UNIVERZA V NOVI GORICI
POSLOVNO-TEHNIŠKA FAKULTETA

INFORMACIJSKA VARNOST PODJETIJ NA GORIŠKEM

DIPLOMSKO DELO

Sani Šeraj

Mentor: mag. Peter Černe

Nova Gorica, 2009

NASLOV

Informacijska varnost podjetij na Goriškem

IZVLEČEK

V diplomskem delu so s teoretskega vidika prikazani standardi in priporočila za informacijsko varnost, ki so najpogosteje uporabljeni pri oblikovanju ustrezne strukture informacijske varnosti v podjetjih. Zagotavljanje varnosti v organizaciji je podrobneje predstavljeno, predvsem pa sistem za upravljanje informacijske varnosti, varnostna politika ter nivoji organizacijske varnosti. Prikazane so vrste brezžičnih lokalnih omrežij, njihove prednosti, slabosti ter varnost oziroma zaščita takih omrežij. Brez protokolov, ki nastopajo ob vzpostavitvi povezav, današnji način dela ne bi obstajal. Predstavljeno je delovanje teh protokolov.

Cilji diplomskega dela so: opis standardov in priporočil s področja informacijske varnosti, predstavitev načinov zagotavljanja varnosti, priprava priporočil za podjetja glede informacijske varnosti ter prikaz implementacije informacijskega sistema v podjetju.

V diplomskem delu pa je z analizo odgovorov na anketo, ki so jo izpolnila podjetja, prikazano dejansko stanje informacijske varnosti v goriški regiji. Glede na rezultate in obdelavo anket smo pripravili splošna priporočila, na podlagi katerih podjetja lahko preverijo stanje svoje zaščite. Formirana so priporočila, s katerimi podjetjem predlagamo popravke informacijskega sistema. Prikazan je tudi primer podjetja, za katerega smo implementirali tako strojno kot programsko opremo ter poskrbeli za njegovo informacijsko varnost.

KLJUČNE BESEDE

Sistem za upravljanje informacijske varnosti (SUIV), diskovna polja (RAID), navidezno zasebno omrežje (VPN), varnost internetnega protokola (IPsec), strežnik, računalniški virus

TITLE

Information security of companies in the Goriška region

ABSTRACT

In the bachelor thesis, standards and recommendations for information security most widely used while designing the appropriate structure of information security in companies are presented from theoretical point of view. The processes of providing security within an organisation are described in detail, especially the *Information Security Management System*, the security policy and the levels of organisation's security. Types of wireless local area networks are presented, their pros and cons, as well as the level of security and types of protection for such networks. The present-day system would never exist without protocols which are activated at connection establishment. The functioning of those protocols is described.

The objectives of the thesis are: a description of standards and recommendations in the field of information security, presentation of ways to ensure the information security of companies, and implementation of an information system in an enterprise.

In the thesis the actual situation in terms of information security in the Goriška region is presented through a questionnaire filled in by the investigated companies. Recommendations are given on the basis of which companies can check the state of their protection. Furthermore, recommendations are given on how companies could improve their information system. An example of a company is included for which we implemented hardware and software, as well as provided information security.

KEYWORDS

Information security management system (ISMS), redundant array of independent disks (RAID), virtual private network (VPN), internet protocol security (IPsec), server, computer virus

KAZALO

KAZALO SLIK

KAZALO TABEL

1 UVOD

V današnjem času, ko je svet računalništva in informatike zelo prisoten tako v življenju posameznika kot tudi v manjših in večjih organizacijah, si je težko zamisliti podjetje brez ustrezne računalniške in informacijske infrastrukture.

Vdori in zlorabe v računalniška omrežja se dogajajo vsak dan in naloga vsakega podjetja je, da te zlorabe prepreči. Vsaka organizacija bi si morala zagotoviti varnost podatkov ter si zavarovati poti do teh. Osveščenost o varnostni politiki je v podjetjih velikokrat nizka. Podjetja se ne zavedajo tveganj, ki jih lahko povzročajo varnostne luknje v njihovih sistemih.

Pojem varnosti je star vsaj toliko kot človeštvo. Začetki zanimanja za informacijsko varnost (ali varnost informacijskih sistemov) segajo v leto 1964, ko so prvi računalniški inženirji ugotovili, da je potrebno tudi podatke v elektronski obliki primerno varovati. Informacijska varnost je pridobila na pomenu predvsem v zadnjih nekaj letih s pojavom omrežij ter hitrim in stalnim napredkom v razvoju računalniške tehnologije. Dejstvo je, da sedanji časi zaznamujejo številne tehnološke, organizacijske in poslovne spremembe. S pojavom večjega števila računalniških komponent (strojnih in programskih) se je eksponentno povečalo tudi število možnih varnostnih groženj. Žal pa za varnostno osveščenost uporabnikov informacijske tehnologije ni značilna eksponentna rast, povečuje se kvečjemu linearno.

1.1 Področje diplomskega dela in obravnavana problematika

Področje diplomskega dela je analiza in ugotavljanje informacijske varnosti podjetij, pri čemer smo se osredotočili na informacijsko infrastrukturo ter njen pomen v podjetjih. Mnogo podjetij še vedno ne prepoznava tveganja in izgub zaradi nezadostne varnosti informacijskih sistemov. Informacije imajo za podjetja dejansko iz dneva v dan večjo vrednost ter so vsak dan podvržene vedno novim nevarnostim in zlorabam. To predstavlja velik strošek v podjetjih ter velik vložek in nujno investicijo, ki prepreči marsikatero nevšečnost v primeru izgube pomembnih poslovnih podatkov. Z diplomskim delom smo se približali temi, ki je v današnjem svetu vse bolj pomembna in nujna za poslovanje.

Za uspešen poslovni rezultat so stroški zelo pomembni, vendar pri postavitvi ustrezne informacijske varnosti to ne sme biti primarno vprašanje, saj nezadostna informacijska varnost lahko pripelje do še večjih izgub. Zelo pomembni dejavniki pri poslovanju so zaupni poslovni podatki, nemoteno poslovanje, obvladovanje in obdelovanje podatkov, ki morajo zagotavljati nemoten pretok informacij in biti ustrezno varnostno zaščiteni. Poleg tega bi radi predlagali rešitev in predlog postavitve varnega informacijskega sistema v nekem podjetju ter s tem ponudili rešitev za marsikatero težavo.

1.2 Cilji in namen diplomskega dela

Glavni cilj diplomskega dela je z analizo informacijske varnosti podjetij na Goriškem ugotoviti, ali so podjetja ustrezno varnostno zaščitena, na podlagi pridobljenih podatkov pa pripraviti splošna priporočila, s katerimi bi podjetja preverjala stanje svoje zaščite.

Uporabljene metodologije v diplomskem delu so predstavitev teorije informacijske varnosti, opis poglavij informacijskega sistema ter anketiranje podjetij za analizo stanja informacijske varnosti podjetij na Goriškem.

1.3 Metoda analiziranja informacijske varnosti

Informacijsko varnost podjetij na Goriškem smo analizirali v začetku leta 2008 s pomočjo ankete, ki nas je pripeljala do zanimivih rezultatov. Anketo smo razdelili med štirideset podjetij, povratne informacije smo pridobili od devetnajstih podjetij. Nato smo analizirali njihove odgovore in na osnovi rezultatov pripravili priporočila glede informacijske varnosti za podjetja.

2 STANDARDI IN PRIPOROČILA S PODROČJA INFORMACIJSKE VARNOSTI

Zaradi kompleksnosti operacijskih sistemov se v poslovnih okoljih pojavlja potreba po sistematičnem obvladovanju informacijske varnosti na organizacijskem nivoju. Takšen celovit način upravljanja varnosti vpeljujejo različni standardi in priporočila, ki obravnavajo področje varovanja informacij. Med najbolj znanimi dokumenti, na katere se lahko organizacije oprejo pri oblikovanju sistema za upravljanje informacijske varnosti, so: COBIT, ITIL, BS7799, PAS56, BS ISO/IEC 13335, BS ISO/IEC 18044, BS ISO/IEC 15408, NIST SP, OCTAVE, OECD, OECD, PD 3000 (Pečnik, 2007). Podrobneje so opisani naslednji: COBIT, ITIL, ISO 17799, OECD.

2.1 COBIT

COBIT (angl. Control Objectives for Information and related Technology) je zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije. Je primerno orodje tako za vodstvo in uporabnike informacijske tehnologije kot tudi za revizorje informacijskih sistemov (Prešeren, 2008). Razvila sta ga IT Govenance Institute in Information System Audit and Control Foundation leta 1996. Zadnja verzija je COBIT 4.0 in je izšla decembra leta 2005.

2.2 ITIL

ITIL (angl. Information Technology Infrastructure Library) je zbirka knjig z opisi in napotki za uvajanje in kakovostno upravljanje s storitvami, ki temeljijo na uporabi informacijske tehnologije (IT). V ITIL-u je dokumentirana t. i. najboljša praksa pri upravljanju s storitvami IT ob sodelovanju mednarodnih strokovnjakov, tako iz javnega kot zasebnega sektorja v gospodarstvu (Prešeren, 2008). Lastnik in razvijalec ITIL-a je britanski OGC (Office of Governement Commerce) oz. Urad za trgovino britanske vlade, prej poznan kot CCTA. ITIL skupaj z Britanskim inštitutom za standarde podpira britanski standard za upravljanje s storitvami IT BS15000 (Information Technology Infrastructure Library, 2008).

ITIL je bil zasnovan konec osemdesetih let in je prvotno služil potrebam britanske vlade, vendar se je hitro izkazala njegova univerzalna uporabnost, tako da se je

kmalu razširil v vse panoge gospodarstva v Veliki Britaniji in v tujini. Nedolgo zatem je ITIL postal najbolj uveljavljeno, na procesih zasnovano ogrodje za uveljavljanje najboljše prakse pri upravljanju s storitvami IT v svetu. Tako danes ITIL predstavlja več kot samo knjižnico. Okrog nje je nastala cela panoga dejavnosti, ki vključuje izobraževanje, potrjevanje znanja posameznikov s certifikati, svetovanje, programska orodja, forum o upravljanju storitev IT in certificiranje podjetij.

2.3 ISO 17799

Standard ISO 17799 je zbirka pravil in metod nadzora za področje informacijske varnosti. Predstavlja priporočilo o varovanju informacij in informacijskih sistemov. Bistvo standarda ISO 17799/BS 7799 je v ocenjevanju in upravljanju tveganj ter varnosti informacij, cilj standarda pa je varnost. Razvili so ga iz BS 7799 (British Standard for Information Security Management) in kot takšen je dobil mednaroden naziv ISO 17799. Upravljalski sistem za varovanje informacij (ISMS – Information Security Management System), ki ga definira standard BS 7799, je delujoč sistem, ki spremlja spremembe varnostnih situacij, jih analizira in tvori ustrezne odgovore glede na sprejeto varnostno politiko. Standard je razvila vlada Velike Britanije s pomočjo industrijskih partnerjev, razvit pa je bil za potrebe malih in srednjih podjetij. Razdeljen je na dva dela: prvi del vsebuje navodila in razlago, drugi del pa predstavlja model za postavitev učinkovitega upravljalskega sistema za varovanje informacij. Formalno sta dva dela izdana kot ISO/IEC 17799 Code of Practice for Information Security in BS 7799-2:2002 Specification for Information Security Management System (Košir in Gregorčič, 2003).

2.4 OECD

Organizacija za ekonomsko sodelovanje in razvoj OECD (angl. Organization for Economic Cooperation and Development) podaja tudi smernice za varovanje informacijskih sistemov in omrežij. Združuje 30 držav članic, ki so zavezane demokraciji in tržnemu gospodarstvu. OECD velja za organizacijo elitnih gospodarstev, saj države članice OECD z manj kot petino svetovnega prebivalstva ustvarijo več kot polovico svetovnega proizvoda.

Predhodnica OECD je bila Organizacija za evropsko ekonomsko sodelovanje (OEEC), ki je bila ustanovljena leta 1948 za izvajanje Marshallovega načrta za povojno obnovo Evrope. Od svoje preureditve leta 1961 si preimenovana OECD prizadeva za oblikovanje močnih in učinkovitih gospodarstev v državah članicah, dviganje ravni zaposlenosti in življenjskega standarda ter za razvoj tako industrijskih držav kot držav v razvoju.

OECD oblikuje globalne standarde in načela na področju gospodarskih in razvojnih politik ter je na tem področju postala elitna in nosilna organizacija na svetu. Članstvo v OECD daje državi članici večjo politično težo ter ji dviguje politično-ekonomsko oceno in kredibilnost. Prestižna podoba države, uvrščene v klub najrazvitejših, že zgolj s tem vzbuja zaupanje in pomeni določeno zagotovilo za varnost poslovnega sodelovanja in morebitnih naložb (Turk, 2007).

2.5 BS ISO/IEC 17799:2005

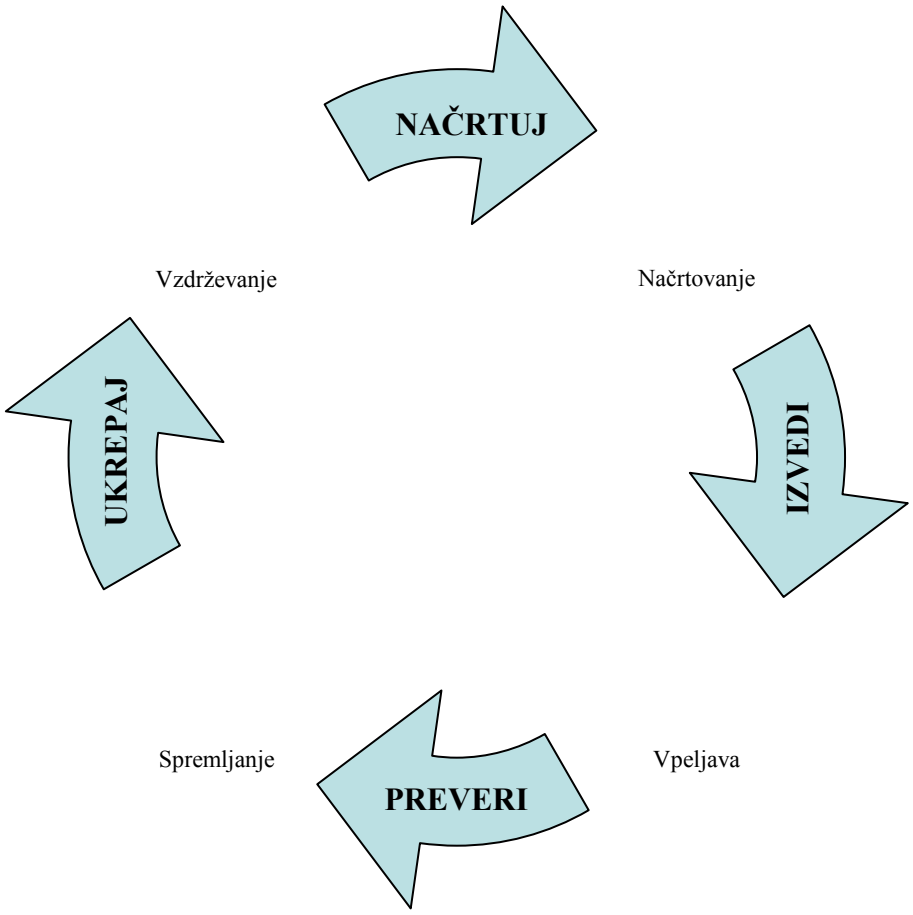
Ob vedno večji odvisnosti od informacijskih tehnologij, odprtosti organizacij in povečevanju pomena informacij v sodobnem poslovanju sta iz želje po ureditvi in poenotenju razmer v organizaciji na področju informacijske varnosti nastala standarda za vodenje varovanja informacij ISO/IEC 17799 in ISO/IEC 27001. Standarda sta poslovodno in od posameznih tehnoloških rešitev neodvisni orodji, ki ponujata celovit pregled varovanja informacij pri poslovanju organizacije. Ocena informacijskih tveganj je osnova za izgradnjo sistema varovanja informacij in njegova temeljna značilnost.

Standard ISO/IEC 17799 ponuja nabor možnih ukrepov za nadzor prepoznanih tveganj, ki so se z leti uporabe v različnih organizacijah po svetu pokazali kot primeri dobre prakse.

Standarda sta celovita v smislu informacijske varnosti. To pomeni, da ne obravnavata le informacijske tehnologije in informacij v elektronski obliki, temveč informacije v vseh možnih oblikah in medijih. V tem smislu je veliko opisanih postopkov povsem organizacijske narave in niso povezani s tehnologijo (npr.: klasifikacija informacij, politika prazne mize, fizično varovanje objektov ali opis varovanja informacij v pogodbah o zaposlitvi) (Rakuš, 2002).

3 ZAGOTAVLJANJE VARNOSTI V ORGANIZACIJI

Za zagotavljanje ustreznega nivoja informacijske varnosti v organizaciji je potrebno vzpostaviti učinkovit sistem za upravljanje informacijske varnosti (SUIV) (angl. Information Security Management System, ISMS). SUIV temelji na principu PDCA (Plan-Načrtuj, Do-Izvedi, Check-Preveri, Act-Ukrepaj) (slika 1), ki pokriva vse faze delovanja SUIV, od njegove vzpostavitve do zrele faze delovanja (Brezavšček, 2007).



Slika 1: Princip PDCA v sistemu za upravljanje informacijske varnosti

Temelj vzpostavitve SUIV v organizaciji predstavljata:

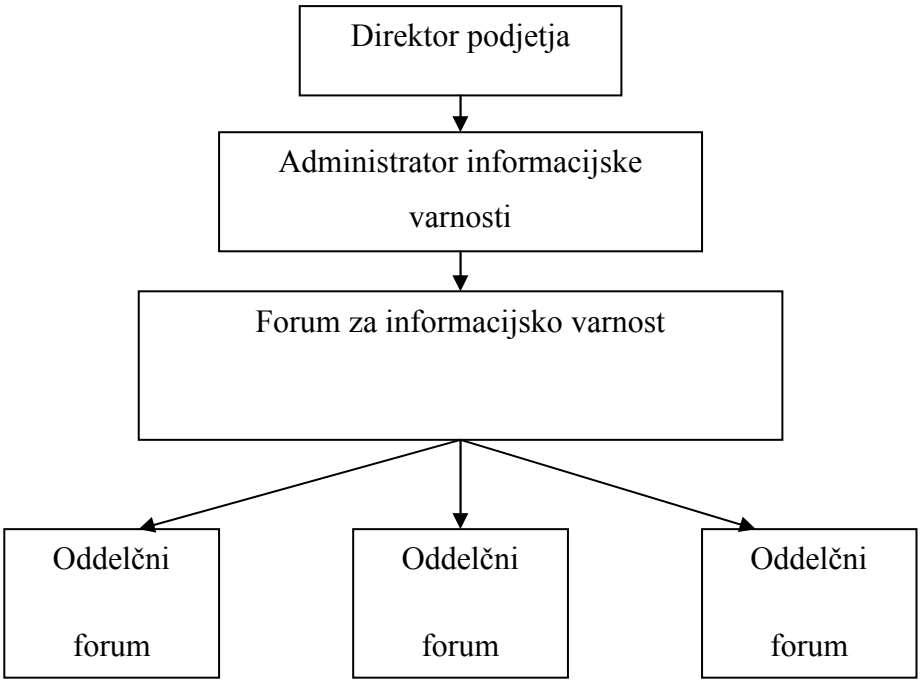
- varnostna politika,
- plan ukrepov v izrednih razmerah.

3.1 Varnostna politika

Varnostna politika zajema zbirko dokumentov, ki opredeljujejo, kako naj organizacija ravna s svojimi dobrinami, da bodo doseženi zastavljeni cilji. Varnostna politika torej opredeljuje tako varnostne zahteve kot tudi postopke za doseganje teh zahtev – varovalne ukrepe. Poleg navodil in postopkov za doseganje varnostnih zahtev morajo biti v varnostni politiki predpisane tudi sankcije za kršitev le-teh. Pri oblikovanju varnostne politike je nujno potrebno sodelovanje vodstva organizacije.

Koraki pri izdelavi in implementaciji varnostne politike so:

- ustanovitev foruma za informacijsko varnost,
- analiza obstoječega stanja in opredelitev glavnih tveganj – izvedba analize tveganj:
    - klasifikacija dobrin in ocena njihove vrednosti,
    - klasifikacija relativnih groženj in ocena pogostosti njihove uresničitve,
    - opredelitev ranljivosti posameznih dobrin na posamezne grožnje,
    - ovrednotenje tveganj,
- definiranje politike varovanja:
    - izbira ustreznih varovalnih ukrepov,
    - implementacija izbranih varovalnih ukrepov,
- spremljanje izvajanja varnostne politike,
- posodabljanje in izboljšave varnostne politike (Vidmar, 2002).



Slika 2: Forum za informacijsko varnost

Člani foruma informacijske varnosti naj bodo vodje posameznih procesov ali njihovi predstavniki. Člani foruma določijo predsednika, ki postane administrator informacijske varnosti. Administrator informacijske varnosti je zadolžen za varnost informacijskega sistema kot celote. Predsednik foruma informacijske varnosti je neposredno podrejen direktorju organizacije (slika 2).

Naloge foruma za informacijsko varnost so posredovanje ustreznih napotkov za delo zaposlenim, redno pregledovanje varnostne politike in izvajanje revizije odgovornosti, povezanih z zagotavljanjem informacijske varnosti. Forum je zadolžen tudi za pripravo krovnega dokumenta, ki vodstvo organizacije zavezuje k izvajanju varnostne politike. Ta dokument vsebuje matriko odgovornosti za informacijsko premoženje. Izbira in opis metod, ki se uporabljajo pri vzpostavitvi za upravljanje informacijske varnosti v organizaciji, sta tudi obveznost in naloga foruma, prav tako kot izbira metod in orodij za izvedbo analize tveganja ter zagotavljanje sredstev za realizacijo načrtov na področju zagotavljanja informacijske varnosti (Brezavšček, 2007).

Varnostna politika mora biti v internih aktih organizacije opredeljena kot obvezujoči predpis, ki ga morajo zaposleni spoštovati. Za morebitno neupoštevanje varnostne politike je potrebno predpisati sankcije. V večjih organizacijah je varnostna politika skupek več dokumentov na različnih nivojih upravljanja:

- navodila in postopki za delo na posameznem področju,
- varnostna politika za posamezno področje,
- krovna varnostna politika.

Z uvedbo različnih nivojev (slika 3) dosežemo boljšo preglednost, obenem pa povežemo nivo najvišjega managementa z operativnim nivojem.

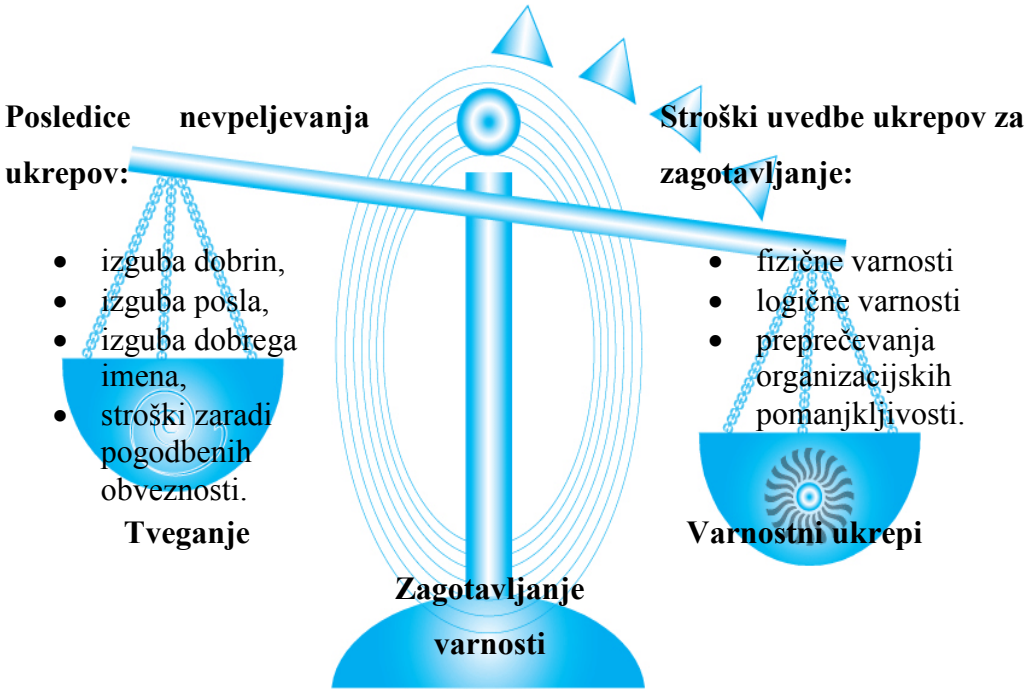
Slika 3: Nivoji organizacijske varnosti

Politika za posamezna področja vsebuje:

- politiko v zvezi z varovanjem osebja,
- politiko elektronske pošte,
- politiko fizičnega varovanja,
- politiko varovanja pred programskimi vsiljivci,
- politiko naročanja storitev pri zunanjih izvajalcih,
- politiko izvajanja, preverjanja in hranjenja varnostih kopij,

- politiko uporabe prenosne računalniške opreme in dela na daljavo,
- politiko dodeljevanja dostopnih pravic (Brezavšček, 2007).

Pri zagotavljanju varnosti v organizaciji moramo vzpostaviti ravnovesje med tveganji za organizacijo ter varnostnimi ukrepi (slika 4).



Slika 4: Zagotavljanje varnosti v organizaciji

3.2 Vloga administratorja informacijske varnosti

Administrator informacijske varnosti je odgovoren za pravilno in usklajeno delovanje celotnega sistema. Odgovoren je za ustrezno delovanje tako sistemske kot programske opreme. Uporabnikom mora omogočiti čim bolj učinkovito delo na informacijskem sistemu. Administrator ima na informacijskem sistemu vse pristojnosti, ki pa jih ne sme zlorabljati, zato mora biti sistemski administrator zaupanja vredna oseba. Z visokimi pristojnostmi sistemskega/varnostnega administratorja je povezana tudi visoka stopnja njegove odgovornosti. Sistemski/varnosti administrator igra eno izmed ključnih vlog že v fazi načrtovanja informacijskega sistema. S svojim znanjem lahko bistveno pripomore k zanesljivosti in varnosti informacijskega sistema.

3.3 Brezžična lokalna omrežja WLAN

Brezžična lokalna omrežja (angl. Wireless Local Area Network, WLAN) so namenjena povezovanju računalnikov s pomočjo radijskih valov. Poleg omrežij WLAN obstajajo tudi druge brezžične tehnologije, kot so bluetooth in mobilna telefonska omrežja. Brezžična lokalna omrežja navadno predstavljajo dopolnitev žičnega lokalnega omrežja v podjetju. Zaradi prednosti, ki jih ponuja tehnologija WLAN, se je uporaba omrežij WLAN, tako v komercialne kot v nekomercialne namene, v zadnjem času zelo razširila.

Prednosti omrežij WLAN so udobnost, mobilnost, prilagodljivost, razširljivost in nizki stroški vzpostavitve. Njihove slabosti pa so nenadzorovan domet radijskega signala, delitev pasovne širine med trenutnimi uporabniki, slabša zanesljivost povezav, nižje hitrosti prenosa. Dodatna slabost, ki pa je pravzaprav samo normalna fizikalna lastnost sevanja, je ta, da moč in s tem hitrost prenosa podatkov padata z razdaljo (Brezavšček, 2007).

3.3.1 Tehnične značilnosti omrežij WLAN

Omrežja WLAN temeljijo na družini standardov 802.11, ki ga je razvil inštitut IEEE (Institute of Electrical and Electronics Engineers). Delujejo na frekvenčnem področju 2,4 in 5 GHz, ki je namenjeno javni uporabi. Najvišja hitrost prenosa podatkov v omrežju WLAN je od 2 Mbit/s do 248 Mbit/s, odvisno od uporabljenega standarda, tipična hitrost prenosa pa od 0,9 Mbit/s do 79 Mbit/s. Temeljni komponenti omrežja WLAN sta dostopna točka z ustrezno anteno in prenosni terminal, npr. prenosni računalnik z radijsko mrežno kartico. Pri izbiri komponent omrežja WLAN moramo biti pozorni na standarde, po katerih so komponente izdelane, za določitev najučinkovitejših pozicij dostopnih točk pa je potrebno izvesti ustrezne meritve (Brezavšček, 2007).

3.3.2 Brezžična omrežja in varnost

V zadnjih letih sta internet in intranet postala nepogrešljiva sestavna dela skoraj vsake strategije podjetja, velikokrat pa je del teh omrežij tudi brezžičen. Kombinirana računalniška omrežja so postala centralni živčni sistem za vsakodnevno

poslovanje, neglede na velikost podjetja ali panogo, v kateri deluje. Skoraj vsa podjetja so v položaju, ko se morajo zanesti na to, da imajo delujoč dostop do omrežnih aplikacij in podatkov v vsakem trenutku, obenem pa morajo skrbeti za varovanje svojih podatkov. Pri fizičnih omrežjih je za vdor v omrežje kritična samo točka, v kateri se podjetje povezuje v svet, pri brezžičnem omrežju pa tovrstnega fizičnega nadzora ni. Vsakdo, ki je dovolj blizu brezžičnemu omrežju, lahko sprejema signale, ki jih omrežje oddaja. Kupci brezžične omrežne opreme velikokrat zmotno menijo, da je domet omrežja zelo majhen. V resnici postane signal z oddaljenostjo le toliko šibak, da ga majhne antene v prenosnem računalniku ne zaznajo več. Z boljšo anteno pa je signal mogoče spremljati tudi na daljši razdalji. Vdiranje v nezaščitena brezžična omrežja ali njihovo izkoriščanje je v tujini tako popularno, da je hitro dobilo kar svoje ime wardriving. Večina proizvajalcev brezžične opreme ponuja različne možnosti varovanja omrežja. Osnovna zaščita je uporaba ključa WEP, ki šifrira pakete v brezžičnem omrežju, vendar je to osnovno zaščito zelo preprosto prebiti. Na internetu je mogoče najti kup programskih orodij, ki omogočajo nepovabljenim osebam odkritje ključa WEP (angl. Wired Equivalent Privacy), če je omrežje dovolj dolgo dosegljivo (Sušnik, 2004).

3.3.3 Kako zaščititi brezžično omrežje?

Če obstaja verjetnost vdora in bi bila škoda, ki bi pri tem nastala velika, je treba temeljito razmisliti o strategiji zaščite. Eden od preprostejših načinov je, da je še brezžično omrežje za požarnim zidom, ki omogoča le povezavo VPN, torej vzpostavljanje navideznega zasebnega omrežja. S tem sicer ne bomo onemogočili dostopa do brezžičnega omrežja, a nepovabljeni ne bodo imeli dostopa do internega omrežja v podjetju. Pri tem načinu obravnavamo brezžično omrežje kot javno in zato potencialno nevarno. Vedeti pa moramo, da so v tem načinu posamezni računalniki v podjetju, ki so priključeni v brezžično omrežje, lahko izpostavljeni morebitnemu vdoru. Drugi način zaščite je uporaba orodij, ki podpirajo standard 802.1x. Gre za standard šifriranja, ki omogoča varno pošiljanje ključev in paketov po omrežju. Pri tej izvedbi tipično potrebujemo strežnik, ki skrbi za šifriranje in razdeljevanje ključev (strežnik RADIUS). Na voljo je tudi veliko strojnih rešitev in rešitev, ki skrbijo za zaznavanje vdorov, šifriranje prometa ipd. Zanimiv pristop ubira rešitev FakeAP (Sušnik, 2004), ki ustvari navidezne dostopne točke (angl. access point).

Morebitni vdiralec bi tako moral najti pravo dostopno točko med 53 000 dostopnimi točkami, ki jih »vidi« v brezžičnem omrežju.

3.4 Navidezna zasebna omrežja

Navidezna zasebna omrežja (angl. Virtual Private Network, VPN) omogočajo povezovanje oddaljenih enot podjetja v navidezno zasebno omrežje in sicer preko uporabe javnih komunikacijskih poti (npr. internet). Tako VPN omogočajo učinkovito in varno komunikacijo med različnimi lokacijami (delo na domu, navidezna pisarna) ter prihranek denarja, saj je za varno povezavo z zasebnim omrežjem uporabljen javni internet in ne dragi medkrajevni vodi.

Omrežja VPN so cenovno zelo ugodna in varna za podjetja, ki želijo omogočiti uslužbencem oziroma uporabnikom dostop do zasebnih omrežij v podjetjih preko uporabe interneta. Običajno VPN sestavljata dva dela: varovano notranje omrežje, ki zagotavlja fizično in administrativno varnost pri prenosih, ter manj varno zunanje omrežje (običajno internet).

Povezave v navideznem zasebnem omrežju so varovane, tako da je nepooblaščenim uporabnikom onemogočen dostop do omrežja (slika 5).

Slika 5: Varovan komunikacijski kanal

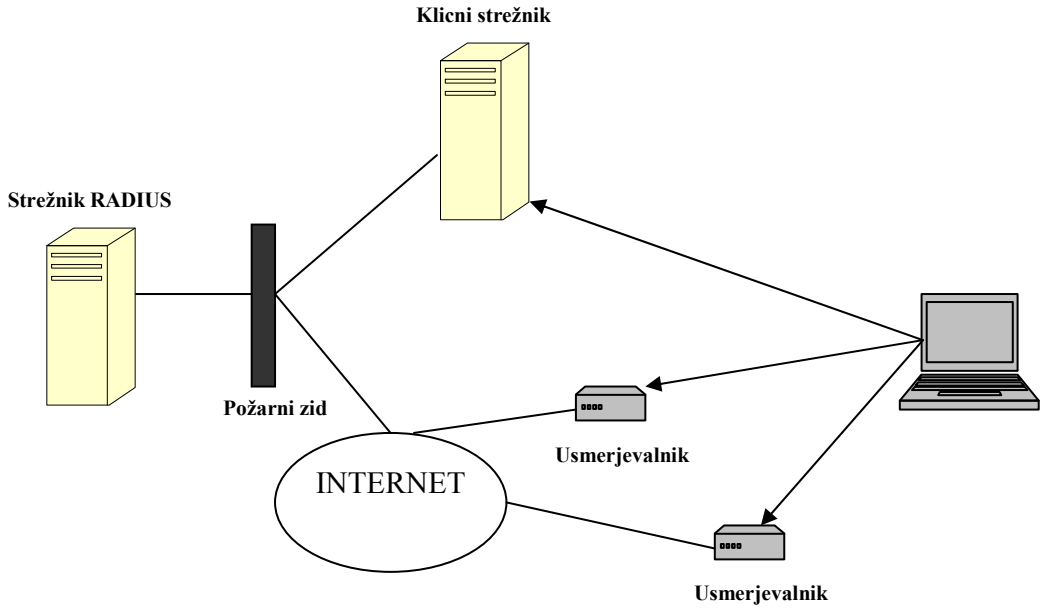
Potreba po navideznih zasebnih omrežjih se pojavi zato, ker internet zaradi slabe varnosti ni primeren za pošiljanje pomembnih podatkov. VPN to težavo reši, saj se vzpostavi varovan komunikacijski kanal med dvema točkama in je tako ves promet, ki poteka po teh kanalih, šifriran.

Za vzpostavljanje navideznih zasebnih omrežij VPN se najbolj uporabljajo naslednji protokoli: PPTP, L2TP, IPSec in SSL (Brezavšček, 2007).

3.5 RADIUS

Odjemalci, ki se želijo priključiti v omrežje s pomočjo oddaljenega dostopa, se morajo najprej overiti, da se preveri njihova identiteta. RADIUS (angl. Remote Authentication Dial-In User Service) omogoča overjanje odjemalcev, ki se priključujejo v omrežje s pomočjo klicnega dostopa, navidezne zasebne povezave VPN ali brezžičnega dostopa. V vseh teh primerih je mogoč centralen nadzor nad vsemi priključitvami v omrežje neglede na njihovo mesto.

Omrežna naprava, na katero se lahko priključujejo oddaljeni odjemalci, pri vsaki priključitvi odjemalca pošlje zahtevo za overjanje strežniku RADIUS, ki nato napravi odgovori, ali je zahteva sprejeta ali zavrnjena (slika 6) (Vidmar, 2002).



Slika 6: Overjanje s pomočjo strežnika RADIUS

V primeru na sliki se odjemalec lahko priključi na klicni strežnik ali pa na določen usmerjevalnik in pri tem lahko uporabi enak način prijave. Ko se odjemalec priključi, strežnik oziroma usmerjevalnik preveri odjemalca tako, da pošlje zahtevo za overjanje strežniku RADIUS, ki odjemalca preveri v svoji bazi odjemalcev. Če je overitev pozitivna, se odjemalec dokončno vključi v omrežje, sicer pa se povezava prekine. Pri tem strežnik RADIUS omogoča tudi dodelitev ustreznih pravic odjemalcu. Seveda lahko določenim odjemalcem dovolimo dostop samo preko določenih strežnikov oziroma usmerjevalnikov. Zaradi varnosti je IP naslov strežnika RADIUS skrit za požarnim zidom, preko katerega se izvaja preverjanje naslovov.

RADIUS ima v splošnem naslednje funkcije:

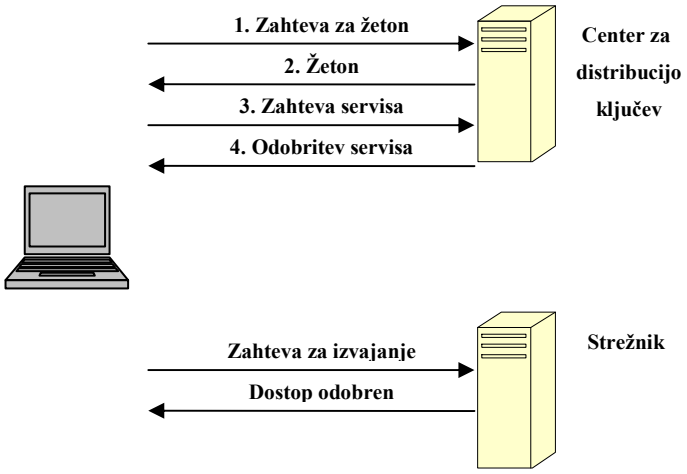
- centralno overjanje odjemalcev za celotno organizacijo,
- centralno obračunavanje,
- centralne varnostne nastavitve.

Centralno overjanje omogoča hranjenje podatkov o odjemalcih na enem mestu, kar poenostavi administriranje. RADIUS omogoča poleg overjanja tudi centralno obračunavanje. Pri tem se za vsakega odjemalca lahko izmeri trajanje priključitve. Če gre za komercialne priključitve, lahko glede na njihovo trajanje, uporabnik plača določeno nadomestilo za uporabo omrežja, kar pride v poštev predvsem za ponudnike internetnih storitev. RADIUS omogoča tudi centralne varnostne nastavitve, kar preprečuje nestandardne načine priključitev, ki lahko povzročijo razne varnostne luknje.

3.6 KERBEROS

Protokol KERBEROS omogoča preverjanje istovetnosti uporabnikov za velika distribuirana omrežja. Razvili so ga v osemdesetih letih 20. stoletja na ameriškem institutu Massachusetts Institute of Technology.

Protokol KERBEROS omogoča overjanje odjemalca in vzpostavljanje varne povezave med odjemalcem in strežnikom (slika 7). V nasprotju z dvosmernim protokolom SSL na strani odjemalca ne zahteva nikakršnega digitalnega potrdila, temveč overjanje izvaja na podlagi dostopnega gesla. Protokol je izjemno prilagodljiv, saj lahko z enega mesta nadziramo vse strežnike in odjemalce.



Slika 7: Preverjanje istovetnosti s protokolom KERBEROS (Vidmar, 2002)

3.7 Požarni zid

Požarni zid (angl. firewall), je strojna ali programska oprema, ki filtrira promet med računalnikom in internetom. Dandanes skoraj vsak uporabnik, ki uporablja internet, potrebuje požarni zid (Pečnik, 2007).

Računalniki, povezani v internet, so stalno podvrženi virusom, črvom in napadom raznih vdiralcev. S požarnim zidom želimo preprečiti vdor v svoj računalnik ali celotno omrežje. Dober požarni zid prepreči ves promet med lokalnim omrežjem in internetom, razen tistega, ki ga izrecno dovolimo.

Požarni zid je učinkovit le v povezavi z drugimi zaščitami računalnikov. Med te sodijo protivirusni programi, kodiranje podatkov, varnostna politika itd.

Naloge požarnega zidu lahko strnemo v:

- blokiranje vhodnega prometa v omrežje glede na izvor ali ponor,
- blokiranje izhodnega prometa iz omrežja glede na izvor ali ponor,
- blokiranje prometa glede na vsebino,
- dovoljevanje dostopa do notranjih virov omrežja,
- izdelavo poročil o prometu omrežja in aktivnostih požarnega zidu.

Blokiranje vhodnega prometa v omrežje glede na izvor ali ponor je najbolj tipična naloga požarnega zidu. Na ta način preprečimo, da bi zunanji uporabniki brez ustreznega dovoljenja dostopali do računalnikov v omrežju.

Pri blokiranju izhodnega prometa iz omrežja glede na izvor ali ponor lahko preprečimo zaposlenim dostop do določenih računalniških virov na internetu ali pa preprosto dovolimo dostop samo do določenih internetnih virov.

Naprednejši požarni zidovi imajo vgrajeno funkcijo blokiranja prometa glede na vsebino. Na ta način se lahko prepreči prehod datoteke z virusi ali pošiljanje neprimerne elektronske pošte.

S požarnim zidom lahko nadziramo dostop do notranjih strežnikov podjetja ali organizacije. Zaposleni ali zunanji uporabniki omrežja navadno vzpostavljajo povezave z omrežjem ali določenim računalnikom v omrežju s pomočjo navideznih zasebnih omrežij, ki omogočajo kodiran prenos podatkov med računalnikom na internetu ali omrežjem. S požarnim zidom lahko nadziramo tako vzpostavljene povezave.

Požarne zidove glede na način uporabe lahko delimo na požarni zid, požarni zid oddelka ali manjše organizacije in požarni zid velikega podjetja.

3.8 Diskovna polja RAID

V današnjih računalniških sistemih je trdi disk največje ozko grlo pri obdelavi in pošiljanju podatkov. Trdi diski so še vedno nezamenljiv medij za shranjevanje in delo s podatki. V zadnjem času razvijajo cenejše optične diske, vendar je njihova zmogljivost prenizka.

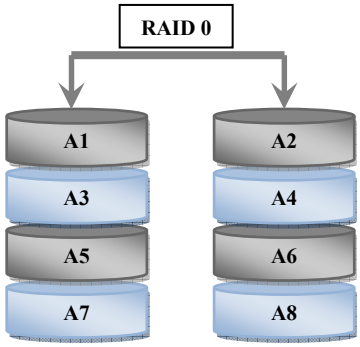
Pri prvih računalniških sistemih so morali disk celo upočasniti, ker procesor in ostale komponente niso bile dovolj hitre, danes pa je prav disk ozko grlo. Sami procesorji lahko upravljajo polje diskov, ki se običajno imenuje polje RAID (angl. Redundant Array of Inexpensive Disks).

RAID označuje množico diskov, med seboj povezanih na določen način. Vsa takšna diskovna polja potrebujejo logiko, ki jih krmili, kar lahko dosežemo s pomočjo

posebnega RAID krmilnika ali z nastavitvami v nekaterih zmogljivejših operacijskih sistemih (Linux, Windows NT, Windows 2000, Windows XP itd.). Obstajajo različni tipi diskovnih polj RAID (Brezavšček, 2007).

3.8.1 RAID 0

Večina diskovnih polj RAID vključuje tehnologijo, ki shranjuje podatke v pasovih (angl. data striping). Najenostavnejša implementacija te tehnike je poznana kot RAID 0 in je zelo razširjena. Pri polju RAID 0 sta potrebna vsaj dva diska. Zapisovanje datotek poteka skoraj dvakrat hitreje, saj se približno polovica datoteke zapiše na en disk, polovica pa na drugega. Prav tako je pri branju, saj bereta oba diska sočasno in tako je hitrost večja za količnik zelo blizu številki 2. RAID 0 ali linearno polje je sistem, v katerem računalnik razdeli podatke na posamezne diske tako, da lahko istočasno bere in piše po vseh hkrati. Na ta način dosežemo višje hitrosti prenosa, zanesljivost pa žal ni odlika takega polja. Če se pokvari en sam disk, izgubimo vse podatke, saj so deli datotek razpršeni po vseh diskih (slika 8) .



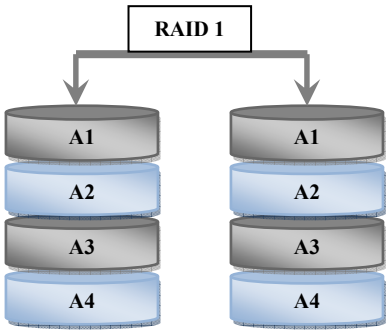
Slika 8: Zapis podatkov na diske v polju RAID 0

RAID 0 je torej primeren, če potrebujemo zgolj hitrost, ne pa varnosti. Za podjetja tak tip polja RAID ni primeren, razen če ga povežemo s kakšno drugo RAID tehniko (Brezavšček, 2007).

3.8.2 RAID 1

RAID 1 je najenostavnejša oblika diskovnega polja, ki ima toleranco na napake. Temelji na konceptu zrcaljenja (angl. mirroring), kar pomeni, da je vsak disk v sistemu natančna kopija drugega. Na sliki 9 je prikazano polje RAID 1 z dvema

diskoma. V primeru okvare enega od diskov v sistemu imamo natančne kopije podatkov na drugem disku. Polje RAID 1 je zelo zanesljivo, vendar zahteva višjo ceno, saj morajo biti diski iste kapacitete, ki pa se ne seštevajo med seboj. Zaradi tega je to polje diskov primerno za male podatkovne baze in manjše sisteme, ki zahtevajo visoko stopnjo zanesljivosti. Polje je hitrejše pri branju in počasnejše pri pisanju v primerjavi z enim diskom (Brezavšček, 2007).



Slika 9: Polje RAID 1 z zrcaljenjem

3.8.3 RAID 2

RAID 2 je izboljšan RAID 1. Pri tem polju je odstotek neizkoriščenega prostora nekoliko nižji. Pri tem načinu se uporablja posebna metoda, imenovana Hammingova koda, ki služi odkrivanju napak za diske, ki nimajo vgrajenega samodejnega zaznavanja napak. Vsi SCSI diski podpirajo samodejno zaznavanje napak, zato se to polje ne uporablja za SCSI diske. Za uporabo tega polja potrebujemo vsaj sedem navadnih diskov. Z vsakimi štirimi biti podatkov se zapišejo še trije nadzorni biti. S pomočjo teh je kasneje mogoče ob odpovedi kateregakoli diska obnoviti podatke, tako da sistem deluje nemoteno naprej. Slabost tega načina je velika izguba prostora (RAID Tutorial, 2008).

3.8.4 RAID 3

RAID 3 je poenostavljena različica polja RAID 2. V njem se ne uporablja t. i. Hammingove kode za odkrivanje napak, temveč le paritetni bit. Za uporabo tega načina potrebujemo vsaj tri diske, pri katerih se na poseben disk zapisuje paritetna informacija, na ostale pa se razdelijo podatki. Pri tem se podatkovni biti zapisujejo izmenično na vse diske. S pomočjo paritete lahko tako ob odpovedi enega diska

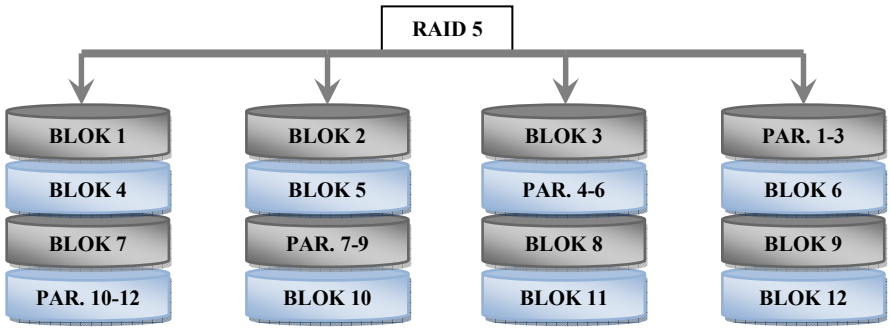
sistem obnovi podatke in nemoteno deluje dalje brez njihove izgube (RAID Tutorial, 2008).

3.8.5 RAID 4

RAID 4 je podoben polju RAID 3. Od njega se razlikuje po tem, da se podatki zapisujejo po blokih (angl. block level) na različne diske. Velikosti blokov lahko spreminjamo, kar nam daje možnost, da s pravilno izbiro nastavitev iz našega diskovnega polja RAID dobimo največ (RAID Tutorial, 2008). Ob nepravilni nastavitvi lahko dosežemo ravno nasproten učinek od pričakovanega, upočasnitev.

3.8.6 RAID 5

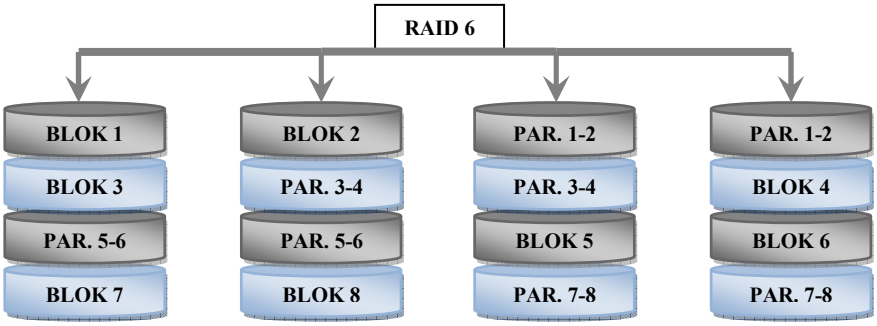
RAID 5 je po zasnovi podoben polju RAID 4, le da se tu pariteta zapisuje na vse diske in ne več na posebej določenega. Ta način je v praksi najbolj uporabljan predvsem zaradi dejstva, da odpravlja ozko grlo paritetnega diska, kar se je pokazalo pri uporabi velikega števila diskov v sistemih RAID 3 in 4. Z uporabo tega sistema sicer izgubimo kapaciteto enega diska, vendar je zagotovljena zanesljivost, saj lahko sistem kljub odpovedi enega izmed diskov obnovi vse podatke in nemoteno deluje dalje (slika 10).



Slika 10: Diskovno polje RAID 5

3.8.7 RAID 6

Diskovno polje RAID 6 je manj uporabljano od RAID 5, deluje pa zelo podobno. Razlika je, da se pri tem načinu pariteta zapiše dvakrat, kar omogoča nemoteno delovanje sistema tudi ob izpadu dveh diskov naenkrat (slika 11).



Slika 11: Diskovno polje RAID 6

3.8.8 RAID 0+1

RAID 0+1 je kombinacija polj RAID 0 in RAID 1, ki združuje prednosti obeh polj. Omogoča tako zrcaljenje (mirroring) kot sistem linearnega polja (striping) brez uvedbe paritete. Za ta sistem potrebujemo najmanj štiri identične diske, kapaciteta diskov pa se razpolovi.

3.9 Zagotavljanje zaupnosti sporočil s šifriranjem

Šifriranje sporočil je pretvorba sporočila v tako obliko, da ga praviloma nepooblaščene osebe ne morejo razumeti. Izvirno sporočilo se z uporabo nekega algoritma in šifre pretvori v nerazumljiv niz znakov. Namen je, da vsebina sporočila ni razumljiva nepooblaščeni osebi, če tako sporočilo prestreže. Uporaba je razširjena v diplomaciji, oboroženih silah, obveščevalni dejavnosti in vedno pogosteje tudi v poslovnem svetu. Za šifriranje (izdelavo šifriranega sporočila) in dešifriranje (pretvorbo šifriranega sporočila v izvirno sporočilo) se danes uporabljajo računalniki. Računalniki so z razvojem algoritmov in podaljševanjem šifre postali nujni za odkrivanje algoritmov in šifer prestreženih tujih sporočil (Gradišar, 2003).

Šifriranje je mehanizem za zagotavljanje zaupnosti občutljivih podatkov/informacij tako med hranjenjem in obdelavo v informacijskem sistemu kot tudi med prenosom po komunikacijskem omrežju.

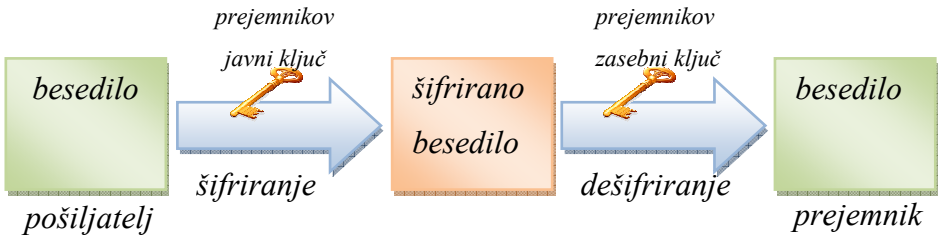
Pri simetričnem šifriranju gre za šifriranje z enakim ključem kot za dešifriranje (slika 12).

Slika 12: Simetrično šifriranje (Gradišar, 2003)

Slabosti simetričnega šifriranja je, da je potrebno dostaviti tudi tajni ključ, da lahko vsebino prejetega sporočila dešifriramo. S tem ko šifrirni ključ prenašamo, ga izpostavimo nepooblaščenemu razkritju. Pomanjkljivost simetričnega šifriranje je, da ključ poznata najmanj dva in da za vsakega, s katerim komuniciramo, potrebujemo drugačen ključ (npr. če 100 zaposlenih želi komunicirati med sabo, potrebujemo 4950 različnih šifrirnih ključev). Da bi se izognili takim težavam, so v sedemdesetih letih razvili asimetrično šifriranje.

Pri asimetričnem šifriranju (slika 13) se za dešifriranje informacij uporablja ključ, ki je različen od ključa, s katerim je bilo sporočilo šifrirano. Oba ključa (ključ za šifriranje in ključ za dešifriranje) sta v matematični povezavi in tvorita par ključev. Par ključev mora biti generiran tako, da velja (Gradišar, 2003, str. 267−269):

- podatki/informacije, ki so bili šifrirani z javnim ključem, lahko dešifriramo izključno s pripadajočim tajnim ključem,
- za zagotovitev varnega postopka šifriranja je dovolj, da je en ključ iz para tajen, medtem ko je drugi ključ lahko javno znan in dostopen vsakomur.



Slika 13: Asimetrično šifriranje (Gradišar, 2003)

3.10 Varovanje komunikacij

Varovanje komunikacij je varovanje podatkov oziroma elektronskih sporočil, ki se prenašajo po omrežjih. Glavne grožnje varnosti elektronskih sporočil so: izredni dogodki, izpad in nihanje električne energije, odpoved elementov omrežja, programski vsiljivci, ohromitev strežnika, vdor v komunikacijo, zanikanje udeležbe v komunikaciji, odpoved človeka in izkoriščanje organizacijskih pomanjkljivosti.

Varovalne funkcije, ki jih želimo zagotoviti, so:

- razpoložljivost sporočila: sporočilo je dostopno v vsakem trenutku, ko ga uporabnik potrebuje;
- zaupnost sporočila: vsebino sporočila lahko prebere izključno tisti, ki mu je sporočilo namenjeno;
- celovitost sporočila: vsebina sporočila se med potjo ne spremeni; prejemnik sporočila lahko morebitno spremembo zazna;
- nepodvajanje sporočila: sporočilo je poslano samo enkrat;
- nezanikanje udeležbe v komunikaciji: pošiljatelj sporočila ne more zanikati, da je on avtor sporočila;
- istovetnost (avtentičnost) udeležencev v komunikacij: udeleženec v komunikaciji lahko preveri, ali komunicira s pravo osebo.

3.10.1 Ohromitev strežnika

Nepooblaščena oseba (napadalec) skuša preprečiti pooblaščenim uporabnikom dostop do storitve stražnika na enega izmed naslednjih načinov:

- obremenjevanje omrežja s prekomernim prometom, tako da je za promet pooblaščenih uporabnikov omrežje preobremenjeno,
- obremenjevanje omrežja s številnimi zahtevami za izvajanje storitve strežnika, tako da strežnik ni sposoben sprejeti zahtev za izvajanje storitve od pooblaščenih uporabnikov,
- sprememba konfiguracijskih nastavitev elementov omrežja z namenom prekinitve komunikacije med pooblaščenim uporabnikom in strežnikom.

V ta namen so bila razvita mnoga programska orodja, ki so na internetu prosto dosegljiva, kot npr. Bonk, LAND, Smurf, Snork, WinNuke, Teardrop in mnoga druga (Brezavšček, 2007).

Posledica ohromitve strežnika je nerazpoložljivost elementov omrežja, kar pa pripelje do nedosegljivosti sporočila v želenem trenutku. Varnostna ukrepi, s katerimi se zavarujemo proti ohromitvam strežnika, so:

- skrbimo za ustrezno kontrolo dostopa in izvajamo strogo politiko upravljanja z gesli,
- na usmernike in vozlišča omrežja namestimo ustrezne filtrirne mehanizme (npr. protivirusna orodja, požarne zidove, sisteme za zaznavanje vdorov),
- onemogočimo vse storitve omrežja, ki jih ne potrebujmo, in na ta način omejimo repertoar priložnosti za napad,
- za vse uporabnike omejimo prostor na disku strežnika, ki ga lahko uporabljajo,
- natančno opredelimo, kakšno je normalno delovanje omrežja, tako da lahko njegovo nenormalno delovanje hitro prepoznamo in napad čim prej zaznamo,
- redno izdelujemo varnostne kopije občutljivih podatkov in konfiguracije sistema.

3.10.2 Vdor v komunikacijo

Nepooblaščena oseba (napadalec) se skuša vriniti v komunikacijo dveh pooblaščenih uporabnikov na enega izmed naslednjih načinov:

- vohljanje po omrežnih paketih (angl. network packet sniffing),
- sleparjenje z IP naslovi (angl. IP spoofing),
- ugrabitev seje (angl. session hijacking).

Posledice tovrstnih vdorov v komunikacijo so, da se nepooblaščeno spremeni ali uniči sporočilo, nepooblaščeno razkrije vsebino sporočila ter da lahko nepooblaščena oseba podvoji sporočilo z namenom okoriščanja. Varovalni ukrepi so implementacija ustreznih mehanizmov za zagotavljanje:

- zaupnosti sporočil,
- celovitosti sporočil,
- verodostojnosti udeležencev v komunikaciji,
- nepodvajanja sporočil.

3.11 Nezaželena pošta

Vsakemu sporočilu, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati, pravimo nezaželena pošta (angl. spam).

Oglaševanje preko elektronske pošte je med podjetji priljubljeno predvsem zaradi majhnih stroškov, preproste uporabe in možnosti doseganja velikega števila uporabnikov v zelo kratkem času. Ravno te prednosti pa so na žalost privedle do vsiljivosti oglaševalcev, ki pošiljajo pošto tudi tistim, ki njihovih vsebin ne želijo prejemati. Zaradi prejemanja nezaželenih komercialnih sporočil, ki so poslana brez dovoljenja, želje ali interesa naslovnika, se vsak dan pojavlja vedno več nezadovoljnih uporabnikov. Oglaševalci bi se morali zavedati, da lahko z nespoštovanjem spletne etike in pošiljanjem sporočil na naključno izbrane elektronske naslove zelo hitro zapravijo svoj ugled in na dolgi rok utrpijo veliko poslovno škodo. Elektronska pošta je z leti izgubila na svoji učinkovitosti, saj zaradi ogromne količine promocijskih sporočil, ki ves čas krožijo po internetu in nas vsako jutro čakajo v poštnem nabiralniku, ne dosega več tako velikega odziva pri ljudeh kot nekoč. Spletni uporabniki zahtevajo izpis iz baze naslovnikov ali pa izbrišejo večino sporočil, še preden jih sploh preberejo, saj jim množica nezaželene pošte krade čas in prostor v elektronskem poštnem nabiralniku, jim gre na živce in jih navsezadnje še ogroža z virusi.

3.11.1 Stroški zaradi prejemanja nezaželene pošte

Posledice se kažejo tudi v podjetjih, saj jim nezaželena pošta povzroča dodatne, nepotrebne stroške. Vanje so vračunane izgube produktivnosti in izgubljene delovne ure ter stroški, ki nastanejo zaradi zakasnjenih poslovnih komunikacij, porabe strežniških virov in dela administratorjev računalniških mrež. Dodatne stroške povzročajo še odprave posledic, povzročenih s strani računalniških virusov, ki se

širijo preko elektronske pošte. Raziskava ameriškega podjetja Ferris Research je razkrila, da so v letu 2003 nezaželena sporočila povzročila ameriškim podjetjem 10 milijard dolarjev stroškov (Skrt, 2003). Podjetje Nucleus Research pa je ugotovilo, da se povprečna produktivnost zaposlenih zaradi prejemanja nezaželene pošte zmanjša za 1,4 %, kar je posledica več kot 13 prejetih nezaželenih sporočil dnevno, ki vsakemu posamezniku ukradejo 6 minut časa (Skrt, 2003).

3.11.2 Preprečevanje nezaželene pošte

Proti nezaželeni pošti se je izredno težko boriti, saj najdejo pošiljatelji vedno nove in nove načine, da pošljejo sporočila v naš poštni nabiralnik. Kljub vsem orodjem in možnostim, ki jih imajo podjetja na voljo za omejevanje nezaželene elektronske pošte, celovite rešitve žal ni. Zaščita pred nezaželeno pošto je sila težavna, saj elektronska sporočila praviloma ne nosijo nekega skupnega imenovalca, po katerih bi jih bilo moč prepoznati in ukiniti. Nezaželeno pošto lahko omejimo, nikakor pa jo ne moremo v celoti odpraviti. Pomagamo si lahko s programi, ki nezaželeno elektronsko pošto blokirajo na e-poštnem strežniku ali pa pri končnem prejemniku e-sporočil (npr. MailWasher, Spam Butcher, Spamnet, Email Remover) (Skrt, 2003).

Koristno in uporabno orodje so tudi t. i. pravila, ki jih vsebujejo programi za prebiranje e-pošte, saj lahko z njihovo pomočjo filtriramo vsa prejeta sporočila. Tako lahko v poštnem odjemalcu nastavimo pravila, s katerimi blokiramo naslove neželenih pošiljateljev ali pa preusmerjamo pošto, ki v glavi ali telesu sporočila vsebuje določene besede, neposredno v koš ali v poljubno izbrano mapo. Pri takšnem načinu filtriranja prejetih sporočil pa moramo biti zaradi njihove nezanesljivosti previdni, saj se lahko zgodi, da se med zavrženo pošto najdejo tudi za naročnika povsem legitimna, zaželena in pomembna e-sporočila.

Količino prejete nezaželene pošte lahko z lastno previdnostjo zmanjšamo tudi sami. Predvsem je potrebno razmisliti, kje vse bomo objavili svoj e-poštni naslov in komu ga bomo posredovali. Pošiljatelji nezaželene pošte lahko namreč s posebnimi programi prečešejo spletne strani ali pa kar naš računalnik ter izbrskajo vse, kar zgleda kot veljaven elektronski naslov. Količine prejete nezaželene pošte lahko omejimo tudi tako, da za potrebe registracije programov, za prijave na e-novice,

poštne sezname ipd. uporabljamo nadomesten naslov, ki ga lahko odpremo pri enem izmed ponudnikov brezplačne e-pošte (npr. Hotmail), ker ga bomo lahko v primeru zlorab in bombardiranja z e-pošto brez večjih posledic ukinili.

Zaradi zaščite pred nezaželeno pošto je že marsikatero podjetje prepovedalo uporabljati službeni e-naslov pri spletnem nakupovanju, za naročanje na različne e-publikacije in vpisovanje na poštne sezname, ki niso povezani z delovnim področjem in delovnimi nalogami zaposlenega. Prejemanje nezaželene pošte lahko podjetje omeji tudi tako, da odstrani vse elektronske naslove s svojih spletnih strani in jih nadomesti z obrazci, preko katerih lahko obiskovalci navežejo stik s podjetjem ali s posameznimi oddelki. V podjetjih lahko veliko storijo tudi z izobraževanjem zaposlenih, z doslednim uvajanjem pravil uporabe elektronske pošte in etičnega trženja ter z uporabo primerne programske opreme, ki bo neustrezna in nezaželena sporočila zaustavila že pred dostavo končnemu naslovniku. Pri svojem poslovanju mora tudi samo podjetje paziti kaj, kako in v kakšni obliki pošilja preko elektronske pošte svojim obstoječim in potencialnim strankam, da ne bo še samo po nepotrebnem pripomoglo k že tako velikim količinam nezaželene pošte.

3.12 Programski vsiljivci

Programski vsiljivci (tabela 1) so programi, ki so izdelani izključno z namenom, da računalniškemu sistemu povzročijo škodo. Prvi programski vsiljivci so imeli samo lokalne učinke. Sredi osemdesetih let so se pojavili prvi programski vsiljivci, ki so se znali razmnoževati med računalniki. Danes se z različnimi programskimi vsiljivci srečujemo vsakodnevno. V povprečju se na dan pojavi več ko 40 novih programskih vsiljivcev. Trenutno je znanih preko 180 000 različnih vrst programskih vsiljivcev. Velika večina napada operacijski sistem Windows, predvsem sisteme Win32 (Brezavšček, 2007).

Posledice škodljivih akcij programskih vsiljivcev so lahko zelo hude, npr.:

- nepooblaščena sprememba, uničenje ali razkritje občutljivih podatkov oziroma informacij,
- nepooblaščena sprememba dostopnih pravic,
- ohromitev strežnika ipd.

Glavne skupine programskih vsiljivcev so programski vsiljivci, ki se razmnožujejo (virusi in črvi), ter programski vsiljivci, ki se ne razmnožujejo (trojanski konji in zlonamerna prenosna koda).

3.12.1 Računalniški virusi

Računalniški virus je programska koda, ki se je sposobna razmnoževati in prenašati v računalniku brez vednosti in volje uporabnika. Ko se razmnoži, lahko tudi prične s škodljivim delovanjem, npr. brisanjem podatkov na trdem disku. Ime virus je dobil, ker je njegovo vedenje zelo podobno biološkemu virusu. Gostitelj virusa je računalniški program oziroma izvršna datoteka. Med razmnoževanjem in prenašanjem se začasno naseli tudi v ostale dele pomnilnika (slikovne datoteke, sistemski del trdega diska itd.).

Poleg uničevanja podatkov lahko virusi povzročajo še druge težave. Pogosto so samo nadležni, npr. izpisujejo sporočila na zaslon. Nekateri virusi se sprožijo šele po tem, ko preteče določen čas od okužbe računalnika, ob določenem datumu ali ko okužijo zadostno število drugih računalnikov. Virus, ki ne povzroča škode, kljub temu troši računalniške vire, na primer obremenjuje procesor in zapolnjuje pomnilnik.

Pred virusi se branimo s protivirusnimi programi, požarnimi zidovi in s sprotnim nameščanjem popravkov programja. Eden od učinkovitih načinov je ta, da ne uporabljamo administratorskih pravic, tako da se virus ne more namestiti na računalnik. S tem se obvarujemo tudi pred vohunskim programjem.

Računalniški virusi niso omejeni samo na osebne računalnike in na operacijski sistem Windows. Obstajajo tudi za ostale operacijske sisteme, na primer UNIX/Linux, in ostale procesorske naprave, kot so mobilni telefoni in dlančniki. Prvi računalniški virusi so se pojavili za velike računalnike, z razmahom osebnih računalnikov pa so se pisci virusov osredotočili tudi nanje.

Eden bolj znanih virusov se imenuje Michelangelo, ki se sproži šestega marca, na obletnico rojstva italijanskega umetnika Michelangela, in zbriše vsebino trdih diskov.

Obstajajo naslednje vrste virusov:

- prevedeni virusi (angl. compiled viruses):
    - parazitski virusi,
    - virusi zagonskega sektorja,
    - kombinirani virusi,
- interpretirani virusi (angl. interpreted viruses):
    - makro virusi,
    - skriptni virusi.

Virusi lahko pridejo v računalnik na različne načine, na primer z okuženimi prenosnimi pomnilniškimi mediji in s programsko opremo, ki jo namestimo z interneta. Najbolj priljubljen način pa je prenašanje virusov po elektronski pošti z okuženimi priponkami (Brezavšček, 2007).

3.12.2 Črvi

Črvi so programski vsiljivci, ki se samodejno razmnožujejo po računalniškem omrežju. Za razmnoževanje ne potrebujejo nobene nosilne datoteke. Glavne razlike med virusi in črvi so, da so črvi samostojni programski vsiljivci, medtem ko virusi potrebujejo za razmnoževanje nosilno datoteko. Črvi se razmnožujejo samodejno brez intervencije uporabnika. Za razmnoževanje izkoriščajo znane ranljivosti in pomanjkljivosti v konfiguraciji, napake v komunikacijskih protokolih in druge slabosti omrežja in omrežnih povezav. Virus pa se razmnoži, kadar ga uporabnik aktivira. Isti črv se navadno pojavi v več različicah. Črvi so velikokrat nevarnejši od virusov in jih je teže odstraniti.

Znani sta dve vrsti črvov:

- poštni črvi: pojavili so se leta 1999, razmnožujejo pa se preko elektronske pošte. Ko črv okuži sistem, se običajno avtomatsko, brez vednosti uporabnika, razpošlje na vse naslove v poštnem imeniku. S svojo prisotnostjo in samodejnim razpošiljanjem preobremenjuje poštne strežnike;
- omrežni črvi: pojavili so se leta 2003. Za razmnoževanje izkoriščajo ranljivosti omrežnih storitev, povezanih z operacijskim sistemom oziroma določeno aplikacijo. Ko črv okuži nek sistem, navadno uporabi ta sistem za

iskanje drugih sistemov, ki tudi uporabljajo kritično storitev. Razmnožuje se najhitreje med doslej znanimi programskimi vsiljivci.

Zlonamerne aktivnosti črvov so obremenitev računalniških virov in omrežja s čim hitrejšim razmnoževanjem, kar lahko ohromi strežnik in naredi omrežje nerazpoložljivo. Črvi lahko namestijo zlonamerno orodje, ki omogoča nadaljnjo zlorabo sistema.

3.12.3 Trojanski konji

Trojanski konj je zlonamerna koda, ki se maskira v legitimen program. Za razliko od virusov in črvov so trojanski konji v sistemu pogosto pritajeni. Običajno je trojanski konj samostojen program v obliki izvedljive datoteke. Po načinu delovanja lahko trojanske konje razvrstimo v naslednje skupine:

- izvajanje funkcije legitimnega programa se ne prekine, vzporedno z njo se izvaja še zlonamerna aktivnost;
- izvajanje funkcije legitimnega programa se ne prekine, vendar se le-ta spremeni tako, da se izvede zlonamerna aktivnost oziroma tako, da se zlonamerna aktivnost prikrije;
- zlonamerna aktivnost popolnoma zamenja funkcijo legitimnega programa.

Zlonamerne aktivnosti trojanskih konjev so pridobiti kontrolo nad sistemom (kraja gesel, dostopne pravice), namestitev zlonamernih orodij, ki omogočajo nadaljnjo zlorabo sistema, ter širjenje vohunskih programov (angl. spyware).

3.12.4 Zlonamerna prenosna koda

Zlonamerna prenosna koda je programska koda, ki se je sposobna prenesti iz nekega oddaljenega mesta v omrežju na lokalni računalnik in se tam izvesti. Za izvajanje navadno ne potrebuje namestitve in kakršnegakoli posredovanja uporabnika. Prenosna koda običajno temelji na eni izmed naslednjih tehnologij:

- ActiveX kontrole,
- JavaScript,
- VBScript,

- flash animacije.

Tehnologija prenosnih kod je bila razvita dobronamerno, vendar se v današnjih časih uporablja tudi za zlonamerna dejanja. Zlonamerna koda je koda, ki izvede zlonamerno akcijo, se ne razmnožuje in navadno napade datoteke na računalniku tako kot virusi in črvi. Velikokrat se uporablja za razširjenje vohunskih programov

Tabela 1: Lastnosti glavnih skupin programskih vsiljivcev

Lastnost	Je samostojna datoteka?	Se razmnožuje?	Način razmnoževanja
Virus	Ne	Da	Interakcija uporabnika
Črv	Da	Da	Samodejno
Trojanski konj	Da	Ne	-
Zlonamerna prenosna koda	Ne	Ne	-

3.13 Protivirusna orodja

Protivirusna orodja so programska orodja, ki omogočajo zaznavanje prisotnosti programskega vsiljivca in njegovo odstranitev v primeru okužbe sistema. Protivirusni program je namenjen predvsem obrambi pred računalniškimi virusi. Z razvojem tehnologije so računalniški virusi spremenili način razmnoževanja in tako so se razvili tudi trojanski konji. Če na računalniku ni nameščenega protivirusnega programa oziroma ta ni dovolj kakovosten, je to verjetno razlog za okvaro strojne ali programske opreme, okvaro datotek s podatki in podobno.

Strokovnjaki za informacijsko varnost so nemalokrat presenečeni, da mnogo uporabnikov ne poskrbi niti za najosnovnejšo varnost računalnikov, torej za dober protivirusni program. Zaskrbljujoče je, da to velja tudi za tisti fizične osebe in podjetja, ki uporabljajo vedno bolj razširjene širokopasovne povezave, ki so zaradi dolgotrajne povezanosti v internet veliko bolj ranljive (Frelih, 2005).

Večina protivirusnih orodij deluje na enem izmed naslednjih principov:

- zaznavanje prisotnosti programskega vsiljivca na osnovi njegovega podpisa. Ta metoda temelji na tradicionalnem pristopu odstranjevanja, je zelo zanesljiva za znane programske vsiljivce, vendar orodja, ki temeljijo na tem pristopu, novega vsiljivca ne prepoznajo, dokler proizvajalec orodja ne posodobi baze programskih vsiljivcev;
- zaznavanje prisotnosti programskega vsiljivca na osnovi obnašanja sistema, kar je novejši pristop. Protivirusna orodja se ukvarjajo s preučevanjem značilnosti obnašanja sistema, ki bi lahko nakazovale, da je v sistemu prisoten programski vsiljivec, npr. avtomatsko masovno razpošiljanje elektronske pošte. Protivirusno orodje poskuša te aktivnosti preprečiti, sumljivo kodo pa izolira, dokler je administrator ne preuči. Prednost je, da orodja, ki delujejo na tem principu, načeloma lahko zaznajo tudi nove programske vsiljivce, katerih podpisov še ne poznajo. Slabost pa je, da če niso tolerance normalnega obnašanja sistema pravilno definirane, se lahko velikokrat sproži alarm po nepotrebnem.

Sposobnosti, ki jih mora imeti protivirusno orodje, so:

- preiskovanje kritičnih komponent sistema (npr. zagonskih datotek, BIOS-a, zagonskega sektorja),
- nadziranje aktivnosti sistema v realnem času (npr. preiskovanje poštnih prilog, datotek, naloženih z interneta itd.),
- nadziranje obnašanja kritičnih aplikacij (npr. poštnih odjemalcev, spletnih strežnikov, programov za prenašanje datotek ipd.),
- periodično preiskovanje trdih diskov in drugih pomnilniških medijev, možnost izvedbe preiskovanja v poljubnem trenutku (na zahtevo),

- zmožnost identificiranja vseh glavnih tipov programskih vsiljivcev (virusov, črvov, trojanskih konjev, zlonamerne prenosne kode) kot tudi zlonamernih orodij, ki jih programski vsiljivec lahko namesti v sistem,
- sposobnost dezinfekcije okuženih datotek in sposobnost izvedbe karantene za okužene datoteke.

3.13.1 Pomembne lastnosti protivirusnih programov

Dober protivirusni program je pri svojem delu uspešen, ko je natančen, zmogljiv, učinkovit in prijazen do uporabnika. Pri tem ne bi smel spremeniti originalnih podatkov oziroma mora imeti uporabnik možnost razveljavitve sprememb. Pomembno je, da protivirusni program pri svojem delovanju ne podvoji sporne programske kode. Dober protivirusni program bi moral čim manjkrat sprožiti lažni alarm kot posledico netočne zaznave sporne programske kode. Zanesljivost oziroma učinkovitost protivirusnega programja je zelo odvisna od tega, kako pogosto se posodabljajo virusne definicije in kako hiter je proces zaznavanja virusov v računalniku.

Protivirusni programi se med seboj razlikujejo tudi po hitrosti delovanja. Nekateri zelo upočasnijo delovanje računalnika, saj za delovanje v realnem času porabijo veliko procesorske in pomnilniške zmogljivosti. Še zlasti veliko jih porabijo tisti programi, ki omogočajo hevristično identificiranje virusov z ugibanjem na podlagi predhodnih izkušenj z okuženimi datotekami oziroma virusi.

Danes večina boljših protivirusnih programov podpira pregledovanje drugotnega toka podatkov (angl. Alternate Data Stream, ADS). Nekatere programske hiše so za pregledovanje ADS izdelale ločena programska orodja. V ADS je mogoče skriti mnoge podatke, težava pa je v tem, da se samo ADS ne da izbrisati, ne da bi se izbrisal prvotni tok podatkov ali datoteka, na katero je vezan ADS.

Protivirusni programi imajo že nekaj časa vgrajeno možnost sprotnega preverjanja dohodne oziroma odhodne elektronske pošte. Tudi to je lastnost, ki je bistvena za kakovost protivirusnega programa, saj se računalnik pri povprečnem uporabniku najpogosteje okuži z virusi, ki pridejo vanj z elektronsko pošto (Frelih, 2005).

4 ANKETA O INFORMACIJSKI VARNOSTI

Namen ankete je bil ugotoviti stanje informacijske varnosti v podjetjih na Goriškem. Anketa (Priloga 1) je bila v začetku leta 2008 poslana po elektronski pošti štiridesetim podjetjem, vrnilo pa se je devetnajst izpolnjenih anket. Sestavljena je iz štirih sklopov: strežniki, varnost podatkov, možnost dela na daljavo in zaščita. Anketo so izpolnjevali predvsem IT strokovnjaki v izbranih podjetjih oziroma strokovnjaki zunanjih podpornih služb, ki vzdržujejo informacijske sisteme družb.

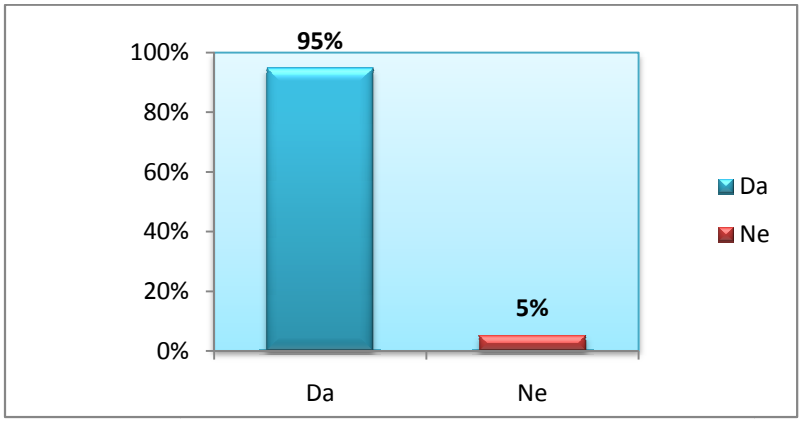
Nekatera vprašanja so bila zasnovana tako, da je anketiranec lahko odgovoril nanj z več odgovori. V nadaljevanju analiziramo informacijsko varnost anketiranih podjetij na osnovi zbranih anketnih odgovorov.

4.1 Strežniki

V vsakdanjem življenju se veliko govori o različnih strežnikih. Nekateri imajo v mislih strojno, drugi programsko opremo, vsi pa so si enotni, da so ključni poslovni sistemi zgrajeni na strežnikih. Podjetja oziroma delovna skupina, v katero je vključenih vsaj pet ljudi, načeloma že potrebuje strežnik.

Vsa anketirana podjetja so imela nad pet zaposlenih, zato smo želeli izvedeti, ali imajo strežnik. Anketno vprašanje se je glasilo:

Ali imate v podjetju strežnike?



Slika 14: Strežniki v podjetjih

Po analizi anket smo ugotovili, da imajo skoraj vsa anketirana podjetja strežnike (slika 14). To je povsem razumljivo, saj bi bilo poslovanje brez strežnika skoraj nemogoče. V praksi naj bi imelo podjetje vsaj domenski strežnik in posledično domeno. Z določitvijo domene se morajo vsi uporabniki overiti, preden lahko dostopajo v sistem. S postavitvijo domene se poveča varnost in centralizira nadzor nad uporabniškimi pravicami.

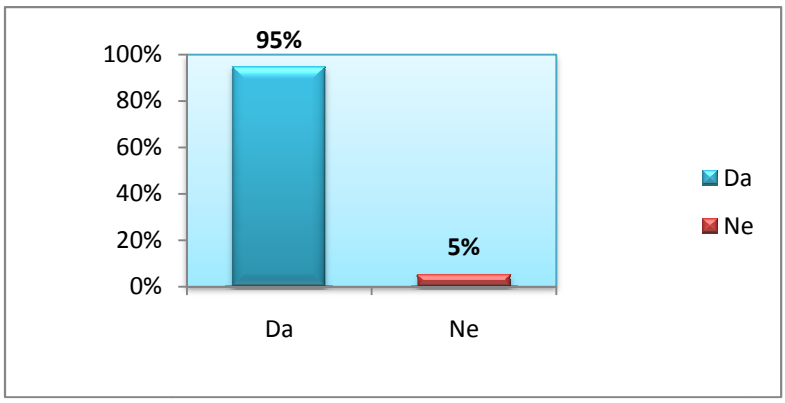
4.2 Varnostno kopiranje

Sodobnega poslovanja si danes skoraj ne znamo več predstavljati brez računalnika. Z njim opravimo večino našega dela in hranimo vse pomembne podatke ter dokumente. A vendar vsak dan tvegamo dogodke, ki lahko poškodujejo ali celo trajno uničijo te dokumente. Izguba podatkov, ki so vitalnega pomena za poslovanje podjetja, pa je za podjetje lahko usodna. Skrb za varnostne kopije in učinkovita obnova podatkov sta zato osnova sodobnega poslovanja. Varnost občutljivih poslovnih podatkov se začne z omejevanjem fizičnega dostopa do teh podatkov in konča s strokovno opravljenim šifriranjem podatkov.

Cilj vprašanj je ugotoviti, ali se podjetja zavedajo pomembnosti svojih podatkov in na kakšen način jih shranjujejo oziroma izdelujejo varnostne kopije.

V tem sklopu so bila postavljena štiri anketna vprašanja. Prvo vprašanje se je glasilo:

Ali uporabljate polja RAID?



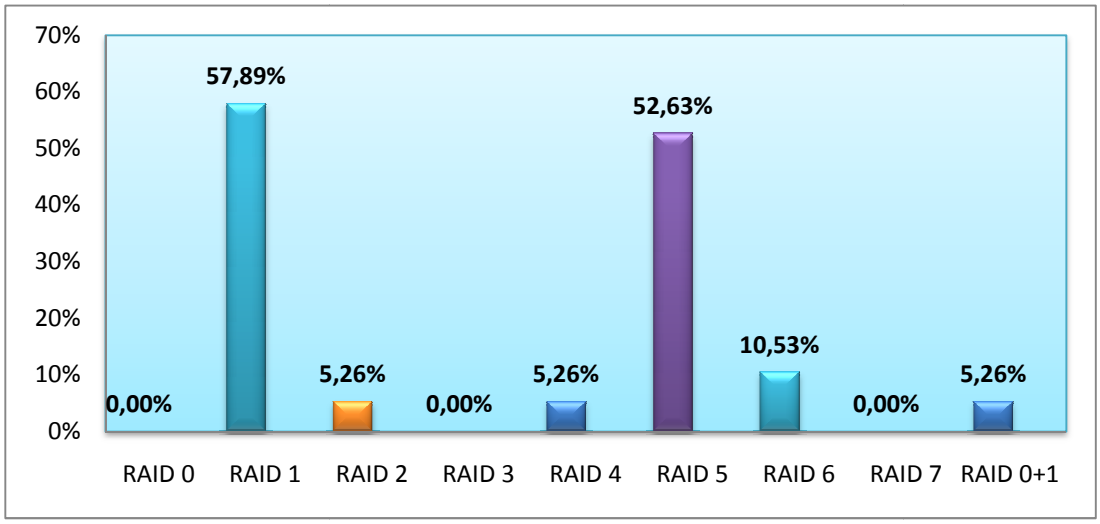
Slika 15: Uporaba polj RAID v podjetjih

Z analizo anket smo ugotovili, da večina podjetij trde diske v strežniku združuje v polja RAID (slika 15).

Naslednje anketno vprašanje v tem sklopu je bilo:

Katera polja RAID uporabljate?

Anketiranci so na to vprašanje lahko odgovorili z več odgovori. Podjetja namreč lahko uporabljajo več različnih RAID arhitektur hkrati.

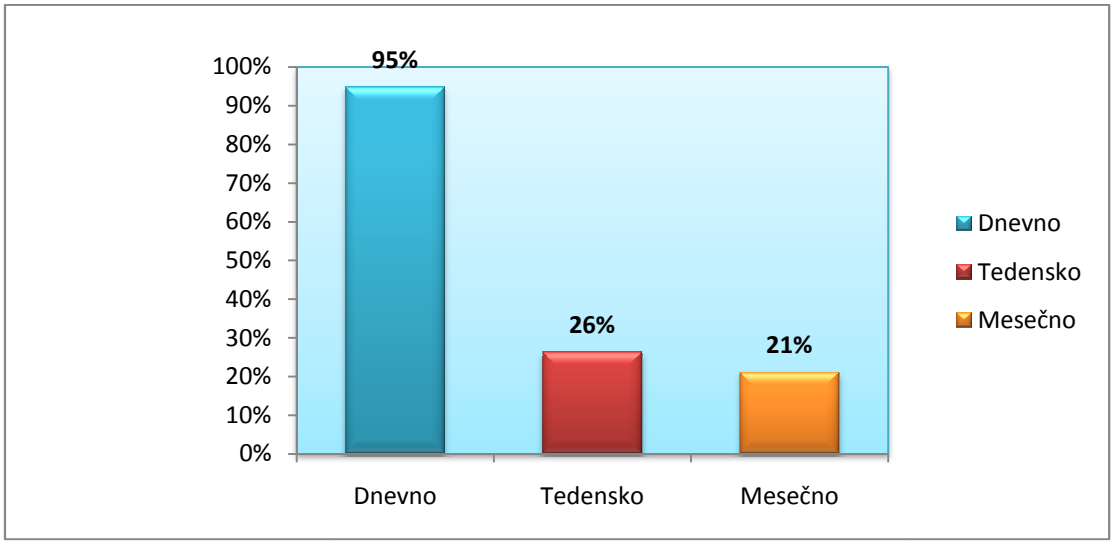


Slika 16: Najbolj uporabljena polja RAID v podjetjih

Najbolj priljubljena tipa diskovnih polj sta RAID 1 in RAID 5. Sledi jima RAID 6 (slika 16), ki ga uporabljajo večinoma v večjih podjetjih oziroma tam, kjer so podatki zelo pomembni. V manjših podjetjih se v praksi odločajo za diskovno polje RAID 1. Pri konfiguraciji diskovnega polja RAID 1 imamo isto vsebino podatkov na obeh povezanih diskih. Če eden izmed njiju izpade ali preneha delovati, samodejno nastopi drugi. Delovanje podjetja je v tem primeru nemoteno. Težava bi nastala, če bi prenehala delovati oba diska.

Tretje vprašanje iz sklopa o varnosti podjetij se je glasilo:

Kako pogosto izdelujete varnostne kopije vaših podatkov?

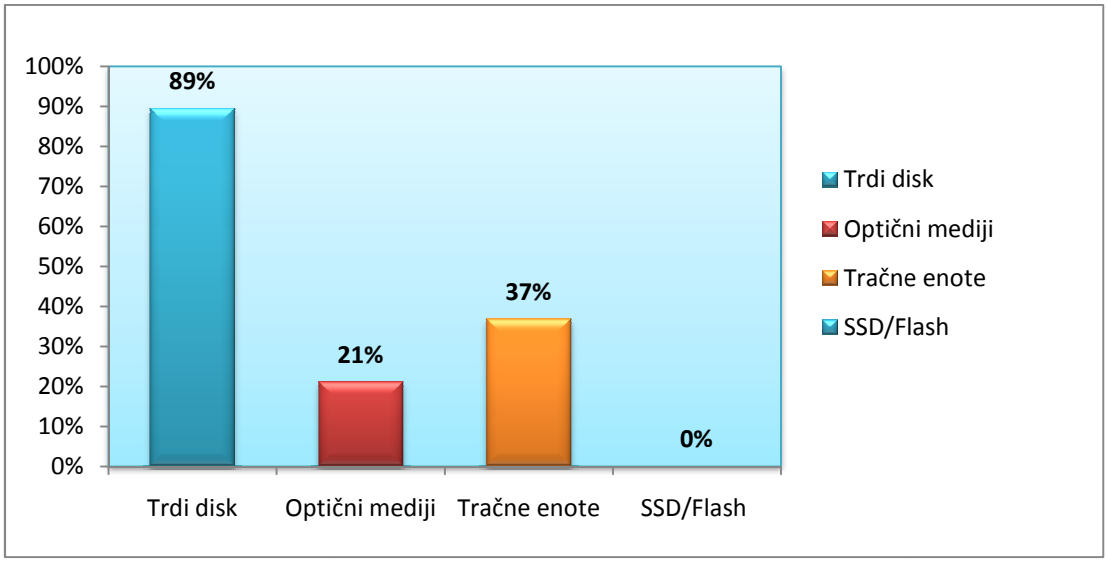


Slika 17: Pogostost izdelovanja varnostnih kopij v podjetjih

Anketa je pokazala, da skoraj vsa anketirana podjetja podatke shranjujejo dnevno. Ta način shranjevanja družbi omogoča vedno zadnjo različico tekočega dela. Tedensko ter mesečno shranjevanje je tudi zelo priljubljeno, vendar zajema več dnevnih varnostnih kopij, ki se jih združi v tedenske oziroma mesečne arhive (slika 17). V praksi podjetja izdelujejo varnostne kopije vsak dan v tednu. Ob nastopu novega tedna pa začnejo znova prepisovati podatke na že obstoječi dnevni arhiv. Ta način omogoča arhiv zadnjih sedem oziroma pet dni. Prva pomanjkljivosti tega pristopa je, da lahko povrnemo prejšnje stanje samo do pet oziroma sedem dni nazaj, druga pomanjkljivost pa je, da potrebujemo osebo, ki dnevno menja arhivske medije.

Zadnje vprašanje tega sklopa je bilo:

Na katere podatkovne medije shranjujete varnostne kopije?



Slika 18: Podatkovni mediji za varnostne kopije

Najbolj priljubljen medij za shranjevanje varnostnih kopij podatkov je trdi disk (slika 18). K takemu načinu shranjevanja podatkov je pripomogla zelo nizka cena trdih diskov ter njihova dolga življenjska doba. Glede na zanesljivost shranjenih podatkov so v praksi najbolj uporabljene tračne enote, saj je njihova kapaciteta velika in življenjska doba zelo dolga. Zapisi so kakovostni in dosegajo tudi do dvajset let življenjske dobe. Primerjavo medijev za shranjevanje podatkov prikazuje tabela 2.

Tabela 2: Prednosti in slabosti podatkovnih medijev

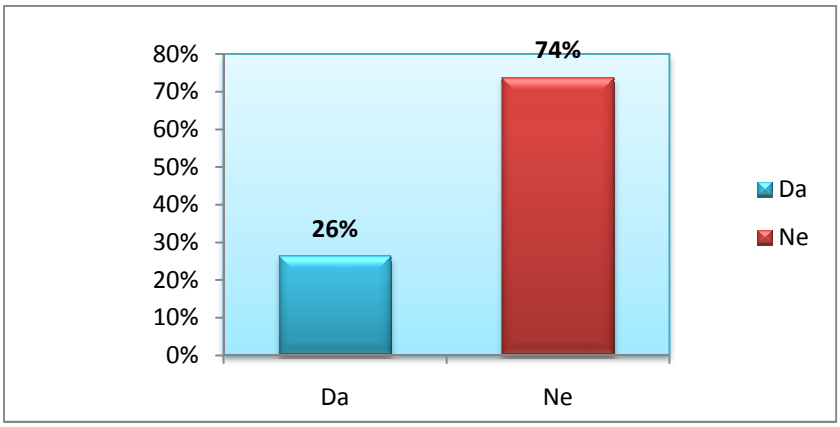
	Prednosti	Slabosti
Trdi disk	Cena Kapaciteta Hitrost zapisovanja	Življenjska doba
Optični mediji	Cena	Življenjska doba Kapaciteta Hitrost zapisovanja
Tračne enote	Življenjska doba (20 let) Kapaciteta	Cena Hitrost zapisa
Mediji SSD/ Flash	Življenjska doba (več kot 10 let)	Cena, Kapaciteta Hitrost zapisovanja

4.3 Smernice informacijske varnosti

Vrednost informacije izvira iz treh njenih lastnosti: zaupnosti, neokrnjenosti in razpoložljivosti (angl. confidentiality, integrity and availability). Informacijski sistem je sestavljen iz treh glavnih delov: strojne opreme, programske opreme in standardov informacijsko varnostne industrije, ki se uporablja kot mehanizem zaščite in preprečitve na treh ravneh: fizičnem, osebnostnem in organizacijskem. Bistveno je, da se ljudem pove (administratorjem, uporabnikom, operaterjem), kako uporabljati produkte, da se zagotovi informacijska varnost znotraj organizacije. Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem.

Na smernice informacijske varnosti se je nanašal sklop treh vprašanj. Prvo vprašanje iz sklopa se je glasilo:

Ali v vašem podjetju sledite smernicam informacijske varnosti?



Slika 19: Sledenje smernicam informacijske varnosti v podjetjih

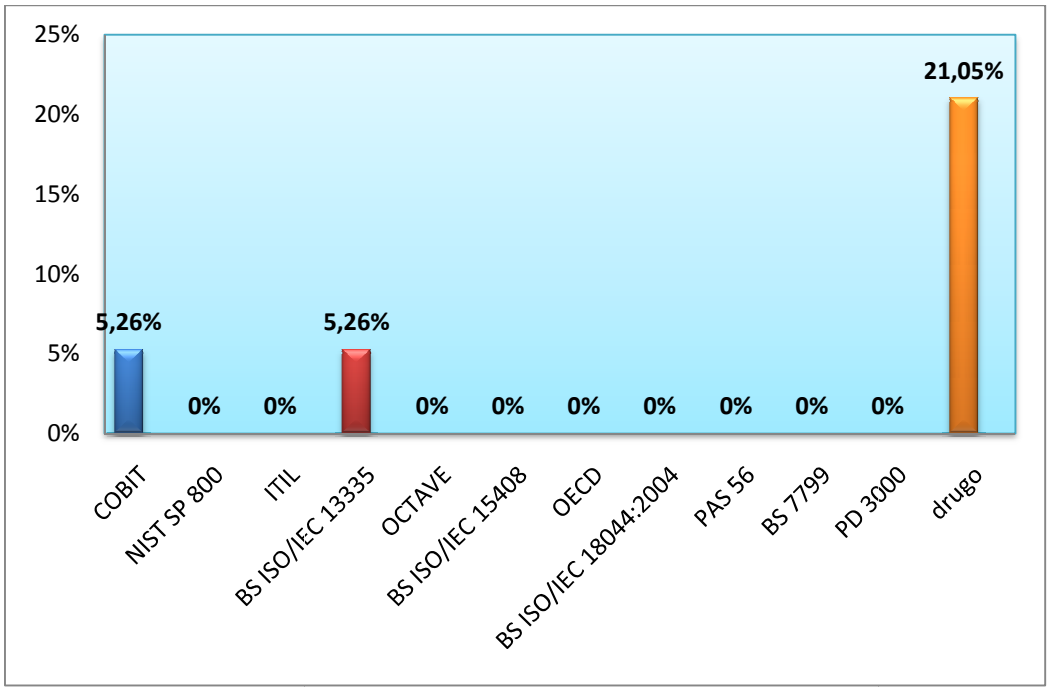
Kljub temu, da se informacijska varnost v podjetjih v zadnjih letih močno povečuje, rezultati ankete kažejo, da le četrtina podjetij na anketiranem območju sledi smernicam informacijske varnosti (slika 19). Razlog lahko iščemo v velikosti anketiranih podjetij, saj so le večja med njimi odgovorila na vprašanje pritrdilno. Seveda za manjša podjetja to ni opravičilo, da ne sledijo smernicam in priporočilom, vsekakor pa ne moremo spregledati dejstva, da za manjša podjetja to predstavlja dodaten strošek, ki pa je lahko v primeru koriščenja zunanjih profesionalnih storitev

relativno majhen. Podjetja vedno bolj spoznavajo pomen informacijske varnosti, zaradi česar se pričakujejo večja vlaganja tudi v ta segment.

Drugo anketno vprašanje iz sklopa je bilo:

Katerim smernicam sledite?

Na vprašanje je bilo možnih več odgovorov. Določena podjetja pa sploh ne uporabljajo nobene od smernic informacijske varnosti.

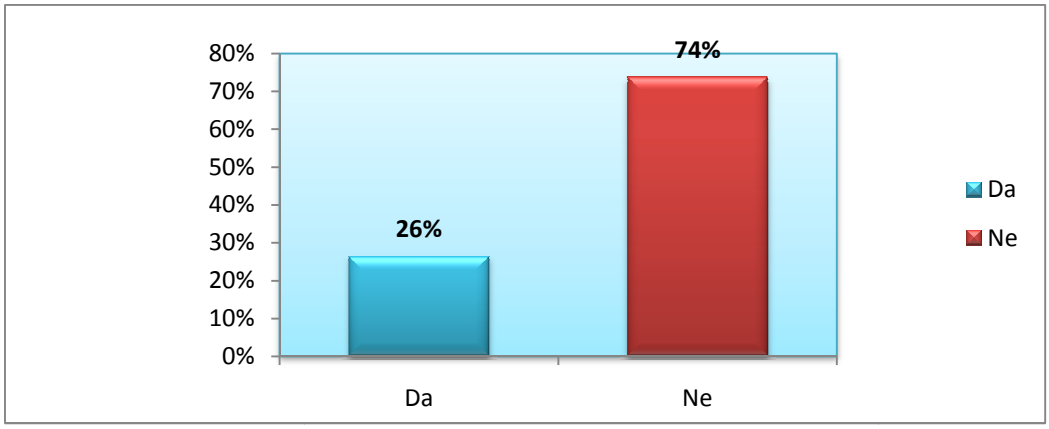


Slika 20: Uporabljene smernice informacijske varnosti v podjetjih

Kot je razvidno iz grafikona (slika 20), večina podjetij sploh ne sledi smernicam informacijske varnosti. Poudariti gre tudi to, da so anketirana podjetja majhna ter da je večina standardov napisanih za velike korporacije.

Tretje anketno vprašanje o smernicah informacijske varnosti je bilo:

Ali ima vaše podjetje sistemskega varnostnega administratorja?



Slika 21: Prisotnost sistemskih varnostnih administratorjev v podjetjih

Tri četrtine anketiranih podjetij nima internega zaposlenega delavca za nadzor informacijskega sistema (slika 21), saj so postavljeni sistemi zelo stabilni in ne potrebujejo mnogo administracije. Vedno več podjetij se zato odloča za zunanje izvajalce, ki so zelo učinkoviti ter cenejši, kot da bi podjetje zaposlilo delavca zgolj za ta namen. Težava nastopi tudi pri izobraževanju tovrstnih internih kadrov, saj so izobraževanja draga, podjetja pa po večini gledajo na to kot na nepotreben strošek. Pri zunanjih izvajalcih pa si lahko zagotovijo izobražen in profesionalen kader, ki ga dobijo praktično na klic.

V podjetjih je smiselno zaposliti IT strokovnjaka, ko se obseg posegov v korekture oziroma vzdrževanje informacijskega sistema drastično poveča. V tem primeru je nižji strošek, če ima podjetje lastnega IT strokovnjaka, kot da plačuje zunanjo podporno službo.

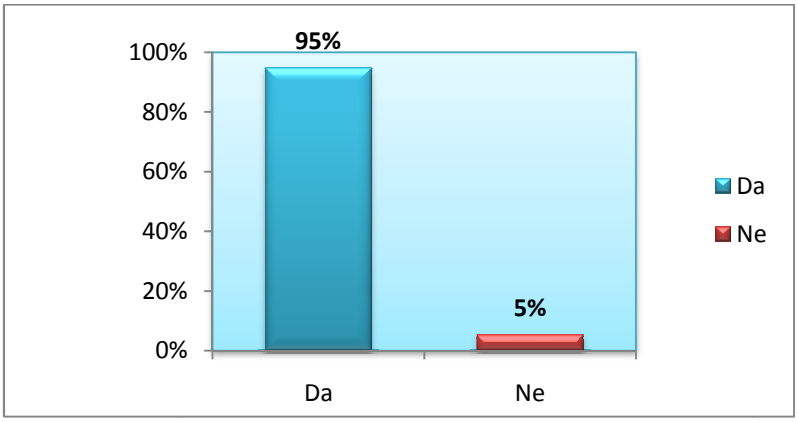
4.4 Oddaljeni dostopi in omrežja

Poslovanje že dolgo ni več omejeno in ga ni potrebno opravljati le v pisarni podjetja. Najnovejši način dela, hkrati pa tudi prilagajanje strankam in vedno večja konkurenca nas silijo, da veliko dela opravimo tudi izven pisarn, hkrati pa se povečuje število mobilnih delavcev, ki morajo svoje delo opravljati izven podjetja (od doma ali s terena) ali iz oddaljenih poslovnih enot. Oddaljenemu načinu dela sledi tudi tehnologija, na eni strani s številnimi prenosnimi napravami (prenosniki, dlančniki, pametni telefoni) z vse večjo funkcionalnostjo, na drugi strani pa s številnimi možnostmi hitrih, tudi brezžičnih komunikacij. Mobilnosti delovne sile

zato še nikoli ni bila tako preprosto udejanjiti, saj je z ustrezno rešitvijo do informacij in poslovnih transakcij mogoče dostopati s katerekoli naprave, od koderkoli in kadarkoli. S tem je mogoče rešiti številne težave, ki so podjetjem z mobilno delovno silo zagotovo znane.

Znotraj sklopa so bila zastavljena štiri anketna vprašanja. Prvo anketno vprašanje je bilo:

Ali imate v vašem podjetju možnost dela z oddaljene lokacije?



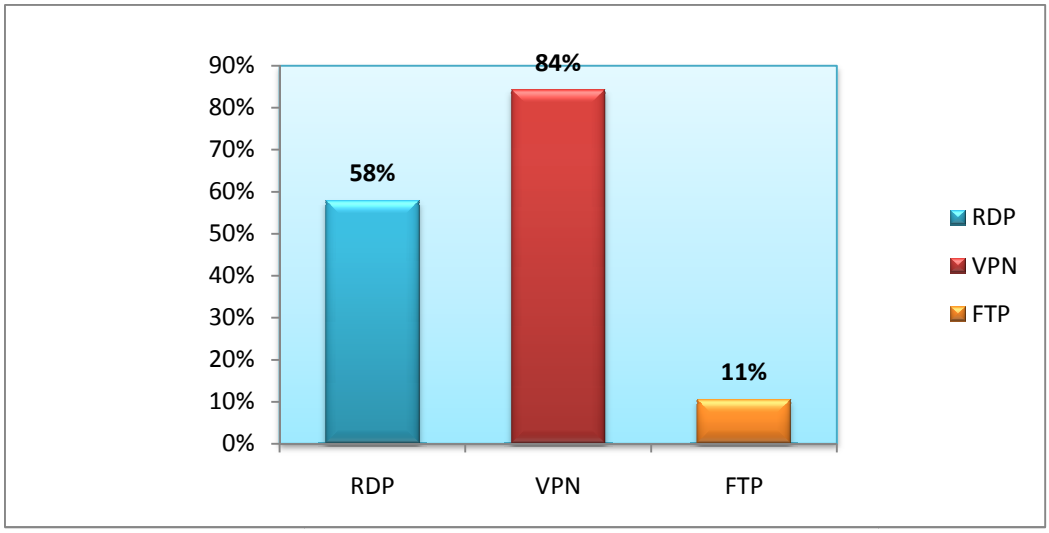
Slika 22: Delo z oddaljene lokacije

Večina podjetij svojim uslužbencem omogoča delo z oddaljene lokacije (slika 22). Z nenehnim tekmovanjem v konkurenčnosti in ponudbi storitev je postalo nujno, da podjetja ponudijo svoje izdelke in storitve preko interneta in klicnih linij. Pri tem pa morajo na enostaven način omogočati dostop do informacij, ki jih želijo uporabniki. Poleg overitev uporabnika na sami aplikaciji je ključnega pomena njegova overitev na dostopu do omrežja, v katerem se nahajajo storitve. V grobem lahko razdelimo dostop do storitev na oddaljen dostop preko klicnih linij in oddaljen dostop do interneta.

Drugo anketno vprašanje v sklopu je bilo:

Kakšen način dostopa na daljavo imate?

Na vprašanje je bilo možnih več odgovorov. Zaposleni v podjetjih lahko dostopajo do računalniških virov na več načinov.



Slika 23: Dostopi do računalniških virov na daljavo

Kot pričakovano skoraj vsako od anketiranih podjetij omogoča uslužbencem tudi delo na daljavo (slika 23).

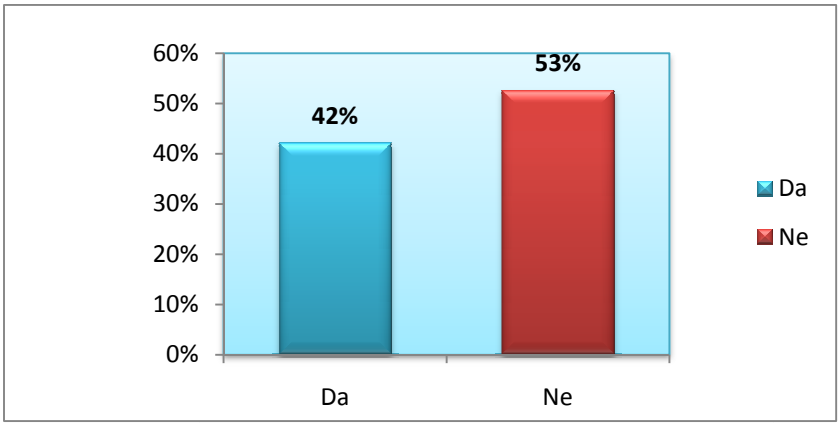
Najbolj uporabljeno je navidezno zasebno omrežje (VPN), ki uporabniku omogoča delo, kot da bi bil v podjetju. RDP je druga izbira podjetij, saj je ta zelo fleksibilna, ker lahko z zelo slabo internetno povezavo deluje brez težav. Pri RDP povezavi pošiljamo na oddaljeno lokacijo samo signal miške in tipkovnice, z oddaljene lokacije pa nam pošilja sliko. FTP je skoraj pozabljen, saj ne ponuja nobene zaščite in je zelo ranljiv. V praksi se ga uporablja za hiter dostop do podatkov zunaj podjetja. Vendar je boljša izbira vzpostavitev VPN povezave, ker se tako oddaljeno varno povežemo v omrežje podjetja in imamo na razpolago podatke, ki jih potrebujemo.

V praksi se uporabljata VPN ter RDP skupaj, kajti RDP uporablja TCP vrata 3389, ki so zelo na udaru napadov. To težavo rešimo tako, da najprej vzpostavimo VPN povezavo, nato pa uporabimo RDP za lokalni dostop do želenega terminala. V tem primeru so lahko TCP vrata 3389 zaprta.

Ker lahko eno podjetje omogoča vse tri načine dostopa na daljavo, je skupni seštevek odgovorov več kot 100 %.

Tretje anketno vprašanje o oddaljenih dostopih in omrežjih je bilo:

Ali imate v vašem podjetju brezžično lokalno omrežje WLAN?



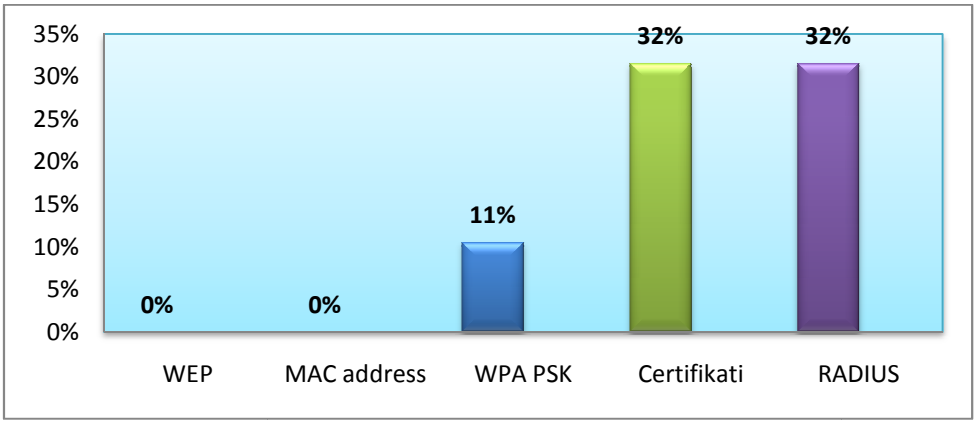
Slika 24: Uporaba brezžičnih omrežij v podjetjih

Večina podjetij brezžičnih omrežij ne uporablja, ker imajo lokalno omrežje tako zasnovano, da bi bila ta izbira nesmiselna (slika 24). Podjetja uporabljajo brezžična omrežja najpogosteje v sejnih sobah, kjer je brezžično omrežje ločeno od glavnega omrežja. V takih primerih se brezžična omrežja uporablja zgolj za dostop do interneta oziroma brezžičnega lokalnega omrežja.

Četrto anketno vprašanje iz tega sklopa se je glasilo:

Kako je brezžično omrežje zaščiteno?

Vprašanje je imelo več možnih odgovorov, nekatera podjetja pa sploh niso izbrala nobene od podanih možnosti.



Slika 25: Zaščita brezžičnih omrežij

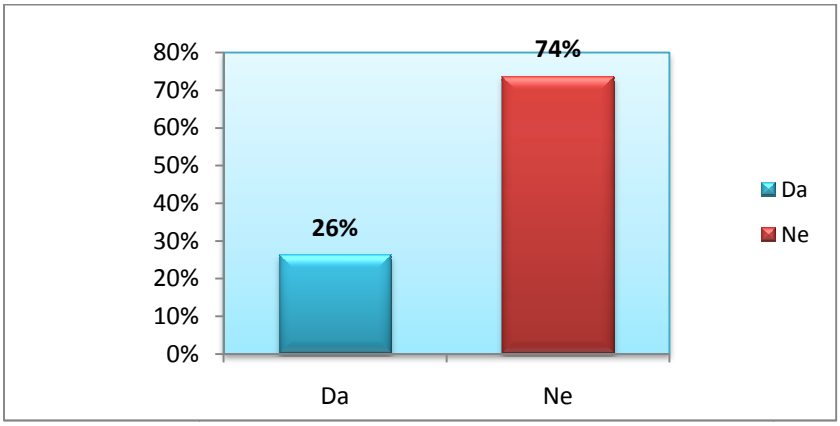
Podjetja, ki so se odločila za brezžično omrežje, uporabljajo prijavo s certifikati ter avtorizacijo prek strežnika RADIUS (slika 25). Taka oblika zaščite je zelo primerna.

V praksi brezžična omrežja zahtevajo dodatni nadzor in s tem povzročajo dodatne stroške podjetju. Uporabljajo se le tam, kjer je to nujno potrebno, ali tam, kjer je zaradi narave dela potrebna mobilnost. Iz rezultatov ankete je razvidno, da nekateri ne uporabljajo nobenega od ponujenih standardov zaščite brezžičnih omrežij.

4.5 Šifriranje podatkov

V informacijski varnosti se kriptografija uporablja za preoblikovanje oblike podatkov v obliko, ki je uporabna samo za pooblaščene uporabnike. Ta proces imenujemo šifriranje. Podatki, ki smo jih šifrirali, se lahko preoblikujejo nazaj v prvotno obliko s pomočjo pooblaščenega uporabnika, ki ima šifrirni ključ. Ta postopek imenujemo dešifriranje. Anketno vprašanje se je glasilo:

Ali pri posredovanju podatkov uporabljate šifriranje?



Slika 26: Uporaba šifriranja v podjetjih

Tri četrtine anketiranih podjetij šifriranja ne uporablja (slika 26), vendar bi bilo pri zaupnih podatkih šifriranje zelo primerno. Šifriranje se pogosto uporablja v bančništvu oziroma pri prenašanju zaupnih podatkov. Šifriranje podatkov nastopa tudi v primeru vzpostavitve lokalnega zasebnega omrežja, kjer se skozi vzpostavljen tunel pretakajo podatki v šifrirani obliki. Večja podjetja so zaradi zaupnosti sporočil, ki se posredujejo znotraj in zunaj podjetja, prisiljena uporabljati šifriranje. Iz rezultatov ankete je razvidno, da je takih podjetij le 26 %. Ostala podjetja se bodisi ne zavedajo, kakšno varnostno luknjo puščajo odprto, bodisi jim je strošek implementacije šifrirnega sistema previsok.

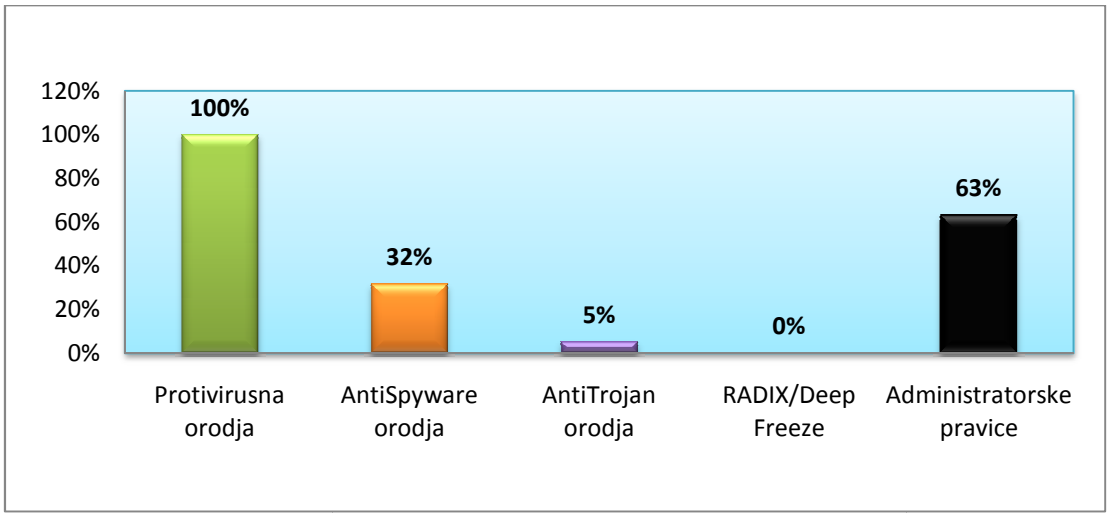
4.6 Zaščita informacijskega sistema

Varnost predstavlja za večino majhnih in srednje velikih podjetij velik izziv. S sistemi, priključenimi na internet, so podjetja vedno znova podvržena različnim zlonamernim grožnjam, kot so virusi, črvi, napadi hekerjev, nezaželena pošta ter neprimerne vsebine. Tako kot veliki poslovni sistemi so tudi majhna in srednje velika podjetja pri svojem vsakodnevnem poslovanju odvisna od lastne IT infrastrukture in interneta. Velika podjetja morajo ravno tako skrbeti za vzpostavljanje ravnotežja med svojimi poslovnimi in varnostnimi zahtevami. Vendar pa za razliko od velikih podjetij majhnim podjetjem primanjkuje znanja in virov s področja informacijske varnosti, zaradi česar so prisiljena iskati enostavne rešitve za upravljanje zaščite pred grožnjami.

Znotraj sklopa so bila zastavljena štiri anketna vprašanja. Prvo med njimi je bilo:

Kako se obvarujete pred virusom ter drugimi zlonamernimi kodami?

Vprašanje je imelo več odgovorov. Podjetja se lahko obvarujejo proti virusom in drugi zlonamerni kodi z več orodji hkrati.



Slika 27: Zaščita proti grožnjam

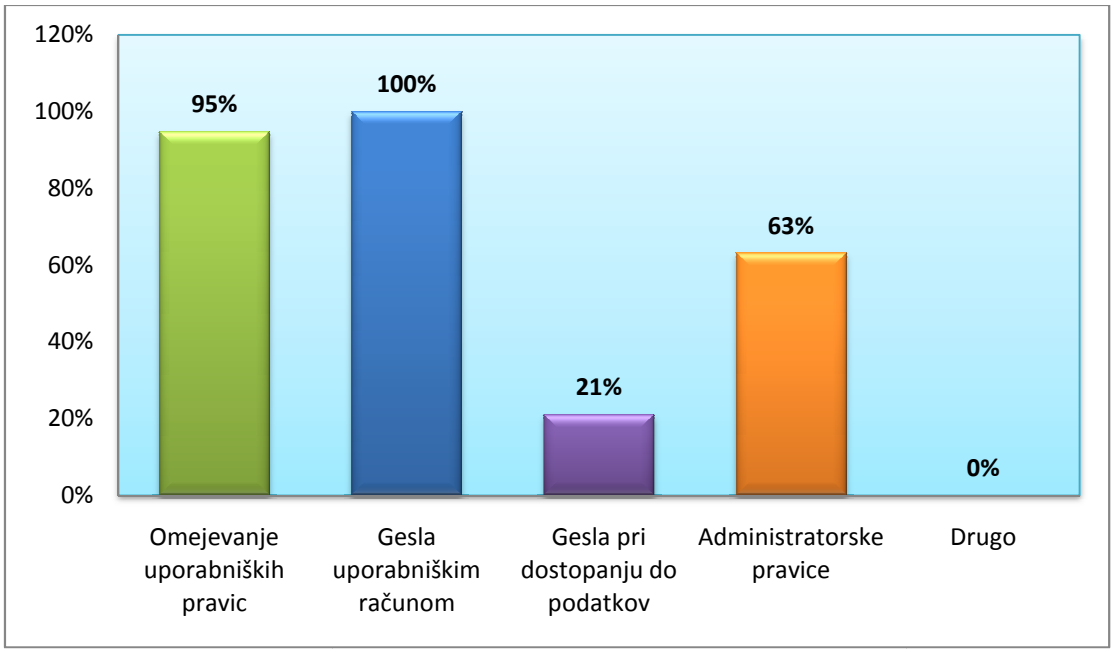
Ugotavljamo, da vsa anketirana podjetja uporabljajo protivirusno zaščito kot zadnji obrambni nivo zaščite pred virusi in črvi (slika 27). Omejevanje uporabniških pravic je na drugem mestu. Omejevanje uporabniških pravic je zelo zanimiva rešitev, saj sam uporabnik ne more namestiti nobene programske opreme, ne more dostopati do

sistemskih datotek in nastavitev ter jih spreminjati. S tem onemogočimo grožnje, ki so povezane z uporabniškimi dejanji. Protivirusni programi žal niso vsemogočna orodja za zaščito informacijskega sistema, saj največkrat prav uporabnik omogoči zagon zlonamerne aplikacije. Zato je dobro omejevati uporabnike s pravicami, kar onemogoča nekatera dejanja nad sistemom. V praksi si je težko predstavljati podjetja brez ustrezne protivirusne zaščite, saj so na trgu protivirusni produkti, ki nudijo celovito zaščito sistema in so danes že v uporabi v podjetjih.

Drugo vprašanje o zaščiti informacijskega sistema se je glasilo:

Kakšen sistem zaščite dostopa do podatkov imate?

Podanih je bilo več možnih odgovorov.



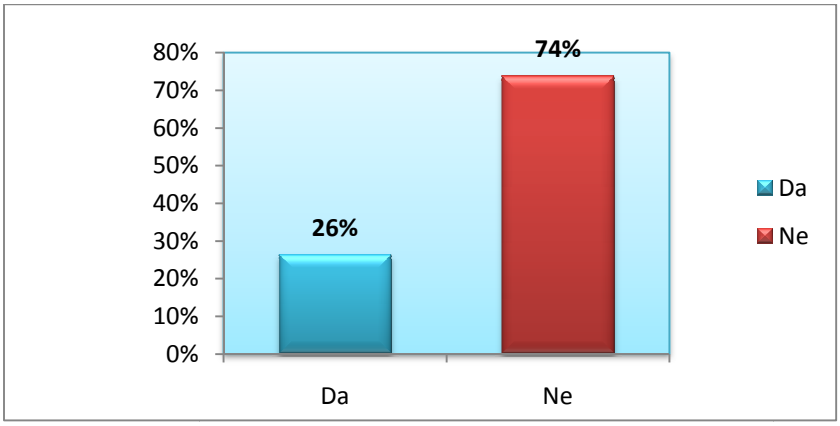
Slika 28: Zaščita dostopa in podatkov v podjetju

Vsa anketirana podjetja uporabljajo gesla za dostop do uporabniških računov (slika 28). Pri geslih za dostop do uporabniških računov je smiselno omeniti, da je to nuja pri sistemih, ki uporabljajo domeno. Pri overitvi z domeno dobi uporabnik »žeton«, s katerim se predstavlja sistemu s svojimi omejitvami in pravicami. Druga izbira je omejevanje pravic uporabnika. Gesla pri dostopu do podatkov pa niso tako uporabljena, ker z domeno pridobimo enotno prijavo (angl. single sign on) in se s tem znebimo ponovnih vpisovanj gesel, ki so včasih zelo zamudna. Administratorske

pravice so tudi zelo uporabljen način dostopanja do podatkov, vendar v praksi ni priporočljiv, saj uporabnikom s tem omogočimo vpogled do skoraj vseh podatkov v podjetju.

Tretje vprašanje v tem sklopu se je glasilo:

Ali ima vaše podjetje plan za ponovno vzpostavitev informacijskega sistema ter strojne opreme v primeru »katastrofe« (angl. Disaster Recovery Planing, DRP)?



Slika 29: Plan v primeru računalniške katastrofe

Glede na velikost anketiranih podjetij je razumljivo, da manjša podjetja nimajo izdelanega plana za ponovno vzpostavitev informacijskega sistema v primeru morebitne računalniške katastrofe (slika 29). Večja podjetja pa DRP imajo. DRP je obsežen proces, ki zajema plane za vzpostavitev informacijske infrastrukture, kot so strojna oprema, programska oprema, mrežne povezave, podatki ipd. Rezultati ankete kažejo, da ima izdelan plan 26 % anketiranih podjetij, vendar gre poudariti, da so za nekatera podjetja plani še v fazi razvijanja.

Za manjša podjetja je alternativa celotnemu planu vzpostavitve informacijskega sistema dobra politika izdelave varnostnih kopij ter pogodba z zunanjimi vzdrževalci za takojšni ukrep in izposojo strojne opreme.

Vsak izpad delovanja informacijskega sistema lahko povzroči podjetju hudo škodo. Dobra praksa in profesionalen kader, ki zna ob morebitni računalniški katastrofi hitro in učinkovito ukrepati, je vsekakor boljša od gore papirja.

5 PRIPOROČILA PODJETJEM

Razlogov, zakaj uvajati sisteme varovanja poslovnih informacij, je več, npr. preprečevanje vdorov v strogo varovane računalniške sisteme, preprečevanje kraje intelektualne lastnine in zaščita sistema pred virusi. Z uvedbo sistema varovanja informacij pa podjetje lahko ohranjanja konkurenčno prednosti in obstoj na svetovnem trgu, zato je pomembno, da podjetja v sistemu varovanja poslovnih informacij vidijo tudi poslovno priložnost. Obvladovanje tveganj, povezanih s človeškimi dejavniki, računalniškimi sistemi in tehnologijo, naravnimi vplivi okolja in obvladovanje tveganj izvedbe poslovnih procesov, so dovolj tehtni razlogi, da bi odločitev o uvedbi sistema varovanja poslovnih informacij moralo sprejeti vsako podjetje, katerega cilj je poslovati kakovostno, uspešno in učinkovito, predvsem pa dolgoročno. Pomembno je, da varnostne zahteve podjetja nastanejo kot posledica poslovnih zahtev in:

- zagotavljajo učinkovitost poslovanja,
- sledijo zakonskim in pogodbenim zahtevam,
- zagotavljajo zmanjševanje tveganj v podjetju.

Glavni razlog za obvladovanje informacijskih tveganj je poslovne narave – kontinuiteta zagotavljanja informacij, ki predstavljajo konkurenčno prednost podjetja.

5.1 Postavitev strežnika

Podjetja naj imajo v organizaciji vsaj en domenski strežnik, da lahko centralizirajo nadzor uporabnikov, računalnikov in mrežnih virov. S tem si zagotovijo zaščito pred nepooblaščenimi uporabniki in lahko znotraj domene razčlenijo uporabnike v različne organizacijske enote, ki imajo točno določene pravice. Sistem naj bo zaradi varnosti podatkov nameščen na diskovnih poljih RAID 1 ali RAID 5. S tem zagotovimo nemoteno delovanje tudi ob izpadu enega od diskov.

Pri omogočanju dostopa uporabnikov oddaljeno do poslovnih aplikacij je najboljša izbira uvedba terminalskega strežnika. Zaradi obsežnosti baz današnjih programov bi bilo delo preko VPN povezave prepočasno. Terminalski strežnik nam omogoča, da

uporabniki, ki se povežejo nanj, delajo na poslovnih programih, nameščenih na strežniku na sedežu podjetja in prenos podatkov znotraj lokalnega omrežja ne vpliva na internetne povezave uporabnika.

5.2 Protivirusna zaščita

Protivirusni program naj bo nameščen na domenskem strežniku in naj omogoča upravljanje po mreži. Posledično imajo tudi ostali računalniki, ki so člani domene, avtomatično nameščen protivirusni program in so s tem zaščiteni proti grožnjam. Podjetje mora imeti nameščen protivirusni program na vseh računalnikih, bodisi s skupinskim upravljanjem preko mreže ali brez njega.

Največjo nevarnost podatkom v podjetjih trenutno predstavljajo računalniški virusi, ki se v prvi vrsti prenašajo preko elektronske pošte in pripetih elektronskih dokumentov ter z vsebino , ki jo uporabniki dobivajo preko svetovnega spleta. Virus lahko v podjetje vnesejo tudi zaposleni preko okuženih medijev, kakšnih drugih nosilcev digitalnega zapisa, ali pa se širijo preko izmenjave dokumentov v lokalnem ali prostranem omrežju. Na področju varovanja pred virusi nastopa več ravni varovanja. Osnovno raven predstavljajo protivirusni programi, ki so nameščeni na osebne računalnike oziroma delovne postaje in strežnike. Ti skrbijo za pregledovanje map in dokumentov na računalnikih in po potrebi dokumente očistijo ali pa jih dajo v karanteno oziroma jih izločijo iz sistema. Priporočljivo je, da se tovrstni protivirusni programi zaženejo ob vklopu računalnika, po potrebi pa jih lahko uporabnik sproži ob vsakem novem prispelem elektronskem dokumentu, ki se lahko nahaja na medijih ali je prišel preko lokalnega omrežja, prostranega omrežja, elektronske pošte ali svetovnega spleta. Višjo raven predstavljajo protivirusni programi za pregledovanje elektronske pošte, ki so nameščeni na poštnem strežniku. Manj zmogljivi tovrstni programi lahko pregledujejo le telo sporočila, medtem ko zahtevnejši programi omogočajo tudi pregledovanje pripetih dokumentov. Pri tem program prestreže elektronsko pošto, izlušči priponko v elektronski pošti, jo odpre in protivirusnemu programu omogoči, da jo pregleda ter po potrebi očisti. Trenutno obstajata dve vrsti programov za pregledovanje elektronske pošte, in sicer programi, ki pošto le odprejo in jo pripravijo za pregled v protivirusnem programu, in programi, ki protivirusno zaščito že vključujejo. Programi za pregledovanje elektronske pošte so običajno

nameščeni bodisi na samostojnem računalniku bodisi na poštnem strežniku, pri čemer je nujno potrebno, da gre tok elektronske pošte najprej preko programa in šele nato na poštni strežnik.

5.3 Oddaljen dostop

Za dostop do podatkov izven lokalnega omrežja se uporablja VPN povezava, tako da se šifrira tunel, ki nastane med uporabnikom in omrežjem. Na ta način zagotovimo varnost povezave. VPN povezava se uporablja, ko želi uporabnik izven omrežja podjetja dostopati varno do podatkov, ki se nahajajo znotraj omrežja podjetja. Pri dostopu do poslovnih aplikacij pa se omogoči RDP povezava. Tovrstna povezava omogoči uporabniku delo, kot da bi bil lokalno v podjetju, tudi če se nahaja izven omrežja podjetja.

5.4 Izdelava varnostnih kopij

Pri nemotenem delovanju oziroma poslovanju moramo biti pozorni tudi na varnostne kopije podatkov, ki jih je potrebno izdelovati dnevno. Najpogosteje se varnostne kopije izdeluje vsak delovni dan posebej. V praksi se te podatke dnevno shranjuje na tračne enote ali na trde diske. Tedenska varnostna kopija podatkov se pripravi tako, da vsak konec tedna naredimo popolno varnostno kopijo, to pomeni, da imamo na koncu meseca najmanj štiri popolne tedenske varnostne kopije. Ob nastopu novega meseca pa začnemo medije prepisovati, če je uporabljeni medij kaseta. Za mesečno varnostno kopijo podatkov je princip podoben kot pri tedenski, le da imamo tokrat 12 medijev, ki jih mesečno uporabljamo za popolno varnostno kopijo sistema. Letna varnostna kopija se pripravi enkrat letno in se jo shrani v arhiv. Zaradi varnosti je pomembna tudi lokacija varnostnih kopij. Velika podjetja oziroma podjetja, ki imajo zelo striktno varnostno politiko zaradi narave dela, najpogosteje prvo varnostno kopijo shranjujejo lokalno, drugo v razdalji deset kilometrov od sedeža podjetja in tretjo varnostno kopijo v razdalji sto kilometrov od podjetja. To pa ni vse za zagotavljanje nemotenega poslovanja. Podjetje mora imeti sistemske skrbnike, ki vzdržujejo, popravljajo in optimizirajo informacijski sistem. Nekaterim podjetjem se ne izplača imeti internega sistemskega skrbnika, zato uporabljajo zunanje vzdrževalce, ki imajo ustrezna znanja.

6 IMPLEMENTACIJA INFORMACIJSKEGA SISTEMA V PODJETJU

Business Solutions je podjetje, ki nudi informacijsko podporo tako strojne kot tudi programske opreme drugim podjetjem. Sestavlja ga 26 zaposlenih, ki so razdeljeni na dva sektorja. Kot član podjetja v oddelku informacijske podpore sem odgovoren za ustrezno informacijsko zaščito podjetij. V nadaljevanju podajamo primer podjetja, za katerega smo izdelali informacijske prvine.

Podjetje ima 25 zaposlenih ljudi. Ukvarja se s prevozništvom in maloprodajo naftnih derivatov. Poleg sedeža podjetja imajo na Primorskem še tri nove poslovne enote. Prav zaradi teh enot se je pojavila potreba po komunikaciji z bazo podatkov, ki se nahaja na sedežu podjetja. Ker trenutna konfiguracija informacijskega sistema ne dopušča varne vzpostavitve povezave z bazo, so se v podjetju odločili za nadgradnjo stojne in programske opreme ter posledično celotnega informacijskega sistema.

6.1 Trenutno stanje v podjetju

Pri delu z računalniki se v podjetju uporablja delovna skupina. Uporabniki dostopajo do vseh računalnikov kot administratorji, saj nimajo lastnih uporabniških računov. S tem imajo dostop do vseh lokalnih in mrežnih virov s polnim nadzorom. To pomeni, da lahko berejo, pišejo in brišejo podatke brez kakršnekoli ovire. Tu nastopi možnost vdora, saj se zlonamernež lahko prijavi na katerikoli računalnik in ima poln dostop do vseh podatkov. Protivirusna zaščita ni poenotena in na nekaterih računalnikih ni nameščena. To lahko pripelje do okužbe z računalniškim virusom najprej na računalniku, ki ni zaščiten, in nato v celotni mreži. Podatkovna baza se nahaja na navedenem računalniku z operacijskim sistemom Windows XP, ki je lociran v pisarni, ki je dostopna vsakomur.

6.2 Želeno stanje v podjetju

Vsak uporabnik dobi nov računalnik z operacijskim sistemom Windows XP Professional. Uvede se strežnik z nameščenim Windows SBS (angl. Small Business Server) 2003. Služil bo kot domenski strežnik, DNS (angl. Domain Name Server) strežnik in poštni strežnik. Pri nastopu domene vsak uporabnik dobi enolično uporabniško ime in geslo, s katerima se overi pri prijavi na računalnik. Uporabnike

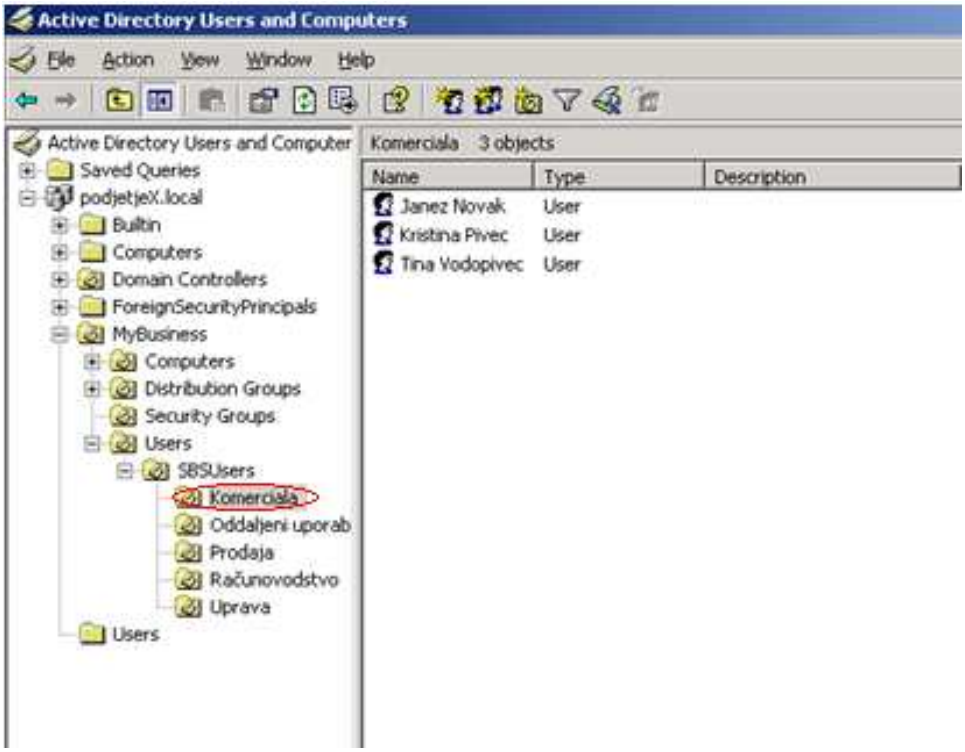
se razdeli v organizacijske enote računovodstvo, komerciala, prodaja, oddaljeni uporabniki in uprava. Vsaki organizacijski enoti oziroma skupini se dodeli ustrezne pravice. Zaradi novih enot se uvede še dodaten strežnik, na katerem ja nameščen Windows Server 2003 Standard, ki bo imel funkcijo terminalskega strežnika. Uporabniki z oddaljenih lokacij bodo preko navideznega zasebnega omrežja VPN dostopali do lokalnega omrežja v podjetju, nato pa se bodo povezali na terminal, ki jim bo omogočal dostop do programov in podatkov. Protivirusna zaščita bo nameščena na domenskem strežniku in s pomočjo skupinskih politik se bo protivirusna zaščita po mreži namestila na vse računalnike v domeni. Strežniki bodo nameščeni v strežniški omari, ki bo locirana v varni komunikacijski sobi. Dostop do komunikacijske sobe bodo imeli samo sistemski administratorji in osebje, zadolženo za varnostne kopije podatkov.

6.2.1 Strežniki

V podjetju je potrebno implementirati dva strežnika. Prvi bo prevzel vlogo domenskega, DNS, DHCP (angl. Dynamic Host Configuration Protocol) in poštnega strežnika, drugi pa vlogo terminalskega strežnika. Za prvega smo izbrali HP-jev strežnik HP ProLiant ML350 G5 (slika 30). Operacijski sistem bo Windows SBS 2003. Drugi strežnik bo HP ProLiant DL180 G5. Na njem bo nameščen Windows Server 2003 Standard.

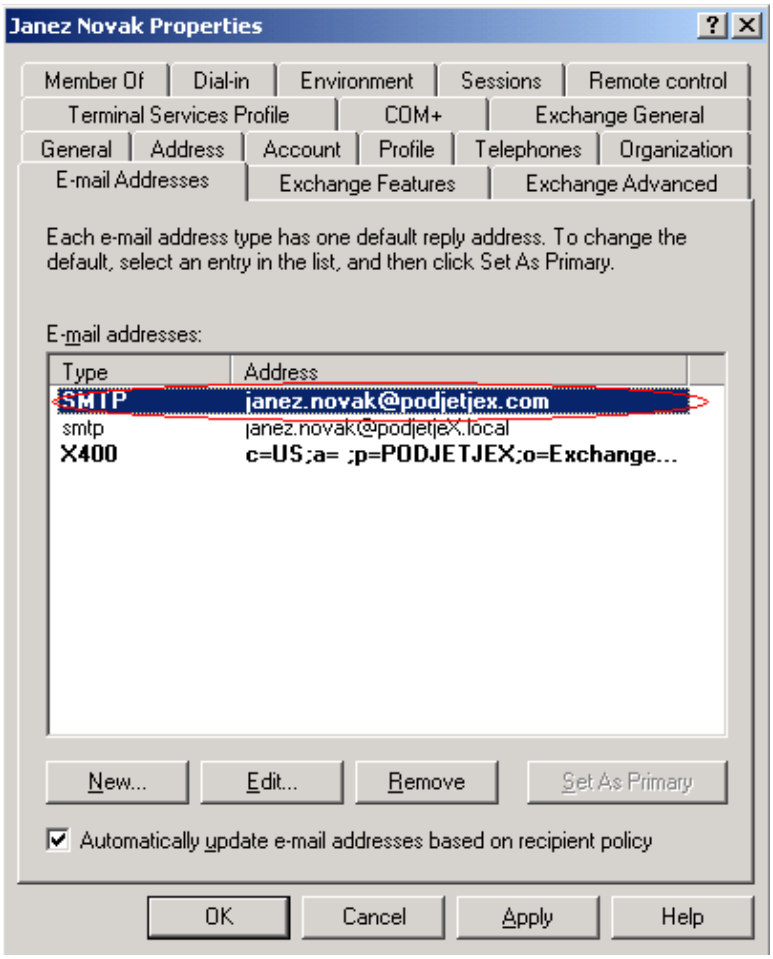
Slika 30: Strežnik HP ProLiant ML-350

Po namestitvi in pravilni konfiguraciji SBS 2003 dobimo za podjetje popolnoma delujočo domeno. Z domeno nastopi aktivni imenik (angl. Active Directory, AD), s katerim lahko upravljamo računalnike in domenske uporabnike. Te razdelimo v različne organizacijske enote (slika 31). Ko imamo enkrat izdelano uporabniško strukturo, je upravljanje uporabnikov enostavnejše.



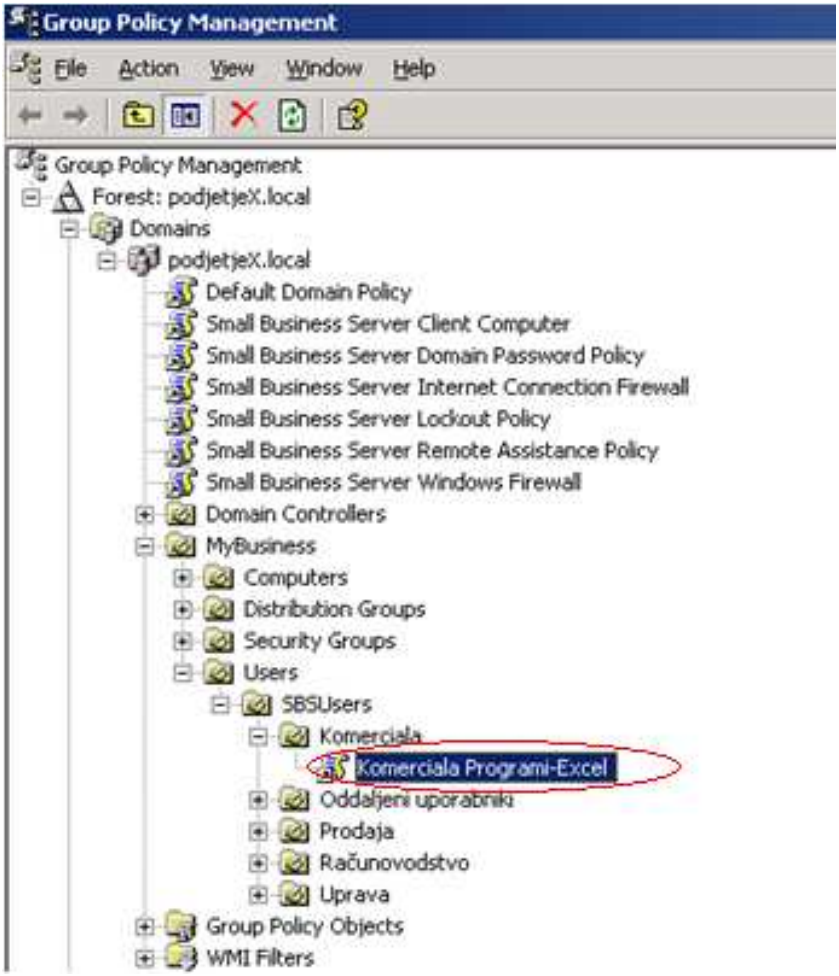
Slika 31: Aktivni imenik uporabnikov in računalnikov

Strežnik bo deloval tudi kot poštni strežnik, zato moramo dodeliti dosedanje poštne naslove vsem uporabnikom, tako da bodo nemoteno prejemali elektronsko pošto (slika 32).



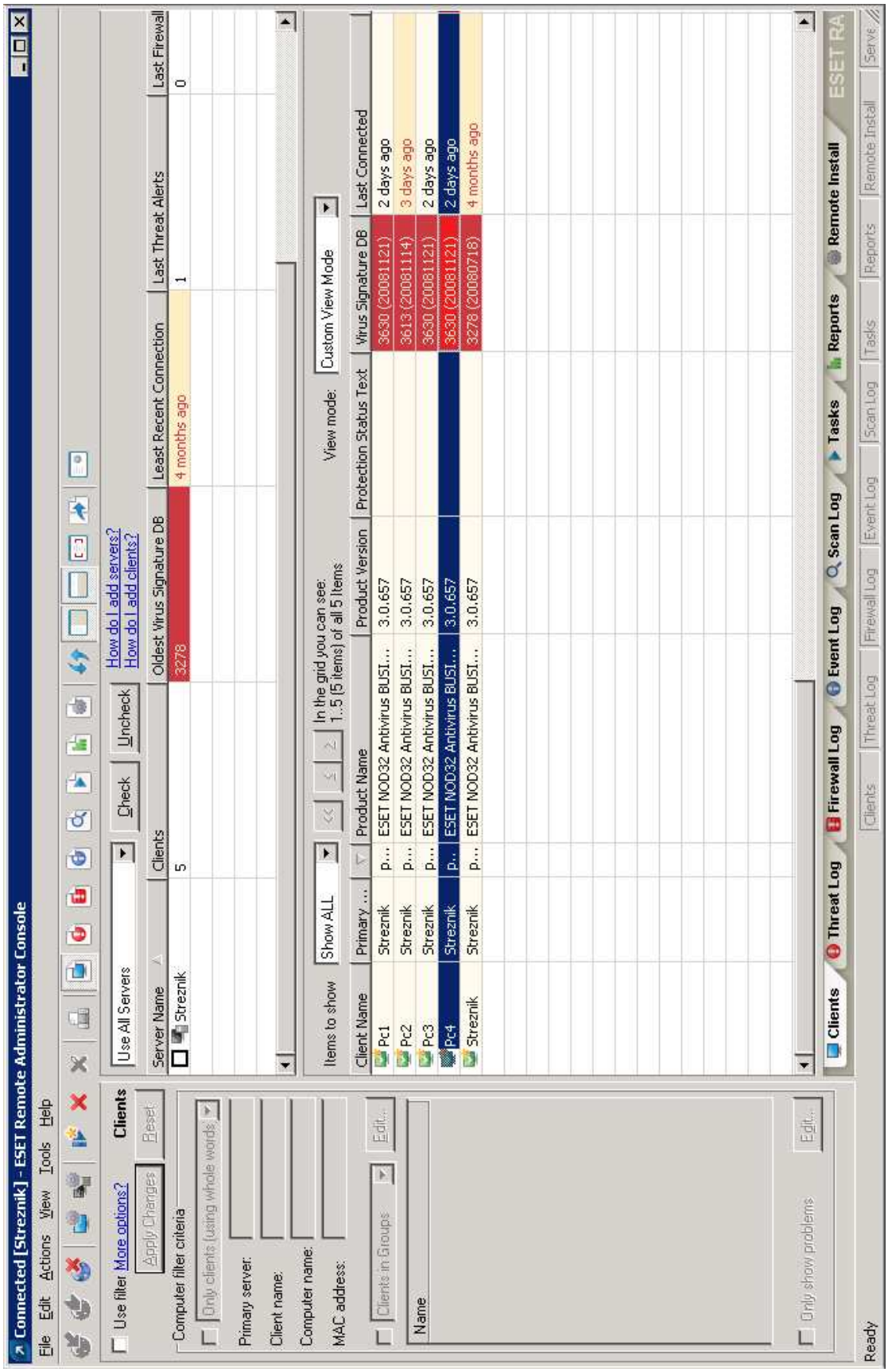
Slika 32: Dodeljevanje starih poštnih naslovov uporabnikom

S pomočjo skupinskih politik lahko namestimo programe preko mreže. Tako npr. v komerciali potrebujejo Microsoftov program Excel, v ostalih enotah pa ne. Skupinske politike omogočajo, da se tovrstni program namesti le uporabnikom, ki ga potrebujejo (slika 33) (Spealman in drugi, 2004).



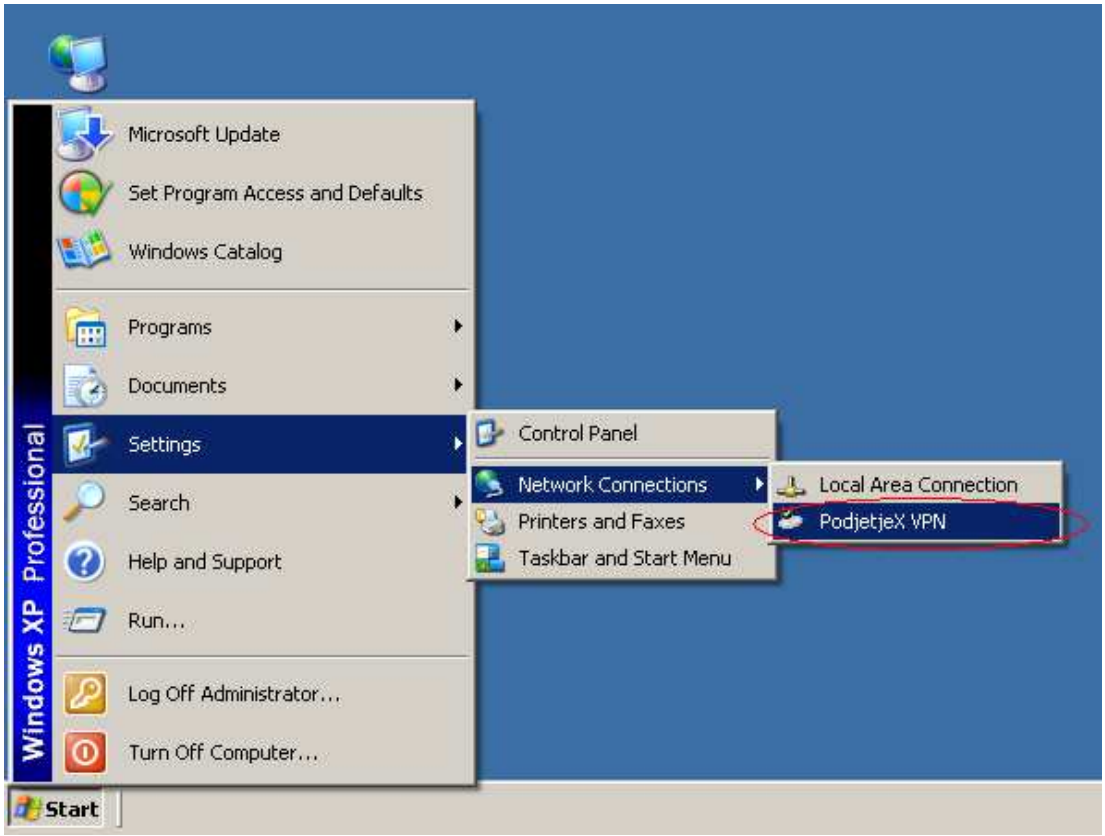
Slika 33: Konfiguracija skupinskih politik za namestitev Excela v komerciali

Na strežniku SBS 2003 bo nameščen tudi protivirusni program NOD32, ki omogoča namestitev in upravljanje po mreži. To pomeni, da ga vsem uporabnikom v domeni lahko namestimo preko mreže, na konzoli pa lahko pregledujemo stanje protivirusnega programa, npr. zadnjo posodobitev, seznam zaznanih virusov ipd. (slika 34).



Slika 34: Konzola programa NOD32 za upravljanje preko mreže

Zaradi velikosti podatkovne baze je oddaljeno delo samo z vzpostavitvijo navideznega zasebnega omrežja VPN nemogoče. Za rešitev tega problema smo uvedli terminalski strežnik, ki bo uporabnikom omogočal dostop do programov in podatkov. Na strežniku ProLiant DL180 je nameščen Windows Server 2003 standard, ki ima vlogo terminalskega strežnika. Terminalski strežnik omogoča uporabnikom delo kot na svoji delovni postaji in je neodvisen od konfiguracije in zmogljivosti lokalnega računalnika. Oddaljeni uporabniki dostopajo do terminalskega strežnika tako, da najprej vzpostavijo VPN povezavo (slika 35), saj si tako zagotovijo varno šifrirano komunikacijo.



Slika 35: Klicanje VPN povezave podjetja

Nato se s pomočjo oddaljenega namizja (RDP) povežejo na terminalski strežnik (slika 36).

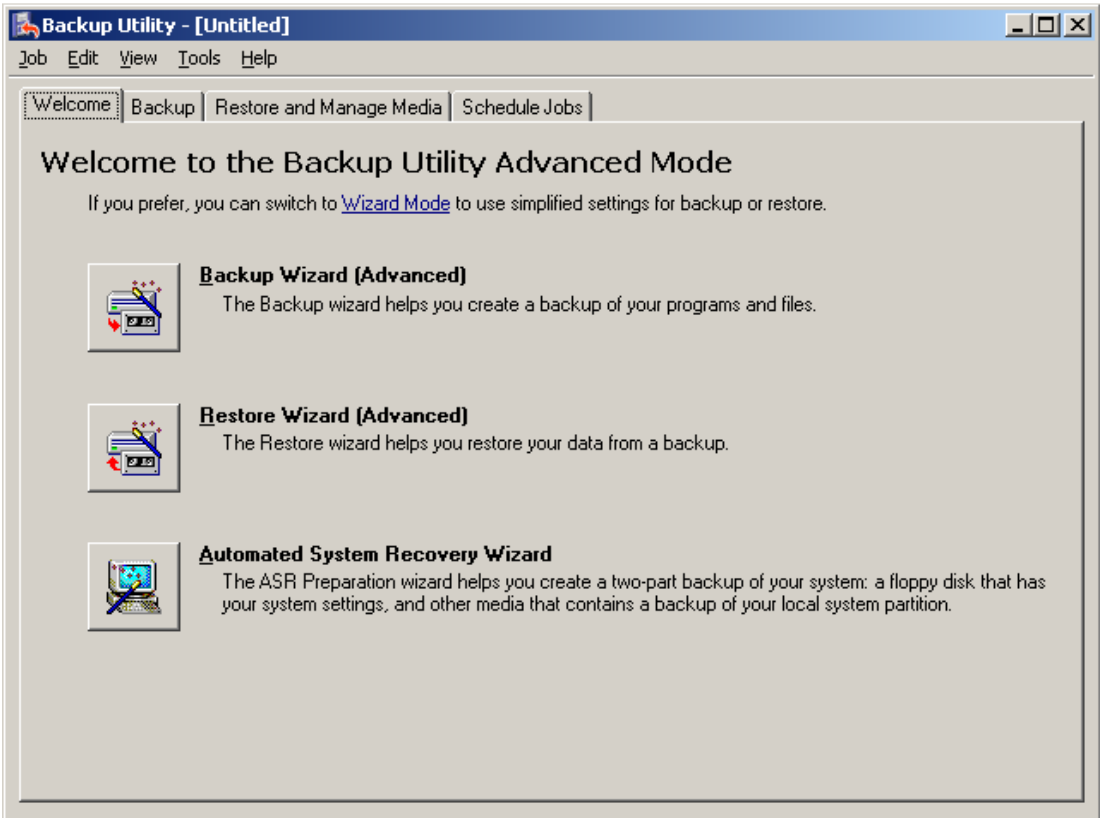
Slika 36: Povezovanje na oddaljeno namizje terminala

Ko se ustrezno identificirajo, se povežejo v svoj profil na terminalskem strežniku in od tam lahko dostopajo do programa podjetja (slika 37).

Slika 37: Dostop do programa na terminalskem strežniku

Zagotoviti moramo tudi varnostne kopije podatkov in konfiguracije na strežniku, ki jih je potrebno izdelovati vsak delovni dan. To naredimo s pomočjo programa za varnostne kopije (slika 38). Konfiguriramo ga tako, da se izvede vsak delovnik. Idealen čas za izvedbo varnostne kopije je, ko vsi uslužbenci zapustijo delovna mesta. V praksi se varnostne kopije izdeluje ponoči in se jih shranjuje na kasete tračne enote, ki se dnevno menjajo. Za menjavo kaset je zadolžena oseba znotraj podjetja, ki ima dostop do komunikacijske sobe. Enkrat tedensko se varnostno kopijo zapiše tudi na optične medije (DVD), ki se shranijo na posebno lokacijo zunaj

podjetja. Tako je zagotovljen obstoj podatkov tudi ob morebitni kraji oziroma požaru, ki bi uničil stojno opremo in podatkovne medije v podjetju.



Slika 38: Program za izdelavo varnostnih kopij

6.2.2 Delovne postaje

Vsak uporabnik bo imel svojo delovno postajo, ki bo članica domene podjetja. Zaradi overjanja morajo imeti dodeljeno uporabniško ime in geslo, s katerim se bodo prijavljali v domeno (slika 39). Prednost domene je, da se uporabniki nahajajo v istem okolju, ne glede na katerem računalniku se prijavijo.

Slika 39: Prijavljanje uporabnika v domeno podjetja

Pomembno je omeniti, da vsem uporabnikom ni omogočeno dostopati do vseh mrežnih mest oziroma podatkov. Dostopajo lahko do točno določenih mest, ki so dodeljena skupinam. Ob prvi prijavi se namestijo programi, ki so določeni glede na pripadnost skupini oziroma oddelku. Edini program, ki se namesti za vse uporabnike, je protivirusni program NOD32.

Na delovnih postajah uporabniki z izjemo administratorja ne morajo ničesar nameščati. S tem blokiramo tudi nekatere viruse, ki izkoriščajo uporabniške pravice za razmnoževanje. Tako zagotovimo, da se nameščajo le ustrezni programi, ki so povezani z delovnim okoljem.

6.2.3 Komunikacijska soba

Komunikacijska soba je prostor, v katerem se nahaja strežniški kabinet (slika 40) s strojno opremo (strežniki, preklopniki, usmerjevalniki, sistemi za neprekinjeno napajanje UPS ipd.). Dostop do komunikacijske sobe je nepooblaščenim osebam strogo prepovedan, soba pa je vedno zaklenjena. Ključa komunikacijske sobe in strežniškega kabineta hranijo v podjetju. Taka rešitev preprečuje, da bi nepooblaščena oseba fizično dostopala do pomembnejše strojne opreme.

Slika 40: Strežniški kabinet

7 ZAKLJUČEK

Področje informatike je eno ključnih področij, na katerih temelji razvoj sodobne družbe. Tehnologija ima izjemen vpliv na celotno družbeno dogajanje. Ogromne količine informacij se po vsem svetu rutinsko shranjuje in prenaša preko računalniških in komunikacijskih omrežij. Prav zato smo postali odvisni od delovanja informacijskih tokov in vsaka motnja lahko povzroči veliko škode. Skupaj s prednostmi, ki jih prinašajo zmožnosti operiranja z ogromnimi količinami informacij, prihajajo na površje tudi grožnje, ki so usmerjene v poslovni svet, delovanje vladnih institucij in življenja posameznikov. Grožnje se skrivajo v možnih goljufijah, ki so izvedene z manipulacijo informacij, z namenoma povzročiti škodo shranjenim in prenašalnim informacijam ter z zlorabo informacijskih medijev. Področje informacijske varnosti se ukvarja s študijem protiukrepov, ki zmanjšujejo zelo resnične in nevarne grožnje. To je področje, ki se v zadnjem času izredno hitro razvija. Pokriva različne tehnike, kot so šifriranje podatkov, računalniška varnost in odkrivanje nedovoljenega delovanja v informacijskih sistemih, ter podaja vrsto napotkov, kako upravljati z informacijsko varnostjo.

Na primeru podjetja smo prikazali izvedbo prvin informacijske varnosti. Zavedati pa se moramo, da je to zgolj začetek in da bo potrebnih še veliko izboljšav ter sledenja smernicam informacijske varnosti. Omeniti je potrebno tudi, da po uvedbi takšnega sistema v podjetju ni bilo zabeleženih nobenih vdorov, groženj in okužb z drugimi zlonamernimi kodami. V nadaljevanju bomo morali biti pozorni na pravočasno zaznavanje groženj informacijske varnosti ter jih kakovostno in uspešno prestreči.

V diplomskem delu so prikazane teoretske prvine komponent, ki v simbiozi tvorijo tudi ustrezno varnostno politiko. Izsledki izvedene ankete kažejo, da informacijska varnost podjetij na Goriškem ni popolna. Potrebno je še dosti izboljšav informacijskih sistemov teh podjetij, da dosežejo ustrezen nivo zaščite. Končni cilj pa ni samo doseganje minimalnega nivoja, potrebno ga je tudi nadgrajevati in vzdrževati. To je proces, ki se nikoli ne konča, saj se v svetu računalništva vsak dan pojavljajo nove priložnost, ki jih mora podjetje izkoristiti za svoje nemoteno poslovanje in razvoj.

8 LITERATURA

Bezavšček, A. (2007). Varnost informacijskega sistema. Skripta, interno gradivo. Univerza v Mariboru: [A. Brezavšček]

Frelih, G. (2005). Zlonamerni programi in zaščita informacijskih sistemov podjetja. Diplomsko delo. (Ekonomska fakulteta, Univerza v Ljubljani), Ljubljana: [G. Frelih].

Gradišar, M. (2003). Uvod v informatiko. Ljubljana: Ekonomska fakulteta.

Information Technology Infrastructure Library. Pridobljeno 25.3.2008 s svetovnega spleta: http://en.wikipedia.org/wiki/ITIL

Košir, R., Gregorčič, F. (2003). Varovanje informacij: standard ISO 17799 in varovanje gesel ter ocena stanja v Splošni bolnišnici Maribor. Seminarks naloga. (Univerza v Ljubljani, Medicinska Fakulteta). Ljubljana: [R. Košir, F. Gregorčič]

Pečnik, J. (2007). Pomen in zagotavljanje varnosti informacijskih sistemov v finančnem sektorju. Magistrsko delo. (Ekonomska Fakulteta, Univerza v Ljubljani), Ljubljana: [J. Pečnik].

Prešeren, T. (2008). Celoviti pristop obvladovanja mobilnih naprav v farmacevtskem podjetju. Magistrsko delo. (Fakulteta za računalništvo in informatiko, Univerza v Ljubljani), Ljubljana: [T. Prešeren].

RAID Tutorial. Pridobljeno 14.1.2008 s svetovnega spleta: http://www.acnc.com/04_01_00.html

Rakuš, J. (2002). Varovanje informacij: standard ISO 17799 in varovanje gesel. Seminarska naloga. (Inštitut za biomedicinsko informatiko, Medicinska fakulteta), Ljubljana: [J. Rakuš].

Skrt, R. (2003). Nezaželena e-pošta in slovenska zakonodaja. Pridobljeno 22.5.2008 s svetovnega spleta: http://www.nasvet.com/nezazelena-posta/

Spealman, J., Hudson, K., Craft, M. (2004). Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure. Redmond: Microsoft Press..

Sušnik, M. (2004). Brezžična omrežja in javnost. Pridobljeno 22.2.2008 s svetovnega spleta: http://e-izdaja.comtron.si/Izdaja4/BREZZICNA.htm

Turk. Ž. (2007). Pot v OECD pomembnejša od cilja. Pridobljeno 14.3.2008 s svetovnega spleta: http://blog.zturk.com/2007/12/pot-v-oecd-pomembneja-od-cilja.html

Vidmar, T. (2002). Informacijsko komunikacijski sistemi. Ljubljana: Pasadena.

PRILOGA 1: ANKETA

Naprej se želim zahvaliti za izpolnjevanje ankete. Rezultati ankete bodo pri diplomskem delu služili za vpogled v stanje informacijske varnosti podjetij v goriški regiji. Anketa je anonimna.

Branža: _____

Število zaposlenih: _____

Število računalnikov v podjetju: _____

Število ljudi v IT oddelku: _____

1. Ali imate v podjetju strežnike?

a) DA b) NE

2. Ali uporabljate polja RAID ?

a) DA b) NE

1) RAID 0 2) RAID 1

3) RAID 2 4) RAID 3

5) RAID 4 6) RAID 5

7) RAID 6 8) RAID 7

9) RAID 0+1 10) RAID 1+0

3. Kako pogosto izdelujete varnostne kopije vaših podatkov?

a) Dnevno
b) Tedensko
c) Mesečno
d) Ostalo:_____
e) Ne delamo varnostih kopij

4. Na katere podatkovne medija shranjujete varnostne kopije?

a) Trdi disk
b) Optični mediji (DVD/CD)
c) Tračne enote
d) Mediji SSD/Flash

5. Ali v vašem podjetju sledite smernicam informacijske varnosti (obkrožite katerim)?

a) DA b) NE

1) COBIT
2) NIST SP 800
3) ITIL
4) BS ISO/IEC 13335
5) OCTAVE
6) BS ISO/IEC 15408
7) OECD
8) BS ISO/IEC 18044:2004
9) Pas 56
10) BS 7799
11) PD 3000

6. Ali ima vaše podjetje sistemskega/varnostnega administratorja?

a) DA b) NE

7. Ali imate v vašem podjetju možnost dela z oddaljene lokacije?

a) DA b) NE

1) RDP
2) VPN
3) FTP

8. Ali imate v vašem podjetju brezžično lokalno omrežje WLAN? Kako je zaščiteno?

a) DA b) NE

1) WEP 2) MAC address

3) WPA PSK 4) Certifikati

5) RADIUS

9. Ali pri posredovanju podatkov uporabljate šifriranje?

a) DA b) NE

10. Kako se obvarujete pred virusom ter drugi zlonamerni kodi?

a) Proti virusna orodja
b) AntiSpyware orodja
c) AntyTrojan orodja
d) RADIX / Deep Freeze
e) Administratorske pravice

11. Kakšen sistem zaščite dostopa do podatkov imate?

a) Omejevanje uporabniških pravic
b) Gesla uporabniškim računom
c) Gesla pri dostopanju do podatkov
d) Drugo:_____

12. Ali ima vaše podjetje plan za ponovno vzpostavitev informacijskega sistema ter strojne opreme v primeru »katastrofe« (angl. Disaster Recovery Planing, DRP)?

a) DA b) NE