvah, informacije o strežniku pravilnikov in navsezadnje seveda informacije o varnostnih pravilnikih.

Kje se pravilniki shranjujejo?

Ker je podatke potrebno nekje shraniti, je shramba pravilnikov pomembna komponenta sistema za upravljanje dostopov. Vsak sistem za upravljanje dostopov ima svoje določeno mesto za shranjevanje pravilnikov (Policy Store), ki se namesti sočasno ob namestitvi samega sistema za upravljanje dostopov. Postopek namestitve ni viden, ker se izvrši avtomatsko. V mnogih primerih je to storitev aktivnega imenika. Nekateri sistemi za upravljanje dostopov uporabljajo kombinacijo aktivnega imenika in posebne podatkovne baze. V zelo redkih primerih pa sistem za upravljanje dostopov dovoljuje po principu namestitve po želji (aktivni imenik ali podatkovna baza). To je bilo prvotno zasnovano tako, da so se lahko informacije hranile v imeniku podjetja. Pri implementaciji ostane še vedno nekaj vprašanj, na katera mora implementacijska ekipa odgovoriti, preden implementira sistem, ker bo sicer na koncu sistem deloval le omejeno in ne bo dosegal svojega prvotnega namena. Shramba pravilnikov je ključnega pomena za sistem za upravljanje dostopov, saj ne more delovati brez njega.

Odpravljanje napak v shrambi pravilnikov je največkrat omejeno na funkcionalnost sistema za upravljanje dostopov sistema. Kot omenjeno zgoraj, shramba pravilnikov je ponavadi imeniška storitev, relacijska podatkovna baza ali njuna kombinacija. To pomeni, da obstajajo različne možnosti replikacije in redundance, ki jih lahko izdelamo in vgradimo v infrastrukturo sistema za upravljanje dostopov.

Podjetje, ki bo implementiralo sistem upravljanja z digitalnimi identitetami, mora razmisliti, kako dobro bo sistem za upravljanje dostopov obvladoval sistemske napake in zato mora v ta namen izdelati sistem po takšni arhitekturi, da bo ustrezal njihovim pričakovanjem.

Sistemi za upravljanje dostopov imajo tudi sposobnost predpomnenja (ang. caching). Predpomnenje informacij o pravilnikih je odvisno od sistema, ki ga uporabljamo. Največkrat te podatke upravlja spletni agent ali obratni namestnik (reverse proxy). Izpraševanje strežnika pravilnikov se nato izvaja periodično, da se lahko predpomnilnik varnostnih dogodkov osveži. Čas osveževanja se lahko seveda poljubno nastavi, poleg tega ga lahko celo uporabljamo kot metodo za odkrivanje napak, kar pa ni priporočljivo. Uporaba predpomnilnika v te namene nam omogoča, da že overjenim uporabnikom dodelimo dostop do virov, do katerih so že dostopali (ker je pravilnik o tem dostopu še v predpomnilniku). Ampak, če želi nek novi uporabnik dostopati do nekega vira podatkov ali če nek že overjen uporabnik želi dostopati do nekega novega vira, o katerem ni pravilnikov v predpomnilniku, tega ne more storiti, ker spletni agent ali obratni namestnik ne moreta komunicirati s strežnikom pravilnikov.

Na tem mestu moramo omeniti, da sistem za upravljanje dostopov obravnava izpad strežnika pravilnikov na drugačen način. Nekateri sistemi dovolijo dostop takoj in overjajo izven svojega predpomnilnika, nato pa osvežijo svoj predpomnilnik, ko je strežnik za politike spet dosegljiv. Na drugi strani pa nekateri sistemi ustavijo vse storitve overjanja in avtorizacije, dokler strežnik pravilnikov ni spet dosegljiv.

Podjetje mora torej pri implementaciji razmisliti o mnogih stvareh, še posebej pozorno mora biti na nedelovanje strežnika pravilnikov in na podlagi tega mora svoj sistem prilagoditi tem zahtevam.

Uporaba shrambe politik

Kot omenjeno zgoraj, so tehnologije za shrambo pravilnikov ponavadi imeniške storitve ali relacijske baze. Zelo pogosto uporablja instanco imeniške storitve ali relacijske podatkovne baze za shranjevanje dodatnih informacij. To ni priporočljivo, ker so nekatere stranke omejene z resursi in kapacitetami. Ekipa, ki bo implementirala sistem, mora upoštevati to tveganje in ga mora stranki tudi pojasniti. Če se stranka s tveganjem strinja, mora podati pisno izjavo, da tveganje razume in da sprejme vso odgovornost.

Shema imenika, ki jo uporablja sistem za upravljanje dostopov, je zelo pogosto toga. Ponavadi imeniki ne sprejemajo dodatkov ali večjih sprememb, ker lahko take spremembe velikokrat ogrozijo funkcionalnost sistema za upravljanje dostopov (npr. sistem za upravljanje dostopov ne ve, kje naj locira podatke, zato ne deluje kot celota). Ekipa, ki bo implementirala sistem, mora razumeti, da dodajanje in spreminjanje sheme imenika strežnika pravilnikov ni preveč priporočljivo. Sheme so pogosto zelo obširne in vsebujejo podatkovne elemente, ki so zelo težko razumljivi, poleg tega pa so zelo pomembni pri delovanju sistema. Pogosto lahko nastopijo tudi težave pri tako velikih shemah.

Pogoste težave

Najbolj pogosta težava je določitev procesa za odkrivanje napak in redundantnost shrambe pravilnikov. Kot že večkrat omenjeno, se sistemi za upravljanje dostopov zelo razlikujejo in mnogi od njih ne morejo na enostaven način prilagoditi procesa za odkrivanje napak in redundantnost. Poleg tega različni sistemi za sistem za upravljanje dostopov obravnavajo procese vsak na svoj način. Ekipa, ki bo vpeljevala sistem, mora imeti v mislih ne samo odkrivanje napak in redundantnost shrambe politik, ampak tudi samo delovanje strežnika pravilnikov.

Vzpostavitev pravilnika

Vzpostavitev pravilnika je ena izmed najbolj kritičnih faz pri implementaciji infrastrukture sistema za upravljanje dostopov. Zelo pomembno je, da moramo natančno razumeti medsebojno povezanost upravljanja avtorizacij in upravljanja overitev.
Ozrimo se malenkost nazaj, upravljanje uporabnikov temelji na procesih in procedurah upravljanja uporabnikove identitete skozi celotni življenjski cikel uporabnika, kar vključuje tudi njegovo nastajanje.

Upravljanje avtorizacij temelji na procesih in procedurah povezovanja identitete uporabnika z njegovo vlogo oz. funkcijo v sistemu. Funkcija uporabnika v sistemu je vezana na specifične aplikacije.
Upravljanje overitev temelji na procesih in procedurah določanja kritičnosti in varnosti podatkov znotraj aplikacij in določa, kakšen nivo veljavnosti je potreben, da uporabnik dobi podatke.

Sistem za upravljanje dostopov pa je odgovoren za nadzor dostopa do omejenih virov na podlagi informacij, ki so bile oddane od ostalih IAM komponent.
Torej, če želimo uveljaviti nadzor dostopa, potrebujemo pravilnike sistema za upravljanje dostopov (nekateri produkti jih imenujejo drugače, vendar je koncept enak). Pravilnik določa, kdo dobi dostop do katerega vira in kdaj, določi, kakšen dostop je dovoljen in pod kakšnimi pogoji. Kadar se vzpostavlja pravilnik, je potrebno razmisliti o naslednjih zadevah:

- Lastništvo pravilnika.
- Na koga vpliva pravilnik?
- Na katere vire vpliva pravilnik?
- Kdaj mora biti vir dostopen (obratovalne ure, datumi, prazniki ipd.)?
- Kaj lahko uporabnik počne s podatki (branje, pisanje, spreminjanje ipd.)?
- Katera vrsta overitve se bo uporabljala?
- Od kod se bo dostopalo do virov (interni dostop, zunanji, fizična lokacija, IP naslov)?

Pravilnike lahko zaradi lažje predstave prikažemo s tabelo:

Ime pravilnika	**Dostop do katerega vira podatkov**	**Dovoljeni dostopi**	**Dovoljene spremembe**	**Avtentikacijka shema**	**Časovna omejitev**	**Zahtevani atributi**
Program X generalni dostop	/finance/*.*	Računovodski oddelek	Beri, piši	Forms	30 minute time-out	Up. ime, EMŠO
Program X Jože Novak	/share/JN/*.*	Jože Novak	beri, piši	Forms	8:00 do 17:00	Up. ime

Ko imamo zbrane podatke o aplikaciji in je tabela dostopov izpolnjena, lahko varnostne pravilnike na enostaven način kreiramo znotraj sistema za upravljanje z dostopi sistema. Preden pravilniki stopijo v veljavo, jih mora pregledati še ekipa, ki bo uporabljala program, pa tudi sistemski tehniki in nenazadnje lastnik podjetja. Verjetno se bodo morale narediti kakšne izjeme, ki se bodo izkazale v testiranju aplikacije in pravilnikov v testnem okolju.

5.4 Upravljanje overitev – Authentication Management

5.4.1 Avtentikacija oz. overitev

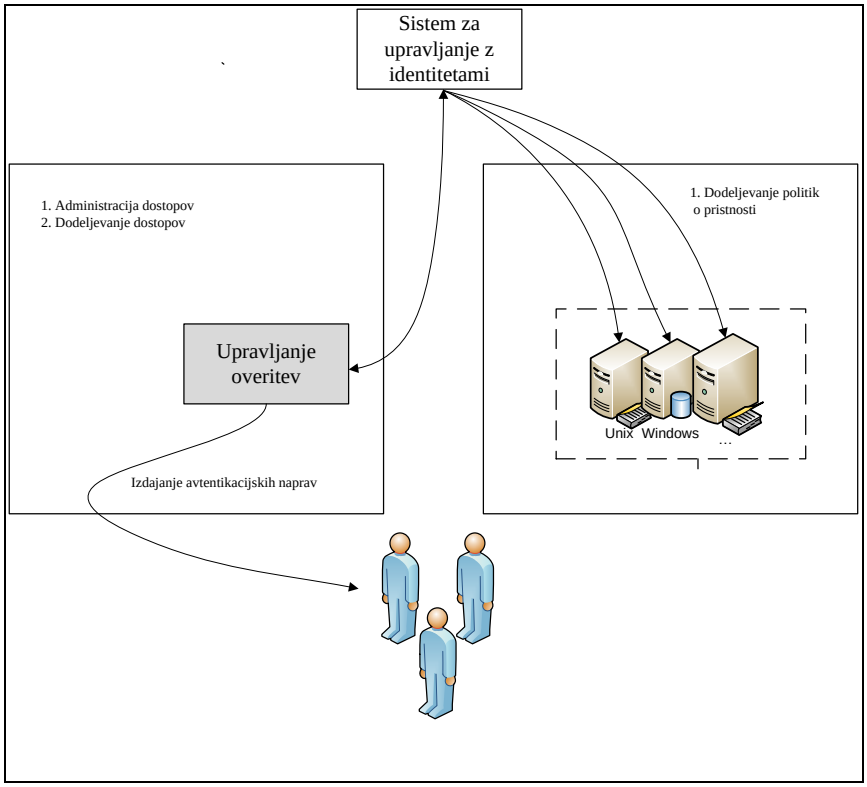
Overitev je proces, ki preveri identiteto nekega uporabnika, ki želi dostopati do zaščitenih podatkov oz. vsebin. Če so uporabniški podatki pravilni, je uporabniku dostop dovoljen, v nasprotnem primeru pa mu je zavrnjen. Uporabniki lahko kot prijavo podajo nekaj, kar vedo (uporabniško ime in geslo), nekaj, kar imajo (certifikat ali SecurID žeton), ali pa nekaj unikatnega, kar imajo (biometrični podatki, kot npr. prstni odtis), ali pa kombinacijo teh.

Overitev je proces preverjanja oz. odločanja o tem, kaj nekdo ali nekaj je in za kaj se pravzaprav izdaja [3]. V domačih in javnih omrežjih se overjanje opravlja s pomočjo dostopnih gesel. Če nekoga prepoznamo po geslu, pomeni, da prepoznamo tudi uporabnika. To je prvi pogoj za nadaljevanje procesa upravljanje identitet. Overitev odgovori na vprašanja, kot so »Kdo si?« in »Kako ti lahko zaupam?«.

V realnem svetu se moramo večkrat identificirati oz. iti skozi proces overjanja, prav tako tudi mi overjamo druge objekte okoli nas. Če na primer nekomu pokažemo svojo osebno izkaznico, se overimo in če nam nekdo pokaže svojo izkaznico, ga prepoznamo in na podlagi njegove identitete mu lahko zaupamo.

Tako imenovanim osebnim izkaznicam v informacijskem svetu pravimo »poverilnice«.

5.4.2 Zgradba sistema za overjanje



Slika 9. Sistem za upravljanje overitev

5.4.3 Sistemi za overjanje

Kot vidimo, sistemi za overjanje od nas zahtevajo neke podatke. Pogosto to vrsto podatkov povežemo s kakšnim dokumentom, ampak na splošno lahko overjanje zahtevamo:

- na podlagi nečesa, kar vemo samo mi,
- na podlagi nečesa, kar imamo samo mi,
- na podlagi tega, kar smo,
- na podlagi kombinacije zgoraj naštetega.

Naštete kriterije imenujemo *faktorji overjanja.* Lahko bi rekli, čim več faktorjev vsebuje overitev, tem bolj varna je. Največkrat se bomo srečali s pojmom *dvojna overitev*. Obstaja več sistemov za overjanje. Najpogostejši so uporabniško ime in geslo, piškotki (cookies), biometrična prepoznava, t. i. pametne kartice (Smart Cards)… Podrobneje si bomo ogledali najpogostejši način za overjanje.

Uporabniško ime in geslo

Skoraj vsak od nas ima bodisi v službi bodisi kje drugje na internetu vsaj eno posebno uporabniško ime in geslo za dostop v sistem. Ko se vpisujemo v kakšen sistem, torej, ko vtipkamo svoje uporabniško ime, se sklicujemo na našo identiteto in ko vtipkamo geslo, jo še potrdimo. Sistem nato na podlagi prepoznanega uporabniškega imena in gesla dodeli oz. dovoli imetniku identitete dostop do zahtevanih podatkov.

Upravljanje gesel

Prednost uporabniških imen in gesel je njihova enostavnost in prav to je tudi njihova slaba stran. V teoriji so gesla skrita in geslo za nek uporabniški račun ve samo ena oseba, vendar v praksi temu ni tako. Tudi gesla imajo pomanjkljivosti, kot npr.:

- Povprečen človek si lahko zapomni le omejeno število gesel (približno 8), zato si ljudje večkrat olajšajo delo tako, da uporabljajo enaka gesla za več uporabniških računov.

- Enostavna gesla lahko zelo hitro uganemo, sploh če so gesla sestavljena iz imena ali priimka. Popolna gesla bi morala biti zelo dolga, morala bi vsebovati številke in velike ter male črke, ločila in druge posebne znake, vendar si ljudje to zelo težko zapomnimo.

- Uporabnike in nekatere programe se da lahko na zelo primitiven način prelisičiti s pomočjo lažnih spletnih form (Fake login screens). Zlonamernež, ki želi ukrasti geslo, se izdaja za administratorja ali pa naredi identično vstopno stran, v katero uporabnik vtipka uporabniško ime in geslo, podatki pa se dostavijo v poštni predal zlonamerneža.

- Uporabniki so večkrat žrtve ribarjenja (ang. phishing). Phishing je v računalništvu nezakonit način zavajanja uporabnikov, namenjen pridobivanju tujih občutljivih osebnih podatkov. Pri takšnem zavajanju poskuša oseba, ki ga izvaja, pridobiti podatke, npr. številke kreditnih kartic, gesla, podatke o računih ali druge osebne podatke tako, da pod pretvezo prepriča žrtev o potrebi po posredovanju teh podatkov. Prevare »phishing« uporabniki običajno prejmejo z neželeno e-pošto ali kot pojavna okna.

- Uporabniki si gesla preprosto zapišejo na listek in ga prilepijo na računalnik ali si jih shranjujejo v datoteko na računalniku.

Poleg naštetih primerov je še več podobnih pomanjkljivosti, ki administratorjem sistemov povzročajo mnogo težav. V marsikaterem IT oddelku se zato poslužujejo politike menjavanja gesel. Uporabniki so prisiljeni, da po določenem času (npr. 30 dni) zamenjajo svoje geslo. Poleg tega lahko menjavanje gesla izboljšajo s tem, da se mora staro geslo razlikovati od prejšnjega ali pa npr. treh prejšnjih gesel. Velikokrat je zahtevana tudi kompleksnost gesel, kar pomeni, da mora imeti geslo natančno določeno dolžino, mora vsebovati velike črke, male črke in številke.

Seveda so lahko politike IT oddelkov zelo dobre in ne dovolijo zlorabe, vendar se velikokrat izkaže, da si uporabniki pač ne morejo zapomniti gesla in si ga preprosto napišejo ga listek, včasih celo nekje poleg računalnika. Zelo pogosto se dogaja, da si uporabniki geslo sestavijo

iz svojega imena, priimka, letnice rojstva, PIN kode ali imena otrok. Vsa ta gesla se lahko hitro uganejo, zato se IT oddelki večkrat odločijo za prepoved določenih fraz v geslu, največkrat pa se da metodo ugibanja preprečiti z omejitvijo števila napačnega vnosa gesla. Če se npr. geslo nekega uporabnika vnese trikrat napačno, se uporabniški račun zaklene. Edini način, da se račun odklene, je ta, da uporabnik pokliče v IT oddelek, se predstavi in zaprosi za odklep svojega računa. Varnostni mehanizem, ki se pri odklepanju lahko uporabi, je ta, da se uporabniku zastavi skrivno vprašanje. Če uporabnik pravilno odgovori na vprašanje, administrator smatra, da je uporabnik, ki želi odkleniti račun, res pravi.

Ponovna nastavitev gesla

Ponovna nastavitev gesla je enostavna procedura z vidika uporabnika, vendar je zelo »utrujajoča« za administratorje na drugi strani telefona. Razne raziskave (vir: Gartner Group) so pokazale da je vsaj 30 % klicev v IT podporo uporabnikom povezanih s ponovno nastavitvijo gesla. V velikih podjetjih to pomeni ogromen strošek, sploh če klici stanejo npr. od 35 do 55 USD. Poleg samega stroška se pojavlja tudi slaba volja uporabnikov in administratorjev.

Da bi zmanjšala stroške, so se mnoga podjetja odločila za sistem za samodejno ponastavitev gesla. Taki sistemi zmanjšujejo stroške in povečujejo produktivnost delavcev v podjetju, uporabnikom pa omogočajo, da si ponastavijo svoje geslo kdaj koli, kjer koli in brez da bi uporabnik vedel svoje staro »pozabljeno« geslo.

Eden izmed načinov samodejnega ponovnega nastavljanja gesla je ta, da sistem uporabniku zastavi vprašanje, na katerega je uporabnik že enkrat odgovoril. Ponavadi so to konzervativna vprašanja tipa »Dekliški priimek tvoje mame?« ali pa »Tvoja prva domača žival?«, lahko pa si uporabnik tudi sam izbere svoje vprašanje in odgovor nanj.
Eden izmed možnih pristopov je tudi ta, da administrator nastavi geslo na neko začasno, nato pa označi opcijo »Change password after next login« in uporabnik mora ob naslednji prijavi v sistem spremeniti geslo.

Proces včlanitve – identifikacija in registracija

Proces včlanitve oz. kreiranja novega uporabnika je najšibkejši člen (gledano z vidika informacijske varnosti) v sistemu za upravljanje identitet. To pa zaradi tega, ker vključuje mnoge mehanizme, ki so med seboj povezani. Ko je neka nova identiteta vnesena v sistem za upravljanje identitet, ji je potrebno dodati pravice za dostop, pravice za vpogled in še kakšne dodatne atribute. Preden osebo registriramo in ji dodamo unikatno ime, jo moramo preveriti. Ponavadi jo preverimo na podlagi dokumentov, ki jih dobimo, in preverimo, če imamo vse potrebne podatke, kot so ime, priimek, datum rojstva, naslov. Šele ko so vsi podatki preverjeni, osebo lahko registriramo, ji dodamo unikatno uporabniško ime, geslo in e-naslov.

Kot vidimo, se velikokrat pojavljajo pojmi registracija, identifikacija, originalna identifikacija in včlanitev. Seveda imajo v podjetju svoj pomen:

Identifikacija *je zmožnost povezovanja nekega digitalnega identifikatorja z neko osebo ali računalniško komponento v informacijskem sistemu (npr. strežnik, računalnik ...)[12]*.

Prvotna identifikacija je *pojem, ki ga uporabljamo za identifikacijo oseb na podlagi prvotnih oz. originalnih dokumentov, kot so rojstni list, potni list, osebna izkaznica [12]*.

Registracija je *proces zbiranja podatkov neke osebe in vseh ostalih podatkov, povezanih z osebo, in ki je v kontekstu s kreiranjem njihove identitete v sistemu za upravljanje identitet [12]*.

Včlanitev se *velikokrat pojavlja skupaj z registracijo – to je v bistvu celotni postopek vnašanja podatkov neke identitete v sistem za upravljanje identitet. Vključuje tako dodajanje atributov za aplikacije, kot tudi dodajanje pravic in vlog, ki so bile originalno določene za neko identiteto [12]*.

Pogoste težave, namigi in nasveti

Pri uvajanju sistema za upravljanje z digitalnimi identitetami pogosto naletimo na težave, ki jih nemalokrat težko rešimo, zato se je treba večkrat držati t. i. »metod dobrih praks« oz. preverjenih metod, ki nam zagotavljajo čim manj zapletov. Nekaj takih lahko na kratko naštejemo tukaj:

- Razvijanje in razširanje obstoječih procesov – večina podjetij ima dobro razvit sistem (bodisi samo na papirju ali v kakršni koli drugi obliki) za registracijo novih uporabnikov v obstočejih sistemov. Informacijski oddelek tesno sodeluje s kadrovskim oddelkom, zato lahko proces poteka dokaj zanesljivo, zato je ključnega pomena, da se obstoječe procedure obdržijo in preoblikujejo v avtomatične operacije, kjer bo prišlo do še manj napak. Z navidez čim manjšim posegom v delovne procese podjetja bodo manj obremenjeni uporabniki in administratorji.
- Vpeljava sistemov za overjanje dokumentov, ki so predloženi pri registraciji uporabnika. Overjanje dokumentov se velikokrat uporablja v podjetjih, kjer je identifikacijski dokument potreben za vnos v sistem za upravljanje z digitalnimi identitetami. Administratorji, ki vnašajo podatke v sistem, morajo biti ustrezno izobraženi in morajo biti sposobni prepoznati ključne fizične lastnosti dokumenta (npr. hologram, vodni žig …). Še posebej priporočljiva je vgrajena možnost za spletno preverjanje dokumenta.
- Vgrajevanje procesov za upravljanje izjem – administratorji morajo imeti navodila, kako ukrepati pri neustreznih ali pomanjkljivih registracijskih formah.
- Vgrajevanje dvojnih kontrol pri ključnih spremembah pravic – proces dodeljevanja ali odvzemanja pravic je šibak člen upravljanja z identitetami. Posebej pazljivi moramo biti pri obeh procesih, kajti napačna poteza nas lahko včasih zelo veliko stane. Priporočljiva je vgradnja dvojnih mehanizmov za potrjevanje spremembe pravic. S tem bomo zmanjšali tveganje za izgubo podatkov oz. da bi naši podatki prišli v napačne roke.

5.4.4 Single Sign-on

Single Sign-On je overitveni mehanizem, ki uporabnikom omogoča, da opravijo postopek overitve na kateri koli računalnik s samo eno prijavo v sistem oz. domeno. Takšen način overitve olajša delo administratorjem sistema, saj ima vsak uporabnik le eno uporabniško ime in geslo. Postopek je zelo udoben tudi za uporabnike, saj jim ni treba pomniti mnogih uporabniških imen in gesel, še bolj enostaven način overitve pa je s pomočjo »Smart Card« (pametne kartice), kjer gesla načeloma sploh ni treba vtipkati, ampak ga je ponavadi vseeno

treba še vpisati. Posledica tega je zmanjšanje klicev v IT oddelek in manj zahtevkov za ponovno nastavitev gesla.

Vsaka prijava na računalnik je sestavljena iz dveh delov. Najprej se uporabnik opravi t. i. »*Interaktivno prijavo«* – mora se prijaviti na lokalni računalnik in ko je enkrat prijavljen na računalnik, mora opraviti še »*Network Authentication*«. Drugi del overitve omogoča dostop do podatkov, ki so na mreži oz. na internetu.

Enotna prijava v sistem je sicer odlična rešitev, vendar pa je izpostavljena tudi določenemu tveganju. V primeru, da pride do zlorabe uporabniškega imena in gesla, ima nepooblaščena oseba dostop do vseh virov podatkov s samo eno prijavo.

Odločitev o uvedbi enotne prijave je zato v veliki meri bolj strateške narave, saj omogoča poenostavljeno vpisovanje v sisteme, olajša delo administratorjem in uporabnikom, saj jim ni potrebno shranjevati različnih gesel.

5.4.5 Stopnje overitve uporabnikov in njihova varnost

Overitvene stopnje opredeljujemo s pojmi *»nizka«, »srednja«* in *»visoka«* stopnja ali s številkami od 0 do 4. Podroben pregled sledi v tabeli [22]:

Stopnja overitve	Razvrstitev tveganja	Opis
0	Anonimni uporabnik	Transakcije, ki ne zahtevajo identifikacije uporabnika ali ne zahtevajo zaščite uporabnikove identitete.
1	Psevdonimni uporabnik	Transakcije, ki ne zahtevajo, da bi se uporabnik identificiral, ampak nudijo možnost komunikacije z uporabnikom.
2	Identificirani uporabnik	Transakcije, ki zahtevajo identifikacijo uporabnika.
3	Identificirani uporabnik in preverjena transakcija	Transakcije, ki zahtevajo identifikacijo uporabnika in preverbo transakcije.
4	Preverjanje integritete izmenjanih podatkov	Sama izmenjava podatkov je dokaz, ki označuje osebo in njeno soglasje, da je opravil transakcijo.

Tabela 2. Stopnje overitev

Opomba: Psevdonim je označevalnik nekega subjekta, v našem primeru uporabnika, ki ne izdaja pravega imena ali druge podrobnosti uporabnika.

5.5 Pregled strateških odločitev

Po temeljitem pregledu strukture sistema za upravljanje z digitalnimi identitetami je potrebno narediti pregled strateških odločitev. Namen tega je pridobiti dejanski pregled nad organizacijo sistema za upravljanje z digitalnimi identitetami. S pomočjo tabele dobimo odgovore na vprašanja, ki bodo služili kot ogrodje za načrtovanje in postavitev strategije uvajanja:

Tehnologija	Operacijski sistem	- Kako je operacijski sistem zaščiten pred nepooblaščenimi dostopi? - Na kakšen način so administratorski uporabniški računi zaščiteni? - Kako je konfiguriran požarni zid, če je nameščen?
	Omrežje	- Do kakšne mere je omrežje zaščiteno pred vdorom? - Ali se podatki, ki se pošiljajo po omrežju, kriptirajo? - Kakšno je delovanje omrežje?
	Podatkovne baze	- Kje se nahajajo podatkovne baze? Ali so za požarnim zidom in DMZ? - Kako se sledi spremembam, ki se vršijo na podatkovnih bazah? - Kako se sledi spremembam, ki jih povzročajo uporabniški računi aplikacij? - Kdo ima neposreden dostop do podatkovnih baz?
	Spletne storitve	- Kakšne spletne storitve se uporabljajo? - Do kakšne mere so spletne storitve združljive s sistemom za upravljanje z digitalnimi identitetami?
	Aktivni imenik	- Kateri imenik bomo izbrali? - Kakšna je zmogljivost imenika? - Kako je imenik združljiv z drugimi komponentami?
	Aplikacije	- Katere aplikacije bomo / že uporabljamo? - Katere aplikacije potrebujejo posebne dostopne pravice? - Kako bodo aplikacije delovale med časom vpeljave (npr. podatkovne baze …)?
Upravljanje uporabnikov	Zagotavljanje in nadzor dostopa do virov	- Kakšne tipe uporabnikov bomo nadzirali? - Do katerih aplikacij bodo uporabniki dostopali? - Kakšen dostop potrebujejo do virov podatkov?
	Upravljanje uporabniških identitet	- Kakšen sistem za upravljanje uporabnikov bomo uporabili? - Kakšna je možnost uporabe na drugi lokaciji?

	Samodejno upravljanje	- Koliko organizacijskih sprememb je potrebnih, da se lahko uporabnik sam včlani v informacijski sistem? - Kako si bo uporabnik lahko sam ponastavil geslo?
Upravljanje dostopov	Nadzor dostopa	- Kateri tip nadzora dostopa bomo uporabili? - Katere dostope bomo nadzirali? - Na kakšen način je možno slediti spremembam?
	Dodeljevanje pravic	- Kako se bodo pravice dodeljevale? - Kdo bo izvrševal dodeljevanje? - Kako se bo sledilo spremembam?
	Pravilniki	- Kateri pravilniki se bodo uveljavljali? - Kdaj bodo pravilniki veljavni? - Kako se obravnavajo morebitne izjeme? - Kako bomo organizirali skupinske pravilnike?
Upravljanje overitev	Način overjanja	- Kakšne overitve lahko uporabimo (enostavne ali zahtevne)? - Kakšne so zahteve, da lahko uporabimo SSO? - Katere podatke rabimo za overitev?
	Upravljanje gesel	- Kakšna gesla dovoljujemo? - Koliko časa uporabniku velja geslo? - Kaj se zgodi, če uporabnik geslo pozabi?
	Stopnja overitve	- Katero stopnjo overitve bomo uporabili?
Trg	Komercialni sistemi	- Ali je smiselno investirati v sistem za upravljanje z digitalnimi identitetami? - Do kakšne mere trenutni sistem ustreza zastavljenim ciljem? - Koliko sprememb / izboljšav potrebuje trenutni sistem? - Kaj lahko zamenjamo / uvedemo? - Kako bomo zamenjali samo določen del sistema za upravljanje z digitalnimi identitetami?

Tabela 3. Načrt za uvedbo sistema za upravljanje z digitalnimi identitetami

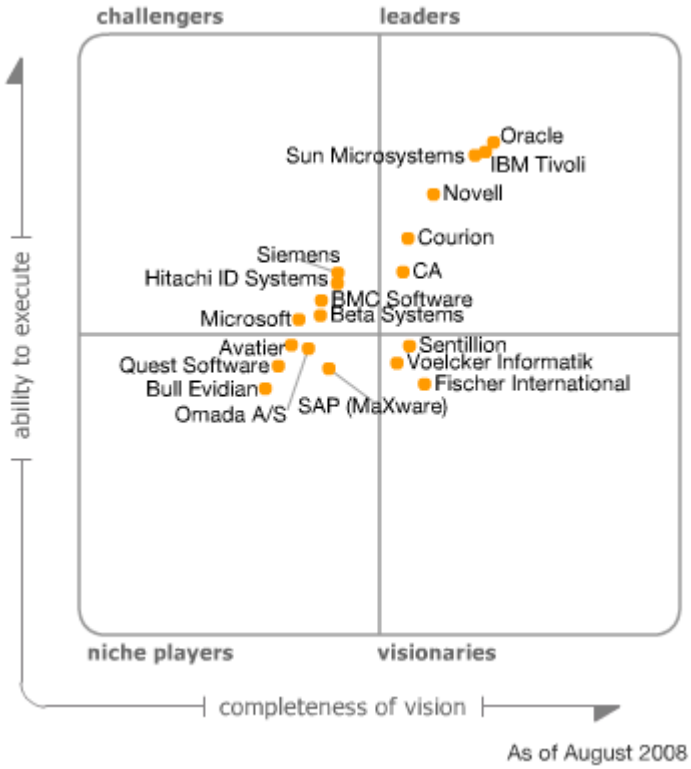
6 Primerjava najpomembnejših sistemov za upravljanje z identitetami

Namen šestega poglavja je, da bralcu prikaže kratek pregled komercialnih sistemov, ki so na voljo na trgu. Seveda gre za ogromne sisteme za upravljanje z digitalnimi identitetami, katerih cene so tudi izjemno visoke. Kratek pregled tržnih deležev bomo predstavili s pomočjo Gartnerjevih podatkov [9].

Na trgu se pojavlja več izdelkov za upravljanje z digitalnimi identitetami, med katerimi so najbolj v ospredju proizvajalci, kot so:

- IBM
- Oracle
- Novell
- Sun
- CA
- Microsoft

Poleg teh proizvajalcev se zelo dobro držijo tudi nekateri drugi proizvajalci, kot so Avatier, Quest, SAP ipd.
Iz spodnjega grafa je razvidno, kateri izdelki so najboljši med najboljšimi, kateri izdelki dosegajo svoj namen. Omenjeni graf je izvzet iz Gartnerjeve raziskave pregleda sistemov za upravljanje z digitalnimi identitetami. Lepo razviden je tudi širok nabor sistemov, ki so na tržišču in kateri so vodilni.



Slika 10. Gartnerjeva raziskava trga (vir: Gartner.com 2008)

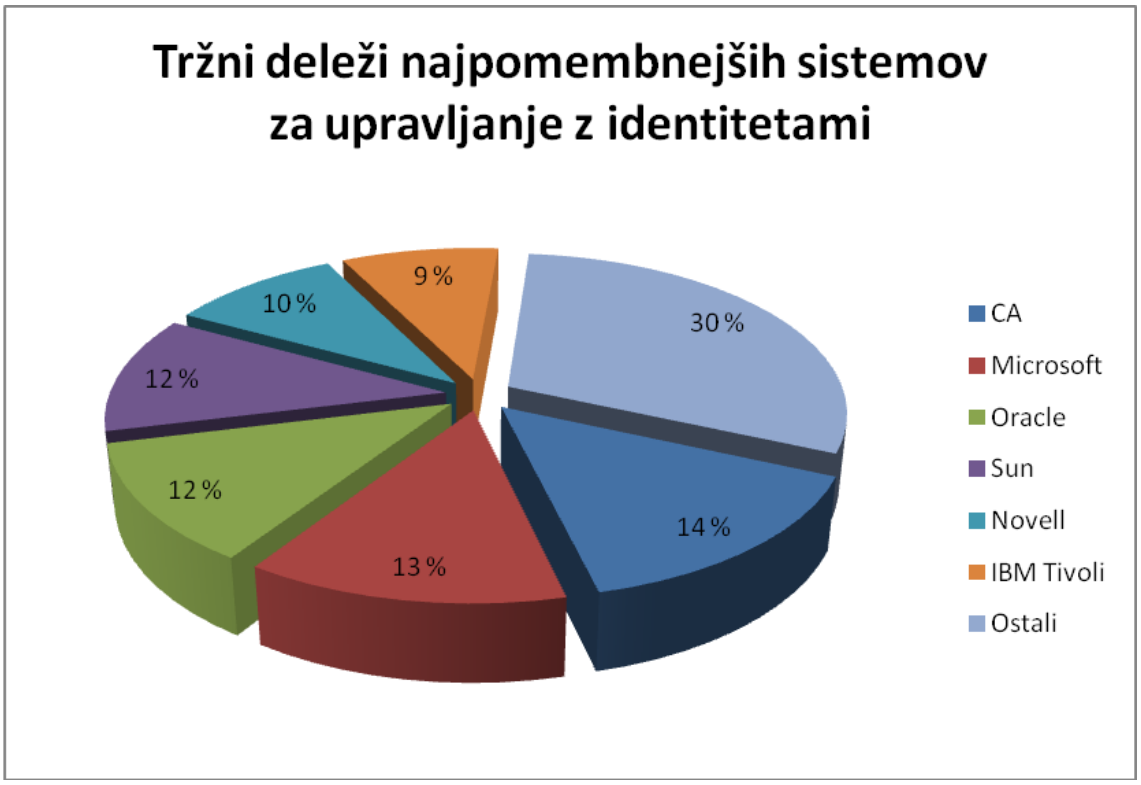
Večina sistemov vsebuje naslednje funkcije:

- upravljanje gesel
- upravljanje življenjskega cikla vloge uporabnika
- upravljanje uporabniških dostopov
- upravljanje dostopov do računalniških virov
- upravljanje ostalih uporabniških poverilnic
- sledenje spremembam identitet

6.1 Tržni deleži

Po Gartnerjevi raziskavi so tržni deleži sistemov za upravljanje z digitalnimi identitetami sledeči:

Med vsemi gre izpostaviti Oracle, ki se mu je tržni delež povečal za 48 % od leta 2006, in IBM Tivoli, kateremu se je tržni delež povečal za 36 %. Zanimivo dejstvo je, da je trenutno vodečemu CA tržni delež od leta 2006 padel za 6 %. Ostali delež predstavljajo proizvajalci in produkti (npr. Quest Software, HP, Siemens, Omada, Avatier in drugi), ki ne dosežejo več kot 4-odstotni tržni delež, zato so na grafu prikazani vsi skupaj.
Na splošno raziskave kažejo, da predstavljajo sistemi za upravljanje z digitalnimi identitetami 16,7 % prodanih izvodov od celotne prodane programske opreme.



Slika 11. Tržni deleži sistemov za upravljanje z digitalnimi identitetami

6.2 Kratek pregled vodilnih sistemov za upravljanje z digitalnimi identitetami

6.2.1 CA – CA Identity Manager release 12 (June 2008 release)

- Izboljšana tehnologija v R12 različici, izboljšani partnerski model in popravljena strategija prodaje in marketinga ponujajo možnost izobraževanja in zavedanja, česa je produkt zmožen.
- CA Identity Manager je osnovan na Identitiy Minder (2002) in eTrust Admin (2000) in zato ima za seboj dolgi repozitorij različic. Obogaten je z mnogimi izboljšavami. CA je prepoznaven kot portflej sistemov za upravljanje z digitalnimi identitetami.
- Ciljna skupina podjetja CA so večja podjetja. Več kot 60 % podjetij, ki uporabljajo sistem za upravljanje z digitalnimi identitetami, več kot 50.000 uporabnikov.
- CA igra aktivno vlogo v mednarodnih tehničnih standardih (SPML) in standardih upravljanja storitev (ITIL).
- CA Identitiy Manager ima obširni nabor funkcij, kot so zmožnost integracije, pooblaščena administracija, spletni vmesnik za urejanje …
- Kot slabost sistema se včasih izkaže preveč uporabniških vmesnikov (oken), ki bi bila lahko združena, vendar so ostale samostojne, kot posledica združevanja programov eTrust in Identity Minder.

6.2.2 IBM Tivoli Identity Manager (TIM) v.5.0 (December 2007)

- IBM Tivoli igra globalno vlogo v upravljanju storitev in se uspešno drži na trgu že 9 let. Zaradi svoje razširjenosti je nameščen v marsikaterem podjetju.
- Tivoli Identity manager je podprt na skoraj vseh platformah, torej deluje skoraj v vsakem okolju, kar je prednost.
- Ponuja simulacijo pravilnikov. Preden se nek varnostni pravilnik doda v delovno okolje, ga je možno poskusiti v testnem okolju.
- Zmožnost vpeljave certifikatov.
- IBM ima prednosti pri prodaji izdelka zaradi ugleda svojega imena in ostalih izdelkov, ki jih ponujajo na tržišču.

6.2.3 Microsoft – Microsoft ILM 2007 Feature Pack 1

- Vsebuje veliko paleto izdelkov: ILM Certificate Management, Management, Agent Software Development Kit (SDK), Identity Manager Rule Generation, Password Management Application and Password Change Notification Service.
- Zelo majhno število podjetij oz. izdelovalcev ima tako močan vpliv na trg s sistemi za upravljanje z digitalnimi identitetami, kot ga ima Microsot zaradi svojih močnih izdelkov za strežnike in računalnike.
- Microsoftov aktivni imenik in podobne tehnologije so zelo razširjeni pri mnogih korporacijah.
- Kljub konkurenci Microsoft ostaja vodilen pri cenah. Za osnovne izdelke za upravljanje z digitalnimi identitetami računa 50 do 65 % cene, ki jo ima konkurenca.
- Mnogim strankam je všeč tesna povezanost aktivnega imenika z ILM in uravnoteženost funkcionalnost / razširljivost in zapletenost ter seveda cena.

6.2.4 Novell – Novell Identity Manager v.3.5.1 (5 Oktober 2007)

- Od leta 2007 je Novell naredil precejšnji korak naprej v smeri razvoja sistemov za upravljanje z digitalnimi identitetami. Novell se s svojim razvojem osredotoča na samo en izdelek, ki pa jim ga uspeva dobro prodajati z zelo dobro podkovanim marketinškim oddelkom.
- Strategija IAM produktov Novella je poudarek na skladnosti in enotnosti varnostnih pravilnikov.
- Novell je število svojih produktov povečal z dobro integracijo v velike mednarodne korporacije, kot so Atos Orogin, in revizijsko hišo Deloitte, pa tudi s svetovnim partnerjem HP in SAP.
- Novell aktivno sodeluje pri odprtokodnih rešitvah. Deluje tudi v Linux okolju in podpira SPML.
- Novell Identity Manager je enostaven za uporabo, zato ga mnoge stranke rade uporabljajo.

6.2.5 Oracle – Oracle IAM Suite and Oracle Identity Manager v9.1

- Po zadnji Gartnerjevi raziskavi je Oracle najboljši izmed vseh proizvajalcev sistemov za upravljanje z digitalnimi identitetami. Oracle je v zadnjem letu pridobil ogromno novih strank, saj ponuja odličen izdelek, ki je izpopolnjen, ponuja veliko paleto zanimivih in uporabnih nastavitev za administratorje.
- Oraclu je uspel prodor v velika podjetja tudi v javnem sektorju kot glavnemu izdelovalcu podatkovnih baz in aplikacij.
- Podjetje na podlagi tega lobiranja uspešno prodaja svoj produkt za upravljanje z digitalnimi identitetami s pomočjo agresivnih marketinških potez.
- V novi verziji programa je vključenih dosti izboljšav, ki v preteklih verzijah niso delovale kot bi morale oz. jih sploh ni bilo.
- Oracle je uspešno integriran v velike mednarodne korporacije, kot so globalne revizijske hiše KPMG, Deloitte, PricewaterhouseCoopers in Wipro.
- Oracle IAM programi so enostavni za uporabo, prijetni na pogled, zato so tudi zelo razširjeni. Imajo odlično podporo uporabnikom, kar je zelo pomembno.

6.2.6 Sun Java System Identity Manager v.8.0

- Sun je uvrščen med najboljše 3 proizvajalce sistemov za upravljanje z digitalnimi identitetami. To jim uspeva z njihovo ekspertno tehnično platformo, njihovimi izkušnjami in dobro sistemsko integracijo.
- Sun je vodilni med proizvajalci, ki ponujajo odprtokodne rešitve. Poleg vseh ostalih produktov ponuja tudi izdelek, ki je namenjen upravljanju z identitetami.
- Identity Manager 8.0 ponuja izboljšano integracijo med upravljanjem pravic in življenjskim ciklom uporabnika, ponuja več skladnosti in izboljšano sledenje spremembam. Poleg tega se je precej izboljšal uporabniški vmesnik.
- 70 % podjetij, ki uporabljajo rešitev SUN-a, ima v sistemu več kot 50.000 uporabnikov, kar jih uvršča med ene izmed najboljših proizvajalcev, ki ponujajo rešitve za velika podjetja.

6.3 Povzetek pregleda tržišča

Vidimo, da je tržišče polno izdelkov za upravljanje z digitalnimi identitetami. Produkti so dosegli kakovostno raven storitev, kajti različice, ki so danes na voljo, so izboljšane in ponujajo vsaj 80 % vseh storitev, ki jih podjetje potrebuje. Trend zadnjih časov kaže, da je odločitev za sistem postala odgovornost vodje podjetja in ne samo vodje informacijskega oddelka. Vsak produkt ima svoje dobre strani, pa tudi slabe. Vendar, kako izbrati pravega? Kako se odločiti za produkt, ki bo ustrezal potrebam podjetja?

Večina podjetij bo najprej pogledala ceno izdelka in izbrala takšnega, ki jim cenovno ustreza in ki jim nudi vsaj osnovno upravljanje z digitalnimi identitetami. Seveda bo pomembna tudi razširljivost sistema in čas, ki bo potreben za integracijo v obstoječi informacijski sistem. Poleg omenjenega mora biti izbrani izdelovalec stabilen na trgu, imeti mora dobro zgodovino.

Druga možnost podjetja pa je v razvoju samostojnega sistema za upravljanje z digitalnimi identitetami, ki bo verjetno najbolj ugoden, vendar bo čas, potreben za integracijo in razvoj, dolgotrajen, odvisno od sposobnosti programerjev v podjetju.

7 Upravljanje življenjskega cikla prijave

Upravljanje življenjskega cikla prijave predstavlja vse aktivnosti in procedure, ki so povezane z overitvijo uporabnika.

V nadaljevanju bomo našteli nekaj od teh aktivnosti:

- Razvoj posebnega pravilnika za upravljanje gesel, ki vključujejo:
  - Konfiguracijo mininalnega standarda – npr. dolžina gesla in njegova kompleksnost (ali mora vključevati velike in male črke, številke, posebne znake).
  - Določitev časa poteka – npr. za uporabniška gesla 30 dni, za servisne administratorske račune 1 leto, za certifikate 2 leti.
  - Uprabniki se morajo pisno obvezati:
    - Da ne bodo razkrili svojega gesla;
    - Da ne bodo zlorabljali gesla;
    - Da bodo ustrezno ravnali in odgovarjali v primeru možne nevarnosti in kršitve varnosti;
    - Da bodo odgovarjali v primeru kršenja pravil.

- Razvoj posebnih procedur za upravljanje avtentikacijskih mehanizmov in izvedba izobraževanja, na katerem se prikažejo poglavitna rizična področja. Tukaj je treba poudariti način, kako uporabnike navajati na pravilno uporabo gesla in kako naj bodo pazljivi pri morebitnih zlorabah, ki se lahko vsakodnevno pojavijo v raznih oblikah, npr. ribarjenje (ang. phishing), zvabljanje (ang. pharming: nepooblaščeno preusmerjanje prometa na strežniku domenskih imen k lažnemu spletnemu mestu), socialni inženiring (ang. social engineering: vrsta napada, pri katerem napadalec prepriča uporabnika ali administratorja sistema, da mu izda avtentikacijske elemente, s katerimi se potem nelegalno prijavi v sistem) …
- Razvoj posebnih procedur za podporo uporabnikom v primeru pozabljenega gesla ali zaklenjenega uporabniškega računa.
- Razvoj postopkov za:
  - Izdajanje uporabniškega imena in gesla, kreiranje gesla kot že omenjeno zgoraj;
  - Aktivacija uporabniškega imena in gesla;
  - Preklic uporabniškega imena in gesla;
  - Zamenjava uporabniškega imena in gesla.

8 Tehnična odločitev v izbranem podjetju

Zadnje poglavje opisuje tehnično odločitev za izbrani izdelek oz. odločitev za sprejeto rešitev. Opisana sta odločena strategija in načrt sistema za upravljanje z digitalnimi identitetami izbranega podjetja.

Pregled strateških odločitev v poglavju 5 je izbranem podjetju, po pregledu vseh podrobnosti sistemov za upravljanje z digitalnimi identitetami, pomagal pri postavitvi strategije za nadaljnje delovanje podjetja.

Podjetje, ki zaposluje okrog 200 zaposlenih, se dnevno ubada s težavami uporabnikov in njihovim upravljanjem. Čeprav ima podjetje močan informacijski sistem, nekatere operacije potrebujejo izboljšanje. Cilj izbranega podjetja je bil jasno določen. Potrebno bo nadaljevati svojo strategijo, razširiti cilje in sčasoma pridobiti celovito lastno rešitev, lahko pa bi investirali v nov izdelek in celotno infrastrukturo postavili na novo.

Ker se nahajamo v ekonomsko težkih časih in vemo, da obstoječi produkti za upravljanje z digitalnimi identitetami niso poceni, je podjetje ostalo pri svoji obstoječi infrastrukturi, saj zaenkrat deluje zanesljivo.

8.1 Tehnični pregled

Pri pregledu tehničnih karakteristik ugotovimo, da delujejo v izbranem podjetju vsi strežniki na platformi Microsoft Windows Server 2003 ali 2008. Trdi diski v strežnikih so kriptirani z ustrezno programsko opremo, uporabniški računi za dostop do strežnikov so zaščiteni. Vsi strežniki pa se nahajajo za požarnim zidom, kar pomeni, da so do neke mere zaščiteni pred vdori.

Omrežje poganja Cisco mrežna oprema, struktura omrežja je dobro zasnovana, omrežje naj bi bilo po prepričanju administratorjev zanesljivo.

Vse podatkovne baze so na strežnikih, ki so za požarnim zidom. Spremembe, ki se vršijo na podatkovnih bazah, so vidne v sistemski dnevnikih. Neposredni dostop do baze imajo samo administratorji, vendar ga potrebujejo le redko.

Podjetje že nekaj časa uporablja Microsoftov aktivni imenik za hrambo uporabniških računov, gesel in računalnikov. Struktura aktivnega imenika v podjetju je urejena in ažurna. Strateško gledano se je podjetje v tej točki izkazalo zelo dobro, saj dosega vse postavljene cilje. Ostali produkti v informacijskem sistemu podjetja so Microsoftovi, zato podjetje nima težav z združljivostjo z ostalimi komponentami. Zaposleni preko spleta dostopajo le do pošte, na voljo imajo tudi VPN povezavo. Overjanje poteka preko LDAP protokola.

Aplikacije, ki jih podjetje že uporablja, v sistemu ne potrebujejo posebnih dostopnih pravic. Tiste, ki jih potrebujejo, imajo svoj poseben uporabniški račun z določenimi pravicami.

8.2 Pregled z vidika upravljanja digitalnih identitet

Aktivni imenik podjetja vsebuje vse uporabnike sistema, domenske administratorje, račune računalnikov in strežnikov v sistemu. Aplikacije, ki omogočajo LDAP overitev, uporabljajo to storitev za preverjanje uporabniških dostopov. Uporabniki imajo dostop do vnaprej določenih mrežnih pogonov in mrežnih tiskalnikov.

Uporabniki se ne morejo sami včlaniti v aktivni imenik, to mora storiti administrator, lahko pa si sami spremenijo geslo. Če uporabnik pozabi geslo ali pa se mu zaklene uporabniški račun, mora to sporočiti administratorju, ki mu uporabniški račun odklene na podlagi skrivnega vprašanja in pravilnega odgovora nanj.

Kompleksnost gesla je nastavljena na nivo, da morajo uporabniki v geslu uporabiti vsaj tri različne nabore znakov. Uporabniško geslo poteče po 60. dnevih in ob zamenjavi ne sme biti enako petim prejšnjim geslom.

Pravice za dostop določajo administratorji s pomočjo skupinskih pravilnikov. Podjetje ima tudi omogočen Single Sign-On. Ker ima podjetje dve poslovni enoti na oddaljenih lokacijah, se uporabniki lahko prijavijo v omrežje tudi iz oddaljenih lokacij, saj so pisarne povezane preko VPN.

8.3 Povzetek tehnoloških odločitev

Če povzamemo zgoraj omenjene tehnične odločitve, ki so v dobri meri že obstajale, lahko povemo, da je izbrano podjetje na dobri poti do lastne izvedbe sistema za upravljanje z digitalnimi identitetami. Aktivni imenik, ki je baza vseh uporabnikov, dostopnih pravic in dostopov, je ustrezno pripravljen za nadaljnjo razširitev. Uporabnike sistem overja na podlagi uporabniškega imena in gesla. Aktivni imenik poskrbi za shranjevanje gesel, vzpostavljeni so pravilniki, ki določajo zgradbo gesla.

Podjetju manjka nadzor nad dostopi, prav tako je premalo sledenja spremembam. S tem je mišljeno pomanjkanje dokumentacije o spremembah uporabniških pravic, sprememba uporabniških dostopov in spremembah o uporabniških računih nasploh. Vsaka sprememba bi v tako organiziranem sistemu morala biti dokumentirana oz. zabeležena v nekem dnevniku. Sicer se administratorji poslužujejo pregledovanja sistemskih dnevnikov, vendar ti dnevniki bolj ali manj ne prikazujejo želenih podatkov. Predlagamo lahko, da podjetje razvije lastno aplikacijo, ki bo beležila dostope in spremembe dostopov.

Da bi bil lastni sistem za upravljanje z digitalnimi identitetami v podjetju popolnoma integriran, potrebuje podjetje postopke za avtomatizacijo procesov. Administratorji izgubljajo preveč časa z urejanjem uporabniških dostopov in s samo administracijo uporabnikov na splošno. Podjetje potrebuje aplikacijo ali dodatek k obstoječemu aktivnemu imeniku, ki bo zmožen samodejne administracije uporabnikov. Politika podjetja prepoveduje integracijo tretjega proizvajalca, zato bo potreben lastni razvoj.

Tabela iz poglavja 5 je bila osnova za tehnično odločitev podjetja pri načrtovanju strategije sistema za upravljanje z digitalnimi identitetami. Odgovorili smo na zastavljena vprašanja in

dobili paket odgovorov, ki bodo služili za nadaljnje projekte informacijskega oddelka podjetja.

Čeprav je podjetje tehnično zelo dovršeno, bo potrebno še kar nekaj velikih organizacijskih sprememb, kar se tiče sledenja spremembam. Trenutno se namreč spremembe beležijo samo na papirju. Torej, administrator mora vedno, ko naredi spremembo, svoje opravilo zabeležiti. Postopek je zamuden, večkrat pa za to opravilo zmanjka časa in tako pride do pomanjkanja dokumentacije.

Strategija podjetja za uvedbo sistema za upravljanje z identitetami je zastavljena dolgoročno. Zastavljene cilje bo podjetje doseglo postopoma, saj bo potrebno razširiti obstoječi informacijski sistem, dodelati procedure. Posegi v infrastrukturo informacijskega sistema so na videz enostavni, vendar temu ni tako. Take spremembe, ki bodo morale biti vpeljane v obstoječi sistem izbranega podjetja, ne bodo enostavne. Zahtevale bodo veliko odgovornega dela in porabljenega časa.

9 Zaključek

Poglavje o upravljanju z identitetami je, kot vidimo, zelo obširno in zadnje čase postaja vse bolj aktualno. Kljub temu nam primanjkuje literature na spletu in v knjižnicah, saj sem imel pri pisanju diplomske naloge težave s pridobivanjem gradiva. Po eni strani nam izdelovalci programske opreme dnevno polnijo poštne predale s komercialnim materialom, ki so vsak po svoje specifični za izdelke na trgu in so bolj reklama, kot pa neka generalno uporabna literatura, kot pomoč pri uvedbi sistema za upravljanje z digitalnimi identitetami.

Pričujoče diplomske naloge sem se lotil s teoretičnega vidika o upravljanju z digitalnimi identitetami. Preveril sem, s kakšnimi problemi se organizacije srečujejo pri upravljanju in zakaj je avtomatizirana rešitev nujno potrebna ali pa vsaj zaželena. Lotil sem se tudi tehničnega pregleda sistema, opredelil sem njegove komponente in jih podrobneje opisal. Da bi se podjetje lažje odločilo za pristop k uvedbi sistema, sem opisal, kakšne lastno razvite sisteme poznamo in kakšne so najpogostejše metode za lastno izdelavo sistema. Po drugi strani pa sem pregledal, kakšno je stanje na trgu s podobnimi izdelki, predstavil sem njihove tržne deleže in na kratko opisal lastnosti posameznih (vodilnih) izdelovalcev.

Diplomska naloga obsega dovolj osnovnih informacij, ki jih organizacija potrebuje, če premišljuje o uvedbi sistema za upravljanje z digitalnimi identitetami. Zaradi zelo obširne tematike ne zajema celotne problematike s tega področja, ponuja pa osnovni pregled vsakdanjih težav informacijskih oddelkov.

Ker sem tudi sam administrator in se dnevno ukvarjam s tematiko upravljanja identitet, je bilo pisanje diplomske naloge zelo koristno zame, saj sem sproti ugotavljal dobre in slabe lastnosti sistema, ki ga uporabljamo pri nas. Povrh vsega sem ugotovil tudi kakšno bi bilo moje delo, če bi uporabljali najboljši sistem za upravljanje za identitet, ki je trenutno na trgu. Sicer pa zlato pravilo sistemskih administratorjev pravi »Don't change a working system« in dokler sistem deluje, ga ni potrebno zamenjavati.

Seznam slik

Seznam tabel

Priloge

Obrazec za registracijo novega uporabnika

Osnovni podatki	
Številka zaposlenega	
Priimek	
Ime	
Uporabniško ime	
Geslo	
e-naslov	

Podatki o dostopih		
Številka dostopne kartice		
Dostop do prostorov	☐ Nadstropje I ☐ Nadstropje II ☐ Nadstropje III	☐ Tehnični prostori ☐ Garaža ☐ Vse
Dostopi do mrežnih pogonov	☐ Mrežni pogon 1 ☐ Mrežni pogon 1	☐ Mrežni pogon 3
Posebne pravice		
Distribucijska lista		

Kadrovski podatki		
Številka zaposlenega		
Oddelek		
Delovno mesto		
Naziv		
Tip zaposlitve	☐ Redna zaposlitev ☐ Honorarna zaposlitev	☐ Določen čas ☐ Nedoločen čas

Kadrovski oddelek **Vodja Oddelka**

Podpis: _____ **Podpis: _____**

IT oddelek **Direktor**

Podpis: _____ **Podpis: _____**

Priloga 1.Obrazec za registracijo novega uporabnika

Literatura

[1] Active Directory Architecture, Microsoft Technet, 2009 dostopno na: http://technet.microsot.com/en-us/library/bb727030.aspx (marec 2009)

[2] Ahuja Jay, Identity Management: A Business Strategy for Collaborative Commerce (2004)

[3] Authentication Definitions, dostopno na: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html (oktober 2009)

[4] Bilhar Mann, Computer Associates International: Seven Habits of high effective identity management, dostopno na: http://www.computerworld.com/s/article/95200/Seven_habits_of_highly_effective_identity_management?taxonomyId=17&pageNumber=2 (oktober 2009)

[5] Ciglarič, M., Krevl, A., Pančur, M.: Strategija upravljanja z digitalnimi identitetami na Univerzi v Ljubljani, različica 1.0, Univerza v Ljubljani, april 2008.

[6] Commercial off-the-shelf products, dostopno na: http://en.wikipedia.org/wiki/Commercial_off-the-shelf (april 2009)

[7] Dr. S Jagannathan, Head of Technological Innovation, Patent and Publication: Social Network and Identity Management SIM- 2009, dostopno na:http://www.iimahd.ernet.in/sim09/Speakers/S_Jagannathan.pdf (maj 2009)

[8] Fred Nickols, Strategy: Definitions and Meaning, dostopno na: http://home.att.net/~nickols/strategy_definition.htm (oktober 2009)

[9] Gartner Research: Magic Quadrant for User Provisioning (julij 2008), dostopno na: http://www.gartner.com (september 2009)

[10] IT Solutions: Automated Password Reset through Speech Recognition, dostopno na: http://www.voiceport.net/PasswordReset.aspx (avgust 2009)

[11] Kaufman Kevin, GIAC Security Essentials Certification (GSEC) Practical Assignment, (2003)

[12] Lynn C. Lawton, Henny, J. Claessems: ISACA, CISA Review Manual (2009)

[13] Marand.si: Rešitve za celovito upravljanje identitet uporabnikov, dostopno na: http://www.marand.si/resitve/upravljanje-identitet/ (junij 2009)

[14] McQuaide Bill, Identity and Access Management - Transforming E-security into a Catalyst for Competitive Advantage, (2003)

[15] MojMikro.si: Upravljanje digitalnih identitet, dostopno na: http://www.mojmikro.si/mreza/uporabno/upravljanje_digitalnih_identitet (september 2009)

[16] Pfitzmann, A., Hansen, M.: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version v0.31 Feb. 15, 2008), dostopno na http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[17] Praprotnik Marko, SIMT d.o.o.; Ena identiteta za enega uporabnika, objavljeno v časniku Finance št. 90, str. 32 z dne 13. maja 2008

[18] Sarva Srinivas , CISA, AICWAI, Cost-effective Implementation of Identity Management, (2005)

[19] Srečanje Technet ESS: Kriza digitalne identitete v heterogenem okolju, Rafal Lukawiecki (Project Botticelli), dostopno na: http://home.izum.si/COBISS/OZ/2006_1-2/html/clanek_07.html (julij 2009)

[20] Sun Identity Management Solutions,dostopno na: http://www.sun.com/software/products/identity/index.jsp (maj 2009)

[21] Syngress, Creating Security Policies And Implementing Identity Management With Active Directory, (2003)

[22] Verdonik, Ivan: revija Monitor, članek z naslovom: Varnostni vidiki Windows 2000, dostopno na: http://www.freeweb.siol.net/ivanver1/ (september 2009)

[23] Wikipedia: Strategija, dostopno na: http://sl.wikipedia.org/wiki/Strategija (oktober 2009)

[24] Windley Phillip J. (O'Reilly Media): Digital identitiy – Poglavje 7, (2005)

[25] ZPS: Lažno predstavljanje ali »phishing«, dostopno na: http://www.zps.si/racunalnik-in-telefon/internet/lazno-predstavljanje-ali-phishing.html?Itemid=311 (september 2009)