UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Simon Simčič

OGROŽANJE KRITIČNE INFORMACIJSKE INFRASTRUKTURE V REPUBLIKI SLOVENIJI

DIPLOMSKO DELO

LJUBLJANA 2007

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Simon Simčič
Mentor: red. prof. dr. Marjan Malešič
Somentor: asist. dr. Uroš Svete

OGROŽANJE KRITIČNE INFORMACIJSKE INFRASTRUKTURE V REPUBLIKI SLOVENIJI

DIPLOMSKO DELO

LJUBLJANA 2007

Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji

Informacijska tehnologija ima v današnjem času vedno večjo vlogo in vedno večji pomen v našem življenju. V diplomski nalogi želim ugotoviti, kako je v Republiki Sloveniji poskrbljeno za informacijsko varnost in kakšna je njena povezava z nacionalno varnostjo. Predstavil bom tudi varnostne mehanizme, s katerimi lahko zagotavljamo informacijsko varnost. Ti mehanizmi pa niso le tehnični, temveč tudi organizacijski in fizični. Prav tako bom opisal tiste akterje, ki informacijske sisteme ogrožajo, in na kakšne načine se jim lahko zoperstavimo. Opisal bom glavne državne akterje, ki so glede na svoje poslanstvo posredno ali neposredno zadolženi za varovanje kritične informacijske infrastrukture. V nalogi bom tudi pojasnil, kaj vse sestavlja kritično informacijsko infrastrukturo in na kakšen način je poskrbljeno za informacijsko varnost s strani države ter kako je za njo poskrbljeno v gospodarstvu. Posebno pozornost bom posvetil informacijski varnosti v državni upravi, kajti le-ta predstavlja tistega ključnega akterja, ki naj bi zagotavljal povezovanje različnih družbenih subjektov z namenom zagotavljanja informacijske varnosti.

Ključne besede: varnost, javna uprava, informacijsko vojskovanje.

Threats to Critical Information Infrastructure in the Republic of Slovenia

Information technology has an ever increasing role and importance in our daily lives. With this graduate paper I wish to establish the level of information security and its connection to national security in the Republic of Slovenia. Accordingly I will present security mechanisms with which we can assure information security. These mechanisms can be not only technical but also organizational and physical. I will also describe subjects that present a threat to information systems and different approaches to counter those threats. I will specify the principal governmental agencies that are tasked directly or indirectly with critical information infrastructure protection. In this paper I will also explain what presents critical information infrastructure in the Republic of Slovenia, which will include an analysis of approach to information security both in the government administration and in the private sector. I will specifically focus on information security in the public administration, due to its important role, which is one of liaison between different subjects in society with the intent to ensure information security.

Keywords: security, public administration, information warfare.

Kazalo

Seznam najpogosteje uporabljanih kratic **5**
1. UVOD **6**
2. METODOLOŠKO-HIPOTETIČNI OKVIR **8**
2.1 Opredelitev ciljev preučevanja / analize 8
2.2 Hipoteze 8
2.3 Ključne metode dela 8
2.4 Struktura analize 9
3. OPREDELITEV POJMOV/TERMINOV **10**
3.1 Informacijski sistem 10
3.2 Varnost 11
3.3 Kritična infrastruktura 12
3.4 Kritična informacijska infrastruktura 13
3.5 Sklep 15
4. DEJAVNIKI, KI VPLIVAJO NA VARNOST KRITIČNE INFORMACIJSKE INFRASTRUKTURE **16**
4.1 Ogrožanje kritične informacijske infrastrukture 17
4.2 Mehanizmi varovanja kritične informacijske infrastrukture« 21
4.2.1 CERT v Sloveniji 23
4.3 Standardi informacijske varnosti 23
4.4 Sklep 25
5. KRITIČNA INFRASTRUKTURA V SLOVENIJI **26**
5.1 Telekomunikacije in informacijska tehnologija 27
5.1.1 Stacionarno telefonsko omrežje 27
5.1.2 Mobilno GSM omrežje 28
5.1.3 Komutacijska paketna omrežja 29
5.1.4 Satelitske povezave in druge oblike javnih brezžičnih omrežij 30
5.2 Upravne storitve in informacijska infrastruktura v državni upravi 31
5.2.1 Vloga človeških virov 39
5.3 Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji 42
5.4 Sklep 45
6. ZAKLJUČEK **46**
7. LITERATURA **50**
7.1 Monografije 50
7.2 Članki 51
7.3 Internetne publikacije 52
7.4 Zakoni in uradne publikacije 54
7.5 Intervju 56

SEZNAM NAJPOGOSTEJE UPORABLJANIH KRATIC

GSM	Global System Mobile
CVI	Center vlade za informatiko
DEUP	Direktorat za E-upravo in Upravne procese
IKT	Informacijska tehnologija
CSIRT	Computer Security Incident Response Team
CERT	Computer Emergency Response Team
FBI	Federal Bureau of Investigation – Ameriški zvezni preiskovalni urad
ARNES	Akademska raziskovalna mreža Slovenije
ISP	Ponudnik internetnih storitev

1. UVOD

S hitrim razvojem informacijsko-komunikacijske tehnologije in njeno vedno večjo uporabnostjo se povečuje stopnja njene vpetosti v naše vsakdanje življenje. Preko interneta plačujemo račune, opravljamo določene upravne storitve, bolj podjetni preverjajo cene svojih delnic in obveznic ali z njimi celo trgujejo. Sorazmerno temu tako raste tudi naša odvisnost od neovirane uporabe in dostopa do informacij, posledično je od teh odvisna naša ekonomska dobrobit.

To skriva v sebi nove elemente ogrožanja naše varnosti, naših vrednot in zmanjšuje naš občutek varnosti. Oviranje dostopa do informacij in onemogočanje opravljanja elektronskih storitev, ki jih vsak posameznik pojmuje kot kritično, predstavlja v današnjem času prihajajočo grožnjo. V zadnjih letih se je med drugim prikazala v obliki napadov za omejevanje dostopa do informacij, napadov računalniških virusov in črvov, kraj identitete ipd.

Informacijski sistem sestavljajo prepletene mreže uporabnikov, ponudniki različnih storitev, telekomunikacijska omrežja in podporni elementi. Ta sistem je ključen tudi kot del splošne kritične infrastrukture, in sicer kot pomemben podporni element splošne infrastrukture. Splošna infrastruktura je od informacijskega sistema odvisna predvsem v smislu povečanja učinkovitosti in pogosto ne predstavlja pogoja za njeno delovanje.

Za takšen naslov naloge sem se odločil zato, ker me področje informatike zanima že od malih nog. Poleg tega sem zadnja leta delal na Centru vlade za informatiko v Sektorju za izdajo digitalnih potrdil, potem v Direktoratu za E-upravo in upravne procese (DEUP), poklicno pot nadaljujem v gospodarstvu, na področju informacijske varnosti. V tem obdobju sem tudi razvil zanimanje za delovanje zapletenih sistemov. Znanje, ki sem ga pridobil v praksi, želim še dodatno podkrepiti s teoretičnim znanjem.

Glede na svoje delovne izkušnje predvidevam, da bom ugotovil, da za informacijsko varnost ni dobro poskrbljeno. Pogosto sem se namreč srečeval z ureditvami na področju

informacijske varnosti, predvsem v državni upravi. Sistematične in dosledne rešitve so bile prej izjema kot pravilo. V tej nalogi želim tudi ugotoviti, zakaj je temu tako.

Zavedam se tudi dejstva, da je informacijska varnost težko merljiv kvantitaven empiričen pojav, še posebej glede na globalno naravo računalniških omrežij. Računalniška varnost pomeni tako zaščito uporabnika kot velikih informacijskih sistemov. Najmodernejši sodobni moderni mehanizmi napada na informacijske sisteme temeljijo ravno na nevednosti uporabnika na področju informacijske tehnologije. Občutek varnosti je, tako kot na drugih področjih, varljiv.

2. METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 Opredelitev ciljev preučevanja / analize

Namen te naloge je preučiti varnostno možnost uporabe informacijsko-komunikacijske tehnologije v naši družbi. V diplomski nalogi bom poskušal opredeliti glavne značilnosti pojmov: informacijsko bojevanje, informacijski sistem, varnost, kritična infrastruktura in kritična informacijska infrastruktura. Nadalje bom poskušal ugotoviti, na kakšen način predstavlja varovanje kritične informacijske infrastrukture za državo relevantno varnostno vprašanje in iz te problematike tudi izpeljal hipotezo. Ugotoviti želim, katere so sodobne grožnje informacijskim sistemom, s katerimi mehanizmi jih lahko varujemo in kakšno je trenutno stanje na tem področju v Sloveniji.

2.2 Hipoteze

Izhajajoč iz varnostne problematike lahko izpeljemo splošno hipotezo, ki pravi: čim večja je prepletenost družbe z informacijsko tehnologijo, tem večja je njena odvisnost od informacijske tehnologije, posledično tudi njena ranljivost.

Nadalje lahko iz tega izvedemo hipotezo, da država, ki je bolj odvisna od informacijske tehnologije, tudi več vlaga v varnostne mehanizme za zaščito informacijskih sistemov, kar želim preveriti na primeru Slovenije. Mehanizmi za varovanje informacijske infrastrukture v Sloveniji so fizični, tehnološki in organizacijski.

2.3 Ključne metode dela

Pri oblikovanju diplomske naloge sem uporabil več metod, da bi raziskal problematiko, ki je z njo povezana. Preden sem pričel pisati nalogo, sem z metodo zbiranja virov zbral in predelal razpoložljivo literaturo, ki je vključevala znanstvene monografije, strokovne članke, uradne dokumente. Pri pisanju uvoda sem uporabil metodo analize vsebine primarnih in sekundarnih virov, prav tako pri opredelitvi ključnih pojmov in konceptov. Pri opisu dejavnikov, ki vplivajo na varnost kritične informacijske infrastrukture, sem uporabil predvsem opisno metodo, da bi opisal vse dejavnike, ki odločilno vplivajo nanjo. Opisno

metodo sem uporabil tudi v nadaljevanju, ko sem predstavil strukturo kritične informacijske infrastrukture v Republiki Sloveniji.

Ta naloga raziskuje vplive na področje informacijske tehnologije z obramboslovnega vidika, vendar pa je za celovito razumevanje področja informacijske tehnologije potrebno vključiti tudi tehnično znanje s področja informacijske varnosti. V nalogi se tako prepletata tehnični in družboslovni pristop.

2.4 Struktura analize

V uvodnem poglavju sem podal nekaj splošnih ugotovitev o informacijskih sistemih in njihovi vlogi v sodobni družbi, hkrati tudi moj pogled na predstavljeno problematiko. V nadaljevanju sem opredelil metodološko hipotetični okvir, kjer opišem cilje in namen preučevanja naloge, opisal sem tudi ključne uporabljene metode, ki sem jih uporabil pri pisanju in zastavil hipoteze.

V naslednjem - tretjem poglavju - bom opredelil temeljne pojme, na katerih temelji analiza, ter njihove temeljne značilnosti. To so informacijski sistem, varnost, kritična infrastruktura in kritična informacijska infrastruktura. Širina zastavljenih pojmov postavlja nalogo v širok okvir.

V četrtem poglavju bom bolj podrobno opisal koncept kritične informacijske infrastrukture, kaj jo sestavlja, kateri splošni dejavniki vplivajo nanjo in kateri so glavni viri ogrožanja, ki grozijo uporabnikom in informacijskim sistemom, ter kakšni so splošni mehanizmi varovanja obeh.

V petem poglavju se bom posvetil Sloveniji. Najprej bom ugotovil, kaj spada v kritično infrastrukturo v Sloveniji in potem ugotovil, kaj sestavlja kritično informacijsko infrastrukturo v Sloveniji, katere institucije so odgovorne za varnost le-te, ter na kakšen način jo lahko varujemo.

V zadnjem poglavju bom strnil ugotovitve, preveril pravilnost postavljenih hipotez ter podal sklep in predloge za morebitna izboljšanja stanja na področju informacijske varnosti v Sloveniji.

3. OPREDELITEV POJMOV/TERMINOV

3.1 Informacijski sistem

Informacijski sistem je termin, ki ga lahko različno opišemo, definicija pa bo odvisna od izhodišča. Poglejmo najprej uradno definicijo termina informacijski sistem, kot jo opredeli Odbor za nacionalno varnost informacijskih sistemov in telekomunikacij Združenih držav Amerike. Opredeljen je kot celotna infrastruktura, osebje in komponente, ki so namenjene zbiranju, obdelovanju, hranjenju, oddajanju, prikazovanju, širjenju in dispoziciji informacij (internet 33). Ta definicija je zelo splošna, saj posameznih tehničnih delov informacijskega sistema ne člení dalje, hkrati opisuje samo funkcijo celotnega sistema. V definicijo so vključeni tudi ljudje, ki s sistemom upravljajo, to so predvsem administratorji, kot njegov del. Spletna enciklopedija Webopedia je bolj skopa. Po njeni definiciji je informacijski sistem tisti, ki zbira in hrani podatke. Tukaj govorimo samo o funkciji informacijskega sistema, ne pa o tem, kar ga sestavlja (internet 1).

Schneier, na primer, opiše bistvene značilnosti informacijskih sistemov (Schneier 2000: 6):

- kompleksni: že operacijski sistem namiznega računalnika je sestavljen iz več tisoč vrstic kode, računalniška mreža pa je lahko sestavljena iz tudi po 1000 računalnikov. Najpreprosteje to vidimo, ko pogledamo, kako veliki so današnji operacijski sistemi. Najnovejša različica operacijskega sistema Windows Vista zahteva osnovno trikrat več prostora in zmogljivosti računalnika kot predhodna različica Windows XP, ki je izšla leta 2001. Slika bo verjetno še bolj jasna, če dodam dejstvo, da je operacijski sistem DOS pred dobrimi 10 leti zasedal samo 3 diskete. Kompleksnost seveda raste z dodajanjem zmožnosti. Stari operacijski sistemi niso bili tako privlačni po videzu, kot so danes. Znali so delati samo eno stvar hkrati, niso se znali povezati z internetom ipd.;
- interaktivni: sistemi se povezujejo z drugimi sistemi, da tvorijo še večje sisteme. Internet je prepletel vsak večji sistem na svetu. Bistvo interaktivnosti je, da sistemi dajejo, prejemajo in medsebojno izmenjujejo informacije;
- emergentni: pomeni, da ne delujejo tako, kot so si to predstavljali razvijalci ali uporabniki. Poglejmo v preteklost, ko so izumili telefon. Sprva so si ga zamislili

kot sredstvo, s katerim bodo naslovnika telegrama obvestili, da prihaja telegram. Tako je tudi z vsako novejšo tehnologijo. Pogledamo lahko na razmah piratstva, ki ga je prinesel internet. Tega postranskega pojava si nedvomno nobeden od prvotnih razvijalcev ni predstavljal ali pričakoval. Statistike internetnega prometa so pokazale, da večino podatkovnega prometa na internetu, več kot 60%, ustvarijo programi za izmenjavo datotek, kot sta na primer bittorent in e-mule (internet 18);

- hroščavi: hrošč je posebna oblika napake. To je emergentna lastnost sistema in ni zaželjena. Ko ima sistem hrošča, se lahko odzove na poseben način in verjetno nerazložljivo, včasih celo neponovljivo. Hrošči so edinstveni glede na sistem. Stroji se lahko pokvarijo, vendar ima le sistem lahko hrošča (Schneier 2000: 6). Pojem »hrošča« izhaja iz računalniške zgodovine, kjer so se med izračuni na prvem računalniku pojavljale naključne neponovljive napake. Med pregledom »drobovja«, računalnik je bil namreč velikosti večje sobe, so ugotovili, da se je v eno elektronko splazil hrošč in povzročal te motnje.

3.2 Varnost

Varnost lahko razumemo kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave. Nadalje lahko nacionalno varnost razumemo kot varnost državnega ozemlja (vključno z zračnim prostorom in ozemeljskimi vodami), varnost življenja ljudi in njihove lastnine, ohranitev in vzdrževanje nacionalne suverenosti ter uresničevanje temeljnih funkcij družbe (socialne, gospodarske, družbenopolitične, kulturne, ekološke idr.). Zagotavljanje varnosti je institucionalizirano v nacionalno-varnostnem sistemu. Nacionalno varnostni sistem sestavlja (Grizold 1999: 25):

Varnostna politika. Varnostno politiko v širšem smislu opredelimo kot dejavnost države za pripravo pred ogrožanjem iz okolja. Cilj varnostne politike je zasnova mehanizmov in sredstev, s katerimi se zagotavljata notranja in zunanja varnost družbe. Vključuje zunanjo, obrambno, gospodarsko, socialno, ekološko, zdravstveno, energetsko, izobraževalno in kulturno politiko.

Varnostna struktura. Varnostna struktura je namenjena zagotavljanju varnosti na ravni celotne družbe in je sestavljena iz dveh prvin: obrambne in notranje-varnostne. Naloge

obrambne prvine so predvsem spopadanje z vojaškim ogrožanjem družbe in skrb za nemoteno delovanje različnih podsistemov v vojni.

Iz zgoraj navedene definicije lahko sklepamo, da napad na informacijsko infrastrukturo predstavlja nacionalno varnostno vprašanje, kajti v primeru uspešnega napada bi bilo moteno normalno delovanje družbe kot celote. V nadaljevanju si bomo pogledali, kako je kritična informacijska infrastruktura vpeta v družbo in zakaj predstavlja problem na ravni nacionalne varnosti. V naslednjih poglavjih si bomo tudi pogledali varnostno politiko in varnostno strukturo Slovenije na tem področju, kdo so vsi akterji na tem področju in kakšne naloge opravljajo.

3.3 Kritična infrastruktura

Tukaj bi bilo potrebno najprej opredeliti pojem kritične infrastrukture. Ta pojem je definirala Komisija predsednika ZDA za kritično infrastrukturo, definicijo sta povzeli (Dunn, Wigert 2004: 24) kot mrežo neodvisnih, večinoma zasebnih, antropogenih sistemov in procesov, ki delujejo skupno in sinergično, da bi ustvarili in usmerjali stalen tok pomembnih dobrin in storitev.

Kritična infrastruktura je opredeljena tudi v Patriot Act-u iz leta 2001, opredeli jo tako, da vključuje sisteme in sredstva, bodisi fizične ali navidezne, ki so tako pomembni za Združene države Amerike, da bi onesposobitev ali uničenje imelo omejujoč učinek na varnost, nacionalno ekonomsko varnost, nacionalno javno zdravje ali varnost ali kombinacijo le-teh (internet 24).

Kot vidimo v definiciji infrastrukture, je poleg infrastrukture oziroma objekta samega pomembno tudi samo delovanje objekta oziroma tiste storitve, ki jih nudi. Sklepamo lahko, da ni potrebno zaščititi samo samega objekta - infrastrukture, temveč storitve, ki jih zagotavlja. To pa spet ne drži, ko govorimo o simbolni kritičnosti, na primer, spomenik ali drug državni simbol. Ko govorimo o sistemski kritičnosti, lahko postavimo pomožne zmogljivosti, ki bi lahko v primeru izpada kritičnih elementov nadomestila njegovo funkcijo. Definicijo kritične infrastrukture je sicer res sestavila ameriška administracija, vendar je lahko splošno veljavna. Če gremo korak dlje in natančneje opredelimo, kaj spada pod pojem kritične infrastrukture, nam bo bolj jasno, kaj vse ta pojem obsega. Obseg

kritične infrastrukture sem pridobil iz statistične obdelave, ki jo bom potem tudi uporabil na primeru Slovenije. Vsaka država, ki je bila opisana v priročniku CIIP Handbook, je drugače opredelila kritično infrastrukturo, sam sem preprosto vzel najpogostejše pojme, ki si sledijo v tem vrstnem redu: energetika (oskrba z električno energijo, tudi oskrba z plinom in naftnimi derivati), telekomunikacije in IT, oskrba z vodo, reševalne službe (tudi policija), bančništvo in finančni sektor ter transport in upravne storitve (tudi E-uprava). To so torej vse tiste storitve, brez katerih država ali družba ne moreta normalno delovati, če torej ne delujejo elementi kritične infrastrukture ali je delovanje teh elementov moteno.

3.4 Kritična informacijska infrastruktura

Kritična informacijska infrastruktura je opredeljena v priročniku CIIP Handbook kot kritična informacijska infrastruktura in je tisti del splošne ali nacionalne kritične infrastrukture, ki je nujno potreben, da se zagotovi kontinuiteta storitev kritične infrastrukture (Dunn, Wigert 2004: 19). Kritična informacijska infrastruktura večinoma sestoji iz informacijskih in telekomunikacijskih sestavin, toda kljub temu ni popolnoma skladna z informacijskim in telekomunikacijskim sektorjem. Vključuje sestavine telekomunikacij, strojne in programske računalniške opreme, internet, satelitske komunikacije, optična vlakna, ipd. (Dunn, Wigert 2004: 20). Vidimo torej, da informacijska infrastruktura podpira delovanje kritične infrastrukture. Ob nedelovanju informacijske infrastrukture sistem kritične infrastrukture verjetno ne bo razpadel, bo pa deloval neučinkovito. Drugače je, če govorimo o podatkih, ki bi jih nekdo ukradel iz tega sistema in jih uporabil za lastno korist. Škoda bi bila najverjetneje neprimerno večja zaradi močno zmanjšanega občutka varnosti, če govorimo o vdoru v elektronski bančni sistem ali če bi neka kriminalna združba prišla do številk kreditnih kartic vseh strank velikega podjetja, kot smo to imeli priložnost videti v primeru kraje podatkov z bančnih kartic slovenskih bank (internet 20).

Še posebej pomembno je varovanje kritične informacijske infrastrukture zaradi:

- njene velike in neprecenljive vloge v gospodarstvu,
- povezovalne vloge, ki jo igra pri povezavi različnih sektorjev kritične infrastrukture (Dunn, Wigert 2004: 19).

Smiselno bi bilo tudi pogledati, kako različne države obravnavajo to tematiko. Avstralci opredeljujejo informacijsko infrastrukturo takole: »vključuje nacionalno omrežje, znotraj

katerega se prenašajo, obdelujejo in shranjujejo informacije; vključuje tudi ljudi, ki upravljajo in vzdržujejo to omrežje, in informacije same« (Dunn, Wigert 2006: 35).

Kanadska kritična infrastruktura je sestavljena iz fizičnih objektov ali objektov informacijske tehnologije, mrež, storitev ali sredstev. Njihovo delovanje in obstoj sta izredno pomembna za zdravje, varnost in ekonomsko dobrobit prebivalcev Kanade ter za učinkovito delovanje kanadskih vlad (internet 32).

Nizozemska kritična informacijska infrastruktura je sestavljena pretežno iz notranje podporne infrastrukture posameznih kritičnih sektorjev, kot so energetika, transport in finančni sektor, dodatno jo podpira še skupek storitev telekomunikacijskega in sektorja energetike. Eksplicitno se ne obravnava kot infrastruktura sama po sebi (Dunn 2004: 126).

Po teh definicijah lahko vidimo, da ne obstaja neka splošno veljavna ali splošno sprejeta definicija kritične informacijske infrastrukture. Vsaka država kritično infrastrukturo definira sama glede na svoje posebnosti. Kot vidimo, vse zgoraj naštete države vključujejo fizično komponento informacijskega sistema. V kanadskem primeru je informacijska infrastruktura vpeta že v definicijo kritične infrastrukture in ni podrobneje razdelana. Zanimivo je dejstvo, da je opredeljen termin ekonomske dobrobiti državljanov, česar ne najdemo pri drugih, oziroma je opredeljen implicitno s terminom nemoteno delovanje družbe.

V avstralskem primeru so eksplicitno omenjeni še podatki, storitve oziroma informacije, ki potujejo po tej infrastrukturi, hkrati je kot kritično opredeljeno tudi osebje, ki to omrežje upravlja, ter znanje, ki ga pri tem pridobi. V nizozemskem primeru je informacijska infrastruktura omenjena zgolj kot podporna dejavnost drugim sektorjem kritične infrastrukture in ločeno ni definirana. V definicijo so sicer vključene tudi storitve telekomunikacij, vendar informacije oziroma podatki sami niso izrecno omenjeni. Moje mnenje je, da je kritična informacijska infrastruktura včasih podporna dejavnost kritični infrastrukturi, včasih pa igra vlogo kritične infrastrukture, vendar je to razmejeno s stopnjo odvisnosti države in njenih subjektov od informacijske tehnologije. Torej, bolj ko je država odvisna od informacijske tehnologije, bolj postaja kritična informacijska infrastruktura »kritična« infrastruktura. To je mogoče najbolj razvidno v velikih proizvodnih podjetjih, ki sestavljajo zapletene stroje, ki potrebujejo veliko sestavnih delov. V raziskavi, ki jo je objavil Dynes v sklopu WEIS (Workhop on economics of information security), je razvidno,

da večdnevni izpad informacijske infrastrukture (predvsem internetne povezave) najbolj vpliva na avtomobilsko industrijo (Scott 2006: 13). Koordinacija dobave podsklopov je bila močno otežena, kar je po enem tednu povzročilo močan upad proizvodnje. Posledice so bile vidne še en mesec po ponovno vzpostavljenem delovanju komunikacij. Omenjeno je sicer bilo avtomobilsko podjetje, vendar bi najverjetneje takšen izpad imel podobne posledice za kakršnokoli veliko podjetje, ki je močno odvisno od koordinacije velikega števila dobaviteljev in kjer je končni izdelek kompleksen.

3.5 Sklep

V tretjem poglavju smo si pogledali opredelitev splošnih pojmov, kot so varnost, kritična infrastruktura in kritična informacijska infrastruktura, koncept kritične infrastrukture smo povezali s pomenom kritične infrastrukture v družbi. Posebej smo si še pogledali, kako kritično informacijsko infrastrukturo opredeljujejo v različnih državah. V naslednjem poglavju si bomo koncept kritične informacijske infrastrukture ogledali bolj podrobno. Pogledali bomo, kateri dejavniki vplivajo na varnost kritične informacijske infrastrukture, kateri so viri ogrožanja kritične informacijske infrastrukture in s katerimi mehanizmi jo varujemo.

4. DEJAVNIKI, KI VPLIVAJO NA VARNOST KRITIČNE INFORMACIJSKE INFRASTRUKTURE

Splošno lahko rečemo, da kritično informacijsko infrastrukturo na različnih ravneh tvorijo informacijski sistemi z različno kompleksnostjo – od velikih računalniških mrež do enega samega računalnika. Če torej začnemo splošno, lahko vidimo, da ločimo 3 vrste dogodkov, ki ta sistem lahko poškodujejo, in sicer (Dunn 2005: 14):

- okvare (failure) so posledice napak v zasnovi sistema ali zunanjega elementa, od katerega je sistem odvisen. Lahko so strojnega ali programskega izvora. Večinoma izvirajo iz sistema samega;
- nesreče vključujejo celoten razpon naključnih in morebitnih škodljivih dogodkov, kot so naravne nesreče, in splošno izvirajo iz okolja;
- napadi so morebitno škodljivi dogodki, ki jih pripravi nasprotnik.

Največ pozornosti se posveča zadnji kategoriji. Grožnje, s katerimi se soočajo informacijski sistemi, lahko pridejo tako od znotraj kot od zunaj. Tisti, ki ogrožajo sistem od znotraj, so škodoželjni uslužbenci in nekdanji zaposleni, ki imajo dostop do informacijskega sistema in ta dostop zlorabijo, da bi povzročili škodo. Verjetnost grožnje od znotraj je statistično pogostejša kot grožnja od zunaj (Dunn 2005: 14). Možnosti okvare in nesreče se lahko zoperstavimo predvsem z vzpostavitvijo nadomestnih sklopov ali celotnih nadomestnih informacijskih sistemov.

Kot smo že omenili, sestavlja kritično informacijsko infrastrukturo poleg materialne tudi nematerialna komponenta. Predstavil bi varnostne implikacije za obe. Zagotavljanje varnosti materialne komponente je relativno preprosto, saj je fizično in prostorsko omejena. V primeru velikih informacijskih sistemov je pogosto omejena v eni zgradbi, kar sicer olajša logistiko, vendar takšna centralizacija prinaša druge grožnje. V primeru velike naravne nesreče (potres, poplava ali požar) je verjetnost močnega fizičnega poškodovanja zgradbe, s tem narašča tudi možnost uničenja informacijskega sistema in podatkov, ki jih hrani. Primer vzpostavitve nadomestnih informacijskih sistemov je na primer NIC (nadomestni informacijski centra), bivšega Centra vlade za informatiko in sedanjega Ministrstva za javno upravo. Varnostni mehanizmi, ki se tam vzpostavljajo, jamčijo delovanje informacijskih

registrov tudi v primeru fizičnega uničenja osnovne lokacije. Varnostne implikacije za nematerialni del kritične informacijske infrastrukture so veliko bolj zapletene zaradi sledečih dejavnikov (Dunn 2005: 17):

- anonimnost akterjev: zagotavljanje anonimnosti je preprosto, dodaten problem predstavlja časovni razpon med dejanskim vdorom in učinki tega vdora. Prav tako razširjanje in dostopnost napredne računalniške tehnologije otežuje identifikacijo akterjev;
- odsotnost meja: škodoželjnih računalniških napadov ne omejujejo politične ali geografske meje. Napadi lahko izvirajo od kjerkoli na svetu in iz večih različnih lokacij sočasno – teh je lahko tudi nad 10.000. Poizvedbe, ki sledijo nizu teh lažnih sledi, ki jih je nekdo nastavil namerno, so lahko zelo zahtevne v pogledu tega, koliko časa in sredstev vložimo v to;
- hitrost razvoja: hiter razvoj tehnologije ima za posledico to, da je čas med razkritjem nove ranljivosti in orodjem, ki to ranljivost izkorišča, zelo kratek;
- nizka cena sredstev: tehnologija, ki se pri teh napadih uporablja, je preprosta, cenovno dostopna in zelo razširjena. Orodja za vdore lahko dobimo na različnih spletnih straneh, prav tako lahko dobimo orodja za šifriranje in za zagotavljanje anonimnosti;
- avtomatizirane metode: metode napadov so postale avtomatizirane in bolj napredne, kar se kaže v večji škodi, ki jo lahko povzroči en sam napad.

4.1 Ogrožanje kritične informacijske infrastrukture

Grožnje lahko razdelimo na nestrukturirane in strukturirane, kot jih opiše Dunn. Nestrukturirane grožnje so naključne in omejene. To grožnjo predstavljajo nasprotniki z omejenimi sredstvi in organizacijo ter omejenimi cilji. Ti akterji imajo omejena sredstva, orodja, znanja in finančno podporo, da bi uspeli izvesti zapleten napad. Ta tip grožnje ne predstavlja grožnje nacionalni varnosti. Vendar lahko takšni napadi povzročijo precejšnjo škodo, če jih spremlja sreča ali jim manjka presoje (Dunn 2005: 15).

Strukturirane grožnje so veliko bolj sistematične in z boljšo podporo. Nasprotniki imajo obveščevalno podporo iz večjega števila virov, obsežno finančno podporo, organizirano profesionalno podporo in dolgoročne cilje. V to kategorijo spadajo tuje obveščevalne službe, kriminalni elementi in profesionalni hekerji, ki se ukvarjajo z informacijskim bojevanjem.

Čeprav nestrukturirana grožnja ne predstavlja neposredne grožnje, pa obstaja bojazen, da bi akter strukturirane grožnje lahko deloval ali se predstavljal kot akter nestrukturirane grožnje (Dunn 2005: 15).

Naj nadalje še opišemo, kdo so dejansko tisti, ki bi lahko ogrozili informacijsko infrastrukturo oziroma informacijske sisteme. Po Schneierju so to hekerji, osamljeni zločinci, škodoželjni zaposleni, industrijski vohuni, mediji, organizirane kriminalne združbe, obveščevalne službe in informacijski bojevniki (Schneier 2000: 43).

- Hekerji

  Heker je oseba, ki eksperimentira z omejitvami sistema zaradi radovednosti ali samega užitka. Hekerji se po tej definiciji ukvarjajo z vdiranjem v sisteme predvsem ljubiteljsko in niso organizirani. Opiše jih tudi kot stereotipno mlade, moške in na družbenem robu. Hekerske skupnosti ne morete združiti, napadejo kar lahko. To je torej razpršena skupina ljudi, ki udari, kjer lahko in tudi tekmuje med seboj in ni homogena. Motivira jih pa predvsem lastni ego, uporništvo in izziv, ki ga vdor predstavlja (Wenger v Svete 2006: 37).

- Osamljeni zločinci in organizirane kriminalne družbe

  Ti povzročijo največ računalniškega zločina. Pogosto nimajo dovolj denarja, znanja ali dostopa. Napadli bodo poslovne sisteme, ker je tam denar. Njihov prvi motiv je pohlep. Kot taki ne predstavljajo grožnje delovanju informacijskega sistema temveč denarju njegovih uporabnikov.

  Organizirane kriminalne združbe uporabljajo tehnologijo na dva načina. Po prvem načinu izvajajo zločinska dejanja tako, da uporabljajo orodja za vdiranje v bančne računalnike, po drugem pa tako, da tehnologijo uporabijo za vodenje in organizacijo drugih poslov. Skratka, uporabljajo bolj prefinjene metode kot posamezni zločinci, ker imajo več sredstev, s katerimi lahko kupijo znanje in dostop do sistema. Mogoče je bil najbolj aktualen primer delovanja organiziranih kriminalnih družb množična zloraba bančnih kartic, zaradi česar so banke zaradi suma zlorabe preklicale skoraj 2000 bančnih kartic. Največjo škodo, ki je nastala, vidim predvsem v izgubi zaupanja uporabnikov v sistem brezgotovinskega plačevanja, ker banke niso postregle s celovito razlago, kako je prišlo do zlorabe. Njihov molk celo nakazuje na možnost, da ne vedo, kako je prišlo do zlorabe.

Prav tako nakazuje, da sta edini resnično varni transakciji, ki ju opravimo z bančno kartico le na bančnem okencu ali na bankomatu, ki je fizično varovan (internet 20).

- Škodoželjni zaposleni (Malicious Insider)

  On je že znotraj sistema, obramba okoli sistema pa ga ne skrbi. Veliko računalniških sredstev se poskuša spoprijeti z zunanjo grožnjo, vendar so nemočni proti notranjemu nasprotniku. Kako daleč so te osebe pripravljene iti, je odvisno od njihove motivacije, torej preprost pohlep ali višji cilj. Razlog, zakaj notranja grožnja predstavlja takšno nevarnost, je v tem, da večina varnostnih mehanizmov, ki jih organizacije vzpostavljajo, ščiti pred zunanjimi grožnjami (Cole, Ring 2006: 8). Hkrati je tudi zaščita pred človekom, ki bi mu morali zaupati, zelo težavna. Obseg te grožnje nam prav tako ni znan, saj veliko primerov zlorab, ki jih povzročijo škodoželjni zaposleni, ni prijavljenih. Problematiko škodoželjnega zaposlenega bom zaradi obširnosti opisal kasneje. Za ilustracijo bi samo opisal enega večjih bančnih ropov, ki ga je izvedel nekdo, ki se je predstavljal za zaposlenega v neki banki v ZDA, kjer si je denar preprosto nakazal na svoj račun. Šlo je za 10 milijonov dolarjev. To je bilo leta 1978, vrednost tega denarja bi danes najverjetneje dosegla 30 milijonov dolarjev (Mitnick 2003: 21). Ta oseba sicer ni bila zaposlena pri banki sami, temveč je bila zaposlena pri podizvajalcu, ki je izvajal vzpostavitev pomožnega sistema za prenos sredstev.

- Industrijski vohuni

  Cilj industrijskega vohunjenja je predvsem pridobiti prednost pred konkurentom, saj stroški vohunjenja predstavljajo le desetino tistega, kar bi porabili, če bi tehnologijo razvili sami. Povzročitelji niso pripravljeni veliko tvegati, kajti v primeru razkritja lahko vohunjenje povzroči veliko škode tistemu, ki se s to dejavnostjo ukvarja.

- Mediji

  Medije si lahko predstavljamo kot podvrsto industrijskega vohuna, s to razliko, da je njihov motiv pridobitev materiala za zgodbo, ki je vredna objave.

- Policija

Policijo si lahko predstavljamo kot nacionalno obveščevalno službo, ker deluje na zakonski osnovi. Tukaj gre predvsem za problem zagotavljanja zasebnosti in ga ne bom posebej obravnaval.

- Teroristi

  Teroristične skupine so bolj usmerjene k temu, da povzročajo škodo, kot da pridobivajo informacije. Teroristične skupine ne uporabljajo tehnološko dovršenih metod, saj jim manjka strokovno znanje. Podobno po poročilih medijev meni tudi FBI (internet 6).

- Državne obveščevalne službe

  To je najbolj dostojen nasprotnik, ki ima zelo dobro finančno podporo, ker dostikrat deluje kot vojaška veja. Pogosteje je njihov namen pridobivanje informacij in ne povzročanje škode.

- Informacijski bojevniki

  Informacijski bojevnik je vojaški nasprotnik, ki poskuša spodkopati zmožnost cilja tako, da vodi vojno z napadi na informacijsko ali omrežno infrastrukturo. Ta nasprotnik ima vsa sredstva obveščevalne organizacije, vendar se razlikuje v tem, da je osredotočen na kratkoročen cilj onesposabljanja nasprotnika in ne na pridobitev dolgoročnih obveščevalnih podatkov.

Če povzamemo, lahko vidimo, da predstavljajo kritični informacijski infrastrukturi grožnjo predvsem hekerji, škodoželjni zaposleni, teroristi in infobojevniki. Pri drugih gre bolj za problematiko ogrožanja zasebnosti posameznika, kar pa ni predmet te naloge. Hkrati to lahko povežemo z strukturo groženj, da edino informacijski bojevnik predstavlja obliko strukturirane grožnje. Vsi drugi (hekerji, škodoželjni zaposleni in teroristi) predstavljajo predvsem nestrukturirano grožnjo. Informacijski bojevniki uporabljajo metode nestrukturiranih groženj, s to razliko, da te metode uporabljajo povezano in sistematično. Prav zaradi tega bi jih brez analize verjetno težko ločili od nestrukturiranih oblik groženj.

4.2 Mehanizmi varovanja kritične informacijske infrastrukture«

Država ima pri zaščiti kritične infrastrukture nedvomno veliko vlogo. Raznolikost in obširnost pojma kritične infrastrukture pa pomeni, da skrb za kritično infrastrukturo spada v domeno različnih državnih in nedržavnih institucij. Varovanju kritične informacijske infrastrukture lahko pristopimo z več idealnih vidikov (Dunn 2004: 21) :

- tehnični: zagotavlja se na tehnični ravni s poudarkom na omrežni varnosti. V tem pogledu se z grožnjami soočimo s tehničnimi sredstvi, kot so požarne pregrade, protivirusna programska oprema, avtentikacijskih mehanizmov in ustanovitev CERT in CSIRT skupin. Požarne pregrade oziroma »firewalls« si lahko razlagamo kot varnostnika na vratih, kjer ti prepuščajo le koristen podatkovni promet. Funkcija požarne pregrade je zavračanje in sprejemanje določenega podatkovnega prometa. Naloge CERT in CSIRT so preventivno delovanje. Podrobneje jih bom predstavil v nadaljevanju.
- na ravni podjetja: varovanje kritične infrastrukture se tukaj razume kot zagotavljanje stalnega delovanja. To pomeni stalen dostop do informacijske infrastrukture in stalno delovanje poslovnih procesov, da bi se doseglo zadovoljivo poslovno delovanje. Sredstva za dosego teh ciljev, poleg organizacijskih in človeških dejavnikov, vključujejo tiste, ki so bili našteti pri tehničnem vidiku. Nekatere države na ta način pristopajo k varovanju informacijske infrastrukture.
- vidik organov pregona: organi pregona vidijo varovanje kritične informacijske infrastrukture predvsem v preganjanju kibernetskega kriminala, kar pokrije zelo širok razpon kaznivih dejanj. Vključuje kršitve avtorskih pravic, računalniške prevare, otroško pornografijo in kršitve mrežne varnosti. Proti takšni obliki kriminala se bori na klasičen način, še posebej s sprejemanjem nove zakonodaje in spodbujanjem mednarodnega sodelovanja.
- nacionalno-varnostni: celotna družba je videna kot ogrožena, deluje se na več ravneh (tehnični, zakonodajni, organizacijski ali mednarodni). Akterji vključujejo državne uslužbence različnih organov ter predstavnike zasebnega sektorja in javnosti.

Glede na spremenjeno varnostno okolje po 11. septembru se predlaga vzpostavitev državnih organov, ki se ukvarjajo s problematiko kritične infrastrukture oziroma kibernetsko

varnostjo, kot so to naredili v več državah (Kanada, Nova Zelandija, Nemčija, Velika Britanija in ZDA) (Dunn 2005: 21). To so tudi vse države, ki so ustanovile specializirane organe, bodisi za varovanje kritične infrastrukture bodisi za informacijsko varovanje. Druge države urejajo to področje tako, da naloge zagotavljanja varnosti vključijo v sklop delovnih nalog že obstoječih ministrstev. Razlog, ki govori v prid vzpostavitvi centralnega organa, je tudi, da je kritična infrastruktura razdeljena med zelo različne akterje, podjetja iz različnih sektorjev in državne institucije. Komunikacija med temi akterji bi bila olajšana, hkrati pa bi ta državna institucija delovala kot povezovalni element.

Naslednji korak pri zagotavljanju informacijske varnosti je vzpostavljanje mehanizmov zgodnjega opozarjanja. To nalogo opravljajo t.i. CERT oziroma CSIRT skupine. Njihova naloga je predvsem, da se odzivajo na varnostne incidente v računalniškem omrežju, tako da jih rešujejo ali pomagajo pri njihovem razreševanju. Prav tako pa poskušajo preprečiti varnostne incidente v svoji sferi odgovornosti. Poznamo jih več vrst. Ločimo jih glede na področja, kjer delujejo. Ločimo CERT, namenjene majhnim in velikim podjetjem, vojaške, akademske, CERT za področje kritične (informacijske) infrastrukture, za področje javne uprave, državni, gospodarski in CERT dobavitelja programske opreme (internet 4). Na tej točki bi pojasnil različno uporabo terminov CERT in CSIRT – to sta namreč sopomenki, CERT je patentirana znamka in kot takšna tudi bolj razširjena, saj je prisotna že od leta 1988. CSIRT je novejši termin. CERT je kratica za Computer Emergency Response Team, CSIRT pa Computer Security Incident Response Team (internet 4).

Ključno je tudi to, da ima vzpostavljeni CSIRT podporo vodstva (West-Brown 2003: 34). Dalje je potrebno določiti občinstvo oziroma odjemalce in odnos z njimi. Obstaja širok razpon storitev, ki jih CSIRT lahko izvaja, in sicer:

- reakcijski: to dejavnost sproži dogodek ali prošnja, kot na primer ogroženega strežnika, širjenje zlonamerne kode, programska ranljivost ali nekaj, kar zabeleži sistem za odkrivanje vdorov. Reaktivne storitve so ključni del nalog CSIRT-a;
- proaktivni: te storitve vključujejo pomoč in obveščanje, da bi pripomogli k pripravi, varovanju in zaščiti sistemov pred napadi, težavami ali dogodki. Izvajanje teh storitev bo zmanjšalo pojav teh dogodkov v prihodnosti;
- postopki za zagotavljanje kakovosti: Ta storitev dopolnjuje obstoječe in uveljavljene storitve, ki so ločene od ravnanja z incidenti in jih izvajajo drugi

oddelki, kot so IT, revizija in oddelek za izobraževanje. Če CSIRT izvaja ali pomaga s temi storitvami, lahko izboljša celokupno varnost organizacije in identificira grožnje in sistemske slabosti. Te storitve so proaktivne in posredno pripomorejo k zmanjšanju števila varnostnih incidentov.

4.2.1 CERT v Sloveniji

Edini CERT v Sloveniji je SI-CERT, ki deluje v sklopu ARNES, njegove naloge pa so koordiniranje obveščanja in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji (internet 21).

V isti predstavitvi tudi piše, »da je SI-CERT omejen na izobraževalno in raziskovalno sfero, saj glede na prepletenost mrež ponudnikov internetnih storitev pri takšni storitvi nima smisla postavljati mej (internet 21). Sklepamo lahko, da slovenski SI-CERT sodeluje s tujimi organizacijami za računalniško varnost.

V intervjuju za spletni časopis Slo-tech je vodja SI-CERT dal sledečo izjavo: „Za varnost (razen seveda za lastno) ne skrbimo aktivno. To je lahko komercialna dejavnost. Enako tudi »penetration« testi. V Sloveniji obstajajo podjetja, ki se komercialno ukvarjajo s tem. V bodoče načrtujemo večji poudarek na preventivni dejavnosti, predvsem preko bolj pogostih obvestil o varnostnih luknjah, navodilih za zaščito in vzpostavitvi baze znanja s področja omrežne varnosti, ki bo dostopna javnosti.” (internet 5).

Kot lahko sklepamo iz navedenega, je skrb za varnost v slovenskih komercialnih omrežjih razdrobljena, SI-CERT ne nudi komercialnih storitev za podjetja. Obstajajo sicer komercialni ponudniki, vendar ostaja vprašanje, če si takšno raven storitve (zaščite) lahko privoščijo le velika podjetja. Spet je vprašanje, če so za porabo sredstev v tej smeri sploh pripravljena, saj vlaganje v varnost ne prinese neposrednih ekonomskih koristi.

4.3 Standardi informacijske varnosti

Če še omenimo naravo razvoja informacijskih sistemov, vidimo, da je razvoj izredno hiter, nove varnostne pomanjkljivosti se pojavljajo vsak dan, hkrati pa tudi postopki, ki jih odpravijo. Posledično je načrtovanje ofenzivnih operacij zoper informacijske sisteme in posledično informacijsko infrastrukturo zaradi spreminjajoče narave informacijske

tehnologije izredno težavno, skoraj nemogoče. Napadalec nikoli ne ve, koliko časa bo nek sistem imel varnostno luknjo. Če torej pogledamo na to z nasprotne plati, lahko ugotovimo, da je najboljša obramba res preventivno delovanje, dosledno odpravljanje varnostnih pomanjkljivosti. Vendar je to izredno težavno, tudi če imamo samo en računalnik. Spremljati novosti je izredno težko, še posebej, če se področje hitro razvija. Problem je tudi z doslednostjo, kar govori v prid oblikovanju organa, ki bi te novosti spremljal in naročnike storitev obveščal ter jim svetoval (CSIRT). Na ravni organizacije je izredno težko zagotoviti doslednost pri odpravi varnostnih pomanjkljivosti, če nimamo vzpostavljenega nekega merila. V nasprotnem primeru imamo stanje, kjer je varovanje informacijskega sistema prepuščeno (ne)znanju in (ne)iznajdljivosti posameznikov znotraj organizacije, ki so odgovorni za delovanje informacijskega sistema, hkrati pa tudi njihovi presoji, kaj je in kaj ni pomanjkljivost oziroma kaj je varnostno sporno. To področje ureja ISO standard 17799, ki se bo preimenoval v ISO standard 27001 – področje informacijske varnosti. Ta standard ureja naslednja področja:

- varnostno politiko,
- organizacijo informacijske varnosti,
- upravljanje z viri,
- varnost človeških virov,
- fizično in okoljsko varnost,
- upravljanje komunikacij in operative,
- nadzor dostopov,
- pridobivanje, razvoj in vzdrževanje informacijskih sistemov,
- ravnanje z informacijskimi varnostnimi incidenti,
- upravljanje z neprekinjenim poslovanjem,
- skladnost.

V ISO standardu so zapisani tudi ključni dejavniki, ki so kritični za uspešno vpeljavo varnostnega standarda, ki so naslednji (ISO/IEC 2005: 13):

a) varnostna politika, cilji in dejavnosti, ki se skladajo s poslovnimi cilji;
b) pristop in okvir do uvajanja, vzdrževanja, nadziranja in izboljševanja informacijske varnosti, ki je v skladu z organizacijsko kulturo;
c) vidna podpora in predanost vseh stopenj menedžmenta;

d) dobro razumevanje tega, kaj informacijska varnost zahteva, ocena groženj in ustrezno ravnanje z grožnjami;
e) ustrezna predstavitev informacijske varnosti vsem menedžerjem, zaposlenim in drugim, da bi se doseglo zavedanje o pomenu informacijske varnosti;
f) razdelitev smernic glede informacijske varnosti in standardov vsem menedžerjem, zaposlenim in drugim;
g) predpisovanje sredstev dejavnosti upravljanja informacijske varnosti;
h) omogočanje primernega zavedanja, urjenja in izobrazbe;
i) vzpostavitev učinkovitega procesa za ravnanje z varnostnimi incidenti;
j) uvedba merilnega sistema, ki služi za oceno ravnanja z varnostjo in nudenje povratne informacije za izboljšave.

Vendar je vpeljava standarda, ki bi bil sam sebi namen, torej, kjer se skladnost s standardom ne bi preverjala, slaba možnost. Standard je potrebno vpeljati celovito, ker tudi sam predvideva revizijo postopkov. Prav tako bi bilo dobro, da revizija varnosti ne bi bila samo interna temveč, da bi jo izvajala neodvisna zunanja institucija.

4.4 Sklep

Posebej smo si pri kritični informacijski infrastrukturi pogledali: dejavnike, ki vplivajo na varnost kritične informacijske infrastrukture; dejavnike, ki ključno vplivajo na varnost informacijske tehnologije. Opredelili smo strukturiranost groženj kritični informacijski infrastrukturi po kompleksnosti ter tiste akterje, ki predstavljajo najverjetnejšo grožnjo, in mehanizme varovanja kritične informacijske infrastrukture. Podrobneje smo si ogledali ISO standard 17799, ki se prvenstveno ukvarja z informacijsko varnostjo. Prav tako smo si pogledali pomisleke, ki ga spremljajo, predvsem vlogo vodstva, ki je ključna. V naslednjem poglavju si bomo pogledali, kako je s kritično informacijsko infrastrukturo v Sloveniji. Ker splošna definicija za kritično informacijsko infrastrukturo ne obstaja, si bom pomagal z opisom najpogostejših sektorjev, ki so jih kot kritične definirale druge države.

5. KRITIČNA INFRASTRUKTURA V SLOVENIJI

Za boljše razumevanje je potrebno tudi podrobneje opredeliti, kaj vse spada pod kritično infrastrukturo in posledično v kritično informacijsko infrastrukturo. Prva delitev je razumevanje pojma kritično, kritično s simbolnega oziroma sistemskega vidika. Glede na simbolni vidik lahko rečemo, da je nek objekt pomemben zaradi njegove vloge v družbi in ne zaradi njegovega vpliva na druge infrastrukture, pri sistemskem vidiku pa se kritičnost ocenjuje glede na vpetost v celoten sistem infrastrukture in posledične medodvisnosti drugih delov. Pomembno je tudi opredeliti, kateri sektorji spadajo pod kritično infrastrukturo. Avtorici Dunn in Wigert sta avtorici zbornika, ki opisuje kritično informacijsko infrastrukturo 14 držav (Avstralija, Avstrija, Kanada, Nemčija, Nizozemska, Norveška, Švedska, Švica, ZDA, Finska, Francija, Italija, Nova Zelandija in Velika Britanija). Kritična infrastruktura je za vsako opredeljena drugače, vendar lahko izluščimo sorodnosti med vsako oziroma razumemo, kaj bi lahko v Sloveniji predstavljalo kritično infrastrukturo. V Sloveniji na nacionalni ravni nikjer ni opredeljeno, kaj spada v pojem kritične infrastrukture. Vendar lahko glede na definicije kritične infrastrukture v različnih državah, ki so opisane v priročniku CIIP Handbook, izluščimo ključne sektorje v družbi. To so:

- energetika (oskrba z električno energijo, tudi oskrba s plinom in naftnimi derivati),
- informacijsko komunikacijsko tehnologijo,
- oskrba z vodo,
- reševalne službe (tudi policija),
- bančništvo in finančni sektor,
- transport,
- upravne storitve (tudi E-uprava).

Ogrožanje informacijskega področja lahko razdelimo na tri glavne komponente: ogrožanje (nacionalne) obrambne informacijske infrastrukture, ogrožanje javne (vladne) informacijske infrastrukture in zasebne informacijske infrastrukture (Svete 2006: 39).
Glede na to, da je predmet naloge preučevanje nevojaške komponente ranljivosti kritične informacijske infrastrukture, se bom posvetil področjem – zasebne informacijske infrastrukture in javne vladne informacijske infrastrukture. Opisal bom stanje na področju

telekomunikacij v Sloveniji. Pri javni (vladni) informacijski infrastrukturi bom opisal delovna področja različnih državnih institucij na tem področju in institucije same.

5.1 Telekomunikacije in informacijska tehnologija

Zakon o elektronskih komunikacijah v svojem tretjem členu opredeli elektronsko komunikacijsko omrežje, kot sledi: »Elektronsko komunikacijsko omrežje so prenosni sistemi in, kjer je to primerno, komutacijska ali usmerjevalna oprema in drugi viri, ki omogočajo prenos signalov po vodnikih, z radijskimi valovi, po optičnih ali drugih elektromagnetnih sredstvih, vključno s satelitskimi omrežji, fiksnimi (vodovno in paketno komutirana, vključno z internetom) in mobilnimi prizemnimi omrežji, električnimi kabelskimi sistemi, če se uporabljajo za prenos signalov, omrežij za radijsko in televizijsko radiodifuzijo ter omrežij kabelske televizije, ne glede na vrsto prenesenih informacij.« (Zakon o elektronskih komunikacijah: 2004). Po zakonski opredelitvi poznamo v Sloveniji sledeča javna omrežja: stacionarno telefonsko omrežje, GSM mobilna omrežja, komutacijska paketna omrežja in satelitske komunikacije.

5.1.1 Stacionarno telefonsko omrežje

Tehnično gledano je to »circuit switched« - vodovno omrežje. To pomeni, da se med dvema točkama vzpostavi stalna povezava, za celotno trajanje pogovora, po prenehanju pa jo je potrebno prekiniti. Na tej tehnologiji temelji analogno telefonsko omrežje (PSTN – kar pomeni Public Switched Telephone Network). Poznamo tudi ISDN, ki je oblika vodovnega omrežja. Oblikovan je tako, da dovoljuje prenos zvoka in podatkov preko običajnih telefonskih bakrenih žic. Posledično dobimo boljšo kvaliteto zvoka in višje hitrosti podatkov kot z obstoječimi analognimi sistemi. Bolj široko je ISDN skupek protokolov za vzpostavitev in prekinjanje vodovne komunikacije, ki pa nudi tudi napredne klicne funkcije za uporabnika, na primer prikaz številke klicočega, vendar sta to stari tehnologiji, ki jih počasi zamenjujejo modernejše oblike komunikacij.

Ko govorimo o stacionarnem telefonskem omrežju, mislimo predvsem na omrežje različnih ponudnikov, ki nudijo storitve klasične telefonije. Vključuje tako PSTN kot ISDN storitev. Pomeni omrežje, ki doseže skoraj vsako gospodinjstvo v Sloveniji. Liberalizacija trga v Sloveniji po sprejemu Zakona o telekomunikacijah pomeni tudi, da sedaj poleg Telekoma obstaja vedno več ponudnikov stacionarne telefonije.

5.1.2 Mobilno GSM omrežje

GSM ali Global System Mobile je trenutno najbolj uveljavljena tehnologija za uporabo v mobilni telefoniji. Odkar je bila predstavljena prva komercialna različica sistema GSM, se je tehnologija uveljavila kot najbolj razširjen, hitro razvijajoči se mobilni standard, ki se uporablja v 170 državah po svetu.

Sistem GSM se deli na tri glavne dele:

- SS - Switching System – preklopni sistem
- BSS – Base Station System – sistem baznih postaj
- OSC – Operation and Support Centre – center za podporo in operativo

Sistem baznih postaj

GSM je v svoji osnovi radijski sistem. Osnova celotnega sistema je radijska komunikacija v frekvenčnem območju 900 Mhz. Radijska zveza poteka med telefonom (mobilni terminal – MT) in bazno postajo. Bazne postaje pokrivajo območje v polmeru 32 km in tvorijo t.i. celice, to so radijska območja, ki jih pokriva bazna postaja.
Mobilni telefoni avtomatsko vzpostavljajo radijske zveze preko radijskega vmesnika z bazno postajo znotraj določene celice. Bazne postaje so med seboj povezane in tvorijo omrežno infrastrukturo, imenovano SS - Switching System. Informacije, ki se izmenjujejo med mobilnim telefonom in bazno postajo znotraj določene celice, se lahko preko mrežne infrastrukture prenašajo med baznimi postajami in celicami ter tako potujejo med mobilnimi telefoni, lahko pa se prenašajo tudi na druga statična ali mobilna omrežja.

Dodatno bi omenil, da GSM tehnologija uporablja poseben tehnični postopek, t.i. "frequency hopping", kar bi lahko prevedli kot frekvenčno skakanje. To je metoda, po kateri oddajnik in sprejemnik preskakujeta po vnaprej določenih radijskih frekvencah. Metoda se uporablja za zaščito pred prisluškovanjem ali za zagotavljanje kvalitete prenosa oziroma zmanjševanje radijskih motenj (Jelič 2003: 5).

Mobilno GSM omrežje v Sloveniji vključuje okoli 1.7 milijona uporabnikov. To je predvsem brezžično omrežje, ki ga poleg uporabnikov sestavljajo še bazne postaje vsakega

od operaterjev. V Sloveniji delujeta dva operaterja GSM in UMTS mobilnih komunikacij. To sta: Mobitel in Simobil, poleg tega je tudi več navideznih mobilnih ponudnikov: Debitel, Izimobil in Mercator ter Tušmobil. Navidezni ponudnik pomeni, da uporablja omrežje drugega ponudnika, ker svojega nima. Vsi trije uporabljajo Mobitelovo omrežje.

5.1.3 Komutacijska paketna omrežja

Da bi razumeli razliko med vodovnimi in paketnimi omrežji, je najbolje razložiti temeljno delovanje med obema. Vodovno omrežje v svoji najbolj osnovni obliki deluje približno takole. Ko se med dvema točkama vzpostavi povezava, se ta povezava vzdržuje skozi celotno trajanje komunikacije. Ker povezujemo dve točki v obe smeri, to povezavo imenujemo vod. Od tod ime vodovno omrežje, ki je temelj klasičnega telefonskega omrežja.

Telefonski pogovori preko klasičnega telefonskega omrežja so danes nekoliko bolj učinkoviti, prav tako niso več tako dragi. Vaš glas je digitaliziran in lahko skupaj s tisočimi drugimi potuje po enem optičnem kablu večino poti. Desetletje nazaj na primer je vaš pogovor zasedel eno linijo med obema točkama, tudi če je bila razdalja med njima zelo velika, v času vašega pogovora pa tega voda ne bi mogli uporabiti drugi (internet 7).

Podatkovna paketna omrežja uporabljajo drugačen princip, ki je bolj učinkovit od vodovnega. Po paketnih omrežjih se vzpostavi kratka povezava, ki traja samo toliko časa, da se pošlje košček podatkov. Imenujemo ga paket (angl.packet) od enega do drugega sistema. Ta paket vsebuje t.i. »payload« oziroma tovor, ki je košček kakršnekoli datoteke ali elektronske pošte, ki ga želimo poslati. Paketno preklapljanje je zelo učinkovito. Dovoljuje namreč usmerjanje paketov po najbolj neobremenjenih in najcenejših povezavah. Računalnika, ki komunicirata med seboj, lahko hkrati komunicirata tudi z drugimi računalniki, ki tako tvorijo omrežja. Ta omrežja se med seboj povezujejo na različne načine in sestavljajo tisto, kar poznamo pod imenom internet. Ime samo namreč izhaja iz ideje o prepletenih mrežah. Internet je tako zbirka velikih mrež, ki se medsebojno povezujejo na stičnih točkah. Na ta način se potem lahko vsak računalnik, ki je povezan z internetom, povezuje z vsakim drugim. Vsak računalnik ima lastno edinstveno razpoznavno številko, ki se imenuje IP številka. IP pomeni internetni protokol, ki predstavlja jezik, v katerem se računalniki pogovarjajo preko interneta. Protokol je vnaprej določen način, kako mora komunicirati program ali računalnik za dostop do neke storitve (internet 9).

Vsak računalnik, ki je povezan z internetom, tako postane del mreže. Ko se povežete z vašim ponudnikom internetnih storitev (ISP – Internet Service Provider), postanete del njihove mreže. Vaš ISP se potem poveže v neko večjo mrežo in tako postane del njihove mreže. V Sloveniji je po zadnjih podatkih približno 900.000 mesečnih uporabnikov interneta (internet 12).

Tukaj govorimo o vseh ponudnikih dostopa do interneta tako komercialnih kot akademskih. Hkrati bom tukaj omenjal tudi njihove povezave v tujino. Komercialni ponudniki so podjetja AMIS, SIOL, K2.net, Perftech, itn. Skupaj je teh ponudnikov 14, vsak pa ima svojo podatkovno povezavo v tujino in uporabnike v Sloveniji, ki uporabljajo različne načine dostopa do interneta, kot ADSL, VDSL, kabelski internet in brezžično omrežje. Edini akademski ponudnik dostopa do interneta je ARNES, ki pa ima tudi svoj CERT.

5.1.4 Satelitske povezave in druge oblike javnih brezžičnih omrežij

Tukaj lahko govorimo bodisi o satelitskih telefonih ali o satelitskem dostopu do interneta. Satelitski dostop do interneta deluje tehnično podobno kot širokopasovni ali klicni dostop. Razlika je edino v tem, da uporabnik uporabi satelitski krožnik in dva modema – za predvajanje in sprejemanje, s to razliko, da se tisti za sprejemanje podatkov povezuje preko satelita. S satelitskimi telefoni je podobno kot z GSM aparati, namesto na bazne postaje se potem povezujejo s komunikacijskimi sateliti v orbiti. Prednost pred GSM omrežji je ta, da nismo omejeni s pokritostjo baznih postaj, temveč imamo lahko dostop do komunikacijskih storitev kjerkoli na svetu.

V Sloveniji uporabljamo različne oblike javnih brezžičnih komunikacijskih omrežij. Podjetje Mobitel je vzpostavilo mrežo brezžičnih dostopnih točk v sistemu »NEO-WLAN«, kjer se lahko uporabniki z svojimi računalniki povezujejo na internet. Podjetje »Volja-tel« pa ponuja brezžični dostop za domače uporabnike in predstavlja alternativo drugim oblikam širokopasovnega dostopa do interneta predvsem tam, kjer druge možnosti dostopa do interneta ni. Slabosti takšnih oblik komunikacije v primerjavi z žičnimi povezavami so slabša odzivnost, nižje hitrosti povezav in bolj zapleteno delovanje.

5.2 Upravne storitve in informacijska infrastruktura v državni upravi

Upravne storitve v Republiki Sloveniji izvajajo različne institucije javne uprave. Ker v nalogi preučujemo vidik informacijske infrastrukture, se bom osredotočil predvsem na institucije državne uprave, ker ta predstavlja jedro, s svojimi storitvami pa obsega vse institucije javne uprave.

Ključna storitev je sistem HKOM (**H**itro **k**omunikacijsko **om**režje). HKOM je interno, zasebno omrežje, ki povezuje »zaključene celote – institucije javne in državne uprave« (Hkom predstavitev 2005: 3). V praksi to pomeni povezave okoli 1600 lokalnih omrežij po vsej Sloveniji. Te končne točke predstavljajo občine, ministrstva in njihove izpostave, upravne enote, centri za socialno delo ipd. Znotraj tega omrežja so vzpostavljene različne storitve, kot so npr. centralni poštni strežnik in lokalni poštni strežniki ter izdajatelj digitalnih potrdil. Hkrati znotraj sistema delujejo različne storitve, kjer je zasebnost toliko bolj pomembna. To je samo skupno omrežje, ki ga ne smemo zamenjevati s skupno varnostno politiko, skupnimi predpisi in skupnimi pravili. To je samo omrežje, ki med seboj povezuje institucije na varen način.

Glede nudenja storitev zunanjim uporabnikom je pa tako, da vsaka institucija skrbi za tiste storitve, za katere je vsebinsko zadolžena. Storitve, ki jih javna uprava Republike Slovenije navzven nudi državljanom so: vpogled v centralni register prebivalstva nudi Ministrstvo za notranje zadeve, spletni portal e-davki Davčna uprava RS, Geodetska uprava RS kataster, Ministrstvo za javno upravo pa portal E-uprava. Obiskovalcev spletnega portala E-uprava je po zadnji raziskavi RIS 2006 okoli 100.000 na mesec, kar predstavlja okoli 13% vseh uporabnikov interneta v Sloveniji (Vehovar, Zupanič 2006: 52). Trend po tej raziskavi kaže na znatno povečanje glede na prejšnje raziskave. Storitve, ki jih uporabniki opravljajo preko interneta, so predvsem oddaja E-dohodnine, vpogled v zemljiško knjigo, uporaba portala E-vem (namenjen je ustanovitvi podjetij) in podaljšanje registracije motornega vozila.

Po mojem mnenju predstavlja velik problem z vidika varovanja kritične infrastrukture - tudi informacijske, pomanjkanje oziroma neobstoj varnostne politike v javni upravi. Varnostna politika je zaželjeno ravnanje zaposlenih, kot ga opredeli vodstvo (Warkentin 2006: 26). Trenutno je stanje takšno, da »Organi javne uprave v trenutku te ocene zelo različno skrbijo

za svojo informacijsko varnost. Medtem ko je ta v nekaterih organih na zadovoljivi ravni, je pri drugih organih javne uprave odrinjena na stranski tir.« (Hajtnik 2002: 6).

»…v nobenem organu ne razpolagajo z jasno opredeljeno in vsa področja obsegajočo informacijsko varnostno politiko, ki bi vodstvu, vsem zaposlenim in zunanjim sodelavcem služila kot neposreden vir pravil in navodil za učinkovito in varno uporabo informacijsko telekomunikacijske opreme in varovanja podatkov.« (Hajtnik 2002: 6).

Nadaljujmo z opisom institucij, ki so na področju informacijske tehnologije v državni upravi stična točka za tehnične zadeve, še posebej za zadeve varovanja informacijske infrastrukture. Bivši Center vlade za informatiko (CVI), ki je po svoji naravi predstavljal centralni organ, na katerega so se lahko naslonile druge institucije za svetovanje in pomoč, je namreč imel vlogo vladne službe, neposredno podrejene vladi oziroma generalnemu sekretarju vlade. Vlogo na tem področju je igralo tudi Ministrstvo za informacijsko družbo RS. Na tem področju so se po koncu leta 2004 zgodile velike spremembe. Naloge Centra vlade za informatiko in drugih institucij je zaradi lažjega pregleda bolj smiselno razvrstiti v kategorije (internet 31):

- strateške;
    - priprava in spremljanje izvajanja strategije elektronskega poslovanja javne uprave RS,
    - izdelava strateških planov skupnih funkcij uprave (informacijska podpora pisarniškemu poslovanju, zakonodajnemu postopku, spremljanju dela vlade in ministrstev, kadrovskemu sistemu, sistemom za odločanje, odnosom z javnostmi in podobno), uvajanja skupne informacijske infrastrukture in prenove poslovanja ter informatizacije posameznih organov,
    - priprava, izdelava in realizacija usklajenega skupnega letnega načrta informatizacije (nabav informacijske opreme in storitev);
- implementacijske;
    - spremljanje, izdelava, skrbništvo, uvajanje in svetovanje s področja metodoloških osnov planiranja in razvoja informacijskih sistemov ter

vodenja, spremljanja in kakovosti informacijskih projektov, kot tudi s področja standardov informacijsko - komunikacijske tehnologije,
- organiziranje, in/ali izvajanje skupnih nabav, distribucije in vzdrževanja skupne informacijske opreme, kot tudi poenotenja in pomoči uporabnikom lokalne informacijske opreme organov,
- planiranje, razvoj, uvajanje in svetovanje s področja aplikativne opreme za skupne funkcije ter po dogovoru za specialne funkcije organov, kot tudi s področja tehnološkega povezovanja skupnih administrativnih registrov in aplikativne opreme oziroma posameznih upravnih informacijskih sistemov;

- posvetovalne;

  - izdajanje mnenj pred nabavami informacijske opreme in storitev posameznih organov v skladu s predpisi, ki urejajo pripravo in sprejem enotnih tehnoloških zahtev, smernic in priporočil za informacijske sisteme v državnih organih,
  - izdelava politike, vzpostavitev, spremljanje in nadzor sistema zaščite in varovanja,
  - strokovno svetovanje in usposabljanje s področja planiranja in razvoja informacijskih sistemov, vodenja projektov, spremljanja in zagotavljanja kakovosti ter same uporabe izdelanih informacijskih rešitev in standardnih orodij;

- operativne;

  - zagotavljanje razvoja in delovanja centralne strežniške infrastrukture ter skupnega telekomunikacijskega omrežja in telekomunikacijskih storitev,
  - zagotavljanje razvoja in delovanja certifikatne agencije,
  - promoviranje informatike v upravi in navzven ter sodelovanje z domačimi in tujimi institucijami s tega področja, na skupnih projektih in drugod.

Ministrstvo za informacijsko družbo je s svojimi direktorati imelo sledeče naloge (internet 22):

- strateške;
  - pripravo razvojnih dokumentov na področju pošte in telekomunikacij,
  - pripravo realizacije nacionalnega programa razvoja telekomunikacij,
  - usklajevanje slovenske telekomunikacijske zakonodaje s predpisi Evropske unije,
  - pripravo programa privatizacije Telekoma ipd;
- operativne;
  - zagotavljanje pomoči gospodarstvu pri uvajanju e-poslovanja in sodelovanje pri razvijanju e-uprave.

Situacija tudi tukaj ni bila idealna, Takrat bi bilo smiselno dve organizaciji in njune naloge združiti, saj je prihajalo do prekrivanja nalog. Če se potrudimo potegniti ločnico med tema dvema institucijama, lahko po opisu nalog vidimo, da je bil CVI obrnjen bolj navznoter v državno upravo, MID pa bolj navzven na gospodarstvo. Vendar se je CVI z eno storitvijo posebej približal državljanom. Junija 2006 je minilo 5 let od začetka delovanja izdajatelja digitalnih potrdil SIGEN-CA, ki je tisti mesec dosegel mejo 50.000 izdanih digitalnih potrdil državljanom in poslovnim subjektom.

Po volitvah leta 2004 sta bila tako CVI kot MID ukinjena, njune naloge pa so si razdelili: Ministrstvo za javno upravo RS, Ministrstvo za gospodarstvo RS in Ministrstvo za visoko šolstvo, znanost in tehnologijo RS. Znotraj teh ministrstev so nastali direktorati, ki posamezno področje specifično urejajo. Na Ministrstvu za javno upravo RS je nastal Direktorat za E-upravo in upravne procese. Njegove naloge so (internet 29) :

- strateške;
  - prenova procesov in pospešen razvoj e-uprave s ciljem približevanja storitev državljanom in gospodarstvu;
- implementacijske;

- zagotavljanje povezljivosti registrov in integracija podatkovnih virov z informacijsko podporo procesom;

- operativne;

  - izboljševanje elektronske podpore odnosom med subjekti v javni upravi in izven nje z uporabo sodobne informacijske in komunikacijske tehnologije,
  - izvajanje javnih naročil s področja informacijske infrastrukture;
  - posvetovalne;
  - spremljanje svetovnega razvoja informacijske infrastrukture in priprava usmeritev in standardov s svojega področja dela,
  - sodelovanje na področju odprave administrativnih ovir;

- druge naloge, ki niso vezane na področje informatike;

  - skrb za izvajanje predpisov, ki urejajo splošni upravni postopek, upravno poslovanje ter dostop do informacij javnega značaja,
  - opravljanje upravnega nadzora,
  - sodelovanje z nevladnimi organizacijami.

Na Ministrstvu za gospodarstvo RS se je oblikoval Direktorat za elektronske komunikacije. Njegove naloge so (internet 28) :

- strateške;

  - priprava predlogov sektorskih zakonov in podzakonskih aktov s področij pošte, elektronskih komunikacij, digitalnega podpisa in sorodnih področij,
  - priprava razvojne strategije za vzpostavitev visoke stopnje konkurenčnosti na trgih elektronskih komunikacij, izvaja se upravljanje razvojnih projektov za pospeševanje razvoja e-komunikacij in vodijo se projekti s sredstvi strukturnih skladov. Direktorat za elektronske komunikacije je odgovoren za upravljanje podjetij Telekom Slovenije in Pošta.

Na Ministrstvu za visoko šolstvo, znanost in tehnologijo RS pa Direktorat za informacijsko družbo. Njegove naloge so (internet 30):

- strateške;
  - skrb za pospešen, usklajen in učinkovit razvoj informacijske družbe, ki temelji na znanju in vseživljenjskem izobraževanju;
- posvetovalne;
  - direktorat pri svojem delu sodeluje z različnimi organizacijami tudi na področju zakonodaje, varnosti in zasebnosti v elektronskem svetu, izobraževanju;
- operativne;
  - spremljanje indikatorjev razvoja informacijske družbe,
  - izvedba znanstvenih in strokovnih srečanj;
- implementacijske;
  - spodbujanje razvoja in lokalizacije programske opreme, temelječe na odprti kodi,
  - izvedba projektov za zmanjševanje digitalnega razkoraka.

Kot vidimo iz naštetega, so nove institucije na tem področju pokrile le del nalog starih institucij – predvsem CVI-ja. Naloge MID sta v celoti prevzela Direktorat za elektronske komunikacije in Direktorat za informacijsko družbo. Posebej bi rad izpostavil problematiko varovanja in zaščite. CVI je imel na seznamu nalog izrecno opredeljeno »izdelavo politike, vzpostavitev, spremljanje in nadzor sistema zaščite in varovanja«. Niti ena od novih institucij se s problematiko varnosti ne ukvarja eksplicitno, implicitno pa lahko domnevamo, da jo je prevzel DEUP »spremlja svetovni razvoj informacijske infrastrukture in pripravlja usmeritve in standarde s svojega področja dela«. Direktorat za informacijsko družbo in Direktorat za elektronske komunikacije se ukvarjata predvsem z strateškimi zadevami. Hkrati se mi opis nalog CVI in MID zdi bolj konkreten in jasen kot pa opredelitev nalog

sedanjih direktoratov, ki so njune naloge prevzeli. Opis nalog pri vseh deluje preveč splošno.

Problematiko, ki je relativno podobna varovanju kritične informacijske infrastrukture, so že opisali, ko so opisovali težave pri uvajanju elektronskega poslovanja v javno upravo Republike Slovenije. Izpostavil bi predvsem »pomanjkanje medresorskega sodelovanja in nesistemsko komunikacijo, preobremenjenost strokovno najbolj usposobljenih kadrov in pomanjkanje kadrovskih in finančnih virov« (Silič, Colnar, Gyorkos 2004: 9). Če sklepamo z vidika varovanja kritične informacijske infrastrukture in z vidika razvoja področja informatike, lahko ugotovimo, da poteza razdelitve pristojnosti med tri direktorate različnih ministrstev nedvomno otežuje komunikacijo, hkrati sredstva za izvedbo projektov deli na tri dele. Dalje še bolj potencira težave, ki so povezane z razvojem informatike, ki zahtevajo tesno sodelovanje vseh vpletenih in celovit pristop. Bolj podrobno bi tudi opisal organizacijsko strukturo Direktorata za E-upravo in upravne procese, kjer je z novo sistemizacijo februarja 2006 vzpostavljen Urad za informatiko in E-upravo. Smisel te ureditve je najverjetneje ločiti upravni del in del, ki se ukvarja z informatiko. Če na to dejstvo pogledamo z drugega vidika, lahko vidimo, da je področje informatike še bolj odrinjeno od vodstva, ker sedaj obstaja še en hierarhični nivo. Sklepamo lahko torej, da ima upravno področje prednost pred področjem informatike. Če bi bila situacija nasprotna, bi verjetno nastal »Urad za upravne procese«. Vprašanje je tudi, če ima takšno drobljenje pristojnosti kakšen pozitiven učinek.

Omenil bi še kadrovske pretrese, ki so spremljali vzpostavitev nove vlade po jeseni 2004. Časnik »Mladina« (internet 19) je objavil članek, kjer analizira vpliv vlade na gospodarstvo. Analizo spremlja podatek, da je bilo v zadnjih dveh letih v 50 slovenskih največjih in najuspešnejših podjetjih zamenjanih 18 direktorjev. Pogosto se vodenje podjetij kroji po strankarskih in družinskih linijah. Skrbi me, da se takšna kadrovska politika izvaja tudi znotraj državne uprave. Berce je, na primer, v svojem prispevku napisal, da informatika v državni upravi potrebuje dobrega strokovnega menedžerja (Berce 2002: 164), da bi lahko začeli področje urejati. Glede na stanje v gospodarstvu lahko domnevamo, da znotraj državne uprave vlada odgovornost zgolj politiki, menedžerji na vseh področjih v državni upravi pa morajo biti odgovorni političnemu vodstvu in ne strokovnim odločitvam.

V poglavju o mehanizmih varovanja informacijske infrastrukture sem opisal ključne dejavnike uspešne implementacije varnostnega standarda ISO 17799. Posebej bi izpostavil dejavnik podpore vseh stopenj menedžmenta. Odnos menedžmenta do informacijske varnosti pa lahko vidimo v predstavitvi Ministra za javno upravo RS dr. Gregorja Viranta pred Državnim zborom RS, kjer je o področju varnosti na informacijskem področju rekel:

»Z varnostjo ne bomo pretiravali. Varnost se včasih fetišizira. Dostikrat, zlasti informatiki, pretiravajo z varnostjo. Poglejmo si primer. Kako danes napovemo dohodnino? Z lastnoročnim podpisom, torej podpišem obrazec, ki ga pošljem. Kdo ta lastnoročni podpis kontrolira? Za določene elektronske storitve bo možen dostop tudi brez elektronskega podpisa, že danes to funkcionira,..., ampak če želim danes priti do evropske zdravstvene kartice, jo lahko naročim na spletni strani Zavoda za zdravstveno zavarovanje brez uporabe digitalnega potrdila« (internet 34).

Minister očitno informacijsko varnost razume kot nekaj, kar se izvaja med državljanom in upravo, pri neki storitvi in ne celovito kot varovanje nekega velikega sistema s preko 20.000 uporabniki. Ta izjava se mi zdi izredno pomembna, saj kaže odnos glavnega funkcionarja ministrstva do nekega vprašanja, ki spada v njegov resor. Njegovo mišljenje bo nedvomno imelo velik vpliv na to področje, še posebej, če je za implementacijo varnostnega standarda ključna podpora menedžmenta oziroma vodstva na vseh ravneh.

Če pogledamo v gospodarstvo in pogledamo, kako je s storitvami za končne potrošnike preko interneta, vidimo, da je kljub relativno nizki rasti prodaje preko interneta v Sloveniji konec leta 2004 150.000 uporabnikov interneta kupovalo preko interneta, kar predstavlja okoli 15% uporabnikov interneta, število nakupovalcev pa se vsako leto poveča za 20.000. Prav tako raste število nakupov in njihova vrednost (Vehovar, Šijanec 2005: 3). Ti uporabniki štejejo varnostne mehanizme ob nakupu za zelo pomembne. Ti mehanizmi so garancija za vračilo denarja, SSL zaščita povezave, izjave o varnosti in zasebnosti ter certifikat spletnemu mestu. je Potrošnikom je najpomembnejša možnost vračila denarja. Na drugem mestu je SSL varovanje povezave. Druga dva mehanizma sta potrošnikom še vedno pomembna, vendar ne tako zelo kot prejšnja dva. Sklepamo lahko, da potrošniki razumejo varnostne mehanizme in se znajo zaščititi v internetu, saj je varnost nakupa s strani potrošnikov ocenjena kot zelo pomembna.

Javna uprava po drugi strani dobro skrbi za varnost uporabnikov z uporabo digitalnih potrdil, ki zagotavljajo pravno veljavo v pravnem prometu preko interneta z javno upravo in tehnično zelo visoko stopnjo varnosti. Možnost zlorabe digitalnega potrdila je namreč proti starejšim oblikam avtentikacije (uporabniško ime in geslo) neprimerno nižja. Javna uprava zahteva uporabo digitalnega potrdila pri veliki večini storitev, ki jih ponuja. Izjemi sta le storitvi: izpisek iz zemljiške knjige in podaljšanje prometnega dovoljenja. Vendar se za razliko od bančnih institucij niso omejili le na digitalna potrdila, ki jih izdajajo sami, temveč se v storitve javne uprave lahko prijavimo tudi z digitalnim potrdilom kateregakoli kvalificiranega overitelja digitalnih potrdil v RS (Pošta CA, NLB CA, Halcom, SIGOV-CA in SIGEN-CA). Število uporabnikov vsaj enega digitalnega potrdila je okoli 36 % uporabnikov interneta, kar je več kot 200.000. Največ uporabnikov ima digitalno potrdilo spletne banke KLIK Nove Ljubljanske banke (Vehovar, Zupanič 2006: 71). Uporabnikom je varnost pomembna vsaj takrat, ko opravljajo finančne transakcije preko interneta. Moje mnenje je, da bi bilo potrebno povečati število uporabnih storitev, kar bo nedvomno povečalo število uporabnikov spletnih storitev, ne pa zmanjševati števila varnostnih mehanizmov. Uporabniki, ki digitalnega potrdila nimajo, so namreč prepričani, da jim uporaba digitalnega potrdila ne omogoča bistveno večjega nabora storitev (Vehovar, Zupanič 2006:71).

5.2.1 Vloga človeških virov

Pri zagotavljanju varnosti želim opredeliti tudi človeški dejavnik in ne samo tehničnega. Pomemben dejavnik tukaj je upravljanje s človeškimi viri. Sem spadajo: notranji akti, zaposlovanje, obveščanje, izobraževanje in usposabljanje, spremljanje in nadzor ter prenehanje zaposlitve (Hajtnik 2002: 20).

Notranji akti

Eden izmed načinov zagotavljanja informacijske varnosti v zvezi s človeškimi viri je, da organ že v opisu posameznega delovnega mesta natančno določi obveznosti delavca, ki bo mesto zasedel, in obveznosti, povezane z samim izvajanjem informacijsko varnostne politike. Skratka, da določi, kaj bo delo (bodočega) zaposlenega obsegalo in kakšne dostopne pravice potrebuje. Raziskave kažejo, da ima veliko zaposlenih dostop do veliko več podatkov, kot jih dejansko potrebujejo.

Zaposlovanje

Preverjanje novih sodelavcev je zaradi Zakona o varovanju osebnih podatkov močno oteženo. Pridobivanje podatkov, ki so za organ ali gospodarsko družbo relevantni, bi lahko brez soglasja zaposlenega predstavljalo nedovoljen poseg v njegovo osebnostno sfero. Pomembni kazalci zanesljivosti so pogoji, ki se nanašajo na finančno stanje oziroma splošno premoženjsko stanje, izpostavljenost izsiljevanju, podatki o nekaznovanosti in podobno. Podatkov o finančnem stanju banke glede na veljavno zakonodajo ne smejo posredovati oziroma jih lahko posredujejo le z privoljenjem komitenta. Podatke iz kazenske evidence lahko pridobijo državni organi, gospodarske družbe in zasebni delodajalci za neizbrisane obsodbe, vendar le v primeru, če še trajajo pravne posledice obsodbe ali varnostni ukrepi ali imajo poseben, z zakonom utemeljen interes. Pomemben dejavnik je tudi preverjanje življenjepisa in podatkov v prošnji, vključno z izpolnjevanjem zahtev glede izobrazbe in izkušenj. Glede na dejstvo, da oseba prostovoljno navaja podatke, je to mogoče šteti kot privolitev, da se ti podatki preverijo.

Obveščanje, izobraževanje in usposabljanje

Pomemben dejavnik zagotavljanja informacijske varnosti je skrb za stalno izobraževanje in usposabljanje zaposlenih. Pomen izobraževanja je v tem, da bo delodajalec zaposlenega zgolj zavezal k nekemu ravnanju. Če mu hkrati ne bo dal možnosti, da bi se o določenem tudi usposobil, ni mogoče pričakovati, da bo delavec, tako kot je zavezan, tudi ravnal. Izobraževanje izpostavi tudi Mitnick, ki pravi, da dobra politika informacijske varnosti, skupaj s primernim izobraževanjem in usposabljanjem, močno vpliva na povečanje zavedanja zaposlenih o pravilnem ravnanju s poslovnimi informacijami (Mitnick 2004: 55). Vendar je politiko potrebno tudi izvajati in kršitve preganjati. Zaposleni namreč ne prijavijo nekega ravnanja, če so prepričani, da njihove prijave ne bodo upoštevane (Cole 2006: 32).

Spremljanje in nadzor

Učinkovito izvajanje odgovornosti za izvajanje varnostne politike, posebnih odgovornosti za zaščito posameznih sredstev ali izvedbo posameznih varnostnih postopkov ali dejavnosti nujno zahteva stalen in učinkovit nadzor. Pomembno je, da so osebe za izvajanje varnostne politike predvidene že v sistemizaciji. Jasna razdelitev pristojnosti in zavedanje zaposlenih, da nadzor obstaja, je pomembna predpostavka, da bo izpolnjevanje obveznosti dejansko učinkovito. Nadzor ne poteka zgolj nad izpolnjevanjem obveznosti, temveč tudi nad spreminjanjem življenjskih okoliščin iz zasebnega življenja zaposlenega, ki posredno vpliva

tudi na njegovo vedenje na delovnem mestu. Pri preverjanju zaposlenih so zaradi zasebne narave podatkov državni organi in gospodarske družbe večinoma omejeni. Kot sem omenil, škodoželjni zaposleni povzročijo največ varnostnih incidentov. Uvod v zelo veliko večino varnostnih incidentov je bil dostikrat spor med zaposlenim in podjetjem (Cole 2006: 40). Opozorilni znaki so, potrebno jih je torej opaziti in stanje poskušati razrešiti, preden se zaostri.

Prenehanje zaposlitve

Tukaj gre za ravnanja ob prenehanju delovnega razmerja. Kadrovska služba mora s službo za informatiko ugotoviti, če dostopne pravice zaposlenega predstavljajo varnostno tveganje in na podlagi ocene ustrezno zmanjšati oziroma ukiniti dostopne pravice še posebej tiste za oddaljeni dostop (Hajtnik 2002: 56).

Za celovit pristop k varnosti je pomembno upoštevanje vseh naštetih postopkov. Vendar, po mojem mnenju, organizacija najbolj dejavno pripomore k lastni varnosti z izobraževanjem. Kot smo videli, je potrebno zagotoviti tako varnostno politiko kot delovanje zaposlenih v skladu s to politiko. Problematike izobraževanja kadrov se je dotaknil Berce, ko je povzel rezultate raziskave OECD za področje razvoja IT v državni upravi. Ugotovitve so bile sledeče: število osebnih računalnikov in njihova povezljivost v omrežja v državni upravi je visoka, čeprav so vlaganja v IT v zadnjih letih nazadovala. Rast vlaganj v IT v Sloveniji zaostaja za povprečjem OECD. Raziskava je tudi pokazala izrazito usmerjenost v tehnologijo in veliko manj v spremljajoče elemente, ki so nujni za optimalno uporabo tehnologije.

»Zaposleni v državni upravi je najpomembnejši in najkompleksnejši proizvajalni dejavnik. Njegovo znanje, organizacijske sposobnosti, njegovo organiziranje, stimuliranje in omogočena podpora z modernimi tehnologijami vplivajo na dobro ali slabo delovanje državne uprave« (Berce 2002: 162). Vlaganje v njegovo kakovost je tako ključnega pomena za zagotavljanje kakovosti dela, prav tako pa je to dejansko tisto, s čimer si organizacije zagotavljajo varnost. Po izsledkih te iste raziskave »slovenske državno-upravne organizacije pospešeno zaostajajo za povprečjem OECD.« (Berce 2002: 167).

Na CVI-ju so tudi na začetku leta 2004 začeli z vzpostavljanjem izobraževalnega središča (Sirnik; 2004: 330). Cilj tega projekta je bil »Razvoj in vzpostavitev celovite rešitve

usposabljanja s področja e-poslovanja« (Sirnik 2004: 331). Projekt je bil sicer ustavljen konec 2004 (Sirnik : 2006). Glede na to, da smo prej omenili, da izobraževanje uporabnikov vpliva na zmanjševanje varnostnih incidentov, saj je » Edini resnično učinkoviti način, da ublažimo grožnjo informacijski varnosti ta, da uporabimo varnostne tehnologije skupaj s politiko informacijske varnosti, ki vzpostavi pravila za vedenje zaposlenih in ustrezno izobraževanje in usposabljanje.« (Mitnick 2002: 410). Hkrati lahko izobraževanje uporabnikov prispeva k bolj racionalni uporabi IT, saj trenutno IT v državni upravi uporabljajo predvsem na osnovni način – za urejanje besedil, preglednic in pošiljanje elektronske pošte (Berce 2002:160). Zelo malo pa se uporabljajo storitve mobilne pisarne ipd. Če sedaj to združimo, nastanek varnostne politike, izobraževanje zaposlenih, izvajanje varnostne politike in še revizija teh delovanj oziroma postopkov lahko predstavlja temelj vzpostavitve varnostne kulture, ki pa ne sme biti v nasprotju z organizacijsko kulturo (ISO17799 2005:17).

5.3 Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji

Kot sem že opisal v poglavju o ogrožanju kritične informacijske infrastrukture, predstavljajo največjo grožnjo informacijski infrastrukturi 4 skupine: škodoželjni zaposleni, hekerji, teroristi in infobojevniki.

Najmanjšo grožnjo predstavljajo prav gotovo teroristi, saj nimajo dostopa do znanja niti do sredstev za izvajanje tehnološko dovršenih napadov. Tako vsaj meni FBI. Prav tako Slovenija do sedaj ni bila tarča terorističnih skupin. Teroristični napad bi po mojem mnenju lahko predstavljal veliko večjo grožnjo fizičnemu vidiku informacijskega sistema in veliko manj nematerialnemu. Odziv na to bi bila okrepitev fizičnega varovanja informacijskega sistema oziroma njegove materialne sestavine.

Bolj sofisticirano grožnjo kot teroristi predstavljajo hekerji, ki lahko ogrozijo nematerialno komponento informacijskega sistema. Najpogosteje jih motivira lastni ego, izziv, ki ga vdor predstavlja, ali pa je motivacija uporništvo (Wenger v Svete 2006: 37). To je primer nestrukturirane grožnje. Glede na globalno naravo interneta lahko pridejo iz katerekoli države na svetu. Mogoče najbolj odmeven primer hekerskega napada predstavlja napad na spletno stran www.gov.si, kjer je heker zamenjal glavno stran. Drugi, bolj grozeč, primer pa

je predstavljal domnevni vdor v spletno bančno storitev Klik Nove ljubljanske banke. Tukaj lahko dejansko vidimo tudi po odmevnih primerih, da se takšne grožnje dotaknejo tudi naše države ne glede na njeno majhnost. Če pa analiziramo drugega, ki je po mojem mnenju dvignil veliko več prahu, ugotovimo, da je napadalec za cilj izbral šibkejši člen - uporabnika. Izkoristil je namreč javno znano funkcionalnost v najbolj razširjenem spletnem brskalniku Internet Explorer podjetja Microsoft, ki bi jo lahko izrabil trojanski konj, ki bi napadalcu omogočil enake dostopne pravice v bančni storitvi, kot jih ima uporabnik sam. Vse skupaj ni bilo nič novega. Avtor trojanskega konja je pač uporabil obstoječega trojanskega konja in ga priredil za delo s »Klikom«. Verjetno bi bilo možno trojanca širiti tudi v drugačni obliki (preko elektronske pošte ipd.), vendar razvoj tega trojanca ni nikoli prišel tako daleč, da bi bilo to možno. Zaščita pred takšnim trojanskim konjem bi znala biti problematična, kajti število uporabnikov je proti številu uporabnikov celotnega interneta zelo majhno. Po drugi strani pa je ta storitev izredno specifična. Govorimo namreč o eni spletni storitvi ene banke. Antivirusni programi ga verjetno ne bi zaznali, saj zaradi prej naštetih razlogov ni razširjen. Zaščito bi bilo možno namestiti na strežnik ali na uporabnikov računalnik, kjer pa se nam porodi vprašanje o izvoru zaščitnega programa, saj uporabnik njegove avtentičnosti ne bi mogel zadovoljivo potrditi (internet 15). Še vedno predstavlja najbolj učinkovito sredstvo obrambe pred hekerji obveščenost in izobraženost uporabnikov in v primeru velikih sistemov dosledna odprava varnostnih pomanjkljivosti. Dalje bi bila smiselna vzpostavitev CSIRT-a, ki bi s proaktivnim pristopom pripomogel k obema dejavnostima.

Naslednji na lestvici so škodoželjni zaposleni. Messmer trdi, da je kiber kriminal pretežno problem znotraj neke organizacije (internet 14). Velika večina varnostnih incidentov ima namreč izvor znotraj organizacije. Moramo pa tudi razumeti, da so to ljudje, ki informacijski sistem najbolje poznajo, še posebej, če gre za administratorje, pogosto tudi intimno poznajo njegove slabosti in pomanjkljivosti. Motivacija za takšno dejanje je lahko različna: jeza , maščevanje, izsiljevanje in pohlep. Če gledamo na orodja (Hajtnik 2002: 20), kot tista, ki lahko pripomorejo k odpravi grožnje škodoželjnih zaposlenih, hitro ugotovimo, da bi kakršenkoli proaktiven pristop organizacije pomenil poseg v zasebnost zaposlenega, ki ga težko upravičimo. Prav tako bi zelo težko ugotovili dejansko stanje zaposlenih, saj je na primer finančno stanje posameznika tajen podatek, ki je znan le njemu in njegovi banki. Ti podatki so zaupni. Prav tako tudi velika večina podatkov, ki bi pričala o dovzetnosti

posameznika za izsiljevanja, bolezni ali njegovemu stanju uma. Ti podatki bi lahko pričali o tem, da bi posameznik lahko škodoval organizaciji.

Če govorimo o primeru, da je motivacija zlobnega zaposlenega jeza ali maščevanje, to lažje razumemo skozi ugotovitev, ki jo je opredelila Messmer, trdi namreč, daso IT administratorji velikokrat introvertirani in internalizirajo stres, izražajo pa se samo v medmrežju. Najprej pogosto zagrešijo blage kršitve, npr. nočejo usposobiti pomožnega delavca. Kršitve se lahko stopnjujejo do te mere, da ogrozijo informacijski sistem organizacije. Zgodnji poseg vodstva bi lahko rešil to težavo, vendar ostaja ugotovitev dejstva, da obstaja problem v domeni kadrovskega oddelka (Hajtnik 2002: 26).

Svojevrsten problem prinaša možnost kraje podatkov, kjer je motivator pohlep. Tukaj bo namreč poskušal zaposleni prikriti svojo dejavnost. Kraje zasebnih podatkov so v ZDA v porastu. Zasebni podatki vključujejo številke kreditnih kartic, naslove elektronske pošte ipd. Murray kot edino rešitev opiše budnost (internet 16), podkrepljeno s tehničnimi rešitvami beleženja dostopov, šifriranja podatkovnih baz in dajanjem določenih dostopnih pravic samo tistim delavcem, ki jih dejansko potrebujejo za opravljanje delovnih nalog.

Zagotoviti zaščito pred to obliko grožnje je zelo težko, saj so to ljudje, ki naj bi jim zaupali (Schneier 2000: 46). Dalje je težava v tem, da obstajajo zakonske omejitve glede podatkov, ki jih lahko pridobimo o posamezniku oziroma zaposlenem. Mimo teh omejitev lahko pridemo le z odredbo sodišča, kar bi zelo težko pridobili, preden je storjen kak zločin.

Če pa govorimo o jezi zaposlenih kot motivaciji, je to problem znotraj podjetja, kjer vodstvo bodisi ne posluša svojih zaposlenih bodisi jih marginalizira. Možno je tudi, da imajo zaposleni previsoka pričakovanja, ki jih vodstvo ne more ali ne želi izpolniti ali se oboji preprosto ne znajo dogovoriti. Skratka, razlog je razhajanje v pričakovanjih vodstva in delavcev. Predlog je sicer še eden, vendar zelo očiten: v primeru prenehanja zaposlitve je potrebno ukiniti vse dostopne pravice zaposlenemu, vendar to zadostuje le v primeru, ko pride do prenehanja zaposlitve. V prej naštetih primerih domnevam, da je zaposleni še vedno na delovnem mestu. Problema škodoželjnega zaposlenega se nikoli ne bo dalo v celoti odpraviti (Cole 2006: 11), lahko se pa njegove posledice omili z različnimi pristopi, z ugotovitvijo in razreševanjem konfliktov znotraj podjetja, tako med sodelavci kot med

vodstvom in podrejenimi, različnimi tehničnimi postopki in mehanizmi za zaščito občutljivih podatkov in selektivnim dodeljevanjem dostopnih pravic do teh.

Primer strukturirane grožnje predstavljajo infobojevniki. Do sedaj smo namreč govorili o nestrukturiranih grožnjah. Sredstva infobojevnikov se ne razlikujejo od tistih, ki jih uporabljajo bodisi teroristi, hekerji ali škodoželjni zaposleni. Smisel infobojevnika bi, po mojem mnenju, predstavljala zmožnost koordinacije učinkov vseh treh skupin za dosego čim večjega oškodovanja informacijskega sistema napadene države oziroma organizacije. Najboljša zaščita proti infobojevniku je vzpostavitev celovitega sistema zaščite informacijskega sistema, kjer pokrijemo grožnjo hekerjev, teroristov in škodoželjnih zaposlenih ter omilimo učinke vseh metod, ki jih infobojevnik lahko uporabi.

5.4 Sklep

V tem poglavju sem poskušal opredeliti tisto, kar v Sloveniji tvori kritično informacijsko infrastrukturo. Orisal sem, kako je sestavljena v gospodarskem sektorju, kakšna je sestava telekomunikacijskega omrežja in kakšna tehnologija se uporablja. Bolj pa sem se posvetil iniciativam državne uprave in načinu, kako se državna administracija posveča področju IKT. Predstavil sem glavne državne akterje na tem področju in spremembe, do katerih je na tem področju prišlo v zadnjih dveh letih. Prišlo je do dokaj obširnih sprememb, ki so močno spremenile politiko države na tem področju.

Opisal sem tudi možne grožnje informacijski infrastrukturi v Republiki Sloveniji. To so teroristi, hekerji, škodoželjni zaposleni in infobojevniki. Opisal sem tudi način, kako se lahko tem grožnjam zoperstavimo oziroma, kako njihove posledice omilimo. Opisal sem glavne značilnosti vsake od skupin, ki ogrožajo informacijsko infrastrukturo in prijeme, s katerimi se lahko zoperstavimo tem grožnjam. Nedvomno največ premisleka povzroča grožnja škodoželjnih zaposlenih, kjer moramo zaposlenim zaupati, statistično največ varnostnih incidentov izvira ravno od znotraj. V naslednjem poglavju bom predstavil svoje predloge za ureditev področja, hkrati pa bom hipoteze, ki sem jih določil na začetku, sprejel ali zavrnil.

6. ZAKLJUČEK

V prejšnjih poglavjih smo opredelili, kaj je kritična informacijska infrastruktura. Opisali smo njene sestavine, kateri dejavniki pomembno vplivajo na njeno varnost, kdo so tisti, ki jo ogrožajo, in na kakšen način jo varujemo. Na kritično informacijsko infrastrukturo lahko vplivajo 3 dogodki: nesreča, okvara ali napad. Največ pozornosti se namenja predvsem zadnjemu - napadom, kjer lahko razločimo dve veliki skupini groženj: strukturirane in nestrukturirane. Najverjetnejša oblika grožnje je nestrukturirana, kamor lahko štejemo kateregakoli posameznika, ki napade informacijski sistem. Ta grožnja bo najpogosteje izvirala iz organizacije same. Najverjetnejša oblika strukturirane grožnje informacijskega sistema bi predstavljala združitev oziroma koordinacija različnih nestrukturiranih groženj za dosego maksimalnega učinka zoper nek večji informacijski sistem.

Opisal sem varnostne mehanizme, s katerimi lahko varujemo informacijsko infrastrukturo in informacijske sisteme same. Teh poznamo več tipov, na nižjih ravneh lahko govorimo o tehničnem varovanju oziroma tehničnem pristopu k varovanju, predvsem varnosti računalniških omrežij. Naslednja skupina varnostnih mehanizmov predstavlja organizacijske varnostne mehanizme, kot so predvsem vpeljava ISO standarda 17799 in vzpostavitev CSIRT skupin. Vendar največjo in najbolj verjetno grožnjo najtežje odpravimo. Govorimo o škodoželjnem zaposlenem. Največja verjetnost statistično je namreč, da bo varnostni incident izviral znotraj organizacije oziroma sistema. Za uspešno soočenje s tem problemom bi organizacije morale veliko spremeniti. Preventiva na tem področju je resda težavna. Pomenila bi namreč ugotavljanje materialnega in psihofizičnega stanja posameznika, z namenom, da bi ugotovili njegovo primernost za neko delovno mesto, posebej za tisto delovno mesto, kjer bo delal z občutljivimi podatki. Zakonodaja namreč ščiti posameznika pred takšnimi kršitvami zasebnosti. Kot sem že omenil, je verjetno najbolje, da bi se zoperstavili tej grožnji z vzpostavitvijo dobre politike upravljanja s človeškimi viri skupaj z budnostjo, ki bi jo podkrepili z raznimi tehničnimi metodami za beleženje dostopov, šifriranjem podatkov in selektivnim izdajanjem dostopnih pravic.

Da bi se uspešno zoperstavili obem skupinam groženj, strukturiranim in nestrukturiranim, bi bilo, po mojem mnenju, potrebno pristopiti celovito, z vključitvijo vseh naštetih mehanizmov varovanja, da bi se torej soočili z grožnjami vseh oblik, tako hekerjev kot teroristov kot škodoželjnih zaposlenih in ne nazadnje infobojevnikov.

Pri pregledu kritične informacijske infrastrukture v Republiki Sloveniji sem opisal, kaj jo sestavlja. Ugotovili smo, da področje kritične informacijske infrastrukture sestavljajo stacionarno telefonsko omrežje, GSM mobilno telefonsko omrežje, paketna komutacijska omrežja, satelitske povezave in druge oblike javnih brezžičnih omrežij ter upravne storitve in informacijska infrastruktura v Republiki Sloveniji.

Informacijska tehnologija je nekaj, kar prepleta družbo v celoti. Poskus točne ozke opredelitve pristojnosti v državni upravi je po mojem mnenju neustrezen. Trenutna organizacija otežuje koordinacijo in usklajevanje dela med njimi. Dejansko je področje podrejeno 3 ministrstvom, kjer imajo ministri vsak svoje motive in vsak svoje prednostne naloge. Področje informacijske tehnologije predstavlja zgolj podporno dejavnost. Skrb za celovito upravljanje z informacijskim sistemom državne uprave tako postane tudi uradno fragmentirana. Razvoj na tem področju zaradi tega stagnira. Trenutna ureditev zelo ozko določi delovna področja direktoratov, hkrati pa medlo opiše njihove pristojnosti.

Moj predlog, v nasprotju s trenutnim stanjem, je vzpostavitev institucije na ravni ministrstva ali pa vladne službe, neposredno podrejene vladi, ki bi vse naloge naštetih direktoratov združila v eni instituciji. Podobno kot je bil včasih Center vlade za informatiko. Hkrati predlagam ustanovitev službe CSIRT, ki bi prevzela reaktivno, proaktivno in nalogo zagotavljanja kakovosti v pogledu varnosti informacijskega sistema. Opisal sem, da CSIRT pomaga pri nalogah zagotavljanja kakovosti. Po mojem mnenju je potrebno zagotoviti skladnost z njihovimi priporočili. Naslednji korak bi bil priprava varnostne politike na ravni celotne državne uprave po ISO standardu 17799, po kateri bi se morali ravnati vsi organi. Zagotoviti bi bilo potrebno še ločeno institucijo, ki bi preverjala skladnost z varnostno politiko, njenega področja pa ne bi omejil samo na državno upravo, temveč bi po potrebi opravljala te storitve tudi za poslovne subjekte. Poleg vsega pa bi morala takšna institucija biti predvsem zavezana strokovnosti in ne političnim odločitvam, kar pa bi politično vodstvo moralo potem tudi razumeti in spoštovati.

Potrebno bi bilo zagotoviti sredstva in politično voljo za izobraževanje uporabnikov, saj, kot sem predstavil, v državni upravi po nekaterih raziskavah veliko porabimo za tehniko, ki je potem uporabniki ne znajo učinkovito uporabiti.

Glede hipoteze, da ločimo varovalne mehanizme zaradi kompleksnosti in raznolikosti groženj kritični infrastrukturi na fizične, tehnološke in organizacijske. Fizični vidik varovanja predstavlja omejevanje fizičnega dostopa do te infrastrukture, tehnološki vidik predstavlja vključevanje namenskih sklopov oziroma podsistemov, ki zmanjšujejo grožnjo pred računalniškimi vdori, napadi trojanskih konjev, računalniških črvov in virusov. Organizacijski vidik varovanja kritične informacijske infrastrukture predstavlja ustanovitev organizacijskih enot, ki skrbijo za informacijsko varnost oziroma razširitev obstoječih organov, prav tako predstavlja varnostni mehanizem sama tehnična struktura informacijskega sistema, ki predstavlja bolj organizacijski kot tehnološki problem. Sem spada tudi vključevanje ustrezne varnostne politike in njena revizija oziroma nadzor nad njenim izvajanjem. Prav tako sodi sem izobraževanje kadrov s področja informacijske varnosti. Še bolj pomembna pa je, glede na grožnjo škodoželjnih zaposlenih, dobra politika ravnanja s človeškimi viri. To hipotezo lahko potrdimo.

Hipotezo, da je odvisnost družbe od informacijske tehnologije odvisna od njene prepletenosti, je težko potrditi. Če si pomagamo s številkami, ugotovimo, da skoraj polovica prebivalcev Slovenije uporablja internet vsaj enkrat mesečno. Profil uporabnikov razkriva, da uporabljajo IT predvsem za dostop do informacije in za uporabo elektronske pošte (RIS - Eurostat). Pri spletnem poslovanju z državno upravo storitve opravlja 30% uporabnikov interneta – 8% za pošiljanje obrazcev državni upravi. IT za posameznika, glede na opisano, torej ne predstavlja nečesa, kar bi bilo kritično. Če se premaknemo stran od uporabniškega vidika in gremo na poslovnega, lahko vidimo, da bi izpad oziroma nedelovanje IT močno otežilo komunikacije, saj 80% uporabnikov uporablja elektronsko pošto. Če domnevamo, da bi namesto enega poslanega elektronskega sporočila prejemnika morali poklicati, bi to močno obremenilo telefonsko omrežje. Težave bi bile z elektronskim bančništvom itd. Nedelovanje IT bi glede na našteto povzročilo škodo predvsem delovnim procesom v gospodarstvu, predvsem v velikih proizvodnih podjetjih, ki proizvajajo kompleksne stroje, in v državni upravi. Hipotezo lahko potrdimo.

Zadnja hipoteza je ta, da večja ko je odvisnost družbe od informacijske tehnologije, več ta družba vlaga v varovalne mehanizme. Izrecno tega dejstva nič ne dokazuje ali zavrača. Raziskave kažejo, da v javni upravi vlagamo več sredstev v tehniko, kot vlagamo v izobraževanje uporabnikov. V obeh primerih zaostajamo za evropskim povprečjem. Kot smo že omenili, je dejansko izobrazba uporabnikov tisto sredstvo, s katerim si organizacije in podjetja lahko zagotavljajo varnost lastne informacijske infrastrukture predvsem pred zunanjimi, deloma tudi pred notranjimi grožnjami. Če izpostavimo stanje v državni upravi, tudi tukaj ne obstaja celovita vseobsegajoča varnostna politika, ki bi sploh definirala oziroma določala ravnanje zaposlenih za preprečevanje varnostnih incidentov. To hipotezo zaradi tega lahko na primeru Slovenije za področje javne uprave zavrnemo. Drugače je na področju spletnega trgovanja, kjer uporabniki močno cenijo varnost, rast tega področja tako postane odvisna od občutka varnosti uporabnikov med spletnim nakupom. Glede na absolutno rast te gospodarske panoge in pomembnost, ki jo uporabniki pripisujejo varnosti, lahko sklepamo, da se uporabniki počutijo varne na spletu. Hipotezo lahko za področje gospodarstva potrdimo.

Po vsem napisanem smo ugotovili, da bi se lahko za varnost v Sloveniji na področju IT v javnem sektorju bolje skrbelo, če upoštevamo razdrobljenost pristojnosti za področje informacijske tehnologije nasploh, neobstoj varnostne politike v vseh državnih organih, pomanjkanje sredstev in politične volje za izobraževanje zaposlenih za učinkovito rabo tehnologije in nenaklonjenost vodstva vprašanju informacijske varnosti. S tem vprašanjem pa je drugače v gospodarstvu, kjer za varnostjo stoji ekonomski interes.

7. LITERATURA

7.1 Monografije

1. Dunn, Myriam in Isabelle Wigert (2004): *International CIIP Handbook 2004*. Zurich: Swiss federal institute of technology. Dostopno na http://cms.isn.ch/public/docs/doc_454_290_en.pdf (2. julij 2007).

2. Mitnick, Kevin(2002): *The art of deception*. New York: Wiley.

3. Directorate for science, technology and industry, committee for information computer and communications policy (2004): *Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security*. Dostopno na http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/81dd07040a1c0e43c1256eb6005423d4/$FILE/JT00169904.PDF (2. julij 2007).

4. Dunn, Myriam (2005): *A comparative analysis of cybersecurity initiatives worldwide*. Dostopno na http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (2. julij 2007).

5. West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle in Mark Zajicek (2003): *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh: Carnegie Mellon software engineering institute.

6. Silič, Marin, Marko Colnar, Marjan Krisper in Joszef Gyorkos (2001): *E-poslovanje v javni upravi 2001–2004*. Ljubljana: Center vlade za informatiko.

7. Pfajfar, Alenka (2004): *Elektronsko poslovanje javne uprave.* Ljubljana: FDV.

8. Hajtnik, Tatjana (2002): *Priporočila za izdelavo varnostne politike*. Ljubljana: Center vlade za informatiko.

9. Cole, Eric in Ring Sandra (2006): *The Insider Threat*. London: Syngress publishing.

10. Schneier, Bruce (2000): *Secrets and Lies: Security in a networked world*. New York: John Wiley.

11. Dunn, Myriam in Isabelle Wigert (2006): *International CIIP Handbook 2006*. Dostopno na http://www.isn.ethz.ch/pubs/ph/details.cfm?id=16156 (2. julij 2007).

12. Vehovar, Vasja in Tina Zupanič (2004): *Internet in Slovenska Država*. Ljubljana: FDV.

13. Vehovar, Vasja in Maša Šijanec (2005): *E-nakupovanje končnih potrošnikov 2004/2*. Ljubljana: FDV.

7.2 Članki

14. Svete, Uroš (2006): Nacionalnovarnostni vidiki ogrožanja informacijske infrastrukture. *Varstvoslovje* 8(1), 31–44.

15. Jelič, Borja (2003): *Pregled mobilnih tehnologij, njihova uporaba in delovanje.* Ljubljana: Mobitel. Interno gradivo.

16. Berce, Jaro (2005): Značilnosti in vplivi uvajanja modernih tehnologij in organizacijskih pristopov v državni upravi. V Metka Stare in Maja Bučar (ur.): *Učinki informacijsko-komunikacijskih tehnologij,* 153–170. Ljubljana: FDV.

17. Merrill, Warkentin in Allen C. Johnston (2006): IT Security Governance and Centralized Security Controls. V Merril Warkentin in Vaughn Rayford: *Enterprise Information systems assurance and System Security*, 16–25. Hershey: Idea Publishing.

18. Sirnik, Iztok (2005): Vzpostavitev središča za usposabljanje. V Novaković Aleksander, Niko Schlamberger, Mojca Indihar Štemberger, Jasna Poženel in Marko

Bajec: *Dnevi Slovenske informatike*, 321–331. Ljubljana: Slovensko društvo Informatika.

7.3 Internetne publikacije

19. Internet 1: Webopedia, Online Computer Dictionary: *System*. Dostopno na http://www.webopedia.com/TERM/s/system.html (11. april 2006).

20. Internet 2: CNN (2006): *U.S. not 'well-prepared' for terrorism*. Dostopno na http://www.cnn.com/2005/US/12/04/911.commission/index.html (11. april 2006).

21. Internet 3: CNN (2005): *A convicted hacker debunks some myths*. Dostopno na http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/ (11. april 2006).

22. Internet 4:GOV-CERT.NL (2005): *Setting up a CSIRT*. Dostopno na http://www.first.org/resources/guides/cert-in-a-box/content/68.html (11. april 2006).

23. Internet 5: Slo-Tech (2004): *Pogovor z Gorazdom Božičem, vodjo varnostnega centra SI-CERT*. Dostopno na http://www.slo-tech.com/clanki/04023/ (11. april 2006).

24. Internet 6: MSNBC (2005): *Internet-based terror attacks unlikely,FBI says*. Dostopno na http://www.msnbc.msn.com/id/10382716/ (11. april 2006).

25. Internet 7: Valdes, Robert: *How VoIP Works***.** Dostopno na http://computer.howstuffworks.com/ip-telephony4.htm (11. april 2006).

26. Internet 8: Wikipedia (2005): *Integrated services digital network*. Dostopno na http://en.wikipedia.org/wiki/Integrated_Services_Digital_Network (11. april 2006).

27. Internet 9: Tyson, Jeff: *How internet infrastructure works*. Dostopno na http://computer.howstuffworks.com/internet-infrastructure1.htm (11. april 2006).

28. Internet 10: Bankart (2005): *Procesiranje Plačilnih kartic*. Dostopno na http://www.bankart.si/bankart.php?menu=si_poslovanje_procesiranje (11. april 2006).

29. Internet 11: Bowen, Jim: *How ATM's work*. Dostopno na http://money.howstuffworks.com/atm.htm (11. april 2006).

30. Internet 12: RIS (2005): *Število uporabnikov Interneta*. Dostopno na http://www.ris.org/index.php?fl=0&id=640 (11. april 2006).

31. Internet 13: RIS (2006): *Uporabniki interneta v Sloveniji*. Dostopno na http://www.ris.org/index.php?fl=1&nt=9&sid=442 (11. april 2006).

32. Internet 14:Messmer, Ellen: *Insider threat looms target*. Dostopno na http://www.networkworld.com/news/2003/1208infowar.html (11. april 2006).

33. Internet 15: Dolhar, Žiga: *NLB-jevih petsto*. Dostopno na http://slo-tech.com/clanki/var01/var01.shtml (18. maj 2007).

34. Internet 16: Conry-Murray, Andrew: *The threat from within.* Dostopno na http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=177105068 (18. maj 2007).

35. Internet 17: Dynes, Scott: *Costs to the U.S. Economy of Information Infrastructure Failures: Estimates from Field Studies and Economic Data*. Dostopno na http://weis2006.econinfosec.org/docs/4.pdf (29. avgust 2006).

36. Internet 18: Meserve, Jason: *Filesharing leads internet*. Dostopno na http://www.macworld.co.uk/news/index.cfm?RSS&NewsID=12469 (29. avgust 2006).

37. Internet 19: Žerdin H. Ali: *Obtožujem!*. Dostopno na http://www.mladina.si/tednik/200632/clanek/slo-tema--ali_h_zerdin/ (11. september 2006).

38. Internet 20: 24ur (2007): *Uporabljali lažne kartice*. Dostopno na http://24ur.com/bin/article.php?article_id=3091919 (20. marec 2007).

39. Internet 21: SI-CERT (2004): *Kaj je SI-CERT*. Dostopno na http://www.arnes.si/si-cert/opis.html (4. julij 2007).

40. Internet 22: Ministrstvo za Informacijsko Družbo (2004): *Predstavitev Ministrstva za Informacijsko družbo*. Dostopno na http://mid.gov.si (4. julij 2007).

7.4 Zakoni in uradne publikacije

41. Internet 23: Presidential directive (2003): *Homeland Security Presidential Directive/Hspd-7; Subject: Critical Infrastructure Identification, Prioritization, and Protection.* Dostopno na http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html (11. april 2006).

42. Internet 24: U.S. Congress: *Uniting and strengthening America Act*. Dostopno na http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h2975eh.txt.pdf (11. april 2006).

43. Internet 25:Državni zbor RS (2004): *Zakon o spremembah in dopolnitvah zakona o vladi republike Slovenije (ZVRS-D)*. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=2004123&stevilka=5120 (11. april 2006).

44. Internet 26: Državni zbor RS (2004): *Zakon o spremembah in dopolnitvah zakona o državni upravi (ZDU-1C)*. Dostopno na http://www.uradni-list.si/1/objava.jsp?urlid=2004123&stevilka=5121 (11. april 2006).

45. Ministrstvo za Javno Upravo (2006): *Akt o notranji organizaciji in sistemizaciji delovnih mest v Ministrstvu za Javno upravo RS*. Ljubljana: Ministrstvo za javno upravo.

46. Internet 27: Državni zbor RS (2004): *Zakon o elektronskih komunikacijah*. Dostopno na http://www.dz-rs.si/index.php?id=101&vt=6&sm=k&q=elektronskih+komunikacijah&mandate=-1&unid=SZ|C12563A400338836C1256E750024D096&showdoc=1 (11. april 2006)

47. Internet 28: Vlada Republike Slovenije (2004): *Predstavitev ministrstva za gospodarstvo*. Dostopno na http://www.vlada.si/?gr1=min&gr2=minMzg&gr3=&gr4=&id=&lng=slo (11. april 2006).

48. Internet 29: Vlada Republike Slovenije (2004): *Predstavitev ministrstva za Javno upravo.* Dostopno na http://www.vlada.si/?gr1=min&gr2=minJavUpr&gr3=&gr4=&id=&lng=slo (11. april 2006).

49. Internet 30: Vlada Republike Slovenije (2004): *Predstavitev ministrstva za Visoko šolstvo, znanost in tehnologijo*. Dostopno na http://www.vlada.si/?gr1=min&gr2=minSzt&gr3=&gr4=&id=&lng=slo (11. april 2006).

50. Internet 31: Center Vlade za Informatiko (2004): *Predstavitev Centra vlade za Informatiko*. Dostopno na http://www.sigov.si/cvi (11. april 2006).

51. Internet 32: Public safety Canada: *About Crtitical infrastructure*. Dostopno na http://www.psepc-sppcc.gc.ca/prg/em/nciap/about-en.asp (13. september 2006).

52. Internet 33: National Security Telecommunications and Information Systems Security Committee: *National Information Security (INFOSEC) Glossary*. Dostopno na http://security.isu.edu/pdf/4009.pdf (21. marec 2007).

53. British standards (2005): *ISO/IEC 17799 Information technology — Security techniques — Code of practice for information security management.* London: British standards publishing.

54. British standards (2005): *ISO/IEC 27001:2005 – Information technology, security techniques, information security techniques, requirements*. London: British standards publishing.

55. Internet 34: Državni Zbor RS: *Predstavitev kandidata za ministra za javno upravo dr. Gregorja Viranta pred matičnim odborom*. Dostopno na http://www.dz-rs.si/index.php?id=96&cs=7&sb=3&sd=0&committee=3&o=220&unid=MDT|875F671CCC9F0636C1256F5B003071CA&showdoc=1 (11. april 2006).

7.5 Intervju

56. Intervju z Iztokom Sirnikom, Podsekretarjem na Ministrstvu za Javno Upravo. Ljubljana 23.2.2006