ŠOLA ZA ČASTNIKE
ŠTEVILKA GENERACIJE
VED ČASTNIK OBVEŠČEVALEC

ZAKLJUČNA NALOGA

SVETOVNI SPLET IN KIBERNETSKE GROŽNJE KOT IZZIV INFORMACIJSKI VARNOSTI V SV

Kandidat-slušatelj: nadporočnik Anton Ajster

Mentor: stotnik Borut Korošec

So-mentor:

Novo mesto, maj 2012

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
SLOVENSKA VOJSKA
POVELJSTVO ZA DOKTRINO, RAZVOJ, IZOBRAŽEVANJE IN USPOSABLJANJE
Šola za častnike

Engelsova ulica 15, 2111 Maribor

Številka:
Datum:

ZAKLJUČNA NALOGA

Svetovni splet in kibernetske grožnje kot izziv informacijski varnosti v SV

Kandidat-slušatelj: nadporočnik Anton Ajster

Mentor: stotnik Borut Korošec

So-mentor:

Novo mesto, maj 2012

POVZETEK

Vse več ključnih sistemov v našem življenju temelji na informacijskih sistemih. Ti predstavljajo temeljni element naše sposobnosti vse od hitrega komuniciranja in oskrbe z osnovnimi dobrinami do najbolj zapletenih varnostnih zadev.

Ranljivost povezanih informacijsko komunikacijskih sistemov je veliko kompleksnejša kot ranljivost posameznih komponent komunikacijsko informacijskega sistema posebej pred notranjim in zunanjim ogrožanjem. Še posebej kompleksno pa je, ko želimo povezati različna operacijska in varnostna okolja. S sprejemanjem kompromisov nastane tveganje za nepooblaščen dostop, spremembo ali uničenje informacij prav tako je ogroženo vzdrževanje integritete in razpoložljivosti spremljajočih komponent oziroma storitev.

V delu se ukvarjam s predstavitvijo spleta, grožnjami, ranljivostmi in analizo tveganj.

SUMMARY

Information systems and cyberspace touches nearly every key service in our lives. They constitite s fundamental element of our ability for rapid communication and fulfilment of our basic needs up to the most complex security things.

Interconnected Communications and Informations Sistems (CIS) are inherently more complex than the individual component CIS and are therefore more vulnerable to internal and external threats.The interconnection of CIS within different operational and security environments increases the risk associated with the compromise and unauthorized modification / delition of information, and the risks associated with maintaining the integrity and availability of the supporting components / services.

At the work I introduse the Internet, threats, vulnerabilities and threats assesement.

KLJUČNE BESEDE

Internet, grožnje, ranljivosti, analiza tveganja, informacija, podatek

KEY WORDS

Internet, Threats, Vulnerabilities, Risk Assesment, Information, Data

KAZALO

1 UVOD

V zaključni nalogi je predstavljen razvoj interneta in svetovnega spleta. Z razvojem je prišlo do enormnega povečanja števila uporabnikov in razširitev na cel svet. Brezmejnost omrežij in velika razširjenost onemogočata učinkovit nadzor. Skladno s takšnim razvojem imamo danes možnost skoraj brezplačno prenašati kamorkoli in komurkoli. Z razvojem komunikacij je prišlo do povezanosti družbe, ki si je pred dvema desetletjema ni bilo možno predstavljati. Dostopnost do informacij je postala trenutna.

Skladno z razvojem spleta (kibernetskega okolja) je prišlo tudi do razvoja kibernetskih groženj. Carl von Clauzevitz je v svoji knjigi O VOJNI definiral vojno »kot nadaljevanje politike z drugimi sredstvi«. Danes to definicijo lahko razširimo tudi v kibernetski prostor. Med kibernetskimi grožnjami se srečujemo s kibernetskim kriminalom, kibernetskim terorizmom, poskusi vohunjenja, nepooblaščenega vdiranja v računalnike, krajo podatkov in drugimi oblikami napadov. Predmet napadov so lahko različna področja, obrambno – varnostno, poslovno, telekomunikacijsko, ali katerokoli drugo. »Ključno je, da gre za brezmejne grožnje, saj geografske razdalje, politične strukture in omejene pravne pristojnosti napadalcem olajšujejo delovanje« (Dokl 2012:11).

V prvem delu naloge predstavljam značilnosti kibernetskega prostora. Ključni sta razširjenost in uporabna vrednost. Predstavil bom osnovne tehnologije, grožnje in zaščito pred grožnjami.

V nadaljevanju naloge povzemam stanje na področju v Slovenski vojski in MORS. Poseben poudarek je namenjen morebitni ranljivosti sistema, povezanost z ostalimi gradniki varnosti in usposobljenost ter osveščenost pripadnikov ter skrbnikov sistemov.

1.1 IZHODIŠČE ZAKLJUČNE NALOGE

Skladno z razvojem interneta in svetovnega spleta in zakonskimi možnostmi, ki dovoljujejo povezovanje interneta z omrežji, ki obdelujejo tajne podatke do stopnje tajnosti INTERNO bom postavil naslednje hipoteze:

HIPOTEZA 1:
Razširjenost kibernetskega okolja, nam omogoča povezljivost in dosegljivost od koderkoli.

HIPOTEZA 2:
Povečane možnosti prenosa podatkov in uporabnost aplikacij vplivata na vsesplošni razvojrazvoj in odvisnost od informacijske tehnike.

HIPOTEZA 3:
Kibernetski napadi na povezan informacijski sistem lahko povzročijo takšno škodo, kot nekdaj konvencionalna vojna.

Skozi nalogo bom preveril hipoteze in v zaključku ponudil rešitve in izzive za eventualno povečanje varnosti komunikacijsko informacijskih sistemov v Slovenski vojski oziroma MORS (KIS SV/MORS).

1.2 NAMEN IN CILJI RAZISKAVE

Namen zaključne naloge je proučevanje kibernetske varnosti omrežij, spoznavanje groženj, akterjev, dimenzij in drugih vzrokov za ogroženost omrežij in ključne informacijske infrastrukture. Po spoznavanju tipov groženj in ranljivosti omrežij se bom osredotočil na ogrožanje in kibernetsko varnost v MORS.

Cilj raziskave je ugotoviti, ali trenutno stanje v Slovenski vojski ustreza potrebam uporabnikov oziroma ali je povezava internega omrežja z internetom smiselna in za kakšno ceno?

Prav tako je cilj raziskave ugotoviti kakšno tveganje predstavlja povezava internega omrežja z internetom.

1.3 METODE DELA

Metode, ki sem jih uporabil v nalogi so naslednje:

- Zbiranje sekundarnih virov (dostopni viri o problematiki);
- Opisna (deskriptivna) metoda (predstavitev interneta, virov ogrožanja,…); in
- Analiza in interpretacija virov (normativna podlaga na področju).

V nalogi bom na podlagi deskriptivne metode obdelal podatke iz pisnih in spletnih virov. Izbira metode je prilagojena posamičnemu obravnavanemu segmentu.

Analitično bom uredil obravnavano problematiko groženj in ranljivosti.

1.4 STRUKTURA ZAKLJUČNE NALOGE

V uvodu predstavljam tematiko naloge.

V osrednjem delu bo predstavljena kratka zgodovina interneta in značilnosti kibernetskega prostora. V nadaljevanju bom omenjeni področji predstavil še za SV in MORS. Ocenil bom ranljivost našega sistema upoštevajoč vse gradnike varnosti.

V zaključku bodo predstavljene ugotovitve iz osrednjega dela naloge in ustreznost trenutnih rešitev. Predstavil bom izzive za povečanje varnosti komunikacijsko informacijskega sistema Slovenske vojske oziroma MORS.

Vse ocene in podatki ne bodo vsebovali tajnih podatkov.

2 INTERNET

»Izraz internet je okrajšava za interconnected network (medsebojno povezano omrežje), pomeni pa globalno med seboj povezano omrežje, ki milijonom računalnikov omogoča vsakodnevno medsebojno komunikacijo« (Egan 2005: 3).

2.1 ZGODOVINA INTERNETA

Začetek interneta sega v leto 1958, ko je predsednik ZDA Einsenhower zahteval proračunska sredstva za inovacije v sklopu ameriške raziskovalne agencije ARPA in so bila odobrena v okviru proračuna letalskih sil ZDA.

Leta 1965 je bil uspešno izveden prvi eksperiment s tehnologijo BBN. Dva računalnika sta med seboj komunicirala s paketno tehnologijo.

V letu 1974 se pojavi prvič izraz internet. Vint Cerf in Bob Kahn iz SRI objavijo prispevek v ACM o protokolu za nadzor prenosa “Transmission Control Protocol”. Zato se ta dva znanstvenika štejeta kot očeta omrežja Internet. Ministrstvo za obrambo ZDA začne eksperimentirati s protokolom TCP/IP in kmalu sprejeme odločitev, da je to najbolj primeren protokol za prenos podatkov v njihovem omrežju ARPANET. To leto štejemo za leto rojstva Interneta. Hrbtenica: 50Kbps ARPANET. Število povezanih računalnikov : 23 +.

1976 Dr Robert M. Metcalfe razvije Ethernet, ki je omogočil izjemno hiter prenos podatkov po koaksialnem kablu. Pojava te tehnologije je ključna za razvoj lokalnih omrežij. Z delom začne projekt za paketni satelitski prenos in njegova praktična uporaba. SATNET, Atlantsko paketno satelitsko omrežje začne delovati. To omrežje poveže Združene države Amerike z Evropo. Presenetljivo je, da ga uporablja tudi konzorcij INTELSAT, ki je v lasti držav izven ZDA in vladnih organizacij iz ameriške administracije. Razvijejo protokol UUCP (Unix-to-Unix Copy), v okviru AT & T Bell Labs, ki potem postane sestavni del operacijskega sistema UNIX.

V letu 1983 je ustanovljen odbor za Internetne Aktivnosti (Internet Activities Board – IAB). Sprejet je odlok, da mora vsak računalnik ali naprava, ki želi biti priključena na ARPANET uporabljati protokol TCP / IP. To velja od 1. januarja 1983 naprej. TCP / IP je postal dejanski internetni . University of Wisconsin razvije imenski prostor omrežja: Domain Name System (DNS). To je omogočilo, da so internetni paketi dobili ime domene, ki jo strežnik baze podatkov DNS-a prevede v ustrezni številčni naslov protokola IP. Ta način naslavljanja je veliko sprejemljivejši za ljudi zlasti pri dostopu do drugih strežnikov, saj si ni bilo več mogoče zapomniti naslove vseh povezanih računalnikov. Hrbtenica: 50Kbps ARPANET, 56kbps CSNET, plus satelitske radio in linijske povezave – število povezanih računalnikov in naprav: 562.

1985 se ARPANET razdeli na dve omrežji: MILNET in ARPANET. MILNET je namenjen potrebam vojske, ARPANET pa je namenjen, da služi kot orodje pri raziskavah informacijskih omrežij in novih omrežnih tehnologij. US Department of Defense še naprej podpira finančno obe omrežji.

V letu 1991 Agencija NSF ustanovi novo omrežje, imenovano NREN, National Research and Educational Network. Namen tega omrežja je bil zagotoviti poligon za raziskave prenosa podatkov z velikimi hitrostmi in mrežnih tehnologij. Omrežje ni bilo namenjeno komercialni uporabi in prenos velikih količin podatkov ni bil dovoljen. Hrbtenica: delna 45Mbps (T3)

NSFNET, nekaj zasebnih hrbtenic, plus satelitske in radio povezave – Število povezanih naprav: 617.000.
Laboratorij za odprte sisteme in mreže Instituta Jožef Stefan, Ljubljana, Slovenija z enkapsulacijo TCP/IP v X.25 (na postaji SPARC +1) poveže Ljubljano z Amsterdamom in vstopi v omrežje Internet. Pred tem si zagotovi dovoljenje omrežja EASYnet, ki ga financirajo raziskovalne ustanove kot je CERN in NIKHEF iz Amsterdama ter IBM za prenos paketov TCP/IP iz Ljubljane v Internet. Paketi potujejo do infrastrukture IXI na Dunaju, od tam prek CERN-a v Ženevi v Amsterdam v institut za fiziko in matematiko NICKEF. DNS (še vedno za Jugoslavijo) se prenese iz Univerze v Berkleyu na računalnik SPARK in vzpostavi delovanje elektronske pošte po protokolu TCP/IP.

Leto 1992 štejemo za začetek obdobja komercializacije Interneta, ki se kaže tudi v napovedi, da bo naslovni prostor internet kmalu izčrpan in da Internet potrebuje nov protokol in sistem naslavljanja. Obstoječi sistem po protokolu IPv4 lahko zadovolji potrebe po 32-bitnih internetnih naslovih le še nekaj let. IETF razvije nov protokol IPv6 in njegov 128-bitni naslovni prostor. Vendar obstoječi sistem 32-bitnih naslovov znan kot CIDR je zelo trdno zasidran. Razvoj IPv6 traja nekaj let. Rešitev je bila izbrana na podlagi evalvacije treh konkurenčnih sistemov.

V letu 1999 je pomemben pojav brezžičnih tehnologij, imenovanih IEEE 802.11b, bolj na splošno znanih kot Wi-Fi, ki postanejo sestavni del vsakega prenosnega računalnika ali naprave.

V letu 2005 se začne, akcija »one Laptop Per Child« projekt, ki ima za cilj zagotoviti ustrezno izobraževanje s cenenimi prenosniki vsem otrokom povsod svetu. Temelj projekta so netbooks - prenosniki za otroke z daljšo življenjsko dobo baterije in vgrajeno v Wi-Fi povezljivost, ki stanejo le 100 USD.
Pojavijo se dlančniki z multi-touch tehnologijo, ter tablični računalniki, in pametni mobilni telefoni. Ta tehnologija dopolnjuje tradicionalno touch-screen tehnologijo, ki omogoča prijazno uporabniško komunikacijo z računalnikom. Pomembnost tega je v nadomeščanju klasičnih tipkovnic.

Internet lahko štejemo med najpomembnejše izume 20. stoletja.

2.2 INTERNET DANES

Decembra leta 2010 v ZDA začnejo z implementacijo 4. generacije brezžičnih omrežij, ki omogoča visoke hitrosti pri povezavi naprav, kot so mobilni telefoni, tablični računalniki, in do ostalih mobilnih naprav. V letu 2011, tehnološka podjetja intenzivno razvijajo tehnologijo, ki bo zagotovila sodobnost in učinkovitost izobraževalnega sistema z uporabo internetnih tehnologij povsod po svetu.

Nove tehnologije, imenovane po protokolu IPv6, bi morale nadomestiti IPv4 tehnologijo. IPv4 omogoča naslove za manj kot 4.300.000.000 neposredno povezanih internetnih naprav. Naslovni prostor IPv4 je izčrpan in problem nastaja zaradi dejstva, da je svetovnega prebivalstva (v letu 2009) že precej več kot 6.500.000.000 in da s pojavom RFID tehnologij potreba po internetnih naslovih postaja čedalje bolj pereča. Teoretična ocena je, da če bi vsak človek na zemlji imel računalnik in mobilni telefon, bi potrebovali 13000000000 internetnih naslovov. V tem času to lahko zagotovi le naslovni prostor protokola IPv6. Vendar je prehod na IPv6 še zmeraj počasen. Statistika pravi, da je le 5% vseh naprav na internet naslovljenih s protokolom IPv6.

Združeni narodi so maja 2011 sprejeli deklaracijo s katero se dostop do Interneta uvršča med človekove pravice.

2.3 SPLET

Splet se je pojavil v letu 1991. 1993 pa se je pojavil prvi spletni brskalnik Mosaic, ki je postal splošno dostopen, z njim pa tudi dostop do svetovnega spleta. Leta 1994 je Mosaic postal drugi najbolj popularen servis na Internetu. Leta 1995 je najmanj 18 milijonov ljudi uporabljalo splet v ZDA in Kanadi. Velika raziskava pa je razkrila, da je bil skupen čas uporabe spleta enak skupnemu času predvajanja vseh sposojenih videokaset v teh dveh državah.

3 VARNOST

Razvoj svetovnega političnega in družbenega življenja v zadnjih dvajsetih letih po hladni vojni je vplival tudi na varnostne okoliščine. V obdobju hladne vojne je imelo varnostno okolje večinoma politične in vojaške razsežnosti, danes pa so v ospredju drugi vidiki širše socialne in kulturno civilizacijske dimenzije. »Sodobna razprava o varnosti se tako usmerja predvsem na referenčne objekte (na koga se varnost nanaša), kdo ali kaj to varnost ogroža (grožnje varnosti) in na kakšen način to varnost zagotavljati (varnostni mehanizmi). To so tri dileme, ki definirajo sodobno varnostno paradigmo (Liotta v Svete 2005: 55). Tradicionalna varnost v smislu vojaške obrambe ozemlja držav je presežena« (Dokl 2012:17).

Varnost in elektronsko poslovanje večina povezuje z rojstvom PGP (1976 sta kriptograf in odvetnik Diffie ter inženir energetike Hellman razvila kriptografijo z javnim ključem).

V zgodovini so za prenos zaupnih informacij vladarji uporabljali posebne sle. V drugi svetovni vojni so Nemci za prenašanje tajnih informacij uporabljali posebne mehanske šifrirne naprave (Enigma), Američani pa so uporabljali Indijance določenih plemen. Cilj razvoja zaščite informacij je bil skrajšati čas kriptiranja in dekriptiranja ter doseči branje v realnem času.

Z razvojem elektronike, komunikacij in informatike pa se je pojavila potreba po varnem komuniciranju. Izmenjava elektronske pošte je bila ena od prvih storitev na internetu. Vsebine sporočil so bolj ali manj zaupne narave, pošta pa je zasebna zadeva. Za dosego želenega cilja so nekateri uporabili kriptografske postopke. Eden od programov za izdelavo varne pošte je PGP (Preety Good Privacy).

Pri kateri koli vrsti elektronskega poslovanja imamo cilj zagotoviti naslednje pogoje za delovanje elektronskega sistema:

- celovitost,
- razpoložljivost in
- zaupnost.

Danes večina uporablja štiri operacijske sisteme:

- Windows
- Linux,
- Unix, in
- Mac OS X

Microsoft Windows operacijski sistemi so bili nekoč zgrajeni na osnovi MS-DOS. Novejši Windows operacijski sistemi ponujajo večopravilnost, ki omogoča izvajanje večih aplikacij hkrati, ne da bi vrnili nadzor procesorju. Windowsi zmeraj obstajajo za strežniške in odjemalske delovne postaje. Jedri obeh verzij sta enaki, le da strežniška vsebuje obilico programov, aplikacij, ponudb in orodij. Strežniški sistemi imajo možnost, da delujejo kot domenski kontrolorji, ki shranjujejo informacije o uporabnikih, za dostop odjemalcev povsod po omrežju, kar olajša nadzor nad sredstvi v omrežju.

Linux je odprto kodna (open souce) verzija operacijskega sistema za osebne računalnike in strežnike, ki je prosto dostopna.

Unix je razvijalo več razvojnih skupin, zato obstaja več različnih verzij. Večinoma se uporablja v profesionalne namene, še posebej na področju sistemov nadzora zračnega prostora (tudi v Slovenski vojski).

Mac OS X je operacijski sistem podjetja Apple, ki je licenciran samo za uporabo na Applovih napravah.

V raziskave za varno uporabo interneta so bila vložena ogromna sredstva. Kljub temu nihče ne zagotavlja varne uporabe, če se ne držite določenih pravil. Zato je potrebno, da vsak uporabnik, ki želi resno poslovati preko spleta upošteva določeno varnostno politiko, ki je osnova, da zaznamo napade in preprečimo poškodovanje našega elektronskega sistema. S tem preprečimo nastanek škode, začasnega izpada sistema itd.

Zato je priporočljivo, da si definiramo varnostno politiko, kjer opredelimo kaj in kako, kakšne so pravice in dolžnosti uporabnikov.

Kibernetski prostor je interakcija med ljudmi, podatki in računalniki, ki so povezani tako, da delujejo drug na drugega.

Pri varovanju podatkov je pomembno, da upoštevamo vse gradnike varnosti. Zagotavljati moramo fizično varnost, tehnično varnost, osebno varnost in informacijsko varnost. Naš sistem je varen le toliko kot je varen najšibkejši člen naše varnosti.

Z ustreznimi ukrepi varnostne politike na področju fizične varnosti, osebne varnosti in informacijske varnosti lahko zagotovimo ustrezno zaščito informacij in preprečimo vdore v računalniška omrežja MORS. Upoštevati moramo, da mora SV zagotavljati ustrezno zaščito informacij tako na mirnodobnih lokacijah, kot tudi v operativnih oziroma taktičnih pogojih.

»V Republiki Sloveniji smo prenovili sistem varovanja tajnih podatkov po zgledu EU in zveze NATO in med tem zanemarili obstoječo varnostno kulturo« (Kovač 2010, 29).

3.1 FIZIČNA VARNOST

Kritični element fizične varnosti so človeški viri. Nacionalni in NATO predpisi predvidevajo kombinacijo organizacijskih ukrepov fizičnega in tehničnega varovanja, kar je lahko le dopolnilo fizičnemu varovanju. Z ustrezno politiko vzpostavitve varnostnih območij ter ostalih ukrepov se zagotovi potreben nivo fizične varnosti.

Fizično varnost zagotovimo tako, ta objekt namestimo v prostor, ki je ograjen z ustrezno ograjo, tako da je možno nadzorovati ter usmerjati gibanje uporabnikov.

Pri fizični varnosti je pomembno, da upoštevamo stopnjo tajnosti in kategorijo obravnavanih informacij. Upoštevati moramo obliko in količino informacij (odvisno ali gre za tiskane medije, opremo ali za elektronsko obliko hranjenja informacij). Pomembno je, da z zadevo upravlja ustrezno preverjeno osebje, ki ima potrebo po vedenju. Upoštevati moramo oceno ogrožanja glede na okolje v katerem delujemo. Tu upoštevamo verjetnost sabotaže, terorističnega napada, subverzije in ostalih kriminalnih aktivnosti. Prav tako je potrebno upoštevati kako bodo informacije shranjene (povzeto po AC/35-D1030:1-2).

Pri načrtovanju varnostnih ukrepov je potrebno načrtovati preprečitev dostopa in ukrepanje proti napadalcem. Zaznati poskuse dostopa do informacij vključno s poskusi vohunjenja. Zagotoviti moramo dostop le pooblaščenim posameznikom, ki imajo potrebo po vedenju. Zaznati in ukrepati je potrebno proti vsem varnostnim kršitvam in kršiteljem.

Ključen je sistem obrambe v globino. Kar pomeni, da ob upoštevanju fizičnih varnostnih ukrepov in ostalih tehničnih varnostnih standardov za nameščanje kritične infrastrukture zagotavljamo potreben nivo varnosti.

V ta namen imamo v SV in MORS vzpostavljena administrativna varnostna območja, kjer obdelujemo in hranimo informacije vključno s stopnjo tajnosti INTERNO. Prav tako imamo glede na potrebe v vojaških objektih varnostna območja II: in I. stopnje, kjer se obdelujejo tajni podatki višjih stopenj skladno z zahtevami Zakona o tajnih podatkih s pripadajočimi uredbami s tega področja.

V varnostnih območjih zagotavljamo nadzor vstopa. Vsi zaposleni imajo ustrezne varnostno identifikacijske priponke in se po objektih lahko gibljejo skladno s pristopnimi pravicami in potrebo po vedenju. Prav tako so definirani postopki za obiskovalce in servisno osebje. Obema kategorijama se zagotovi potrebno spremstvo skladno z varnostno operativnimi postopki oziroma hišnim redom objekta.

3.2 TEHNIČNA VARNOST

Na osnovi varnostne ocene se objekti v stalni uporabi SV ali MORS tehnično varujejo z ustreznim protivlomnim in protipožarnim sistemom. Signali so speljani v nadzorne centre, kjer se spremlja stanje. Vsi alarmi se prenašajo intervencijskim skupinam, ki nato preverijo alarm oziroma ukrepajo skladno s predpisanimi postopki.

Prav tako je potrebno poudariti, da imamo administrativna območja ograjena z varnostno ograjo.

Za prostore, kjer se nahaja ključna informacijska tehnologija običajno izvedemo še dodatne varnostne ukrepe, čeprav se nahajajo najmanj v administrativnih varnostnih območjih. Običajno vstop v te prostore dodatno nadziramo s kombinacijskimi ključavnicami in ustreznimi cilindričnimi ključavnicami. Zahteve so enake kot za II. varnostno območje.

3.3 OSEBNA VARNOST

Prelomnico na področju osebne varnosti predstavlja vstop Slovenije v Evroatlantske povezave v letu 2004 in s tem sprejem novega Zakona o tajnih podatkih s spremljajočimi uredbami. Popolnoma na novo je bilo urejeno področje varnostnega preverjanja – usklajen in poenoteno z zahtevami povezav.

Vsi zaposleni v MORS so preverjeni skladno s 35. členom Zakona o obrambi (Ur. L. RS, št. 104/2004-UPB1), kar zagotavlja potrebni nivo za dostop do informacij stopnje tajnosti INTERNO. Vsi posamezniki, ki imajo potrebo po dostopu do višjih stopenj tajnosti se preverjajo skladno s postopki Zakona o tajnih podatkih (Ur. L. RS, št. 50/06-UPB), Uredbo o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Ur. L. RS, št. 71/06)

3.4 INFORMACIJSKA IN OMREŽNA VARNOST

Zaradi čedalje večjega pomena omrežij v sodobni družbi postajajo omrežja sama referenčni objekt varnosti. »Čedalje večja odvisnost družbe od omrežne informacijske infrastrukture (predvsem ključne informacijske infrastrukture) je vplivala na nastanek nove varnostne predstave, ki je usmerjena v zavarovanje omrežja samega, izgubo, krajo ali uničenje podatkov ter prekinitev informacijskih tokov« (Dokl 2012: 27).

Informacijsko – komunikacijska oprema v vseh pomembnih družbenih podsistemih je v sodobnih družbah postala nepogrešljivo sredstvo in prvina delovanja, s čimer omogoča uravnotežen razvoj.
Prav slednje predstavlja razlog za vrednotenje informacijske dimenzije,ki je pomemben element in dejavnik varnosti. Ločimo omrežno varnost, ki se nanaša izključno na delovanje in zanesljivost informacijskih sistemov. V kolikor je zaznana grožnja varnosti države oziroma nacionalni varnosti,država omeji zbiranje podatkov ali blokira informacijski tok,

Ključna prednost elektronskega poslovanja je, da so nam na voljo skoraj neomejene možnosti povezovanja, prilagajanja in optimiranja v delovnih procesih. Nismo več omejeni na lokalen prostor, ampak smo povezljivi povsod.

Pri povezovanju s partnerji v elektronski obliki, moramo skladno z varnostno politiko zagotoviti varne komunikacije. To je osnova za varen prenos podatkov.

Če nimamo definirane ustrezne varnostne politike in je vsakomur omogočeno, da nenadzorovano “brska” po informacijskem sistemu lahko pride do nepooblaščenega kopiranja podatkov in s tem odtoka podatkov nepooblaščenim osebam oziroma organizacijam.

V slučaju, ko komuniciramo preko svetovnega spleta nezaščiteno, smo pod nadzorom raznih tajnih služb in ostalih posameznikov ter organizacij, ki se ukvarjajo z vohunjenjem.

3.4.1 INFOSEC

»INFOSEC opredeljuje varnostne ukrepe in postopke za varovanje informacij med njihovo obdelavo, hranjenjem in prenosom v komunikacijskih, informacijskih ali drugih elektronskih sistemih pred nepooblaščenim razkritjem, spreminjanjem ali uničenjem informacij, kakor tudi zaščite celovitosti in razpoložljivosti komunikacijskega in informacijskega sistema kot celote« (Korošec 2012: predavanja VED).

INFOSEC področje zajema COMSEC, COMPUSEC in TRANSEC. Uporabljamo le odobreno programsko in strojno opremo. Na delovnih postajah in strežnikih morajo biti nameščeni protivirusni programi, uporabljati je potrebno ustrezne požarne pregrade, proxi strežnike itd. Poskrbimo, da so vse zadeve v sistemih sledljive. Uporabnikom omejimo dostop do nameščanja programske opreme in ostalih nastavitev v sistemu, ki so v domeni sistemskih administratorjev. Razvijemo politiko gesel, da preprečimo nepooblaščen dostop v sistem, omejimo tiskanje in kopiranje datotek na diskete ter prenašanje podatkov na USB ključke, itd.

INFOSEC opredeljuje minimalne standarde varovanja zaupnih informacij, spremljajočih sistemskih storitev in resursov na področju komunikacijskih, informacijskih in drugih elektronskih sistemov, ki hranijo, obdelujejo ali pošiljajo zaupne podatke.

Ukrepe moramo upoštevati celoten življenjski cikel. Pomembno je, da stalno zagotavljamo zaupnost informacij, celovitost in razpoložljivost informacij.

Na tem mestu velja omeniti tudi industrijsko varnost, kjer s partnerji pogodbeno rešujemo vprašanje posredovanja podatkov tretjim organizacijam, kjer opredelimo, da se poslovni podatki ne smejo posredovati tretji organizaciji brez našega soglasja.

Varno E-poslovanje zagotovimo z zavarovanjem prostorov, ustreznim motiviranjem in ozaveščanjem zaposlenih. Svojo informacijsko, komunikacijsko in programsko opremo redno posodabljamo.

KIS opremo, ki je namenjena za iznos iz varnostnega območja, mora glavni varnostni častnik pregledati in potrditi iznos. Vse tajne informacije in komponente morajo biti pravilno deklasificirane oziroma odstranjene. Enako velja kadar je potrebno vrniti opremo proizvajalcu na popravilo.

Skladno z zahtevami za razpoložljivost sistema se vse lokacije opremijo z UPS oziroma drugimi potrebnimi napravami, ki zagotavljajo neprekinjeno delovanje sistemov.

Vse navedeno predstavlja varnostno politiko in je osnova za varnost naših podatkov pred tretjimi osebami.

Uvajanje in uporabo programske in komunikacijske opreme v MORS in SV opredeljuje 8. člen Pravilnika o varovanju komunikacijskega in informacijskega sistema MORS.
»Organizacijska enota, pristojna za informatiko in komunikacije (SIK) izdela minimalne skupne kriterije, ki jih morajo pri nabavi in uvajanju nove opreme upoštevati NOE in organi v sestavi.

Uvajanje v uporabo nove strojne, programske in komunikacijske opreme, ki je sestavni del oborožitvenih in zajemajo prenos podatkov, mora odobriti organ za varnostno odobritev sistema na predlog SIK.

Uporaba strojne programske in komunikacijske opreme, ki ne ustreza predpisanim minimalnim kriterijem, v KIS MO ni dovoljena. Uporaba testne opreme brez predhodne pisne odobritve pooblaščene osebe za varnost v KIS MO, ni dovoljena.

Izjemoma je brez posebne odobritve dovoljena uporaba programske opreme, ki je:

- sestavni del elektronskih knjig (elektronski imeniki, telefonski imeniki, enciklopedije, slovarji, časopisi, katalogi, učbeniki itd.);
- sestavni del kompleta oborožitve, vojaške opreme, specialne operativne tehnike, merilne tehnike, računalniške strojne opreme in ni povezana v enoten in avtonomen KIS MO.

3.4.2 Analiza in ocena groženj

Iz dneva v dan se srečujemo z vse večjo uporabo socialnih omrežij. Vse več uporabnikov sodeluje na Facebooku, Twiterju, itd. Nihče pa se ne vpraša, zakaj so vzpostavljena tovrstna omrežja in kdo stoji za njimi. Dejstvo je, da je preko 90 % strežnikov teh omrežij v ZDA. Med tem ko države zaostrujejo politiko na področju varstva osebnih podatkov, večina uporabnikov prostovoljno objavlja v socialnih omrežjih ogromne količine slikovnega in tekstovnega materiala. Socialna omrežja so zato odličen poligon za obveščevalne službe in vse ostale, ki iščejo podatke o določenih osebah.

Po ocenah Cisco Systems je globalno cyber kriminal že prehitel svetovno trgovino z drogami in fizični kriminal. Danes je eden od najvažnejših trendov vse večja kompleksnost napadov na informacijske sisteme. Zato je potrebno zaščititi celoten informacijski sistem in ne le klasična področja – dostop do interneta, prenosnih računalnikov in mobilnih naprav.

»RAND [(Research And Development) je neprofiten globalni miselni trust (think tank), ustanovljen kot pomoč pri raziskovanju in analiziranju za potrebe oboroženih sil ZDA (http://www.rand.org/, 20. 5. 2011). RAND izpostavlja tri ključne skupine varnostnih groženj informacijskim sistemom. Fizične, elektronske in psihološke. Opazimo lahko, da ima danes

posameznik zaradi uporabe modernih tehnologij možnost vplivanja na stabilnost informacijskih in komunikacijskih sistemov prek vseh treh oblik groženj, kar je za nekaj desetletij nazaj bilo povsem nepredstavljivo« (Dokl 2012: 28).

Z objavo množice depeš ameriškega zunanjega ministrstva je posameznik zatresel legitimnost velesile ZDA in celoten mednarodni ustroj. Na tak način lahko posameznik s spretno uporabo informacijske tehnologije predstavlja resno varnostno grožnjo različnim institucijam in omrežjem.

Poleg informacijske in omrežne varnosti je izrednega pomena tudi zasebnost v virtualnem prostoru. Zaradi brezmejne narave in lastnosti interneta je najprej veljal kot precej odporen proti nadzorovanju z različnih ravni, predvsem zaradi svoje velikosti. Delno se zasebnost izgublja zavestno pri uporabi socialnih omrežij, pomembno pa je zmanjšanje zasebnosti zaradi povečanega nadzora zaradi preprečitve kaznivih dejanj.

Potencialne grožnje za ključno infrastrukturo, ki se lahko uniči ali poškoduje, predstavljajo teroristični napadi, naravne nesreče, malomarnost, nesreča ali vdor hekerjev, kriminalna dejavnost in zlonamerno vedenje.

»Splošno ogroženost lahko ocenimo v okviru globalnega varnostnega okolja, v katerem se pojavlja cyber-terorizem kot vrsta terorizma, ki vključuje računalnike, omrežja in informacije ki jih vsebujejo. Zaradi vse večje povezanosti posameznikov, družbe in raznih organizacij v računalniška omrežja se pričakuje vse več napadov cyber - teroristov in vse večjo škodo, ki naj bi prerasla običajne oblike terorizma« (Weimann 2006:148).

»Nacionalni preiskovalni svet ZDA trdi, da bodo jutrišnji teroristi zmožni narediti s tipkovnico več škode kot z bombami« (Weimann 2006:147).

V raziskave za varno uporabo interneta so bila vložena ogromna sredstva. Kljub temu nihče ne zagotavlja varne uporabe, če se ne držite določenih pravil. Zato je potrebno, da vsak uporabnik, ki želi resno poslovati preko spleta upošteva določeno varnostno politiko, ki je osnova, da zaznamo napade in preprečimo poškodovanje našega elektronskega sistema. S tem preprečimo nastanek škode, začasnega izpada sistema itd.

3.4.2.1 Ocena ogroženosti informacijskega sistema

Najuspešnejši so tisti kibernetski napadi, ki so izredno intenzivni in trajajo kratek čas, primer je kibernetski napad na Estonijo leta 2006, kjer je bila država praktično ohromljena. Padel jim je bančni promet, internetne komunikacijske poti so zabeležile 400 krat večji promet od običajnega.. Zavedati pa se moramo, da je bila tedaj Estonija ena naprednejših uporabnic spleta tudi kot država in je svojim državljanom že tedaj omogočala elektronsko poslovanje z državno upravo. Prišlo je do ohromitve elektronskega poslovanja (Tikk 2008).

Daljše trajanje napada zaradi aktivne obrambe in krpanja varnostnih lukenj ima tako manj možnosti za uspeh kot kratki dobro načrtovani napadi. Prav tako ponovljeni napadi istega tipa nikakor ne dosegajo istih učinkov kot ob prvem napadu.

»Napake sistemskih administratorjev oziroma neaktivnost sistemskih administratorjev ima ključen vpliv na varnost, saj z omejenim izborom znanj in orodij za preprečevanje napadov napadalec pridobiva tehnološko prednost« (Dokl 2012: 70).

V več izvedenih študijah je bilo ugotovljeno, da se največji procent napadov na informacijske sisteme (IS) izvede znotraj same organizacije, da pa ne moremo izključiti možnost napadov od zunaj, predvsem na IS, ki so povezani v javna omrežja.

V informacijskem sistemu, ki ni ustrezno nadzorovan, je tudi uvedba najmodernejših tehnično tehnoloških rešitev brez pravega pomena, kar pomeni, da je potrebno zagotoviti tudi ustrezno kadrovsko strukturo, ki bo izvajala aktivnosti varovanja IS.

Oceno ogroženosti informacijskega sistema MORS lahko ocenimo poleg globalnega tudi skozi lokalno varnostno okolje. Lokalno varnostno okolje predstavljajo lokacije MORS, na katerih se nahajajo elementi IS, vključno z elementi javnega komunikacijskega omrežja in infrastrukture, ki se uporablja za potrebe MORS ter vsi zaposleni na MORS, zunanji dobavitelji opreme in storitev ter izvajalci. Znano je, da še tako dobri organizacijski in tehnično tehnološki ukrepi ne zagotavljajo 100 % varnosti.

3.4.2.2 ANALIZA TVEGANJA

Za vsak informacijski sistem je potrebno izdelati analizo tveganja, ki je študija ranljivosti, groženj, verjetnosti izgube ali zmanjšanja učinkovitosti varnostnih ukrepov. Te študije praviloma delamo varnostni častniki.

S pripravo analize tveganj pomagamo vodstvenim delavcem razumeti za kakšna tveganja gre, kateri tipi groženj nas ogrožajo, kaj se lahko zgodi in kakšne posledice lahko pričakujemo ter kaj lahko naredimo, da zmanjšamo tveganje.

Prednost tovrstne analize je, da vodilni sprejemajo odločitve na osnovi informiranja o grožnjah, s tem lahko opravičijo proračunska sredstva, ker so grožnje objektivno ocenjene.

Pri analiziranju tveganj uporabljamo kvalitativni in kvantitativni pristop k poročanju rezultatov. Po sprejetju protiukrepov naredimo analizo efekta ukrepov in po potrebi spremenimo prepoznano ranljivost KIS.

Pri kvantitativnem pristopu se osredotočamo na merjenje analize stroškov priporočenih ukrepov.

Pri kvalitativnem pristopu določamo relativno razvrščanje tveganj in prepoznavamo neposredna področja za izboljšave. Pri tem načinu je otežena ocena stroškov protiukrepov.
Pri varnostnih principih analiziranja tveganj se osredotočamo na možno izgubo tajnosti, celovitosti in razpoložljivosti sistema.

Ključno je, da se zavedamo kdo so tarče. Gre za posameznika, poslovni subjekt ali državni organ? Skladno s posledicami, ki jih lahko napad povzroči lahko gre za nepooblaščen dostop, izgubo možnosti uporabe neke storitve, krajo podatkov ali poškodovanje oziroma uničenje podatkov. Pri cenitvah upoštevamo verjetnost in pogostost napada ter možnost nastale škode.

4 OMREŽJA MORS

4.1 OMREŽJE INTRANET MO/SV

Omrežje INTRANET MO/SV je v celoti v lasti in upravljanju MO in SV. V njem se izvaja večina vseh poslovnih procesov ter procesov vodenja in poveljevanja. Zaradi enostavnejšega zagotavljanja komunikacijsko informacijske varnosti to omrežje ni povezano z drugimi omrežji oziroma drugimi KIS.

V času načrtovanja, razvoja in izgradnje tega omrežja Republiki Sloveniji niso bili na razpolago varnostni standardi zavezništva za varovanje tajnih podatkov. Tudi ustrezna (certificirana) oprema za izgradnjo tajnih omrežij za Slovenijo ni bila dobavljiva. Ne glede na vse omejitve je MO skupaj s SV zgradilo omrežje, ki izpolnjuje varnostne zahteve za obravnavo podatkov stopnje tajnosti INTERNO. Omrežje ima varnostno dovoljenje za delovanje (varnostna akreditacija) za to stopnjo tajnosti.

Pomnilniški mediji, ki se uporabljajo za shranjevanje tajnih informacij, morajo obdržati največjo stopnjo tajnosti za katero so bili uporabljeni, dokler informacijam, ki so na njih pravilno znižana ali razveljavljena stopnja tajnosti, ali je medij deklasificiran in uničen skladno s predpisanim postopkom.

Sama ključna infrastruktura se stalno nadgrajuje. Večji del omrežja ima zagotovljeno neprekinjenost delovanja. Vsi ključni strežniki in ključne delovne postaje so priklopljene na UPS napajanje tako, da so storitve in aplikacije uporabnikom stalno na voljo. Komunikacije potekajo po optičnih povezavah. Izven administrativnih območij poteka komunikacija v šifrirani obliki po najetih vodih.

Za omrežje so izdelani varnostno operativni postopki, kjer so upoštevane vse varnostne zahteve varnostne politike in so z njimi seznanjeni vsi uporabniki. Upraljalec sistema je sektor za informatiko in komunikacije MORS (SIK).

4.2 JAVNO RAČUNALNIŠKO OMREŽJE MO/SV (PUB MO/SV, TUDI INTERNET MO/SV)

V MORS je bila sprejeta določitev, da se interno omrežje INTRANET ne poveže z internetom, ker glede na zmanjševanje virov nimamo potrebnih zmogljivosti za potrebno izvajanje nadzora in reagiranje. Da uporabnikom zagotovimo potrebno varnost na internetu je postavljeno ločeno omrežje PUB, kjer uporabnikom preko ene vstopne točke zagotavljamo dokaj varen način dostopa na splet. Sicer je nekaj negodovanja zaradi manjših hitrosti prenosa podatkov na račun varnosti.

Tudi to omrežje je v celoti v lasti in upravljanju MO in SV. Uporablja se za dostop do svetovnega spleta in njegovih storitev ter izmenjavo sporočil brez stopnje tajnosti. Preko proxi strežnika se zagotavlja ustrezen nadzor, ki preprečuje napade direktno na uporabnike. Komunikacije v upravnih območjih potekajo po optičnih povezavah. Med vojašnicami pa v zaščiteni obliki po najetih vodih.

Z vidika podpore poslovnim procesom MO in SV čedalje bolj prihaja do izraza težnja uporabnikov in posameznih vsebinskih nosilcev po povezavi zasebnega omrežja MO/SV (INTRANET) z računalniškim omrežjem ostalih državnih organov in javnim računalniškim omrežjem (INTERNET).

4.3 RAČUNALNIŠKO OMREŽJE OSTALIH DRŽAVNIH ORGANOV

To omrežje se uporablja za dostop do storitev državne uprave. Na omrežju je dovoljeno obdelovati tudi podatke INTERNO. Omrežje upravlja Ministrstvo za javno upravo in je tudi v njegovi pretežni lasti.

Znotraj MO/SV ni povezano z nobenim javnim ali zasebnim računalniškim omrežjem MORS.

5 POVEZOVANJE OMREŽIJ

Pri povezovanju omrežij moramo zagotoviti večplastno varovanje. Računalniško okolje mora zagotavljati zaščito vseh ravni omrežja, tako delovnih postaj, strežnikov kot tudi prehodov med omrežji. Prehod med dvema omrežjema imenujemo vrata (gateway).

Prehodi oziroma vrata so vhodno izhodne točke v omrežje. Vsako tovrstno povezovanje sistemov zahteva strog nadzor in upoštevanje varnostne politike.

Strežniki so računalniki v skupni rabi, ki izvajajo različne funkcije. Shranjujejo datoteke in izvajajo različne aplikacije, ki so na voljo vsem uporabnikom omrežja. Običajno jih namestimo v varovane prostore in jih nadziramo.

»Z ločitvijo računalniškega okolja si olajšamo izoliranje omejenih in kritičnih sistemov« (Egan 2005:31).

Za dosego akreditacije povezovanja med internetnim in internim omrežjem je potrebna vzpostavitev fizične, personalne, informacijske in dokumentacijske varnosti pri čemer so bistvenega pomena naslednje aktivnosti:

- vzpostavitev varnostnih območij,
- izdelava potrebnih formacij,
- postavitev usposobljenega kadra na ustrezna formacijska mesta,
- izdelava varnostnega načrta in VarOP (varnostnih operativnih postopkov).

Danes si več ne moremo predstavljati sistema brez ustrezne protivirusne zaščite na vseh ravneh, ker število napadov vztrajno narašča. Zato je ključno upravljanje in odstranjevanje pomanjkljivosti ter zaznavanje vdorov. Za zaznavanje vdorov uporabljamo posebna orodja, ki ves čas spremljajo promet. Tu se nam največkrat pojavi težava z zmogljivostjo, ker se zmogljivost omrežij stalno povečuje.

6 ZAKLJUČEK

Svetovni splet je iz dneva v dan bolj razširjen. Z razvojem je prišlo do enormnega povečanja števila uporabnikov in razširitve na cel svet. Pri brezmejnosti in tako velikem številu uporabnikov je učinkovit nadzor praktično nemogoč.

Glede na razširjenost spleta se nam potrdi prva hipoteza. Kibernetsko okolje nam dejansko omogoča povezljivost in dosegljivost od koderkoli.

V drugi hipotezi trdimo, da povečane možnosti prenosa podatkov in uporabnost omrežij prav tako vplivata na razvoj in odvisnost od informacijske tehnike. Tudi ta hipoteza se skozi nalogo potrdi. Praktično nobena organizacija več ne more konkurenčno delovati brez informacijsko komunikacijske tehnologije. Potrebno je imeti mobilni telefon, računalnik, organizacija mora imeti na spletu svojo stran. Komuniciranje s komerkoli na svetu je možno v realnem času ne kot nekdaj, ko si ga težko dobil po telefonu oziroma je pošta potovala lahko tudi mesec dni in več.

V tretji hipotezi sem trdil, da kibernetski napadi na povezan informacijski sistem lahko povzročijo takšno škodo, kot nekdaj konvencionalna vojna. Tudi ta hipoteza se potrjuje. Že če pogledamo kibernetski napad na Estonijo 2006. Padel jim je bančni promet, internetne komunikacijske poti pa so zabeležile 400 krat večji promet od običajnega. Vse komunikacijske poti so bile praktično prekinjene ali preobremenjene. Zavedati pa se moramo, da je bila tedaj Estonija ena naprednejših uporabnic spleta. Kot država je svojim državljanom že tedaj omogočala elektronsko poslovanje z državno upravo.

Trenutno se Slovenija ne srečuje zgolj s problematiko neustrezne tehnične zaščite in nerazumevanja problematike, temveč jo tako kot ostale države po svetu pesti težava neustrezne pravne ureditve. Trenutna zakonska ureditev namreč onemogoča odkrivanje in preiskovanje informacijskih zlorab.

Varnost omrežij je ključna za delovanje informacijskih sistemov. Najpomembnejša je varnost ključne informacijske infrastrukture.

Skozi nalogo sem analiziral tudi informacijsko komunikacijske sisteme MORS in SV. Predvsem gre tu za notranje omrežje Intranet in internetno omrežje PUB MORS, ki nista povezana. Glede na to, da v intranetnem omrežju poteka vsa službena korespondenca z izjemo obdelave, pošiljanja in hranjenja tajnih podatkov stopnje ZAUPNO in višje ocenjujem, da je trenutna rešitev glede na večje število lokacij, kjer sta omrežji nameščeni boljša, kot če bi omrežji povezali in nato nadzirali promet.

Poznamo primer vdora hrvaških hekerjev v Pentagon, prav tako imajo težave druge države, ki imajo interna omrežja povezana z internetom.

V MORS je bila sprejeta odločitev, da nam trenutna tehnološka opremljenost, kot tudi razpoložljivi človeški viri, ne zagotavljajo zadostne garancije, da v primeru povezave intraneta z internetnim omrežjem ne bi prišlo do vdora v omrežje in do kraje podatkov. Dokler sta omrežji ločeni lahko do podatkov pride le nekdo od znotraj. Napade od znotraj v večini primerov rešujemo z vsakoletnim varnostnim osveščanjem v okviru usposabljanja za dostop do tajnih podatkov ter z preventivnim varnostnim osveščanjem vseh uporabnikov. V okviru storitvenega centra v 11. bataljonu za zveze pa tudi izvajamo nadzor na delom omrežja, ki ga upravlja SV, medtem, ko celotni omrežji upravlja in nadzira SIK.

Glede na domačo in tujo prakso je povezovanje omrežja, ki obdeluje tajne podatke stopnje tajnosti INTERNO možno povezati v združeno omrežje. Vsekakor lahko tovrstna povezava lahko poteka le preko enih vrat (gateway), kjer izvajamo nadzor prometa. Vendar potrebujemo za tovrsten nadzor izurjene in izkušene sistemske administratorje, ki bodo sposobni odkriti napadalce in jih onemogočiti. Zveza NATO je financirala vrsto raziskav na tematiko povezovanja omrežij različnih stopenj in ima definirano politiko povezovanja, vendar tudi njihovi strokovnjaki trdijo, da je z varnostnega stališča bolje, da so omrežja ločena, ker s tem je tveganje izgube podatkov zmanjšano.

V kolikor nimamo razpoložljivih človeških virov za nadzor vrat med omrežjema oziroma nimamo ustrezne tehnične opreme je bolje, da sistemov ne povežemo in delamo kot sedaj – ločeno internetno in intranetno omrežje.

7 LITERATURA

1. CARR, Nicholas (2011). Plitvine: kako internet spereminja naš način razmišljanja, branja in pomljenja. Ljubljana: Cankarjeva založba

2. DOKL, Jure (2012). Kibernetska varnost omrežij. Ljubljana: Fakulteta za družbene vede

3. EGAN, Mark (2005). Varnost informacij: grožnje, izzivi in rešitve: vodnik za podjetja. Ljubljana: Pasadena

4. KOVAČ, Mojca (2010). Obravnavanje nacionalnih tajnih podatkov v informacijsko – komunikacijskem sistemu. Ljubljana: Fakulteta za družbene vede

5. WEIMANN, Gabriel (2006). Terror on the Internet: the new arena, the new challenges. Washington, DC: United states institute of Peace

VIRI

1. Allen, J. (June 2005) Governing for Enterprice Security, Networked Systems Survivability Program, Carnegie Mellon University

3. Guidelines on Physical Security, AC/35-D/1030

2. Security Within the North Atlantic Treaty Organisation (NATO), C-M(2002)49

4. TIKK, Eneken (2008). The Estonian Case, Ankara: Cyber Terrorism Course

5. Ob 20 letnici Interneta v Sloveniji: Kratka zgodovina interneta: www.isoc-drustvo.si/. (10. 5. 2012)

6. RAND [(Research And Development): http://www.rand.org/, (20. 5. 2011)

SEZNAM UPORABLJENIH KRATIC

ARPA - Advanced Research Projects Agency = Agencija za napredne raziskovalne projekte
ARPANET- omrežje Agencije za napredne raziskovalne projekte

CERN – European Organization for Nuclear Research
CIDR – Classless Inter-Domain Routing
CIS - Communications and Informations Sistems
COMPUSEC – računalniška varnost
COMSEC – varnost komunikacij
CSNET – omrežje v katero so bili povezani prvi računalniki
EASYnet – evropsko raziskovalno omrežje
EU – Evropska unija
IETF - Internet Engineering Task Force
INFOSEC – informacijska in komunikacijska varnost
IS – informacijski sistem
IS MORS/SV - informacijski sistem Ministrstva za obrambo oziroma Slovenske vojske
KIS SV/MORS – komunikacijsko informacijski sistem Slovenske vojske / Ministrstva za obrambo Republike Slovenije
MILNET – prvo vojaško internetno omrežje v oboroženih silah ZDA
MO - ministrstvo za obrambo
MORS – Ministrstvo za obrambo Republike Slovenije
NATO - North Atlantic Treaty Organisation
NIKHEF – National Institute for Nucklear and High energy physics
NSF – National Science Foundation
NSFNET – Omrežje National Science Foundation
NREN, National Research and Educational Network
PGP (Preety Good Privacy) – eden od programov za izdelavo varne pošte
PUB – internetno omrežje
RFID – radiofrekvenčna identifikacija
SIK – Sektor za informatiko in komunikacije
SV – Slovenska vojska
TRANSEC – varnost prenosa informacij
UUCP - Unix-to-Unix Copy
VarOP - varnostni operativni postopki
ZDA - Združene države Amerike

IZJAVA O AVTORSTVU

PRILOGA 6

IZJAVA O AVTORSTVU ZAKLJUČNE NALOGE

Kandidat (ka) / Slušatelj (ica) (čin ime in priimek) nadporočnik Anton Ajster izjavljam, da sem avtor/ica zaključne naloge z naslovom Svetovni splet in kibernetske grožnje kot izziv informacijski varnosti v SV, ki sem jo napisal/a pod mentorstvom stotnika Boruta Korošča.

S svojim podpisom zagotavljam da:

- je zaključna naloga izključno rezultat mojega lastnega dela,
- so vsa dela in mnenja drugih avtorjev, ki jih uporabljam v zaključni nalogi, navedena oziroma citirana v skladu s SOP ŠČ za izdelavo in oblikovanje zaključne naloge na ŠČ,
- se zavedam, da je plagiatorstvo kaznivo po Zakon-u o avtorskih in sorodnih pravicah, (uradno prečiščeno besedilo – ZASP UPB3, Uradni list RS, št. 16/2007, z dne 23. 2. 2007), prekršek pa podleže tudi ukrepom disciplinske odgovornosti v skladu z Zakonom o obrambi in Pravili službe v Slovenski vojski,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo zaključno nalogo in moj status v Slovenski vojski.

S podpisom se odrekam vsem materialnim pravicam v zvezi z zaključno nalogo in dovoljujem uporabo zaključne naloge v študijske namene.

V Mariboru, dne 24. 5. 2012 Podpis: