UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

DIPLOMSKO DELO

VEČDIMENZIONALNOST PROBLEMA VARNOSTI PODATKOV IN PRISTOPI REŠEVANJA

Ljubljana, september 2004 ANDREJ KALIGARIČ

IZJAVA

Študent Andrej Kaligarič izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom prof.dr. Borke Jerman Blažič in dovoljujem objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____ Podpis:_____

Kazalo

1. Uvod

"Zatorej, kar omogoča modremu poveljniku da napade in osvaja, da dosega stvari preko dosega običajnih ljudi – je vnaprejšnje poznavanje."

"Napadi ga, kjer ni pripravljen, pojavi se, kjer se te ne pričakuje."

"Te vojaške stvari, ki vodijo do zmage, ne smejo biti predhodno razkrite."

Sun Tsu – Umetnost vojskovanja, približno 490 pr.n.št.
... oziroma nekaj misli, povezanih s pomenom zaupnosti, razpoložljivosti, celovitosti podatkov in informacij ...

Pričujoče diplomsko delo predstavlja poskus orisa problematike varnosti podatkov in informacij (tj. zagotavljanja zaupnosti, celovitosti in razpoložljivosti le-teh) - v besedilu pa je ponujenih in vsaj grobo očrtanih tudi nekaj možnih vidikov in poti njenega razreševanja.

Varnost informacij je zapleten problem. Njegove tehnične, psihološke, sociološke, pravne ter ekonomske razšeznosti se prepletajo v gosto povezano in včasih slabo pregledno in težko razumljivo celoto. V tem delu se ne bom poglabljal v posamezne vidike tega področja. Tukaj ne bo podrobnejše količinske ali kakovostne analize o tej tematiki. Prav tako do delo nima pretenzij predstavljati se kot celovita slika obravnavane realnosti. Namen tega besedila je zgolj obravnava problematike varnosti podatkov in informacij z vidika enega samega cilja, to je poskusa opredelitve nekaj izmed najbolj merodajnih obrisov predmeta obravnave.

Varovanje podatkov in informacij pa v sodobnem svetu zavzema čedalje bolj kritično vlogo. Govorim namreč o stvarnosti globalizacije, prehoda gospodarsko razvitejših držav iz faze industrijske v postindustrijsko družbo – v družbo, temelječo na znanju posameznikov in sposobnostjo deljenja tega znanja med njimi v namen doseganja skupnih in posebnih ciljev. V družbo, kjer so edina stalnica pravzaprav spremembe, kjer sta vsaj navidez antitetični potezi hitrosti in točnosti pogosto odločilna dejavnika. V družbo, kjer normalno odvijanje običajnega življenjskega ritma čedalje bolj sloni na informacijsko-telekomunikacijski tehnologiji in brez nje pravzaprav sploh ni več mogoče. In vendar je tehnologija samo sredstvo za doseganje postavljenih ciljev; točneje – zgolj eno znotraj spleta potrebnih sredstev. Kot bo v nadaljevanju prikazano, so prav maloprej omenjeni in pogosto zanemarjeni "mehkejši" vidiki – psihološka, sociološka plat osrednjega pomena; svojo ključnost dajo slutiti že po površnem, bežnem pregledu organizacijski, ekonomski, pravni, politični dejavniki. Prepričan sem, da je v namen doseganja postavljenih ciljev neizogibna uporaba uravnoteženega spleta različnih in raznolikih prijemov, tj. vplivanja na različna, komplementarna področja stvarnosti.

Potrebno pa je imeti v mislih, da je ni "srebrne krogle", ki bi nas hitro in zlahka otela vseh težav. Na to je mogoče gledati kot na neko splošno načelo pri zapletenih problemih z mnogimi, raznolikimi potezami. Področje varnosti podatkov in informacij pa gotovo ima take značilnosti.

V nadaljevanju se bom lotil predstavitve pomena informacij samih in njihove varnosti. Nadaljeval bom s pogledov na stanje okoli varnosti podatkov in informacij v izbranih okoljih. Ta

se prepleta z obravnavo različnih vidikov, okoliščin in določljivk varnosti podatkov in informacij. Zatem pa bo tekla kratka predstavitev in obravnava standarda ISO 17799, kateri je vir priporočil o dobrih običajih oz. ravnanjih pri zagotavljanju varnosti informacij. Končno bom navedel nekaj svojih zaključnih misli.

2. Podatki in sistemi ter njihova varnost

Univerzalnost napram krajevnemu značaju ugotovitev

Lahko se domneva, da utegnejo obstajati med regijami in državami razlike glede tipologije groženj oz. strukture in pomembnosti posameznih dejavnikov, ki opredeljujejo varnostno situacijo v danem okolju. Zato pa ugotovitev, nanašajočih se na dano stvarnost v kraju in času v splošnem ni mogoče brezskrbno posploševati. In vendar avtor tega besedila menim, da raziskave, kot so tiste predstavljene v okviru BECC (2001) in ECIS (2001) in o katerih bo tekla beseda kasneje - dajo slutiti, da so si tako težave oz. grožnje kot ranljivosti sistemov same po sebi širom sveta pogosto zelo podobne po svoji naravi (bistvu). To pa bodisi zaradi zanašanja na podobno tehnologijo kot zaradi dejstva, da – kot bo pokazano v nadaljevanju tega besedila – je konec koncev temeljni izvor ranljivosti človek. Narava le-tega pa ima širom sveta kljub prisotnosti različnih družbenih, pravnih, ekonomskih in tehnoloških okolji v osnovi iste temeljne značilnosti, ki se odražajo v njegovem delovanju. Iz tega prepričanja bom v nadaljevanju tega dela izhajal – in po potrebi ugotovljeno posebej komentiral, kjer bom menil, da bo to potrebno.

2.1 Podatki, informacije in informacijski sistem.

Kakršnokoli združbo ljudi že vzamemo v analizo (podjetje, javna uprava, vojska, neformalna združba prijateljev) je njen obstoj in delovanje odvisen od bolj ali manj formalnega podsistema ravnanja s podatki in informacijami, torej tudi izmenjave le-teh med njenimi člani. To pa je informacijski sistem.

Le-tega se lahko pojmuje kot (Gradišar, Resinovič, 1996, str. 92) “sistem, v katerem se generirajo, arhivirajo in pretakajo sporočila in informacije”. V njem se torej generirajo, zbirajo, razvrščajo, obdelujejo in preoblikujejo ter pretakajo in na ustrezen način prikazujejo podatki in informacije. Ta sistem sestavlja skupina različnih, med seboj tesno povezanih sklopov.

Tako je temeljna sestavina le-tega nabor postopkovnih, logičnih in matematičnih metod s katerimi se obdelujejo podatki. Menim, da bi naj bili v te metode integrirani odgovori na zahteve po varnosti.

Nadaljnja komponenta je izhodni blok, kogar sestavljajo vsi izhodi (dokumenti in informacije), ki naj zadovoljijo informacijskim zahtevam uporabnikov storitev informacijskega sistema. Ker so potrebe uporabnikov izhodišče pri snovanju tega podsistema se vse ostale komponente v veliki meri temu prilagajajo (Gradišar, Resinovič, 1996, str. 95). Avtor tega diplomskega dela pa menim, da iz tega izhajajo tudi varnostne zahteve (npr. potrebe po deljenju informacij napram potrebam po omejevanju dostopa in zagotavljanju celovitosti; potrebe po ustrezni ravni razpoložljivosti informacij nasproti stroškom tega početja).

Naslednji sklop je informacijska tehnika in tehnologija. Strojna in programska oprema olajšata ali sploh omogočata izvajanje velikega dela informacijskih procesov, kot jih danes poznamo (isti vir). Zato ni težko razumeti, zakaj se v strokovnih krogih toliko pozornosti namenja prav ustreznemu ravnanju s temi sredstvi[1]. Kot pa se v tem viru tudi opozarja je informacijska tehnologija dandanes nedvomno pomembna sestavina informacijskega sistema – poznavanje in razumevanje tega področja pa temu navkljub pomeni le parcialno razumevanje informacijskega sistema. V nadaljevanju bo prikazano, da preprosto ni realno pričakovati rešitev težav s področja varnosti, vkolikor se za doseganje tega cilja zanašamo zgolj na tehnologijo – npr. na šifriranje podatkov ali na uporabo protivirusnih sredstev – zanemarja pa ustrezne organizacijske in nasploh poslovodne prijeme. Namreč, kot maloprej omenjeno pripada ljudem levji delež kar se tiče vzrokov ranljivosti sistema. Njihova vloga je lahko bodisi v skrbi za nemoteno izvajanje informacijskega sistema, v upravljanju informacijskega procesa – in konec koncev seveda v uporabi rezultata tega procesa (Gradišar, Resinovič, 1996, str. 95).

Osrednjega pomena je nadalje sklop podatkovnih zbirk – slednji je po Gradišarju in Resinoviču poleg samega sklopa metod najpomembnejša sestavina informacijskega sistema. Potreba po razpoložljivosti, zaupnosti in celovitosti podatkov in informaciji se veča (že samo zaradi tesnejšega povezovanja med različnimi osebki, potrebe po čedalje hitrejšem a pravilnem reagiranju). Zato pa sam menim, da bi naj imel čedalje večjo vlogo naslednji – kontrolni blok. Ta predstavlja sistem vgrajenih kontrolnih mehanizmov, katerih vloga je zagotavljanje varovanja sistema, njegovega nemotenega delovanja (Gradišar, Resinovič, 1996, str. 96). Po mojem razumevanju bi naj ravno preko vpliva na primerno zasnovo kontrolnega bloka in tudi posledičnega odraza na zasnovo ostalih blokov priporočila kakršna jih ponuja ISO 17799 blagodejno vplivala na celovitost, zaupnost in razpoložljivost podatkov. Seveda pa bi naj predhodno dobro (s)poznali značilnosti in določljivke teh blokov. Kakorkoli že, se v praksi izkaže, da je pogosto to področje sorazmerno zanemarjeno. Ali pa pogosto obstaja neka bolj ali manj meglena ozaveščenost o tem vidiku – a je izpeljava nepopolna ali neprimerna. V nadaljevanju tega dela bom poskušal osvetliti nekaj možnih razlogov za to.

2.2 Ključna vloga varnosti podatkov in informacij v naših družbah

Kakšne posledice pa ima lahko to zanemarjanje? O vitalni pomembnosti podatkov in informacij se verjetno zlahka in hitro zedinimo, če le pomislimo na to, kje le-ti tako ali drugače nastopajo in kakšno vlogo imajo. Naj le pomislimo na različna omrežja, na katera se naša družba zanaša pri opravljanju svojih najosnovnejših funkcij. Sem sodijo poveljevanje in kontrola, energetski sistem, finančna in telekomunikacijska omrežja, prevoz (Ghosh, 2003, str. 22). Oborožene sile in politična oblast ter izvršilna oblast širom po svetu gradijo svojo (pre)moč čedalje bolj na sposobnosti čimbolj učinkovitega zbiranja, obdelave in prikaza ter uporabe informacij za odločevanje; po drugi strani pa postaja čedalje bolj ključno, da se sovražniku/nasprotniku dotok informacij čimbolj moti/onesposobi. Kot odraz tega nimam v mislih samo stremenje po vključevanju najsodobnejše informacijske in telekomunikacijske tehnologije (v nadaljevanju tudi: ITkT) v običajno opremo posameznega vojaka in v boju proti kriminalu (Schengenski informacijski sistem).

[1] To je razvidno npr. v standardu ISO 17799, katerega obravnava bo tekla v nadaljevanju.

Misel gre tukaj tudi (in morda – predvsem) na sisteme kot so vohunsko omrežje Echelon oz. na njihove zmogljivosti in obseg sredstev, vloženih v njihovo izgradnjo in obratovanje. Tukaj pa se že gibljemo na temno področje ITkT: naj samo spomnim na dejstvo, da se je omenjeno omrežje kljub lepo zvenečim deklariranim ciljem in namenom uporabljalo (zlorabljalo) tudi za gospodarsko vohunjenje lastnim zaveznikom.

Povedano pa sodi že na področje, ki ga označuje pojem "informacijsko vojskovanje". Tukaj gre razumeti (Ghosh, 2003, str. 22) takšno delovanje neke skupine ljudi, ki je usmerjeno v onesposabljanje ali povzročanje praktične neuporabnosti sovražnikovih ključnih omrežij[2]. Na porastu pa je tudi gospodarsko vohunjenje, kar lahko po svoje sodi tudi v zgornjo kategorijo (vohunjenje tako državnim kot zasebnim subjektom), prav tako kot tudi kršenje zasebnosti (tudi v najhujših oblikah kjer so na udaru kreditne kartice, vozniška dovoljenja in podatki storitev socialne varnosti). Varnostni incident, kjer sta prizadete zaupnost, celovitost in razpoložljivost podatkov in informacij pa lahko predstavlja več kot le znatno ekonomsko škodo. Lahko pomeni ogrožanje človeških življenj. In vendar lahko tudi sklicevanje na varnost brani takšno delovanje, ki ni zgolj nefunkcionalno ampak lahko celo ogroža načela, na katerih naše družbe slonijo (demokratičnost, ipd.).

Elektronsko poslovanje

Kot že nakazano, je v stvarnosti globalizacije poudarek dan na neprestanem stremenju tako posameznika in organizacij k izgradnji in ohranjanju konkurenčnosti, merjeno bodisi s kvantitativnimi kot kvalitativnimi pokazatelji. Relativni pomen hitre in učinkovite interakcije posameznika in organizacije z drugimi ljudmi in organizacijami pa narašča – je in postaja čedalje bolj ključna za uspešno konkuriranje na svetovnem trgu. Zaradi tega postaja čedalje bolj osrednja vloga elektronskega poslovanja, zaradi možnosti, ki jih to orodje ponuja v smeri doseganja in ubranitve konkurenčnih prednosti. Zato bom v nadaljevanju tega razdelka poskušal predstaviti nekaj dejstev okoli varnostne situacije kar se elektronskega poslovanja tiče, v svetu in v Sloveniji.

Ko govorim o elektronskem poslovanju pa se bom naslanjal na eno od mogočih opredelitev, po kateri je to proces poslovnih aktivnosti, kjer se uporabljajo elektronske tehnologije, metodologije in postopki (Definicija elektronskega poslovanja, 2004).

Kot že povedano, se zaradi različnih teženj kot npr. po povezovanju na globalni ravni in rastoče potrebe po deljenju informacij, zahtev po hitrosti in zniževanju stroškov čedalje bolj zanašamo na informacijsko in telekomunikacijsko tehnologijo. Pomen oz. vloga deljenja informacij je sicer lahko različen v različnih primerih – a postaja vse bolj ključen. Anderson omenja raziskave (Anderson, 2004b, str. 9), kjer je bilo ugotovljeno, da obstoji pri večjih podjetjih večja verjetnost pridobitve koristi od deljenja informacij kakor pri manjših, isto pa velja za podjetja v bolj razšežnih dejavnostih. Prav tako se ugotavlja, da je deljenje informacij tem bolj dragoceno, kolikor bolj je konkurenca v dani dejavnosti ostra.

[2] Le-te se opredeljuje in o teh poteka obravnava tudi v (JEC, 2002, str. 12-19).

Informacijska tehnologija bi naj, kot nakazano, predstavljala temelj oblikovanja globalnega trga, ta pa bi naj spominjal na teoretičen model popolne konkurence (nizki transakcijski stroški, nizke vstopne ovire in izboljšan dostop do informacij za tržne udeležence) (SURS, 1999, str. 183). V istem viru je mogoče zaslediti napovedi, da bi naj v nekaj letih (vzeto od trenutka ocene) razvoj in širitev informacijskih tehnologij prispevali vsaj 30% delež stopnje rasti gospodarstva ZDA; naložbe v te tehnologije pa bi naj predstavljale v tistem obdobju okoli 45% vseh gospodarskih naložb v isti državi. Po istem viru se v informacijski tehnologiji prepozna sredstvo za prerazporeditev moči med panogami; spretna izraba priložnosti, ki jih nove tehnologije prinašajo lahko popelje podjetja in panoge do uspeha - izpostaljajo pa se nevarnosti tisti, ki tega ne zmorejo/nočejo. Informacijsko-telekomunikacijska tehnologija ponuja priložnosti kot so zniževanje stroškov, vzpostavljanje in dolgoročno krepitev odnosov s kupci. Kar se e-poslovanja tiče ima prevladujoči pomen t.i. B2B poslovanje (medpodjetniško poslovanje) napram B2C (podjetje s porabniki). Podjetje bi naj za uspeh v hitro spreminjajočih se razmerah (sploh majhna podjetja) osredinila se bodisi na kupca, na iskanje novih trgov, na boljšo sodelovanje/integracijo med partnerji v verigi vrednosti (SURS, 1999, str. 184).

2.3 ITkT (Informacijska in telekomunikacijska tehnologija) v Sloveniji

Kakšen pa je položaj Slovenije kar se tiče prežetosti s prvinami informacijske družbe? Občutki glede tega so mešani. Podatek ispred nekaj let (in tudi zaradi tega morda omejene veljavnosti) kaže (SURS, 1999, str. 40), da je vsaj v bližnji preteklosti v Sloveniji vladalo precejšnje zanimanje za storitve informacijske družbe (on-line medicinska diagnoza, stiki s politiki, izobraževanje na daljavo, informacije o potrošniških pravicah, opravljanje uradnih/upravnih storitev). Izmerjeno zanimanje je bilo višje od povprečja držav EU. Novejše poročilo eEurope+ 2003 (EU, 2004) dejansko kaže na sorazmerno ugoden položaj Slovenije na tem področju[3].

Podobno visoko zanimanje (tudi v razmerju do omenjenega povprečja) je po zborniku SURS nastalo tudi glede drugih področij, kot so finančni management (on-line upravljanje bančnega računa, ipd), ogled virtualnih muzejev, načrtovanje potovanj in izletov, pregledovanje on-line časopisov, posredovanje informacij o blagu in storitvah, iskanje zaposlitev, sklepanje finančnih pogodb. Res pa je, da vsaj kar je avtorju tega dela dano vedeti, se ta načelni interes ni v večji meri prelevil v dejansko uporabo e-storitev[4].

3. Stanje na področju varnosti podatkov in informacij v svetu

Zgoraj je bila med drugim opredeljena vloga podatkov in informacij tako širše pojmovano – za družbo, kot ožje, za podjetje ali posameznika. Obenem sem se dotaknil obravnave možnih težav oziroma njihovih žarišč. Preučevanje slednjega bom skušal sedaj še razširiti in poglobiti tako, da bi najprej začel s predstavitvijo nekaj dejstev okoli varnostne situacije – tako v svetovnem merilu, kakor tudi ožje, za Slovenijo.

[3] V mnogih pogledih bi naj bila država še med vodilnimi znotraj takratnih kandidatk za pristop k EU, čeprav se prednost v mnogih primerih – celovito gledano – neprestano in dokaj hitro manjša.

[4] Navsezadnje se npr. zaenkrat tudi kvalificirani digitalni certifikati izdani s strani SIGEN-CA niso tako uveljavili kot je bilo želeno, vsaj pri fizičnih osebah ne.

Zanimivo izhodišče je lahko povzetek misli Andersona, kateri sam že uvodoma (Anderson, 2004) nakazuje na možno ozadje tega področja; zanimiva je med drugim tudi raziskava, opravljena pred več kot štirinajstimi leti s strani CSTB (Computer Science and Technology Board) pri NAS (National Academy of Sciences) v ZDA za to državo, kjer se med drugim poskuša ugotoviti razloge problemov v pomanjkljivi varnosti podatkov in informacij. Poglavitne "krivce" za dano situacijo pa raziskava odkriva med zelo hitrim tempom tehnoloških (in predvsem arhitekturnih) sprememb, v sorazmerno počasnem tempu državnih intervencij na trgu (preko programov nakupa in evaluacije), izvoznih kontrol, pomanjkanja potrošnikovega razumevanja tveganja in zelo omejenim možnostim (pogajalske moči, op. avt.) ki jo imajo porabniki programske opreme napram prodajalcem.

Kaj pa gre povedati o varnosti podatkov v praksi? Po eni strani se gotovo niso (in najverjetneje ne bodo) uresničile obljube o skorajšnjem prihodu "zares varne" tehnologije. In vendar je potrebno priznati, da se po drugi strani niso uresničile napovedi o katastrofalnih varnostnih incidentih (naprimer, afere Enron, WorldCom in Long Term Capital Management v bistvu niso bile posledica odpovedi informacijsko-varnostnega sistema) (Odlyczko, 2004, str. 1, 6-7). Sorazmerno zaskrbljujoče pa je spoznanje, da je pri zelo zapletenih sistemih kot je npr. operacijski sistem potrebno veliko več napora vložiti v izgradnjo zagotavljanja dovolj visoke ravni varnosti (z odkritjem in odpravo/omilitvijo vseh slabosti) kot pa je za napadalca odkriti dano kritično napako in uspešno zaobiti varnost sistema.

3.1 Raziskava CCSS – stanje v ZDA

V nadaljevanju bo predstavljeno nekaj izmerjenih dejstev okoli stanja varnosti (nanaša se bolj ali manj direktno na problematiko varnosti omrežja).

Raziskave CCSS (Anketa o računalniškem kriminalu in varnosti) izvaja CSI (Inštitut za računalniško varnost), izdelane pa so na podlagi manjšega namenskega vzorca IT strokovnjakov v ZDA. Kljub tej in še nekaterim omejitvenim značilnostim so širše sprejete kot veljaven (čeprav grob) presek varnostne situacije v ZDA v danem letu. V nadaljevanju bo predstavljenih nekaj izmed dejstev, ki izhajajo iz ankete CCSS za leto 2003 (CSI, 2004), s primerjavami gibanj glede na prejšnja leta.

Število pomembnih incidentov je iz leta v letu sorazmerno stabilno. Celotni ocenjeni letni stroški zaradi varnostnih incidentov so pri anketiranih (n=513 enot) v letu 2003 znašali preko 200 mio USD). Največji delež v omenjenih je ponovno imela kraja zasebnih podatkov (dobrih 70 mio USD); sledijo napadi zavrnitve storitev (DoS), zatem pa incidenti v zvezi z računalniškimi virusi in zloraba s strani notranjih ljudi (cca. dobrih 27 mio USD; škoda zaradi le-te je ocenjena na slabih 12 mio USD). Znižal se je delež finančnih goljufij. Povprečni posamezni incident je terjal 2.7 mio USD stroškov.

V zadnjih nekaj letih je v ZDA opaziti trend padanja zaznanih primerov nepooblaščene uporabe dostopa do omrežja; slednje so bile tudi najbolj citirana postavka zaznanih zlorab (preko 80% celote). Vztrajno visoko ostaja nasprotovanje najemanju "spreobrnjenih" hekerjev (68% vprašanih).

Zaskrbljujoč je podatek, da je le manjši (del osebkov, ki so utrpeli varnostni incident to prijavilo pristojnim oblastem (cca. 30% - čeprav ta delež raste napram istovrstnim vrednostim iz začetnih let izvajanja ankete v okviru CSI. Takšno vedenje pa daje potuho povzročiteljem teh incidentov. Večina vprašanih ni razložila vzrokov neprijavljanja – izmed tistih, ki so odgovorili pa jih je večina preprosto navedla, da niso vedli točno na kateri organ oblasti se obrniti. Izkušnje posameznikov, ki so se odločili za ukrepanje kažejo, da pogosto ni temu kriva samo neozaveščenost oz. neznanje ljudi ampak tudi nejasna delitev pristojnosti med različnimi organi izvršilne oblasti. Razlogi za neobveščanje oblasti pa so tičali tudi drugod – nekaj najpogostejših pa je bilo: strah pred negativno publiciteto (70% vprašanih), bojazen, da bi konkurenca to informacijo izkoristila (61% vprašanih), kot tudi prepričanje, da je rešitev brez vpletanja oblasti boljša (56% vprašanih).

Rastoči delež vprašanih kot zaznano točko vdora v omrežje navaja Internet (78%), medtem ko je delež klicnega dostopa nizek in je podvržen trendu padanja (18% vprašanih); podobno velja za druge notranje sisteme. Podobno navaja večina vprašanih (53%), da je bil izvor napada na njihovo nahajališče svetovnega spleta izven podjetja; 18% jih poroča o izvoru tako izven kot znotraj podjetja, 24% pa tega ne ve določiti. Kot verjetne vzroke napadov navaja rastoč delež vprašanih samostojne hekerje (82%) in tuje vlade (28%), navaja pa se tudi nezadovoljnje zaposlene (77%), konkurente znotraj ZDA (40%) ter tuje korporacije (25%). Problem pa predstavlja dejstvo, da mnogo vprašanih pravzaprava ne ve, kaj se z omrežjem dogaja – a je bilo napadeno ali ne (15%). Ta delež je skozi leta stabilen. Nepoznavanje sestavnih delov sistema in njihovih povezav je sicer temelj t.i. varnosti preko obskurnosti (security through obscurity) - no, vsaj dokler imamo v mislih tuje osebke; ne zdi se mi pa najbolj pametno, da bi sami ne poznali svojega sistema.

Tipologija zaznanih oblik incidentov je pestra: omenjajo se virusi (82%), zloraba dostopa do Interneta s strani notranjih uporabnikov (80%), zlorabe prenosnih računalnikov (59%), nepooblaščen dostop s strani notranjih uporabnikov (45%), napadi zavrnitve storitve (DoS attacks) - (42%); vdori v sistem (36%), sabotaža (21%), kraja podatkov v lasti organizacije (21%), finančna goljufija (15% stabilna), zlorabe telekomunikacijskih sredstev (10%), prisluškovanje telekomunikacijam (6%), neposredno prisluškovanje prometu na mreži (1%). Ob zaznavi napada je 93% vprašanih namestilo ustrezne popravke, nekaj več kot polovica jih ni obvestilo oblasti; 30% je oblastem poročalo, 21% pa je poiskalo pravno pomoč.

Zelo velik delež vprašanih je uporabljal neko vrsto tehnične zaščite: protivirusne programe in požarne stene, neko vrsto fizične zaščite in neke vrste kontrole dostopa (vsak izmed teh najmanj pri 91% vprašanih). Izgleda pa, da je tisti, ki se za to ni odločil v splošnem imel tehtne razloge: nihče od tistih, ki so se tako opredelili ni sodila v zgornji del spektra poročane višine škode , posledice incidentov. Precej je tudi narasla uporaba sistemov za zaznavanje vdora (v tej anketi jih je 73% respondentov uporabljala); 69% vprašanih uporablja šifriranje datotek, le okoli 11% pa biometriko.

3.2 Oris stanja v EU in v Sloveniji

Pri primerjavi (RIS2002, 2004) situacije v Sloveniji v razmerju do izbranih držav EU (v nadaljevanju tudi: EU) je bila opažena v splošnem zelo dobra (praviloma vsaj primerljiva)

penetracija ITkT. Precejšnje zaostajanje pa kaže Slovenija pri tistih tehnologijah, ki jih vir omenja kot najbolj napredne (intranet, extranet, videokonference) (RIS2002, 2004, str. 7). Z vidika predmeta pričujoče diplomske naloge pa je najbolj zanimiv del raziskave, ki se ukvarja z varnostjo. Tukaj je delež slovenskih podjetij, ki je utrpelo neke vrste varnostnega incidenta bistveno višje od evropskega povprečja (75% vprašanih napram v povprečju 19% pri izbrani skupini držav). Večji del te razlike pa gre pojasniti s težavami, povežanimi z virusi (96% slovenskih podjetij je v 12 mesecih pred raziskavo registriralo probleme z računalniškimi virusi).

Drugih vrst varnostnih incidentov (nepooblaščen dostop, manipulacija s programsko opremo, kraja identitete, on-line goljufija) je bilo v Sloveniji v splošnem precej manj. Nepooblaščen dostop do notranjega omrežja (1% respondentov, v izbranih državah EU 15%), škodljiv poseg v programsko opremo podjetja (Slovenija - 3%, izbrane države EU 11%), kraja identitete (imen in gesel) (Slovenija 0%), EU 7%) ter online prevara (Slovenija 0%, EU 5%). In vendar je le polovica teh primerov imela samo zanemarljive posledice (RIS2002, 2004, str. 106). Po istem viru le manjši delež podjetij meni, da so bile posledice varnostnih incidentov, ki so jih doživeli zelo resne, s tem da je pri manjših podjetjih ta delež v splošnem višji kot pri večjih (verjetno bodisi zaradi odvisnosti od manjšega števila računalnikov kot manjše skrbi za primerno zaščito, ki je prisotna pri manjših podjetjih)(isti vir). Res pa je, da so to pač ocene vprašanih. Če nekoliko poenostavim: glede na v splošnem slabo ozaveščenost in implementacijo zaščitnih ukrepov menim, da je povsem možno, da je situacija vsaj kar se tiče vdorov in kraje podatkov tudi nekoliko drugačna od tukaj ocenjene.

Zanimive so razlike med zaznavanjem izvora grožnje (RIS2002, 2004, str. 9): slovenska podjetja se bolj bojijo hekerjev in sedanjih zaposlenih; manj pa nekdanjih zaposlenih, kupcev oz. dobaviteljev/drugih partnerjev (bojazen je pri srednjih podjetjih nekoliko višja; pri mikro podjetjih izmerjene bojazni praktično ni). Po drugi strani se v izbranih državah EU praviloma srečamo z dajanjem večje teže nevarnosti grožnje, ki jo prestavljajo nekdanji zaposleni in poslovni partnerji. Kričeče moteč pa je po mojem tudi podatek, da bi naj imelo samo 8% slovenskih podjetij izdelano in dokumentirano neko formalno varnostno politiko – s čimer se Slovenija uvršča na zadnje mesto v omenjeni skupini (izbrane države EU v povprečju – 35%) (tukaj sicer menim, da ni jasno ali se to nanaša le na varnost omrežja ali celovito gledano). Ko pa gre za varnost podatkov v Internetu podjetja najprej pomislijo na lastne kadre (42%) in na svojega ponudnika storitev dostopa (36%), kot tudi na specializirana podjetja.

Uporaba aktivne varnosti npr. požarne stene je v Sloveniji relativno redka (28%; izbrane države EU 44%), kar pa bi po oceni RIS lahko bila posledica politike gostovanja v Sloveniji, kjer bi naj imelo manj podjetij svoj strežnik (za gostovanje spletnih nahajališč pa bi uporabljali storitve ponudnika dostopa do Interneta). Kakorkoli že, s širšo uvedbo povezave v Internet kot so ADSL ali kabelski Internet se mi zdi takšna politika še posebej vprašljiva. Tudi pri gospodinjstvih. Izpostavljenost je iz tega gledišča sedaj sorazmerno manjša (junija leta 2002 preko 71% gospodinjstev klicni dostop); a se tudi tukaj situacija spreminja – in izpostavljenost se povečuje.

Pri implementaciji on-line prodaje je eden od ovir njegovemu širšemu razmahu resda neuporaba online prodaje pri njihovih dobaviteljih – a tudi negotovost okoli varnosti podatkov (in ta skrb je veliko višja od povprečja EU držav) (RIS2002, 2004, str.9). Res pa je, da raziskava RIS o e-

poslovanju (RIS2002, 2004b, str. 180) nakazuje, da je med navedenimi razlogi neuporabe e-poslovanja varnost v primerjavi z drugimi dejavniki (npr. nezainteresiranost; čakanje na nadaljnji razvoj; visoki stroški) manj pomembna.

Slovenska podjetja kažejo nadpovprečno načelno zanimanje za storitve e-Uprave, dejanska uporaba pa je nekje v povprečju. Tudi tukaj pa prevladuje mnenje, da je potrebno še veliko postoriti na področju varnosti, da bi lahko bila varnost e-poslovanja primerljiva s tisto pri tradicionalnem – in tukaj je nezaupanje višje kot v povprečju v izbranih EU-državah (30% nasproti 40%). Glede na ugotovitve Ghosha (2003) in JEC (Joint Economic Committee) (Security in the information age, JEC, 2002, str. 1-10) – (predstavljane v nadaljevanju) bi se torej kazala potreba po izgradnji uspešnejšega sodelovanja med državo in zasebnih sektorjem.

Nasplošno pa je mogoče reči (RIS2002, 2004a), da velika večina podjetij s sedanjim ali načrtovanim dostopom do Interneta omogoča zaposlenim dostop do le-tega (nasplošno, kot tudi posebej svetovnega spleta in e-pošte). Zelo malo podjetij pa ima formalen pravilnik o uporabi Interneta za zaposlene (7%, največ med velikimi) – skoraj polovica velikih podjetij pa omejuje dostop do določenih vsebin (pa vendar le 16% celote to počne; 73% jih ne). Nadzor nad uporabo Interneta s strani zaposlenih pa je v splošnem nizek. Petina podjetij se strinja, da postaja uporaba v zasebne namene problem, slaba polovica pa se ne strinja (bolj srednja, manj majhna podjetja). Nasprotno pa kažejo gospodinjstva (SIBIS, 2004) relativno nizko zaskrbljenost o varnosti na Internetu (nižjo od povprečja v EU in državah pristopnicah - 63% napram 79% v EU); prav tako je precej nižji delež rednih uporabnikov Interneta, katerim se je pogosto zgodilo, da so jih pomisleki v zvezi z varnostjo odvrnili od online nakupa (4% napram EU povprečju 24%).

4. Posledice pomankljive varnosti podatkov in informacij v podjetju

Dosedaj je bilo ponujenih nekaj dejstev in misli o različnih grožnjah, vrstah zlorab na področju varnosti podatkov in informacij o njihovi razširjenosti in posledicah – npr. izgubi zasebnosti, finančni škodi, izgubi kupcev, osramotitvi podjetja v javnosti, motenj pri poslovanju in negotovosti. Sledi nekaj bolj konkretnih misli o omenjenem.

Varnost podatkov in informacij v luči vloge in pomena zaupanja v sodobnem poslovanju

Zgolj naštevanje groženj in možnih škod ni dovolj. Zato bi tukaj želel nekoliko poglobiti vsaj eno samo (po mojem kritično) posledico (ne-)varnosti podatkov: zaupanje. Kritično pa zato, ker kot rečeno je čimgloblja in učinkovita interakcija med različnimi posamezniki in organizacijami čedalje bolj bistvena določljivka uspešnosti. Sodelovanja pa ni brez zaupanja – oz. sta obseg in kakovost sodelovanja praviloma sorazmerna ravni obstoječega zaupanja med partnerji.

Torej, tako z vidika teorije kot prakse ima zaupanje osrednjo vlogo v poslovanju (BECC, 2001; ECIS, 2001, str. 188-203) – domnevam da toliko večjo pri e-poslovanju, kjer je delež neopredmetene komponente pri medsebojnih odnosih praviloma toliko večji.

Stroka jasno poudarja (BECC, 2001, str. 263-264) kako velik vpliv ima na (ne)uspešnost e-trgovine podjetja s porabniki (B2C) zaupnost podatkov in lojalnost kupca do podjetja, ki tudi s tega izhaja. Nekaj ključnih dejavnikov pa so pri tem med drugim prav izgradnja zaupanja v očeh

kupca, pravilno delovanje programske opreme uporabljene v transakcijah, kot seveda varnost transakcij s podatki.

Isti vir zatrjuje, da je tudi v primeru medpodjetniškega e-poslovanja ključnega pomena zaupanje, ki obstaja med strankami, kot tudi proaktivna vloga podjetja pri trženju ideje e-poslovanja partnerjem. Brez ustreznega zagotovila in seveda tudi naknadnega dokazila o varnosti tega početja, si je težko predstavljati kakšen večji uspeh. Takšno ravnanje pa bi naj v končni fazi bilo vsaj na dolgi rok nagrajeno s primerno donosnostjo.

V BECC (2001, str. 20) se jasno izraža oceno, da je ravno pomanjkanje zaupanja ena od glavnih "krivcev" sorazmerno nizke ravni e-trgovine na področju Azije-Pacifika. Pri tem se poudarja, da glavni problem ni nezaupanje v varnost tehnologije same, temveč nezaupanje v človeško kompomento. Ali točneje – negotovost povezano z nepredvidljivostjo prihodnih dogodkov in negotovostjo glede reakcije partnerja nanje. Taka bolj ali manj racionalna bojazen pa lahko – kakor v Singapurju – pripelje do tega (BECC, 2001, str. 20), da podpora države, ki bi naj ustvarjala ugodno okolje za utrditev zaupanja in katero se v tem tekstu večkrat zagovarja gotovo sama po sebi ni zadostno zagotovilo uspešne uveljavitve e-poslovanja.

Čeri zlorabe Interneta v podjetju

Sedaj pa bi pogled nekoliko zožil. S širšega področja e-poslovanja, o katerem sem sedaj govoril bi v tem razdelku usmeril pogled na vidik komunikacij znotraj in med podjetij. Bilo je namreč veliko govora o rastočem pomenu povezovanja osebkov v omrežja, o izmenjavi podatkov po le-teh – in o nevarnostih, ki se tukaj skrivajo. Tukaj je ponovno v ospredju omrežje omrežij – Internet. Če torej ostanem pri tem, so tveganja, kateremu je izpostaljena organizacija pri povezavi v Internet raznovrstna (BECC, 2001, str. 754): uporaba v neposlovne namene, zlonamerna koda, programska oprema z napakami, zavrnitev storitve, nenamerne napačne poslovne transakcije (npr. e-pošta napačnemu naslovniku), goljufija, hekanje, spodrsljaji pri odnosih z javnostmi[5] (npr. osebno mnenje, ki pa je razumljeno kot stališče podjetja), neprimerna e-pošta (npr. nadlegovanje), podatki slabe kakovosti – ki pa se uporabljo v poslovne namene), piratstvo, kraja informacij (tudi preko prestrezanja), nenamerno razkritje informacij. Velikega pomena je zato jasna opredelitev dopustnih uporab Interneta; ta opredelitev bi se naj skladala s cilji organizacije.

Druga odprta rana - notranji uporabniki in kraja podatkov

Vrnil se bom k nekoliko širšemu pogledu na problematiko varnosti in obenem stopil na drugo področje. Dosedaj že bilo že večkrat poudarjeno, bi naj bili notranji ljudje ena najresnejših groženj varnosti podatkov in informacij. Poleg zgoraj omenjenih oblik groženj je ena najbolj razširjenih tudi kraja podatkov v lasti podjetja s strani zaposlenih. Raziskava podjetja Ibas bi naj pokazala (UK businesses lose £billions in Intellectual Property (IP) theft, 2004), da je 69.6% t.i. plavih ovratnikov (blue collars) ukradlo dokumente oz. informacije (intelektualno lastnino) v lasti podjetja, ko so podjetje zapustili.

[5]Formalno najtočnejši prevod bi tukaj bil - "netočna reklama"; mislim pa, da "spodrsljaj pri odnosih z javnostmi" vsebinsko boljše opisuje misel v nadaljevanju.

Zanimiv je podatek, da 58.7% vprašanih meni, da je nepooblaščen odvzem intelektualne lastnine najmanj tako sprejemljiv kot je sprejemljivo pretiravanje pri prijavi škode zavarovalnici. Samo 28,2% meni, da je kraja intelektualne lastnine popolnoma nesprejemljiva. V zvezi s tem je najbolj pogosto opravičilo za krajo bilo, da je tako ali tako oseba ustvarila dokumente/datoteke in ji le-te potemtakem delno pripadajo. Verjetnost kraje je bolj verjetna pri moških kot pri ženskah.

Po omenjenem viru bi naj bil najboljši način preventive ta, da bi oseba, ki zapusti delovno mesto morala podpisati pravno zavezujoči dokument na odslovilnem intervjuju, kjer bi izjavila, da ni odvzela elektronskih[6] kopij kakršnihkoli dokumentov podjetja ali datotek.

Najpogostejše oblike ukradene intelektualne lastnine so po pričakovanjih (v % zaposlenih, ki so zapuščali podjetje): adresarji e-pošte (54.3%), prodajne prospekte/predstavitve (32,6%) ter baze podatkov o kupcih/informacije o kontaktih (30,4%).

Najpogostejša metoda kraje intelektualne lastnine je po izsledkih te raziskave pošiljanje elektronskih kopij dokumentov in datotek na osebni e-poštni naslov.

Prekinitve v transakcijah

Nadaljnje boleče področje je za podjetja tematika prekinitev v transakcijah (transaction breaks). Preprečevanje oz. lažje in hitrejše reševanje le-teh bi lahko bilo prav tako še eno od gibal vpeljave sistema varovanja podatkov. Vzrok tem prekinitvam najdemo bodisi v napakah v programski opremi, človeških napakah oz. preprosto v nesporazumu med poslovnimi partnerji ter v nesrečah – škodnih dogodkih. Prekinitve v transakcijah oziroma njihovo reševanje pomenijo skoraj vedno človeško intervencijo in pogajanja med partnerji. Ocenjuje se, da se take prekinitve dogodijo pri približno 11% transakcij, udeležence pa stanejo več milijard dolarjev letno (BECC, 2001, str. 69-70). Po istem viru lahko stanejo problematične transakcije 300% več od tistih, kjer intervencija ljudi ni potrebna; povprečna cena trasakcije pa se tako poveča za več kot 20%. Pravkar povedano pa lahko konec koncev pomeni, da se zlahka dogodi celo, da znašajo stroški povezani s prekinitvami v transakcijah več kot 40% stroškov poslovanja. Zanemarjanje napak je včasih lahko tudi ekonomsko upravičeno – gotovo pa je zelo tvegano in možnostno nevarno področje: lahko pripelje do netočnih podatkov, skritih stroškov in sprejemanja napačnih odločitev (BECC, 2001, str. 72), kar ima lahko konec koncev nezanemarljive posledice.

5. Tehnični vidiki varnosti

Po motrenju stanja okoli varnosti in obravnavi posledic ugotovljenih dejstev, bo sedaj tekla beseda o nekaterih vidikih vzrokov, ki ležijo v ozadju – in to predvsem iz tehničnega vidika. Tukaj se bom med drugim na kratko dotaknil vpliva na varnost podatkov, ki ga imajo napake v programski opremi/neustrezno nastavljanje programske opreme in na problem prevelikega zanašanja na tehnična sredstva za zagotavljanje varnosti, omenil bom vidik zagotavljanja netveganosti okolja. Podrobnejša analiza dejavnikov, povezanih z netehničnimi vidiki (sociološki, psihološki, pravnimi vidiki) se pravzaprav ne bo vršila na tem mestu (v 6. točki), temveč v naslednjih točkah.

[6] "Elektronskih" - domnevati gre, da se to nanaša na podatke kakršnekoli narave – ne zgolj elektronskih.

5.1 Ugotovitve Inštituta SANS o ranljivosti programske opreme – primer Microsoftove opreme.

Deset izmed najbolj perečih ranljivosti posameznega izdelka (govorimo o Microsoft-ovi programski opremi, ki je najbolj razširjena v svetovnem merilu, tudi v Sloveniji) je po ocenam inštituta SANS (SANS, 2004) v naslednjem vrstnem redu: Internet Information Services (IIS), Microsoft SQL Server (MSSQL), Windows Authentication, Internet Explorer (IE), Windows Remote Access Services, Microsoft Data Access Components (MDAC), Windows Scripting Host (WSH), Microsoft Outlook and Outlook Express, Windows Peer to Peer File Sharing (P2P), Simple Network Management Protocol (SNMP):

Pomislimo lahko na to, da je Microsoftova platforma (v nadaljevanju tudi: OS Windows) (zaenkrat) precej ranljiva, da se nahaja v krepko več kot 90% uporabniških računalnikov gledano v svetovnem merilu in da so ti uporabniki v splošnem zelo slabo seznanjeni s pomembnostjo varnosti podatkov, načini za njeno uresničitev ali preprosto niso pravilno motivirani. Izgledalo bi torej, da se večjih težav z varnostjo s kakršnimi se soočamo dandanes, ne bomo rešili tako hitro.

Primerna politika nameščanja popravkov je praktično predpogoj za resno spopadanje z vsemi izmed navedenih ranljivosti, isto pa velja tudi za proaktivno in konzervativno nastavljanje opreme. Omenjene pa so bile samo ranljivosti sistemov z Microsoftovo opremo zato, ker kot rečeno, je ta platforma daleč najbolj razširjena (na računalnikih za končne uporabnike, nezanemarljiv delež pa ima tudi pri strežnikih). Ni pa samo zelo razširjena – je tudi precej ranljiva). Menim pa, da je bistvo opisanih ugotovitev, dovolj splošno, da je vsaj do neke mere neodvisno od konkretne platforme – zatorej pa zaradi svoje splošnosti sprejemljivo za obravnavo glede na namen te diplomske naloge.

MS IIS - Microsoft Internet Information Services (IIS)

Tudi razširjeno prepričanje, da je najbolje ohraniti tovarniško privzete nastavitve programske opreme ni nujno najbolj modro početje. Po oceni Inštituta SANS (2004) je ravno takšno ravnanje vzrok najbolj pereči ranljivosti v omrežju Internet. Na prvem mestu v klasifikaciji ranljivosti SANS se trenutno nahaja MS IIS. Konkretno pa gre kot razlog temu iskati v šibkostih pri dodatnih aplikacijah tega proizvajalca za prikaz funkcionalnosti strežnika, kot tudi v omenjenih nevarnih privzetih nastavitvah strežnika. Mogoč problem pa predstavlja tudi programska oprema tretje strani. Ta lahko bodisi sama po sebi predstavlja šibko točko (lahko ima napake, vsebuje lahko zlonamerno kodo) ali pa v kombinaciji z osnovnim programov pomeni povečano ranljivost tako oblikovane celote.

V namen obrambe pred grožnjami izpostavlja isti vir tudi možnost uporabe posebnih orodij za testiranje, ki jih proizvajalec dane opreme ponuja. Pred tem (pa tudi nasplošno) pa je najboljše orožje proti zlorabam primerno izobraževanje, nenazadnje tudi preko poznavanja/spoznavanja značilnosti same opreme in lastnosti/posebnosti njenega vključevanja v sistem – tudi preko temeljitega preučevanja dokumentacije proizvajalca. Resnici na ljubo, slednja sicer ni vedno tako kakovostna kot bi naj bila, tako glede točnosti, obsega, razpoložljivosti[7].

[7] Pripomba se pravzaprav v konkretnem nanaša na primer Microsoftove dokumentacije, vir podatka pa je uslužbenec pri uveljavljenem slovenskem proizvajalcu programske opreme).

MS SQL strežnik

Po raziskavah SANS (2004) se glede na varnostne težave z MS-SQL strežnikom poudarja pomen ustrezne politike gesel, sploh administratorskih. Prav tako je ključna prisotnost (in izvajanje) ustrezne politike ravnanja z uporabniškimi računi in overovljanja. V zvezi z uporabniškimi računi pa gre tudi poskrbeti za ustrezno politiko dodeljevanja in upravljanja z pravicami uporabnikov pri dostopu in uporabi sistema. Osrednjega pomena je praksa sprotnega (in pravočasnega)[8] nameščanja popravkov programske opreme, pa tudi premišljena in proaktivna konfiguracija sistema. Pri tem mislim tako na nastavitve uporabniške programske opreme in sistemskih storitev v splošnem a tudi na primerno nastavitev zaščitnih sredstev (npr. pri požarnih stenah posebno pozornost pri odločitvi o nadzoru določenih vrat).

Menim pa, da je razvidna tudi potreba po odgovornejšem ravnanju proizvajalcev programske opreme (pa naj bo to posledica samoregulative ali – verjetneje – regulative in ukrepov državnih oblasti) kar se tiče dajanja v promet ustrezno pripravljenga paketa programov. Pri tem mislim tudi na dejstvo, da mnogi uporabniki nimajo(nimamo) dovolj poglobljenega znanja, da bi sami poskrbeli za ustrezno konfiguracijo (ali pa ni časa/drugih sredstev). Mnogi uporabniki prav tako sploh ne vedo, da imajo določen izdelek inštaliran (npr. okrnjena različica SQL strežnika pri MS OfficeXP), kar jih lahko izpostavi tveganju, brez da se tega sploh zavedajo.

Overovljanje pri različicah OS Windows

Pri zagotavljanju varnosti se izpostavlja tudi pomen ustreznega overovljanja in kontrole dostopa; to področje (oz. njegova vloga) pa je španska vas za večino vpletenih v uporabo informacijskih sistemov. Rekel pa bi, da to med drugim pomeni večjo ranljivost za določeno vrsto napadov kot npr. napadi s preskakovanjem (leapfrog attacks), kar lahko pomeni razsežnejšo ranljivost.

Na področju, katerega se sedaj dotikamo se najpogosteje navajajo težave okoli gesel. Često se dogaja, da ali so le-ta šibka, ali jih preprosto ni ali pa so slabo zaščitena. Pa tudi operacijski sistem ali druga programska oprema pri svojem delovanju včasih razpolaga z administratorskimi pravicami a se poslužuje šibkega ali neobstoječega gesla. Prav tako je včasih problem uporaba splošno poznanih zgostitvenih algoritmom, ki se pri overovljanju uporabljajo. To velja sploh v povezavi z morebitno neselektivno dostopnostjo do izvlečkov teh gesel (digest). Problem predstavlja uporaba šibkih algoritmov uporabljenih pri overovljanju v mreži. Pogosto je pri omrežjih, kjer so prisotni računalniki z različnimi operacijskimi sistemi npr. iz razloga združljivosti uporabljen dani algoritem, ki je včasih najmanj primeren. To pa pomeni, da tudi gesla, ki bi se jih sicer imelo za močna postanejo neprimerno bolj ranljiva.

V povezavi s tem pa se ugotavlja nujnost testiranja jakosti gesel – a to z istimi orodji, kot jih uporabljajo hekerji. Pokazatelji šibkosti sistema so lahko npr. tudi obstoj aktivnega računa, ko lastnik (zaposleni) zapušča podjetje. Pomembno je usrezno izobraževanje zaposlenih o pomenu in načinu uporabe močnih gesel, prisotnosti morajo biti postopki s katerimi se zagotavlja, da poteka uporaba v skladu s sprejetimi načeli (gesla dane zapletenosti, starost gesel, zgodovina uporabljenih gesel, minimalna dolžina, (ne)uporaba reverzibilne enkripcije gesel). Vse zgoraj pa

[8] Pri tem pa je potrebno imeti v mislih ugotovitve, obravnavane v točki 6.2 tega besedila.

bi naj bilo zasnovano s preprostim dejstvom v mislih, da je vsako geslo ranljivo skozi čas. Obravnavana politika bi naj obsegala tudi omejitev in spremljanje dostopa do računalniškega sistema (predvsem krmilnika domene, varnostnih kopij) pa tudi preverjanje in popravljanje, po potrebi pravilno nastavljanje/odstranjevanje neprimerno nastavljene opreme (tukaj mislim npr. na omrežne kartice v promisc načinu – kar omogoča tudi nepoklicanim pregled omrežnega prometa). Sem sodi tudi morebitna uporaba overitvenih žetonov kot tudi biometričnih sredstev.

Spletni brskalnik MS Internet Explorer

Velik je tudi pomen omejitve dostopa do spletnih vsebin (posebno bi se naj pazilo npr. da ni v skupini zaupanja vrednih spletnih nahajališč kakšno nahajališče, ki si tega ne zasluži) kot tudi sprotnega krpanja varnostnih lukenj in namenjanje ustrezne pozornosti primerni konfiguraciji brskalnika. To se kaže v dejstvu, da so nevarne spletne strani pogosto posebej zlonamerno izdelane, da izkoristijo slabosti brskalnikov. Omenjeno pa lahko pripelje do razkritja piškotkov, lokalnih datotek ali podatkov pa tudi izvedbo krajevnih programov oz. prenosa nepooblaščene kode na uporabnikov računalnik in njeno izvedbo. Mogoč pa je tudi popoln prevzem ranljivega sistema.

Storitve oddaljenega dostopa pri OS Windows (RAS – Remote Access Services)

Problematična je lahko tudi neprimerna politika deljenja resursov. To lahko izkoristijo zlonamerni uporabniki – med drugim se lahko ustvari odskočna deska za širjenje virusov. Pereč problem je pri vsem tem (tudi tukaj) privzeta nastavitev opreme s strani proizvajalca. Kjučna bi naj bila postavitev ustreznega overovljanja, ki naj bi bilo predpogoj za sleherni dostop do deljenih resursov; omejiti bi bilo potrebno deljene resurse na tiste zares nujno potrebne in obenem konzervativno nastaviti pravice uporabnikov. Zaradi zmanjšanja možnosti sleparjenja pri izkazovanju identitete računalnika v mreži, bi se naj dajalo prednost uporabi IP naslovov pred domenskimi imeni. Zmanjšalo bi se naj uporabo anonimnega dostopa in posvetilo ustrezno pozornost sestavljanju mreže iz računalnikov z različnimi operacijskimi sistemi (kjer obstaja tveganje, da bi lahko iz razloga združljivosti bili uporabljeni neprimerni sistemi overovljanja).

Veliko pozornost bi bilo potrebno prav tako posvetiti omejevanju dostopa na daljavo do sistemskega registra, kot tudi paziti na pravilno konfiguracijo sistema nasploh (tudi z onemogočanjem določenih komunikacijskih vrat). Tudi tukaj je ključno sprotno nameščanje popravkov, tokrat v zvezi s storitvami RPC (Remote Procedure Call).

Microsoft Data Access Components (MDAC) in Windows Scripting Host (WSH)

Pri uvodoma navedeni ranljivosti sistema MDAC se posebej izpostavlja potencialna nevarnost privzetih nastavitev oz. prisotnost hroščev pri tej komponenti; ustrezna politika nameščanja popravkov/posodabljanja komponent bi naj zagotovila primerno stopnjo varnosti.

Ta komponenta bi naj bila onemogočena, razen v primeru ko je nujno potrebna. To velja sicer nasplošno, za katerokoli storitev sistema. Kar pa je v praksi pogosto tvegano in težko izvedljivo. Vsekakor, omejiti bi kazalo možnosti samodejnega izvajanja skript, svetuje pa se tudi uporabo protivirusnih programov in skrb za ustrezno ponastavljanje pravic dostopa do datotečnega sistema, kjer je to mogoče (NTFS) (privzete nastavitve namreč pogosto niso primerne).

Odjemalci e-pošte in novičarskih skupin MS Outlook in Outlook Express

Pri ranljivostih odjemalcev za elektronsko pošto Microsoft Outlook in Outlook Express je še posebej očitna potreba po ustreznem izobraževnju uporabnikov in ustrezni politiki ravnanja z e-pošto. Potrebna pa je tudi primerna politika ravnanja s programsko opremo (če program ni potreben, bi ga bilo potrebno deinštalirati).

Soležno vzajemno deljenje datotek (Peer to Peer file sharing)

Stvar zase pa je področje soležnega vzajemnega deljenja datotek. Tukaj se poleg tehničnih in sociooloških ranljivosti prepotentno pojavijo tudi pravni vidiki (npr. kršenje avtorskih pravic; neprimerne vsebine). Tukaj bi naj pomagala ustrezna politika dopustne rabe Interneta, pa tudi nadzor prometa v omrežju in drugih resursov (npr. porabe prostora na napravah za hranjenje podatkov), omejevanje pravic za inštalacijo programske opreme, uporaba posredovalnega strežnika (proxy server) za kontrolo dostopa kot tudi izstopno filtriranje (egress filtering) (čeprav prehod na uporabo protokola HTTP pri P2P (Peer to Peer) sistemih pomeni manjšo uspešnost te metode). Neizbežna pa je tudi uporaba ustrezne protivirusne opreme širom podjetja.

Preprosti protokol za ravnanje z omrežjem – SNMP (Simple Network Management Protocol)

Prav tako bi se naj uporabljalo le varne SNMP aplikacije pri administracij omrežja. Nadziralo pa bi se naj tovrsten promet (zlonamernež lahko pridobi obilo koristnih informacij o sistemu po tej poti). Svoj delež pri zaščiti imata tudi primerno filtriranje notranjega prometa in prometa SNMP - v konkretnem med notranjim in zunanjim omrežjem, kakor tudi primerna politika kodiranja podatkov, overovljanja ter ravnanja s pravicami uporabnikov sistema.

5.2 Varnost podatkov in prispodoba verige – ljudje kot najšibkejši del

Kaj pa utegne predstavljati najšibkejšo točko v danem informacijskem sistemu? V teoretični literaturi se pogosto navaja misel, da je sistem le toliko varen, kot je varen njegov najšibkejši del.

Praksa potrjuje takšno razmišljanje – in kaže na to, da smo najpogosteje ravno ljudje ta najšibkejši člen. Nadvse zanimiv je v tej smeri prispevek slovitega nekdanjega hekerja James-a Chapple-a o preizkušnji odpornosti informacijskega sistema danega podjetja pred vdori (Chapple, 2002, 14-17). Podjetje je "spreobrnjenega" hekerja najelo v ta namen. Sistem žaščite je bil navidezno zelo dober. Kritični podatki so se nahajali na zaklenjenih strežnikih, varnostne popravke se je redno nameščalo, nepotrebne storitve so bile onemogočene in nepotrebna programska oprema odstranjena. Prav tako so bila v uporabi močna gesla in ni bilo enostavnega načina za neposreden dostopa do strežnikov. Tej dolgi verigi varnostnih ukrepov navkljub, je Chapple-u uspelo uspešno vdreti v sistem in priti do najbolj skrbno varovanih podatkov v manj kot 30 minutah. "Podvig" mu je uspel s posrednim vdorom, tako da je izkoristil ranljivost, ki so jo predstavljale sorazmerno slabo zaščitene delovne postaje (predvsem delovna postaja administratorja).

Na podlagi tega Chapple poudarja, da hekanje ni linearno; izkušeni heker se po potrebi premika sem ter tja po omrežju in poizveduje, iščoč šibko točko. Ko to najde, jo vzame kot torišče za

napad na sistem: iz nje poskuša izvleči čimveč relevantnih informacij. Ko mu uspe doseči zadostno raven nadzora nad šibko točko, pogosto ustvari zadnja vrata (back door) in slabost zamaskira, da bi lahko neopaženo in neovirano nadaljeval z nepooblaščeno uporabo; često inštalira vohljača (sniffer) v namen zbiranja omrežnega prometa. V praksi se izkaže, da komercialna programska oprema za odkrivanje šibkih točk v sistemu sama po sebi ne zadostuje – to pa zato, ker bodisi ne odkrije vseh ranljivosti ali pa "odkrije" tudi neobstoječe. Izkušeni in odločeni heker pa bo temeljiteje testiral. Zato pa se kaže potreba po sistematičnem testiranju in rangiranju problematičnosti odkritih ranljivosti.

Pa tudi kar se tiče notranjih ljudi - po eni strani se tudi sredstva zaščite pred zunanjim grožnjami pogosto upravičeno uporabljajo tudi nasproti notranjim ljudem (insiders). Šokantna s svojo konkretnostjo je po svoje ugotovitev raziskave objavljene na spletnem nahajališču "The Economist" (The weakest link, 2002) v kateri se jasno poudarja, da je 70% varnostnih incidentov katerih posledice so ovrednotene na več kot 100.000 USD posledica dejanj notrajnih ljudi organizacije (insiderjev).
A ta sredstva pogosto ne predstavljajo dovoljšnje zaščito pred le-temi. Ocenjuje se, da obstaja manj kot kot 40% verjetnost razločevanja notranjega napada od legitimne uporabe omrežja. Kljub temu, bi naj orodja analize prometa omogočala zaznavo neobičajnih vzorcev prometa (kot je npr. neobičajna gostota prenosov datotek v oddelku, kjer so bile pred kratkim napovedane odpustitve). Včasih je proti insiderjem celo smiselno najeti pomoč zunaj podjetja; v zvezi s tem je možno uporabiti tudi sredstva kot so "lonci medu" (v principu strežniki-vabe, ki bi naj posnemali delovanje notranjega omrežja in zavarovali pravo omrežje pred napadalcem); slednji so se že pokazali kot koristno orodje tudi proti tem zlonamernim notranjim ljudem.

A če že govorimo o konceptu verige, lahko kot že rečeno zlahka ugotovimo, da je kar najpogosteje ravno človek najšibkejši del sistema. Kot se omenja v raziskavi omenjene publikacije (The weakest link, 2002), je predvsem potrebno imeti dobro v mislih besede enega najbolj znanih hekerjev, ko je ta pričal pred Komisijo Senata ZDA za vladno računalniško varnost: K. Mitnick je na podlagi lastnih izkušenj jasno poudaril, da mu je le redkokdaj bilo potrebno lotiti se tehničnega napada na sistem. Izpostavil je, da je človeška plat računalniške varnosti zlahka zlorabljena in stalno znova spregledana. Kljub vsemu podjetja porabijo velike zneske za požarne stene, naprave za šifriranje in varen dostop. Problem ni samo v tem, da je to sama po sebi parcialna rešitev in da pogosto te delne rešitve niso usklajene med seboj ali niso povsem v skladu s cilji in načeli podjetja. V njih se pravzaprav skriva skupna temeljna slabost – nobeno izmed teh sredstev se pravzaprav ne sooča zadovoljivo s temeljno ranljivostjo sistema – ljudmi.

V istem viru (The weakest link, 2002) se po drugi raziskavi ponuja elemente v podporo tej tezi: najbolj običajen način vdora v sisteme je preko družbenega inženiringa (social engineering). Raven varnosti se lahko bistveno poveča ravno preko zelo enostavnih in poceni rešitev, kakršne so vzpostavitev boljših gesel in njihove tajnosti (niti administratorji naj ne bi poznali gesla posameznih uporabnikov) in prakse, da se zaposleni odjavijo od računalnika ob odhodu.

Ugotavlja se, da je lahko v dobri meri na ravnateljevanju temelječ sistem (preko politik in postopkov) stroškovno zelo učinkovit. Istočasno pa se na primeru biometričnih sredstev potrjuje

misel, da lahko pomankljivi postopki onesmislijo še tako napredno tehnologijo. Navaja pa se izsledke neke raziskave, ki bi naj pokazala, da temu navkljub polovica vseh pisarniških delavcev ni nikoli bila deležna kakršnegakoli usposabljanja o varnosti. Prav tako naj bi po drugi raziskavi 73% družb nikoli ne zahtevalo od zaposlenih, da ponovno preberejo varnostne politike potem ko pristopijo k zaposlitvi; dve tretjini podjetij pa sploh ne preveri ali so zaposleni sploh prebrali tovrstno politiko (The weakest link, 2002). Glede na omenjeno menim, da bi verjetno bila smiselna uvedba izobraževanja porabnikov tudi s pomočjo prilagojene programske opreme, katere naloga bi bila glede na kontekst uporabe soočati uporabnike z najpomembnejšimi prvinami informacijske varnosti v danem kontekstu. Torej tudi preko opozarjanja in dajanja navodil oz. informacij glede na kontekst, na dano situacijo uporabe opreme. Prav tako naj ne bi bilo dopuščeno uporabniku nadaljevati z danim, neprimernim početjem (ali vsaj naj bi se nespoštovanje pravil zabeležilo in varno shranilo).

Zanimiva ugotovitev je tudi da, da bi se naj v sklopu varnostne politike zagotovilo odhod vseh zaposlenih slej ko prej na dopust – v namen preprečitve vzdrževanja nepravilnosti v sistemu s strani danega posameznika. Pomembno pa bi bilo tudi ponujati ustrezne napotke odgovornim za varnost, da bi tej ustrezno ravnali v primeru odkritja kršitev varnosti s strani poslovodnega osebja (The weakest link, 2002).

Narava ljudi pa je vzrok mnogim težavam tudi pri izvajanju fizičnega varovanja. Ljudje pogosto vidimo to, kar smo vajeni ali hočemo videti. Poleg tega, se običajno poskušamo izogibati konfliktu z drugimi ljudmi (npr. predvsem ko so le-ti visoko situirani v hierarhiji podjetja).

Posebej se izpostavlja potreba po kontroli pogodbenih strank, saj so dobro znani primeri, kjer so bili posredno ali neposredno vpleteni v zlorabe. Namreč, če že samo pravo osebje pogodbenih izvajalcev ni bilo krivo za zlorabe, pa so varnost ogrožali zlonamerni osebki, ki so se izdajali kot pooblaščeno osebje le-teh (Pepper, 2002, str. 22-23).

5.3 Varovanje informacij: vidik netveganosti (safety) in njeno zagotavljanje

Varovanje podatkov pa po drugi strani pomeni tudi obvarovanje pred škodnimi dogodki, za katerimi ne stojijo nujno neposredno ljudje, ki bi z lastnim aktivnih delovanjem pomenili grožnjo podatkom in informacijam. Tukaj smo na področju zagotavljanja netveganosti okolja – ta vidik se sicer ponavadi navaja bolj v neposrednem v zvezi z varnostjo ljudi. Obravnava drugih vidikov se ponavadi odvija po takem kopitu. In vendar se isti dejavniki, ki ogrožajo ljudi pogosto pomenijo (lahko tudi usodno) grožnjo varnosti podatkov in informacij (torej: pretežno celovitosti in razpoložljivosti).

Naslednji razdelek bo povzet po Dunn (2003). Del aktivnosti, povezanih z zagotavljanjem fizične varnosti se nanaša na zagotavljanje ustrezne netveganosti delovnega okolja in sistemov samih. V smeri doseganja tega, bi se naj podjetje najprej lotilo ustrezne analize načinov odpovedi (failure modes), ter s tem povezane analize nevarnosti. Temu pa sledi snovanje sistema blaženja tveganja nastopa varnostnih incidentov. Na samo tveganje je mogoče do določene mere vplivati na več načinov, v glavnem pa lahko ločimo tri področja delovanja: vplivanje na zanesljivost in kakovost sestavnih delov (preko preoblikovanja in/ali odvečnosti); povišanje notranje varnosti sistema (preko sprememb pri osebju, preoblikovanjem sistema kot sklopa komponent ter preoblikovanja postopkov). Nazadnje nam preostane še prilagoditev zunanje

varnosti. Običajno se vrstni red aplikacije posamezne vrste varoval giblje po omenjenem vrstnemredu. Omejitev na prevzem zgolj posemezne vrste varovanja pa praviloma ni dovolj.

Vendar obstajajo pomisleki (Ghosh, 2003, str. 6, 16-17), da pristop kot ga opisuje Dunn ni nujno najbolj primeren v vseh okoliščinah. Tradicionalni pristop torej zahteva najprej ugotovitev glavnih možnosti odpovedi sistema, nakar bi se naj ocenilo verjetnost in posledice vsake od njih posamezno; pri tem se predpostavlja, da je verjetnost multiple simultane odpovedi zelo malo verjetna in odprava predraga. Ne da bi se spuščal v podrobnosti naj samo poudarim, da ta pristop premalo upošteva posledice sočasnega nastopa in morda sinergije različnih dejavnikov. To pa ima lahko pri sistemih, katerih delovanje je z varnostnega vidika kritičnega pomena zelo hude, če ne celo usodne posledice - tukaj je za primer vzet vesoljski program Apollo 13. Zato sem mnenja, da bi se naj v primerih, pri katerih je s strokovno analizo ugotovljena verjetnost nastanka potencialno res izjemne škode posvečalo več pozornosti možnosti interakcije različnih dejavnikov. Torej več pozornosti, kot bi ocena verjetnosti nastanka škodnih dogodkov na prvi pogled kazala. To pa tako zaradi objektivne nesposobnosti napovedovanja in ocenjevanja prihodnjih dogodkov in njihovih posledic (nenazadnje tudi zaradi nepoznavanja/nesposobnosti pravilnega in popolnega poznavanja vseh merodajnih dejavnikov in povezav med njimi). A tudi zaradi subjektivne komponente ocenjevanja – kljub vsesplošnemu priseganju na znanstvemo metodologijo se v praksi pogosto izkaže, da smo pri presojanju in odločevanju pač ljudje – kar bi naj pomenilo, da čustva, nepovabljena, vstopajo in vplivajo v proces našega delovanja, kar lahko prinaša nepredvidljive (in neracionalne), gotovo pa neoptimalne izide. Ob povedanem pa ostaja samoumevno, da so celotni stroški lastništva neke rešitve (in dotične pričakovane koristi) konec koncev eno izmed glavnih vodil oblikovanja zasnove sistema oz. njegovih delov. Pri tem nam je lahko cilj, da se v primeru odpovedi sistem preklopi v tak način delovanja, kjer ne more imeti nedopustnih škodljivih posledic na okolje in svoje naloge ne opravlja več (fail-safe) ali da kljub odpovedi sistem deluje še naprej (fail-operate), to pa preko ustreznih rezervnih komponent ali celo odvečnosti.

Orodja za zagotovitev netveganosti sistema (oziroma njegovega vpliva na okolje) – oz. gradniki tega podsistema so lahko naslednji: od mehanizmov za zagotavlje pravilnosti delovanja kar se tiče vhodov/izhodov računalniškega podsistema in vhoda/izhoda efektorja. Lahko pa se poslužujemo tudi uporabe zapornih (prekinitvenih) mehanizmov (interlocks) (s tem bi upoštevali pogoje fizičnega okolja) ter stražnih mehanizmov (watchdog timer) za izključitev efektorja v primeru okvare računalniškega sistema. Zadnja linija v bitki za varnost pa je mehanizem za ročni izklop v sili, pod kontrolo operaterja.

5.4 Nekaj vidikov ravnanja z varnostjo podatkov in informacij v podjetju.

V 4.poglavju sem se dotaknil nekaterih vidikov varnosti podatkov in informacij v podjetju - tematik pomena zaupanja pri poslovanju, o nevarnostih zlorabe Interneta v podjetju in problematike kraje podatkov s strani notranjih ljudi. Proti koncu tega razdelka bo govora o nekaj možnih poti, kako se spopasti s težavami pri ravnanju z varnostjo, da bi podatke in informacije branili pred pretečimi grožnjami; a do tega bom prišel preko obravnave izsledkov raziskave o ravnanju z varnostjo omrežja v podjetju, kjer se bo razgalilo nekaj občutljivih področij.

5.4.1 Primer uporabe omrežja v podjetjih z vidika varnosti informacij

Raziskava o uporabi Interneta v podjetjih je podkrepila domneve o ljudeh kot resnem viru ranljivosti (BECC, 2001, str. 755-764). Mnogo zaposlenih Internet napačno uporablja ali zlorablja, najsibodi zaradi pomanjkljivega razumevanja nevarnosti, pomanjkanja ozaveščenosti ali škodoželjnosti (BECC, 2001, str. 751). Raziskava je pokazala, da je bilo v nekaterih primerih okoli 80% uporabe Interneta v podjetju za neposlovne namene – in vendar je bil zaznan občutni odpor zaposlenih do kakršnihkoli omejitev.

Naprimer, zaposleni so izkazali velika pričakovanja v zvezi z zagotavljanjem zasebnosti njihove e-pošte[9]. Podobno visoka so bila pričakovanja o zasebnosti dostopa do svetovnega spleta (kjer bi naj bila mogoče uporaba mehanizmov beleženja, nenazadnje za kontrolo dostopa do spletnih vsebin in nadzora nad poskusi zaposlenih hekanja zunanjih nahajališč). In vendar so zaposleni kot prej omenjeno pokazali izrazit odpor do kakršnegakoli spremljanja (monitoring) e-pošte in nasploh dostopa do Interneta preko beleženja in poročanja iz dnevnikov – kar seveda zmanjšuje praktične možnosti zmanjšanja tveganj kot so hekanje in uporaba virov v neposlovne namene.

Še bolj sovražna je bila reakcija na predlog nadzora (surveillance) nad njihovimi aktivnostmi v Internetu. Pa tudi sicer primernih in zadostnih sredstev s katerimi bi podjetja uresničevala kontrolo nad odgovornostjo zaposlenih (overovljanje, ukrepi proti lažnemu zanikanju, vidnost preko spremljanja in nadzora) v večini primerov niso bili na razpolago. To velja predvsem kar se tiče pomanjkanja zadostnega števila pooblaščenih ljudi, ki bi imeli čas in sposobnost vršiti nadzor. Z vidika podjetja bi prav tako bila smiselna uvedba cenzure (to pomeni omejevanje namernega ali nenamernega dostopa in ustvarjanja dvomljivih in občutljivih vsebin). To bi bilo mogoče uvesti preko klasifikacije spletnih nahajališč in shem reguliranja vsebine – to pa tako iz zakonskih kot moralnih razlogov (in tudi, jasno, ravnanja z odnosi z javnostmi). Problem pa je "zgolj" v tem, da so tudi tukaj zaposleni izkazali precejšnjo mero sovražnosti do takih ukrepov (bodisi do omejevanja dostopa do spletnih vsebin kot skeniranja e-pošte za neprimerne vsebine). Zaposleni v preučevanih podjetij so izkazali visoko stopnjo pričakovanja, da bo podjetje zaupalo v njihovo sposobnost primernega in varnega ravnanja pri uporabi Interneta – to pa je v nasprotju s potrebo podjetja po omejitvi uporabe Interneta.

Raziskava je izpostavila tudi v splošnem pomanjkljivo poznavanje politike s strani zaposlenih. Dodatno pa so bile sankcije pogosto sporne oz. nejasne, prav tako se je izkazala potreba po globljem razjasnjevanju dejstev okoli lastništva spletnih vsebin (ali so last podjetja ali zaposlenih) (BECC, 2001, str. 755-764). Nazadnje pa v tem viru priznava pomen spoštovanja načel etike (prijaznosti, poštenja in pravičnosti, zaupanja, pripravljenosti do deljenja informacij in pomoči drugim).

Skratka, pokazala se je visoka stopnja ogroženosti sistema (ob pomanjkljivi ozaveščenosti), pomanjkanju holističnega pristopa pri razvoju varnostne politike in v zvezi s tem prevelikim zanašanjem na tehnična sredstva ob zanemarjanju pravnih vidikov (zaščite avtorskih pravic in drugih zakonskih zahtev) – to pa predvsem v luči ranljivosti, ki jo za podjetje predstavljajo ljudje

[9] Tukaj bi naj sicer bila načeloma možna uporaba spremljanja za kontrolo nad problemom poslovne zaupnosti, nevarnosti nadlegovanja.

oz. njihovo vedenje. Res pa je, da pomanjkanje sredstev – in pravzaprav predvsem časa – vodi ravno v rastočo nujnost zanašanja na opremo za take naloge. Pri tem vir poudarja, da tudi kadar so se zaposleni zavedali, da neko vedenje ne ustreza predpisani politiki, so pogosto to enostavno zanemarili – tukaj pa se kaže potreba bo ustreznem sankcioniranju v smeri uveljavljanja politike; pa tudi sporazumno omejevanje neposlovne uporabe Interneta/drugih sredstev podjetja. Kot že omenjeno pri raziskavah RIS-a, pa je potrebno upoštevati tudi "eksternalije" neposlovne uporabe Interneta – pridobljene veščine lahko zaposleni uporabi tudi v poslovne namene. Polega tega pa se navaja tudi dejstvo, da je dostop do Interneta (oziroma njegov obseg) pogosto viden kot privilegij, kar je mogoče uporabljati pri pogajanjih o pogojih nagrajevanja.

5.4.2 Izhodišča in ukrepi zagotavljanja varnosti podatkov in informacij v podjetju

V namen zagotavljanja varnosti (BECC, 2001, str. 755-764) gre izpostaviti potrebo po namenjanju znatno višje pozornosti izobraževanju in usposabljanju – tudi (ali še posebej) vodilnih delavcev, kateri bi naj tudi dajali zgled zaposlenim. Vir poudarja potrebo po formalnem sistemu izobraževanja in ozaveščanja zaposlenih o problematiki varnosti, ustreznega preverjanja pridobljenih sposobnosti pred samo uporabo sredstev, primerne pomoči in ozaveščanja, ki bi naj šli z roko v roki z uporabo, glede na kontekst.
Omenja pa se, da se je pri vsem povedanem potrebno zavedati, da bodo določeni zaposleni vedno kršili pravila, ne glede na stopnjo zaščite. Zato bi naj bilo potrebno uporabiti raznovrstni pristop k zagotavljanju varnosti – ključna področja so (BECC, 2001, str. 755-764): zagotavljanje razvoja v osnovi zelo varnega sistema, posvetitev dovoljšnje pozornosti človeški plati varnosti, dodeljevanje in nadzorovanje odgovornosti zaposlenih, pa tudi minimalno zanašanje na vedenje zaposlenih oziroma širšo uporabo nadzorne opreme. To pa pomeni, da tudi ta vir prepoznava potrebo po vzpostavitvi ustreznih varoval, ki bi naj ne dopuščala zaposlenemu, da nadaljuje z določeno aktivnostjo, če ni bilo predhodno ustrezno poskrbljeno za varnost.

Vir navaja, da bi kazalo obširneje uporabiti koordinirani pristopa ravnanja z varnostjo, nenazadnje preko formalne organizacije, ustrezne razpoložljivosti sredstev, formulacije koordiniranih politik, razdelitev pristojnosti, spopadanja z nespoštovanjem pravil kot tudi občasnega preverjanja primernosti politik – pač v skladu z hitrim spreminjanjem varnostne situacije v poslovnem, sploh e-okolju. Potrebno pa je prav tako spodbuditi sodelovanje med različnimi akterji. To pa velja tudi v odnosu do poslovnih partnerjev, kjer je prav tako potrebno prepričevanje.

Za uresničevanje povedanega v zgornjih treh odstavkih se predlaga vrsto prijemov (BECC, 2001, str. 728, 755-764), o katerih bo govora v naslednjih treh odstavkih. Ugotovitve se sicer nanašajo na zagotavljanje varnosti pri uporabi Interneta, naj pa pripomnem, da sam menim, da je te ugotovitve smiselno in mogoče v veliki meri posplošiti tudi na druga področja, kjer bi se naj zagotavljalo varnost. Tukaj ne mislim le na zagotavljanju varnosti komunikacij v splošnem, temveč tudi pri uvodoma omenjenem problemu kraje podatkov oz. pri prekinitvah v transakcijah. Prav tako bi se naj spodnje ugotovitve sicer nanašale na okolje, ki ga predstavlja podjetje – mislim pa, da je na njih mogoče gledati tudi kot na del širše obravnave (kakršna bo tekla v 7. poglavju, glede sodelovanja države, gospodarstva in vojske).

V namen doseganja višje ravni varnosti zagovarja v prejšnjem odstavku omenjeni vir potrebo po sodelovanju:

- izobraževalnih inštitucij (zaradi izobraževanja javnosti – sedanjih in bodočih e-porabnikov; za ponujanje ustreznega usposabljanja sedanjih zaposlenih in managerjev o dopustnih ravnanjih; pa tudi za izobraževanje samih IT-strokovnjakov kar se tiče varnosti).

- medijev: zaradi informiranja javnosti o obstoječih tveganjih kot tudi nasplošno o problematiki varnosti (po možnosti čimbolj objektivno).

- ustvarjalcev tehnologij: le-ti bi naj razvijali in ponudili ustrezno programsko in strojno opremo.

- regulatorna telesa kot so državne inštitucije bi naj ponudila ustrezno regulativo kot podlago za napore za večjo varnost.

- organi podpore panogi oz. gospodarstvu (kot npr. Gospodarska zbornica) bi naj ustvarili in podpirali formalne interesne skupine, kot bi se to pač pokazalo za potrebno – v namen zaščite pred novimi tveganji in napadi.

- podjetja: bi naj skupaj z osebki iz prejšnje točke podpirala raziskovanje – od samega postavljanja izhodišč do izvedbe raziskav in preko primerne publikacije izsledkov analiz doprinesla k razširjanju znanja in ponujanju na razpolago podjetjem in stroki; pri tem je mišljeno tudi raziskovanje etičnih vidikov te problematike.

- varnostni strokovnjaki: le-ti bi naj skrbeli za neprestano nadgrajevanja svojega znanja in sposobnosti in tudi preko tega skrbeli za razvoj ustreznih politik in programov ravnanja za podjetja.

Ravno v smeri doseganja boljše organizacije e-poslovanja se pri (BECC, 2001, str. 264-265) poudarja pomen ustreznega izobraževanja in usposabljanja zaposlenih, opozarja pa se tudi na potrebo po posvečanju primerne pozornosti vidiku medsebojne združljivosti različnih rešitev. Pomembni gradniki zaupanja v medpodjetniškem e-poslovanju pa so med drugim (BECC, 2001, str. 603):
- razpoložljivost in preglednost dokazov (tj. sposobnost identificirati, locirati v fizičnem prostoru in oceniti vsakega od predmetov menjave, drugo stranko in tržnega prostora ter drugih vmesnih členov. Koristna je prisotnost posrednikov za identifikacijo in lokacijo kot so to digitalni certifikati – pa tudi za ocenjevanje kot so inšpekcijski certifikati.
-reputacija oz. priporočila s strani izkušenih in zaupanja vrednih strani; znaki odobritve.
-varnost transakcij s podatki – zaupnost, integriteta, overovitev in zaščita proti lažnemu zanikanju (non-repudiation) in alternativ, ki zmanjšajo nevarnost razkritja podatkov (anonimnost in pseudonimnost).
-varovalke proti izpostavljenosti tveganju, kot so garancije, zavarovanje.

Velja pa tudi, da so v sodobnem svetu spreminjajoče se okoliščine terjale in bodo tudi v prihodje terjale prilagajanje postopkov, osebja in njegovega znanja in sposobnosti. To pomeni, da mora osebje spremeniti podobo o sebi in dojemati se kot skupnost, temelječo na znanju – mora

spreje(ma)ti novo kulturo z bistveno prilagodljivejšimi delovnimi vlogami. Čedalje bolj se uveljavljajo mrežne organizacijske oblike, kjer je delo razdeljeno na začasne time ljudi, ki so sicer iz različnih oddelkov. Za uvedbo sprememb je nujno potrebno ustvariti ugodno okolje, dovzetno za spremembe in zagotoviti ustrezni projektni management, priporočljivo je imeti v mislih Cochrane-ova načela sodelovanja (sodelovanje, navdušenje, izogibanje duplikaciji, minimiranju pristranskosti, stalnem posodabljanju, zagotavljanju merodajnosti in dostopnosti, izboljšanja kakovosti in neprekinjenosti) (BECC, 2001, str. 728).

6. Sociološki in psihološki ter ekonomski vidiki varnosti

V dosedanji obravnavi sem najprej poskušal lotiti se splošnejšega pregleda stanja glede varnosti podatkov in informacij doma in v svetu. Poskušal sem pogledati, kakšne grožnje pretijo varnosti podatkov pa tudi pretežno iz tehničnega vidika vsaj grobo nakazati kje so vzroki težav in kje bi morda šlo iskati rešitve. Večkrat sem izrecno omenil, da je za uspešno delovanje na tem področju razumevanje in upoštevanje človeškega dejavnika ključnega pomena. Znano je, da imajo v družbenoekonomskem sistemu v katerem živimo ekonomske spodbude odločilno vlogo pri vedenju ekonomskih subjektov. Zato menim, da je preiskovanje ekonomskega ozadja varnosti podatkov in informacij preprosto nuja. Zdaj bom poskušal tolikokrat nakazano in grobo orisano tudi poglobiti.

6.*1 Sociološki in psihološki vidiki varnosti*

Na podlagi lastnih raziskav o ekonomskih, sociooloških in psiholoških vidikih varnosti svetuje tudi Odlyzko (2004), da kaže nameniti več pozornosti drugim, netehnološkim vidikom, če si res želimo razumevanja problematike varnosti v realnem svetu. Potrebno se je namreč zavedati že samo obstoječega ekonomskega ozadja – o potrebi po tehtanju med koristmi in stroški dane rešitve. Tudi s tem v mislih bi bilo dobro preučiti spodbude posameznih igralcev, saj mnogi imajo interes preložiti stroške varnosti na druge subjekte ali pa uporabiti sredstva zaščite npr. za ohranjanje monopolne situacije (zlorabo tržnega položaja).

Vsebina informacije zatorej ni edini merodajni dejavnik pri opredelitvi problematike njene zaščite, ampak je potrebno upoštevati še kopico drugih, tj. kontekst. Poleg omenjene ekonomske plati pa nastopajo sicer še npr. tako sociološki kot psihološki dejavniki – in vsi ti dejansko združno ovirajo uspešno uvedbo in uporabo varnostnih mehanizmov.

Odlyzko poudarja, da je eden osnovnih problemov pri varnosti podatkov in informacij v sorazmerni nezdružljivosti človeške narave s formalnimi sistemi – izkaže se namreč, da je izjemno težko uravnovesiti zahteve po varnosti na eni strani ter fleksibilnostjo na drugi. Ljudje smo pogosto nagnjeni prilagajati pravila našim željam – in ne obratno. Seveda smo tudi pri svojem medsebojnem delovanju pod vplivom kulture, ki jo v dani skupnosti delimo. Prav tako se avtor tega diplomskega dela sam spominjam na (pogosto negativne) učinke dejstva, da se ljudje pri svojem vedenju ravnamo po skriptah in stereotipih, sklepamo na podlagi ne vedno najbolj točnih kognitivnih hevristik in se nanašamo tako ali drugače na bolj ali manj pomanjkljive kognitivne zemljevide – pri tem pa smo pogosto zelo togi pri spreminjanju le-teh, tudi v primeru (racionalno gledano) precej očitnih disonanc. Ravno tako je pogosto na dlani spoznanje, da je izid rešitve nekega problema odvisen od načina, kako se ta problem predstavi.

Težava pa je tudi v tem, da formalne sisteme gradi ožja skupina ljudi, ki so formalnih sistemov navajeni – običajno pa imajo le-ti bore malo potrpljenja za omenjene človeške dejavnike in za družabne odnose nasploh, saj od drugih ljudi pričakujejo razumevanje in vedenje podobno svojemu.

Po drugi strani so te iste človekove značilnosti tiste, ki lahko ugodno prispevajo k varnosti, saj se ljudje bolje znajdejo v negotovih, nedoločenih situacijah – sem pa sodijo tudi družbene okoliščine. In ravno takšne značilnosti imajo često situacije v stvarnosti, kjer potekajo e-transakcije v določenem kontekstu – to pa omogoča neko dodatno raven varnosti. Naj pojasnim: kot primer navaja Odlyzko sorazmerno hiter uspeh in široko razširjenost faksirnih naprav: čeprav faksiran podpis vis-a-vis originalnemu je pravzaprav bistveno zmanjšal objektivno raven varnosti podpisa je ta tehnologija bistveno pripomogla k gospodarskemu razcvetu svetovnega gospodarstva. To pa zato, ker ljudje ocenjujemo varnost glede na kontekst (družbeni, pravni, ekonomski) – in je varnost dejansko do neke mere od teh odvisna.

Nadaljnji problem pri varnosti informacij v povezavi z ljudmi je po istem viru v naslednjem. Na mnogih področjih je mogoče poznavanje tehnologije oddaljiti od končnih uporabnikov – in pri tem varnost ne trpi. Pri varovanju informacij temu v splošnem žal ni tako (izjeme so lahko npr. SSL/TLS). Življenje v informacijski družbi pomeni čedalje večjo vpletenost ljudi s tehnologijo – in ljudje so kot rečeno prav najpogostejši vzrok ranjivosti sistemov. Namreč, kljub obširni razpoložljivosti informacij o tematiki varnosti se še vedno (vedno znova) dogaja, da ljudje nasedajo na različne zlonamerne trike, kot je npr. "nigerijska potegavščina" in različni primerki t.i. družbenega inženiringa.

Zato pa, čeprav se je tudi avtorju tega diplomskega dela zdela kot najbolj naravna rešitev vpeljava bolj obsežnega in boljšega izobraževanja – bi se glede na povedano reklo, da se je to resda izkazalo kot potrebno, nikakor pa ne zadostno – že samo zaradi naraščajoče zapletenosti ITkT sistemov. Pa tudi na psihološki oz. sociološki ravni se ljudje in skupnosti ljudi ravnamo po neki vrsti analize stroškov in koristi (cost benefit analysis) – sprejemamo rešitev problema le do tiste mere, dokler čutimo, da nam neugodnosti od dodatne varnosti ne presežejo koristi od le-te (primer je cestno-prometna varnost). Kot v realnem svetu smo tudi v e-različici nekako pripravljeni živeti v ne povsem varnem okolju. Odlyzko pa opozarja, da je pri tem problem tudi v tem, da sta lahko v kibersvetu bodisi hitrost napadov kot njihova magnituda mnogo večji.

Da pa se ne kaže ravno vdati črnogledosti je razvidno iz dejstva, da so tudi tisti posamezniki, ki namerno škodijo sistemom – zgolj ljudje – in se prav tako ne vedejo vedno racionalno, delajo napake in se soočajo z zapletenostjo sistemov, katere tako ali drugače napadajo. Pa tudi primer boja medijev plačljive televizije s pirati jasno kaže, da ustrezna uporaba nabora pravnih, tehnoloških in poslovnih prijemov omogoča ohranitev rasti in donosnosti dane dejavnosti kljub nevarnostim in škodam.

6.2 Ekonomika omrežij, nasprotna izbira, tragedija skupnega in varnost

Podobno meni Anderson (2004, str. 1), da je mogoče doseči občutnejši napredek pri zagotavljanju varnosti le, če se ne omejimo na tehnicističen pogled na varnost (uporaba boljših modelov politik kontrole dostopa, preverjenih požarnih sten, boljših načinov zaznavanja vdorov

in zlonamerne kode, boljših orodij za evaluacijo sistema) – pogled bi naj bilo torej potrebno razširiti. Pri tem bi naj v izjemno pomoč lahko bil mikroekonomski inštrumentarij (mrežne eksternalije, asimetrija informacij, nasprotna izbira, odvračanje odgovornosti, tragedija skupnega).

S teorijo ekonomike omrežij je tako mogoče zelo dobro pojasniti zakaj smo priča toliko varnostnim luknjam v programski opremi in tako počasnem krpanju le teh (t.i. Microsoftova filozofija). Teorija predpostavlja naslednje: da je koristnost izdelka sorazmerna količini njegovih uporabnikov; obstoj visokih stalnih stroškov in zelo nizkih mejnih stroškov; visokih stroškov za uporabnike pri prehodu med različnimi tehnologijami. Glede na povedano obstaja tendenca uveljavljanja nekaj dominantnih podjetij na takih trgih. Tukaj pa zaradi zelo pozitivne povratne informacije "zmagovalci" še dodatno utrdijo svoj položaj tako, da si pridobijo zanimanje proizvajalcev komplementarnih izdelkov – in tako še dodatno ojačajo svoj položaj ter otežkočajo položaj konkurence. Najpomembnejši zaključek pa je, da je izjemnega pomena za nov izdelek hiter nastop in uvedba. Z vidika proizvajalca danega izdelka pa je tudi ekonomsko racionalno, da dajo na trg izdelke, ki ohranijo višjo vrednost v očeh proizvajalcev komplementanih dobrin preko višje uporabnosti in prilagodljivosti – čeprav ob tudi znatno nižji prijaznosti do uporabnika ter višjimi stroški podpore, s katerimi se ta mora soočati – ter dejstvom, da je za uporabnike težje zagotoviti ustrezno varnost.

Zaradi logike, na kateri temelji ekonomika omrežij smo prav tako priča dejstvu, da proizvajalci pogosto trmasto vztrajajo pri vpeljavi nekega lastnega standarda, namesto da bi uporabili dobro znanega in testiranega. Uporabljajo npr. lastne patentirane algoritme (čeprav so le-ti po naravi pomankljivi). To vse z namenom, da bi povečali vezanost uporabnikov na njihove rešitve. Pri tem jih varnost takih rešitev pravzaprav veliko ne zanima.

Anderson (2004b, str. 6) omenja nekaj raziskav o procesih odpravljanja hroščev v programski opremi v praksi. Omenja se IBM, za katerega je veljalo, da se je lotil odpravljanja hroščev operacijskega sistema osrednjih računalnikov (mainframe computers) šele osmič, ko so bili poročani. Zanimiva pa je tudi raziskava o optimalni pogostosti nameščanja varnostnih popravkov z vidika porabnikov. Namreč, za precej racionalno se je izkazala praksa, da kupci ne namestijo popravkov tem prej, ko so ti na razpolago, to pa zaradi tveganja, da bodo po namestitvi popravka ključni sistemi odpovedali – optimalni zamik bi naj znašal od treh tednov do enega meseca. O aktualnosti tega problema se prepričamo že samo s tem, če se spomnimo na sedanje zaplete v zvezi s paketom popravkov SP2 (service pack 2) za MSWindowsXP in povzročeno nejevoljo pri številnih podjetjih (med njimi je tudi IBM), pri katerih je stabilnost ključnih aplikacij seveda osrednjega pomena.

Prav tako pa proizvajalci programske opreme odlašajo z odpravo ugotovljenih hroščev, ker preprosto predstavlja postopek testiranja popravkov, zbiranja popravkov v servisni paket in razpečevanjem velikemu številu kupcev določen strošek. Velja pa tudi, da je lahko interes državnih oblasti, da proizvajalce spodbujajo k zakasnjeni javni objavi napak, zaradi uporabe odkritih ranljivosti (domnevno) pri nalogah zaščite državne varnosti – popravki naj bi bili obljavljeni šele, ko jih tretji začnejo izkoriščati.

Problem predstavljajo prav tako zaskrbljenost podjetij o lastni podobi v javnosti. Zato podjetja pogosto odlašajo z objavo ugotovljenih hroščev do trenutka, ko niso tako ali drugače prisiljeni v to (nenazadnje tudi zaradi informacijske asimetrije v povezavi z odnosom principal - agent med ravnateljstvom in lastniki).

Zaradi zgoraj povedanega Anderson navaja (2004b, str. 10), da bi naj bila dana prednost programskim izdelkom za katere je znano čimbolj obširno testiranje, po načelu vzporednosti (predvsem pomembno je obširno beta-testiranje).

Prav tako Anderson (2004b, str. 9-10) opozarja na potencialno negativen vpliv nizke vertikalne integracije pri proizvodnji programske ali strojne opreme (varnost je odvisna od interakcije strojne in programske opreme iz različnih virov). To bi naj veljalo še sploh v povezavi z zakonodajo, kakršna je Evropska direktiva o elektronskem podpisu (po določbah le-te je imetnik odgovoren za morebitne varnostne incidente). Takšna regulativa lahko namreč še bolj spodbuja proizvajalce, da uporabijo lastne, bolj ali manj obskurne oblikovanje in mehanizme pri izdelavi svojih proizvodov (zaradi logike, izhajajoče iz ekonomike omrežji, kot maloprej opisano).
Nadaljnji nauk izhajajoči iz predpostavk te teorije je dejstvo, da so proizvajalci motivirani postaviti cene glede na zaznano vrednost za uporabnike in pri tem na široko uporabljati diskriminacijo cen (in ustrezno prilagoditev izdelkov); tukaj se varnost izdelka prilagaja dani cenovni politiki. Opozoriti pa gre (Odlyzko, 2004a), da težnja k cenovni diskriminaciji nosi s seboj tudi probleme zasebnosti, ker organizacije težijo k pridobitvi (na bolj ali manj prikriti način) čimveč informacij, ki bi jim omogočile karseda popolno diskriminacijo cen.

Sorodno temu je spoznanje o smotrnosti uporabe kontrole nad tržnimi potmi s strani proizvajalcev, spodbujanju razvoja proizvajalcev komplementanih dobrin. Sem sodi pa tudi dejavnost v zvezi s snovanjem relativno nezdružljivih sistemov, katerih se je težko lotiti s povratnim inženiringom (reverse engineering) – in seveda poskušanjem zaobiti podobne zaščite pri konkurentih. Primeri, ki jih Anderson navaja so npr. omejevanje uporabnosti neoriginalnih rezervnih delov oz. potrošnega materiala. Primer poskusa diferenciacije izdelka in povišanja stroškov zamenjave dobavitelja pa je pravzaprav tudi Microsoftova storitev overovljanja “Passport”).
Prav tako je možno pojasniti, zakaj se dogaja, da sorazmerno slabi izdelki izrivajo iz trga boljše (nasprotna izbira), kar je logičen pojav ob znatni asimetriji informiranosti med prodajalci in kupci; to pa je še posebej potencirano, kadar preizkuševalec/ocenjevalec izdelka ni isti kot pa osebek, kateri trpi posledice morebitnega napačnega delovanja le-tega. Kot primer slednjega lahko razumemo situacije, kjer management kupi opremo danega znanega, uveljavljenega ponudnika z relativno močno blagovno znamko, čeprav ta ni niti nujno najboljša možna – to pa zato, ker – paradoksalno – nadzorni mehanizmi tako vedenje morda celo podpirajo in spodbujajo kot dobro gospodarjenje.

Iz priporočil v zgornjih nekaj vrsticah razberem potrebno nameniti posebno pozornost nakupu opreme, ki bi naj bila neposredno ali vsaj posredno (certifikacija pooblaščenih ocenjevalcev) potrjena s strani zaupanja vredne tretje strani (po možnosti kake državne ustanove). Predpogoj za učinkovitost tega zamisli pa tiči – ponovno – v postavitvi in izvajanju ustrezne politike spodbud (zakonskih, ekonomskih) vis-a-vis ocenjevalcev, kateri bi naj dejansko čim bolj objektivno

zasledovali svoje delo. Pomankljivi (tudi) na tem področju bi naj bili naprimer znani "Common Criteria" (Anderson, 2004a, str. 1, 6), ker se je menda v praksi izkazalo, da so se ocenjevalci pogosto uklonili volji svojih komitentov in niso delovali v korist uporabnikov sistemov – ker ni bilo predvidenih ustreznih sankciji ali se te niso izvajale pravilno. Največji problem pa bi naj bil po istem viru, da lahko pravila kakršna so Common Criteria pomenijo neupravičeno prerazporeditev odgovornosti za varnost delovanja sistema od proizvajalca na uporabnika – obenem pa neveščemu uporabniku dajo nek neutemeljen občutek varnosti – kar pa ima lahko zelo neugoden vpliv na varnost. Naj se pa poudari, da je omenjeni problem zares pereč le kadar se tiče tistih področij, ki so kritičnega pomena za organizacijo – npr. kjer je pod vprašajem konkurenčna prednost podjetja.

7. Vlaganja v varovanje informacij

7.1 Ocena donosnosti

Kot na kateremkoli drugem področju, če smo že prišli do spoznanja, da imamo problem, se je pač smiselno vprašati, kako ukrepati – kako alocirati redka sredstva, ki jih imamo na razpolago na takšen način, da bodo vlaganja sorazmerna potrebam in da se bo iz vloženih sredstev izcimil kar največji možni izplen v obliki povečane varnosti.

Kljub vsem dosedaj opisanim težavam je mogoče ugotavljati, da ozaveščenost organizacij o pomenu varovanja podatkov in informacij vendarle raste.

Ghosh omenja, da bi naj pri poskusu ovrednotenja implikacij varnosti upoštevali oceno vrednosti informacij, ki bi izgubljena ali izgubljenega produkcijskega časa medtem ko je sistem neuporaben – to pa primerjati z denarno vrednostjo vložka v varnost, ki bi bil lahko odvrnil napad (Ghosh, 2003, str. 8).

Večja ozaveščenost pa spodbuja osebke k iskanju bolj konkretnih, dodelanih metod in pokazateljev donosnosti vlaganj v varnost informacij, katerih popularnost dejansko zadnja leta narašča. Ena najpopularnejših je ROSI (return on security investment). Kot pa pogosto pri novostih se tudi tukaj dogaja, da je še veliko nejasnosti in nerazumevanja okoli teh mer (Gordon, Loeb, 2002, str. 28).

Naprimer, pogosto se dogaja, da se pri ocenjevanju uspešnosti investicij uporablja računovodski pojem ROI (donosnosti na vložena sredstva). Dejansko pa to temelji na zgodovinskih vrednostih, potrebno pa bi oceniti bodoče vrednosti relevantnih tokov (kar bi kazalo na uporabo koncepta IRR (notranje stopnje donosa) za ROSI.

In vendar – se tudi tukaj opozarja (Gordon, Loeb, 2002, str. 30), da bi želja po zasledovanju maksimalne IRR zlahka pripeljala (in dejansko v mnogih primerih pripelje) do napačne odločitve. Investicijo bi se naj iz finančnega vidika ocenjevalo glede na maksimalno neto razliko med sedanjo vrednostjo donosov na eni strani in vloženih sredstev na drugi – torej maksimalno NPV (Neto sedanjo vrednostjo investicije). Mnoga podjetja pa prav tako napačno tolmačijo vlogo pokazateljev, kot sta IRR oz. NPV pri ocenjevanju uspešnosti investicij v varnost – to pa v smislu, da ne upoštevajo dejstva, da so le-ti po svojem bistvu ex ante pokazatelji (torej se nanašajo na predvidene vrednosti relevantnih spremenljivk v prihodnosti). Za oceno uspešnosti

tovrstnih investicij bi se naj torej uporabljalo ex post mere oz. primerjalo bi se naj tiste prve s temi drugimi. Kar pa je praviloma zelo zahtevna naloga.

Zasledovanje IRR pa ni najbolj smiselno še iz drugega razloga. Pogosto smo namreč soočeni z napačnim prepričanjem, da je smiselno vlagati v zagotavljanje varnosti do točke, kjer so željene investicije enake pričakovani škodi, ki je posledica varnostnih incidentov. Kot povedano v zgornjih nekaj vrsticah, bi naj bil (finančni) cilj podjetja maksimiranje razlike med koristmi in stroški investicije v varnost. Tukaj pa je vsaj v namen razumevanja lahko v pomoč mikroekonomski inštrumentarij – konkretno, dodatne (oz. mejne) koristi in stroški. Namreč, nima smisla povečevati vrednost investicije v varnost do točke, kjer je dodatni strošek večji od dodatne predvidene koristi. Gordonovi teoretični izračuni so pokazali, da bi naj optimalna raven investicij v varnost ne presegala več kot približno eno tretjino pričakovane škode.

7.2 Ocena soodvisnosti

A pravkar navedene mere se nanašajo na posamezno podjetje. In vendarle so različni osebki v stvarnosti soodvisni. Kadar pa smo priča pojavu soodvisne varnosti – ko je torej varnost danega osebka odvisna od varnosti drugih subjektov – je izjemnega pomena obstoj primernega spleta spodbud, ki naj usmerjala vse subjekte k bolj ali manj skladnemu ravnanju okoli zagotavljanja varnosti (Kunreuther, Heal, Orszag, 2004).

V omenjenem članku me opisana situacija pravzaprav spominja na mikroekonomski koncept t.i. "pripornikove dileme". Če posamezni osebek vlaga v zagotavljanje varnosti si lahko zagotovi določene koristi iz tega naslova. Ne glede na to, če tudi drugi subjekti ne ravnajo podobno, vlagatelju ne more nikakor uspeti zmanjšati tveganja do te stopnje, da bi utegnilo vlaganje biti upravičeno. Zato v končni fazi sploh ne vloži v varnost (vsaj ne do stopnje, ki bi bila sicer zaželjena). Čeravno je potencialni varnostni incident zanj lahko tudi usoden. In čeprav bi tako vlaganje morda bilo v interesu širšega okolja.

Zaradi povedanega pa je v primerih, kjer je javni interes ogrožen, intervencija države prepotrebna. Pa tudi v podjetjih – tam kjer je več enakovrednih in varnostno soodvisnih organizacijskih enot ali kjer obstaja morda ena ali nekaj vplivnejših enot, je izrednega pomena, da čimveč enot (oz. glavne enote) združno uvede in izvaja ustrezno politiko zagotavljanja varnosti. Čimveč enot sprejme to zavezo, tembolj so druge motivirane, da naredijo isto. In s takšnim delovanjem dejansko zmanjšajo tveganje, kateremu so izpostavljene vse enote - druge kot tudi same.

Na ravni podjetja, panoge ali gospodarstva so lahko spodbude bodisi v obliki samoregulative ali regulative in standardov izdanih s strani tretje strani (države); država pa lahko intervenira tudi s primerno fiskalno politiko (npr. davčne olajšave) – če je tržna struktura taka, da je eden ali nekaj glavnih tržnih igralcev, se lahko država če že ne drugače z ustreznim prepričevanjem loti le-teh – drugi bi naj bili potem bolj motivirani slediti. Nadalnji možni vir spodbud bi bilo zavarovanje, katerega bi se osebki lahko posluževali. V stvarnosti soodvisne varnosti pa so zadeve zaradi težavnosti določanja vzročno-posledičnih povezav med dogodki (in preko tega pripisanja odgovornosti) mnogo bolj negotove. Podobne slabosti je mogoče pripisati morebitni zakonski ureditvi odgovornosti. Po drugi strani pa je tudi res, da si je v odsotnosti neke občutnejše

spodbude ali prisile (konkretne grožnje ali kakšnih vidnejših pozitivnih učinkov vlaganj) težko predstavljati, da bi se subjekti sami odločili za kakšne korenitejši ukrep, sploh pa ne vzdrževali določeno povišano raven varnosti za daljši čas.

Zato pa se (Kunreuther, Heal, Orszag, 2002, str. 1) tudi na tem področju svetuje uporabo spleta državne regulative, zavarovanja in inšpekcij s strani specializiranih zasebnih podjetij.

7.3 Ocena skupnega pristopa države, gospodarstva in vojske

Pravkar je bilo govora o pomenu in vlogi soodvisnosti pri opredeljevanju varnosti podatkov in informacij. Prav tako je bilo čisto na začetku tega besedila govora o tem vidiku varnosti z gledišča vloge podaktov in informacij v naši družbi. Iz povedanega na omenjenih dveh točkah kot navsezadnje iz pripomb/ugotovitev na mnogih drugih mestih v tem delu je mogoče doumeti, da varnost ni "stvar za soliste". V splošnem velja, da lahko samo tesno sodelovanje omogoči vpletenim doseganje lastnih ciljev kar se tiče varnosti. Potrebna je torej koordinacija – kar pomeni tudi prilagajanje. Za doseganje tega cilja pa je nujno neko osnovno soglasje, skupno razumevanje problematike, iskanje stičnih točk. Ravno s tem namenom pa obravnava Ghosh problematiko oblikovanja varnih omrežij o kateri bo govora v nadaljevanju.

7.3.1 Problematika varnosti omrežij

V tem razdelku je povzetek in komentar misli S. Ghosh-a (2003). Pri snovanju zaščite omrežja bi naj vzeli v obzir njene glavne značilnosti/dejstva v zvezi z njo (Ghosh, 2003, str. 11-17): omejitev dostopa do poslanih paketov (po čemer se tehnologija temelječa na razpršenem oddajanju kot je Ethernet in IP omrežja ravno ne odlikujejo), kodiranje vsebine paketov zaradi zmanjšanja tveganja izpostavljenosti, obveščanje pošiljatelja v primeru nedostave paketa. Pri tem se treba zavedati, da je uspešnost kodiranja časovno omejena (zaradi tega je lahko problem medpomnilnikov v omrežjih tako pereč). Pri zagotavljanju varnosti prav tako ne smemo nikoli izgubiti izpred oči namena, ki je temelj prenosa paketov – kar pa teži biti v nasprotju s potrebo po omejitvi dostopa. Slednja pa, skupaj s potrebo po obveščanju pošiljatelja o (ne)prispelih paketih terja dodatne komunikacijske in procesne zmoglivosti – kar pa zlahka pomeni večjo obremenitev omrežja in tudi preko tega počasnejšo komunikacijo. Prav tako prinaša zahteva po kodiranju dodatno obremenitev sistema. Zahtevi iz prejšnih dveh točk pa se soočata ravno z realno težavnostjo zagotavljanja dovoljšnje procesne zmogljivosti po omrežju. Vsebina v zgornjem delu tega odstavka pa jasno prikazuje pomembnost zgodnjega upoštevanja omenjenih dejavnikov (pravzaprav integracije omenjenih dejavnikov) že v fazi planiranja in oblikovanja omrežja. Empirija kaže, da je poznejše ukprepanje pogosto težje in dražje. Primeri v podporo tej ugotovitvi so lahko napori za izgradnjo varnejšega Interneta in uporaba požarnih sten v podjetjih (zahteva velik davek v obliki manjše zmogljivosti; isti avtor pa tudi omenja, da bi naj po nekaterih ocenah preko 80% napadov bilo povzročenih s strani notranjih ljudi). Ena najbolj perečih težav s katerimi imamo opravka pri zagotavljanju varnosti pa je dandanes rastoča zapletenost sistemov, katere bi naj zaščitili. Potrebno je namreč stalno iskati in odpravljati ranljivosti ter pri tem ohraniti zadostno objektivnost.

Nadalje, kot že omenjeno povzroča glavobole (ali bi jih morala) strojna zasnova omrežij oz. dejstvo, da so omrežja zasnovana na elektronskih stikalih ranljiva oz. sorazmerno zlahka

izpostavljena nestabilnosti (ali točneje – metastabilnosti). Temu pa je najti vzrok v asinhroni naravi velikega dela komunikacij ter posledični težavi zagotavljanja pogojev, ki so znotraj meja uporabnosti stikal – kar ima lahko tudi hujše posledice. V vsakem primeru pa je take težave težko identificirati in rešiti. Dejansko pa so omenjeni problemi vsaj deloma tudi posledica premajhne pozornosti namenjene vidikom varnosti pri snovanju sistema, vzrokov temu pa je več: po eni strani je že samo oblikovanje zelo zahtevna naloga (tudi z vidika sorazmerne redkosti sredstev, nenazadnje denarja in časa). Po drugi strani pa je kot nakazano inkorporacija zaščite v obstoječo obliko omrežja še mnogo težja od samega osnovnega oblikovanja omrežja.

Zaradi pomanjkljivosti tradicionalnega pristopa oblikovanja varnosti v omrežjih ponuja Ghosh drugačen pristop, temelječ na identifikacij temeljnih ranljivosti (preko poznavanja značilnosti omrežja), sinteze modelov možnih napadov in testiranjem le-teh.

Tukaj se že nakazuje prepričanje Ghosh-a, da je korist uporabe analitičnih metod pri tem početju precej omejena. Razlog temu je v zapletenosti analizirane realnosti; modeliranje in simulacija bi naj bila glavno orodje snovalca zasčite sistema. Slednja namreč omogočata zgodnje odkrivanje napak pri oblikovanju (in to na stroškovno učinkovit način), služita za identifikacijo potencialnih problemov kot tudi za oceno zmogljivost prihodnjega sistema.

Grožnje varnosti omrežja deli ta vir na notranje in zunanje. Notranjo grožnjo predstavljajo npr. zlonamerni zaposleni, hekerji, neizobraženi uporabniki. Primer zunanjih groženj pa so teroristi, hekerji, bivši zaposleni, vohuni tujih držav ali konkurentov (tujih, domačih), to pa iz političnih ali ekonomskih razlogov, pa tudi tožbe zaradi zakonske odgovornosti.

Tem grožnjam so se podjetja tradicionalno zoperstavila z mehanizmi sledenja spremembam, kriptografijo, overovljanjem. Čeprav so ta sredstva sama po sebi gotovo v pomoč, so omejena na nižjo raven. Dandanes raste zavedanje o potrebnosti zasledovanja stabilnosti in razpoložljivosti. Sistem zagotavljanja varnosti bi naj neprestano nadziral promet znotraj omrežja in med omrežij v namen odkrivanja nepooblaščenih dejanj/dejavnosti, prav tako pa bi naj vseboval mehanizme za zagotavljanje odpovedne varnosti ob morebitnih odpovedih delov sistema, predno bi slednje privedle do posledic večjih razsežnosti. Potrebno je predvideti možnost prisotnosti zlonamernih ali nepoučenih uporabnikov, nikoli pa precenjevati varnost sistema.

Podobno kot Anderson (2004, str. 6) tudi Ghosh meni, da Common Criteria ne predstavljajo zadovoljivega odgovora na sodobne zahteve po varnosti. Tokrat pa zato, ker le-ti bi naj namreč resda težili h kombinaciji velikega števila varnostnih atributov v enovit standard – slednji pa ni celovit.

Zanimivo in spodbudno je, da tudi organi Kongresa ZDA jasno ugotavljajo potrebo po večji vlogi države. To je mogoče doumeti tudi iz poročila JEC (2002, str. 1-10). Država bi naj ozaveščala gospodarstvo in spodbujala k sodelovanju kar se tiče lotevanja in razreševanja varnostnih problemov; podjetja bi naj zasnovala in prevzela primerno varnostno politiko.

V ozadju teh ugotovitev je spoznanje, da je velik del infrastrukture ZDA (ki je potencialno cilj terorizma oz. je kakorkoli ogrožena) v rokah zasebnikov – torej bi zaradi skupnih interesov javni in privatni sektor morala več in bolje izmenjevati podatke in informacije. Zasebni sektor je glede na povedano tako rekoč na udaru – a nima dostopa do vladnih informaciji o možnih grožnjah;

nasprotno pa imajo državni organi v splošnem obilo informacij in edinstveno analitično sposobnost – in vendar pogosto ne razpolagajo s specifičnimi informacijami o napadih, predvsem napadih na računalniške sisteme v ZDA a izven sistemov pod državnim nadzorom. V istem viru se zatrjuje, da bi morala gospodarstvo in javni sektor zatorej graditi varnost na istih treh temeljih: primerni varnostni politiki, tehnologiji, ljudeh.

Za prihod na skupni imenovalec glede opredelitve varnosti pa gre najprej ugotoviti, kje obstoje ključne razlike pri pojmovanju varnosti med civilnimi državnimi oblastmi, vojsko in gospodarstvom. Zlahka se ugotovi, da je temeljno razhajanje že pri opredelitvi groženj. In vendar je tok dogodkov pripeljal do situacije, kjer so do določene mere grožnje vsem navedenim skupinam osebkov skupne. Pri tem gre misel na pojem "informacijskega vojskovanja", katerega sem bežno omenil že na zacetku tega dela (str. 5). Skupni problem vsem trem segmentom pa so brez dvoma zlonamerni "notranji ljudje" (insider-ji) – pod ta pojem lahko v grobem uvrščamo nezadovoljne sedanje kot tudi pred kratkim odpuščene zaposlene.

7.3.2 Sistemski pristop zagotavljanja varnosti – na primeru omrezij

Izhodišče varovanja podatkov v mreži bi naj tičalo po eni strani v ugotavljanju posebnosti in preko tega prednosti in slabosti nekega omrežja – na prednostih pa bi temeljila inkorporacija varovanja v omrežje. Potrebno pa je tudi poskrbeti za integracijo varovanja v delovanje mreže. Za primer ZDA ugotavlja, da so državna uprava, vojska ter gospodarstvo do pred kratkim (in v določeni meri imajo še sedaj) vsak svojo opredelitev zahtev varovanja podatkov. Da je zaznati občuten premik (zaenkrat vsaj v razmišljanju čeravno ne še v dejanjih) se gre zahvaliti po eni strani konzervativnim proračunskim omejitvam s katerimi se soočajo tako podjetja kot država kot tudi zaskrbljenost glede državne varnosti. Ta premik pa pa bi naj omogočil boljšo alokacijo resursov pa tudi učinkovitejšo delitev stroškov varnosti (Ghosh, 2003, str. 1).

Zato pa Ghosh predlaga (Ghosh, 2003, str. 7): integracijo regionalnih in vsedržavnih omrežij kot tudi integracijo omrežij fizičnih oseb, vlade, vojske ter gospodarstva; vsakemu sporočilo, ki ga katerokoli omrežje ustvari bi se naj dodelilo ustrezno raven varnosti; nazadnje, bi se naj vgradilo boljšo zaščito za varnostne resurse pred človeškimi napakami.

Kot že poudarjeno, je v stvarnosti soodvisne varnosti zagotavljanje primerne ravni zaščite v splošnem nemogoče brez tesnega sodelovanja različnih soodvisnih osebkov. A da bi bilo mogoče sodelovati, je najprej potrebno zediniti se glede skupne opredelitve varnosti. Na tem bi naj temeljila prizadevanja za odpravo šibkosti danega omrežja na vsaki njegovi ravni.

Ghosh opozarja, da je mogoče biti pri varovanju podatkov in informacij uspešen samo preko holistične obravnave tega področja. Poleg že izraženega spoznanja o nevarnosti neutemeljenega občutka varnosti se je prav tako potrebno zavedati, da niti ni najpomembneje koliko informacij imamo na razpolago, ampak kako jih uporabljamo (Ghosh, 2003, str. 6). Sam menim, da bi zadnjo ugotovitev veljalo interpretirati bodisi z vidika vrednosti, ki jih imajo informacije lahko za nas a tudi koliko so lahko le-te pomembne za nepooblaščene pridobitnike. Z malo pridobljene informacije nam lahko zlonamerni osebki veliko škodijo. Pa tudi če slednji pridobijo veliko količino informacij – če so ključne dobro zaščitene, si verjetno ne bodo veliko pomagali.

Ghosh pa opozarja tudi na to, da nobena tehnološka rešitev ne more predvideti in popraviti človeške napake. Torej bi se naj zaščito prilagajalo različnim skupinam predhodno kategoriziranih podatkov, ne pa navprek. Dejansko naj bi se oblikovalo informacijski sistem glede na zasledovanje ciljev celovitosti, zaupnosti in razpoložljivosti. To bi naj po mnenju avtorja tega diplomskega dela pomenilo tudi omejevanje količine in vrste podatkov s katerimi se ravna v sistemu, bodisi v fazi planiranja sistema kot izvajanja.

Vzpostavitev varnosti pa bi naj bila rezultat zaporedja ugotovitev in analize zaznanih groženj, ugotovitev njihovih potencialnih posledic na ključne atribute varnosti sistema ter alokacijo potrebnih resursov glede na sorazmerno pomembnost resursov.

Poudariti je potrebno, da ni pod vprašanjem varnost kot taka ampak stopnja zaščite, ki naj bo uporabljena, način ocene zaščite ter izbira med stroški in učinkom pri implementaciji varnosti v omrežju. Zemljepisna porazdeljenost omrežij kot tudi asinhronost marsikaterih komunikacij pa namigujeta na iskanje varovanja na zahtevo.

Pri analizi problema varnosti v omrežjih Ghosh izhaja iz značilnosti omrežja – te pa so: deljenost (med mnogimi uporabniki – kar pomeni – ranljivost), fizična razdalja (zaradi zemljepisne porazdeljenosti) ter prisotnost medpomnilnikov (buffers) pri stikalnih vozliščih (slednji lahko predstavljajo ranljivo točko sistema zaradi možnosti prestrezanja, kjer ima napadalec možnost shraniti podatke in ima tako lahko ves čas izcimiti najrelevantnejše informacije iz le-teh (omenja se primer kreditnih kartic, kjer so te lahko veljavne več let a pri katerih ni zadostnega zagotovila zaupnosti pri Internetnih transakcijah v celotnem času veljave).

Eden prvih resnejših poskusov države zbližati poglede civilnih državnih oblasti, vojske in gospodarstva je Network Rating Model, ki ga predlaga Agencija za narodno varnost v ZDA (NSA). Zelo na kratko, ta model predpostavlja, da mora vsako varno omrežje posedovati nekaj temeljnih značilnosti – in to neglede na sektor, v katerem se nahaja (gospodarstvo, državna uprava, vojska) ali na kakšno kontrektno grožnjo, ki mu preti. Te značilnosti so označene kot “atributi” varne mreže, so pa rezultat soočanja ukrepov zaščite in zaznanih težavnih področij.

S povedanim pa je že podana osnova za oris že omenjenega Ghosh-ovega konceptualnega okvira omrežne varnosti. Predstavljamo si ga lahko kot dvorazsežno matriko, kjer sta osi označeni kot “stebri” in “atributi”. Te dve osi predstavljata ortogonalni pogled na varnost podatkov. Na osi stebrov tako najdemo sestavne dele omrežja, kateri složno podpirajo varnostni ustroj celotnega omrežja – in katerim pretijo grožnje. Vsakega izmed stebrov je mogoče neodvisno razvijati in ocenjevati, pomembno pa je, da dano jakost ali šibkost izbranega stebra ni mogoče prenesti na drugega. Stebri so: sistemski, komunikacija, fizični, osebje, izvedbeni, aplikacija, zmogljivost, točnost oblikovanja.

Sistemski steber predstavlja programsko opremo, katera omogoča delovanje omrežja in predstavlja temeljno infrastrukturo, ki predstavlja podstat višjeravenski aplikacijski programski opremi.

Komunikacija predstavlja povezave in naprave, ki povežejo posamezne komponente v omrežje. Fizična komponenta obsega opremo, material, kot tudi dokumente, povezane z omrežjem. Osebje obsega ljudi, povezane z delovanjem oz. uporabo omrežja. Izvajalni del (operational) se

nanaša na postopke, politike, kot tudi smernice, ki skupaj sestavljajo varnostni ustroj organizacije. Pod "aplikacijo" razumemo višjeravensko programsko opremo, ki se izvaja na omrežju. Delovanje(performance) se nanaša na razmik normalnih vrednosti parametrov delovanja in prepustnosti omrežja. In še zadnji – pri "pravilnosti oblikovanja" gre za pravilnost sistema kot celote.

Kot "atribute" pa razumemo eno ali več lastnosti, katero mora imeti kakršnokoli varno omrežje in mora biti opredeljeno neodvisno od katerekoli grožnje. Atributi so zasebnost, celovitost, odgovornost, razpoložljivost, zanesljivost, povezljivost, sposobnost obnove po nesreči, zakonska odgovornost, negotovost.

Zasebnost je mišljena kot nameravana ali omejena raba na določeno osebo, skupino, razred; nanaša pa se na podatke, kontrolne signale in prometni tok. Celovitost pomeni zagotavljanje istovetnosti med želeno in prikazano informacijo – zagotavljanje torej, da informacija ni bila nepooblaščeno spremenjena, ustvarjena, uničena ali vnešena. Nanaša pa se tudi na postopke. Pri pojmu "odgovornost" mislimo na izjavo ali predstavitev razlogov, vzrokov in motivov v smeri ponudbe upravičevalne analize ali razlage, katero se da dokumentirati ali izslediti in določiti lastništvo. Razpoložljivost pomeni delujoč in prisoten ali pripravljen za takojšnjo uporabo s strani pooblaščenih uporabnikov. Zanesljivost pa po drugi strani označuje sposobnost ustvarjanja konsistentnih rezultatov v zaporednih poskusih. Beseda "povezljivost" se poenostavljeno nanaša na naprave, katere sestavljajo omrežje, vključno z računalniki, terminali in povezavami med njimi ter podporno opremo. Sposobnost obnove pomeni povratek v prvotno stanje po nesreči – in neprekinjenost poslovanja.

Zakonska odgovornost se tiče pravnih vidikov oz. obveznosti, ki bi se lahko nanašale na imetje, tudi informacije. Negotovost se nanaša na nesposobnost popolnega poznavanja varnosti sistema, kot posledice v preteklosti uspešno opravljenega vdora – oz. nesposobnosti popolnega poznavanja posledic le-tega. Gre pravzaprav za posplošitev pojma "zaznavanja anomalij" pri vedenju nekega uporabnika preko sledi za presojo.

Varno omrežje je potemtakem tisto, pri katerem atributi prežemajo vsakega od stebrov. Odločitve o žaščiti pa se torej sprejemajo glede na zaznano grožnjo, ki preti določenemu stebru in/ali atributu, po drugi strani pa se upošteva stopnjo tveganja, ki jo je vodilni organ npr. ravnateljstvo podjetja pripravljeno sprejeti.

Postopek za ocenjevanje danega omrežja glede na ponujeni teoretični okvir bi naj izhajal iz neke standardne ravni ogroženosti (relativne ali absolutne) in nekega okolja. Pri točkah, kjer se v matriki modela križata dani atribut in steber bi se naj ocenilo jakost razsežnosti prikazane v njunem preseku. Sledi primerjava posamenih vrednosti kar se tiče danega stebra z dano stopnjo ogroženosti – ali pa se po drugi strani sooči vrednost jakosti posameznega atributa napram želeni vrednosti atributa. Slednja pravzaprav predstavlja analizo stroškov in koristi oz. raven tveganja, ki jo je odločevalec pripravljen sprejeti. Za vsako konkretno omrežje se posamezni element matrike lahko gleda z vidika slabosti (torej ranljivosti ali grožnje) ali jakosti (izraženo kot robustnost mehanizma). Če iščemo varnostni okvir nanašajoč se na na skupino več omrežij, dobimo to tako, da "združimo" matrike dotičnih omrežij, pri čemer pri posameznem elementu matrike vzamemo presek (najbolj strogo oceno).

Ghosh na koncu še poudarja, da je varnost omrežja neprekinjeni proces in ga je potrebno občasno preverjati.

V namen uresničevanja zaupnosti kot tudi celovitosti je zanimiva tudi zamisel o sledenju transakcijam. Možnosti okoli tega je več; obstajajo celo predlogi o uvedbi enoličnega lokalizatorja podjetja – UBL (Uniform Business locator) ali (s primerno mero etičnosti) podobne rešitve kot je sarkastično poimenovani t.i. "Veliki Požarni Zid", kjer kontrolira Kitajska Internetni promet; tovrstne možnosti bodo se bolj obsežne s širso uvedbo Ipv6 in posledično večjo sposobnostjo naslavljanja (BECC, 2001, str. 725).

8. Pravni vidiki: pomen standardov in primer neustrezne regulative

Dotaknil sem se socio-psiholoških in ekonomskih vidikov varnosti podatkov in informacij. Že pri obravnavi le-teh je bilo mogoče slutiti v ozadju tudi razšeznost, ki jo predstavljajo pravna ureditev in iz nje izhajajoče spodbude oz. vpliv regulative na vedenje medsebojno odvisnih družbenih akterjev. V nadaljevanju najprej sledi konkreten primer tega vpliva, ki bi naj nazorno pokazal kakšen pomen ima ustrezno postavljen pravni okvir na (z gledišča družbe) (ne)ustrezno ravnanje posameznikov in organizacij. Kasneje pa bo še splošnejši pregled vloge in pomena standardov in regulative.

8.1 Primer bankomatov v Združenem Kraljestvu

V duhu povedanega v nekaj zgornjih točkah tudi Varian svari pred prevelikim (slepim) zanašanjem na tehnologijo, ko govorimo o zagotavljanju varnosti (Varian, 2004). Nasprotno pa poudarja vlogo države kar se tiče zagotavljanja in uresničevanja ustreznih zakonskih določb, ki naj predstavljajo vir primernih spodbud gospodarskim osebkom. Po tej poti bi naj bilo boljše poskrbljeno za varnost in bi naj bilo to breme pravičneje razporejeno med igralci (torej glede na možnost, ki jo ima dani osebek vplivati na varnostne določljivke in tako na končno varnostno situacijo). Tukaj se npr. ponovno opozarja, da nam lahko tehnična sredstva (v konkretnem – kriptografija) pomagajo pri varnosti le toliko, kolikor jih znamo pravilno uporabljati. Veliko pozornosti se ji je namenilo, sorazmerno zanemarjeni pa so bili vidiki, kot so pravilna uporaba računalniške opreme s strani navadnih uporabnikov in uvedba spodbud za izognitev prevaram in zlorabam. Kot primer navaja Varian bankomate v Veliki Britaniji, kjer je analiza vzrokov zlorab pokazala, da je mogoče večino tezav pripisati človeškemu dejavniku: napačnemu inštaliranju, pomankljivi nastavitvi in ravnanju z bankomati s strani krajevnih bank – ne pa neustreznosti kriptografiskih zaščit. Vzrok takšnem stanju pa bi naj bil v neustreznem sistemu spodbud: v času pisanja članka je Združenem Kraljestvu v nasprotju z ZDA bilo dokazno breme o opravljeni napaki, ki je bila vzrok zlorabi, na strani porabnika (Varian, 2004). V takih in podobnih primerih bi torej potrebno uvesti ustrezne sheme spodbud, kjer bi se skušalo zagotoviti ustrezno ravnovesje med odgovornostjo različnih vpletenih strank. Ta bi naj bila sorazmerna vplivu, ki jo posamezna stranka ima na možne dejavnike tveganja. Med drugim je glede na pisanje Variana mogoče razumeti, da bi bilo potrebno poskrbeti, da bodo posamezne vpletene stranke sorazmeren del stroškov varnosti internalizirale.

S takim razmišljanjem v ozadju so v ZDA bolj premišljeno postavili primernejši pravni okvir. Tako je bilo z inštalacijo videokamer in varnostnim usposabljanjem zaposlenih doseženo, da so

banke soočene z manjšimi stroški varnosti, so pa temu navkljub pri tem vidiku zagotavljanja varnosti primerjalno bolj uspešne. Podoben primer so lahko zavrnitev storitve pri porazdeljenem napadu (DDoS attack: Distributed Denial of Service attack), kjer se zlorablja računalnike nevednih porabnikov storitev širokopasovnega dostopa do Interneta. Ker pa je povprečen uporabnik sorazmernno nevešč in nemočen kar se tiče zagotavljanja varnosti, meni Varian, da bi bilo bolj primerno velik del odgovornosti prevaliti na ponudnika tovrstnih storitev.

8.2 Vloga in pomembnost standardov ter regulative

Pomen in vlogo standardov (SURS, 1999, str. 68) je mogoče videti v omogočanju urejenih, enotnih – preko tega torej racionalnih procesov. Njihov pomen se kaže na različnih ravneh: pri poslovnih osebkih določajo enotnost notranjih postopkov, zagotavljajo ustrezno kakovost poslovanja pa tudi olajšajo upravljaje in nadzor. Tudi tukaj je torej mogoče ugotavljati, da igra zakonodaja zelo pomembno vlogo. Ta predstavlja formalni okvir poslovanju, ureja pravice in dolžnosti poslovnih partnerjev. Neustrezna zakonodaja ovira razvoj, pravočasno spreminjajoča se zakonodaja, ki sledi spreminjajočim se potrebam poslovnih osebkov pa lahko igra vlogo spodbujevalca razvoja – naprimer, z uveljavljanjem standardov na nacionalni ravni. Prav tako je seveda ključna vloga države pri usposobitvi ustrezne infrastrukture (SURS, 1999, str. 180).

Menim pa, da v sodobnem svetu, kjer je medregijsko in meddržavno sodelovanje velikega in rastočega pomena ta potencialno blagodejni učinek enotnih standardov in nasploh enotnih "pravil igre" da prenesti tudi na meddržavno raven. In da ima vsaj tako velik pomen kot na nacionalni ravni (kar je avtorju tega besedila znano, so razlike in tako potencialne ovire razvoju poslovanja načeloma med državami oz. regijami večje kot znotraj posameznih entitet). Pri tem mislim tako na bilaterarno sodelovanje, še bolj pa multilaterarno, v okviru mednarodnih organizacij in integracij (tukaj imam v mislih naprimer EU in WTO. Konkretni primeri so tudi napor za pravno ureditev elektronskega podpisa ali sporazum TRIPS). Verjamem namreč, da je zaradi rastoče medsebojne povezanosti (gospodarske, politične) v interesu vseh vpletenih strani dogovarjanje in sprejemanje – ter spoštovanje – enotnih pravil delovanja, ki bi zmanjšala ali odpravila ovire različnim oblikam sodelovanja, zmanjšala negotovost in to sodelovanje še spodbujala. Pravilnost te trditve se po mnenju avtorja pričujočega diplomskega dela kaže tudi npr. na aktualnem (a banalnem?) primeru težav pri izmenjavi podatkov o potnikih pri letalskem prometu med ZDA in EU. Tej podatki bi lahko pomembno vplivali na stopnjo varnosti – in vendar (vsaj na površju) zaradi neskladne zakonodaje med osebkoma do te izmenjave zaenkrat brez težav ne prihaja (vsaj v zadovoljivem obsegu ne).

V Sloveniji se poleg splošnejših norm iz civilnega in kazenskega prava tesneje ukvarja s področjem e-poslovanja več sorazmerno konkretnejših pravnih aktov. Sem sodijo npr. Zakon o elektronskem poslovanju in podpisu (ZEPEP) in dopolnila tega zakona (ZEPEP-A), dopolnjeni Zakon o varovanju potrošnikov (ZVPot-UPB1), Zakon o varstvu osebnih podatkov (ZVOP-1) (ki pa v trenutku pisanja ni še v veljavi), Zakon o upravnem postopku (ZUP), Zakon o plačilnem prometu (ZPlaP). Sem je mogoče uvrstiti še Zakon o dostopu do informacij javnega značaja (ZDIJZ), Zakon o poštnih storitvah (ZPSto-1) in k tej regulativi pripadajoče podzakonske akte.
Pred nekaj meseci sta se zgornjim pridružila še Zakon o elektronskih komunikacijah (ZEKom)(ki sicer obravnava tudi občutljivo področje zakonitega prestrezanja komunikacij),

katerega namen je preureditev trga telekomunikacijskih storitev in bi naj predstavljal osnovo za usklajevanje z zakonodajo EU in Zakon o pogojnem dostopu do zaščitenih elektronskih storitev (ZPDZES)(slednji bi naj tudi pomagal v boju proti piratstvu).
Zgoraj omenjena regulativa predstavlja poskus postavitve pravnega okvira odvijanju dogajanja informacijske družbe, zato menim da načeloma gre nanjo gledati z naklonjenostjo. In vendar so se pojavljale (Makarovič, 2004; Pepevnik, 2001, str. 34) in se še vedno pojavljajo ocene, da zakonodaja s tega področja ni prilagojena potrebam vpletenih osebkov in da tudi pri pomembnih vidikih ni vedno skladna tako z regulativo znotraj države kot tudi z mednarodnimi določbami ter da je pomanjkljiva – pravkar povedano pa pomeni, da v mnogih primerih deluje zaviralno na razvoj e-poslovanja. Spremembe na tem področju, kakršne so bile dopolnitev ZEPEP in sprejetje nove zakonodaje, bi naj pomenile poskus odpraviti pomanjkljivosti obstoječe zakonodaje oz. urediti in podpirati prizadevanja različnih strani za razvoj uravnavanega področja. Napori gredo tudi v smeri mednarodnega usklajevanja, vse to pa bi naj samo po sebi vendarle predstavljalo pozitivni signal države. Kar se omenjenega Zakona o elektronskih komunikacijah tiče, se je avtorju tega dela zdelo zanimivo in potencialno koristno tudi določilo, ki vsaj formalno zavezuje oblikovalce zakonodaje na področju telekomunikacij k sodelovanju z javnostjo.

9. Predstavitev standarda ISO 17799:2000 in po njem prevzetega slovenskega standarda

9.1 Uvodna beseda o standardu.

BS7799:1999 oziroma ISO/IEC 17799:2000 je v bistvu kodeks priporočil, dobrih običajev v zvezi z varnostjo, katerega dvojček je britanski standard BS7799-2:2002 (ki pa v trenutku pisanja še ni sprejet kot standard ISO). Naj samo ponudim grob obris BS7799-2:2002, ki sicer ni predmet obravnave tega diplomskega dela. V principu BS7799-2:2002 "dvojček" prvo omenjenega britanskega standarda, njegov obseg pa gre od samega planiranja, sprejetja, uvajanja in izvajanja SRIV (ISMS-Information Security Management System) – sistema za ravnanje z informacijsko varnostjo, ki velja za praktično uresničitev smernic BS7799:1999. Ta drugi del standarda bi naj pripomogel k uveljavitvi kodeksa priporočil preko oblikovanja politike varovanja informacij, opredelitve in ocene tveganja, določitve znotraj tega t.i. merodajnega tveganja (applicable risk), oz. tisti del tveganja, za katerega določimo plan ravnanja. Le-ta lahko obsega sprejetje, izogib ali prenos tveganja na drugi subjekt, ali kombinacije le-teh. Za konec pa še določimo predmet kontrole ter seveda kontrolne mehanizme in orodja.

Če se vrnem k predmetu obravnave tega razdelka – je po svoje zanimiv članek Ward-a (2004), da kar lepo število let po njegovem sprejetju, BS 7799/ISO 17799 v matični državi ni doživel kakšnega večjega uspeha – vsaj po številu certifikaciji sodeč ne. Veliko je zanimanja za to tematiko in tudi za sam standard – a v njegov prevzem je vložilo napore zgolj določeno število v glavnem manjših podjetij oz. oddelkov podjetij. Presenetljivo pa je, da ima standard sorazmerno malo privržencev tudi v vrstah ITkT podjetij. V literaturi je mogoče najti mnenja o več različnih možnih vzrokih za takšno stanje. Eden od glavnih "krivcev" bi naj bila množica cele vrste praviloma necelovitih, ozko usmerjenih priporočil oz. predlaganih standardov, ki so si pogosto tekmec drug drugemu in se včasih bolj ali manj prekrivajo kar se tiče področja obravnave. S to oceno se strinja tudi Ward ter izpostavlja dejstvo, da pomanjkanje celovitega standarda na

področju varnosti pravzaprav ovira komunikacijo ter tudi preko tega sodelovanje med poslovnimi osebki. In vendar bi naj bile prednosti BS 7799 vseobsegajoč značaj in dejstvo, da je za razliko od npr. NIST-ovih veliko bolj usmerjen v poslovni svet.

Ward izpostavlja, da bi naj bil nadaljnji vzrok sorazmerno slabemu sprejetju standarda tudi mlačen odnos države do standarda[10]. Torej, čeravno bi naj bilo zanimanje ITkT osebja precejšnje, ostaja nezainteresiranost ravnateljstva huda ovira: poznavanje tovrstnih standardov je pri majhnih in srednjih podjetjih pogosto pomanjkljiva; management pogosto vidi standard kot samo še en produkt državne birokracije, izvor stroškov brez neke bolje opredeljene (in kvantificirane) koristi; varnosti prekrški so pogosto prav tako neustrezno ocenjeni in sankcionirani v razmerju do ostalih prekrškov. Poleg tega se opozaraja, tudi zavarovalne ustanove v praksi ne usmerjajo osebkov k večji pozornosti do različnih vidikov varnosti preko ustreznih spodbud.

Skratka, Ward pogreša večjo vlogo države, ki naj bi vzpostavila neki varnostni minimum - začenši s posegi na področju regulative in nadzora nad njenim izvajanjem. Skupaj z ustreznim izobraževanjem bi naj sčasoma tudi dosegla, da bi ljudje ponotranili ta nauk. Tukaj ponuja Ward primerjavo s tehničnim pregledom vozil oz. z varnostnim pasom pri avtomobilih.

9.2 Varovanje informacij – ISO 17799:2000

9.2.1 Pomen in smoter varovanja podatkov in informacij

Kot je mogoče razbrati iz standarda ISO/IEC 17799:2000 (v nadaljevanju tudi: "standard"), je cilj varovanja podatkov in informacij[11] obvarovanje podatkov in informacij samih kot tudi procesov, sistemov in omrežij pred različnimi nevarnostmi. S tem bi se naj zagotovilo želeno neprekinjenost poslovanja, zmanjšalo poslovno škodo ali omogočilo, da bi se ji izognili, pač v skladu s politiko in cilji podjetja. Kot piše v standardu, je namen tega početja konec koncev ohranjanje konkurenčnosti, likvidnosti, donosnost, kot tudi zadostitev zakonskim zahtevam in ustrezna podoba v javnosti. Sredstvo za doseganje tega cilja pa bi naj bila premišljena uporaba ustreznih politik, načinov ravnanja (practices), postopkov, organizacijskih struktur in funkcij programske opreme (ISO/IEC 17799, 2000, VIII). To varovanje se nanaša na podatke in informacije v različnih oblikah in shranjene na različnih medijih na določenem mestu ali v prenosu (na papirju, v elektronski obliki, izgovorjene v pogovoru, ipd.); tiče pa se na ohranjanja: zaupnosti (omejevanje dostopa le pooblaščenim), celovitosti (torej varovanje pravilnosti in celovitosti informacij kot tudi procesnih metod) in razpoložljivosti (zagotavljanje pooblaščenim uporabnikom dostop do podatkov, informacij in sorodnih sredstev, kadar je to potrebno).

Globalizacija in s tem rastoča povezanost gospodarstev in zanašanje na ITkT, rastoča povezanost javnih in zasebnih omrežij tudi v luči deljenja informacijskih virov pomenijo večjo izpostavljenost podjetij grožnjam, ki pretijo varnosti. Uveljavitev porazdeljenega računalništva pomeni težjo zagotavljanje omejevanja dostopa (ISO/IEC 17799, 2000, VIII).

---

[10] Tako z vidika implementacije le-tega znotraj državnih organov kot splošneje, do sprejetja ustrezne zakonodaje, ozaveščanja in pomoči gospodarskim subjektom, ki bi naj prevzela napotke standarda.

[11] V standardu se v glavnem uporablja izraz "varovanje informacij" - morda bi bilo primerneje "podatkov in informacij"; kakorkoli že, v nadaljevanju bom uporabljal to drugo alternativo, kjer bom menil, da je potrebno.

9.2.2 Ocena tveganj, opredelitev varnostnih zahtev in izbira kontrol

Standard najprej nakazuje potrebo po ugotavljanju varnostnih zahtev (nanašajočih se ali le na del organizacije ali na celoto). To pa se nanaša tako na ugotavljanje izpostavljenosti tveganju (torej na konkretne grožnje sredstvom, na ranljivosti in verjetnosti nastanka škode ter seveda pričakovanem obsegu in vrednosti škode) kot na zakonske zahteve (zakonodaja in druga regulativa, pogodbene zaveze) ter posebna načela, cilje in zahteve glede obdelave informaciji (v luči podpore poslovanju).

Ugotavljanje varnostnih zahtev (in izbira kontrol) bi naj potekalo na različnih ravneh, mora pa upoštevati vse komponente poslovnega sistema, vse dele informacijskega sistema v vsej njihovi (možnostni) heterogenosti, potrebno pa je ta postopek občasno ponoviti zaradi morebitnih sprememb v okoliščinah (ISO/IEC 17799, 2000, IX).

V standardu se priznava, da zaradi izjemne raznolikosti okoliščin samih vse kontrole pač niso primerne v vsakem primeru, poudarja pa se nujnost upoštevanja tudi nedenarnih dejavnikov.

Pri povedanem v zadnjih treh odstavkih bi samo nekaj na kratko pripomnil: prvič, menim da je potrebno še posebej upoštevati možnosti obstoja izrazitejših potez soodvisne varnosti (in skušati, če je smiselno in potrebno, vplivati na druge deležnike, kot se v standardu tudi nekajkrat omenja). Pri ocenjevanju tveganja bi tudi morda bilo koristno posluževati se nasveta zunanjega strokovnjaka iz tega področja – že samo zato, ker bi naj le-ta bolje poznal vsaj splošnejša področja, katerim je potrebno nameniti ustrezno pozornost, pomagal pa bi naj tudi najti relativno najboljše rešitve v dani situaciji. Podjetje pa bi v interakciji z njim osvetlilo še specifike svojega poslovanja in tako prispevalo k večji prilagoditvi končne rešitve svojim potrebam. Pa tudi vkolikor obstojajo pomisleki o preveliki "prodajni usmerjenosti" strokovnjaka – soočanje njegovih argumente z lastnimi lahko vendarle pripelje do boljše opredelitve samega problema in možnih rešitev. V ISO/IEC 17799 pa se proti koncu uvoda opredeljuje tudi skupino kritičnih dejavnikov, potrebnih za uspešno uvedbo sistema varovanja informacij (ISO/IEC 17799, 2000, X):

a.) upoštevalo bi se naj skladnost ciljev in aktivnosti kar se tiče varnosti na eni strani in poslovnih ciljev na drugi;

b.) pristop implementacije varnosti ne more biti v neskladju s kulturo organizacije.

c.) jasna podpora ravnateljstva je neizogibna

d.) dobro razumevanje varnostnih zahtev, ocenjega tveganja in njegovega upravljanja.

e.) uspešno trženje varnosti poslovodstvu in zaposlenim

f.) ponujanje napotkov, smernic o politiki varovanja informacije in standardov vsem zaposlenim pa tudi pogodbenim strankam.

g.) zagotoviti je potrebno primerno izobraževanje in usposabljanje o tej tematiki

h.) seveda pa je potrebno razpolagati s celovitim in uravnoteženim sistemom za ocenitev uspešnosti ravnanja z informacijsko varnostjo – in usmerjanja povratne informacije nazaj v informacijsko-varnostni sistem.

9.2.3 Izdelava varnostne politike in organiziranje varovanja[12]

Zagotavljanje varovanja izhaja iz ocene tveganja, kateremu so podjetje oz. njegova sredstva izspostavljeni, čemur je dvojček ravnanje z le-tem. V zvezi s tem se mi poraja asociacija na ugotovitve RIS, navedene v tem diplomskem delu, katere kažejo na nekakšno različnost pri zaznavanju tveganj med izbranimi državami EU in Slovenijo. Sprašujem se ali je to dejansko odraz različnosti okoliščin med tema dvema skupinama ali so zaključki in prepričanja v Sloveniji morda nekoliko neustrezni (ker je problematika varnosti informacij v splošnem manj poznana in razvita).

Vrhnja stopnja procesa zagotavljanja varnosti podatkov in informacij je izdelava, uvedba, izvajanje ter vzdrževanjem politike varovanja informacij v podjetju. Kar se tega tiče, se glede na ugotovitve RIS položaj slovenskih podjetij že v izhodišču kaže kot razmeroma sila neugoden. Le manjši delež podjetij ima izdelano varnostno politiko. Varnostna politika pa bi naj bila ustrezno dokumentirana na različnih ravneh, občasno pa bi naj bila predmet ponovnega pregleda/preverjanja in ovrednotenja. Ta stopnja bi naj zagotovila formalizirano usmerjane in podporo ravnateljstva varovanju informacij. Rekel bi, da je potrebno zatorej imeti pred očmi ustrezna organizacijska načela – pri samem snovanju in izvajanju sistema upoštevati npr. že omenjena Cochrane-ova načela sodelovanja (konec razdelka 5.4 tega dela).

Fazi izdelave politike sledijo napori organiziranja v krovnih in specifičnih dokumentih opredeljenega varovanja. Izhodišče v tej fazi je sestava infrastrukture varovanja informacij. Tukaj bi se naj oblikoval poslovodni odbor za ravnanje z varnostjo informacij; opredelilo bi se naj usklajevanje snovanja in implementacije varovanja informacij širom organizacije, pa tudi dodelilo pristojnosti in odgovornost za njih zaščito. Sem sodi tudi določitev postopka pooblaščanja za uporabo sredstev obdelave informacij pa tudi odločitev o vprašanju medorganizacijskega sodelovanja, o morebitnem posluževanju strokovnega svetovanja s področja varnosti informacij oziroma neodvisnem pregledu politike informacijske varnosti. To bi naj omogočalo sledenje trendom v gospodarstvu in panogi, spremljanju standardov in metod zagotavljanja varnosti ter obstoj primerne točke v organizaciji, kjer bi se naj obravnavalo varnostne incidente. ISO 17799 priporoča, da bi naj za to fazo bil značilen multidisciplinaren pristop, kjer bi naj sodelovali poslovodstvo, ostali uporabniki, administratorji, oblikovalci aplikacij, presojevalci (varnostni revizorji) in varnostna služba pa tudi strokovnjaki s področji kot je zavarovalništvo in ravnanje s tveganjem.

Standard pa posebej izpostavlja problematiko varovanja informacij pri dostopu tretjih strank. Potrebno bi opraviti ugotavljanje tveganja, da bi preko tega določili vpliv na varnost in zahteve kar se varovanja tiče. Predvideti bi potrebno tudi možnost, da ta tretja stranka kasneje pokliče

[12] Povzeto po ISO/IEC 17799 (2000, str. 1-8).

še nadaljnjo stranko v razmerje. Posebej se obravnava tudi vidik zunanjega izvajanja (outsourcing).

9.2.4 Klasifikacija sredstev in nadzor nad njimi ter varnostno preverjanje osebja[13]

V ISO 17799 se v nadaljevanju daje priporočila glede področja klasifikacije sredstev in snovanja ustreznih kontrol. Namen klasificiranja je boljša prilagojenost varovanja kar se tiče ravni zaščite in prioritet. Ta opravila se začnejo pri sestavi seznama sredstev, čemur sledi klasifikacija informaciji glede na varnostne zahteve (in tudi opredelitev primernega označevanja in rokovanja). Izreden pomen pa ima pri tem korak dodeljevanja odgovornosti za posamezna sredstva. Posamezna odgovorna oseba mora potemtakem skrbeti za primerno varnost kar se dotičnega sredstva tiče. Pri tem se pristojnost glede tega početja lahko delegira, odgovornosti pa ne.

Naslednje področje v standardu se ukvarja z vidiki varnosti, tesneje povezanimi z osebjem. Tukaj se poudarja potrebnost integracije varnostnih zahtev v opise delovnega mesta in upoštevanje le-teh pri procesu kadrovanja. Skrb za varnost informacij bi naj namreč predstavljala eno od zadolžitev, ki jih sleherno delovno mesto terja. To med drugim pomeni, da bi se naj jasno opredelilo pogoje zaposlovanja iz vidika varnosti. Vzpostavilo bi se naj primerno politiko varnostnega preverjanja uslužbencev (kar vključuje tudi redno spremljanje v teku zaposlitve), pa tudi doseglo dogovore o zaupnosti podatkov in informacij tudi v razmerju do tretjih strank, kot že omenjeno v raziskavi podjetja Ibas (3. točka 4. poglavja tega dela – o kraji podatkov). Posebej se poudarja potrebo ustreznega usposabljanja uporabnikov glede področja varnosti informacij. In vendar naj spomnim, da je bilo poudarjeno, da ljudje nis(m)o nujno najbolj prilagojeni formalnim sistemom. To je potrebno imeti stalno v mislih in se lotiti implementacije sistema varovanja informacij s precejšnjo mero pragmatičnosti.

Standard pa namiguje tudi na potrebo po pozornosti na "lažne alarme" oz. potegavščine (hoaxes) oz. napade preko družbenega inženiringa. Kot je bilo v tem diplomskem delu vedno znova poudarjeno je največja grožnja varnosti informacij pogosto ravno v naravi ljudi oz. njihovi dovzetnosti do manipulacije s strani napadalcev. Tukaj gre lahko za bolj ali manj nedolžne šale[14], lahko pa pride tudi do hujših primerov. Le-ti lahko vsebujejo izrazitejšo komponento zlonamernosti – kot npr. sporočilo po e-pošti o možni okužbi z virusom, kjer "dobronamerni" pošiljatelj svetuje, kako preveriti prisotnost virusa in se ga ročno znebiti ... z izbrisom tistega, kar se nekoliko strokovno bolj podkovanemu posamezniku izkaže kot ključna sistemska datoteka operacijskega sistema! Izobraževanje uporabnikov je torej tukaj ključno, da bi le-ti (vsi mi) bili seznanjeni z nevarnostjo in jo razumeli ter vedeli kako primerno ukrepati. Za vsak slučaj pa prisotnost ustrezne politike nadzora dostopa gotovo ne škodi – tudi preko ustreznega ravnanja s pravicami porabnikov in vsiljenih postopkih za izvedbo dane naloge.
Standard pa se loteva tudi vprašanja ukrepanja ob varnostnih incidentih in motnjah. Tukaj bi se naj zagotovil obstoj sistema poročanja varnostnih incidentov kot tudi domnevnih pomanjkljivosti

[13] Povzeto po ISO/IEC 17799 (2000, str. 9-14).

[14] Naprimer, avtorju tega diplomskega dela je bilo poslano sporočilo e-pošte o grožnji, ki bi jo naj predstavljali virusi, dobljenih po SMS e-sporočilih.

pri sistemu varovanja informacij in nepravilnega delovanja programske opreme. Informacije o tovrstnih težavah bi naj hitro prišle preko ustreznih kanalov do poslovodstva; tudi v ta namen je velikega pomena ustrezno izobraževanje zaposlenih kot tudi tretjih strank o postopkih za poročanje o različnih vrstah incidentov, nesporno nastalih ali domnevnih. Seveda pa je za analizo in reševanje incidentov (oz. njihovih posledic) nujno potrebno razpolaganje s sistemom zbiranja dokazov. Potrebno pa bi tudi zagotoviti sistem učenja na podlagi izkušenj iz preteklih incidentov. Neizogibna pa je tudi uvedba pravičnega a strogega disciplinskega postopka. Namreč – računalniški virusi so sami po sebi tako v Sloveniji kot v svetu nesporno pomembna grožnja varnosti podatkov (in imajo drage posledice!); in vendar nam npr. raziskava CCSS (CSI, 2003) kaže, da so posebno dragi tudi incidenti, kjer je posledica kraja lastnine v obliki kraje podatkov in takšne ali drugačne zlorabe notranjih ljudi (insider-jev).

9.2.5 Fizična zaščita in zaščita okolja: varovana območja, varovanje opreme in splošni nadzor[15]

Standard opredeljuje tudi fizično zaščito in zaščito okolja. Tukaj sodi najprej ustanovitev in organizacija varovanih območij znotraj prostorov podjetja. V sklopu teh dejavnosti najdemo določitev prostorskega obsega danega varovanega območja (enega ali več) in lastnosti, ki jim mora zadostiti to območje (tudi fizično zaščitenih pred nepooblaščenim dostopom do podatkov, škodnimi vplivi ali motjami). Posebej se poudarja zahtevo po osamitvi dostavnih in nakladalnih ombočij glede na ostali del podjetja. S tem v zvezi se opredeljuje nadzor fizičnega vstopa v prostore pa tudi ukrepe za zaščito pisarn, drugih prostorov in sredstev podjetja in napotke za urejanje režima dela v varovanem območju. Jasno je, da bi naj bila raven zaščite sorazmerna tveganju in možni škodi.

Nadaljnja kategorija znotraj fizične zaščite je varovanje opreme. Posebej se izpostavlja področje primernega umeščanja in žaščite opreme same, pa tudi zagotavljanja nemotene oskrbe z električno energijo. Nadalje, sem sodijo žaščita kabelskih vodov, vzdrževanje opreme ter njeno varovanje izven prostorov podjetja – pa tudi varno uničenje in odstranitev opreme po uporabi oz. njena ponovno uporaba.

Sledi podsklop splošnega nadzora, kjer standard podpira zamisel sprejema politike “prazne mize in praznega ekrana” kot tudi politike dopustnih odstranitev lastnine podjetja.

9.2.6 Ravnanje s komunikacijami in obratovanjem[16]

Standard se seveda loteva tudi področja komunikacij in ravnanja z obratovanjem. Tukaj so najprej predmet obravnave obratovalni postopki in odgovornosti, ki bi naj bili prežeti z duhom zagotavljanja varnosti informacij. Obratovalni postopki bi naj bili dokumentirani (z varnostjo v mislih), spremembe v obratovanju bi se naj spremljalo. Uvesti bi bilo potrebno ustrezne postopke za ravnanje z varnostnimi incidenti, v zvezi s tem pa bi bilo koristno uvesti pri osebju tudi ločitev dolžnosti. Koristna bi tudi bila ločitev razvojnih in obratovalnih sredstev, neizogibna pa

[15] Povzeto po ISO/IEC 17799 (2000, str. 14-20).
[16] Povzeto po ISO/IEC 17799 (2000, str. 20-33).

je tudi obravnava vprašanja ravnanja s sredstvi za obdelavo informacij, ki so izven našega neposrednega nadzora (ponovno se pojavlja tematika sodelovanja s tretjimi strankami).

Poleg samih varnostnih postopkov standard obravnava, širše gledano, področje načrtovanja sistema in njegovega prevzema. Pri tem bi se naj namenilo ustrezno pozornost načrtovanju zmogljivosti, kot tudi določitvi jasnih kriterijev za odobritev in prevzem. Posebej bi potrebno biti pozoren na uvedbo primernih kontrol za zaščito pred zlonamerno programsko opremo.

Nadalje, standard ISO 17799 izpostavlja pomen izvajanja kakovostnega skrbništva nad sistemom – tukaj je mišljeno tako varnostno kopiranje informacij (izvajali bi se naj postopki za redno varnostno kopiranje in preverjanje teh kopij). Obenem bi se naj beležilo aktivnosti osebja, ki uporablja zmogljivosti za obdelavo informacij pa tudi beležilo napake oz. okvare. Tukaj sodi tudi ustrezno ravnanje z omrežjem, kjer bi naj bile postavljene primerne kontrole. Seveda pa je poglavje zase tudi varno ravnanje z nosilci podatkov. Standard obravnava vprašanje izmenljivih računalniških nosilcev podatkov, pa tudi pomemben vidik primernega uničenja nosilcev podatkov. Sem sodijo tudi postopki varnega ravnanja z informacijami pa tudi skrb za varovanje sistemske dokumentacije.

Znotraj področja komunikacij je potrebno upoštevti tudi zadeve v zvezi z izmenjavo informacij in programske opreme z osebki izven organizacije. Pri tem bi naj tako delovanje temeljilo na pisnem dogovoru, kjer bi se naj urejalo tudi vprašanje varovanja nosilcev podatkov med samim prenosom pa tudi ustrezno žaščito elektronskega trgovanja[17], elektronske pošte (preko opredelitev tveganja in izdelave politike), zagotavljanje varnosti pri elektronskih pisarniških sistemih kot tudi na javno dostopnih sistemih ali drugih oblikah/načinih izmenjave informacij. Seveda se ni mogoče izogniti tudi morebitnim zakonskim zahtevam s tega področja.

9.2.7 Nadzor dostopa [18]

Naslednje poglavje je nadzor dostopa. Poleg formulacij poslovnih zahtev kar se tiče nadzora dostopa (preko izdelave ustrezne politike in pravil v ta namen, kot opisano zgoraj), bi se naj zagotovilo ustrezen sistem ravnanja z uporabniškim dostopom. Tukaj bi se naj zagotovilo ustrezen režim prijave/odjave pri dostopu do sredstev, kot tudi ustrezno ravnanje s pravicami (tudi občasno preverjanje postavljenega tovrstnega sistema). Kot pomemben vidik se v praksi izkaže primerno ravnanje z gesli.

Tukaj pa se standard že dotakne odgovornosti uporabnikov, izpostavlja pa se tudi nujnost primernega varovanja opreme v odsotnosti uporabnikov.

Nadzor dostopa do omrežja

ISO 17799 se tukaj zopet dotika problematike omrežja, kjer poudarja potrebo po uvedbi primerne politike uporabe omrežnih storitev. Zagotovljena bi naj bila prisotnost primernih

[17] V angleškem besedilu "Electronic commerce security". V slovenskem prevodu se uporablja izraz "varovanje elektronskega poslovanja"; zdi pa se mi, da ni povsem asno ali je res govora o e-poslovanju (kot potencialno širši kategoriji) ali o e-trgovini.

[18] Povzeto po ISO/IEC 17799 (2000, str. 33-47).

vmesnikov med omrežjem organizacije in omrežjem drugih organizacij oz. javnimi omrežij. Prav tako bi se naj zagotovilo primerne mehanizme overovljanja za uporabnike in opremo kot tudi kontrolo dostopa do informacijskih storitev. Ukrepi v smeri ureditve varovanja omrežja pa so lahko uporaba vsiljene poti, pozorno overjanje pri zunanjih povezavah, overjanje samega vozlišča, varovanje logičnih vrat za administracijo na daljavo, morebitna ločitev omrežij , nadzor omrežnih povezav in usmerjanja v omrežju ter končno še varovanje omrežnih storitev. Menim, da je ta vidik še posebnega pomena, saj prevzemajo komunikacije znotraj podjetja ter med podjetjem in okoljem čedalje večjo vlogo. S tem pa se potencialno povečuje tudi izpostavljenost podjetja grožnjam. Kot je razvidno z obravnave najbolj perečih ranljivosti v programski opremi na začetku tega diplomskega dela (in tudi sicer vpoštevaje celotno lestvice inštituta SANS o 20 najhujših ranljivostih programske opreme), so med najbolj perečimi ranljivostmi v programski opremi šibkosti pri spletnem strežniku, SQL strežniku, spletnem brskalniku, deljenju resursov, različicami Outlook programov za e-pošto. Obenem pa se pri poslovanju čedalje bolj zanašamo na storitve le-teh. Tako ali drugače so le-ti udeleženi v komunikacijah ne le med podjetjem in okoljem a vedno bolj tudi znotraj podjetja – in tako ali drugače v različni meri tudi v gospodinjstvu.

Zelo aktualna grožnja so napadi zavrnitve storitev (DoS oz. DdoS: Denial of Service oz. Distributed DoS). Ni od danes spoznanje (SURS, 1999, str. 185), da so cilji tega lahko kar komercialni – zniževanje ugleda skrbnika spletnih strani zaradi slabih storitev in nedosegljivosti strežnika. Lahko pa gre za samodokazovanje in dokazovanje slabosti strežnika pa tudi – izjemoma – zrušitev strežnika zato, da se lahko zlonamernež nato lažno prestavi kot zrušen strežnik in pobira podatke uporabnikov (primer SiOL-a pred nekaj leti).

Podobno nadlogo predstavljajo ogromna količina neželenih e-sporočil (v glavnem preko e-pošte). Zbiranje elektronskih naslovov za tako početje lahko poteka v komercialne in nekomercialne namene. Do naslovov je mogoče priti na več načinov: npr. (avtomatično) brskanje po spletnih straneh, registracija uporabnika na danem spletnem nahajališču, nastavitve brskalnika. Omenjeno bi se naj imelo v mislih tako pri oblikovanju spletnega nahajališča (npr. domnevam, da bi bilo koristno navesti kot kontaktnega točno določen naslov ali skupino naslovov, ki bi bili uporabljeni samo v ta namen in bi tako predstavljali vstopno točko, kjer bi mogoče vhodno pošto filtrirati in pregledati).

Prav tako se kaže kot ključno omejevanje/nadzor dostopa do vsebin, ki se v tem standardu opredeljuje. Razlogi so npr. grožnje informacijskemu sistemu podjetja, ki jih predstavljajo zlonamerno oblikovana spleta nahajališča, pa tudi možnost kršenja določil zakonodaje in težav pri odnosih z javnostmi (pred leti – npr. primer Dow Chemicals) ali nevarnosti okužbe z virusi. In ravno slednji (virusi) so, kot že povedano, v slovenskem poslovnem okolju po RIS najbolj pereča grožnja, še posebej majhnim podjetjem.

Overjanje

Nemalo preglavic pa v zvezi s področjem iz predzadnjega odstavka povzroča overovljanje in nadzor dostopa. ISO 17799 se seveda loteva tudi obravnave slednjega. Eden od vidikov je nadzor dostopa do operacijskega sistema. Tukaj kot mogoče rešitve obravnava standard samodejno prepoznavanje terminala, sistem ravnanja z gesli, kontrolirano uporabo sistemskih

pripomočkov in časovno omejitev povezave, morda pa tudi alarm v sili za osebno varovanje uporabnikov. Posebno pozornost bi se naj namenilo snovanju ustreznih postopkov prijavljanja na terminal in s tem v zvezi tudi prepoznavanju in overjanju uporabnikov. Beležilo bi se naj tudi (ne)uspešne dostope do sistema.

Dostop do aplikacij

Obenem je potrebno nadzorovati tudi dostop do aplikacij. Pri tem je mišljeno omejevanje dostopa do informacij (samo lastniku ali pooblaščenim uporabnikom) in po potrebi tudi osamitev občutljivih aplikacijskih sistemov, pač v skladu s sprejeto varnostno politiko. Predvsem bi naj to veljalo za preprečevanje dostopa do orodji in sistemske programske opreme, ki bi lahko zaobšle sistemske ali aplikacijske kontrole. Prav tako bi potrebno zagotoviti da bi dan aplikacijski sistem ne ogrožal drugih, s katerimi deli določene informacijske vire.

Beleženje dogodkov

ISO 17799 pa navaja, da bi se naj spremljalo tudi dostop in uporabo sistemov, tj. beleženje in pregled dogodkov kot tudi, v konkretnem, spremljanje same uporabe (kar bi naj izhajalo iz izdelanih postopkov in opredelitve dejavnikov tveganja. Posebnega pomena je pri tem tudi skrb za sinhronizacijo ur. Vse to bi naj omogočalo preverjanje učinkovitosti uporabljenih kontrol in skladnost dejanskega stanja okoli politike dostopa z željenim. Pripomnil bi, da sem mnenja, da bi tudi to področje pri slovenskih podjetjih potrebno bolje razviti. Kot že prej povedano prikazuje RIS sorazmerno ugodno informacijsko-varnostno situacijo v Sloveniji (če izključimo področje virusov). In vendar naj tudi na tem mestu ponovno pripomnem, da se ne morem znebiti občutka, da je morda dejanska slika nekoliko drugačna od prikazane. Omenjene raziskave RIS se zanašajo na poročanje podjetij, na njihove ocene. Virusi oz. njihove posledice pa so morda v splošnem bolj "opazni" kot delovanje kakšne druge grožnje (ne nujno manj nevarna). Če podjetja pravzaprav niso ustrezno ozaveščena in postavljeni mehanizmi zaščite so precej skromni (tukaj mislim tudi na beleženje dogajanja) – a smo res lahko prepričani, da so rezultati raziskave zanesljivo veljavni? Namreč, če ne veš kaj se pri tebi (in okoli tebe) dogaja, je pravzaprav vprašanje ali lahko zares uspešno ravnaš z varnostjo. Po eni strani boš v izhodišču težko sprejel neko odločitev, saj ne moreš točno vedeti, kakšno je stanje okoli merodajnih okoliščin. Pa tudi primerne povratne informacije zelo verjetno ne bo na razpolago. Sicer pa bi izgledalo, da tudi v ZDA situacija glede poznavanja stanja lastnega informacijskega sistema ni vedno rožnata (glede na ugotovitve iz CCSS).

Delo na daljavo in prenosna računalniška oprema

Področje zase je tudi prenosna računalniška oprema in tematika dela na daljavo. Upoštevati je potrebno možnost delovanja v nezaščitenem okolju. V primeru teledela je načeloma mogoč večji vpliv tudi na zagotavljanje varnejšega okolja; drugje pa pridejo verjetno v poštev predvsem ukrepi vplivanja na druge dejavnike. Teledelo na slovenskem zaenkrat ni tako razvito kot v drugih razvitejših gospodarstvih – kar pa je (če ironiziram) morda po svoje tudi dobro, saj glede na ugotovitve RIS so pri obstoječjih oblikah teledela znanje s področja varnosti podatkov in informacij kot tudi postavljeni ukrepi za njeno zagotavljanje precej skromni.

9.2.8 Razvijanje in vzdrževanje sistemov[19]

Naslednje poglavje se podrobneje ukvarja z razvijanjem in vzdrževanjem sistemov, kjer bi se naj ugotavljalo, opredeljevalo in analiziralo varnostne zahteve tega področja. Kadar je to mogoče, bi potrebno seveda varnostne zahteve (vključno z rezervnimi ukrepi) opredeliti pred samo izgradnjo operacijskega sistema, bi pa naj bile podvržene postopku upravičevanja, dokumentiranja in končne odobritve. Glede na to določilo standarda bi samo poudaril pomen uporabe preverjenih orodji za vzdrževanje sistema (in njih pravilne uporabe). Na primeru orodij za vzdrževanje omrežja: ena od desetih najpomembnejših ranljivosti programske opreme ob izvedbi raziskave je po SANS ravno uporaba SNMP orodij. Pri tem je s pojmom "sistem" mišljena tako infrastruktura, kot tudi poslovne aplikacije vključno z različnimi aplikacijami, ki jih razvijajo uporabniki. Posebej se v smislu doseganja ustreznega varovanja izpostavlja pomen ustreznega oblikovanja in implementacije postopkov poslovanja v zvezi z uporabo aplikacij oz. storitev.

Varovanje aplikacijskih sistemov

Tukaj bi se naj posvečalo primerno pozornost varovanju aplikacijskih sistemov, kamor sodi preverjanje vhodnih podatkov, nadzor notranje obdelave podatkov, overjanje sporočil in preverjanje izhodnih podatkov. S tem v zvezi so koristne kontrole uporaba sledi za presojo (audit trail) in dnevnikov aktivnosti. Te bi naj bile po možnosti vkomponirane v aplikacijske sisteme (tudi tiste, ki jih uporabniki sami snujejo). V smeri zagotavljanja varovanja informacij pa utegne biti zelo koristen tudi prispevek kriptografskega nadzora – pri čemer bi potrebno najprej izdelati politiko uporabe tovrstnega orodja, definirati uporabo šifriranja, digitalnega podpisovanja, storitev za zaščito proti lažnemu zanikanju kot tudi ravnanja s ključi. Opredeliti bi torej potrebno zaščito kriptografskih ključev samih in definirati standarde, postopke in metode uporabe. Tovrstna zaščita lahko pride prav še posebej takrat, ko drugih inštrumentov zaščite ni na voljo (vsaj v zadostnem obsegu ne).

Kar se pa vidika združljivosti tiče, bi se naj pri nakupovanju in uporabi programske opreme bilo pozorni tudi na možne omejitve uporabnosti pri strojni in programski opremi, takšne vrste, kot jih motri in skuša uveljaviti pobuda TCPA (Anderson, 2004c, str. 8-13). V teoriji, bi nakup take opreme lahko pomenil ne samo nezdružjivost z drugo programsko in strojno opremo in večjo odvisnost od določene skupine proizvajalcev/dobaviteljev, ampak tudi potrebo po pozornejšem iskanju združljive strojne in programske opreme kot tudi otežilo komunikacijo z okoljem. Obstajala bi možnost določanja združljivosti določene opreme z določenimi podatki – in nezdružljivost drugačne kombinacije...; zato menim, da bi tak sistem potencialno ogrožal vsaj eden vidik varnosti podatkov (razpoložljivost). Nekateri avtorji sicer navajajo, da bi tovrstna sredstva zlahka utegnila biti predmet zlorab – uporabljena bi lahko bila v družbeno ne najbolj zaželene namene, npr. za preprečevanje razkrivanja nepravilnosti znotraj podjetja s pomočjo notranjih ljudi oz. "whistle-blowinga". Da je celotna zadeva še bolj zapletena pa kaže dejstvo, da bi bila potrebna koordinacija glede tega vidika tudi s strankami izven podjetja.

[19] Povzeto po ISO/IEC 17799 (2000, str. 47-56).

Varovanje sistemskih datotek

Posebnega pomena pa je znotraj vzdrževanja sistemov varovanje sistemskih datotek. To bi naj pomenilo v praksi kontrolo nad produkcijsko programsko opremo, zaščito podatkov uporabljenih pri testiranju, nadzorovalo bi se naj dostop do knjižnic izvorne kode programske opreme. Odgovornost in s tem skrb za spremljanje celovitosti sistema bi se naj dodelilo lastniku.

Prav tako omenja ISO 17799 potrebo po vpeljavi ustreznega varovanja informacij in aplikacijske programske opreme pri postopkih razvoja in vzdrževanja sistema. Pri tem bi naj okolje projektiranja in podpore strogo nadzorovali. Standard navaja, da bi naj bili poslovodje, kateri so odgovorni za aplikacijske sisteme bili odgovorni tudi za varnost projektnega ali podpornega okolja. Prav oni bi naj zagotovili, da se predlagane spremembe v sistemu pregledajo in preverijo – v izogib težavam z varnostjo sistema ali obratovalnega okolja. Sem sodijo postopki za nadzor sprememb, tehnični pregled sprememb v operacijskih sistemih pa tudi omejevanje sprememb programskih paketov.

Omrežna varnost

V to področje sodijo pozornost na in obramba proti različnim virusom, omrežnim črvom, prikritim kanalom, trojanskim konjem in logičnimi bombami ter v povezavi z nadzorom nad pogodbenim zunanjim razvojem programske opreme. Pomembno sredstvo boja proti tem grožnjam je primerno izobraževanje uporabnikov o nevarnosti, ki jih posamezne grožnje predstavljajo. In primerna politika nameščanja popravkov programske opreme – in tudi njeno ustrezno izvajanje.

In vendar – strogo sledenje politiki o vzdrževanju programske opreme v takšnem stanju, kot ga podpira proizvajalec ni brez tveganj. ISO 17799 vsebuje takšen napotek; takšno razmišljanje je tudi empirično podkrepljeno (SANS, 2004). In vendar izsledki ištituta SANS (navedeni v začetnem delu tega teksta) kažejo tudi na to, da sta nepremišljena uporaba ne dovolj preverjene (čeprav originalne) programske opreme ali "poigravanje" z nastavitvami lahko zelo nevarna. Pri vseh šestih najhujših ranljivostih Microsoftove programske opreme je za vsaj del ranljivosti odgovorna neustrezna tovarniška ponastavitev programske opreme. Dejansko menim, da bi morali lastniki informacijskih sredstev skrbeti, da so na tekočem kar se tiče informiranosti o odkritih slabosti in njihovem odpravljanju – in se danemu stanju aktivno prilagajajo, bodisi neposredno ali preko sodelovanja s posebej za področje varnosti odgovornim osebjem. Tudi na tem področju je potrebna proaktivnost. Vir omenjenih informacij pa bi se naj formalno določil in odobril – in naj ne bo nujno samo proizvajalec, ampak tudi morebitne druge verodostojne (npr. državne) inštitucije, morebitna medpodjetniška združenja, specializirana podjetja. To pa zato, ker "več glav več ve". In ker imajo lahko različni subjekti različne interese se to (domnevam) utegne zrcaliti v obsegu in kakovosti ter pravočasnosti informacij. Interesi proizvajalca pa se nujno ne ujemajo z interesi drugih osebkov. Aktivna vpletenost oz. proaktivnost pa bi naj pomenila tudi obširno in ponavljajoče se testiranje sistema z namenom odkrivanja ranljivosti – to pa tako z namenskimi orodij proizvajalcev (kot svetuje inštitut SANS – str. 12 tega dela, točka o MS IIS) a

tudi z orodji, ki jih uporabljajo hekerji, kakor svetuje Chapple (1. odstavek na str. 16 tega dela)[20]. Načelo proaktivnosti pa ne sme pomeniti prenagljenosti. Tudi nastavljanje programske opreme in nameščanje popravkov pomeni določeno tveganje, zato pa se svetuje določen odlog pri nameščanju. Tem krajši kolikor bolj je razširjeno testiranje omenjenih na različnih sistemih.

9.2.9 Ravnanje z neprekinjenim poslovanjem[21]

Standard obravnava tudi problematiko ravnanja z neprekinjenim poslovanjem (v namen preprečavanja nepredvidenih hujših prekinitev poslovnih aktivnosti oz. kritičnih poslovnih procesov – ali točneje zmanjševanja motenj oz. škode, ki jih taki dogodki prinašajo). Sem bi naj sodili vidiki izdelave postopkov ravnanja z neprekinjenim poslovanjem, kjer bi se naj analiziralo vpliv možnih prekinitev, izdelalo in izvedlo načrte za neprekinjeno poslovanje (kjer bi se naj startalo iz enotnih izhodišč, okvira načrtovanja). Tukaj bi naj uporabljali splet preventivnih in obnovitvenih ukrepov). Tudi tukaj pa je pomemben vidik preverjanje in vzdrževanje ter občasno preverjanje načrtov. Nasploh pa bi potrebno občasno preverjati ustreznost dejanskega varnostnega stanja sistemov z varnostnimi politikami in standardi – to pomeni preverjanje izvedenih varnostnih postopkov v skladu s politikami kot tudi preverjanje tehnične skladnosti (oz. analizo pravilne implementacije kontrol). Vzpostaviti pa bi potrebno tudi kontrole za zaščito orodij za presojo. Kot rečeno Ghosh trdi, da je pomen stabilnosti in razpoložljivosti v sodobnem svetu čedalje pomembnejši. Rekel bi, da dogodki kot so teroristični napadi septembra 2001 na stolpnici WTC v New Yorku so lahko v svoji skrajnosti dokaz pomena ureditve tega področja. Brez tega bi podjetja kot so npr. Merril Lynch utrpela mnogo hujše posledice kot so jih sicer – mnoga bi preprosto propadla – in zaradi prepletenosti njih poslovanja z drugimi gospodarskimi subjekti bi lahko bile posledice kratkomalo katastrofalne.

9.2.10 Skladnost z zakonskimi zahtevami[22]

Končno se v ISO 17799 poudarja nujnost skladnosti z zakonskimi zahtevami. V ta namen je najprej potrebno ugotavljanje veljavne zakonodaje, obstoj in lastnina pravic intelektualne lastnine, varovanje arhivskih zapisov v organizaciji, zasebnost in varovanje osebnih podatkov, preprečevanje zlorabe sredstev za obdelavo informacij in upoštevanje zakonskih vidikov uporabe kriptografije. Organizirati je potrebno ustrezno zbiranje dokazov, sistema presoje sistemov, kamor sodi tudi ustrezno varovanje, tako podatkov kot drugih sredstev. Potrebno pa je tudi preverjanje skladnosti varnostne politike in tehnične skladnosti z določili zakonov/druge regulative. Tukaj bi naj prišli na pomoč strokovni svetovalci, notranji ali zunanji. Posebej je potrebno biti pozoren na ta vidik v primeru ustvarjanja informacij v eni državi in prenosa v drugo.

10. Zaključne misli

10.1 Ugotovitve in mnenja avtorja

[20]Pri slednjih le zatem ko se prepričamo o varnost njihovega delovanja.
[21] Povzeto po ISO/IEC 17799 (2000, str. 57-60).
[22] Povzeto po ISO/IEC 17799 (2000, str. 60-65).

10.1.1 Pomen ozaveščanja, izobraževanja v smeri izgradnje zaupanja kot temelja poslovnega sodelovanja – z vidika vloge države

Mislim da je nesporno, da iz tega besedila izhaja, da sodi varovanje informaciji v področje, ki ga obsega (pogosto zlorabljeni) pojem "nacionalnega interesa". Izkušnje iz ZDA (CSI, 2004) kažejo, da predstavljajo neznanje posameznikov, nezaupanje, neorganiziranost in topost državnih organov (izvršilne in sodne veje oblasti) pogosto ploden substrat za razvoj za varnost zelo neugodnih okoliščin. Ugotoviti bi potrebno naprimer zakaj zelo velik delež osebkov, ki so doživeli varnostni incident, kjer bi lahko poiskali pomoč oblasti, tega niso storili. In škušali bi naj zmanjšati število pripadnikov te skupine – pri tem je neizbežno lotiti se tudi vzpostavitve ustreznih mehanizmov, ki naj bi iskali in ponudili ustrezno ravnotežje kar se tiče razkrivanja in zaupnosti informacij. Varnost pa je predpogoj le-tega – in bi verjetno bila tudi njegova posledica. Razlogi zadržanosti do večje uporabe storitev t.i. e-uprave s strani slovenskih podjetij nenazadnje tičijo tudi v nezaupanju v varnost dotičnih storitev.

Pogojno ugodno pa je lahko sorazmerna nezaskrbljenost porabnikov to te tematike (podobno v nekem smislu kot je bilo ugotovljeno pri podjetjih v Sloveniji napram tistim v EU). Ali vsaj tako bi se reklo na prvi pogled. A morda je tudi tukaj neozaveščenost in nasploh nepoznavanje te problematike eden glavnih razlogov za to. Kar pa utegne pomeniti, da se lahko (neutemeljen) optimizem zlahka prevali v (neutemeljeno) zadržanost – če se npr. dogodi, da pride do zlorabe večjih razšeznosti, kjer porabniki "dobijo po grbi" - in v zvezi s katero bi se vršila bolj ali manj pompozna in tendenciozna negativa publiciteta.

V tekstu je bilo tako na več mestih govora o osrednjem pomenu zaupanja pri poslovanju. Tukaj pade misel na pojem vrednosti življenske dobe zvestobe kupca a tudi že samo na dejstvo, da so raziskave pokazale, da je načeloma bistveno dražje iskati nove kupce kot zadržati stare (pri okvirnem opredeljevanju razlike se pogosto omenja množenje za faktor 5, često pa je večji).

Neodvisne inštitucije splošno priznane verodostojnosti bi lahko s certificiranjem igrale tukaj pomembno vlogo. Seveda pa bi koristilo, da bi država dala svoj "blagoslov" (certifikacijo) takim strokovnim institucijam – kar bi naj jim povečalo kredibilnost in jih dejansko morda tudi prisililo k (bolj) profesionalnem delovanju. Tudi tukaj pa obstaja potencialno druga plat medalje – kot naprimer zaplet glede (bolj ali manj utemeljene) ocene, ki ga je pred kratkim Sloveniji podelilo podjetje Verisign. Organizacija, ki se med drugim ukvarja s spletno identifikacijo in pooblaščanjem plačil je namreč našo državo uvrstilo v krog najbolj tveganih držav na svetu kar se tiče varnosti e-poslovanja! (Internet Security Intelligence Briefing, 2004, str. 10)

Pomen resne in aktivne podpore države se mi zdi toliko pomembnejši ob dejstvu, da bi začeten samostojen poskus razvoja e-poslovanja s strani zasebnega osebka v neugodnem okolju povsem mogoče doživela neuspeh (kot neugodno tukaj mislim tudi zakonsko neprimerno ali sploh neurejeno in z neprimernimi ekonomskimi spodbudami posejano okolje). Enkrat pa, ko je zaupanje načeto, ga je zelo težko nazaj povrniti. Toliko težje, če je okolje temu nenaklonjeno. In pomembem akter, kateri ima vsaj določeno kontrolo nad spremenljivkami okolja je država.

Zaradi ugotovitev o čedalje večji prepletenosti interesov zasebnega in javnega sektorja kar se tiče področja varnosti informacij, se mi zdi primerno, da bi država jasneje uredila in preko primerne

promocije in izobraževanja informirala organizacije in posameznike o načinih in pogojih sodelovanja med državo in zasebniki.

Država bi naj pomagala bodisi neposredno (npr. preko ustreznega trženja - ustrezne promocije, izobraževanja, nekako takole kot je sedaj npr. proti kajenju) ali posredno (npr. podporo zasebnim specializiranim organizacijam, ki bi naj pod ugodnimi pogoji skrbele za izobraževanje uporabnikov; certificiranje programske opreme in spodbudo uporabe le-te (npr. davčne olajšave); v primeru ugotovitve odgovornosti za incident pa bi naj se sprejelo zakonsko določene sankcije in s tem v zvezi tudi ponudilo možnost zavarovanja – ob upoštevanju načela bonus/malus).
Pri "promociji" varnosti informacij mislim na ozaveščanje in globlje izobraževanje o problematiki varnosti, osvetljevanje njenih najbolj kritičnih vidikov, manj (po)znanih (a pomembnih) področij, rušenje stereotipov in ustaljenih stališč in prepričanj, napotke in posredovanje znanja za uresničevanje ali ravnanje z obstoječim sistemom varovanja podatkov in informacij (bodisi neposredno, bodisi preko preusmerjanja na druge, zasebne vire podpore). Po mojem bi naj bilo potrebno vključevanje te snovi v šolske programe; bilo bi naj včasih morda predpogoj za sklenitev delovnega razmerja (čeprav v omejenem obsegu) – podobno kot je sedaj znanje jezikov, vozniško dovoljenje.

S tem v zvezi se v (BECC, 2001, str. 34) omenja koristnost nastopa države z ustreznim izobraževanjem o varnostnih mehanizmih, torej z izgradnjo zaupanja v tehnološko plat varnosti – a tudi v človeško, vse to pa v namen spodbujanja sodelovanja med udeleženci na trgu.
Pri tem domnevam, da bi koristi prinašalo tudi ustrezno izobraževanje o pravnih vidikih kot tudi dostop do načina za sorazmerno poceni in hitro reševanje nastalih sporov. Pri tem mislim na v poslovnem svetu čedalje bolj uveljavljajo izvensodno reševanje sporov (mediacija, arbitraža); kar pa se tiče razmerij med končnimi porabniki in podjetij, bi koristila uvedba lika razsojevalcev, omejeno pristojnih za civilnopravne (ali morda do določene mere tudi kazenskopravne) zadeve (kot npr. italijanski "Giudice di Pace").

V (BECC, 2001, str. 589) se označuje priporočena področja, kjer bi naj se osredinilo napore v smeri večje uveljavitve e-trgovine. Menim da je mogoče sprejeti podobne zaključke tudi kar se nasplošno tiče trženja varnostnih praks:

-potrebno bi ponuditi izbrane, celovite in neodvisne informacije o tej tematiki, tako osebam kot organizacijam, že samo v smeri povišanja ozaveščenosti in učinkov višje ravni. Tukaj je osrednjega pomena medsebojno sodelovanje države in privatnega sektorja.
-potrebno je ustrezno usposabljanje, ki naj bi olajšalo implementacijo varnega poslovanja.
-končno, bi bilo potrebno zagotoviti ustrezno infrastrukturo.

Država pa bi lahko pomagala tudi tako, da bi prva dala zgled in ne le "porivala" osebke k uporabi nekega sredstva ampak jih k temu tudi "pritegnila". Avtor tega dela sem si že pred leti priskrbel spletno digitalno kvalificirano potrdilo SIGEN-CA. Pričakovanja so bila velika, nenazadnje tudi pri sodelovanju z javno upravo. Dejanske možnosti (vsaj zaznane) pa dosedaj dokaj skromne.

Zato pa menim, da se kaže potreba po uporabi analize varnosti širšega dometa – kjer bi naj se dotaknili ne zgolj identifikacije šibkih točk in odgovornosti za njihovo odpravljanje, ampak tudi

spodbud v ta namen.

Kakor že povedano, bi seveda tudi pri vidiku izgradnje zaupanja odigrale potencialno pomembno vlogo zavarovalnice: po eni strani bi lahko zmanjšale negotovost v zvezi s transakcijo tako pri prodajalcu kot pri kupcu; premišljena shema spodbud (kjer bi se nagradilo "igranje po pravilih") bi naj prav tako spodbudila ponudnike k večji pozornosti do varnosti in poslovne integritete. Tukaj se lahko preko ustreznih spodbud posamezni odgovorni stranki nakazuje pot do primernejšega varnostnega ravnanja. Kar se tiče podjetij pa to pomeni tudi to, da skušajo doseči bolj varno ravnanje s strani svojih partnerjev, tudi kupcev. Takšna večja pozornost pa bi se zelo verjetno nazaj povrnila v obliki zaupanja, katero bi nadalje blagodejno vplival na razvoj partnerstva. V tem vidim eno od (potencialnih) koristi Evropskih integracij. V tem trenutku se kot ovira konkretni izpeljavi pravkar povedanega kaže sorazmerna neizkušenost zavarovalnic pri ocenjevanju tovrstnega tveganja.

Poleg omenjena mi pride na misel znani rek, po katerem tam, kjer so odgovorni za nekaj vsi, ni konec koncev odgovoren nihče. Zato se mi zdi ustrezno porazdeljevanje pristojnosti in odgovornosti glede na možnosti vpliva stranke osrednjega pomena. In kakor omenjeno na primeru bankomatov – je tudi tukaj vloga zakonodajalca bistvena. Morebitno nastale stroške zaradi preprečljivih a ne preprečenih incidentov bi naj močnejša stran ponotranila (oz. stranka, ki ima na večjo možnost vpliva na (ne)nastop danega dogodka). In vendar menim, da smo zaradi dejstva soodvisne varnosti lahko zares uspešni le, če se tudi uporabniki (organizacije ali posamezniki) bolje spopadajo s problematiko varnosti. Kakor velja načelo, da bi moral vsak posameznik biti na tekočem kar se tiče sprememb zakonodaje (in svoje delovanje ustrezno prilagajati), bi naj veljalo, da se mora sorazmeren del odgovornosti prevaliti tudi na uporabnika. Preprosto sklicevanje na neveščost in nemoč uporabnika pomeni dajanje potuhe nepremišljenosti in malomarnosti.

10.1.2 Varnost podatkov – nekaj vidikov s stališča podjetja

O analizi tveganja

Glede na že vse povedano, pa pri ocenjevanju tveganja ne kaže preveč nalahko jemati bodisi strogost ocenjevanja verjetnosti posameznega dogodka, bodisi možnost sočasnega nastopa različnih škodnih dogodkov in možnega vpliva nastopa takega preseka na poslovanje. Namreč, kljub morda zelo majhni verjetnosti nastopa, so lahko posledice katastrofalne. Ali če karikiram – podjetje propade samo enkrat. Ne zagovarjam paranoidnega vedenja – le glede na predstavljena dejstva in mnenja odsvetujem objestnost in preveliko samozaverovanost, oz. malomarnost pri opravljanu analize tveganja. Pomen pravkar povedanega se po mojem mnenju lahko posebej vidi pri inštitucijah, katerih delovanje pravzaprav temelji na zaupanju – npr. pri finančnih inštitucijah. Menim, da težave pri uvajanju znamenitega novega informacijskega sistema Sigma v NLB kažejo na nevarnost nepremišljenosti. NLB je tokrat šlo sorazmerno brez večjih težav – le z rahlo skrhanim ugledom – in nepotrebnimi stroški. Zlahka pa si predstavljam, da bi jo lahko precej slabše odnesla, v najbolj črnem scenariju tudi zaradi zavajajočih negativnih informacij od ust do ust (word-of-mouth, katere imajo pri ljudeh pogosto najvišjo verodostojnost, a so povsem nepredlvidljive in izven nadzora). Menim, da bi se bilo vse skupaj zlahka končalo s kakšnim manjšim pravcatim navalom na bančne poslovalnice (bank run).

Po drugi strani je potrebno biti zadržan do prenagljenosti - prevelike širokogrudnosti kar se tiče dodeljevanja sredstev za zmanjšanje tveganja – kot je bilo omenjeno v besedilu tega diplomskega dela, je pogosto celo investicija v višini ene tretjine pričakovane škode čisto dovolj. Ugotovitev v standardu, da morajo biti stroški zmanjševanja tveganja sorazmerna ravni zaznanega tveganja in pričakovani škodi je torej na mestu. A govorimo o kategorijah dodatnih (in ne celotnih) stroškov in koristi. Kot je bilo že povedano, nima smisla dodatno vlagati v varnost več, kot to dodatno vlaganje doprinese. To bi bilo približno tako, kot da bi se v imenu dobrobiti podjetja odločili povečati proizvodnjo (in prodajo) v podjetju do točke, ko bi pričakovani celotni prihodki enaki pričakovanim celotnim stroškom – kot je znano, bi idealno popolnoma izničili dobiček, dejansko (ex post) pa je povsem mogoče, da bi prišli celo do izgube.

Omembe vredno se mi zdi poudarjanje oz. izpostavljanje po eni strani tistih kontrol, ki bi naj pomenile eksogeno dane zahteve (zakonske) od zahtev znotraj podjetja. Čeprav sta oba razreda vsak po svoje zelo pomembna, vendarle menim da velja, da ni pametno enega zanemarjati na račun drugega. Skreganost z ekonomsko logiko na daljši rok pripelje do tega, da se podjetje slej ko prej sesuje vase. Če pa ta neskladnost sama po sebi (že) ne poskrbi za to na neposreden način, lahko posredno prikliče v igro pravni okvir okolja, v katerem se podjetje nahaja – kar lahko v končni fazi zada milostni udarec poslovnemu osebku.

Vnaprej zamišljeno delovanje nasproti improvizacij – ravnanje s prekinitvami v transakcijah

Domnevam, da potreba po hitrem a točnem, zanesljivem in tudi s tem učinkovitem delovanju sistemov narekuje tudi zmanjševanje števila in ostrosti napak – in stroškov. Bilo je že omenjeno koliko so lahko drage prekinitve v transakcijah. Menim torej, da bi naj filozofija zasledovanja sistema reševanja prekinitev pri transakcijah (npr. t.i. TPRN – Trading Partner Resolution Net - po (BECC, 2001, str. 74-75)) šla z roko v roki z izgrajevanjem sistema varovanja podatkov in informacij. To pa je po mojem eden izmed razlogov, ki stojijo za trditvijo standarda, da bi se naj kar največjo pozornost namenilo že sami fazi opredeljevanja in oblikovanja poslovnega (in znotraj njega – informacijskega) sistema. To pa pomeni tudi vzpostavitev ustreznih kontrol za zagotavljanje varnosti informacij. Kot se je omenilo v tem diplomskem delu, se je npr. naknadno utrjevanje varnosti svetovnega spleta izkazalo kot zelo trd oreh. Pa tudi morebitne prekinitve v transakcijah so lahko zelo drage.

V zvezi s tem pa je verjetno eden največjih izzivov ta, da je mnogo sistemov, ki niso bili zasnovani z dovolj pozornosti za varnost in katere je zato potrebno spremeniti – ob sprijaznitvi z dejstvom, da ni mogoče zagotoviti varnosti samo s tehničnimi sredstvi. Neizogibno je ustrezna uporaba ravnateljevanja in vpeljave primernih postopkov – potrebna pa sta čimbolj popolna privrženost zaposlenih in poslovodstva. V dobi rastoče medsebojne odvisnosti je uspešno sodelovanje med partnerji ključnega pomena za ohranitev konkurenčne sposobnosti (npr. v smeri snovanja strateških partnerstev med različnimi osebki - denimo strateških mrež). To pa bi naj pomenilo, da se verjetno v marsikaterem primeru soočamo z okoliščino soodvisne varnosti med povezanimi osebki. Kot pa se navaja v ISO 17799 (ISO/IEC 17799, 2000, VIII)., bi v luči zagotovitve ustrezne ravni varnosti skušali doseči angažiranost vseh deležnikov (dobaviteljev, kupcev, lastnikov, drugih javnosti) in morebiti iskali zunanjo strokovno pomoč.

Varnost informacij je posebej pereče vprašanje tudi (ali še posebej?) pri majhnih podjetjih, tudi v Sloveniji. Le-ti konkurirajo z osredinjanjem na tržne niše oz. osnovanjem lastnega delovanja okoli neke redke osrednje sposobnosti, ki jim zagotovlja strateško prednost. In tej osebki imajo pomembno vlogo v gospodarstvu - tako po številu kot po ustvarjeni dodani vrednosti. In vendar tako psihološko/sociološki razlogi kot zakonska določila (npr. varovanje osebnih podatkov), pogosto niso najbolj naklonjeni postavitni primernih in željenih kontrol. Pa tudi viri (t.i. človeški, finančni) so predvsem pri manjših podjetjih pogosto sorazmerno skromni (naprimer, nova oz. splošneje – mala podjetja so verjetno še posebej ranljiva, bodisi zaradi sorazmerne nerazpoložljivosti sredstev (tudi človeških), bodisi ker se v zvezi s tem veliko ukvarjajo že s samih zagotavljanjem lastnega golega obstoja ali rasti). Zato pa vidim tukaj možnost za uveljavitev specializiranih podjetij s področja varnosti informacij, tudi zaradi rastoče ozaveščenosti o tej problematiki, v katere izgradnjo (bi naj) pristeva(la) tudi država. Storitve ozaveščanja, svetovanja, izobraževanje in izvajanja varovanja nasploh bi morda bile še posebej koristne v sklopu spleta storitev, ki jih t.i. podjetniški inkubatorji nudijo novim podjetnikom. In vendar je tudi tukaj mogoče najti pozitivno plat – omenjeno je že bilo dejstvo, da si zaposleni z neposlovno uporabo spleta pridobivajo tudi dodatne izkušnje, ki v praksi pridejo pogosto prav tudi pri odobreni rabi. Pozitivni učinki tega pa bi naj prišli vpoštev predvsem pri manjših podjetjih (kjer je potrebno načeloma bolj raznovrstno znanje). Kot namigujejo navedbe RIS-a v tem delu, tiči verjetno tudi tukaj vzrok, da je pri majhnih podjetjih to področje (navidezno?) bolj zanemarjeno.

10.2 Sklep

V sedanji stvarnosti so usode posameznikov, gospodinjstev, podjetij in države neločljivo prepletene ena z drugo. To pomeni, da grožnje enemu osebku tako ali drugače ogrožajo tudi drugega. Učinkovita in uspešna obramba z vidika posameznega subjekta v namen zagotavljanja okolja, ki bi naj predstavljal kar se da ugodno podstat za razvoj blaginje družbe pa je zato mogoča samo pri čimbolj složnem sodelovanju vseh vpletenih v smeri doseganja tega cilja. Pri tem pa je potrebno paziti, da zahteve po obvarovanju varnosti ne pomenijo neutemeljen/prekomeren poseg v človekove pravice oz. temeljne inštitucije demokratične družbe.

Od zamisli do udejanjanja pa je pot še dolga, strma in vijugasta. Mnogo je bilo storjenega – še mnogo več pa bo potrebno narediti. In pri tem se je potrebno zavedati, da je tehnologija zgolj sredstvo za doseganje cilja. Prepogosto pa se nanjo gleda kot na nekakšno čudežno orodje, ki nas bo domala kar samo od sebe odrešilo vseh težav. Zanemarja pa se netehnološke vidike. Izrazito izstopajoča pa se, nasprotno, pojavlja potreba po ozaveščanju javnosti o pomenu in vlogi varovanja informacij, po obsežnejšem in kakovostnejšem izobraževanju in vzgoji o varnosti, postavitvi primernega pravnega okvira in ekonomskih spodbud v podporo tem prizadevanjem. Menim, da utegne imeti poenotenje na pravnem, gospodarskem, političnem, tehnološkem, organizacijskem in vseh ostalih merodajnih področjih znotraj naše družbe zelo pozitivne posledice – bodisi na nacionalni in mednarodni ravni. Sprejetje in primerno izvajanje standarda ISO 17799 je lahko korak v tej smeri. Za vse pravkar omenjeno pa sta potrebni trdna volja in pristna ter odločna zavezanost k doseganju skupnih ciljev s strani vseh vpletenih igralcev, javnih in zasebnih.

Literatura

1. Anderson Ross: Economics and Security Resource Page. Computer Laboratory, University of Cambridge.
[URL: http://www.cl.cam.ac.uk/users/rja14/econsec.html], 15.03.2004.

2. Anderson Ross: Why Information Security is Hard – An Economic Perspective. Computer Laboratory, University of Cambridge.
[URL: http://www.acsac.org/2001/papers/110.pdf], 15.03. 2004a, 8 str.

3. Anderson Ross: Open and Closed systems are equivalent (that is, in an ideal world). Computer Laboratory, University of Cambridge.
[URL: http://www.cl.cam.ac.uk/ftp/users/rja14/toulousebook.pdf], 15.03.2004b. 15 str.

4. Anderson Ross: Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore. Computer Laboratory, University of Cambridge.
[URL: http://www.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf], 15.03.2004c. 13 str.

5. BECC-Bled Electronic Commerce Conference: "e-Everything: e-commerce, e-government, e-household, e-democracy : Proceedings". Volume 1: Research. Fourteenth Bled Electronic Conference. Kranj : Moderna organizacija, 2001. 816 str.

6. Chapple James: The hacker on your side. CSC World : Winter 2002. El Segundo, USA : Computer Sciences Corporation, 2002, str. 14-17.

7. Dunn William: Designing safety-critical computer systems. IEEE Computer, Washington, IEEE Computer Society Press, 36 (2003), 1., str. 40-46.

8. ECIS - European Conference of Information Systems : Global co-operation in the new millennium: proceedings of the 9th European Conference on Information Systems, volume 1. Kranj : Moderna Organizacija, 2001. 606 str.

9. Ghosh Sumit: Principles of secure network systems design. XXVI. Berlin : Springer Verlag, 2002. 209 str.

10. Gordon Lawrence, Loeb Martin: Return on information security investments: myths vs. realities. Strategic finance. november 2002, 84, 5, str. 26-31.

11. Gradišar, Resinovič: Informatika v poslovnem okolju. 1. natis. Ljubljana : Ekonomska fakulteta, 1996. 479 str.

12. JEC: Security in the information age. New challenges, new strategies. JEC – Joint Economic Committee. United States Congress, 2002. str. 1-19

13. Kunreuther, Heal, Orszag: Interdependent security: implications for homeland security policy and other areas. Policy Brief, no. 108.The Brookings Institution. 2002.
[URL: http://www.brookings.edu/comm/policybriefs/pb108.pdf], marec 2004. 8 str.

14. Makarovič Boštjan: "Drafting E-legislation: Amendments to Existing Legislative Instruments or a New Information Society Act ". 18th BILETA Conference : Controlling Information in the Online Environment. 2003
[URL: http://www.bileta.ac.uk/03papers/makarovic.html], 02.04.2004

15. Odlyzko Andrew: Economics, Psychology and Sociology of Security. Digital Security Center, University of Minnesota.
[URL: http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf], 15.03.2004. 8 str.

16. Odlyzko Andrew: Privacy, Economics, and price discrimination on the Internet. Extended abstract. Digital Security Center, University of Minnesota.
[URL: http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf], 17.03.2004a. 18 str.

17. Pepevnik Prodnik Vesna: Marketinški vidiki uvajanja elektronskega poslovanja v slovenska podjetja. PDMEP - Posvetovanje diplomantov in magistrantov s področja elektronskega poslovanja. Zbornik posvetovanja. Tretje posvetovanje diplomantov in magistrantov s področja elektronskega poslovanja. Kranj : Moderna organizacija, 2001. 120 str.

18. Pepper Bill: Passing past the guard. CSC World : winter 2002. El Segundo, USA : Computer Sciences Corporation, 2002.
[URL: http://www.csc.com/aboutus/uploads/worldwinter02.pdf], 17.03.2004, str. 22-23.

19. SURS: Elektronsko poslovanje in statistika. Zbornik referatov 9. mednarodnega statističnega posvetovanja. Ljubljana : Statistični Urad RS, 1999, 464 str., graf. prikazi, tabele.

20. Varian Hal. Managing Online Security Risks. New York, ZDA : New York Times, 2000.
[URL: http://partners.nytimes.com/library/financial/columns/060100econ-scene.html], 17.03.2004.

21. Ward Steve. BS 7799 – What's the point?. SWA, 2003.
[http://www.swa-solutions.com/Publications/BS7799_WhitePaper.pdf], 17.03.2004, 12 str.

Viri

1. CSI – Computer Security Institute: 2003 Computer Crime and Security Survey. San Francisco, ZDA : CSI, 2004.

2. Evropska Unija: eEurope+ 2003 Progress Report. 2004. [URL:http://europa.eu.int/information_society/topics/international/regulatory/eeuropeplus/index_en.htm], 17.03.2004**.**

3. Internet Security Intelligence Briefing – July 2004. Verisign UK ltd. **[**URL: http://www.verisign.com/static/006583.pdf], 05.09.2004. 13 str.

4. ISO/IEC 17799: 2000. Mednarodni standard. Informacijska tehnologija – kodeks varovanja informacij. Prva izdaja. Mednarodna organizacija za standardizacijo/Mednarodna elektrotehniška komisija. 2000.

5. Definicija elektronskega poslovanja. RIS (Raba Interneta v Sloveniji). **[**URL: http://www.ris.org/si/ris99/epodef.html], 15.03.2004.

6. RIS2002 : Podjetja : Internet in informacijske tehnologije. Comparisons Slovenia - EU: Enterprises 2002. [URL:http://www.sisplet.org/ris/uploads/publikacije/2003/SIBIS_RIS_DMS_october_2003_x_vesna4.doc], 15.03.2004.

7. RIS2002 : podjetja : Internet in informacijske tehnologije. RIS. [URL: http://www.sisplet.org/ris/uploads/publikacije/2003/25 uporaba interneta in ict.pdf], 15.03.2004a.

8. RIS2002 : podjetja : Elektronsko poslovanje. RIS. [URL: http://www.sisplet.org/ris/ris/vnosi/Upload/uploadFiles/eposlovanje1.pdf], 15.03.2004b.

9. SANS Institute: The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus. SANS Institute, 2003. [URL: http://www.sans.org/top20/], 16.03.2004.

10. SIBIS: Country report No. 10. Fakulteta za družbene vede. Ljubljana, 2003. [URL: http://www.sisplet.org/ris/ris/dynamic/readpublications.php?sid=40], 16.03.2004.

11. Slovar ITkT. Ljubljana : Laboratorij za telekomunikacije, Fakulteta za Elektrotehniko, Univerza v Ljubljani. [URL: http://www.ltfe.org], 15.03.2004.

12. UK businesses lose £billions in Intellectual Property (IP) theft. Ibas a/s. [URL: http://www.ibas.com/news/disk-doctor-services.htm], 15.03.2004.

13. The weakest link : Survey - Digital security. The Economist. 24. okt. 2002. [URL: http://www.economist.com/surveys/displayStory.cfm?story_id=1389553], 17.03.2004.

Slovarček tujih izrazov

-ADSL (asymmetric digital subscriber line): nesimetrični digitalni naročniški vod
-applicable risk: merodajno tveganje
-B2B (business to business): podjetje s podjetjem
-B2C (business to consumer): podjetje s porabnikom
-backdoor: zadnja vrata
-bank run: naval na banke
-blue collar: plavi ovratnik
-buffer: medpomnilnik
-cost-benefit analysis: analiza stroškov in koristi
-Denial of Service (DoS) attack: napad zavrnitve storitve
-DDoS attack (Distributed Denial of Service attack) : zavrnitev storitve pri porazdeljenem napadu
-egress filtering: izstopno filtriranje
-fail-safe mode: odpovedno varen način
-fail-operate mode: način delovanja v primeru odpovedi sistema
-failure modes: načini odpovedi
-hoax: šala, potegavščina
-information warfare: informacijsko vojskovanje
-insiders: notranji ljudje
-interlock: zaporni (prekinitveni) mehanizem
-IRR (Internal rate of return): notranja stopnja donosa
-ISMS (Information Security Management System): sistem za ravnanje z informacijsko varnostjo
-leapfrog attacks: napadi s preskakovanjem
-message digest: izvleček obvestila
-monitoring: spremljanje
-NPV (Nett present value): neto sedanja vrednost
-outsourcing: zunanje izvajanje
-P2P (Peer to Peer): soležno vzajemno deljenje datotek
-promisc mode: promiskuitetni način
-proxy server: posredovalni strežnik
-reverse engineering: povratni inženiring
-security through obscurity: varnosti preko obskurnosti
-sniffer: vohljač
-social engineering: družbeni inženiring
-SSL (Secure Socket Layer): sloj varnih vtičnic
-surveillance: nadzor
-TLS (Transport Layer Security): varnost transportnega sloja
-transaction break: prekinitve v transakcijah
-watchdog timer: stražni mehanizem
-word of mouth: beseda od ust do ust