UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

PRILAGAJANJE VARNOSTNIH POLITIK IN INFORMACIJSKE GROŽNJE SKOZI ČAS

Ljubljana, september 2008 JOŠT ŠTRUKELJ

IZJAVA

Študent Jošt Štrukelj izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. Turk Tomaža , in da dovolim njegovo objavo na fakultetnih spletnih straneh.

Izbrisano: JOŠT ŠTRUKELJ

Izbrisano: URK TOMAŽ

V Ljubljani, dne 11.09.2008 Podpis: _____

KAZALO

Izbrisano: Kazalo

Oblikovano: Naslov TOC, Tabulatorji: Ne pri 15,98 cm

Izbrisano: ¶

KAZALO SLIK IN TABEL

Kazalo slik:

Kazalo tabel:

Oblikovano: Kazalo vsebine 2

Oblikovano: Preveri črkovanje in slovnico

Oblikovano: Navaden, Tabulatorji: Ne pri 15,98 cm

Izbrisano: Uvod . 1¶
1 Informacijski sistemi in informacijska varnost . 2¶
1.1 Informacijski sistemi . 2¶
1.2 Sestava informacijskih sistemov . 3¶
1.3 Informacijska varnost . 4¶
2 Varnostna politika – temeljni dokument informacijske varnosti . 5¶
2.1 Varovanje informacijskega sistema . 5¶
2.2 Izdelava oziroma vzpostavitev varnostne politike informacijskega sistema . 6¶
2.3 Varnostni standardi . 8¶
2.4 Obvladovanje tveganj informacijske varnosti . 10¶
3 Soodvisnost informacijskih groženj in varnostne politike skozi čas . 12¶
3.1 Informacijska varnost in tehnologija pred letom 2000 . 12¶
3.1.1 Informacijski sistemi, tehnologija in uporabniki . 13¶
3.1.1.1 Informacijski sistemi . 13¶
3.1.1.2 Informacijska tehnologija . 13¶
3.1.1.3 Uporabniki . 14¶
3.1.2 Kronološki pregled informacijskih groženj, nevarnosti in ranljivosti . 14¶
3.1.2.1 Začetki škodljive programske kode do leta 1970 . 14¶
3.1.2.2 Škodljiva programska koda v 70. in 80. letih . 15¶
3.1.2.3 Škodljiva programska koda v 90. letih . 18¶
3.1.3 Informacijske zaščite in rešitve . 21¶
3.1.4 Varnostne politike obdobja pred letom 2000 . 21¶
3.2 Pregled stanja na informacijskem področju danes . 22¶
3.2.1 Informacijski sistemi, tehnologije in uporabniki . 23¶
3.2.1.1 Informacijski sistemi . 23¶
3.2.1.2 Informacijska tehnologija . 24¶
3.2.1.3 Uporabniki . 24¶
3.2.2 Informacijske grožnje, nevarnosti in ranljivosti . 25¶
3.2.3 Informacijske zaščite in rešitve . 28¶
3.2.4 Varnostne politike po letu 2000 . 31¶
4 Informacijska varnost v prihodnosti . 32¶
4.1 Predvidevanja informacijske varnosti . 33¶
4.2 Svetovni splet, splet 2.0 in varnost . 34¶
4.3 Kibernetični kriminal, kibernetični terorizem in ... [1]

Oblikovano: Pisava: 11 pt

Oblikovano: Pisava: 11 pt

Uvod

Uporaba informacijske tehnologije je postala v razvitem svetu nekaj tako samoumevnega kot vožnja z avtomobilom. Uporabljamo jo na vsakem koraku, tudi takrat, ko se tega sploh ne zavedamo. Z razvojem smo ugotovili, da nam lahko olajša življenje in vse, kar počnemo. Od informacijske tehnologije imamo koristi tako v zasebnem kot poslovnem življenju. Informacijska tehnologija je postal pomemben del našega vsakdana. Lahko bi trdili, da brez nje sodoben človek ne more preživeti.

Kako in zakaj je danes položaj takšen, se nihče več ne sprašuje. Pomembno je le, da tehnologija deluje in da delo, pa naj bo to v privatnem ali poslovnem svetu, poteka brezhibno brez motenj. Pri informacijski tehnologiji, ki temelji na informacijah, predstavljajo velik del motenj varnostna tveganja, ki jih je treba obvladovati. Pri uporabi informacijske tehnologije se uporabniki zavedamo, da obstaja veliko tveganj, ki nam lahko povzročijo težave, vendar kljub temu problematiki, po mojem mnenju, posvečamo premalo pozornosti. Razvoj informacijske tehnologije je omogočil nove funkcionalnosti, odprl nova obzorja, pokazal nove možnosti in prinesel toliko ugodnosti, da smo informacijsko varnost začasno odrinili na stranski tir. V zadnjem času smo lahko v medijih pogosto zasledili najrazličnejše pomisleke glede varnosti osebnih podatkov na spletu in podobno. Ampak to je le delček varnostnih tveganj, katerim smo z uporabo informacijske tehnologije izpostavljeni.

Pri iskanju podatkov o informacijski varnosti sem zasledil veliko literature. Pri prebiranju sem oblikoval mnenje, da tipičnega uporabnika te vrste literatura ne zanima oziroma uporabnik ne sledi priporočilom in nasvetom, dokler incidenta ne izkusi na lastni koži. Varnostni incident nam lahko povzroči veliko škode in nepotrebnih skrbi. Statistike namreč prikazujejo osupljive rezultate spletnega kriminala, ki naj bi v preteklem letu že celo presegel rezultate tako imenovane narkomafije.

V diplomskem delu želim predstaviti problematiko informacijske varnosti prek razvoja varnostnih politik in informacijskih groženj skozi čas. Zanimiva je predvsem povezanost obeh kategorij v razvoju, kako sta se odzivali na razvoj ene in druge in kakšna je bila interakcija med njima. V uvodnih dveh poglavjih sem povzel teoretične vidike informacijskih sistemov in varnostnih politik. V četrtem poglavju sem predstavil razvoj informacijskih groženj in varnostnih politik skozi čas. Pregled sem razdelil na obdobje pred letom 2000 in po njem. V nadaljnjem poglavju sem pripravil pregled prihodnosti informacijske varnosti. Zadnje poglavje pa obsega študijo primera na podjetju Eles, d. o. o. Pri pisanju sem se osredotočil predvsem na varnostna tveganja poslovnega uporabnika, ki so kompleksnejša kot varnost nekega tipičnega uporabnika. Razlika je predvsem v samem obsegu uporabe informacijske tehnologije, ki je pri poslovnem porabniku bistveno večji. Hkrati so poslovni uporabniki, podjetja in organizacije, zaradi zanimivosti podatkov, s katerimi razpolagajo, zanimivejši za spletne kriminalce kot tipični uporabniki. Varnosti je treba posvečati več pozornosti in sredstev.

1 Informacijski sistemi in informacijska varnost

1.1 Informacijski sistemi

Informacijski sistem je sistem, ki je urejen in organiziran tako, da nam je v pomoč pri odločanju, poslovanju ali delovanju. Informacijski sistem temelji na nekih osnovnih lastnostih oziroma izvajanju aktivnosti. Kot osnovne lastnosti informacijskega sistema lahko opredelimo zbiranje, shranjevanje, obdelavo in posredovanje podatkov ter rezultatov med uporabnike informacijskega sistema. Cilj informacijskega sistema je torej izključno pomoč uporabnikom.

Informacijske sisteme lahko delimo na različne načine. Ena izmed njih je delitev na formalne in neformalne, delimo jih tudi na računalniško podprte in računalniško nepodprte informacijske sisteme, v splošnem pa jih delimo na transakcijske in poslovno-inteligenčne. Različni nivoji zaposlenih potrebujejo za svoje delo različne informacije. V današnjem tehnološkem obdobju so informacijski sistemi nujno potrebni za delovanje vsakega posameznika v poslovnem svetu, prav tako pa so nam v privatnem življenju v veliko pomoč. Sodobno oblikovan informacijski sistem nam omogoča (Gradišar & Resinovič, 2001, str. 387):

- hitrejše in bolj kakovostno delo;
- lažje iskanje in odločanje, saj nam podatke poišče, oblikuje in predstavi na način, ki tvori informacijsko podlago za naše odločanje in učinkovitejšo uporabo znanja;
- kakovostnejši nivo komunikacije znotraj in zunaj organizacije.

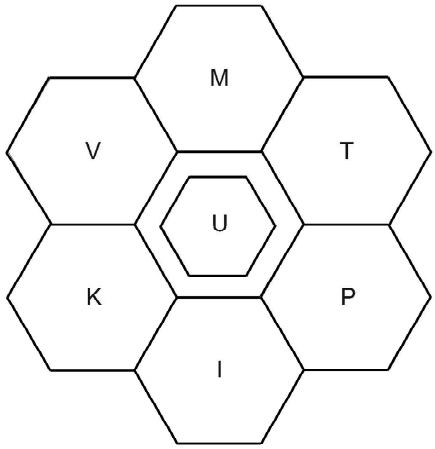
Informacijske sisteme pojmujemo kot kombinacijo v bazi podatkov shranjenih podatkov, človeških sposobnosti in tehničnih pripomočkov, ki proizvajajo informacije za podporo odločanju in poslovanju.

Informacijski sistemi so potemtakem le del nekega večjega sistema, na primer poslovnega, ki je hkrati le del nekega večjega sistema, kot na primer podjetja. Pomeni torej, da so informacijski sistemi samo člen v daljši verigi, kot je recimo gospodarstvo. Vemo, da je veriga le toliko trdna, kolikor je trden najšibkejši člen. Varnost informacijskih sistemov je bila v preteklosti dokaj prezrta kategorija, vendar pa danes igra iz dneva v dan pomembnejšo vlogo.

1.2 Sestava informacijskih sistemov

Sestavo informacijskih sistemov lahko prikažemo z naslednjo sliko.

Slika 1: Vsebinski sklopi elementov IS ali sestavine informacijskega sistema



Vir:M Gradišar, G. Resinovič,Informatika v poslovnem okolju, 2001, str. 340.

Elemente slehernega informacijskega sistema s slike 1 lahko razdelimo na sedem vsebinskih sklopov (Gradišar & Resinovič, 2001, str. 340):

- **Vhodni blok (V):** Vhodni blok predstavlja množica vnosnih form, preko katerih poteka vnos podatkov. Vnos je lahko računalniško podprt, tako da je forma prikazana na zaslonu, ali pa ni računalniško podprt in zahteva ročni vpis na papir.
- **Metode (M):** Sklop proceduralnih, logičnih, matematičnih metod, s katerimi se obdelujejo podatki, da bi prišli do želenih rezultatov. Tipični postopki obdelave podatkov so zajemanje, razvrščanje, urejanje, računanje, arhiviranje, iskanje, reproduciranje, komuniciranje, preverjanje.
- **Tehnika (T):** Informacijska tehnologija temelji na tehničnih sredstvih in omogoča dejansko transformacijo podatkov.
- **Podatkovna baza (P):** Podatkovna baza hrani podatke v določeni podatkovni strukturi.
- **Izhodni blok (I):** Izhodni blok mora prikazovati izhodne informacije. Pogoj za transformacijo podatkov v informacije je poleg obdelave podatkov tudi ustrezen način prikaza informacij, saj postane podatek informacija takrat, ko za uporabnika postane uporaben. Če je uporabna informacija v prikazu skrita ali nejasno prikazana, za uporabnika ne predstavlja nobene uporabnosti.
- **Kontrolni blok (K):** Kontrolni mehanizmi informacijskega sistema morajo zagotavljati preverjanje vhodnih podatkov in izločati tiste nepravilne vnosne podatke, ki so nepotrebni ali napačni za ustrezen zapis v podatkovno bazo.

- **Udeleženci (U):** Udeleženci so ljudje, ki skrbijo za informacijski sistem in ga upravljajo ter uporabljajo izhode informacijskega sistema.

1.3 Informacijska varnost

Pod terminom informacijska varnost razumemo varovanje informacij v sistemu in varovanje informacijskih sistemov pred različnimi nevarnostmi in grožnjami, ki se pojavljajo pri vsakodnevnem poslovanju. Med te nevarnosti in grožnje štejemo posege, kot so nepooblaščen ali nezakonit dostop do informacijskega sistema, uporaba, razkritje, razdor, sprememba ali uničenje informacij, pridobljenih na nedovoljen način (Štrakl, 2003, str. 19).

Informacijska varnost oziroma varnost informacij je že od nekdaj zelo pomembna tema. V antičnih časih so si izmišljali najrazličnejše metode, postopke in načine, kako zaupne informacije zakriti tako, da bodo razumljivi točno določenemu uporabniku. Egipčanska civilizacija je razvila pisavo v obliki hieroglifov, kjer imajo podobe različen pomen (Wikipedia). Prvi znani šifrirni ključ je izumil Julij Cezar. Vsako črko v abecedi je zamenjal s črko štiri mesta pred njo v abecedi na način A-Č, B-D … Ker je bila splošna pismenost na nizki ravni, je bila metoda nadvse učinkovita. Iz antičnih časov poznamo še eno nadvse enostavno iznajdbo za šifriranje sporočil. Okoli lesene palice vnaprej določene debeline ovijemo trak blaga, na katerega nato napišemo sporočilo. Ko trak odvijemo s palice, besedilo na traku nima nikakršnega smisla. Naslovnik oziroma prejemnik sporočila mora nato poiskati palico enake debeline in prebrati sporočilo. Debelina palice predstavlja nekakšen šifrirni ključ, ki mora biti znan in določen. Tako kot danes, ko je treba šifrirne ključe za šifriranje sporočil vnaprej izmenjati.

Kljub temu da je prvi šifrirni ključ že zelo star, razvoj informacijske varnosti ni potekal tako hitro. V srednjem veku niso bili tako inovativni, hkrati pa velja, da je bila pismenost še na nižjem nivoju kot v antičnih časih. V srednjem veku so kot ukrep informacijske varnosti večinoma uporabljali voščene pečate. Nekoliko hitrejši razvoj šifriranja in s tem informacijske varnosti je prišel z obema vojnama z nemškim izumom šifrirnega stroja Enigma.

Zahteve po kakovostnejši informacijski varnosti so se začele strmo povečevati z razvojem informacijske tehnologije in razvojem interneta ter vseh njegovih funkcionalnosti. Danes se potrebe in zahteve po informacijski varnosti povečujejo dnevno in temu ni videti konca, saj je kakovostno informacijsko varnost vsak dan težje doseči. Nekateri strokovnjaki za informacijsko varnost v šali trdijo, da je 100-odstotna varnost mogoča le, če sta mrežna vtičnica in omrežni kabel en centimeter narazen.

2 Varnostna politika – temeljni dokument informacijske varnosti

Varnostna politika informacijskega sistema je dokument, ki poda celovit pogled na varnost informacijskega sistema in zajema vse dejavnike, organizacijska pravila in postopke, ki kakor koli vplivajo na varno in zanesljivo delovanje celotnega informacijskega sistema.

Varnostna politika je pomemben dokument za nemoteno poslovanje, zato bi vsako podjetje moralo imeti sestavljeno ustrezno varnostno politiko, katere del je tudi varnostna politika informacijskega sistema. Podjetja v naprednejših in razvitejših gospodarstvih se tega seveda že dalj časa zavedajo, pri slovenskih podjetjih in organizacijah pa je šele v zadnjih letih prišlo do spoznanja, kako pomembna je varnostna politika informacijskega sistema. Pred tem so izvajali le posamezne korake vpeljevanja varnostne politike, in ker ni bilo spisanega nekega enotnega, celovitega dokumenta, je zaradi necelovitosti in neorganiziranosti velikokrat prišlo do uresničenja varnostnih groženj (Egan & Mather, 2001, str. 174).

2.1 Varovanje informacijskega sistema

Pri varovanju informacijskega sistema moramo upoštevati naslednje koncepte:

- zaupnost,
- celovitost in razpoložljivost,
- najnižji privilegij,
- hitrost nadzora.

Izhajajo iz angleške kratice CIA(angl. *Confidentiality, Integrity and Availability*). Ti koncepti zajemajo udeležence v procesu varovanja informacijskega sistema, ki so osebje, postopki in tehnologija (Egan & Mather, 2001, str. 176).

Pri sestavljanju varnostne politike moramo zgoraj naštete koncepte še posebej upoštevati, saj bomo le tako dosegli primerno kakovost varovanja informacijskega sistema. Zaupnost pomeni, da posredujemo ali omejujemo dostop do informacij ali informacijskega vira z vidika zaupnosti oziroma ohranjanja tajnosti informacij ali informacijskega vira. To lahko dosežemo s šifriranjem prenosov in šifriranjem shranjenih podatkov.

Celovitost zagotavlja, da so nepooblaščenim osebam onemogočeni dostop, spreminjanje in brisanje informacij. Zagotavlja obstoj kontrol, ki so potrebne za zaščito celovitosti in neoporečnosti informacij in informacijskih virov.

Razpoložljivost zagotavlja, da imajo pooblaščene osebe dostop do informacij in informacijskih virov kadar koli in kjer koli, saj je tako zagotovljena optimalna uporabnost informacij in informacijskih virov.

Najnižji privilegiji pomenijo, da imajo zaposleni dostop samo do tistih informacij in informacijskih virov, ki so nujno potrebni za njihovo tekoče delo. Dostop do drugih informacij in informacijskih virov se jim onemogoči. Koncept najnižjih privilegijev je zelo pomemben v celotni shemi varnostne politike, saj se s previsokimi privilegiji poveča tveganje podjetja.

Zadnji iz sheme konceptov varovanja informacijskega sistema je hitrost nadzora oziroma ravnotežje med hitrostjo in stopnjo nadzora posameznih delov varnostne politike (Egan & Mather, 2001, str. 178).

2.2 Izdelava oziroma vzpostavitev varnostne politike informacijskega sistema

Za izdelavo varnostne politike informacijskega sistema obstaja več metod, načinov ali standardov. Vsaka organizacija ali podjetje si lahko postavi svoje lastne omejitve ali standarde glede na lastne želje in potrebe po varovanju informacijskega sistema. O varnostnih standardih bom več napisal v poglavju 3.3.

Izdelava varnostne politike in kot posledica posodabljanje varnostne politike informacijskega sistema se morata, za doseganje optimalne učinkovitosti, v organizaciji ali podjetju odvijati nenehno. Praksa kaže drugačne rezultate, saj se pogosto dogaja, da podjetje vzpostavi varnostno politiko glede na neko stanje, vendar je nato ne posodablja, kar stopnjo tveganja zopet dvigne na višjo raven. Vzpostavljanja in posodabljanja varnostne politike informacijskega sistema se je priporočljivo lotiti z organizacijo skupine za informacijsko varnost, ki skozi celotno obdobje skrbi za optimalno organiziranost, stalno posodabljanje in izvajanje varnostne politike.

Za prvi korak izdelave varnostne politike informacijskega sistema bi torej lahko vzeli ustanovitev skupine za informacijsko varnost, katere namen in odgovornost je, da skrbi v prvi fazi za pripravo, vzpostavitev, upoštevanje in posodabljanje varnostne politike informacijskega sistema. Organizacija skupine je priporočljiva predvsem, ker imajo člani skupine sicer širok razpon varnostnih nalog, vendar pa lažje delujejo usklajeno s skupnimi cilji, ki so v skladu s poslovno strategijo organizacije ali podjetja. Uprava podjetja se mora v vsakem trenutku zavedati, kako pomembna je za poslovanje varnostna politika, in mora biti pobudnik in podpornik uvedbe varnostne politike v podjetju. Tako se lahko izogne marsikateremu neprijetnemu položaju v primeru uresničitve varnostnih tveganj.

Drugi korak izdelave varnostne politike informacijskega sistema je izdelava spiska vseh informacijskih virov, ki jih organizacija ali podjetje poseduje ali jih bo posedovala v danem okolju. Med te informacijske vire štejemo (Štrakl, 2003, str. 21):

- računalniško opremo (osebne računalnike, strežnike ...),
- komunikacijsko opremo,
- podatkovne zbirke,
- podatkovne nosilce,

- druga osnovna sredstva (stavbe, opremo prostorov, napajalnike ...),
- dokumentacijo (uporabniško, sistemsko, arhive ...),
- sistemsko in uporabniško programsko opremo,
- človeške vire,
- notranje in zunanje storitve,
- druge vire, ki nastopajo v informacijskem sistemu.

V tem koraku izdelave varnostne politike informacijskega sistema je naloga skupine za informacijsko varnost ali katerega drugega telesa, ki je zadolženo za varnostno politiko, da vsak informacijski vir ustrezno varnostno klasificira glede zaupnosti, celovitosti oziroma razpoložljivosti, glede na privilegije in pa glede na hitrost nadzora. Prav tako je treba vsakemu informacijskemu viru določiti skrbnika, ki prevzame odgovornost za informacijski vir s stališča informacijske varnosti.

V tretjem koraku je za vsak posamezen informacijski vir izdelana natančna analiza tveganja. Izdelamo podroben spisek ocen ranljivosti in varnostnih groženj za vsak posamezen informacijski vir. Na osnovi parametrov varnostne klasifikacije, ocene ranljivosti in ocene groženj dobimo nato oceno varnostnega tveganja. Pri izdelavi analize tveganja moramo biti pozorni, da se ne omejujemo le na sredstva informacijske tehnologije, ampak moramo upoštevati tudi druge, v naslednjem poglavju omenjene dejavnike, ki nastopajo v organizaciji ali podjetju in posledično vplivajo na varnost informacijskega sistema, saj bo le tako varnostna politika informacijskega sistema uspešna in učinkovita.

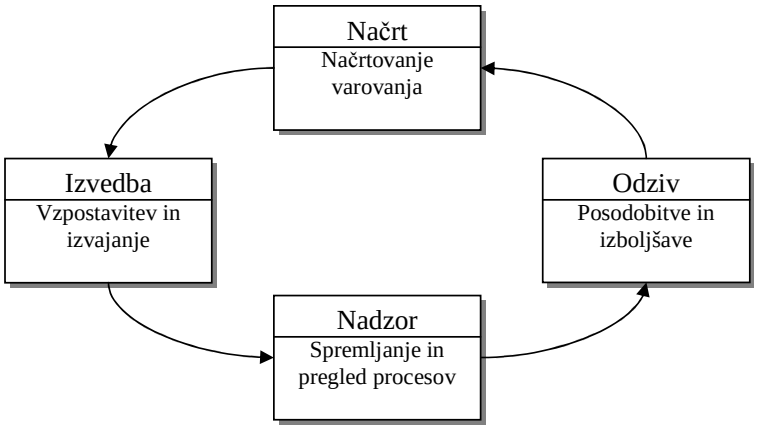
Analiza tveganj vsakega informacijskega vira poda neko osnovo za izdelavo varnostne politike informacijskega sistema organizacije ali podjetja. Običajno je v shemi varnostne politike določena neka osnovna hierarhija dokumentov, vendar pa je lahko struktura dokumentov od politike do politike različna, saj organizacije ali podjetja delujejo v različnih okoljih, poslovnih in kulturnih, in imajo zato različne poglede, potrebe in želje. Najpogosteje videna organiziranost varnostne politike informacijskega sistema je sestavljena iz krovne varnostne politike, v kateri so opisani in razloženi načelni pristopi podjetja k varovanju informacijskega sistema. Krovno varnostno politiko mora obvezno sprejeti uprava organizacije ali podjetja in je zato zavezujoča za vse uporabnike informacijskega sistema. Posamezni elementi varnostne politike so podrobneje obdelani v dokumentih v obliki varnostnih navodil ali pravilnikov, namenjenih uporabnikom informacijskega sistema podjetja. V teh dokumentih so opredeljene specifične varnostne zahteve, naloge, postopki in odgovornosti. Na kakšen način so te kategorije obdelane, je lahko povsem subjektivna odločitev organizacije ali podjetja, da prilagodi obliko dokumenta svojemu poslovanju.

Ko je varnostna politika informacijskega sistema definirana do želenega nivoja, se izvede ustrezne aktivnosti, ki obstoječi informacijski sistem in poslovne procese uskladi z določili varnostne politike. Varnostna politika informacijskega sistema je s tem implementirana.

Proces pa se na tem mestu še ne konča, saj je naloga skrbnika varnostne politike, da od tu naprej skrbi, da je varnostna politika informacijskega sistema »živ« proces. Za doseganje optimalne učinkovitosti varnostne politike je potrebno nenehno prilagajanje na spremembe, ki se odvijajo v informacijskem in poslovnem sistemu. Treba je nenehno spremljati procese in njihovo skladnost z varnostno politiko ter po potrebi prilagoditi procese ali varnostno politiko.

Demingov krog zelo dobro prikazuje opisani cikel.

Slika 2: Demingov krog



Vir: M. Štrakl, Varnostna politika informacijskega sistema, 2003, str. 22.

Izdelava in implementacija varnostne politike informacijskega sistema organizaciji ali podjetju ne zagotavlja boljšega varovanja, če se določil varnostne politike ne upošteva dosledno oziroma ne izvaja v praksi. Ozaveščenost o načinu izvajanja določil med uporabniki mora biti zagotovljena, zaradi tega mora organizacija ali podjetje poskrbeti za potrebna izobraževanja s področja varovanja informacij. Prav tako ni dobro, da je varnostna politika izdelana tako, da predstavlja oviro pri opravljanju poslovnih procesov organizacije ali podjetja.

2.3 Varnostni standardi

Pri zagotavljanju informacijske varnosti, pri sestavljanju varnostnih politik, zmanjševanju tveganj, odpravljanju ranljivosti in odzivanja na grožnje varnostni standardi v praksi predstavljajo različne možne poti, odvisno od posameznega standarda, izdelave varnostne politike. Varnostne standarde pripravljajo različne inštitucije, pokrivajo pa različna področja. Na področju varovanja informacij so najbolj razširjeni standardi BS 7799 (ISO 17799), CoBIT, NIST, BSI Baselines, GASSP, GMITS, ITIL, OCTAVE, COSO. Namen standardov je uvajanje sistematičnih pristopov varovanja podatkov. Na področju varovanja informacij je v praksi najpogosteje uporabljen standard ISO (angl. *International Standard Organization*) 17799, ki ga bom v nadaljevanju okvirno opisal.

Način izdelave varnostne politike informacijskega sistema je izbira organizacije ali podjetja, saj se delovanje in poslovanje organizacij ali podjetij med seboj zelo razlikuje. Odločitev, katere kriterije in metodologije bodo organizacije ali podjetja izbrale za izdelavo, je popolnoma prepuščena njim samim. Omenil sem že, da imajo za izdelavo varnostne politike informacijskega sistema več možnosti, vendar se v literaturi in tudi praksi največkrat omenja izbira standarda ISO 17799 oziroma njegovih naslednikov.
Standard ISO 17799 je razvila in sestavila vlada Velike Britanije s pomočjo industrijskih partnerjev. Standard je razdeljen na 12 glavnih kategorij (Prevod standarda BS ISO/IEC 17799:2005):

1. Ocena in obravnava tveganja – opredeli in obravnava tveganja, s katerimi se srečuje organizacija ali podjetje pri svojem delovanju.

2. Varnostna politika – obravnava formalne usmeritve in podpore za varovanje informacij. Poudarja pomen sodelovanja vodstvenih struktur pri ustvarjanju in vpeljevanju sistema varovanja informacij v celotni organizaciji ali podjetju.

3. Organizacija varovanja informacij – obravnava organizacijsko infrastrukturo, ki je temelj za učinkovito zaščito podatkov v sami organizaciji in pri prenosu podatkov izven organizacije.

4. Upravljanje sredstev – obravnava in opredeljuje skrb in odgovornost za varovanje informacijskih sredstev organizacije ali podjetja in klasificira informacije glede na pomen in občutljivost.

5. Varovanje človeških virov – kategorija natančno opredeli izbor kadra, izobraževanja in odgovornosti zaposlenih. Opredeli postopke za zmanjšanje tveganja človeške napake, kraje, poneverbe in izrabe zmogljivosti. Poudarja ozaveščenost pomembnosti in vrednosti informacij.

6. Fizična zaščita in zaščita okolja – obravnava fizično varovanje in dostop do opreme ter informacij, s ciljem preprečiti nepooblaščen fizični dostop, škodo in motnje v prostorih organizacije in informacijah.

7. Upravljanje komunikacij in produkcije – obravnava pravilno in varno delovanje zmogljivosti za obdelavo informacij. Določa odgovornosti in postopke za upravljanje ter postopke ravnanja v primeru okvar ali vdora v sistem.

8. Nadzor dostopa – obravnava dostopa do informacij, zmogljivosti za obdelavo informacij in poslovnih procesov, ki so nadzorovani na podlagi poslovnih in varnostnih zahtev. Pravila za nadzor dostopa morajo vsebovati politike za širjenje informacij in dodeljevanje pravic.

9. Nakup, razvoj in vzdrževanje informacijskih sistemov – zagotavlja, da je varnost celosten del informacijskega sistema. Informacijski sistemi vključujejo operacijske sisteme, infrastrukturo, poslovne aplikacije, ne specializiranih izdelkov ter storitev in znotraj organizacije razvitih aplikacij. Načrtovanje in vpeljava informacijskih sistemov, ki podpirajo poslovne procese, sta lahko bistvenega pomena za varnost. Pred razvojem in vpeljavo informacijskih sistemov je treba prepoznati in doseči soglasje glede varnostnih zahtev, ki v organizaciji ali podjetju obstajajo.

10. Upravljanje incidentov pri varovanju informacij – opredeljuje uradne postopke za poročanje o incidentih in postopke o ravnanju ob zaznavi incidentov. Bistveno je predvsem pravočasno ukrepanje.

11. Upravljanje neprekinjenega poslovanja – obravnava neprekinjeno poslovanje in zaščito kritičnih poslovnih procesov pred posledicami večjih okvar informacijskih sistemov ali nesreč ter zagotovitev njihovega pravočasnega ponovnega delovanja.

12. Združljivost z zakonskimi zahtevami – obravnava preprečevanje kršitve zakonov, kršitve statutov, zakonskih ali pogodbenih obveznosti in vsakršnih varnostnih zahtev.

Informacijska varnost oziroma varnostna politika, organizirana po standardu ISO 17799, omogoča celovit pregled varnosti, ki je predpogoj za učinkovito varnost v organizaciji ali podjetju. Obvezno pa se mora vsaka organizacija ali podjetje zavedati, da je vpeljava varnostnega standarda, katerega koli, šele prvi korak k informacijski varnosti. Varnostno politiko, izdelano po standardu, je treba nato še dosledno upoštevati, jo obnavljati, torej slediti razvoju tehnologij in razvoju standarda, se izobraževati. Samo izdelava varnostne politike po vzoru standarda nam ne zagotavlja informacijske varnosti.

Razlog za uporabo varnostnih standardov je zagotovitev sistematičnega pristopa k reševanju informacijske varnosti. Kriteriji, ki so nam v pomoč pri odločanju za izdelavo varnostne politike, so (M. Štrakl, 2003, str. 23):

- hiter razvoj in rast informacijskih sistemov, hkrati pa odprtost sistemov, interakcija med sistemi in povezanost z internetom;
- porast informacijskih groženj za programsko, delovno in mrežno opremo, kar je posledica izjemno hitrega razvoja informacijske tehnologije;
- nenehno odkrivanje novih ranljivosti v obstoječih in novih informacijskih tehnologijah, kar ima posledično lahko negativen vpliv na poslovanje organizacije ali podjetja;
- zahteve po večji konkurenčnosti organizacije ali podjetja, kar vpliva na učinkovitost in produktivnost opreme, osebja in procesov, hkrati pa zahteve po čim nižjih stroških;
- vse večje potrebe in zahteve po usklajenem poslovanju s svetovnimi regulatorji (Sarbanes-Oxley Act, Basel II, Privacy and Data Protection Legalisation);
- tržni primanjkljaj strokovno usposobljenega kadra in ključnih znanj na področju varovanja informacij.

2.4 Obvladovanje tveganj informacijske varnosti

Obvladovanje tveganj (angl. *Risk Management*) je v teoriji pojmovano kot nasprotje poslovni spretnosti. V stvarnosti pa upravljanje in ravnanje s tveganjem predstavlja grajenje poslovno uspešnejšega poslovnega sistema, ki zmore nase prevzeti največje možno tveganje na najvarnejši možni način. Za poslovno uspešnost ni dovolj, da se tveganju odrečemo, ampak kako tveganje varno sprejmemo.

Za doseganje informacijske varnosti podjetja je priporočljivo, da podjetje izdela natančno shemo upravljanja in ravnanja s tveganjem, saj bo takšna shema podjetju pomagala pri prepoznavanju različnih groženj in nevarnosti, ranljivosti in odzivov na nevarnosti ter seveda pri iskanju primernega načina za odpravo vseh teh pomanjkljivosti. Podjetje mora poskrbeti, da so orodja za upravljanje in ravnanje s tveganjem, kot na primer orodja za ponovno vzpostavitev informacijskega sistema (angl. *Disaster Recovery*), orodja za planiranje neprekinjenega poslovanja (angl. *Business Continuity Planning*) in orodje za planiranje obvladovanje tveganja (angl. *Enterprise Risk Management*), usklajena.

Organizacijsko planiranje obvladovanja tveganj je ponavljajoč se organizacijski proces, ki nenehno identificira in išče načine odpravljanja tveganja v podjetju ter jim sledi. V preteklosti so podjetja prepustila obvladovanje tveganj finančnim in pravnim delom podjetja, danes pa se je obvladovanje tveganj zaradi hitrega razvoja informacijske tehnologije v veliki meri preselilo tudi v informatiko (Proctor, 2007, str. 3).

Strokovnjaki analitičnega podjetja Gartner (2007) predvidevajo, da je glavna naloga informatike na področju varovanja informacij v prihodnosti prehod iz starega sistema varovanja informacij, kjer se je varovalo informacijski sistem kot celoto, na nov sistem, kjer z obvladovanjem tveganj v povezavi s poslovnimi funkcijami podjetja ocenimo, katero od tveganj nam predstavlja največjo nevarnost in s tem katero področje informacijskega sistema moramo najbolj zavarovati. Cilj informatike je, da organizacija ali podjetje nemoteno posluje, kar pomeni, da se zavarujemo tam, kjer nam preti največja nevarnost.

Optimalno porazdelitev tveganj dosežemo z varnostnimi standardi, ki so sestavljeni tako, da je tveganje z upoštevanjem varnostnih standardov kar najnižje. O varnostnih standardih, najpogosteje uporabljenih v ta namen, sem pisal v poglavju 3.3. Obvladovanje tveganj informacijskih sistemov postaja pomembna naloga informacijske varnosti, kar v preteklosti ni bila.

Obvladovanje tveganj lahko razdelimo na tri glavne komponente, te se delijo na podkomponente. Tri glavne komponente so (Caldwell & Mogull, 2006, str. 3):

- ocenjevanje tveganja,
- ublažitev ali sprejemanje tveganja,
- sporočilo tveganja.

Ocenjevanje tveganja je osredotočeno na zbiranje, analiziranje in ocenjevanje rizičnih informacij, tako da se lahko ukrepanje kar najhitreje začne. Ko je tveganje enkrat identificirano, je možnost, da bi ta oblika tveganja organizaciji ali podjetju škodila, zelo zmanjšana, saj so na ukrepanje pripravljeni. Nekatere oblike tveganja se pojavljajo pogosteje kot druge in ni nujno, da bo imela ena oblika tveganja enak vpliv na vse organizacije ali podjetja. Vplivi in s tem tudi škoda, ki jo neka oblika tveganja lahko povzroči, so si med seboj

lahko zelo različni. Ocenjevanje tveganja je sestavljeno iz analize in vrednotenja. Analiza tveganja uporabi znane grožnje in ranljivosti, podatke analizira in identificira nevarnosti ter tako napove tveganje. Vrednotenje tveganja primerja ocenjeno tveganje z danimi parametri in tako določi pomembnost oblike tveganja. Ocenjevanje tveganja je lahko kvalitativno ali kvantitativno in doseženo prek avtomatiziranih ali ročnih metod.

Ublažitev ali sprejemanje tveganja skrbi – ko sta oblika tveganja in njegov vpliv enkrat identificirana – da se sprejme in izvede določene ukrepe, ki bodo vpliv tveganja ublažile ali zmanjšale. Tu bi opozoril, da je zmotno razmišljati, da je edina možnost tveganje zmanjšati, saj obstajajo primeri, ko se tveganje sprejme. Vendar pa to ni odločitev informatike, ampak poslovnega dela podjetja. Imamo več možnosti, kako obvladati tveganje (Byrnes, Noakes-Fry & Nicolett, 2006, str. 2–6):

- Sprejemanje tveganja: v primeru, da je možnost pojava tveganja neznatna ali da bi bil njegov vpliv resnično majhen, se organizacija ali podjetje lahko odloči tveganje sprejeti.
- Izogibanje tveganju: ko se oceni, da bodo stroški visoki, prebroditev pa težka, se je tveganju bolje izogniti.
- Premestitev ali delitev tveganja: kadar je tveganje del poslovanja in stroški predvidljivi, se organizacija ali podjetje lahko odloči, da bodo premestili ali delili tveganje prek zavarovanj, pogodb, garancij ali dogovorov o sodelovanju.
- Zmanjšanje ali ublažitev tveganja: pogosto je tveganje pri poslovanju preprosto prisotno; v takem primeru potrebujemo različna orodja, ki nam pomagajo tveganje zmanjšati ali ublažiti.
- Ignorirati tveganje: ignorirati tveganje je zelo nevarno.

Sporočilo tveganja je, da mora biti upravljanje in ravnanje s tveganjem usklajeno z vsemi deli organizacije ali podjetja, da se bomo vplivi in posledice tveganja najnižji. Identificiranje in analiziranje tveganja mora biti prioriteta vsake organizacije ali podjetja.

3 Soodvisnost informacijskih groženj in varnostne politike skozi čas

3.1 Informacijska varnost in tehnologija pred letom 2000

Informacijska tehnologija in informacijska varnost sta produkta 20. stoletja. Razvoj informacijske varnosti in tehnologije sem v diplomski nalogi razdelili na dve obdobji, in sicer na obdobje pred začetkom uporabe svetovnega spleta in obdobje po začetku uporabe.

Pred začetkom uporabe svetovnega spleta je bil nivo informacijske varnosti precej višji kot po začetku. Drži, da je bila uporaba svetovnega spleta v obdobju po nastanku veliko nižja, kot je danes. Svetovni splet se je uporabljalo za enostavnejše oziroma osnovne operacije, predvsem zaradi enostavnejših tehnologij, ki so bile takrat na voljo. Začetek uporabe svetovnega spleta lahko razdelimo v štiri večje skupine. V prvi je komunikacija prek elektronske pošte.

Elektronsko pošto so ob njenem pojavu ob koncu 60. let uporabljali le naprednejši uporabniki. V drugo skupino bi uvrstil uporabo svetovnega spleta kot leksikon oziroma enciklopedijo informacij. Pojavili so se spletni iskalniki, kot so Google, Altavista in podobni. To so bili začetki njihovega bolj ali manj uspešnega razvoja. V tretjo skupino sem uvrstil prenos podatkov. Zaradi tehnologije, ki je omogočala le omejen, počasen in razmeroma drag prenos podatkov, so uporabniki funkcijo osvojili počasi. V največji meri smo s svetovnega spleta prenašali le programsko opremo manjšega obsega, glasbene datoteke in nekatere druge malenkosti. V četrto skupino sem uvrstil prve korake spletnega bančništva. Spletno bančništvo je, zaradi posedovanja ključnih podatkov, ob pojavu postavilo povsem nova, višja merila informacijske varnosti.

3.1.1 Informacijski sistemi, tehnologija in uporabniki

3.1.1.1 Informacijski sistemi

Informacijski sistemi so se pojavili v 20. stoletju z razvojem informacijske tehnologije oziroma informatike. Z razvojem vse kompleksnejših strojev in razvojem računalniške tehnologije v drugi polovici stoletja so se pojavili tudi računalniško podprti informacijski sistemi. Razvoj informacijskih sistemov in razvoj informacijske varnosti sta potekala vzporedno v soodvisnosti.

Vpliv informacijske varnosti na razvoj informacijskih sistemov je bil v 20. stoletju relativno nizek, kar se dobro opazi predvsem v kronološkem pregledu razvoja informacijskih groženj, nevarnosti in ranljivosti, ki sem ga pripravil v nadaljevanju. Opaziti bo, da se je varnost informacijskih sistemov večinoma razvijala le kot odgovor na varnostne incidente ali varnostna tveganja.

Kot največji izziv pri zagotavljanju varnosti informacijskih sistemov se je izkazal razvoj interneta in vseh njegovih funkcionalnosti.

Osnovna pomanjkljivost, zaznana pri informacijskih sistemih in skupna vsem različnim operacijskim sistemom, je bila pomanjkljiva razdelitev vlog uporabnikov operacijskih sistemov.

3.1.1.2 Informacijska tehnologija

Za preteklo stoletje je značilen začetek razvoja informacijske tehnologije. Hitremu razvoju informacijske tehnologije pa žal ni sledil hiter razvoj informacijske varnosti. Omejena uporaba tehnologije je botrovala majhni potrebi po hitrem razvoju informacijske varnosti. Podjetja so varnostne incidente reševala ad hoc in po večini dokumenta varnostne politike informacijskega sistema niso imela napisanega.

Za razvoj informacijske varnosti je pomembnih predvsem zadnjih deset let 20. stoletja, ko se je informacijska tehnologija razvijala najhitreje. S širitvijo uporabe osebnih računalnikov in

razcvetom svetovnega spleta so hekerji pridobili nove možnosti dostopa do vse večje količine podatkov. Varnost poslovnih sistemov je bila pod vse večjim pritiskom informacijskih tveganj in nevarnosti.

3.1.1.3 Uporabniki

Uporabniki v 20. stoletju so prešli iz visokospecializiranih strokovnjakov, ki so vodili razvoj tehnologij, do povsem tipičnih uporabnikov, ki tehnologije uporabljajo dnevno, tako na delovnem mestu kot v vsakdanjem življenju. Zgodovinska dejstva pripovedujejo, da je za podoben prehod informacijska tehnologija potrebovala 50 let, kar je v primerjavi s stroji industrijske revolucije malo.

Ob koncu 20. stoletja, ko so se prvič pojavile resne informacijske grožnje in nevarnosti, so bili tipični uporabniki večinoma najstniki in odrasli, mlajši od 50 let. Starejše generacije (nad 50) so imele z navajanjem na novo delovno orodje – osebni računalnik – težave. Najstniki so osebne računalnike uporabljali po večini že zelo vešče. Osebni računalnik je počasi začel prevladovati kot glavno delovno orodje v pisarnah in na drugih delovnih mestih (Isselhorst, 2007, str. 3).

3.1.2 Kronološki pregled informacijskih groženj, nevarnosti in ranljivosti

Škodljiva oziroma zlonamerna programska koda velja v širši javnosti za pereč problem dokaj kratek čas. Mediji v zadnjih letih redno poročajo o novih in novih informacijskih grožnjah, nevarnostih in ranljivostih. Realnost je nekoliko drugačna. Prvih razvitih računalnikov resda ni napadla škodljiva ali kakšna druga zlonamerna programska koda, kar seveda ne pomeni, da groženj, nevarnosti in ranljivosti ni bilo. Prvi maloštevilni uporabniki informacijske tehnologije niso bili dovolj usposobljeni, da bi informacijsko tehnologijo zlonamerno izkoriščali, prav tako pa to ni bil njihov namen. Z razvojem se je položaj bistveno spremenil. Nove informacijske tehnologije so ponudile nove možnosti, ideje in izzive, tako na dobri kot tudi na slabi strani, predvsem pa je to postalo očitno s pojavom širokopasovnih povezav, ki omogočajo precej boljšo povezljivost. Za boljšo predstavo sem v naslednjih poglavjih kronološko predstavil razvoj škodljive oziroma zlonamerne programske kode skozi čas.

3.1.2.1 Začetki škodljive programske kode do leta 1970

Strokovna javnost si sicer ni enotna, kdaj se je v resnici pojavil prvi računalniški virus, dejstvo pa je, da ga prvi računalnik, ki ga je izumil g. Charles Babbage, ni imel. Ideja o računalniškem virusu se je pojavila v štiridesetih letih 20. stoletja z delom madžarskega znanstvenika Johna von Neumanna (1903–1957). V svojih študijah in raziskavah je von Neumann preiskoval teorijo naprav in programov, ki so se sposobni sami razmnoževati in obnavljati. V letu 1959 je britanski matematik Lionel Penrose v seriji člankov z naslovom »Samoreproduktivni stroji« (angl. *Self-Reproducing Machines*) predstavil svoje videnje o avtomatičnih samoobnovitvenih oziroma samorazmnoževalnih programih. Penrose je predstavil enostavni dvodimenzionalni model, katerega struktura je bila zgrajena tako, da se je

lahko program aktiviral, spreminjal in množil sam. Ta model je bil kmalu uporabljen tudi na računalnikih IBM 650. Te raziskave in študije niso bile opravljene z idejo o postavitvi osnov za razvoj računalniških virusov, temveč z idejo zagotoviti temelje za nadaljnji razvoj informacijske tehnologije.
Leta 1962 je skupina inženirjev ameriškega podjetja America's Bell Telephone Laboratories razvila računalniško igro Darwin, ki je simulirala delovanje računalniškega virusa. Nasprotna igralca sta napisala vsak svoj program, ki sta se nato bojevala med seboj. Programa sta lahko sledila drug drugemu, se razmnoževala in uničevala drug drugega. Cilj igrice je bil pridobiti kontrolo nad bojiščem z izbrisom nasprotnega programa. Na podoben način danes delujejo zlonamerni programi, vendar igrica ni bila izdelana s tem namenom (VirusEncyclopedia, 2008).

Na tej stopnji razvoja zlonamerne programske kode še ni bilo govora o izdelavi varnostne politike v današnjem pomenu, saj podjetja niso imela potrebe po tako specifičnem dokumentu.

3.1.2.2 Škodljiva programska koda v 70. in 80. letih

V začetku sedemdesetih let so na omrežju ARPANET, ameriškem vojaškem omrežju, ki šteje za predhodnika današnjega interneta, odkrili enega prvih računalniških virusov. Virus Creeper se je po omrežju širil prek računalnikov z uporabo modemov. Njegov namen je bil pridobiti nadzor nad računalnikom in se kopirati na druge v omrežje priključene računalnike. Creeperju je sledil virus Reaper, katerega naloga je bila izbrisati virus Creeper. Reaper je imel prav tako sposobnost samostojnega širjenja po omrežju in prevzemanja nadzora nad računalniki. Napisan je bil anonimno in še danes ni jasno, ali ga je napisala druga oseba kot Creeperja z namenom izbrisa ali ga je napisala ista oseba, da bi popravila napako.

Leta 1974 se je pojavil virus z imenom Zajec (angl. *Rabbit*). Ime izhaja iz njegove lastnosti oziroma sposobnosti množiti se zelo hitro. Ko je prišel v sistem, je začel delati kopije samega sebe in s tem slabil računalniški sistem. Ko se je dovolj namnožil,je s tem popolnoma onesposobil sistem.

Leta 1975 je bila napisana računalniška igrica Prodirajoča žival (angl. *Pervading Animal*), za katero analitiki še danes niso enotnega mnenja, ali je bil to prvi primer trojanskega konja ali samo še en primer virusa. Ob zagonu igre se je ta kopirala v datoteke sistema. To je počela ob vsakem zagonu, kar sicer ni uničevalo sistema, ga je pa zelo upočasnilo in oviralo.

V začetku osemdesetih let so računalniki začeli pridobivati uporabno vrednost in vse več posameznikov je začelo samostojno razvijati računalniške programe. Napredek v komunikacijskih povezavah je omogočil boljšo in širšo povezljivost, kar je bila idealna podlaga za razvoj trojancev[1]. Množično so se pojavili prvi trojanci, ki pa niso imeli sposobnosti samostojnega množenja, so pa v primeru namestitve na računalnik povzročili

[1] Trojanski konj – v informatiki je to oblika škodljive programske kode.

ogromno škode. Ker je bila Applova platforma v začetku osemdesetih prevladujoča, se ne gre čuditi, da je največ zlonamernih programov nastalo prav za računalnike na platformi Apple II. Virus Elk Cloner se je širil prek okuženih disket na operacijskem sistemu Apple II. Ob zagonu računalnika z okužene diskete se je kopija virusa samostojno zagnala. Sam virus ni oteževal dela računalnikom, njegov namen je bil le okužiti neokuženo disketo. Tako se je počasi širil. Ob zagonu je Elk Cloner prikazoval šale, utripajoče besedilo in vrteče se slike.

Brain je bil prvi virus za kompatibilne računalnike IBM, napisan oziroma zaznan leta 1986. Brain se je v nekaj mesecih razširil po celem svetu, okužil pa je zagonske sektorje računalnikov. Zaradi pomanjkanja oziroma slabe informacijske in varnostne ozaveščenosti je bil uspeh virusa Brian zelo velik. Napisala sta ga 19-letni pakistanski programer Basit Farooq Alvi in njegov brat Amjad. Avtorjev ni bilo težko odkriti, saj so bili njuni podatki zapisani v programski kodi. Virus ni bil napisan z namenom povzročanja škode, temveč z namenom preizkusiti stopnjo privatnosti. Z namestitvijo na žrtev ni povzročil nikakršne škode, shranil se je v zagonske sektorje in spremenil ime diska v »©Brain«. Predvidevajo tudi, da je bil Brain prvi vohunski tip virusa, kar pomeni, da je virus vsakič, ko je želel kdo brati okužene datoteke, prikazal prvotne podatke.

V letu 1987 sta se poleg drugih pojavila virusa Vienna in Lehigh. Za virus Vienna se še danes ne ve, kdo je njegov resničnih avtor. Kot mogoča avtorja se pojavljata predvsem Swoboda Franco in Burger Ralf, ki pa za nastanek virusa obtožujeta drug drugega.

Lehigh je bil prvi virus, ki je povzročil poškodovanje podatkov, shranjenih na trdih diskih. Na srečo nikoli ni ušel iz nadzorovanega okolja univerze Lehigh, kjer so ga naredili. Virus je najprej okužil sistemske datoteke command.com, nato pa je začel uničevati datoteke in nazadnje uničil še samega sebe. Takšen način delovanja je torej na koncu pripeljal do popolnega uničenja podatkov na računalniku.

Suriv je skupina virusov, katerih avtor ni znan, domneva se le, da je bil virus narejen v Izraelu. Prav tako kot pri virusu Brain se ne ve, ali je bil to le poizkus, ki je ušel iz kontroliranega območja, ali je bil to namensko narejen in spuščen virus. Avtor je poizkušal spremeniti proces nameščanja datotek v formatu *.exe.

Zadnji večji virus v letu 1987 je bil šifrirani kaskadni virus (angl. *Cascade*). Da se je aktiviral, je bilo vidno, ko so se ikone na zaslonu premaknile v osnovno (stratno) vrstico. Virus je bil sestavljen iz dveh delov, in sicer virusa kot osnove in šifrirne metode. Šifriranje je služilo zakrivanju virusa, saj je bil virus prikazan drugače v vsakem okuženem dokumentu. Ob zagonu dokumenta je kontrola prenesla šifrirni postopek, ki je dešifriral virus in prenesel kontrolo nad dokumentom nanj. Kaskadni virus je v zgodovini razvoja škodljivih programov predstavljen kot predhodnik polimorfičnih[2] virusov. Kaskadni virus je večjo škodo povzročil le leta 1988 v belgijski pisarni podjetja IBM. IBM je incident uporabil za razvoj boljšega antivirusnega programa.

[2] Značilnost polimorfičnih virusov je, da nimajo stalne programske kode, ampak imajo sposobnost prilagajanja.

Konec leta 1987, v decembru, pa se je pojavila prva širše razširjena oblika škodljive oziroma zlonamerne programske kode v obliki mrežne epidemije. Imenovala se je Črv božičnega drevesa (angl. *Christmas Tree Worm*). Črv je bil napisan v programskem jeziku REXX, množil oziroma širil pa se je prek operacijskega sistema VM/CMS-9. Ob namestitvi na računalnik, seveda nezaželeni, se je črv prikazal v obliki božičnega drevesca in hkrati poslal kopije samega sebe na vse naslove, ki jih je našel v sistemskih datotekah (angl. *Names, netlog*). Črv je bil spuščen v britansko omrežje z neke zahodnonemške univerze z namenom testiranja.

Leto 1988 je bilo leto prvih večjih epidemij in potegavščin zlonamerne programske opreme. Prvi tak je bil virus Jeruzalem, ki je bil opažen v ZDA, Evropi in Bližnjem vzhodu na petek, 13. maja. Zelo slaba stran virusa Jeruzalem je bila, da je uničil vse podatke, shranjene na okuženem računalniku. Zaradi njegove razširjenosti so tisti petek poimenovali Črni petek. Zanimivo, da informacijski strokovnjaki še danes posvečajo izredno pozornost petkom 13.

Leto 1988 je tudi leto prvih ustanovitev malih antivirusnih podjetij, ki so izdelovala dokaj enostavne skenerje, ki so pregledovali računalnike. Uporabniki skenerjev, torej programov, ki so delovali kot skenerji, so bili še posebej navdušeni nad dodatnimi programi, nekakšnimi imunizatorji. Ti programi so posredovali različni zlonamerni programski opremi, ko se je hotela namestiti na računalnik, signal okuženosti. Bili so torej nekakšni zavojevalci zlonamerne programske opreme. Imunizatorji so delovali, dokler število virusov, črvov in druge zlonamerne programske opreme ni resnično naraslo. Imunizatorji so bili sposobni delovati le proti znani zlonamerni programski opremi.

Kljub temu da je bila antivirusna programska oprema na razpolago zastonj ali po izredno nizki ceni, proizvajalcem ni uspelo bistveno navdušiti večjega števila uporabnikov, saj se ti še niso popolnoma zavedali, kaj pomeni informacijska varnost. Poleg tega pa so imeli še eno veliko pomanjkljivost, saj antivirusni programi proti novim virusom niso delovali. Vsak primerek zaznane zlonamerne programske opreme je bilo treba dodati na listo, drugače protivirusna zaščita ni delovala. Tudi dejstvo, da so bili uporabniki zelo slabo podučeni in niso verjeli ne v zlonamerno programsko opremo ne v protivirusno programsko opremo, ni koristilo razširjenosti antivirusne programske opreme.

Prelomno je bilo leto 1988, tudi zaradi organizacije prvega elektronskega foruma na temo protivirusne varnosti 22. aprila. Forum se je imenoval Virus-L in je deloval na omrežju Usenet, ustvaril pa ga je g. Ken van Wyk.

Prve večje potegavščine z uporabo virusa segajo v leto 1988. Zanimivo je, da niti niso uporabili virusa. Dovolj je bilo, da so razširili govorice, na različne načine, o virusih, in uporabniki so se ustrašili ter govorice jemali resno. Resno potegavščino si je privoščil Robert Morris, ki je javnost najprej opozoril, nato pa v omrežje spustil črva Morris, ki je v 12 minutah okužil ogromno računalnikov (300.000). Deloval je na podoben način kot Črv

božičnega drevesa, torej pošiljal je ogromno število kopij samega sebe in tako dodobra zapolnil promet na mreži, v nekaterih primerih mrežo tudi popolnoma zasedel in s tem ustavil promet. Celotno škodo, ki jo je povzročil črv Morris, ocenjujejo na okoli 96 milijonov ameriških dolarjev.

Proti koncu 80. let so na Nizozemskem v okviru policije začeli aktivni boj proti organiziranemu internetnemu kriminalu. Razvili so antivirusni program, ki je bil sposoben onesposobiti virus Datacrime, in ga za simbolično vsoto enega dolarja najprej prodajali le lokalno. Kmalu je povpraševanje naraslo in prodanih je bilo še več primerkov, vendar pa so kmalu ugotovili, da je antivirusni program pomanjkljiv. Kljub temu da je bila izdelana naslednja verzija, pa to na dolgi rok ni rešilo problemov.

Decembra 1989 je bila svetovna javnost priča domiselni prevari z disketami. 20.000 disket z naslovom »Informacijska disketa o aidsu«, ki so vsebovale trojanskega konja, je bilo poslanih na različne naslove v Evropi, Afriki, Avstraliji in na naslove Svetovne zdravstvene organizacije (angl. *World Health Organization*). Naslovi so bili ukradeni iz podatkovne baze »PC Business World«. Ob zagonu diskete se je trojanski konj preselil v sistem in tu zagnal skrit škodljivi program, ki se je namestil v sistem. Virus je ostal skrit do devetdesetega zagona računalnika, ko je virus zakodiral in zakril vse datoteke, spravljene na računalniku. Vidna je ostala ena sama datoteka, v kateri je bilo spravljeno sporočilo in številka bančnega računa, kamor naj bi uporabniki nakazali denar, da pridobijo podatke nazaj. Zaradi obilice podatkov o avtorju trojanskega konja tega ni bilo težko izslediti. Kljub temu da je bil Joseph Popp že pred tem razglašen za neprištevnega, so ga italijanske oblasti obsodile v odsotnosti (Virus Encyclopedia, 2008).

Pri zgornjem časovnem pregledu škodljive programske kode lahko opazimo, da se je razvoj škodljive kode pričel kot poizkusi zmogljivosti nove tehnologije. Z razvojem so pričeli škodljivo kodo uporabljati s škodljivimi nameni. Z vse več varnostnimi incidenti je sledil tudi razvoj varnostne politike kot eden izmed načinov reševanja ali preprečevanja incidentov. Tarče so bili po večini poslovni sistemi. Hekerji se s podatki privatnih uporabnikov takrat še niso ukvarjali.

3.1.2.3 Škodljiva programska koda v 90. letih

Če bi lahko osemdeseta leta prejšnjega stoletja na področju škodljive programske kode opisali kot leta raziskovanja in tipanja, so devetdeseta predvsem leta pospešenega razvoja škodljive programske opreme. Začetek je bil sicer zmeren, nadaljevanje pa nedvomno eksplozivno. Razlog je bil predvsem v sočasnem razvoju informacijske tehnologije.

Na samem začetku devetdesetih let, torej leta 1990, se je pojavilo več različnih polimorfičnih virusov, od katerih je prišel najbolj do izraza virus Kameleon, ki je predstavljal posodobitev virusov Vienna in kaskadnega virusa. Kameleon je bil šifriran ter se je z vsako okužbo modificiral. Vendar ni bil dolgo učinkovit, saj so se proizvajalci antivirusnih programov zelo potrudili, da so izdelali programe s sposobnostjo ustavljanja polimorfičnih virusov.

Začetek devetdesetih let in deloma tudi nadaljevanje sta bila predvsem v znamenju velikega števila virusov z bolgarskim poreklom. To so bili virusi z imeni Murphy, Nomenclatura, Beast ter drugi in njihove izpeljanke. Posebno aktiven in prodoren je bil avtor virusov z vzdevkom Dark Avenger, ki je izdelal in razposlal po več virusov letno. Posebnost njegovih virusov je bila drugačna tehnika zakrivanja in šifriranja virusa, povsem nova pa je bila lastnost, da je virus ob zaznavi avtomatično okužil vse dokumente na računalniku, tudi tiste, ki so bili označeni kot dokumenti samo za branje (angl. *read-only*). Za širjenje svojih »kreacij« je uporabljal elektronsko oglasno desko, kar mu je omogočilo zelo hitro širjenje virusov. Elektronska oglasna deska je delovala tako: ko je nekdo naložil virus na oglasno desko, mu je bilo omogočeno, da z nje sname virusov, kolikor hoče.

Leto 1991 je bilo, kar zadeva škodljivo programsko kodo, relativno mirno. Število vseh opaženih virusov je naraslo do številke 300.

Leto 1992 je posebno predvsem po tem, da so napadalci prenehali napadati sisteme IBM in MS-DOS, saj so proizvajalci teh sistemov popravili luknje in odpravili druge pomanjkljivosti, hkrati pa se je vse več uporabljalo IBM in MS-DOS. Tako so postajali vse priljubljenejši predvsem zagonski virusi in njihovo število se je dnevno povečevalo.

V tem letu se pojavi prvi protiantivirusni program z imenom Breskev (angl. *Peach*). Deloval je tako, da je uničil oziroma izbrisal podatkovno bazo antivirusnega programa. Ker antivirusni program ob zagonu ni zaznal podatkovne baze, je domneval, da se zaganja prvič, in tako ponovno namestil bazo. Medtem pa je imel virus čas, da se namesti in okuži podatke v sistemu.

V marcu 1992 je prišlo do izbruha virusa Michelangelo. To je bil eden prvih izbruhov računalniških virusov, ki je bil medijsko dobro pokrit. O virusu Michelangelo se je začelo govoriti že v letu 1991. Pred njegovim izbruhov so strokovnjaki napovedovali, da bo okužil vsaj 5 milijonov računalnikov, vendar je bila na koncu ta številka veliko manjša – nekaj tisoč.

Z vsakim letom so pisci škodljive računalniške kode jemali svoj delo resneje. Leto 1993 je prineslo veliko virusov različnih novih oblik in tehnologij. Sproščeni so bili virusi kot na primer: Carbuncle, Emmie, Bomber, Urugvay in Cruncher, ki so vsi uporabljali nove tehnologije zakrivanja samega sebe med kodo okuženih dokumentov in datotek. Prav tako v letu 1993 je Microsoft predstavil svoj prvi antivirusni program za zaščito svoje programske opreme. Na začetku so neodvisni testi antivirusnega programa pokazali veliko učinkovitost programa, vendar pa je ta začela s časom bledeti in projekt razvoja antivirusnega programa so s tem ustavili.

Pojav škodljive programske kode na kompaktnih ploščah (angl. *Compact Disk*) je bil opažen v letu 1994. Zaradi hitre širitve medija je bilo okuženih ogromno število računalnikov.

Prvi primer škodljive programske kode za Okna 95 (angl. *Windows95*) se je pojavil na začetku leta 1996 pod imenom Boza. Celotno leto 1996 je bilo zelo produktivno z vidika škodljive programske kode za programe podjetja Microsoft. Na pomlad istega leta se je pojavil prvi epidemičen virus za Okna 3.x, ki ga je povzročil Win.Tentacle in je bil prvi Windowsov virus, zaznan izven kontroliranega okolja. Poleti je bil zaznan virus OS2.AEP, katerega cilj je bil okužiti datoteke OS2.EXE. Delovanje virusa je bilo nadvse enostavno, saj se je dokopal do datoteke in jo preprosto uničil ali pa je omogočil dostop drugega sorodnega virusa. V drugi polovici leta so izdelovalci škodljive programske kode prvič napadli Microsoft Excel z virusom Laroux. Virus so skoraj popolnoma sočasno odkrili na dveh različnih kontinentih. Deloval je na podoben način kot virus MS Word, na principu makrov[3]. Njihova naloga oziroma cilj je pretihotapiti se v datoteke in tam izvajati različne operacije, odvisno od naloge.

Tudi v letu 1997 se je večinoma nadaljeval trend napadov in izdelovanja škodljive programske kode za različne verzije programa Windows. Da se bolj razširjeni in popularnejši računalniški programi težko izognejo škodljivi programski kodi zaradi svoje zanimivosti, je postalo jasno, ko je bil zaznan virus LinuxBliss, prva škodljiva programska koda za operacijske sisteme Linux. Večinoma so bili to trojanski konji.

Prva škodljiva programska koda v obliki internetnega črva z imenom Homer je bila zaznana aprila 1997. Homer je za svoje širjenje uporabljal strežnike FTP[4]. Nekako v tem času je škodljiva programska koda postala vse razpoznavnejša predvsem zaradi medijske razpoznavnosti in pa razširjenosti programske opreme, kateri je škodovala. Ravno to pa jo je naredilo še privlačnejšo zlonamernim programerjem. Junij 1997 je prinesel prvo škodljivo programsko kodo, ki je šifrirala sama sebe. WIN95.Mad je bil virus za Okna 95, pojavil se je predvsem v Rusiji in povzročil pravo epidemijo. Snovalci virusa Esperanto so bili prvi, ki so poskusili narediti virus, ki bi bil sposoben škodovati več platformam (DOS, Windows in MacOS) hkrati, vendar poskus ni bil uspešen.

Bolj ko se je bližal konec 90. let, več škodljive programske kode se je razvijalo. Podjetje Microsoft in vsa njihova programska oprema je zaradi svoje razširjenosti postalo zelo interesantna tarča. Trojanski konji so postali zelo priljubljeni med razvijalci škodljive kode. V letu 1998 je bilo razvito večje število trojancev, namenjenih kraji osebnih gesel in omogočanju oddaljenega dostopa do računalnikov. Prav tako se je nadaljevala distribucija škodljive kode prek kompaktnih diskov, ali je bilo to načrtovano, velikokrat pa tudi ne. Predvsem znan je primer revije PC Gamer, ki je v angleški, slovenski, švicarski in italijanski različici vsebovala virus Marburg. Hekerji so prišli do spoznanja, da jim za vsako novo programsko opremo ali novo verzijo programske opreme ni treba izdelati novega virusa. Izdelajo le novo verzijo škodljive programske opreme oziroma virusa.

[3]Makri so pravila oziroma vzorci, ki predvidijo, kako je določena vhodna sekvenca porazdeljena v izhodni sekvenci glede na določeno proceduro porazdeljevanja.

[4] Protokol za prenos datotek.

V letu 1999 se je trend nadaljeval. Vseeno bi omenil makrovirus Caligula in internetnega črva Melissa, ki sta bila medijsko razpoznavnejša. Caligula je virus za program MS Office. Njegova značilnost je iskanje zaščitenih datotek in baz podatkov, vzpostavljanje zveze s skritim oddaljenim strežnikom in pošiljanje odtujenih podatkov na ta strežnik. Melissa pa je črv, narejen za program MS Outlook. V programu je črv poiskal imenik in na prvih 50 naslovov razposlal kopije samega sebe. Končni rezultat je bila seveda preobremenitev omrežja (Virus Encyclopedia, 2008).

Kot resno informacijsko in varnostno tveganje so s približevanjem konca stoletja in tisočletja računalniški strokovnjaki omenjali menjavo datuma s 19** na 20**. Starejši informacijski sistemi naj ne bi imeli predvidene te menjave. Domnevali so, da lahko pride do večjih kolapsov informacijskih sistemov, dodatno pa so zgodbo napihnili mediji. Podjetja so porabila veliko denarja za različne simulacije in analize možnih scenarijev, vendar lahko zdaj, ko je minilo že skoraj desetletje, ugotovimo, da je bila skrb mogoče pretirana in medijsko napihnjena.

3.1.3 Informacijske zaščite in rešitve

S pojavom zlonamerne kode, ki je izkoriščala pomanjkljivosti in ranljivosti, se je seveda pojavila potreba po razvoju obrambnih mehanizmov, ki so bili sposobni učinke zlonamerne kode izničiti in odpraviti. Strokovnjaki informacijske tehnologije so se naloge lotili na različne načine.

Večino načinov sem opisal že v zgornjih poglavjih, saj so se zaščite razvijale vzporedno, resda z zamikom, z razvojem zlonamerne kode.

3.1.4 Varnostne politike obdobja pred letom 2000

Pojav varnostnih politik oziroma njihovo izdelavo in implementacijo bom razdelil na tri obdobja. Obdobje pred svetovnim spletom, kot prvo, je bilo obdobje, ko termin varnostna politika še ni bil v uporabi oziroma se ga ni povezovalo z informacijsko tehnologijo. Razlog je predvsem v nizkem odstotku uporabe novih tehnologij. Varnostnih politik, ki bi z navodili, pravili ali primeri najboljše prakse predpisovale načine varovanja informacijskih sistemov, v današnjem pomenu varnostne politike niso potrebovali in tudi ne uporabljali. Varnost je predstavljala predvsem fizična varnost.

V drugem obdobju s pojavom svetovnega spleta je informacijska tehnologija zabeležila skokovito rast informacijskih groženj, nevarnosti ter ranljivosti. Reševanje oziroma obvladovanje varnostnih tveganj je postalo prioriteta, saj je predstavljalo resno nevarnost poslovnim sistemom in s tem poslovanju podjetij. Pojavila se je potreba po izdelavi varnostnih politik informacijskega sistema.

Proces razvoja varnostnih politik informacijskih sistemov je bil dolgotrajen in se še odvija. V preteklosti vodstvo in zaposleni, torej uporabniki, varnostnim politikam niso posvečali

pozornosti. Prevladovalo je mnenje, da varnostne politike poslovanje ovira, saj predpisuje varnostne postopke, ki ovirajo poslovne procese. Danes se uporabniki zavedajo, da so varnostni ukrepi nujno potrebni.

Tretje obdobje pojava varnostne politike bom opisal v nadaljevanju.

3.2 Pregled stanja na informacijskem področju danes

Danes si življenja brez interneta ne znamo predstavljati. Internet je postal vsestransko uporaben, je učinkovito sredstvo za komuniciranje v poslovnem in privatnem okolju. V poslovnem okolju je obvezno komunikacijsko sredstvo postala elektronska pošta, ki že v veliki meri nadomešča papirno poslovanje. Z množično uporabo elektronske pošte so se odprle nove možnosti varnostnih zlorab, zato je treba biti pri njeni uporabi zelo pazljiv. Za podjetje je ključnega pomena, da uporabo elektronske pošte dosledno opredeli v varnostni politiki, kjer naj bodo napisana natančna navodila za uporabo.

Internet je prek spletnih iskalnikov zaradi hitrosti in preprostosti postal zelo priljubljen način iskanja potrebnih informacij. V nekaterih jezikih so za iskanje informacij po internetu prek spletnih iskalnikov celo vpeljali novo besedo, ki večinoma izhaja iz izpeljanke imena spletne strani www.google.com. V nemškem jeziku je to glagol »googeln« (http://www.dict.leo.org/), v angleškem jeziku glagol »to google« (angleško-angleški slovar). Pasovne širine in s tem prenos podatkov so se povečali in postali kakovostnejši, ponudniki spletnih storitev z agresivnim marketingom ustvarjajo vse večjo potrebo po svojih storitvah. Uporabniki uporabljajo internet za prenašanje različne programske opreme, glasbenih in filmskih datotek itd. S tem so vse bolj izpostavljeni tveganjem, povezanim z informacijsko varnostjo.

Vse več finančnih inštitucij (banke, investicijske hiše …) ponuja dostop do svojih storitev prek interneta. Spletno bančništvo doživlja hiter razvoj. Analitično podjetje Forrester Research je v svojem sporočilu iz leta 2003 (marec) navedlo, da je petina Evropejcev uporabljalo spletno bančništvo, predvidevana pa je bila podvojitev števila uporabnikov do konca leta 2007. V naslednjih letih se bo število uporabnikov spletnega bančništva letno povprečno povečevalo za 21 odstotkov.

Svoje usluge oziroma storitve so začeli na internetu ponujati tudi državni uradi. Tako lahko prek interneta državljani pridobivamo različne dokumente, potrdila in podobno (e-uprava). Nekatere države so prek interneta omogočile volitve. Seveda so to večinoma države razvitega sveta. Državne ustanove razpolagajo z zelo občutljivimi podatki, zato informacijski varnosti posvečajo posebno pozornost, vendar je tveganje še vedno prisotno.

Razširjenost interneta so za prodajo svojih izdelkov in storitev izkoristili trgovci in vzpostavili spletne trgovine (angl. *e-Commerce*). Po raziskavah hiše Forrester Research je rast spletne trgovine v letu 2006 znašala 25 odstotkov, podobna pa je bila rast tudi v letu 2007 (23%). Ker se pri internetnem poslovanju uporablja občutljive podatke, je zelo pomembno, da imajo podjetja informacijsko varnost dobro urejeno. Poleg tehnično zagotovljene varnosti morajo

podjetja informacijsko varnost urediti tudi z dokumenti varnostnih politik, kjer so opredeljena varnostna priporočila in navodila za varno uporabo informacijske tehnologije.

3.2.1 Informacijski sistemi, tehnologije in uporabniki

3.2.1.1 Informacijski sistemi

Nikakor ne moremo med obdobjema pred prehodom in po prehodu v novo tisočletje potegniti črte in reči, da se je zgodila hitra in opazna sprememba, vendar pa je razvoj informacijskih tehnologij tako hiter, da že obdobje dveh let pomeni velike razlike. S povečevanjem uporabe informacijskih tehnologij so tudi proizvajalci poskrbeli, da so operacijski sistemi uporabniku prijaznejši, varnejši, funkcionalnejši. Proizvajalci nenehno posodabljajo svoje izdelke z namenom zagotavljanja večje varnosti. Ena bistvenih novosti, ki so jo z razvojem vpeljali v svoje sisteme, je razdelitev vlog uporabnikov v sistemu. Tu mislim predvsem na točno določeno vlogo, kdo je v sistemu administrator in kdo uporabnik. To je danes zelo pomembno, saj so operacijski sistemi nastavljeni tako, da ima administrator vse upravljavske in nadzorstvene pravice nad sistemom, navaden uporabnik pa pravice omejene na svoj uporabniški račun. Administrator lahko torej v operacijskem sistemu upravlja vse funkcije, kar je seveda pravilno, vendar se problem pojavi, ko v operacijski sistem vdre zlonamerna koda oziroma zlonamernež. Če je uporabnik v tistem trenutku v operacijski sistem prijavljen kot administrator, ima vdiralec enake pravice kot administrator. Operacijski sistem lahko samo nadzira, lahko ga poškoduje, odtuji pomembne podatke ali nam na kakršen koli drug način škoduje. Zato je zaradi varnostnih razlogov priporočljivo, da se – ko uporabljamo računalnik in ne potrebujemo administratorskih pravic – v operacijski sistem prijavimo kot uporabnik z omejenimi pravicami delovanja v sistemskem delu operacijskega sistema. Priporočljiva je seveda tudi redna menjava gesla in uporaba kompleksnega gesla. Vsa zgoraj navedena dejstva so zelo pomembni sklopi varnostnih politik in jih varnostni standardi, na podlagi katerih so varnostne politike napisane, zelo natančno opredeljujejo.

Raziskave (Isselhorst, 2007, str. 3) so namreč pokazale, da 60 odstotkov uporabnikov informacijske tehnologije redno uporablja svetovni splet in da ta odstotek narašča. Zaradi tako množične uporabe svetovnega spleta so se tudi grožnje in nevarnosti povečale. Raziskano je, da je 63 odstotkov uporabnikov vsaj enkrat napadel[5] računalniški virus, 35 odstotkov je vsaj enkrat napadel trojanski konj in 10 odstotkov uporabnikov je vsaj enkrat napadel način ribarjenja (angl. *Phishing*). Med uporabniki so razširjeni različni načini, kako se teh najpogostejših napadov ubraniti oziroma kakšni so ukrepi proti napadom. Najbolj razširjeni so različni protivirusni programi, saj jih uporablja kar 90 odstotkov uporabnikov. Veliko manj jih ima nastavljene požarne zidove (angl. *Firewall*), ki so dokaj učinkovita obramba pred večino informacijskih groženj in nevarnosti. Zaskrbljujoč pa je predvsem podatek, da 26 odstotkov uporabnikov ni nikoli izvedlo varnostnega pregleda[6] svojih osebnih računalnikov,

[5] Kot napad je tu mišljen poskus vdora v operacijski sistem uporabnika.
[6] Varnostni pregled je preverjanje učinkovitosti varnostne politike in razlik med zapisano varnostno politiko in dejanskim stanjem. Temelji na urejenem metodičnem pristopu.

zatorej predstavljajo veliko grožnjo za druge »zdrave« računalnike oziroma računalniške sisteme.

3.2.1.2 Informacijska tehnologija

Tako kot se je tipični uporabnik v slabem desetletju razvil in spremenil, se je tudi tehnologija razvila oziroma posodobila. Če tehnologijo primerjamo s predhodnim obdobjem, predstavlja tipično informacijsko tehnologijo v današnjem obdobju zelo zmogljiv osebni računalnik s hitro ADSL-povezavo. Zaslediti je celo že trend menjave običajnega omrežja, opremljenega z navadnim omrežnim kablom, z omrežjem, opremljenim s kabli z optičnimi vlakni. Optična ali steklena vlakna so izredno tanka vlakna nepretrgane dolžine in izredno čistega silicijevega stekla ter posebne plastne indeksne konstrukcije. Cilj optičnih vlaken je prenašanje podatkov na daljše razdalje, pri večjih hitrostih in boljši kakovosti. Optična vlakna prenašajo podatke s pomočjo svetlobe (Velikonja, 2006).

Menim, da se bo razvoj informacijske tehnologije tudi v prihodnosti odvijal s podobnim tempom kot do zdaj. Veliko je namreč še izzivov (naslednji korak je mogoče umetna inteligenca), na katere strokovnjaki še niso našli odgovora. Predvsem pa bo razvoj kratkoročno šel v smeri višje prenosne hitrosti, večjih kapacitet pomnilnikov na fizično manjšem prostoru, enostavnejše uporabe, lažje mobilnosti itd.

3.2.1.3 Uporabniki

Čeprav je med obdobji relativno kratek čas nepopolnih desetih let, se moramo zavedati, da se področje informacijske tehnologije razvija neverjetno hitro. Danes kupljena računalniška oprema je v pol leta zastarela in neuporabna za izvajanje najkompleksnejših računskih operacij, saj razvoju računalniške opreme sledi razvoj programske opreme. Tudi zahteve tipičnega uporabnika se povečujejo z razvojem informacijske tehnologije.

Struktura in nivo uporabnikov sta se v slabih desetih letih opazno spremenila. Danes so tipični uporabniki tako rekoč vsi. Računalniško tehnologijo uporabljajo otroci, najstniki in odrasli. Zelo opazen porast uporabe računalniške tehnologije je med najstniki in otroki. Kar 70 odstotkov najstnikov uporablja računalniško tehnologijo dnevno, veščih uporabe računalniške tehnologije pa je tudi več kot 50 odstotkov otrok. V tej skupini najmlajših se z razvojem pojavlja zanimivo stanje, ki so ga raziskovalci področja informatike opazili in utemeljili. Uporabnike informacijske tehnologije so razdelili na v digitalnem jeziku izvirno govoreče (angl. *Native Speakers of Digital Language*) in digitalne priseljence (angl. *Digital Immigrants*) (Lowendhal, Morello & Daum, 2007, str. 3–19).

V prvo skupino spadajo tisti najstniki in večinoma vsi otroci, za katere je informacijska tehnologija nekaj povesem običajnega, vsakdanjega, normalnega. Lahko bi napisali, da so se z informacijsko tehnologijo rodili. Ta skupina ne pozna obdobja brez digitalnega zapisa podatkov, brez mobilnih telefonov, prenosnih računalnikov itd. So po večini popolnoma vešči uporabe tehničnih pripomočkov in ne razmišljajo o svetu brez digitalnih pripomočkov.

V skupino digitalnih priseljencev spadamo vsi drugi, ki se, nekateri bolj, drugi manj, spominjamo obdobja brez informacijske tehnologije oziroma obdobja, ko je bila informacijska tehnologija domena visokotehnološko razvitih skupin. Vsi smo se morali na nove tehnologije privaditi, se naučiti uporabe in tehnologijo predvsem sprejeti. Ob tem se pojavi sicer zanimiv paradoks, da so digitalni priseljenci informacijske tehnologije razvili in vpeljali v uporabnikov vsakdan in s tem na nek način poskrbeli za formacijo skupine digitalnih izvirnikov (Lowendhal et al., 2007, str. 1–6).

Ob tej razlagi bi rad opozoril, da natančen razvoj prve skupine še ni povsem začrtan, saj je generacija še zelo mlada in po večini še ni delovno operativna. Torej ne moremo povzeti prednosti in slabosti razlik med skupinama, ki sem ju zgoraj opisal, oziroma težko predvidimo, v kakšni meri jim bo to drugačno ali napredno pojmovanje digitalne tehnologije pripomoglo k boljšemu delovanju in večji opravilni uspešnosti.

3.2.2 Informacijske grožnje, nevarnosti in ranljivosti

Glede na predhodno obdobje se grožnje in nevarnosti danes pomensko niso bistveno spremenile. So pa pridobile kompleksnost in pogostost napadov. Posebna tema v novejšem obdobju je ranljivost informacijskih sistemov. Ranljivost informacijskih sistemov se je namreč povečala za 800 odstotkov v primerjavi s prejšnjim obdobjem. Tako veliko povečanje si lahko razlagamo predvsem s povečanjem števila uporabnikov in z dejstvom, da so imele tradicionalne nevarnosti in grožnje, kot na primer virusi, črvi in trojanci, vse manj učinka. Večje število uporabnikov je zlonamerneže pripeljalo do dejstva, da so pričeli izkoriščati naivnosti uporabnikov. Uporabljali so predvsem metode socialnega inženiringa, ribarjenja, zavrnitve storitev oziroma onemogočanje storilnosti (angl. *Denial of Service*[7]), kraje identitete (angl. *Identity Theft*), vdorov prek spletnih strani (angl. *Cross-site-scripting*), napadov vrinjene osebe (angl. *Man-in-the-Middle*) ter nekatere druge (Isselhorst, 2006, str. 6, 7).

Obdobje od začetka stoletja do danes bom zajel v enem odstavku, saj še ne obsega polnih deset let, se je pa v nepolnem desetletju primerilo nekaj zanimivih varnostnih incidentov. Predvsem bi izpostavil virus Ljubezensko pismo (angl. *Love Letter*), ki je dobesedno čez noč okužil milijone računalnikov po svetu, uporabljal pa je podobno metodo kot virus Melissa. Oblasti so filipinskega hekerja, avtorja virusa, izsledile, vendar jim ga ni uspelo obtožiti kriminalnega dejanja, saj na Filipinih hekanje ni prepovedano. Naslednji večji incident je onesposobil spletne strani nekaj svetovno večjih ponudnikov spletne trgovine (eBay, Amazon, Yahoo ...) z uporabo tehnike zavrnitve storitev. Virus Ana Kurnikova je v svojem sporočilu obljubljal ogled slik znane teniške igralke. Ob poskusu ogleda se je virus razposlal na vse v imeniku najdene internetne naslove. Strokovnjake je virus prestrašil predvsem s tem, ker je bil napisan v zelo enostavnem programskem jeziku, takšnem, da so ga lahko uporabili tudi povsem neizkušeni pisci zlonamerne programske kode. Naslednji večji poskus uporabe virusa kot pripomočka za nadaljnji napad se je zgodil z virusom Code Red. Napadalci so želeli

[7] DoS – Zavrnitev storitve (angl. Denial of Service).

pridobiti kar največjo procesorsko moč za izvedbo napada na spletno stran Bele hiše. Ko se je delovna postaja okužila z virusom, so jo napadalci lahko prevzeli in tako oblikovali ogromno skupino delovnih postaj (angl. *Bootnet*), katerih procesorsko moč so nato uporabljali za napad. Napad je bil uspešno preprečen z zaustavitvijo virusa. Ob pojavu je virus Nimda veljal za najkompleksnejše napisani virus, saj je uporabljal do pet različnih metod okužbe ter samorazmnoževanja med delovnimi postajami. Spletni črv Klez je za širjenje uporabljal spletne naslove iz žrtvinega imenika. Na okuženi delovni postaji je brisal dokumente ali datoteke, jih zakrival, se razmnoževal in skrival med dokumente, nadomeščal vsebino dokumentov ali datotek z ničtimi vrednostmi in podobno. Njegova sposobnost širjenja je bila izjemna. Danes na spletu obstaja ogromno črvov, napisanih po njegovem zgledu. V letu 2002 se je zgodil največji napad z zavrnitvijo storitve, katerega načrt je bil prizadeti vseh 13 glavnih (ang. *Root*) strežnikov, ki zagotavljajo komunikacijske mape za celotno spletno strukturo. Zaradi dobre stopnje varnostnih varovalk strežniki niso utrpeli nikakršne škode, kakor tudi uporabniki niso zaznali težav v omrežju. Pojavilo pa se je vprašanje varnosti spleta. Črv Slammer je poznan kot črv, ki se je širil najhitreje. V treh urah se je razširil po celem svetu. Povzročil je tudi ogromno gospodarsko škodo, saj je okužil bančne avtomate, onemogočil strežnike letalskega prometa ... Črv MyDoom je bil eden prvih, ki je za delovanje uporabil socialni inženiring. Pojavil se je v obliki spletne pošte, kot opozorilo uporabniku, da je pošiljanje neke prej poslane pošte spodletelo. Veliko število uporabnikov je temu nasedlo. Vendar pa ta črv ni povzročil velike gospodarske škode.

Zadnji veliki primer zlorabe informacijske tehnologije z metodo kraje identitete so odkrili v avgustu 2008 v ZDA, kjer so odkrili krajo več kot 40 milijonov številk in osebnih gesel računov in kreditnih kartic. Krajo je izpeljala organizirana združba spletnih kriminalcev med letoma 2005 in 2008 in velja za do zdaj največjo izpeljano zlonamerno mednarodno operacijo. Z vdori v računalniške sisteme devetih ameriških trgovcev v lasti podjetja TJX Corporation so namestili zlonamerno programsko opremo, s katero so nato pridobili podatke. Poudariti je treba, da velik del krivde za vdore nosi podjetje samo, saj je brez dovoljenja hranilo nekatere bančne podatke (Reuters, *11 Chardged in TJX Network Security Breach*, 2008)

V spodnji tabeli je prikazanih nekaj najpogostejših razlogov, zakaj se napadalci odločajo za napade.

Tabela 1: Razlogi za napad

Razlog za napad	2005	2006	2007
Želim biti najboljši napadalec	95.870	300.858	197.413
Samo za zabavo	179.234	175.241	95.664
Izziv	59.991	72.287	60.314
Politični razlogi	61.068	77.350	31.073
Patriotizem	53.168	30.207	28.307
Maščevanje	17.847	11.489	10.120
Ni podatka	26.662	84.929	58.014

Vir: Zone-h, 2008.

Pereča težava, ki lahko ob neustreznem ukrepanju hitro preraste v nevarnost, pa je pomanjkanje izobraženega strokovnega kadra s področja varnosti informacijskih sistemov. Vzrokov za pomanjkanje je več. Predvsem nastajajo zaradi neskladnih rešitev ponudnikov varnostnih rešitev, pomanjkanja strokovnjakov in edinstvene prepletenosti strokovnega znanja, ki je potrebno in pomembno za varovanje informacij. Podjetja v preteklosti niso bila pripravljena vlagati v storitev, ki jim posredno ali neposredno ne prinaša nikakršnih dobičkov, hkrati se podjetja nevarnosti niti niso zavedala. Bo pa za podjetja postalo izobraževanje kadrov s področja varovanja informacij čedalje pomembnejše. Vzgojiti usposobljen kader za varovanje informacij je težavna naloga predvsem zaradi nezrelega trga, pomanjkanja standardov in velikega števila ozko usmerjenih rešitev. Hkrati število nevarnosti narašča iz dneva v dan, količina tehnologije, potrebne za nemoteno poslovanje, prav tako. Ustrezno izobrazbo danes se lahko pridobi z opravljanjem vrste različnih certifikatov, od katerih vsak pokriva določen del panoge varovanja informacij (Dolinar, 2003, str. 30).

Naslednjo tabelo pa prilagam za prikaz množičnosti napadov.

Tabela 2: Število napadov po letih

Število napadov	2005	2006	2007
Januar	45.929	43.585	62.092
Februar	47.059	37.061	52.697
Marec	41.175	38.630	54.842
April	48.995	43.007	40.919
Maj	41.735	86.135	41.410
Junij	43.870	51.888	17.797
Julij	41.469	95.461	56.763
Avgust	41.917	130.645	38.362
September	31.853	69.643	29.236
Oktober	40.724	52.421	31.681
November	35.000	50.940	31.925
December	34.114	52.945	23.181
Skupaj	**493.840**	**752.361**	**480.905**

Vir: Zone-h, 2008

3.2.3 Informacijske zaščite in rešitve

Glede na predhodno obdobje, torej pred letom 2000, so informacijske zaščite in rešitve sledile razvoju informacijskih groženj in se razvijale v skladu s potrebami.

Opaziti pa je bilo, da so uporabniki informacijskih tehnologij postali vse pozornejši na svojo lastno varnost. Popolno varnost je sicer skoraj nemogoče zagotoviti, saj z uporabo spletnih povezav v vsakem primeru izpostavimo svoje podatke nevarnostim, ki prežijo na nas. Z uporabo rešitev in nasvetov za povečanje informacijske varnosti pa se lahko veliki večini teh nevarnosti izognemo.

V nadaljevanju odstavka bi rad opozoril le na nekaj najbolj tipičnih in osnovnih informacijskih varnostnih rešitev, ki so v tem tisočletju postale širše poznane in uporabljene, prav tako pa jih zasledimo v večini publikacij z napotki za izdelavo varnostnih politik.

Kot prvo bi izpostavil uporabo požarne pregrade[8], saj predstavlja nekakšno prvo linijo obrambe za naš informacijski sistem. V informatiki požarni zidovi sestavljajo elektronsko varnostno ograjo okoli določenega računalniškega okolja. Požarni zidovi so programska oprema, katere namen je dovoliti, preprečiti ali samo prečistiti in preveriti podatke, ki pridejo po računalniški mreži do računalnika ali računalniškega sistema. Požarni zid je lahko

[8] Besedna zveza požarni zid izhaja iz angleške besede »firewall«. Beseda ima zgodovinski pomen, saj so nekoč hiše gradili tako, da so v steno vgradili zid iz opeke, ki je ob požaru preprečeval širjenje ognja. (http://www.wikipedia.org/)

implementiran kot varnostna naprava ali kot programska oprema na računalnikih. Lahko jih primerjamo s ključavnicami na oknih in vratih, saj vstop dovolijo le pooblaščenim uporabnikom in podatkom, druge pa zadržijo zunaj. Kot večina varnostnih zaščit tudi požarni zidovi žrtvujejo hitrost na račun varnosti. Požarne zidove lahko razdelimo v tri večje kategorije:

1. požarni zidovi, ki filtrirajo pakete;
2. požarni zidovi s tehnologijo inšpekcija izvora (angl. *Stateful Inspection*);
3. požarni zidovi na ravni aplikacij ali strežnikov proxy.

Delovanje požarnih zidov, ki filtrirajo pakete, je omejeno na pregledovanje glave paketov ali informacij o glavi oziroma naslovu paketov, ne spuščajo pa se v pregledovanju celotne vsebine oziroma telesa paketov, saj bi za to potrebovali še več časa. Požarni zidovi, ki pregledujejo podatke s tehnologijo inšpekcije izvora, pregledujejo oziroma nadzorujejo stanje transakcije paketa podatkov. Primerjajo prihajajoče pakete s predhodnimi izhodnimi paketi in tako preverja legitimnost. Požarni zidovi to storijo na podlagi tabele povezav in tako omogočajo dodatno zaščito, ker poleg preprostega filtriranja preverja tudi vsebino podatkovnih paketov in naslove pošiljatelja in prejemnika paketa. Tretja kategorija požarnih zidov, ki delujejo na ravni aplikacij in strežnikov, pa je najvarnejša, saj ti požarni zidovi preberejo in ponovno napišejo vsak posamezni paket. Z vidika varnosti je to zelo pozitivno, saj hekerji težko napišejo neustrezno vsebino v telo paketa. Tu se lahko v primeru slabše tehnologije lahko pojavijo težave s prepustnostjo podatkov, saj je takšno delovanje izredno zamudno (http://www.wikipedia.org/wiki/Firewall, 2008).

Naslednje priporočilo za izboljšanje informacijske varnosti je stalno posodabljanje nameščene programske opreme. Posodabljanje večine programske opreme je trivialno opravilo, saj se oprema večinoma posodablja avtomatično in nekako nismo pozorni na proces posodabljanja. Pogosto nam je celo v napoto, saj nam pomeni odvečno opravilo, ko moramo za posodobitev programske opreme ponovno zagnati svoj računalnik. Ker se programska oprema stalno posodablja, lahko povzroči motnje v pretoku podatkov po mreži. Vendar pa se vsekakor moramo zavedati, da ponudniki programskih oprem ne izdajajo novih verzij računalniških programov le zaradi lepotnih popravkov, ampak prav v največ primerih zaradi varnostnih popravkov ali dodanih funkcij zaščite pred novo zlonamerno kodo ali pred novimi oblikami varnostnih tveganj. Redno posodabljanje programske opreme nam tako lahko prepreči marsikatero preglavico z izgubo ali odtujitvijo podatkov.

Ko tipični uporabnik začne razmišljati o informacijski varnosti, najprej pomisli na protivirusno programsko opremo. V splošnem protivirusna programska oprema uporablja dva načina za zaščito informacijskih sistemov pred zlonamerno kodo: podpise virusov in hevristiko. Podpis virusa je pravzaprav njegova identifikacija, tako kot pri ljudeh. Problem pri podpisu je, da ga moramo poznati vnaprej, če želimo potrditi njegovo istovetnost. Pri podpisih računalniških virusov je to dokaj težko zaradi njihovega hitrega razvoja in dokaj enostavnega menjavanja podpisov. Avtor virusa lahko podpis virusa le malenkostno spremeni, in že ima novo verzijo virusa, ki jo protivirusna programska oprema ne prepozna. Načinu

prepoznavanja zlonamerne kode s podpisom, ki ga moramo poznati vnaprej, pravimo »reaktiven« način prepoznavanja. Zaradi dinamičnosti razvoja zlonamerne kode je protivirusna industrija razvila aktivnejši način prepoznavanja, ki se imenuje »hevristika«. Pri tem načinu prepoznavanja zlonamerne kode gre za razvoj protivirusne programske opreme, ki išče vzorce, ki lahko pomenijo zlonamerno kodo. Seveda je predpogoj za takšno programsko opremo zbirka podatkov o znanih vrstah zlonamerne kode. Hevristična protivirusna programska oprema se od ponudnika do ponudnika zelo razlikuje, saj so uporabljeni različni načini prepoznavanja vzorcev, baze podatkov znane zlonamerne kode med ponudniki in pa možnosti testiranja protivirusne programske opreme so si različne. Žal hevristični način zaenkrat še ni dovolj uspešen in pogosto sproži lažne alarme, kar seveda za uporabnike pomeni določeno motnjo in pa ne nazadnje tudi stroške. Vendar pa se področje razvija in takšna aktivna zaščita z uporabo hevristične metode postaja čedalje učinkovitejša.

Poleg vseh zgornjih pa priporočila za sestavo varnostnih politik priporočajo še uporabo naslednjih varnostnih rešitev. Za povezavo dveh ali več oddaljenih lokacij med seboj, kar največkrat potrebujemo za nemoteno poslovanje, uporabimo varne zasebne povezave oziroma virtualna zasebna omrežja. Pretok podatkov v virtualnem zasebnem omrežju je zaščiten z določenim šifriranjem in tako onemogoča, da bi podatke razpoznale nepooblaščene tretje osebe. Primer virtualnega zasebnega omrežja je povezava pooblaščenega posameznika prek »tunela« oziroma zaščitene povezave na elektronski poštni strežnik domačega podjetja z neke oddaljene lokacije, recimo hotelske sobe. Prav tako so virtualna zasebna omrežja zelo priročna za povezavo oddaljenih lokacij istega podjetja, povezavo podružnic podjetja med seboj in podobno. Za postavitev virtualnih zasebnih omrežij (v nadaljevanju bom uporabljal kratico VPN[9]) potrebujemo na obeh straneh povezave določeno strojno in programsko opremo. Priključitev v takšno omrežje pa običajno poteka večstopenjsko prek domenskih gesel, gesel za oddaljen dostop, različnih identifikacijskih certifikatov in podobno. Ker je takšno dostopanje pogosto zamudno, se na tržišču pojavlja različna strojna oprema, ki omogoča dostop z enkratnim vpisom (angl. *Single Sign On*). Dostop z enkratnim vpisom gesla se sicer lahko omogoči tudi drugače, vendar se tako znižuje nivo varnosti. Vsekakor pa so VPN-omrežja dobrodošla rešitev v primerjavi z najemom posebnih zasebnih linij, ki omogočajo direktno povezavo oddaljenih lokacij, ker je najem takšnih linij navadno zelo drag.

Za učinkovito zagotavljanje informacijske varnosti je priporočljivo uporabiti varni internetni protokol sloj varnih vtičnic (angl. *Secure Sockets Layer*), ki omogoča šifrirano povezavo in komunikacijo med strežnikom in odjemalcem. Komunikacija med strežnikom in odjemalcem poteka tako, da odjemalčev brskalnik pošlje zahtevo po komunikaciji s spletno stranjo z varovanim prenosom SSL[10] oziroma TLS[11]. Strežnik, ki uporablja šifriranje z javnim ključem in digitalnim potrdilom, se predstavi, dokaže, da je res pravi strežnik, in s tem vzpostavi komunikacijo. Odjemalčev brskalnik ustvari ključ za šifriranje s simetričnim ključem, ga

[9] Angl. Virtual Private Network
[10] Angl. Secure Socket Layer
[11] Angl. Transport Layer Security

šifrira s strežnikovim javnim ključem in pošlje strežniku. Strežnik ta šifriran ključ prejme in dekodira s privatnim ključem. Šifriranje od tu naprej poteka le še s simetričnim ključem, kar je bistveno hitrejše in lažje za kontrolo podatkov, saj se kakršno koli spreminjanje podatkov v datotekah zelo lahko in hitro odkrije. Strežnik lahko zahteva tudi identifikacijo odjemalca. Ta to stori z digitalnim certifikatom oziroma potrdilom.

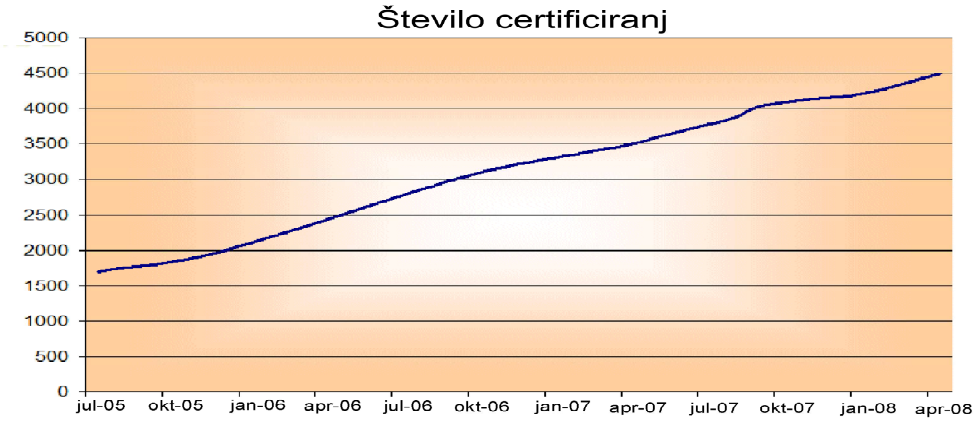
Biometrija je tema, o kateri se v zadnjih letih v svetu pojavlja veliko polemik, ali je to pravi način za varovanje informacij, saj je meja med varovanjem in učinkovitim nadzorom ter posledično krajo identitete tenka. Poleg tega biometrija ni nezmotljiv način, saj je poznan primer uporabe biometrije iz Velike Britanije, kjer je Raymond Easton dokazal, da imata lahko dve osebi enak del DNK-zapisa, za kar je izračunana verjetnost 1 : 37000000 (http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/, 2008).

3.2.4 Varnostne politike po letu 2000

Enako kot pri informacijskih tehnologijah tudi pri spremembi varnostnih politik ni primerno potegniti črte in napisati, da so varnostne politike v novem tisočletju povsem drugačne. Razvoj je sledil in sledi spremembam na informacijskem področju. Torej so se s spreminjanjem obvladovanja varnostnih tveganj oziroma razvojem groženj, nevarnosti in pomanjkljivosti spreminjale tudi varnostne politike.

Bistvene spremembe je zaznati predvsem v številu organizacij in podjetij, ki se za izdelavo in vpeljavo varnostnih politik odločajo. To se dogaja vedno pogosteje, kar je pozitivno. Pri izdelavi varnostnih politik organizacij ali podjetja sledijo predvsem obstoječim varnostnim standardom, ki zelo natančno obravnavajo varnostna poglavja. Za podjetja je priporočljivo, da izdelajo dokument varnostne politike, kjer je informacijska varnost opredeljena širše. Na podlagi tega dokumenta nato izdelajo pravilnike in navodila, kjer področja informacijske varnosti podrobneje obdelajo in opredelijo natančna navodila za varovanje informacij v delovnih procesih. Tako je organizacija varovanja informacij urejena bolj življenjsko in prijaznejše za uporabo. Uporabnikov ne bomo omejevali z nelogičnimi varnostnimi ukrepi, ki bi ovirali delovne procese.

Slika 3: Število certificiranj ISO/IEC 27001



Vir: ISO 27001 security, 2008

Ne smemo se slepiti. Uporabniki s svojim neupoštevanjem predstavljajo največjo pomanjkljivost varnostnih politik. Varnostne politike se običajno vpeljuje naknadno, ko je sistem poslovanja že vzpostavljen. Tako jih uporabniki sprejmejo kot nepotrebno motnjo v utečenem delovnem procesu.

Z varnostno politiko oziroma varnostnimi pravilniki in navodili preprečiti oziroma omejiti posledice socialnega inženiringa, prek katerega v zadnjih letih iz organizacij ali podjetij odteče največ informacij, je izziv, s katerim se strokovnjaki na področju informacijske varnosti trenutno spopadajo. Težava socialnega inženiringa je v tem, da uporabniki, napadeni s socialnim inženiringom, ne vedo, da so bili napadeni. Tako napadalcu nevede odpro pot do podatkov podjetja ali organizacije. Proti socialnemu inženiringu se najučinkoviteje borimo z ozaveščanjem in izobraževanjem uporabnikov.

4 Informacijska varnost v prihodnosti

Po kratkem pregledu preteklih in sedanjih dejstev bi lahko rekli, da nas čaka na informacijskem področju, predvsem pa na področju informacijske varnosti in varnosti informacijskih sistemov zelo burna prihodnost. Predvidevanja seveda že obstajajo. Temeljijo na izkušnjah in vizijah informacijskih strokovnjakov. Napovedati kar koli je težko, kajti to je ekstremno hitro razvijajoča se panoga. Strokovnjaki (Gartner) s področja informacijske varnosti so kot kritično naraščajoče kategorije informacijskih groženj in nevarnosti izpostavili predvsem izkoriščanje ničtega dneva (angl. *Zero-Day Exploits*), trojanske konje, nezaželeno elektronsko pošto (ang. *SPAM*[12]), krajo identitete ter druge.

[12] Nezaželena elektronska pošta.

4.1 Predvidevanja informacijske varnosti

Predvidevati, kako se bo področje informacijske varnosti razvijalo,je zelo nehvaležna naloga. Strokovnjaki s področja informacijske varnosti predvidevajo, da bo do leta 2010 70 odstotkov od 2000 največjih svetovnih podjetij premestilo upravljanje in nadzor nad informacijsko varnostjo iz različnih varnostnih skupin v druge informacijske oddelke.

Informacijska varnost bo torej porazdeljena po različnih vejah informatike in ne bo več centralizirana v eni sami skupini.

Skupine ali oddelki za informacijsko varnost imajo trenutno funkcijo upravljanja in nadzora informacijske varnosti za celotno organizacijo ali podjetje. Njihove funkcije so v veliki meri standardizirane, vendar pa zelo obsežne in s tem zamudne. Prava funkcija skupin ali oddelkov za informacijsko varnost je tako bolj strateško naravnana. Skrbijo za načrtovanje informacijske varnosti, za spremljanje razvoja informacijske varnosti, spremljanje razvoja novih groženj, nevarnosti in ranljivosti in administracijo pa bodo v prihodnosti vse bolj prepuščali drugim oddelkom, predvsem zaradi zamudnosti teh nalog. S tem se bodo znižali stroški informacijske varnosti in povečali se bosta preglednost in učinkovitost. Razlog, da informacijska varnost ni že danes oblikovana na tak način, leži v dejstvu, da podjetja po večini trenutno še nimajo informacijske varnosti oblikovane in razvite do te mere, da bi jo skupine ali oddelki za informacijsko varnost lahko predali rutinskim izvajalcem (Scholtz & Wallin; 2007, str. 2–6).

Aktivnosti, iz katerih sestoji delo skupin ali oddelkov za informacijsko varnost, so po večini sestavljene iz naslednjih nalog (Scholtz & Wallin; 2007, str. 2–6):

- administracija varnostne infrastrukture kot na primer: požarne pregrade, protivirusni programi in sistemi za zaznavanje ali preprečevanje vdorov;
- administracija uporabnikov;
- spremljanje in nadzorovanje varnostne infrastrukture ter iskanje, zaznavanje in odprava kršitev varnostnih politik;
- iskanje, spremljanje in odpravljanje novih groženj, nevarnosti in ranljivosti.

Glede na napovedi strokovnjakov Gartnerja (2007) lahko sklepamo, da informacijski oddelki podjetij že danes razmišljajo o načinih delitve funkcije informacijske varnosti na različna opravila oziroma procese. Decentralizacija informacijske varnosti kot cilj lahko namreč pripelje do zmešnjave pri delovnih procesih. Strokovnjaki za informacijsko varnost so danes namreč mnenja, da za opravljanje vseh funkcij informacijske varnosti ne potrebujejo ljudi s strokovnim znanjem. Ena takih je predvsem administrativni del informacijske varnosti. Težava je tehnična pokritost in spremljanje razvoja informacijske varnosti. Tu je namreč potrebno strokovno osebje z dobrim tehničnim znanjem. Težko je torej določiti procese, kako naj se upravljanje in ravnanje z informacijsko varnostjo preseli oziroma razdeli po oddelkih v podjetju, saj bi za to potrebovali veliko strokovnih sodelavcev. V nasprotnem primeru za

administracijo resnično ne potrebujemo tehničnega strokovnjaka. Rešitev bi bila torej v centralni tehnični podpori informacijski varnosti in po oddelkih ločena administracija (Gartner, 2007).

4.2 Svetovni splet, splet 2.0 in varnost

Leta 1989 je Tim Berners-Lee izumil svetovni splet oziroma WWW[13]. Svetovni splet (v nadaljevanju WWW) je bil izumljen za povezovanje računalnikov med seboj, medtem ko splet 2.0 med seboj povezuje uporabnike. S takšno definicijo se g. Berners-Lee sicer ne strinja v celoti in pravi, da je bil njegov osnovni namen povezati med seboj ljudi. Splet 2.0 je torej nadgradnja WWW in izkorišča tehnologije in standarde, ki so bile razvite že za WWW.

Za uporabnika je oziroma pomeni WWW povezavo s svetom. Na začetku razvoja informacijske tehnologije so nekateri vodilni igralci na tem področju izrazili predvidevanje, da velikost trga informacijske tehnologije v prihodnosti vidijo v obliki petih med seboj povezanih superračunalnikov, ki bodo zadovoljili potrebe vseh uporabnikov. Ob tej izjavi se moramo zavedati, da so bili takrat računalniki fizično nekaj 10-krat večji, kot so danes, vendar to ni pravi pomen te izjave. Trditev sloni na ideji internetnega oblaka. Z razvojem spleta 2.0 bo prišlo do pojava, ko ne bomo potrebovali prednameščene programske opreme na vstopni točki, ampak bomo vse potrebno za delo našli v internetnem oblaku. Od tod bomo jemali vsa sredstva za delo, informacije, tu se bomo povezovali z drugimi obiskovalci oblaka in podobno. Za delo bomo potrebovali le tehnični pripomoček za dostop do internetnega oblaka (Drakos, 2006, str. 2–4). Ideja vsekakor zveni zanimivo, vendar je njena uresničitev v bližnji prihodnosti vprašljiva. Eden od razlogov je tudi zagotovitev ustreznega nivoja varnosti.

Moramo se zavedati, da se vzporedno z razvojem spleta 2.0 razvijajo tudi nove nevarnosti ter odkrivajo nove ranljivosti. Skrb za zadostno varnost informacijskih sistemov bo zato postala še pomembnejša, kot je bila. In seveda bodo, po mojem mnenju, varnostne politike postale še pomembnejše in nujne za implementacijo v poslovni sistem (Mesojedec, 2008, 18 (3), str. 60–63)

4.3 Kibernetični kriminal, kibernetični terorizem in kibernetične vojne

Kibernetični kriminal je razpršena aktivnost in zelo dobičkonosno orientirana. Redko oziroma skoraj nikoli ni strateško načrtovana, temveč zelo kratkoročne narave. Metoda, ki najbolje ponazarja delovanje kibernetičnega kriminala, je metoda udari-beži (angl. *hit and run*). Kibernetičnega kriminala se ne da preprečiti ali iztrebiti, predvidevanja so celo, da se bo pojavljal vse pogosteje, saj so kibernetični kriminalci zelo kreativni in se zelo hitro selijo tja, kjer je denar. Trenutno je ocenjeno, da se svetovni obseg kibernetičnega kriminala giblje med 10 in 40 milijardami ameriških dolarjev. Njegov čar je predvsem v nizkih investicijah in visokem doprinosu izvedenih napadov. Po uspešnosti se kibernetični kriminal loči na dve

[13] WWW – ang. World Wide Web

kategoriji. V prvi so predvsem množični napadi, kot so kraja identitete, manipulacije z delnicami in delniške prevare. Napadi, usmerjeni na točno določeno tarčo, kot so različna izsiljevanja, varovanja spletnih strani v smislu »plačaj, da ne pride do zavrnitve storitve« in storitvenega izsiljevanja. Koliko so vredni posamezni osebni podatki, lepo prikazuje naslednja tabela:

Tabela 3: Vrednost osebnih podatkov na spletu

Vrsta podatka	**Vrednost v $**
Podatki ameriške kreditne kartice z podatki za verifikacijo	1 - 6
Celoten paket osebnih podatkov ameriškega državljana	14 - 16
Aktiven račun za spletno trgovanje	300
Veljavni podatki o elektronskem naslovu	3
Z zlonamerno kodo kontrolirani računalniki - zombiji	6 - 20 na PC
Strani za "ribarjenje"	3 - 5 na stran
Preverjen račun za spletno plačevanje - PayPal	50 - 500
Nepreverjen račun za spletno plačevanje - PayPal	10 - 50
Skype uporabniški račun	12

Vir: Marcus Ranum, Tenable Security, Symantec, 2008

Predvidevanja prihodnosti kibernetičnega kriminala vključujejo »razvoj« in povečanje različnih vrst izsiljevanj. Do zdaj so tatovi razmišljali, kako »milijon ljudem speljati po 1 evro«, v prihodnosti pa naj bi se spremenilo, kako »eni osebi speljati milijon evrov«. Kriminal tako je in bo ostal problem.

Cilji kibernetičnega terorizma so bolj globalni. Ideja kibernetičnih teroristov je povzročiti veliko škode z javnimi napadi in hkrati zasejati strah med ljudi in ne samo povzročiti materialno škodo. Tarče kibernetičnega terorizma so običajno sistemi civilne infrastrukture, napadi pa pomenijo veliko škode, uničenje in tudi smrt. Najbolj so torej ogrožena javna podjetja, ki upravljajo infrastrukturo kot na primer: vodovod, plinovod, naftovod, električne napeljave, ceste, železnice in podobno.

Zanimivo pa je, da se kibernetični terorizem pojavlja v obliki kibernetičnega nadlegovanja, torej brez velikih in uničujočih posledic. Prav tako je težko verjeti, da bi lahko kibernetični terorizem v prihodnosti postal tako učinkovit (uničujoč) in »cenovno učinkovit« (za izvajalce seveda), kot je to stvarni terorizem. Mogoče le v primeru, da postanejo kibernetični teroristi bolj sofisticirani, kot so v tem trenutku. Do zdaj še ni poznan primer uničujočega kibernetičnega napada z resnimi posledicami. Pravi teroristični napadi imajo veliko večjo odmevnost. Edini primer, da je teroristom z napadom uspelo nekaj spremeniti, je iz novejše zgodovine – Španija, Madrid 2004. Teroristični napad je sprožil zamenjavo vlade in umik španskih vojakov iz Iraka.

Zakaj kibernetičnega terorizma ne uporablja več teroristov, obstaja več teorij, prevladuje pa mnenje, da kibernetični teroristi niso dovolj dobro izurjeni in da imajo pravi teroristični napadi veliko večji učinek. V prihodnosti lahko pričakujemo, da se bo stopnja kibernetičnega terorizma povečala, vendar le na nivoju nadlegovanja in ne na nivojih resnega uničevanja.

Pojem kibernetične vojne zveni zelo znanstvenofantastično. Zelo težko predstavljivo je namreč, da bi vojne potekale le v kibernetičnem prostoru. Tam bi se lahko le začele, nadaljevale pa s konvencionalnim spopadom. Velika težava kibernetičnih vojn je predvsem v organizaciji. Vzemimo primer, ko bi neka država ali skupina pripravljala kibernetični napad na nekoga drugega kot začetek vojne. Pripravi se tehnologijo, določi se časovne okvire, ko pa pride do odločitev za začetek, se pojavi problem: »Napada ne moremo izvesti, ker je žrtev včeraj posodobila svojo strojno in programsko opremo. Naše orodje/orožje ni učinkovito proti tem posodobitvam.« Sliši se nekoliko komično, vendar je povsem realno.

V prihodnosti ne moremo pričakovati, da se bodo kibernetične vojne v pravem pomenu pojma dejansko zgodile, lahko pa pričakujemo, da bo informacijska tehnologija imela vedno večjo vlogo v kakršnih koli bojevanjih, pa čeprav še tako nesmiselnih (Ranum, 2008).

4.4 Tehnične rešitve varnosti informacijskega sistema in proizvajalci

V tem poglavju bi želel na kratko predstaviti sodobne tehnične rešitve varnosti informacijskih sistemov, hkrati pa podati še analizo primerjave med proizvajalci in njihovimi produkti, ki sem jo zasledil na spletu in je po mojem mnenju dovolj objektivna, da se jo predstavi.

Moj namen ni ocenjevati različne proizvajalce in njihove produkte, pač pa podati primerjavo med proizvodi in okvirno oceniti, kaj je pri izbiri nekega produkta za varovanje informacij in informacijskih sistemov pomembno.

Sistemi varovanja informacij in informacijskih sistemov so sestavljeni iz več komponent, povezanih v celoto. Različni proizvajalci ponujajo različne rešitve. Težko trdimo, da lahko v produktu enega proizvajalca dobimo združene vse potrebne komponente, obstajajo pa dobri približki, vse pa je odvisno od naših potreb, želja in sestave našega sistema ali omrežja. V tabeli, ki sem jo zasledil na spletu in je produkt dela spletne publikacije NetworkWorld in avtorja Joela Snyderja, je predstavljenih nekaj največjih in najboljših svetovnih proizvajalcev

informacijske tehnologije za varnost informacij in informacijskih sistemov. Proizvodi so razvrščeni glede na skupno oceno več kriterijev. Prav ti kriteriji se s spreminjanjem informacijske tehnologije zelo spreminjajo, saj je potrebno na nove nevarnosti in grožnje poiskati nov odgovor oziroma rešitev in s tem seveda običajno nov način oziroma metodo za reševanje nevarnosti in odpravljanje groženj. Trenutno je na lestvici pomembnosti med lastnostmi nekega proizvoda za varovanje informacij najvišje orodje oziroma način, kako napravo oziroma proizvod upravljati. Upravljanje je zelo pomembno, saj nam lahko zmanjša stroške, pripomore k hitrejši reakciji in zagotovi višjo stopnjo varnosti. Upravljanju sledi skupina kriterijev z enako stopnjo pomembnosti. Zmogljivost, sistemi za preprečevanje vdorov in lastnosti virtualnih zasebnih omrežij so po mnenju avtorja po pomembnosti na drugem mestu. Sledijo še druge kategorije, za katere avtor meni, da so manj pomembne. Zanimivo pa je, da v proizvode nameščena protivirusna programska oprema ne vpliva na oceno varnostnih proizvodov.

Tabela 4: Primerjava največjih svetovnih proizvajalcev produktov za varovanje IS

Kategorija	Utež	Juniper ISG-1000	Juniper SSG-520M	IBM System x3650	Nokia IP290	Crossbeam C25	CheckPoint UTM-1 2050	Cisco ASA5540	Secure Computing Sidewinder 2150D	Fortinet FortiGate 3600A
Upravljanje	20%	4,25	4,25	3,75	3,75	3,75	3,75	4	3,25	3
Zmogljivost	15%	4,5	3,5	4,5	3	3	3	3,25	4,5	4
Sistem za preprečevanje vdorov	15%	4,5	1,5	3,25	3,25	3,25	3,25	2,75	2,5	1
Virtualne zasebne mreže	15%	4	4	4,7	4,7	4,7	4,7	4,5	3	3,3
Visoka razpoložljivost	10%	5	5	5	4	5	5	3	3	3
Struktura opreme	10%	4,5	4,75	5	4,5	5	4	4,5	5	5
Podpora pri nameščanju	5%	5	5	3	5	3	3	4	4	4
Podpora IPv6	5%	3,5	3,5	3,5	4	3,5	3,5	3	2	3
Poraba energije	5%	4	4	1	5	3	4	4	2	3,5
Protivirusna programska oprema	0%	NP	3,8	NP	3,1	3	3	NP	3,6	3,9
Skupaj	**100%**	**4,38**	**3,8**	**3,99**	**3,94**	**3,87**	**3,82**	**3,68**	**3,35**	**3,17**

K tabeli pripada naslednja legenda:

- NP – ni podatka
- Ocene so od 5 (najboljša) do 1 (najslabša)

***Vir: NetworkWorld, 2008*.**

5 Študija primera: Podjetje Elektro Slovenije, d. o. o., in stanje informacijske varnosti

Za študijo primera sem izbral podjetje Eles,[14] d. o. o., kjer sem dobil priložnost sodelovati na projektu prenove varnosti informacijskega sistema. Tako sem se seznanil z izivi s področja informacijske varnosti, s katerimi se podjetje srečuje pri vsakdanjem poslovanju. Za Eles je zaradi strateškega pomena, ki ga ima za Slovenijo, informacijska varnost zelo pomembna. Spoznal sem, kako kompleksen je proces vpeljave varnostne politike v tako velik in razvejan sistem, kot je podjetje Eles d. o. o.

Eles je edino elektroenergetsko prenosno podjetje v državi. S svojim prenosnim omrežjem, ki na 400-, 220- in 110-kV napetostnem nivoju obsega 141 daljnovodov v skupni dolžini 2.600 kilometrov, 20 razdelilno-transformatorskih postaj s 33 energetskimi transformatorji skupne moči 3.951 MVA, 252 odklopnikov, 814 ločilnikov, 1.428 merilnih transformatorjev, 565 prenapetostnih odvodnikov in vrsto drugih visokonapetostnih naprav, povezuje proizvajalce in odjemalce električne energije in zagotavlja nemoteno obratovanje slovenskega elektroenergetskega sistema. Po določilih energetskega zakona je Eles javno podjetje v 100-odstotni državni lasti, ki so mu zaupane naloge prenosa električne energije in upravljanja prenosnega omrežja. S hčerinskimi družbami Eles skrbi tudi za organiziranje trga z električno energijo in izvajanje izobraževalnih programov. V letu 2008 je imelo podjetje Eles nad 500 zaposlenih (Internetna dokumentacija Elesa).

5.1 Poslanstvo in vizija

Temeljno poslanstvo podjetja je, da s skrbnim razvojem, gradnjo in vzdrževanjem prenosnega omrežja, zagotavljanjem sistemskih storitev ter varnim in zanesljivim obratovanjem zagotovi vsem dobaviteljem in odjemalcem kakovosten in nepristranski prenos električne energije.

Vizija podjetja je organizirati in usposobiti Eles v sistem, ki bo energetska hrbtenica Slovenije in popolnoma kos izzivom, ki jih prinašajo tržne zakonitosti in konkurenčno okolje združene Evrope (Internetna dokumentacija Elesa).

5.2 Dejavnosti družbe

Eles je v skladu z energetsko zakonodajo pristojen tako za upravljanje kot za razvoj in vzdrževanje prenosnega omrežja, ki je del elektroenergetskega sistema. EES sestavljajo poleg prenosnega omrežja še omrežja neposrednih odjemalcev, distribucijska omrežja ter porabniki in proizvajalci. Tako je prenosno omrežje vezni člen med proizvodnjo in odjemom ter povezava z drugimi energetskimi sistemi v Evropi. Za doseganje varnega obratovanja povezanega EES UCTE morajo posamezna prenosna omrežja dosegati visoke standarde kakovosti. Eles mora svoje naloge izvajati tako, da dosega standarde, ki se nanašajo predvsem

[14] Elektro Slovenije

na varnost in zanesljivost obratovanja, pa tudi na tolerančni pas nekaterih obratovalnih spremenljivk. Za doseganje varnega obratovanja povezanega evropskega EES mora Eles zagotavljati s sporazumi dogovorjene standarde zanesljivosti in zadostnosti obratovanja. To dosega z obvladovanjem mehanizmov za obvladovanje pretokov energije znotraj Slovenije in prek njenih meja ter zanesljivim obratovanjem, ki ga dosegamo z učinkovitim vzdrževanjem in pravočasnim investiranjem v nove objekte.

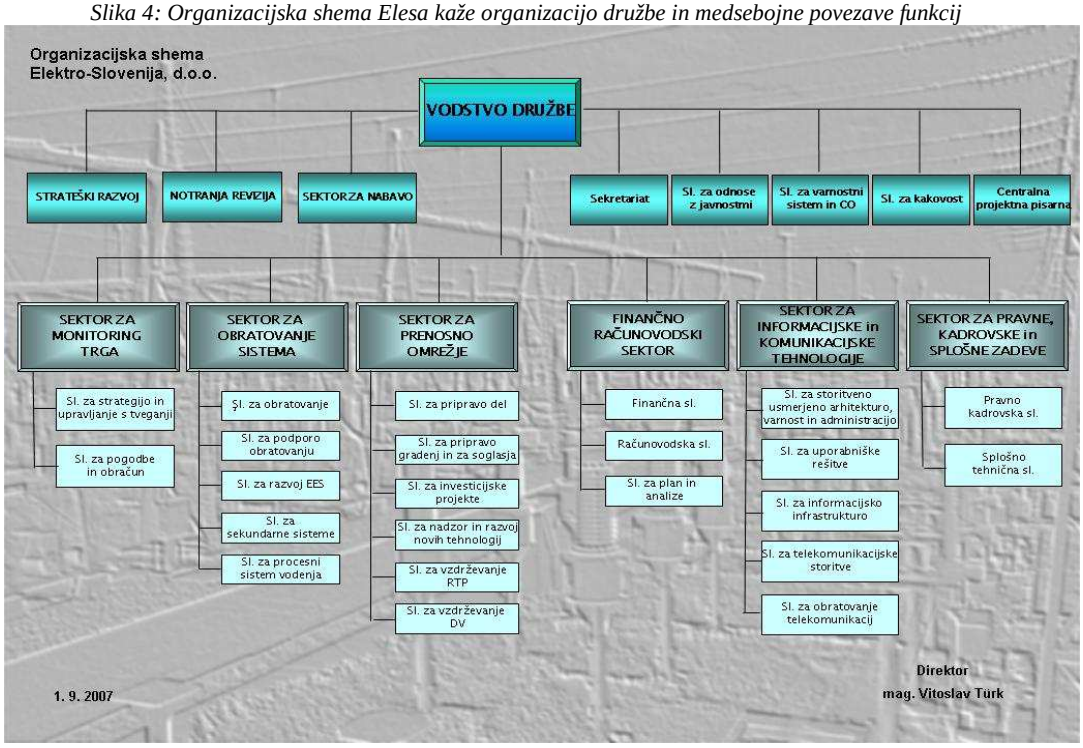
Eles je član v evropskih združenjih (UCTE, ETSO), kjer dejavno sodeluje pri pripravi pravil in mehanizmov za čezmejno trgovanje z električno energijo ter varno in zanesljivo obratovanje prenosnega omrežja. Dogovorjena pravila in mehanizme vnaša v domače podzakonske akte in skrbi za njihovo izvajanje.

Eles s svojimi odvisnimi družbami dopolnjuje temeljni poslovni program, s tem da dobaviteljem in odjemalcem električne energije omogoča trgovanje na borzi ter ponuja kakovostne storitve s področja trgovanja z električno energijo, zagotavlja prodajo telekomunikacijskih storitev in funkcionalno izobraževanje zaposlenih v vseh slovenskih elektroenergetskih podjetjih.

5.3 Organiziranost družbe

Delovanje in vodenje Elesa je organizirano v trinivojski organizacijski strukturi, ki poleg vodstva zajema še šest sektorjev.

Slika 4: Organizacijska shema Elesa kaže organizacijo družbe in medsebojne povezave funkcij



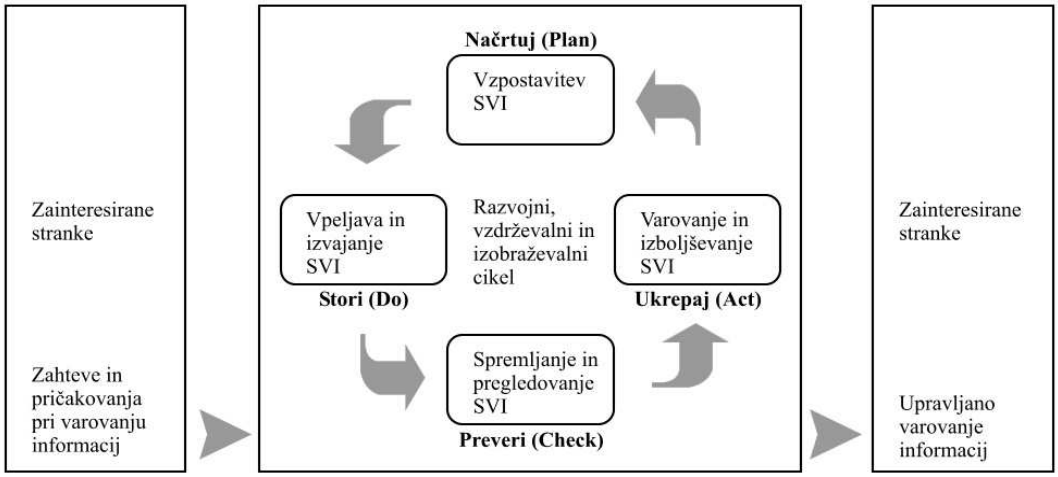
Vir: Interna dokumentacija ELES

5.4 Varovanje informacij in informacijskih sistemov na Elesu

Varovanje informacij je pomemben element poslovanja podjetja. V Elesu vzpostavljajo in vpeljujejo ter v delu, kjer je sistem vpeljan, tudi izvajajo, spremljajo, pregledujejo, vzdržujejo in izboljšujejo dokumentiran sistem varovanja informacij. Sistem razvijajo v vseh poslovnih dejavnostih organizacije in za celoten nabor tveganj, ki jo ogrožajo. Vsebinsko sistem varovanja informacij temelji na modelu PDCA, ki je prikazan na sliki 5. Sistem varovanja informacij obsegajo:

- telesa sistema varovanja informacij, ki so nosilci uvajanja, spremljanja in izboljševanja sistema. To so sveti za sisteme upravljanja, tim za varovanje informacij, služba za civilno obrambo in varnostni sistem ter posamezne odgovorne osebe;
- dokumentacija sistemov varovanja informacij in vodenja kakovosti.

Slika 5: Model PDCA



Vir: Interna dokumentacija ELES

5.5 Nadaljnji razvoj informacijske varnosti na Elesu

Za podjetje oziroma organizacijo, kot je Eles, d. o. o., je nadaljnji razvoj informacijske varnosti zelo pomemben. Zaradi njegovega strateškega pomena za Slovenija in Evropsko unijo je naloga podjetja, da vzpostavi visok nivo informacijske varnosti.

Eles skrbno spremlja trende na področju informacijske varnosti. Za redno spremljanje, sledenje in prilagajanje varnosti informacijskih sistemov na novosti, ki se pojavijo na tržišču, znotraj podjetja skrbi delovna skupina, sestavljena iz zaposlenih iz različnih sektorjev podjetja. Po potrebi za pomoč pri izvajanju zahtevnejših operacij varovanja informacijskega sistema in varovanja informacij pogodbeno najamejo zunanje strokovnjake s področja, s primernim znanjem in referencami.

Odkrivanje in odpravljanje informacijskih tveganj poteka v okviru delovne skupine sistematično. V ta namen je izdelan seznam informacijskih tveganj, na podlagi katerega je

pripravljen plan njihovega odpravljanja. Odprave tveganj trenutno izvajajo v poslovnem omrežju, kjer so kot tveganja identificirana kraja poslovnih podatkov, uničenje poslovnih podatkov in onemogočen dostop do poslovnih podatkov. Urejena je bila politika gesel, s čimer se je zmanjšala možnost vdora v informacijski sistem, kar bi lahko pripeljalo do uresničitve enega od identificiranih informacijskih tveganj. Uvedeno je bilo obvezno samodejno nameščanje popravkov in posodobitev programske opreme, s čimer se je povečala informacijska varnost in prav tako zmanjšalo tveganje vdorov. Proces odpravljanja informacijskih tveganj podjetje obravnava kot živ in gibljiv proces, ki se nenehno pregleduje, izvaja in obnavlja. S tem je zagotovljeno učinkovito obvladovanje informacijskih tveganj.

V bližnji prihodnosti Eles pripravlja prenovo varnosti informacijskega sistema, s čimer bo zagotovil varovanje z najnovejšimi tehnologijami in koncepti. Prednost novega sistema bo centralno upravljanje in nadzor nad informacijsko varnostjo, kar bo delo zaposlenih ki se ukvarjajo z varnostjo bistveno olajšalo, hkrati pa močno povečalo nivo varnosti informacijskega sistema.

Sklep

Ko sem se diplomske naloge lotil, sem varnost informacijskih sistemov dojemal kot pomembno panogo, s katero so uporabniki dovolj dobro seznanjeni, da sistemi delujejo. V predelani literaturi, prebranih člankih, novicah in podobni dokumentaciji sem zasledil, da to ni vedno tako.

Večje organizacije in podjetja posvečajo varnosti informacijskih sistemov zaradi občutljivosti svojega poslovanja bistveno več pozornosti, kot pa to počno zasebni uporabniki. Iz pridobljenih informacij lahko ugotovim, da samo množičnost in pa sreča pogojujeta izmikanju nevšečnim situacijam. Mnogokrat uporabniki uidejo spletnemu kriminalu samo zaradi nesposobnosti hekerjev.

Kot ugotovitev v svoji diplomski nalogi bi rad izpostavil, da sta shema in kompleksnost varnostnih politik skozi čas, torej z razvojem groženj, nevarnosti in ranljivosti, bistveno napredovali, vendar pa se odzivata z zamikom, torej kot posledica oziroma odgovor na nove oblike zlonamernih dejanj. Prav tako bi kot ugotovitev izpostavil, da je varnostna politika eden od instrumentov za reševanje varnosti informacijskega sistema, ki ga uporabljajo predvsem podjetja z večjimi poslovnimi sistemi.

Kot rak in rana varnostnih politik se skozi vso zgodovino pojavljajo predvsem uporabniki, torej neživljenjskost varnostnih politik. To bi lahko utemeljil kot dejstvo, da so varnostne politike mnogokrat napisane tako, da jih je v praksi zaradi oviranja poslovnih procesov neživljenjsko dosledno upoštevati, predvsem pa jih uporabniki niso pripravljeni dosledno upoštevati, kar seveda pripelje do varnostnih incidentov.

Dejstvo je, da organizacije in podjetja varnostne politike urejajo prek vpeljevanja različnih standardov, in nemalokrat se pripeti, da varnostne politike sestavljajo ljudje, ki z dejanskim

procesom delovanja niso dovolj dobro seznanjeni, kar lahko pripelje do omenjenih situacij. Ker pa so varnostne politike kompleksni dokumenti, ki jih je treba izdelati tako, da se prilagajajo vsem procesom, lahko takšne nesrečne položaje razumemo. Težko pa oporekamo dejstvu, da so standardi najprimernejši način izdelave varnostne politike za večje, kompleksnejše sisteme, saj karseda dobro pokrivajo najširši spekter delovanja organizacij ali podjetij.

Kot temeljno ugotovitev pa bom izpostavil razmišljanje, da je treba varnostne politike vzpostaviti tako, da bodo služile hkrati organizaciji ali podjetju in uporabnikom. Glede na možnost spremljanja izdelave varnostnih politik v podjetju ELES, d. o. o., bi kot primerno rešitev izpostavil izdelavo varnostnih politik v dveh fazah, in sicer kot organizacijski predpis, ki obravnava varnost informacijskih sistemov širše, ter nato v obliki priprave navodil, ki opredeljujejo varovanje v ožjem smislu, torej bolj prilagojeno dejanskim delovnim procesom podjetja.

V zaključku bi rad poudaril, da so varnostne politike potrebne v vsaki organizaciji, podjetju, skupnosti kakor tudi zasebno, saj se stopnja spletnega kriminala povečuje iz dneva v dan.

Literatura in viri

1. Abrams, C. (2006). *Seven Ways Your Organization Can Benefit from Web 2.0*. b.k. Gartner.
2. Byrnes, F. Christian (2006a). *The Top Five Issues of Chief Information Security Officers*. b.k. Gartner.
3. Byrnes, F. Christian (2006b). *Information Security Plan Development*. b.k. Gartner.
4. Byrnes, F. Christian, Noakes-Fry, K. & Nicolett, M. (2006). *Risk Assessment Approaches for IT Security Risk Management*. b.k.Gartner.
5. Caldwell, F. & Mogull, R. (2006). *Risk Management and Business Performance Are Compatible*. b.k. Gartner.
6. Dolinar, P. (2003). *Varnost pri poslovanju*. Štirinajsta delavnica o telekomunikacijah VITEL. Brdo pri Kranju.
7. Di Maio, A. (2007). *Web 2.0 in Government: Blessing or Curse?* b.k.Gartner.
8. Drakos, N. (2006): *Will Web 2.0 Finally Brake Your Enterprise Applications?*.b.k. Gartner
9. Egan, M. & Mather, T (2001). *Varovanje informacij – grožnje, izzivi in rešitve*. Založba Pasadena, d.o.o.
10. Feiman, J. & Pescatore, J. (2008). The Creative and Insecure World of Web 2.0. b.k. Gartner.
11. Gradišar, M. & Resinovič, G. (2001). *Informatika v poslovnem okolju*. Ljubljana: Ekonomska fakulteta.
12. Horjak, M.(b.l.). Vpliv varne informacijske tehnologije na ekonomsko uspešnost podjetja. MFC&L d.o.o., Ljubljana. Najdeno dne 15.3.2008 na spletnem naslovu http://www.mfc-2.si/pdf/vpliv_varne_informacijske_tehnologije_na_ekonomsko_uspesnost_podjetja.pdf
13. Hudomalj, E. (b.l.). *Varnost informacij*. Medicinska fakulteta, 2006/2007. Najdeno dne 15.3.2008 na spletnem naslovu http://www.mf.uni-lj.si/~jure/pred_bib/prosojnice/rk/Varnost200607.pdf
14. http://www.altavista.org/, 2008
15. http://www.google.com/, 2008
16. http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/biometrija/.2008
17. http://www.palsit.si/. 2008
18. http://www.securityfocus.com/. 2008
19. http://www.varnostne-novice.com/. 2008
20. http://www.wikipedia.org/. 2008
21. http://www.zone-h.org/, 2008
22. Interna dokumentacija podjetja ELES, d.o.o.
23. ISO 27001 Security. (2008) Najdeno dne 20.6.2008 na spletnem naslovu http://www.iso27001security.com/html/27001.html

24. Lopez, J. et al. (2006). Gartner's Top Predictions for Industry Leaders, 2007 and Beyond. b.k. Gartner.
25. MacDonald, N. & Feiman, J. (2007). Market Definition and Vendor Selection Criteria for Source Code Security Testing Tools. b.k. Gatrner.
26. Mesojedec, U. (2008): *Retrospektiva prvih pet let spleta 2.0*. Revija Monitor, marec, letnik 18, številka 3, str. 60-63
27. Nicolett, M., Proctor, Paul E. & Williams, Amrit T. (2006). *Use Vulnerability Management for Controls and Compilance*. b.k. Gartner.
28. Pescatore, J. & Feiman, J. (2008). *Security Features Sholud Be Built Into Web 2.0 Applications*. b.k. Gartner.
29. Poznič, T. (b.l.). *Informacijska varnost in digitalna forenzika*. Viris d.o.o. Maribor. 2006. Najdeno dne 15.3.2008 na spletnem naslovu http://www.tovarnapodjemov.org/docDir/zazeni%20idejo_informacijska%20varnost%20in%20digitalna%20forenzika.pdf
30. Proctor, Paul E. (2007). *The Top 10 Risk and Security Audit Findings to Avoid*. b.k. Gartner.
31. Proctor, Paul E. et al. (2007). *Key Issues for Security and Risk Management Role Research*, 2007. b.k. Gartner.
32. Ranum, Marcus J. (2008). *Cyberwar, Cyberterror, Cyberbrime*. IDC IT Roadshow 2008. Hotel Mons
33. Scholtz, T. & Wallin, Leif-Olof (2007). *Security Operations Change as Programs Mature*. b.k. Gartner.
34. Slovar. Najden na spletnem mestu http://dict.leo.org/. 2008
35. Slovar informacijskih izrazov. Najden na spletnem mestu http://www.islovar.org. 2008
36. Spletni forum: Ravbarji in žandarji. Najden na spletnem mestu http://rz.hicsalta.si/?cat=6. 2008
37. Symantec. Najdeno 15.5.2008 na spletnem naslovu http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/SHHOS_Mar07_NL_Final.pdf
38. Štrakl, M. (2003). *Varnost politika informacijskega sistema*. Štirinajsta delavnica o telekomunikacijah VITEL. Brdo pri Kranju.
39. Tracy, L. e tal. (2007). *IT Key Metrics Data 2008: Frequently Asked Questions*. b.k. Gartner.
40. Velikonja, A. (2006). *Optična vlakna*. Najdeno na spletnem naslovu dne 3.7.2008 http://www.publikacije.net/.
41. Virus Encyclopedia. Najden na spletnem naslovu http://www.viruslist.com/en/viruses/encyclopedia. 2008
42. Wagner, R. et al.(2006). *Predicts 2007: Secure Business Enablement Essential to Information Security*. b.k. Gartner.
43. Wagner, R. (2006). *Secure Business Enablement Essential to Information Security*. b.k. Gartner.
44. Washingtonpost. Najden dne 20.6.2008 na spletnem naslovu http://www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html.

45. Welsch, G. et al. (2008). *Ein Nationales IT – Frühwarnsystem für Deutschland*, Positionspapier der ITK-Wirtschaft. Najdeno na spletnem naslovu www.enisa.europa.eu/pages/05_02.htm#5
46. Young, G. e tal. (2007). *Hype Cycle for Information Security, 2007*. b.k. Gartner.
47. Zupan, L. (b.l.): *Slovenija Skozi prizmo informacijske varnosti*. Najdeno na spletnem naslovu dne 20.4.2008 http://www.ipmit.si/IPMITstrani/ipmitslo.nsf/V/KD4BDF479B5D38FDFC1256ED90054909B/$file/Slovenija%20skozi%20prizmo%20informacijske%20varnosti.pdf.

Izbrisano: PRILOGA

Priloga

Slovar tujih izrazov

Tuji izraz	Slovenska razlaga
Intrusion Detection System (IDS)	Sistem za zaznavanje vdorov
Intrusion Prevention System (IPS)	Sistem za preprečevanje vdorov
Denial of Service (DoS)	Zavrnitev storitve
Virtual Private Network (VPN)	Virtualna zasebna omrežja
Single Sign-On	Dostop z enkratnim vpisom gesla
Phishing	Ribarjenje
Cross-site-scripting	Vdor preko spletne strani
Man-In-the-Middle	Vdor vrinjene osebe
Identity Theft	Kraja identitete
Bootnet	Skupina računalnikov pod tujim nadzorom
High Availability (HA)	Visoka razpoložljivost
World Wide Web (WWW)	Svetovni splet
Confidentiality, Integrity & Avaliability (CIA)	Zaupnost, integriteta in razpoložljivost
International Standard Organization (ISO)	Mednarodna standardna organizacija
Disaster recovery	Ponovna vzpostavitev
World Health Organization (WHO)	Svetovna zdravstvena organizacija
Native Speakers of Digital Language	Digitalno izvirno govoreči
Digital Immigrants	Digitalni priseljenci
Secure Socket Layer (SSL)	Sloj varnih vtičnic
Transport Layer Security (TLS)	Transportni nivo varnosti