

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Matevž Oset

Kibernetsko ogrožanje slovenske energetske kritične infrastrukture

Magistrsko delo

Ljubljana, 2015

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Matevž Oset

Mentor: izr. prof. dr. Uroš Svete

Kibernetsko ogrožanje slovenske energetske kritične infrastrukture

Magistrsko delo

Ljubljana, 2015

Kibernetско ogrožanje slovenske energetske kritične infrastrukture

Infrastrukturno okolje, ki se vse bolj informatizira in povezuje, to zahteva tudi od organizacij, ki izvajajo dejavnost proizvodnje, prenosa in distribucije energije. Za te organizacije ta proces predstavlja velik varnostni izziv. V medmrežje morajo namreč vse bolj odpirati nadzorne in krmilne sisteme, ki so bili zasnovani v obdobju, ko informacijska varnost ni bila pomembna in nimajo nujno vpeljanih ustreznih varnostnih mehanizmov. Upravitelji teh sistemov se tako srečujejo s tehtanjem med učinkovitim delovanjem in varnostjo in pogosto prevlada prva zahteva. Tako organizacije ogrožajo standardni viri ogrožanja in vektorji napadov, prav tako pa tudi specifični, kot je nazorno pokazal zlovešč napad Stuxnet v letu 2010. Delo predstavlja poskus celovitega pregleda konceptov, sistemov in dobre prakse varovanja informacij na področju kritične infrastrukture. Pri tem je poudarek na kibernetiski varnosti industrijskih nadzornih sistemov, vrstah napadov, metodah za oceno varnosti in za njeno izboljšanje ter poskusu izdelave analitičnega orodja, s katerim lahko izvajalec analize oceni informacijsko-varnostno stanje štirih relevantnih področij: procesov, tehničnih sistemov, kadrovskih virov in sistemov za krmiljenje in nadzor ter s tem ugotovi celovito nominalno stanje kibernetiske varnosti organizacije, vključno z nadzornim sistemom. Orodje, ki nominalno varnost informacijskega sistema izrazi z določenim indeksom, v delu apliciramo na dveh organizacijah, nato pa izvedemo priporočila za izboljšanje informacijske varnosti v organizaciji. Aplikacija orodja prikaže izrazito različne rezultate, zato bi bilo delo smiselno nadaljevati ter s pomočjo tega orodja ugotoviti, kakšna je nominalna ogroženost slovenske energetske kritične infrastrukture, nato pa izvesti še presojo z drugimi orodji in metodami, s katerimi bi lahko izvedli analizo vrzeli med nominalnim in dejanskim varnostnim stanjem.

Ključne besede: Kibernetiske grožnje, informacijska varnost, industrijski nadzorni sistemi (ICS, SCADA), kritična infrastruktura.

Cybernetic threats to slovenian energy critical infrastructure

Infrastructure environment, which is ever more computerized and interconnected, demands the same to be done by organizations that deal with production, transport and distribution of energy. That process presents a significant security challenge for those organizations as they must open up their control systems, which were designed in a time when information security was not important, to the internet and which do not necessarily have proper security mechanisms in place. Systems administrators must therefore weigh the demands for efficiency and security and often the former prevail. These organizations are thus threatened by conventional as well as specific threats and vectors of attack as the now infamous Stuxnet attack has clearly demonstrated. This thesis represents an attempt at a comprehensive overview of concepts, systems and best practices of information security in the field of critical infrastructure with emphasis on cybernetic security of industrial control systems as well as an attempt to produce a nominal information security analytic tool with which a conductor of analysis may assess information security of four relevant aspects: processes, technical systems, human resources and supervision and control systems, and thus determine a holistic nominal state of cyber security of an organization, including its control systems. The tool, which expresses nominal information security of an organization with a defined index, is also applied to two organizations, followed by recommendations for improvement of information security therein. Application of the tool produces significantly different results, therefore it would be reasonable to continue research into to what extent the Slovenian energy critical infrastructure is actually threatened using this tool, followed by an analysis with other tools and methods, with which we could carry out a gap assessment between nominal and actual state of security.

Keywords: **Cybernetic threats, information security, industrial control systems (ICS, SCADA), critical infrastructure.**

Vsebina

1	Uvod z utemeljitvijo relevantnosti	9
2	Metodološko-hipotetični okvir	12
2.1	Predmet preučevanja, namen in cilji	12
2.2	Hipoteze	12
2.3	Uporabljena metodologija	13
2.4	Struktura dela	15
3	Konceptualno-teoretični okvir	17
3.1	Kibernetika in kibernetski prostor	17
3.2	Splošna varnost, informacijska varnost, energetska varnost	18
3.3	Kritična infrastruktura	24
3.4	Viri ogrožanja kritične infrastrukture ter informacijski viri ogrožanja.	28
3.5	Sistemi za upravljanje elektroenergetske kritične infrastrukture	28
3.6	Družbeni vidiki informacijske varnosti ter vrste napadov, usmerjene v uporabnike	36
3.7	Nekateri znani napadi na energetske ključno infrastrukturo	39
3.8	Zlonamerna programska koda in kibernetski viri ogrožanja elektroenergetske kritične infrastrukture	42
3.9	Vektorji in vrste napadov	50
3.10	Tehnični sistemi za izboljšanje informacijske varnosti	53
3.11	Organizacijske rešitve varovanja kritične infrastrukture	59
3.12	Standardi in priporočila na področju varovanja informacij in SCADA	61
4	Razvoj orodja in aplikacija orodja	68
4.1	Pregled obstoječih orodij in metod	68
4.2	Načela razvoja analitičnega orodja	74
4.3	Sestava in delovanje orodja	76
4.4	Primeri aplikacije orodja	78
4.5	Interpretacija rezultatov in priporočila	80
5	Razprava in zaključek	85
5.1	Razprava	85
5.2	Potrditev hipotez	88
5.3	Priporočila za nadaljnje raziskovanje	89
6	Literatura	91

Priloge	103
Priloga A: Vprašalnik	103
Priloga B: Primer opredeljenega varnostnega območja po ANSI/ISA-99 (Byres 2010).	110
Priloga C: Ocenjevalni list za tveganje informacijskega sredstva orodja OCTAVE (Caralli in drugi 2007: 127).	111
Priloga Č: Primer lista s kalkulacijo indeksa RAV za informacijski sistem (ISECOM 2010: 69).	112

Seznam kratic

- CCTA: Centralna agencija Velike Britanije za komunikacije in telekomunikacije (Central Communication and Telecommunication Agency).
- CIA: zaupnost, celovitost, dostopnost (Confidentiality, Integrity, Availability);
- CRAMM: Metoda analize in upravljanja tveganj CCTA (CCTA Risk Analysis and Management Method)
- DMZ. Demilitarizirano območje (Demilitarized Zone)
- DDoS: Distribuirana zavrnitev storitve (Distributed Denial of Service)
- DoS: Zavrnitev storitve (Denial of Service)
- ENISA: Agencija Evropske unije za mrežno in informacijsko varnost (European Union Agency for Network and Information Security).
- HMI: vmesnik med človekom in napravo (Human-Machine Interface)
- IAEA: Mednarodna agencija za jedrsko energijo (International Atomic Energy Agency).
- ICS: industrijski nadzorni sistem (Industrial Control System); SCADA je podzvrst ICS.
- IDS: Sistem za zaznavanje vdora (Intrusion Detection System)
- IKT: Informacijsko-komunikacijska tehnologija
- IPS: Sistem za preprečevanje vdora (Intrusion Prevention System)
- ISA: Mednarodno združenje za avtomatizacijo (The international Society of Automation)
- ISACA: Združenje za nadzor in presojo informacijskih sistemov (Information Systems Audit and Control Association)
- LAN: lokalno omrežje (Local Area Network)
- NCCIC: Ameriški narodni center za integracijo nacionalne kibernetске varnosti in komunikacij (National Cybersecurity and Communications Integration Center)
- NSA IAM: Metodologija presoje varnosti informacijskih sistemov organizacije NSA (NSA INFOSEC Assessment Methodology)
- NSA IEM: Metodologija ocene varnosti informacijskih sistemov organizacije NSA (NSA INFOSEC Evaluation Methodology)
- NERC: Severnoameriška korporacija za zanesljivost elektrike (North American Electric Reliability Corporation)

- NIST: Ameriški nacionalni inštitut za standarde in tehnologijo (National Institute of Standards and Technology).
- OCTAVE: metoda ocenjevanja operativno kritičnih groženj, sredstev in ranljivosti (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- PKI: javna infrastruktura ključev (Public Key Infrastructure)
- PLC: Programabilni logični nadzornik (Programmable logical controller)
- RAM: Bralno-pisalni pomnilnik (Random Access Memory)
- RTU: oddaljena terminalska enota (Remote Terminal Unit)
- SCADA: Sistem za nadzor in pridobivanje podatkov (Supervisory Control And Data Acquisition)
- SMTP: Preprosti protokol za prenos pošte (Simple Mail Transfer Protocol)
- SNMP: Preprosti protokol za upravljanje omrežja (Simple Network Management Protocol)
- UPnP: Univerzalni sistem priključi in igray (Universal Plug and Play)
- VPN: Navidezno zasebno omrežje (Virtual Private Network)
- WAN: prostrano omrežje (Wide Area Network)
- WHQL: laboratorijsko testiranje kakovosti gonilnikov strojne opreme v sistemu Windows (Windows Hardware Quality Laboratory testing)

1 Uvod z utemeljitvijo relevantnosti

Junija 2010 so različni mediji po svetu začeli poročati o črvu, ki je prizadel iranske organizacije, ki se ukvarjajo z bogatenjem urana. Bolj podroben pregled pove, da je šlo za usmerjen napad s črvom, ki vsebuje rootkit, namenjen logičnim kontrolerjem v sistemih SCADA nemškega proizvajalca Siemens AG. Črv se je širil prek operacijskih sistemov Microsoft Windows, nato pa okužil logične kontrolerje na aplikacijski plasti modela OSI. Skoraj 60 % vseh okuženih sistemov je bilo v Iranu (McMillan 2010).

Kot se je izkazalo, ni bilo naključje, da je napad prizadel prav iranske sisteme. Ni znano, kakšno škodo je Stuxnet povzročil, znano pa je, da je bil napad pripravljen tako, da je bil usmerjen v iranske organizacije, ki so del državnega programa za bogatenje urana. Poročila IAEA kažejo, da so med koncem leta 2009 in začetkom leta 2010 v iranskem obratu za bogatenje urana Natanz zamenjali več kot 900 centrifug, čeprav za Iran velja mednarodna prepoved nakupa te vrste opreme (Albright in drugi 2011, 2–5). Virus naj bi bil namenjen širjenju zgolj po mreži Iranskih obratov za bogatenje urana, vendar pa se je zaradi dodatka, ki naj bi ga strokovnjaki izraelske enote 8200 vključil vanj, začel širiti tudi po drugih sistemih (Sanger 2012). Ocenjuje se, da je Stuxnet okužil skupaj več kot 100.000 računalniških sistemov (Zetter 2012).

Prav tako ni jasno, kakšen je izvor Stuxneta, vendar pa je verjetno, da so ga razvili s podporo ameriških in izraelskih vlad (prav tam).

Sodobno elektroenergetsko omrežje nadzirajo, upravljajo in z njimi komunicirajo sistemi, imenovani industrijski nadzorni sistemi SCADA. Takšni sistemi se uporabljajo že desetletja. V svoji osnovi niso bili zasnovani, da bi bili varni pred vdori z orodji IKT, zato je njihovo zavarovanje izredno težko, še posebej iz dveh razlogov. Prvi je, da jih izdelujejo različni proizvajalci, ki uporabljajo svoje protokole in specifikacije. Težava se sicer zmanjšuje z implementacijo odprtih protokolov. Druga težava je, da se za komunikacijo s sistemi SCADA vse manj uporabljajo zaprti sistemi¹ in vse bolj javno dostopna mreža, internet, saj to omogoča veliko znižanje stroškov upravljanja. Čeprav komunikacijski protokoli in podrobnosti o implementaciji sistema niso vedno

¹ Na primer samostojne optične mreže

javno dostopni in so zelo raznoliki, lahko posamezniki do takšnih podatkov pridejo s pasivnim zbiranjem (Team CYMRU 2009).

Takšno početje že dlje časa opaža tudi zasebna ekipa strokovnjakov za informacijsko varnost, ki se imenuje Ekipa Cymru; ta je vzpostavila svoje omrežje darknet, na katerem zapisuje aktivnosti. Omrežje darknet je del usmerjenega, dodeljenega prostora z naslovi IP, v katerem naj ne bi bilo nikakršnih storitev ali strežnikov, torej naj bi bil ta prostor prazen, črn. Kljub temu na nekaterih izmed teh območij obstajajo porti, ki naj bi bili vstopne točke v sisteme SCADA. Ves prihajajoči promet v ta prostor naj bi bil torej sumljiv, saj ne bi smelo biti vanj usmerjenega nič primernega vsakdanji rabi omrežja. Promet, ki prihaja v to omrežje, običajno ustvarjajo iskalni protokoli; te izvajajo programska orodja, ki iščejo ranljiva omrežna vrata. Skupina ugotavlja, da 90 % vsega prometa prihaja s kitajskih naslovov, dodatnih pet odstotkov pa še iz Tajvana (Team CYMRU 2009).

Energetska kritična infrastruktura, katere del je elektroenergetska infrastruktura, je med najpomembnejšimi. To potrjuje na primer študija Vladnega urada Združenega kraljestva². Analizirala je 11 infrastruktur, ki zagotavljajo 59 kritičnih procesov. Avtorji so ugotovili, da energetska infrastruktura zagotavlja 57 od teh 59 kritičnih procesov in da se ji po pomembnosti lahko približa le še telekomunikacijska infrastruktura (Lukasik in drugi 2003, 8). Kot eno izmed najbolj kritičnih elektroenergetsko infrastrukturo opredeljuje tudi Prezelj, ki jo po kritičnosti uvršča na peto mesto, za hrano, zdravili in laboratoriji ter bolnišnično in predbolnišnično nego (Prezelj 2009, 479). Medtem ko se zdi, da slovensko elektroenergetsko kritično infrastrukturo bistveno bolj kot kibernetski viri ogrožanja ogrožajo naravne in druge nesreče, kot je na primer žled, je vprašanje informacijske varnosti v takšnih organizacijah še vedno zelo pomembno; te namreč upravljajo svoje omrežje prek digitalnih informacijskih sistemov.

Napad, ki bi onemogočil elektroenergetsko kritično infrastrukturo, bi imel torej lahko zelo hude posledice za razvito družbo, kakršna je slovenska. Verjetno zelo ekstremna ponazoritev onemogočenja električne infrastrukture v družbi, ki se nanjo močno zanaša, je izpad prenosnega omrežja na severovzhodu ZDA in Kanade leta 2003. Izpad, ki je trajal manj kot 12 ur, je prizadel približno 55 milijonov ljudi.

² UK Cabinet Office

Povzročilo ga je več dejavnikov, predvsem povečana poraba, izpad ene od elektrarn in verižna preobremenitev prenosnega omrežja (New York Independent System operator 2008).

Izpad je onemogočil več sistemov kritične infrastrukture, med drugim dele vodnega omrežja, javnega transporta in telekomunikacij, zaustavljena je bil tudi proizvodnja v tovarnah. Ker so ljudje za zagotavljanje svetlobe začeli prižigati sveče, se je bistveno povečalo število požarov. Izpad, ki je kasneje dobil ime Severovzhodna zatemnitev leta 2003, pa je zahteval tudi nekaj smrtnih žrtev (Greeno 2003).

Pričujoče delo bo poskus ugotovitve mere realne nevarnosti, da bi prišlo do dejanskega napada na električno kritično infrastrukturo, tveganja, da v Sloveniji do takšnega napada pride, in ranljivosti slovenske elektroenergetske kritične infrastrukture.

2 Metodološko-hipotetični okvir

2.1 Predmet preučevanja, namen in cilji

Predmet preučevanja dela so koncepti, povezani s kibernetško varnostjo elektroenergetske kritične infrastrukture.

Namen dela je prispevek k razumevanju kibernetške varnosti slovenske elektroenergetske kritične infrastrukture.

Cilji so:

- opredelitev vseh s predmetom preučevanja povezanih konceptov in njihova povezava v koherenten teoretičen ovir;
- izdelava analitičnega orodja za nominalno ugotovitev kibernetške varnosti posameznih subjektov, ki delujejo v elektroenergetskem sektorju;
- evalvacijska analiza kot primer aplikacije tega orodja.

Organizacije, v katerih se bo izvedla analiza, morajo za dosego namenov dela zadostovati določenim pogojem:

- delovati morajo na področju Republike Slovenije (RS);
- kot primarno dejavnost morajo opravljati distribucijo, prenos ali proizvodnjo električne energije;
- upravljati ali soupravljati morajo sistem za nadzor in zbiranje telemetričnih podatkov (SCADA oz. ICS).

2.2 Hipoteze

Delovni hipotezi sta dve:

Hipoteza 1:

- kibernetške grožnje ne ogrožajo bistveno podjetij, v katerih se izvaja raziskava.

Ta hipoteza vsebuje implikacijo, da je slovenska ključna infrastruktura primerno zavarovana pred kibernetskimi grožnjami. Hipoteza bo predvidoma potrjena ali ovržena na podlagi določene ocene, ki bo izšla iz analize ogroženosti, pri čemer je

moj cilj, da bo ocena izražena z določenim številčnim indeksom. Po izdelavi orodja in indeksa, s katerim bom lahko meril ogroženost, bom postavil določeno mejo na indeksu, za katero bom lahko opredelil infrastrukturo za bistveno ogroženo, če bo vrednost mejo presegla, oziroma za nebistveno ogroženo, če vrednost meje ne bo presegla.

Hipoteza 2:

- družbeni vidiki kibernetских groženj v podjetjih, v katerih se izvaja raziskava, predstavljajo večji vir ogrožanja varnosti kot tehnični.

Poseben poudarek preučevanja bodo družbeni vidiki kibernetiske varnosti, torej takšni, ki izhajajo iz ali se nanašajo na zaposlene oziroma bivše zaposlene v upravljavcih te infrastrukture. Relevantna teorija kaže na to, da je t. i. najšibkejši člen v varnostnih sistemih človek (Janczewski in Colarik 2007, 173–228) in da večino napadov izvedejo posamezniki, ki delujejo znotraj organizacije, ki jo napadajo (Gundert 2009, 25–27).

Hipoteza bo sprejeta, če bo vrednost indeksa, ki se nanaša na družbeni vidik kibernetских groženj, nižja od povprečja preostalih indeksov.

2.3 Uporabljena metodologija

Temeljna metoda, ki jo bom uporabil za doseg namena tega dela, je evalvacijska analiza.

Evalvacija, poslovenjeno vrednotenje (Kustec Lipicer 2007, 24), je »posebna faza določenega procesa, ki se pojavlja ob koncu tega procesa in omogoča spoznati učinke, koristi, naravo, obseg, kvaliteto nekega posega ali določenih lastnosti, tudi dosežkov posameznikov in skupin« (prav tam).

Termin je torej zelo širok, v primeru tega dela pa ga bom omejil na vrednotenje določenih sistemov korporativne varnosti, predvsem sistemov varovanja informacij.

Z vrednotenjem na splošno odgovarjamo na naslednja vprašanja (Rossi in drugi 1999, 5–39):

- kakšna sta narava in obseg problemov;
- kje se problemi pojavljajo ter na koga in kako nanj vplivajo;

- kakšne so lastnosti problemov in njihovih učinkov, da želimo uvesti določene kontrole in ukrepe za njihovo premostitev;
- kateri so izvedljivi ukrepi, ki jih lahko uporabimo;
- katere so ustrezne ciljne skupine za te ukrepe;
- ali se ukrepi izvajajo ustrezno in ali so izvedeni vsi predvideni ukrepi;
- ali so ukrepi učinkoviti pri zasledovanju zastavljenih ciljev;
- ali so stroški, ki so s tem povezani, sprejemljivi glede na želene rezultate.

Vsa ta načela lahko uporabimo za vrednotenje sistemov korporativne informacijske varnosti, moramo pa seveda prilagoditi razumevanje konceptov, ciljev, problemov, ukrepov in metod za njihovo implementacijo, kar je razvidno v naslednjem poglavju.

Sledi opredelitev evalvacijske metodologije, skladno s klasifikacijo po Pattonu (Patton 1987, 45).

Metode, ki bodo uporabljene za preučevanje predmeta tega dela, so:

- primerjalna analiza,
- analiza primarnih in sekundarnih virov,
- izdelava analitičnega orodja,
- aplikacija analitičnega orodja na možnih deležnikih s pomočjo vodenega izpolnjevanja anketnega vprašalnika;
- interpretacija rezultatov in podajanje izhajajočih predlogov.

Osnovna enota evalvacijske analize je organizacija, opredeljena v poglavju 2.1.

Strategija vzorčenja temelji na avtorjevem predhodnem poznavanju predmeta preučevanja in na izboru osnovne enote preučevanja na podlagi poznanstev. Opredelitev preostalih mogočih enot preučevanja je nepotrebna, ker to ni skladno z namenom dela.

Pod pogojem, da zagotovim več kot eno sodelujočo organizacijo, bom med njunima rezultatoma evalvacijske analize izvedel tudi osnovno primerjavo.

Zbiral bom podatke, ki skupaj sestavijo oceno ustreznosti sistema korporativne varnosti in sistema varovanja informacij. Šlo bo za 100–150 specifičnih vprašanj, ki se nanašajo na omenjena sistema in so zbrana v vprašalniku. Podatke bom zbiral

tako, da bom vprašanja v osebni razgovor postavil pristojnim osebam in jih po potrebi pojasnil.

Kakovost in natančnost podatkov zagotavljam s predhodno temeljito izdelavo konceptualno-teoretičnega okvira, preciznostjo in načeli vprašalnika, opredeljenimi v poglavju 4.1. Subjekti zagotavljajo kakovost in natančnost s svojimi kompetencami in poznavanjem predmeta preučevanja.

Preverljivost in zanesljivost podatkov zagotavljajo reference, deponirane pri mentorju avtorja tega dela.

Po aplikaciji merskega orodja bodo rezultat analize priporočila, ki bodo izhajala iz vprašanj. Predlagal bom, da kontrole, ki jih lahko apliciramo na enoti analize, pa niso implementirane, v organizaciji vzpostavimo. Prav tako bom izpostavil, na katerem področju je izpolnjeno najmanj kontrol.

Posebno je treba izpostaviti izziv poslovenjenja pojmov, s katerimi se v delu srečujemo. Velika večina literature, iz katere sem črpal, je namreč v angleščini, prav tako se je angleščina vzpostavila v predmetu preučevanja kot prevladujoč jezik. Izraze sem prevedel s pomočjo pojmovnika in slovarja Varnost v elektronskih komunikacijah in informacijski tehnologiji (Meše 2003). Če nisem našel ustreznega prevoda, sem izraze smiselno prevedel sam ali pa sem jih zapisal v izvirniku.

2.4 Struktura dela

Delo je sestavljeno iz konceptualno-teoretičnega okvira, ki je temeljna sestavina dela. V njem opredelimo vse relevantne koncepte, ugotovimo, kakšne so mogoče operacionalizacije obstoječih metod, ter oblikujemo izhodišča za pripravo analitičnega orodja.

Tako opredelimo koncepte kritične infrastrukture, varnosti, kibernetске varnosti, varovanja informacij, preverimo, katere so največje grožnje korporativni in informacijski varnosti, kateri so najbolj izstopajoči do sedaj znani napadi, katere so znane grožnje kritični infrastrukturi, ki je predmet tega dela, nato pa opredelimo znane metode za premostitev teh težav ter merska orodja za ugotavljanje njihove uspešnosti in učinkovitosti.

Na podlagi konceptualno-teoretičnega aparata pripravimo mersko orodje ter ga operacionaliziramo. Potek in rezultati so opisani v drugem delu, ki pa je veliko krajši od prvega.

3 Konceptualno-teoretični okvir

3.1 Kibernetika in kibernetiski prostor

Sodobno razumevanje pojma kibernetika je vpeljal Norbert Wiener s svojim delom Kibernetika ali nadzor in komunikacija pri živalih in strojih (Weiner 1964, 16). Kibernetika je znanstvena študija nadzora in komunikacije pri živalih in strojih.

Sicer je v najširšem pomenu kibernetika interdisciplinarna veda, ki se ukvarja z nadzornimi sistemi, njihovo sestavo, omejitvami in možnostmi (Richards 2007, 2). Koncepti, ki jih kibernetika preučuje, so med drugim učenje, kognicija, prilagajanje, družbeni nadzor, komunikacija, učinkovitost, povezljivost itd. Področja znanosti, na katere vpliva kibernetika ali pa so vplivala na kibernetiko, so med drugim teorija iger, sistemska teorija, sociologija, psihologija, filozofija, arhitektura in teorija organizacij. Danes kibernetika ni splošno priznana kot samostojna znanstvena disciplina, predvsem zaradi kompleksnosti in posledičnega pomanjkanja koherentnosti, so se pa močno razvile iz nje izhajajoče, bolj specializirane discipline, kot so npr. računalniška znanost, umetna inteligenca ipd. Nato je v poljudnem razumevanju pojma prevzela pomen filozofska komponenta, ki trdi, da se sistemi definirajo s svojimi abstraktnimi odnosi in tokom informacij in ne toliko z materialnimi komponentami (Heylighen in Joslyn 2001, 1–5).

Takšno razumevanje pojma kibernetika vsebuje tudi pričujoče delo. Gre namreč za analizo varnosti odnosa med komponentami, ki tvorijo kompleksno mrežo, ki jo razumemo kot kritično. Pomembno je tudi razumevanje, da se pojem kibernetiko v tem delu ne nanaša na kibernetiko na splošno, temveč na pojem kibernetiski prostor³. Ta je sicer tesno povezan s pojmom kibernetike, vendar se na začetku ni pojavil kot teoretičen koncept, pač pa kot knjižni izraz v romanu Nevromant Williama Gibsona iz leta 1984. Sčasoma je postal ta pojem tudi opredeljen teoretičen koncept, ki ga lahko definiramo kot »elektronski, navidezni prostor za izmenjevanje informacij v računalniških in drugih (mobilnih, socialnih) omrežjih, ki omogočajo stalno povezljivost in komunikacijo« (Bernik in Prislán 2012, 168).

Razvili sta se dve temeljni teoriji kibernetikega prostora: neoliberalna in neorealistična. Prva trdi, da je kibernetiski prostor samostojen svet, njegove uporabnike pa opredeli kot zunanje akterje in opazovalce, ki se razvijajo skupaj s

³ Po angleško Cyberspace

procesom. Del zagovornikov te teorije trdi, da je razvojni proces prostora organski, drugi del pa, da ga je treba nadzorovati in vanj posegati za preprečitev zlorab. Druga teorija je nastala iz vojaških in strateških raziskav. Kljub priznavanju velikega pomena komunikacijskih tehnologij trdi, da je kibernetiski prostor takšen kot vsak drug in ni vir nove moči, temveč le nov prostor, v katerem se razporeja že obstoječe razmerje moči. Kibernetiski prostor razume kot podaljšek realpolitičnega prostora, celo bojišča (Bernik in Prislan 2012).

Manjikian trdi, da ne glede na to kibernetiski prostor zaradi njegove navideznosti odlikujejo tri temeljne lastnosti, ki ga razlikujejo od drugih prostorov: sposobnost mobilizacije uporabnikov, tudi tistih, ki se v procese težko vključujejo s tradicionalnimi metodami; sposobnost v vsakem trenutku zagotoviti velike količine nereguliranih informacij ter sposobnost krčiti in odpravljati geografske razdalje in ovire med uporabniki. (Manjikian 2010)

3.2 Splošna varnost, informacijska varnost, energetska varnost

Varnost je zelo širok koncept, glede katerega ni popolne usklajenosti, vendar za potrebe tega dela zadošča Grizoldova opredelitev: »Varnost, v najširšem pomenu stanje, v katerem je zagotovljen uravnoteženi fizični, duhovni in gmotni obstoj posameznikov, skupnosti in naravnega okolja, in dejavnosti za zagotavljanje takšnega stanja. V ožjem smislu v. pomeni predvsem državno varnost (zanjo se je uveljavil pomen nacionalna v.) in javno v., katere predmet so državljani, njihovo premoženje ter javni red in mir.« (Voglar 2000, 139). Po eni strani lahko varnost razumemo kot odsotnost škodljivih groženj določene družbe, po drugi pa je varnost dejavnost za zaščito in obrambo pred grožnjami (Prezelj 2000, 12). Ugotovimo lahko torej, da je pojmovanje varnosti večplastno, predvsem se je treba osredotočiti na nacionalno, torej skupno in posameznikovo (človekovo) varnost.

Za znanstveno in analitično obravnavanje varnosti velja, da so nanj ves čas vplivale tri teoretične in politične paradigme: realizem, liberalizem in radikalizem (Svete 2005, 34). Realizem predpostavlja, da je edino merilo državne (nacionalne) varnosti njena vojaška moč in da lahko torej država poveča svojo varnost le s povečanjem vojaške moči. Države ves čas tekmujejo za omejene dobrine in si prizadevajo priti do zanje ugodnega ravnotežja sil. Suverena država je tu torej edini akter v mednarodnem okolju, okolje pa je povsem anarhično (Svete 2005, 36). Zanimivo je, da je bilo do

šestdesetih let o varnosti napisanega zelo malo, saj se je ni obravnavalo kot samostojen znanstveni koncept. Realizem predpostavlja kot poglavitni mir tako imenovani negativni mir, ki pomeni zgolj odsotnost enega dejavnika ogrožanja varnosti, to je vojne. Za stabilnost je pomembnejši pozitivni mir, ki predpostavlja odpravo strukturnega nasilja oziroma relativnega pomanjkanja večine svetovnega prebivalstva (Møller 2004, 2). Ugotovimo lahko, da je ta koncept enodimenzionalen, saj predpostavlja le nacionalno ozemeljsko suverenost. Verjetno najpomembnejši koncept varnosti sodobne družbe je koncept večdimenzionalne varnosti kopenhavnske šole. Prvi koraki k takemu konceptu so se začeli pojavljati na začetku osemdesetih let 20. stoletja s poročilom Palmerjeve komisije, ki zanika realizem v mednarodnih odnosih, zavrača varnostno kompetitivnost in poudarja, da je poglavitna metoda za doseg varnosti sodelovanje (Prezelj 2000, 24).

Tako pridemo do liberalizma, ki poudarja veliko pomembnost mednarodnih in nadnarodnih struktur; te preprečujejo, da bi se države vedle samovoljno, saj imajo preveliko ekonomsko ali politično moč (npr. OZN, mednarodne korporacije). Država je še vedno glavni akter, vendar je povezana z vsemi drugimi državami. V njihovem okviru delujejo tudi preostale organizacije in vsi ti akterji morajo med seboj sodelovati. Če je realizem kompetitivni model, je liberalizem korporativni. Del zagovornikov liberalizma tudi zagovarja tezo, da je nujen pogoj za doseg globalne varnosti gospodarsko liberalna demokracija (Svete 2005, 40). Premik k takšnemu pojmovanju varnosti je bil najočitnejši na koncu osemdesetih let, takrat pa je imela tudi največjo veljavo kopenhavska šola. Njeni predstavniki so razdelili varnost na vojaško, ekološko, gospodarsko, politično in družbeno.

Tretja smer razmišljanja, imenovana tudi konstruktivizem, pa kot glavnega oblikovalca varnosti ne predpostavlja materialnih akterjev, kot so države, temveč vzorce razmišljanja (ideologije, norme ipd.). Ti so seveda od države do države različni, zato je različno tudi pojmovanje varnosti. Eden izmed zagovornikov te teorije, Arnold Wolfers, tako poda definicijo varnosti, ki pravi, da je ta odsotnost groženj naučenim ključnim vrednotam (Svete 2005, 46).

Po opredelitvi varnosti kot pojma znanstvenega preučevanja in razslojitve preučevanja se je pojavil še problem izbire referenčnega okvira varnosti, torej varnost predvsem koga in česa, pa tudi pred kom (čim), od koga in s čim (s kakšnimi

sredstvi). Z novim obravnavanjem varnosti se nujno spremeni in poglobi tudi obravnavanje človekove varnosti. Po pojmovanju države kot edine entitete, ki je deležna varnostnega obravnavanja, se je preučevanje sčasoma usmerilo tudi na societalno raven, torej na skupine, kot so narodi, verske ločine, spol in podobno ter še kasneje na človeka kot posameznika (Møller 2004, 7). Pojem človekove varnosti se prvič pojavi kot predmet preučevanja leta 1994. Razvojni program Združenih narodov je takrat namreč objavil koncept človekove varnosti v letnem poročilu Human Development Report (Prezelj 2000, 24).

Človekova, torej osebna varnost občana določene države se ne sklada nujno s konceptom varnosti države, v kateri prebiva. Še več, ta dva pojma sta si lahko pogosto celo nasprotna (Svete 2005, 58). Prvi pomemben pristop k obravnavanju človekove varnosti so temeljne človekove dobrine. Posameznik potrebuje zagotovljene materialne zmožnosti, zdravstveno oskrbo ter varnost pred kriminalom in urejeno okolje. Drugi koncept trdi, da je človekova varnost nad državno varnostjo in jo je včasih treba razreševati z nastopom proti državi. To se kaže po eni strani v znotrajdržavnih konfliktih, po drugi strani pa z vojaškimi operacijami za vsilitev, vzpostavitev, graditev in ohranitev miru. Zagovorniki tretjega pristopa, t. i. razvojniki, zagovarjajo tezo, da je najpomembnejši način za dosego človekove varnosti njegov razvoj. Zagotavljanje minimalnih življenjskih pogojev namreč ni dovolj, treba je celostno povezati vse preostale strategije za uresničevanje varnosti. Četrty koncept je koncept nove varnosti (New security). Predpostavlja, da so najpomembnejši dejavniki za človekovo varnost država in njene institucije. Natančneje, šibke institucije povzročajo ogroženost človeka⁴, varnost pa se povečuje s krepitvijo teh institucij (Svete 2005, 96). Država torej s konceptualnim razvojem preide od subjekta varnosti k sredstvu za njeno zagotavljanje.

Čeprav to delo raziskuje tudi vidike državne varnosti, je pomembneje, da se nanaša na varnost organizacij, ki z zagotavljanjem delovanja kritične infrastrukture vzpostavljajo človeško varnost. Tako kot trdi na primer Liotta (Liotta 2002, 475), smo v sodobni družbi brisanja ločnic med človeško in državno varnostjo, pa tudi med nacionalno in mednarodno varnostjo. Uvaja se koncept societalne varnosti, torej varnosti družbe, ki pa ga ne zagotavlja nujno država ali pa ga ta zagotavlja z

4 Tu gre za to, da država ne more preprečiti ogrožanja človekove varnosti, ki se kaže v epidemijah, kriminalu, terorizmu ipd.

netradicionalnimi sredstvi, torej namesto z monopolom nad silo z regulacijo delovanja družbe (Liotta 2002, 473–475).

Kot relevantnega je treba dodati še pojem sekuritizacije, enega temeljnih prispevkov kopenhavnske šole. Ta skladno s konstruktivistično teorijo vpelje procesno razmišljanje o varnosti, opredelitev koncepta, sredstev ali procesa kot varnostno pomembnega in skozi proces politizacije ustvarjanje potrebe po njegovem zavarovanju, s tem pa pridobivanje politične moči za družbeno oblast (McDonald 2008, 563–588). Medtem ko določeni avtorji trdijo, da je takšen pogled na varnost problematičen, saj lahko vsebino, kontekst in naravo sekuritizacije določajo zgolj dominantni akterji (prav tam), je ta pomemben za pričujoče delo. Očitno je namreč, da je kibernetski prostor v zadnjih desetletjih postal pomemben predmet družbene varnosti in blagostanja.

Informacijska varnost

Naslednji temeljni koncept, ki ga je treba za namene tega dela opredeliti, je informacijska varnost. V kibernetskem okolju gre namreč pri varovanju kritične infrastrukture za številne vidike varovanja informacij.

Informacijska varnost je po definiciji organizacije ISO zagotavljanje zaupnosti, celovitosti in dostopnosti informacij, poleg tega pa so lahko v ta koncept zajete še avtentičnost, nezatajljivost in zanesljivost podatkov (Calder 2005, 10).

Kljub razmeroma preprosti definiciji tega koncepta se z njim ukvarja veliko literature in dejavnosti, pa tudi več disciplin v okviru računalniških ter upravnih znanosti, ki obravnavajo ranljivosti, vire ogrožanja ter zavarovanje pred njimi. Sledi obdelava koncepta informacijske varnosti s poudarkom na varnosti informacijskih sistemov za obvladovanje elektroenergetske kritične infrastrukture.

Ameriški pravni sistem informacijsko varnost definira kot »varovanje informacij in informacijskih sistemov pred nepooblaščenim dostopom, uporabo, razkritjem, motnjami, spremembami ali uničenjem, tako da se zagotavlja celovitost, zaupnost in dostopnost sistema« (Cornell University Law School).

ISACA opredeli ta termin kot to, kar zagotavlja v podjetju varnost informacij pred razkritjem nepooblaščenim osebam (zaupnost), neprimerno spremembo (celovitost) in preprečitev dostopa, ko je to potrebno (dostopnost) (ISACA 2014).

V strokovni literaturi lahko zasledimo naslednje definicije informacijske varnosti: »Informacijska varnost zajema uporabo fizičnih in logičnih kontrol dostopa do podatkov, da se zagotovi njihovo ustrezno uporabo in da se prepreči nepooblaščen ali nenamerno spremembo, uničenje, razkritje, izgubo ali dostop do avtomatiziranih ali ročnih zapisov in datotek ter izgubo, poškodbo ali neprimerno rabo informacijskih sredstev.« (Peltier 2001, 266).

Medtem ko je takšna definicija zelo celovita, lahko najdemo v strokovni literaturi tudi bistveno krajšo, ki je skladna z opredelitvijo ISO: »Računalniška varnost je zagotavljanje celovitosti, zaupnosti in dostopnosti računalniških sistemov.« (Pfleeger in Pfleeger 2003, 29).

Organizacija in izvajanje informacijske varnosti preprečuje kibernetске napade. Njihove žrtve so lahko posamezniki, organizacije in države (Bernik in Prislan 2012, 61), pri čemer pa se vse te tri skupine združujejo v omrežja, ki so sama postala pomemben referenčni objekt, na katerega se varnost nanaša. Ko govorimo o varnosti omrežij, govorimo o dveh vidikih te varnosti:

- notranji omrežni varnosti organizacij, ki se nanaša na celovitost, dostopnost in zanesljivost podatkov v samem omrežju;
- omrežni varnosti, usmerjeni v okolje, ki se nanaša na interakcijo med organizacijami in odjemalci njihovih informacij (Svete 2005, 105–107).

Skupine potencialnih žrtev so tudi skupine potencialnih napadalcev. Po Berniku in Prislanovi imajo države naslednje motive za izvajanje informacijskega bojevanja:

- vohunjenje; države vzpostavljajo velike sisteme za nadzor nad vsemi komunikacijskimi sredstvi in potmi, številni med njimi so tudi prikriti in celo nezakoniti. Med takšnimi dejavnostmi lahko izpostavimo sistem Echelon, ki ga upravljajo ZDA, VB, Avstralija in Nova Zelandija. Zasnovan je tako, da poskuša preprečiti vsakršno komunikacijo v svetu, jo filtrira in v njej išče za naročnika pomembne podatke. Tudi podjetji Google in Microsoft sta ameriškim

obveščevalnim službam že posredovali podatke o evropskih uporabnikih njihovih storitev;

- aktivno bojevanje; pri tem gre lahko za podporo klasičnemu, kinetičnemu vojskovanju, uporabo informacij na vojnem območju, vzporedno aktivnostjo vojskovanja za ustvarjanje ustreznega psihološkega stanja ali asimetričnega vojskovanja držav v kibernetnem prostoru;
- informacijske operacije; te so usmerjene v preučevanje okolja in vplivanje na psihološko stanje oziroma miselnost ljudi v tem okolju. Gre za poskus preoblikovanja stanja informacijskega okolja, pri čemer se za doseg teh ciljev uporabljajo tudi napadi na sisteme. Takšno dejavnost se opravlja tako v miru kot v obdobju konfliktov;
- propagandna dejavnost; pri tem gre za prenos standardnih propagandnih metod in sredstev v kibernetni prostor, aktivnosti, ki jih zajema, pa so spravljane informacij v medije, ideološki pozivi, odvrčajoče informacije, zadrževanje informacij ter sodelovanje in dogovarjanje z mediji.

Energetska varnost

Definicij energetske varnosti je v strokovni literaturi izjemno malo, pri čemer je večina teh definicij implicitnih.

Eno definicijo lahko najdemo v OPEC-ovi publikaciji OEC Energy Review: »(Energetska) varnost je omajana, ko je dobava (energije) prekinjena na nekaterih mestih do meje, da ta povzroči nenadno, znatno in stalno povišanje cen.« (Mabro 2008).

Naslednjo definicijo lahko zaznamo v delu The Economics of Energy Security: »Energetsko nevarnost lahko opredelimo kot izgubo blagostanja, do katere lahko pride zaradi spremembe cen ali razpoložljivosti energije.« (Bohi in drugi 1996).

Mednarodna agencija za energijo definira energetsko varnost kot termin, ki se nanaša na neprekinjeno zagotavljanje energije za sprejemljivo ceno (International Energy Agency 2013).

Grošelj energetsko varnost Definira kot »zagotavljanje zadostnih količin energije po ekonomsko sprejemljivih cenah iz različnih in razpršenih virov ter tranzitnih poti« (Grošelj v Prezelj 2009, 32).

Iz teh definicij izhaja, da lahko energetska varnost opredelimo predvsem kot zagotavljanje za delovanje družbe sprejemljivih količin energije po sprejemljivih cenah.

3.3 Kritična infrastruktura

Danes je težko opredeliti infrastrukturo kot nekritično. V preteklosti je veljala definicija kritične infrastrukture kot infrastrukture, katere daljše motenje bi lahko imelo večje vojaške in ekonomske posledice (Dunn in Moteff v Prezelj 2009, 9), danes pa se skladno s spremembo varnostnih paradigem kritičnost infrastruktur subjektivizira in je odvisna tudi od konteksta. Kritične infrastrukture so po svoji naravi večnamenske in zagotavljajo zelo širok spekter družbenih aktivnosti, dobrin in storitev. Zato lahko rečemo, da predstavljajo globalna sredstva za nedoločljive cilje (Prezelj 2009, 9).

Definicija kritične infrastrukture vsebuje dva elementa: infrastrukturo in kritičnost, pri čemer drugi pojem omeji prvega. Tako lahko ta pojem opredelimo kot mreže oziroma sisteme med seboj kompleksno povezanih elementov, ki zagotavljajo kontinuiran dotok dobrin in storitev, nujnih za varnost in blagostanje prebivalstva (Michel-Kerjan v Prezelj 2009, 10). Takšna definicija je torej definicija pojma infrastrukture, ki je nekoliko omejen na določen, kritičen segment. Vendar je takšna definicija zelo podobna sami definiciji infrastrukture. To SSKJ opredeli kot »temeljne naprave, objekte, zlasti prometne, ki omogočajo gospodarsko dejavnost določene skupnosti«. Podobno definicijo podaja slovar angleškega jezika Collins Cobuild: »Infrastruktura države, družbe ali organizacije je sestavljena iz osnovnih objektov, transportnih, komunikacijskih in energetskih, ki jim omogočajo delovanje.« (Sinclair 1997, 865). Še eno splošno definicijo lahko najdemo v slovarju angleškega jezika American Heritage: »Osnovni objekti, storitve in naprave, ki so potrebni za delovanje skupnosti ali družbe, na primer transportni in komunikacijski sistemi, vodovodi in daljnovodi, ter javne ustanove, med drugim šole, pošte in zapori.« (Moteff in Parfomak 2004). Vse te definicije bi torej težko razločili od definicije kritične infrastrukture, še posebno če upoštevamo element kritičnosti. Tako moramo za uspešno definicijo kritične infrastrukture poleg navedbe splošne definicije nujno naštetih segmente, ki so kritični.

Opredeljevanje kritičnosti predstavlja svojevrsten izziv, saj je, kot ugotavlja Prezelj, kritičnost opredeljena slabo, to pa zato, ker se spreminja skozi čas in ker je to subjektivna kategorija. Zato obstaja tudi vrsta nacionalno veljavnih definicij kritičnih

infrastruktur. Poročilo OECD o varovanju kritične infrastrukture [...] (OECD 2008) navede naslednje definicije:

- Avstralija: kritična infrastruktura je definirana kot fizični objekti, dobavne verige, informacijske tehnologije in komunikacijska omrežja, katerih uničenje, degradacija ali nedostopnost za daljše obdobje bi občutno vplivali na družbeno ali ekonomsko dobrobit naroda oziroma na avstralsko zmožnost izvajanja nacionalne obrambe in zagotavljanja nacionalne varnosti;
- Kanada: kanadsko kritično infrastrukturo sestavljajo tisti fizični in informacijski objekti, mreže in sredstva, katerih motenje ali uničenje bi za Kanadčane in učinkovito delovanje kanadskih vlad imelo resne posledice;
- Nemčija: kritična infrastruktura so organizacije in pomembni objekti, katerih nedelovanje ali poškodba bi pomenila daljše pomanjkanje potrebščin, občutne motnje javnega reda in druge opazne posledice;
- Nizozemska: kritična infrastruktura se nanaša na tiste produkte, storitve in procese, katerih prekinitev ali izpad bi pomenil večje družbene motnje. Te bi pomenile velike žrtve in veliko ekonomsko škodo;
- Združeno kraljestvo: nacionalno kritično infrastrukturo sestavljajo tista sredstva, storitve in sisteme, ki podpirajo tamkajšnje ekonomsko, politično in družbeno življenje in katerih pomembnost je tolikšna, da bi njihova izguba: 1) pomenila veliko izgubo življenj, 2) imela velik vpliv na nacionalno gospodarstvo, 3) imela druge hude družbene posledice v skupnosti ali 4) bila neposredna grožnja nacionalni vladi;
- ZDA: sistemi in sredstva, fizična ali virtualna, tako pomembna za ZDA, da bi njihovo onemogočenje ali uničenje ohromilo občo varnost, varnost nacionalnega gospodarstva, nacionalnega javnega zdravstva ali katerokoli kombinacijo teh elementov.

Definicija kritične infrastrukture, kot jo ponuja direktiva Evropskega sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite, je naslednja: »Kritična infrastruktura pomeni infrastrukturno zmogljivost, sistem ali njun del, ki je v državah članicah in je bistven za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi ter katerih okvara ali uničenje bi imelo v državi članici resne posledice zaradi nezmožnosti vzdrževanja teh funkcij« (*Direktiva sveta ES št. 114/2008*).

Kratka analiza teh definicij nam najprej pove, da skupnega elementa, vsaj dobtedno poimenovanega, med njimi ni. Lahko pa izluščimo elemente, ki se pojavljajo najpogosteje. Formulacija vseh definicij je, da je narava kritične infrastrukture, kakor je definirana, takšna, da bi imelo njeno bistveno motenje resne posledice. Če bi povzeli štiri najpogosteje ponavljajoče se elemente definicij, bi prišli do sledeče opredelitve: kritična infrastruktura so sistemi in objekti, katerih bistveno motenje v delovanju bi imelo občutne družbene in ekonomske posledice.

V slovenski strokovni literaturi se pojavlja terminološka zagata o izbiri termina kritična, ključna ali vitalna infrastruktura. V tem delu bom uporabljal izraz kritična infrastruktura; ta po Prezlju najbolj kaže na to, da gre za infrastrukturo, ki je kritična za delovanje družbe (Prezelj 2010, 7–8).

Slovenska elektroenergetska kritična infrastruktura

Elektroenergetska kritična infrastruktura, ki jo lahko uvrstimo med tri podsektorje sektorja energetske kritične infrastrukture, je ena izmed najpomembnejših kritičnih infrastruktur. Ugotovimo lahko, da ta infrastruktura zagotavlja vrsto družbeno pomembnih procesov in da zajema procese, kot so proizvodnja, prenos in distribucija električne energije. Ker je skladiščenje električne energije tako rekoč nemogoče, je onemogočeno oblikovanje strateških rezerv, zato je ta podsektor tudi eden izmed bolj ranljivih. Dodatno k ranljivosti prispeva dejstvo, da je Republika Slovenija neto uvoznica električne energije (Ministrstvo za gospodarstvo 2010) in da je posledično pri zagotavljanju nemotenega oskrbovanja družbe odvisna od zunanjih družbeno-političnih dejavnikov.

Slovensko elektroenergetsko kritično infrastrukturo upravlja 24 podjetij, od tega je deset dobaviteljev električne energije. Proizvajalcev je enajst, od tega sta dve podjetji skupini proizvajalcev: prvi je Holding slovenske elektrarne, ki združuje štiri proizvajalce, drugi pa GEN energija, d. o. o., ki združuje tri. Borzen, d. o. o., je organizator trga z električno energijo, SODO, d. o. o., sistemski operater distribucijskih elektroenergetskih omrežij, Eles, d. o. o., pa sistemski operater prenosnega elektroenergetskega omrežja (Javna agencija RS za energijo 2013). Sistemski operater prenosnega omrežja in sistemski operater distribucijskega omrežja sta gospodarski javni službi (Javna agencija RS za energijo 2011, 21).

Medtem ko je prenosno omrežje v lasti in upravljanju enega podjetja, so distribucijska omrežja, ki bi jih moralo upravljati podjetje SODO, še vedno v lasti in upravljanju posameznih distribucijskih podjetij, SODO pa jih ima v najemu. Poleg tega to podjetje nima ne kadrovskih ne tehničnih zmožnosti za upravljanje zakonsko določene gospodarske javne službe. Gre torej za normativno ureditev področja, ki se trenutno ne izvaja (Ministrstvo za gospodarstvo 2010).

Poraba električne energije v RS je v letu 2010 znašala 12.158 GWh in je bila glede na leto 2009 za 8 % večja, od tega 2 % zaradi priklopa Črpalne hidroelektrarne Avče. Proizvedene je bilo 15.260 GWh energije, od tega so 28 % proizvedle hidroelektrarne, 31,8 % termoelektrarne, 35 % Jedrska elektrarna Krško, 4 % pa mali proizvajalci. RS je izvozila 10.717 GWh, uvozila pa 8.599 GWh. Skupnega prenosa energije je bilo 23.126 GWh (Javna agencija RS za energijo 2011, 21). Kakovost oskrbe končnih odjemalcev z električno energijo se izboljšuje. Iz lastnih vzrokov je bilo v letu 2010 skupaj v povprečju 37 minut na odjemalca nenačrtovanih prekinitev dobave energije, iz vseh pa 81. Skupaj z načrtovanimi prekinitvami je bil povprečen slovenski odjemalec brez električne energije 181 minut, prekinitev pa je bilo 2,66. Glede na trajanje nepričakovanih prekinitev oskrbe z električno energijo na odjemalca je RS v evropskem povprečju. Slovenska elektroenergetska podjetja so v zvezi s kakovostjo napetosti v letu 2010 imela 357 pritožb, od tega sta jih bili dve tretjini upravičeni.

Prezelj in Grošelj ocenjujeta, da bi lahko zaradi izpada slovenske elektroenergetske kritične infrastrukture posledice čutile tudi sosednje države, predvsem Hrvaška, Avstrija in Italija, zaradi nekdanje skupne infrastrukture pa tudi nekdanje države članice SFRJ (Prezelj 2009, 37–38, 152). Posledice dobave električne energije bi bile občutne takoj, pri čemer bi nekateri objekti (npr. bolnišnice) zase z uporabo generatorjev nekaj časa še lahko zagotavljali delovanje, nato pa bi prenehali delovati tudi oni. Ekonomske posledice prekinitve bi se pokazale kot izgubljena proizvodnja, neizrabljena že plačana proizvodna sredstva, stroški za ponovni zagon procesov, škoda na opremi, neposredni stroški, povezani z zdravjem ljudi, ipd. Neposrednih smrtnih žrtev naj ne bi bilo, neposredna škoda naj bi bila srednja, posredna pa zelo velika. Pri kratkotrajni prekinitvi bi bil med prebivalstvom, ki bi posledice občutilo v prvih 12 urah, prisoten nemir, sčasoma tudi panika. Grošelj navaja, da bi škoda

zaradi izpada elektroenergetskega podsektorja v Sloveniji dnevno znašala več sto milijonov evrov (Prezelj 2009, 37–40).

3.4 Viri ogrožanja kritične infrastrukture ter informacijski viri ogrožanja.

Prezelj grožnje kritični infrastrukturi razdeli v tri skupne kategorije:

- naravne grožnje (naravne nesreče, kot so poplave, potresi, požari ipd.);
- namerne grožnje (npr. kriminal, terorizem, vojna ipd.);
- nenamerne grožnje (npr. napake pri uporabi, nesreče, sistemske napake ipd.).

Kot posebno podkategorijo naravnih nesreč lahko izpostavimo žled. Primer tega je Slovenija doživela pozimi leta 2014, njegove posledice pa so bile katastrofalne. V določenem trenutku je brez oskrbe z električno energijo ostalo 350.000 ljudi, kar predstavlja 15 % odstotkov vsega prebivalstva Slovenije. Poškodovanih je bilo več kot 2.000 kilometrov električnih vodov. Kumulativna posredna škoda v obdobju nastajanja tega dela še ni znana, je pa ocenjena na približno 400–500 milijonov evrov. Posledica ujme, povezana z elektroenergetsko kritično infrastrukturo, pa je bila med drugim tudi to, da se je približno 10 ljudi resno zastrupilo z ogljikovim monoksidom, ker so neustrezno porabljali električne agregate (Svete in Malešič 2014, 19–68).

Poleg tega Prezelj navaja še druge specifične vire ogrožanja, ki se lahko aplicirajo na posamezne sektorje in podsektorje. Za namene tega dela so najpomembnejši grožnja pomanjkanja usposobljenih kadrov, čezmerna obremenitev infrastrukture in prekinitev dobave surovin (Prezelj 2009, 148–149). To delo se bo osredotočilo predvsem na kategorijo namernih groženj in nekaterih nenamernih, posebno teh s področja informacijske varnosti.

3.5 Sistemi za upravljanje elektroenergetske kritične infrastrukture

Sistemi za upravljanje in krmiljenje elektroenergetske infrastrukture običajno pomenijo programabilne logične kontrolerje na najnižjem nivoju za posamezne sisteme, distribuirane kontrolne sisteme za posamezne procese in sisteme za pregled, nadzor in pridobivanje podatkov⁵ (SCADA) na najvišjem nivoju (Stoufer in

⁵ Supervisory Control and Data Acquisition

drugi 2011, 2–1). Ti sistemi so si dokaj različni glede na tehnologijo, ki jo uporabljajo, glede na infrastrukturo pa so si dokaj podobni. Običajno sistem SCADA sestavljajo naslednji podsistemi:

- merilne naprave na posameznih točkah infrastrukture;
- delovni instrumenti, kot so na primer ventili, releji in podobno;
- lokalni procesorji in terminalske enote (PLC, RTU), ki komunicirajo z merilnimi instrumenti in delovno opremo. Procesorji pridobivajo vhode iz merilnih instrumentov, skozi različne protokole in logične kontrolerje pa krmilijo delovne instrumente;
- sistemi za komunikacijo med merilnimi napravami, delovnimi instrumenti in procesorji. Ti so lahko tako prek kabla kot brezžični;
- gostiteljski računalniški sistemi (HMI), ki delujejo kot osrednja točka nadzora in upravljanja. Na tej točki običajno deluje človeški operater, ki nadzoruje procese, pregleduje podatke in razrešuje alarme;
- komunikacijski sistemi dolgega dosega med lokalnimi procesorji in gostiteljskimi računalniškimi sistemi, ki lahko potekajo prek telefonskih kablov, satelitskih povezav, mikrovalov, paketnega prenosa podatkov itd. (Robles in Choi 2009).

Dejavniki tveganja za sisteme SCADA

Sistemi SCADA so običajno sposobni samostojnega izvajanja običajnih, preprostih logičnih procesov brez nadzora centralnega operaterja. Najpogosteje uporabljajo programski jezik IEC 61131-3, s katerim sistemski inženirji lahko sami programirajo delovanje sistema prek logičnih kontrolerjev in oddaljenih terminalov. Programska oprema, s katero se lahko sisteme upravlja, je lahko odprta ali zaprta. V prvem primeru to pomeni, da jo lahko operater sam spreminja, kar pomeni, da takšna oprema lahko krmili različne vrste sistemov SCADA.

Sistemi SCADA so bili v začetku zasnovani kot zaprti sistemi, torej takšni, da jih je fizično mogoče upravljati le prek določenih terminalov, ki so bili ločeni od vseh drugih omrežij, vendar pa se je to v zadnjih dveh desetletjih spremenilo. Zahteve po veliki odzivnosti in delovni fleksibilnosti sistemskih operaterjev so pomenile, da jim je moral biti zagotovljen oddaljen dostop do teh sistemov prek drugih računalnikov v omrežju oz. domeni. Dodatna je bila zahteva vodstvenih delavcev, da lahko kadarkoli

dostopajo do pomembnih podatkov o stanju njihovih sistemov. Vse to je pomenilo, da so sistemi SCADA zdaj običajno povezani z drugimi računalniki v domenah, do njih pa je mogoče dostopati tudi prek oddaljenih povezav prek navideznih omrežij (Riptech 2001). Poleg tega omrežja pogosto niso ali pa so slabo razčlenjena, kar pomeni, da v omrežju tako rekoč ni preprek za širjenje zlonamerne programske kode med sistemi.

Še več, NCCIC ugotavlja, da so prav vsi sistemi, ki so jih v preteklih letih pregledovali, povezani v omrežje podjetja. V povprečju je tako v družbah po pričevanju direktorja NCIC med nadzornim in delovnim omrežjem 11 povezav, v določenih primerih pa so med omrežjema identificirali tudi 250 neposrednih povezav (Byres 2012, 2).

Dodatna težava je, da vse večja povezljivosti do sistemov za upravljanje omrežja ni nujno skladna z dobrimi praksami IT-varnosti, poleg tega pa je treba to povezljivost urediti tako, da bosta lahko med seboj komunicirala dva različna sistema. Varnostni protokoli so zato pri takšnih povezavah zelo omejeni (Riptech 2001). Zgodi se lahko tudi, da varnostnih mehanizmov pri takšnih dostopnih točkah niti ni⁶. Osebe, ki upravlja to omrežje, namreč zahteva določeno mero učinkovitosti in lahkotnosti dostopa, zato prihaja pri implementacij varnostnih politik tudi do političnih konfliktov med upravitelji omrežja in varnostnimi inženirji. Dodatna težava je, da ti upravitelji omrežja tudi neradi sodelujejo pri implementacij popravkov za te sisteme. Ti namreč včasih povzročijo nevšečnosti, kot so motnje v delovanju (SANS Institute 2005).

Zaradi zahteve po večji povezljivosti in preprostosti dostopa je pri operaterjih sistemov SCADA pogosta praksa, da si med sabo delijo gesla za dostop do računalnikov oziroma računov, ki upravljajo s sistemom, lahko pa celo uporabljajo isti nadzorni uporabniški račun. To seveda pomeni lažje dostopanje do sistema, popolnoma pa onemogoči sledljivost in močno oteži varnost sistema (SANS Institute 2005).

Večja povezljivost in preprostost dostopanja nista bili nujno uravnoteženi z izboljšanimi varnostnimi mehanizmi. Tako so zelo redki sistemi za zaznavanje

⁶ Zasledimo lahko primer, ko je v ZDA imelo neko infrastrukturno podjetje, ki ima več kot 4 milijone odjemalcev na nekem objektu, anteno za brezžično omrežje. Varnostni ocenjevalec je lahko na to omrežje iz svojega vozila v 15 minutah ustvaril celoten zemljevid omrežja, v 20 minutah pa je lahko komuniciral s poslovnim omrežjem in pridobival poslovna poročila. (Sauver 2004)

vdorov, prav tako ni nujno, da bi imeli računalniki, prek katerih se upravlja sistem, nameščen protivirusni program ali požarni zid. Nezavarovana je lahko tudi komunikacija, ki poteka po brezžičnih povezavah; te so lahko tudi standardni protokoli za brezžične povezave brez varnostnih mehanizmov, to je 802.11 (SANS Institute 2005).

Vse to so splošni problemi, ki jih lahko obvladujemo s splošnimi varnostnimi praksami IT, obstajajo pa tudi problemi, ki so specifični za sisteme SCADA. Prvi je, da imajo lokalni procesorji za delovne instrumente znane varnostne ranljivosti, ki pa jih je težko odpraviti, saj je njihova moč dokaj slaba in bi jih varnostne nadgradnje še bolj oslabile. Drugi problem je, da so ti procesorji namenjeni dolgotrajnemu delovanju in se jih lahko uporablja celo deset let in več. Tudi programska oprema, ki se uporablja za upravljanje sistema, je ranljiva za napade in ima napake v zasnovi (SANS Institute 2005).

Informacijski sistemi so načeloma prilagodljivi in je mogoče napake v varnostnih zasnovah kode odpraviti dokaj hitro, pri sistemih ICS pa je drugače, saj je največji poudarek pri zasnovi teh sistemov na stabilnosti delovanja in se varnostne rešitve preverjajo dolgo. Tako je povprečno obdobje med odkritjem in javnim razkritjem varnostne ranljivosti v sistemih ICS 331 dni, lahko pa trajajo tudi več kot 1000 dni (Knapp 2011, 33).

Zadnja velika težava je fizična varnost; te točke so namreč razporejene čez velika območja, pri nas tudi prek celotne države, zato so pomembni tudi varnostni sistemi, ki vsiljivcem onemogočajo vstop v objekte. Pasivni varnostni sistemi, na primer ključavnice in protivlomna vrata, niso dovolj, potrebno je tudi fizično varovanje ter varovanje z videonadzorom (SANS Institute 2005).

Vsi ti dejavniki manjše varnosti nujno pomenijo, da so sistemi SCADA dokaj ranljivi za kibernetске napade, že testiranje ranljivosti pa ima lahko neželene posledice. Samo pregled inventarja, t. i. ping sweep, lahko pomeni izpad delovanja sistema, vseeno pa so penetracijski testi pri ocenjevanju varnostni sistema zelo pomembni. Treba je pazljivo tehtati med aktivnim in pasivnim testiranjem, pri čemer pasivno testiranje skorajda ne more vplivati na delovanje sistema, vendar ne prikaže nujno vseh njegovih ranljivosti. Aktivno testiranje po drugi strani lahko vpliva na delovanje sistema, njegovi rezultati pa so bolj zanesljivi (Duggan 2005).

Komunikacijski protokoli

Komunikacijski protokoli v kibernetiki pomenijo sisteme formatov digitalnih sporočil in pravila za izmenjavo teh sporočil med računalniškimi sistemi. Vse mrežne arhitekture so načeloma osnovane na standardiziranih modelih OSI sedmih plasti komunikacije, kot sledi (Kalapatapu 2004 in Krutz 2006, 43–48):

- plast 1: fizična plast, ki definira povezavo računalnika do fizičnih omrežnih prenosnih medijev. Gre za pretvorbo podatkovnih paketov v električne in mehanske signale. Tu se uporabljajo standardi, kot je RS-232 ali RJ-459;
- plast 2: podatkovna povezava; to plast sestavljata dva dela, in sicer MAC (media access control) in LLC (logical link control), skrbi pa za določanje enot sporočil, način ugotavljanja napak med točkami, odpravo napak, omrežno topologijo, kontrolo pretoka in mehanizme dostopa do prenosnega medija. Protokoli, ki se uporabljajo na tej plasti, so na primer ARP (address resolution protocol), ki določa MAC-naslove strojne opreme tako, da jih razbere iz IP-naslovov, ali PPP (point to point protocol), ki se uporablja za pošiljanje IP-sporočil prek povezav med točkami;
- plast 3: omrežje; opravljanje usmerjanja, naslavljanja, zaznavanja napak in nadzora nad prometom med točkama. Med drugim se na tej plasti uporabljata protokola IP (internet protocol), ki dodeljuje naslove pošiljateljem in sprejemnikom podatkovnih paketov, ter ICMP (internet control message protocol), ki se uporablja za nadzor poti prenosa podatkov od vira do naslova in za preverjanje razpoložljivosti gostiteljev za sprejemanje podatkov;
- plast 4: prenos; pri tem gre za vzpostavitev logične povezave med oddajajočo in sprejemajočo točko ter za zagotavljanje celovitosti komunikacijske seje. Ta plast torej zagotavlja, da bo komunikacijski paket prišel z ene točke na drugo. Na tej plasti se uporabljajo protokoli, kot so TCP (transmission control protocol), ki zagotavlja zanesljivo povezavo, odpravljanje napak in nadzor pretoka informacij, ali UDP (user datagram protocol), ki je protokol za prenos podatkov z manj funkcionalnostmi kot TCP;
- plast 5: seja; ta plast vzpostavi želeno povezavo, skrbi za prenos podatkov med sejo in sprosti povezavo. Plast podpira povezavo simplex, duplex in pol-duplex. Na tej plasti se uporabljajo protokoli, kot so RPC (remote procedure

call), ki podpira zahteve enega računalnika na omrežju do drugega, in NFS (network file system), ki podpira delitev datotek med računalniki;

- plast 6: prezentacija; opravlja pretvorbe in prevode podatkov za plast aplikacije, šifriranje in dešifriranje ter kompresijo podatkov. Protokoli, ki se uporabljajo na tej plasti, so na primer http (hypertext transfer protocol), ki se uporablja za dostop do svetovnega spleta, jpeg, standard za prikaz grafike, ter mpeg, standard za prikaz in kompresijo videoposnetkov;
- plast 7: aplikacija; najvišja plast v modelu. Opravlja nadzor nad mrežnim pretokom informacij in podpornimi funkcijami aplikacij. Potrjuje, da je prejemnik sporočila prisoten. Protokoli, ki se uporabljajo na tej plasti, so med drugim FTP (file transfer protocol), ki podpira prenos datotek med računalniki, SMTP (simple mail transfer protocol), ki podpira prenos e-poštnih sporočil, ter SNMP (simple network management protocol), ki zbira podatke o omrežju in jih predstavlja v konzolah za nadzor omrežja.

Podatki se prenašajo po plasteh navzdol, vsaka plast vsebuje tudi podatke z vseh zgornjih plasti. Tako na primer plast 5 vsebuje tudi podatke s plasti 6 in 7.

Opisan model se imenuje Open Systems Interconnections (OSI) Model in je sicer referenčen pri modeliranju komunikacije med računalniki, vendar se danes uporablja tudi model Transmission Control Protocol (TCP)/Internet Protocol (IP), ki ima štiri plasti (Krutz 2006, 48–50). Te so:

- plast 1: omrežje, ki je ekvivalent OSI plasti 1;
- plast 2: internet; tu delujejo protokoli, kot so IP, ICMP, ARP in PPP;
- plast 3: prenos gostitelj-gostitelj; tu delujeta npr. protokola TCP in UDP;
- plast 4: aplikacija; tu delujejo protokoli FTP, SMTP, SNMP in Telnet, ki omogoča upravljanje oddaljenega računalnika z emulacijo terminala.

Sistemi SCADA za prenos podatkov med oddaljenimi terminali in nadzornimi računalniki uporabljajo različne komunikacijske protokole, ki so osnovani na zgornjih modelih. Danes sta najpogostejša protokola DNP3 in T101 oziroma IEC 870-5-101 z razširitvami, ki omogočajo komunikacijo prek protokola TCP/IP. Starejši sistemi pogosto uporabljajo protokol MODBUS (Makhija 2003).

T101 je skupek standardov, ki jih je leta 1995 izdelala Mednarodna elektrotehnična skupina (IEC) kot odprt standard za prenos telemetrije za SCADO. Trenutno ga najbolj uporabljajo v evropski elektroenergetski industriji. T101 omogoča neenakomerno in enakomerno komunikacijo med nadrejeno in podrejeno napravo, prioritizacijo in klasifikacijo podatkov ter sheme za ciklično in spontano posodabljanje podatkov ter za njihov prenos (Bhattacharyya 2008, 519).

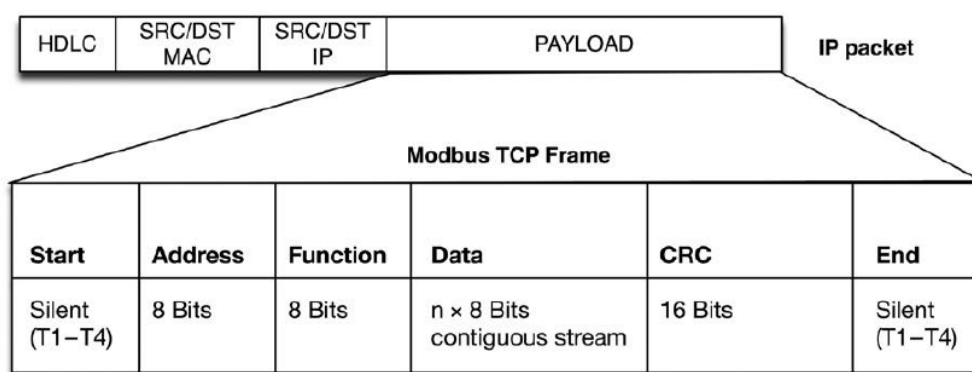
Tudi protokol DNP3 je bil zasnovan predvsem za SCADO in je odprtokoden. Omogoča visoko zanesljivost integritete podatkov, fleksibilno strukturo, več aplikacij ter minimalno obremenitev omrežja. Protokol je bil izdan leta 1993 (Makhija 2003, 4).

Protokol T101 se uporablja predvsem v Evropi, protokol DNP3 pa predvsem v Severni Ameriki. T101 se uporablja samo v komunikaciji med dvema točkama, DNP3 pa lahko uporabimo v različnih infrastrukturah komunikacije. Poleg tega je DNP3 bolj prilagodljiv, ker je odprtokoden in ga je mogoče uporabiti v navezi s TCP/IP, T101 pa ne.

MODBUS je tretji bolj razširjeni protokol, ki se uporablja za sisteme SCADA. Protokol so ustvarili že leta 1979 in ni namenjen sistemom SCADA. Nastalo je že nekaj revizij, ki so omogočile na primer povezavo prek Etherneta in uporabo TCP/IP. Tudi MODBUS je odprt protokol, ki je dokaj preprost za implementacijo in omogoča preprosto komunikacijo med več napravami v omrežju (Byres 2004).

Slika 3.5 prikazuje sestavo IP-paketa v protokolu MODBUS TCP. IP-paket je, kot je običajno, sestavljen iz identifikatorja, fizičnega naslova, IP-naslova in podatkovnega okvirja. Slednji je sestavljen iz začetnega dela, naslovne oktave, funkcijskega navodila, podatkov, dveh oktav, ki zagotavljata preverbo integritete okvira, in končne oktave. Od običajnega okvira TCP se okvir MODBUS razlikuje v tem, da je veliko bolj preprost – ne vsebuje na primer informacij o portih.

Slika 3.1: IP-paket v protokolu MODBUS TCP



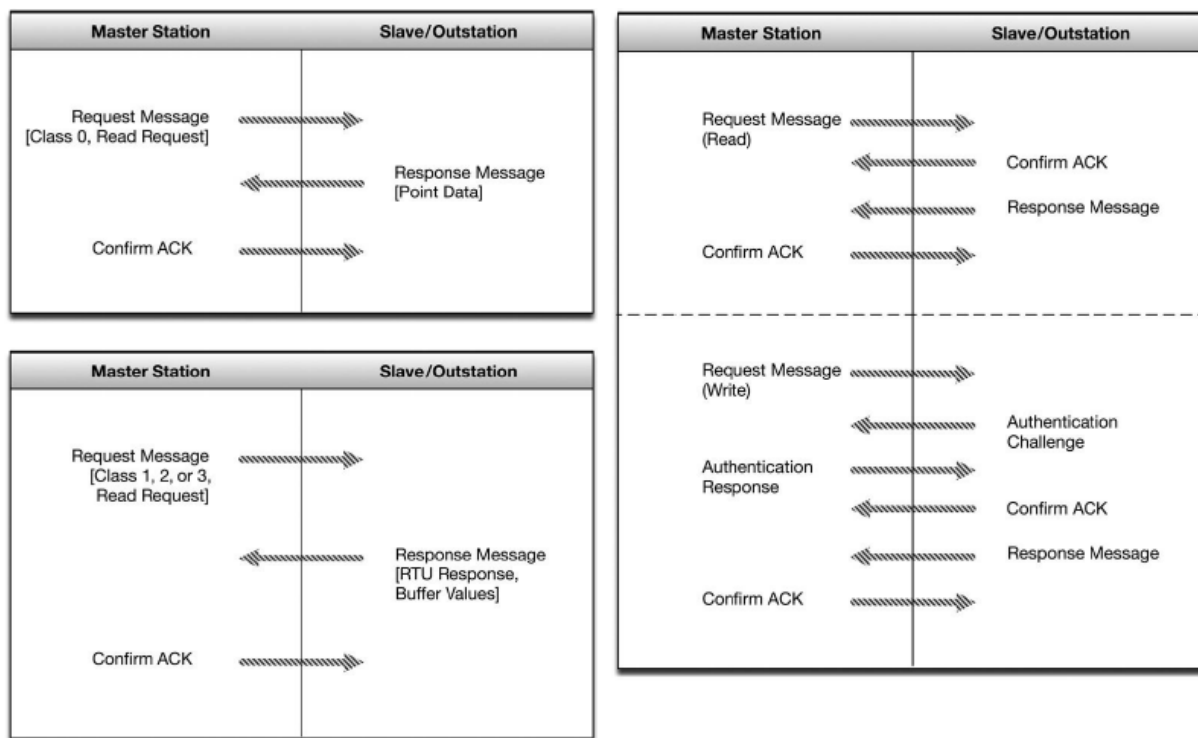
Vir: Knapp (2011, 59)

Poleg teh treh obstaja še več protokolov. Uporabljajo se lahko tudi protokoli, ki so vgrajeni v operacijske sisteme MS Windows ali Linux, npr. OLE in SSH, na splošno pa se delijo v modele fieldbus ali TCP/IP prek Etherneta. Pomemben je protokol Profibus podjetja Siemens, saj je bil prav za ta protokol osnovan črv Stuxnet (Krutz 2006, 44).

Večina teh protokolov ne ponuja nobenih varnostnih mehanizmov, kot je enkripcija ali avtentikacija, zato je ločitev omrežij toliko pomembnejša. Zaznamo lahko izjemo, protokol Secure DNP 3, ki za vsak ukaz zahteva avtentikacijo operaterja, vendar pa ta protokol pogosto ni implementiran, ker je procesorsko bolj zahteven. Slika 3.2 prikazuje delovanje nezavarovanega protokola in delovanje zavarovanega protokola DNP 3 v primerjavi z nezavarovanim protokolom. Pri slednjem gre za običajno sosledje prošnje, odziva in potrditve pri vzpostavitvi povezave, nato pa zahteve sistema gospodarja za sekvence, pošiljanja podatkov iz RTU-ja in potrditve sistema

gospodarja. Princip delovanja je podoben tudi pri zavarovanem protokolu, pri vzpostavljanju povezave se izvede še korak avtentikacijskega izziva.

Slika 3.2: Delovanje nezavarovanega protokola DNP 3 na levi in zavarovanega protokola DNP 3 na desni strani



Vir: Knapp (2011, 68–70)

3.6 Družbeni vidiki informacijske varnosti ter vrste napadov, usmerjene v uporabnike

Varnost informacijskih sistemov ni odvisna zgolj od tehničnih značilnosti. Medtem ko so parametri sistemskih nastavitev običajno nespremenljivi, smo uporabniki v varnostnih sistemih veliko bolj volatilna spremenljivka.

Pričujoče delo predpostavlja, da je v družbah, ki upravljajo elektroenergetsko kritično infrastrukturo, družbeni vir ogrožanja varnosti večji od tehničnega, torej da je nevarnost zunanega napada brez poznavanja določenih varnostnih mehanizmov manjša kot nevarnost, da je napadalec notranji ali pa da je pridobil določene občutljive informacije od nepozornega zaposlenega. Relevantna teorija kaže na to, da je t. i. najšibkejši člen v varnostnih sistemih človek (Janczewski in Colarik 2007, 173–228) ter da večino napadov izvedejo posamezniki, ki delujejo znotraj organizacije, ki jo napadajo (Gundert 2009, 25–27).

Po NIST je treba za izboljšanje družbene varnosti pri zaposlenih in uporabnikih izvajati naslednje kontrole:

- ob zaposlovanju je treba definirati položaj zaposlenih, pri čemer je treba ločiti potrebne zadolžitve od nepotrebnih in določiti zaposlenim najmanjši možen dostop, občutljivost položaja, ustrezen izborni proces ter izobraževanje in usposabljanje;
- ob administraciji zaposlenih in uporabnikov je treba izvajati upravljanje uporabniških računov, kar vsebuje zahteve, izdajanje in zapiranje uporabniških računov, nadzor uporabnikov in upravljanje teh funkcij, presoje in nadzor ter zaznavanje nepooblaščenih in nezakonitih dejavnosti;
- ob prekinitvi delovnega razmerja je treba upoštevati predvsem, ali je bila ta sporazumna ali ne. Če je bila sporazumna, je treba odstraniti pravice in privilegije, račune in avtentikacijska sredstva, prevzeti vse ključe, osebo seznaniti z vsemi njenimi nadaljnjimi odgovornostmi v zvezi z zasebnostjo in zaupnostjo, zagotoviti vračilo lastnine in dostop do podatkov, nad katerimi je imela ta oseba nadzor. Če je bila prekinitev nesporazuma, je treba dostop do vseh podatkov zaposlenemu nemudoma onemogočiti (Swanson in Guttman 1996, 27–30).

Poseben primer, ki ga je treba izpostaviti, so nezadovoljni uslužbenci, tudi bivši. Zaznamo lahko veliko primerov, v katerih so odpuščeni ali sicer nezadovoljni uslužbenci z dostopom do varnostno občutljivih podatkov in sistemov namerno povzročili veliko škodo. Tako lahko izpostavimo primer, v katerem je odpuščeni avstralski upravljavec sistema SCADA za ravnanje z odpadno vodo večkrat vdrl v sistem, vodo spustil v naravno okolje ter s tem povzročil veliko gospodarsko škodo in

pogin živali (Abrams in Weiss 2008) ali pa razvpiti primer Edwarda Snowdna, vrhunskega specialista za informacijsko varnost, zaposlenega v Ameriški agenciji za nacionalno varnost, ki je zaradi prepričanja, da je vohunjenje agencije za podatki ameriških državljanov in tujcev protiustavno, dokaze o tem dolgo zbiral, nato pa prebegnil v tujino in jih javno objavil.

Socialni inženiring

Medtem ko je mogoče, da napad izvede nezadovoljen trenutni ali bivši uslužbenec organizacije, je mogoče tudi, da zaposleni napadalcem nehote predajo občutljive informacije. Metoda psihološke manipulacije, s katero napadalec od žrtve pridobi informacijo, se imenuje socialni inženiring (Goodchild 2011, 2).

Običajne tehnike socialnega inženiringa so kraja gesel z ugibanjem⁷, pridobivanje zaupanja z različnimi prijateljskimi gestami, kraja identitete in pretvarjanje z namenom pridobitve gesel, informacij o računih, ključev, osebnih informacij, podrobnosti o sistemih in podobno. Napad ni cilj sam po sebi, temveč je sredstvo za doseg cilja, kot je finančna korist ali dostava zlonamerne programske kode (Mitnick 2002, 21–231).

Takšni napadi so dokaj razširjeni; ena izmed raziskav je pokazala, da je bila v zadnjih letih žrtev takšnega napada do polovica od 850 profesionalnih informatikov z vsega sveta. Najobičajnejši napad je t. i. phishing sporočilo, nato ponarejena stran socialnega omrežja. Najbolj ranljivi za napad so novi uslužbenci v organizacijah, nato podizvajalci, pomočniki vodstvenih delavcev, kadroviki, vodstveni delavci in informatiki. Ista raziskava je pokazala, da je zavedanje te nevarnosti visoko, da pa izvajajo varnostno usposabljanje za takšno nevarnost v manj kot tretjini organizacij. (Dimensional research 2011)

Proti takšnemu napadu se je mogoče zavarovati le s stalnim usposabljanjem in ozaveščanju zaposlenih. Po besedah svetovno znanega hekerja in tvorca besedne zveze socialni inženiring v tem pomenu Kevina Mitnicka na svetu ne obstaja tehnologija, ki bi lahko preprečila takšen napad (Mitnick 2002, 232).

⁷ Znan primer je kraja gesla za socialno omrežje Twitter in e-pošto ameriške guvernerke Sarah Palin, ki so ga napadalci pridobili tako, da so uganili odgovor na varnostno vprašanje za izgubljeno geslo, ki ga je nastavila žrtev (Goodchild 2011, 2)

Ribarjenje

Ribarjenje oz. phishing napad je napad, ki uporabi elemente socialnega inženiringa in ima tri značilnosti: posnemati mora varen oz. zaupanja vreden vir, vsebovati mora povezavo do dejanske spletne strani in zahtevati mora občutljive podatke (Ramzan 2010, 434). Tipičen primer napada je posnemanje elektronskega sporočila spletne banke, ki uporabnika obvesti, da mora za dostop do svojega bančnega računa spremeniti geslo s povezavo do spletne strani, ki je kopija spletne strani banke. Uporabnik bo tako izvajalcem napada dal podatke za dostop do svojega bančnega računa, vključno z geslom za dostop do spletne banke.

Izvajalci napada lahko uporabijo ugrabljene strežnike tako za pošiljanje sporočil kot za posnemanje spletnih strani. Teh jim ni treba graditi, saj obstajajo orodja, ki imajo kopije teh strani že vgrajene, kopije pa je treba le naložiti. Vsa sredstva za takšen napad je mogoče najeti (Ramzan 2010, 435).

Učinkoviti načini varovanja pred takšnimi napadi so večfaktorska avtentikacija, filtriranje e-pošte, orodja proti ribarjenju, SSL, analitika ozadja (Ramzan 2010, 442–447) ter varnostno ozaveščanje uporabnikov.

3.7 Nekateri znani napadi na energetske ključno infrastrukturo

Arhiv industrijskih varnostnih incidentov⁸ v svoji analizi incidentov v nadzornih sistemih in sistemih SCADA ugotavlja, da je bila med leti 1982 in 2010 sestava incidentov takšna:

- 50 odstotkov incidentov je bilo nesreč;
- 30 odstotkov incidentov je povzročila zlonamerna programska koda;
- 11 odstotkov incidentov so povzročili zunanji napadalci;
- 9 odstotkov incidentov so povzročili notranji napadalci. (Byres 2012, 1)

Ugotovimo lahko, da je polovica vseh incidentov povzročena namerno. Poleg v uvodu omenjenega Stuxneta sledi nekaj nazornih primerov kibernetских napadov na energetske infrastrukturo.

Eksplodija sibirskega plinovoda leta 1982

⁸ RISI, dostopno prek www.securityincidents.org.

Leta 1981 je polkovnik direktorata, zadolženega za pridobivanje zahodne tehnologije, Vladimir Vetrov, zaradi razočaranja nad razmerami v ZSSR poslal francoski obveščevalni službi veliko zbirko podatkov, povezano z industrijskim vohunstvom Sovjetske zveze. Med drugim je zbirka vsebovala imena 250 KGB-jevih agentov, zadolženih za pridobivanje zahodne tehnologije, ter seznam tehnologij, ki jih je KGB želel pridobiti. To zbirko podatkov je po informacijah tedanjega direktorja ameriške obveščevalne agencije francoski predsednik Mitterand osebno predal ameriškemu predsedniku Reaganu, kar je vodilo v obširno protiobveščevalno akcijo obveščevalno-varnostnih agencij NATA (Weiss 2007). Po pričanju tedanjega direktorja CIE je to povzročilo sledenje KGB-jevim agentom; ti so pridobivali programsko kodo od kanadskega programerskega podjetja, ki je kodo dobavljal za krmiljenje sistemov za nadzor plinovodov. Agenti CIE naj bi v kodo dodali ukaze, ki bi po daljšem obdobju ustreznega delovanja poškodovali turbine, črpalke in valje (The National Security Archive 2013). Ta logična bomba je po Reedovemu pričevanju povzročila na Ruskem sibirskem plinovodu junija 1982 eksplozijo z močjo treh kiloton TNT-ja, ki je uničila velik del plinovoda.

Aurora

Septembra 2007 so raziskovalci v raziskovalnem centru Ameriškega ministrstva za energijo⁹ izvedli nadzorovan poskus, v katerem so po poročanju ameriške novinarske družbe CNN simulirali hekerski napad na kontrolni sistem elektrarne. Napadalci so izkoristili varnostno luknjo v zasnovi nadzornega sistema, spremenili delovni cikel testnega generatorja in s tem povzročili njegovo »tresenje, kajenje in nato zaustavitev« (Meserve 2007). Simulacija je bila izvedena z namenom prikazati, kakšno moč imajo lahko kibernetiski napadi na elektroenergetsko infrastrukturo. CNN-ov članek pa navaja, da se strokovnjaki bojijo, da bi lahko dejanski večji in koordinirani napadi povzročili »škodo, ki bi jo popravljali mesece«. NERC je še leta 2010, tri leta po izvedenem eksperimentu in prikazu varnostne luknje, izdala dodatne smernice za preprečitev takšnega dogodka. Nekateri nadzorni sistemi še danes niso ustrezno zavarovani pred tem napadom (Knapp 2011, 37).

Stuxnet

⁹ U.S. Department of Energy

Stuxnet se je začel širiti prek okolja MS Windows z uporabo štirih hkratnih napadov na ničti dan¹⁰. Programski paket je bil velik 500 KB in je bil tako eden izmed največjih, ki so jih kdaj uporabljali. Poleg tega je bil spisan v več programskih jezikih, opremljen pa je bil tudi s ponarejenimi certifikati WHQL za gonilnike za strojno opremo, ki so jih napadalci ukradli od podjetij JMicron in Realtek (Matrosov in drugi 2010, 11–14). Tako je napad ostal nezaznan. Dve spletni strani na Danskem in v Maleziji sta bili uporabljeni kot centra za vodenje in nadzor nad programsko opremo ter za posodabljanje (prav tam: 24).

Črv je ob okužbi napadel ključno komunikacijsko knjižnico, imenovano s7otbxdx.dll, ki skrbi za komunikacijo med PLC-ji v sistemu SCADA in operacijskimi sistemi MS Windows. Originalno knjižnico je preimenoval in na to mesto postavil svojo knjižnico. Tako je nadomestna knjižnica skrbela za pretok informacij med sistemi za nadzor in logičnimi kontrolerji (Falliere in drugi 2011, 48).

Stuxnet je bil usmerjen v sisteme Siemens S7-300, motorje centrifug, črpalk in podobno, ki delujejo na določenih razponih obratov. Parametre je spremenil tako, da so motorji delovali na nepravilnih obratih, hkrati pa je v nadzorne sisteme pošiljal telemetrijske podatke, ki so bili prikazani kot pravilni. Napad naj bi tako lahko uničil centrifuge zaradi pretiranih vibracij.

Flame

Virus Flame, poznan tudi kot Skywiper, je virus, katerega obstoj je maja 2012 objavilo rusko podjetje Kaspersky (Kaspersky Lab 2012). Poročilo navaja, da gre za najkompleksnejši virus v zgodovini, njegov namen pa je zbiranje podatkov.

Flame se lahko širi prek omrežja LAN ali prek USB-ključkov in je za računalniški virus nenavadno velik, večji od 20 MB. Po okužbi sistema omogoča, da se naložijo še dodatni moduli. Uporablja pet različnih šifrirnih metod in bazo podatkov SQLite za shranjevanje strukturiranih podatkov. Napad je neviden, saj moduli programa niso prikazani kot procesi, njegove spominske strani pa so zaščitene pred branjem, pisanjem in izvajanjem ter zato nedostopne. Flame uporablja podobne ranljivosti kot Stuxnet, ob napadu pa preveri, katera protivirusna oprema je nameščena na računalnik in temu prilagodi svoje obnašanje. Podpisan je z lažnim certifikatom

¹⁰ Do takrat je bil to prvi napad, ki je uporabil štiri hkratne ranljivosti na ničti dan (Zetter 2010).

Microsoft PCA (Skywiper analysis team 2012, 9–57). Po tem, ko so mediji objavili njegov obstoj, je Flame iz kontrolnih sistemov prejel ukaz za izbris programa in kakršnihkoli sledi, da je na sistemu kdaj obstajal (BBC 2012).

V nasprotju s Stuxnetom namen Flama ni povzročanje neposredne škode, pač pa zbiranje podatkov. Virus je zmožen snemanja zvoka, zbiranja sekvenc tipk na tipkovnici, zajemanja slik z zaslona ter shranjevanja in prenašanja risb Autocad, PDF-, besedilnih dokumentov itd. (Skywiper analysis team 2012, 9–57)

Tako kot Stuxnet je tudi Flame ter še nekateri drugi virusi verjetno proizvod ameriških in izraelskih varnostno-obveščevalnih služb¹¹.

3.8 Zlonamerna programska koda in kibernetiki viri ogrožanja elektroenergetske kritične infrastrukture

Publikacija NIST-a Uvod v računalniško varnost razdeli običajne grožnje računalniški varnosti v naslednje kategorije:

- napake in opustitve dolžnega ravnanja;
- goljufije in kraje;
- sabotaza zaposlenih;
- izguba fizične in infrastrukturne podpore;
- zlonamerni uporabniki (hekerji);
- industrijsko vohunjenje;
- zlonamerna koda;
- vohunjenje tujih držav in
- grožnje zasebni varnosti (Gutmann in Roback 1995, 21–29).

Te kategorije lahko glede na funkcionalnost razdelimo na strojne, človeške, in programske, glede na namen pa na zlonamerne napade ter napake in nesreče. Opredelili smo že strojne komponente in njihove ranljivosti, v nadaljevanju pa bomo opredelili še zlonamerno programsko kodo ter nevarnosti, ki izhajajo iz uporabnikov.

Taksonomija zlonamerne programske kode

¹¹ Glej npr. Naughton 2012, Sanger 2012, Zetter 2012.

Vrst zlonamerne programske kode je več. Erbschloe na primer vrste takšnih programov razdeli v e-poštne in druge viruse, trojanske konje in druge kode, ki delujejo po principu zadnjih vrat, črve, združene oz. zmešane grožnje, časovne bombe, spyware, adware in stealware. Izpostaviti je treba, da očitno akademskega konsenza glede taksonomije zlonamerne programske opreme ni. Številne gospodarske družbe, ki se ukvarjajo s kibernetiko varnostjo, imajo svoje sezname vrst zlonamerne programske opreme, različno pa jo navajajo tudi nekateri znanstveni viri. Najpogostejše omenjeni tipi so virusi, trojanski konji, črvi, adware in spyware. Sledi seznam zaznanih vrst zlonamerne programske opreme in njihov opis.

Zlonamerna programska oprema se lahko namesti, kadar obstajajo naslednje komponente:

- masovni spomin (trdi diski);
- RAM;
- procesor ali primerljiva naprava;
- operacijski sistem.

Zlonamerna programska koda se lahko namesti in zaganja kot viden proces, skriti proces ali kot stalen proces. V primeru operacijskega sistema MS Windows se te vrste programov med seboj razlikujejo tako, da je viden proces uporabniku viden, kadar odpre seznam procesov in ga v tem seznamu lahko tudi prekine, skriti proces pa ni viden, bodisi je vključen v kak drug proces bodisi je vključen v rootkit. Ti procesi so skriti tudi pred protivirusnim programom. Stalen proces je najtežje odstraniti, saj se tudi po deinstalaciji ali odstranitvi ponovno naloži iz različnih virov. Ti so skriti v sistemskih mapah in registrskih ključih, ki zaženejo program ob zagonu sistema (Filiol 2010, 749)

Virusi

Računalniški virus je program, ki je sposoben samostojne replikacije in izvajanja nelegitimne kode, kot je spreminjanje parametrov programa ali sistema in sklic na drugo datoteko ali program. Virus mora za takšno dejanje pridobiti ustrezne pravice, zato je običajno priložen zagonski datoteki, ki je lahko tudi del običajnega programa. Če uporabnik zažene zagonsko datoteko, se virus zažene hkrati s tem. Širi se lahko na dva načina: lahko takoj začne iskati druge gostitelje, jih okuži, ko jih najde in

prenese uporabniške pravice nanje, ali pa se takoj zapiše v spomin gostiteljevega sistema, ostane aktiven v ozadju in se širi ob zaganjanju posameznih datotek. Sodobni virusi so sposobni onemogočiti datoteke z definicijami virusov protivirusnih programov, ob širjenju pa se lahko tudi spremenijo, zato jih je težje prepoznati (Jancziewski in Colarik 2007 in Total defense 2013).

Običajno imajo računalniški virusi tri komponente:

- replikacijski mehanizem, ki omogoča virusu razširjanje med posameznimi sistemi;
- sprožilec, ki izvede replikacijski mehanizem oziroma nalogo;
- nalogo, ki je običajno sprememba datotek ali nastavitev v računalniškem sistemu ali pa drugačna povzročitev škode na gostiteljskem sistemu (Erbschloe 2005, 19).

Erbschloe (prav tam) razdeli računalniške viruse v naslednje skupine:

- virus zagonskega sektorja sistema, ki se zapiše v glavni zagonski zapis sistema in se tako izvede vsakič, ko se naloži operacijski sistem računalnika. Takšen virus se sicer načeloma ne razširja prek omrežja, se pa zapiše v vsak zapisljiv premični medij, ki ga vstavimo v računalnik;
- virus, ki briše podatke; običajno so to vnaprej določeni podatki, ki jih virus ob okužbi poišče in zbriše;
- virusi, ki okužijo določene datoteke. Te so najpogostejše zagonske datoteke (končnice .exe, .bat ali .com), knjižnice (.dll) ali določena grafična, video-, glasbena in podobna vsebina;
- makro virusi, ki se širijo prek makro navodil v programskih orodjih MS Office. Ti virusi so del besedilnih ali podatkovnih datotek in se širijo z njihovo uporabo na različnih sistemih;
- e-poštni virusi, ki se širijo prek e-poštne odjemalcev. Ko se računalnik okuži, poštni odjemalec pošlje e-poštno sporočilo z virusom vsem stikom, zapisanim v imeniku. Takšni virusi se širijo z izjemno hitrostjo in lahko preobremenijo poštne strežnike;

- polimorfni nevidni virusi, ki spremenijo obliko vsakič, ko okužijo različen sistem. Te viruse je nemogoče odkriti s protivirusnim programom, ki deluje na osnovi baz znanih napadov;
- lažni virusi; ti so običajno osnovani kot lažna obvestila o virusih, ki se razpošljejo prek distribucijskih seznamov in od uporabnikov zahtevajo, naj o tem obvestijo še druge ljudi;
- virusi, ki okužijo sistem s socialnim inženiringom, ki uporabnika z lažnim obvestilom prisilijo v to, da odpre določeno povezavo ali potrdi zahtevo, ki potem okuži sistem;
- kombinacija teh vrst virusov.

Črvi

Črvi so druga vrsta zlonamerne kode, ki je sposobna samostojne replikacije, vendar pa za razliko od virusa za to ne potrebuje gostiteljske datoteke in je tako samostojen program. Medtem ko se virusi širijo na gostiteljskem sistemu in omrežju, se črv širi po omrežjih prek standardnih protokolov. Gostiteljski sistem se lahko s črvom okuži brez posredovanja uporabnika; ta samostojno vdre prek napak v zasnovi sistema ali pa ga nevede zažene uporabnik. Čeprav črv lahko izvaja podobne funkcije kot virus, je njegov namen predvsem zbiranje informacij o aktivnostih strežnika in mrežnem prometu ter posredovanje teh informacij njegovemu izdelovalcu (Jancziewski in Colarik 2007 in Total defense 2013).

Črve lahko razdelimo na:

- preproste (I-črve), ki za svojo širitev izkoristijo varnostne luknje v aplikacijah ali omrežnih protokolih;
- makro črve; to so hibridni programi, združeni črvi za prenašanje prek omrežja in virusi za dostavo kode. Odprtje dokumenta, ki je na primer pripet v e-poštnem sporočilu tako okuži e-poštno aplikacijo (virus), ta aplikacija pa nato avtomatično razpošlje ta dokument vsem stikom v imeniku (črv);
- e-poštni črvi, namenjeni izključno širjenju prek e-poštnih sporočil, bodisi zaradi napake uporabnika bodisi zaradi ključne varnostne pomanjkljivosti e-poštnega odjemalca.

Črv je zmožen izjemno hitre replikacije in razpošiljanja. Črv z imenom CodeRed je na primer v petih urah in pol okužil 400.000 MS spletnih strežnikov (Filiol 2010, 755–757).

Trojanski konji

Trojanski konj je program, ki je zasnovan tako, da izvede legitimno funkcijo, hkrati pa tudi nepoznano oziroma nezaželeno dejanje. Tako lahko trojanski konj sistem okuži z virusom ali namesti neželen program, kot je na primer keylogger, in tako pridobiva podatke. Lahko tudi ustvari zadnja vrata, prek katerih lahko napadalec prevzame nadzor nad sistemom. Trojanski konj se lahko zažene le z dejanjem uporabnika, njegova dejanska funkcija pa je razkrita šele z njegovo uporabo (Whitman in Mattord 2011, 48).

Boti in botneti

Bot, okrajšava za besedno zvezo spletni robot, je programska aplikacija, ki prek interneta izvaja avtomatizirane dejavnosti. Te so običajno preproste in ponavljajoče se, izvaja pa jih lahko bistveno hitreje in učinkoviteje kot človek. Običajna uporaba je legitimna, saj se uporablja za indeksiranje spletnih strani, lahko pa se uporablja tudi zlonamerno. Običajno boti, povezani v mrežo, izvajajo napade DDoS ali krajejo podatke (Symantec Corporation 2013).

Mreže botov, botneti, so dokaj nov, težje zaznaven način za dostavo znane zlonamerne programske kode. Botnet je zlonamerna mreža okuženih sistemov, imenovanih tudi zombijev, ki so se okužili z zlonamerno programsko kodo. Uporabniki teh sistemov ne vedo, da so njihovi računalniki okuženi, saj ti delujejo kot običajno. Napadalec, imenovan tudi pastir, te sisteme organizira v mrežo na enak način, kot bi organiziral običajno mrežo. Zombiji so lahko razpršeni po vsem svetu in lahko med sabo komunicirajo, velikost botneta pa je lahko od nekaj sto do več milijonov sistemov (Filiol 2010, 756–758).

Botneti se uporabljajo za obširne napade, kakršni so napadi DDoS, širjenje spama, kraja podatkov, gostovanje lažnih spletnih strani in večfazni napadi (Filiol 2010, 759).

Vzpostavitev zadnjih vrat

Zadnja vrata so način vdora v gostiteljski sistem. Virus ali črv nastavi sistemsko komponento, ki dovoljuje napadalcu, da dostopa do sistema s posebnimi poverilnicami. Napadalec tako lahko izvaja napade mimo varnostnih sistemov. (Whitman in Mattord 2011, 49).

Polimorfna zlonamerna programska oprema

Polimorfna programska oprema je takšna, da nenehno menja način, na katerega se prikazuje protivirusnim programom, zato je varnostni sistemi, ki delujejo na podlagi prepoznavanja znanih napadov, ne morejo zaznati. Ti programi se izogibajo zaznavi tako, da spreminjajo svojo velikost in zunanje datotečne karakteristike (Whitman in Mattord 2011, 50).

Vohunska programska oprema

Ta pojem, po angleško spyware, uporabljamo za določitev računalniške tehnologije, ki zbira informacije o organizaciji ali posamezniku brez njegove privolitve ali vedenja. Na gostiteljski sistema se namesti kot del virusa ali kake sicer ustrezne aplikacije ali pa z uporabo prevare uporabnika. Za razliko od virusov in črvov se vohunska programska oprema ne širi sama, po namestitvi pa zbira podatke o vedenju uporabnika, na primer pritisnjenih tipkah, obiskanih spletnih straneh, shranjenih geslih in podobno. Informacije, ki jih program zbira, se uporabljajo predvsem za marketinške namene, za osebno profiliranje uporabnika, pa tudi za industrijsko vohunjenje (Erbschloe 2005, 25).

Oglaševalska programska oprema

Ta termin, po angleško adware, označuje programsko opremo, ki ob uporabi samodejno oddaja oglase. Njen namen je, da njen izdelovalec prek uporabe aplikacije služi denar. Sama po sebi je oglaševalska programska oprema nenevarna in celo legitimna oblika izdaje programske opreme, ki je tako za uporabnika cenejša, kot bi bila sicer, ali celo brezplačna. Vendar se pogosto združuje z vohunsko programsko opremo, ki omogoča, da so oglasi, ki se pojavljajo na uporabnikovem sistemu, namenjeni prav za uporabnika (Erbschloe 2005, 27).

Keylogger

Keylogger je programska oprema, ki omogoča napadalcu, da zapisuje sekvence pritiskov gumbov na tipkovnici tarče. Glede na tehničen način delovanja obstaja 6 vrst keyloggerjev:

- hipervizorski keylogger, ki deluje pod nivojem operacijskega sistema, in sicer kot virtualna naprava;
- jedrni keylogger, ki deluje v povezavi z rootkitom in je prikazan kot gonilnik za tipkovnico ter ga je zelo težko odkriti;
- keylogger, osnovan na API, ki deluje kot ukaz v operacijskem sistemu in zbira podatke kot samostojna aplikacija. Takšen keylogger porabi precej sistemskih sredstev in ga je najlažje odkriti;
- keylogger, osnovan na prestrezanju obrazcev, ki preverja vpisovanje v obrazce, predvsem spletne;
- keylogger, osnovan na injekciji v spomin, ki spremeni tabele delovnega spomina in tako omogoča keyloggerju, da zaobide funkcijo operacijskega sistema Windows, ki zahteva za vsako spremembo sistema odobritev uporabnika;
- keyloggerji, ki analizirajo pakete in tako prestrezajo nešifriran paketni promet prek protokola http.

Keyloggerji so pogosto obvladovani z oddaljene lokacije in največkrat pošiljajo podatke neposredno na to lokacijo (Pctools 2013).

Logične bombe

To je zlonamerna koda, ki je do določene časovne točke, dejanja ali do izpolnitve kakega drugega pogoja neaktivna, nato pa se izvede. Logična bomba je običajno del virusa ali trojanskega konja, njen namen pa je, da pred izvedbo napada neopazno okuži čim več sistemov. Logične bombe se pogosto uporabljajo kot sredstvo za izsiljevanje (Erbscloe 2005, 25).

Rootkit

Rootkit je prikrit tip zlonamerne programske opreme, ki deluje tako, da pred običajnimi metodami ugotavljanja prikriva določene procese ali aplikacije, na primer spyware. Program na sistemu pridobi administratorske pravice, nato pa prilagodi obstoječo programsko opremo, tudi protivirusne programe. V nasprotju z večino

drugih vrst programske opreme je odkrivanje in odstranjevanje rootkita skoraj nemogoče, še posebej če je nameščen v jedru operacijskega sistema. Če gre za rootkit firmwara, pa je mogoča odstranitev le z zamenjavo strojne opreme. Rootkiti lahko gostiteljski sistem uporabijo tudi za napad na druge sisteme, ne da bi uporabnik za to vedel.

Programska oprema za izsiljevanje in krajo, cryptolocker

Med letoma 2012 in 2014 zelo razširjena oblika zlonamerne programske opreme spada v skupino t. i. ransomwara oziroma programske opreme za izsiljevanje. Ta se razdeli v dve podskupini: na eno, ki šifrira datoteke, in drugo, ki jih ne, pri čemer je prva bistveno nevarnejša za organizacije. Takšna vrsta zlonamerne programske opreme ni nova. Prvi primeri takšnih programov so se pojavili še pred letom 1990, a v zadnjem času so ti napadi pogostejši; napadalcem namreč omogočajo, da si s takšnimi napadi pridobijo precejšnjo materialno korist. Škoda, ki jo je povzročil najbolj razširjen primer takšnega napada, t. i. cryptolocker, ni znana, vendar jo lahko ocenimo na več kot 10 milijonov evrov, res pa je, da so gospodarske družbe, ki se ukvarjajo z varnostjo informacijskih sistemov, popravile hevristične algoritme v svojih aplikacijah, zato se grožnja takih programov zmanjšuje.

Napad deluje tako, da se gostiteljski sistem okuži s trojanskim konjem; ta nanj namesti programsko kodo, ki začne šifriranje datotečnega sistema oz. shranjenih datotek, do katerih ima uporabnik pravico zapisovanja z zelo močnim, 2048-bitnim ključem. To ne velja samo za gostiteljski sistem, pač pa za vse datoteke v organizaciji. Nekatere različice cryptolockerja so bile pisane tudi specifično za določene vrste diskovnih polj, priklapljenih na omrežje (Hruska 2014). Ko program zaključi šifriranje datotek, se uporabniku prikaže pogovorno okno z informacijami, da so bile njegove datoteke šifrirane z navodili, da mora na določen način¹² plačati določen znesek. Če to stori, mu napadalci pošljejo ključ za dešifriranje datotek in aplikacijo za dešifriranje.

O uspešnosti napada pričajo podatki raziskave univerze v Kentu, v kateri je 41 % uporabnikov, ki so se okužili s cryptolockerjem, odgovorilo, da so plačali odškodnino, napad pa jih je doživelo okoli 10 % (Boiten in Hernandez-Castro 2014).

¹² Običajno z uporabo t. i. bitcoinov, plačanih prek omrežja TOR.

Izogibanje zaznavi

Z razvojem protivirusnih programov in požarnih zidov se je razvila tudi sposobnost zlonamerne programske kode, da se prilagodi tehnikam teh programov in jih zaobide.

Zlonamerna programska oprema za ta namen uporablja tri tehnike:

- nevidnost oz. prepričevanje gostiteljskega sistema in njegovih varnostnih mehanizmov, da zlonamerne programske kode ni. To lahko doseže s skrivanjem v sektorjih, ki jih operacijski sistem ne uporablja in ki jih tudi protivirusni program ne nadzoruje, ali z rootkiti;
- polimorfnost oz. stalno spreminjanje podobe kode z namenom, da preslepi protivirusne programe, ki uporabljajo za zaznavo sezname obstoječe zlonamerne kode. Polimorfnost se lahko doseže s prepisovanjem kode z identičnimi, a drugače zapisanimi ukazi ali z dopisovanjem naključnih in nepomembnih ukazov, pa tudi z drugimi načini;
- ovijanje kode; koda se lahko tudi zakrije s šifriranjem, dekompresijskimi tehnikami in načrtnim kompliciranjem kode, z namenom zakasnitve ali preprečitve analize kode, ki jo izvajajo protivirusni programi, ali s poskusom napada protivirusnih programov z deinštalacijo, onemogočenjem ali preobremenitvijo (Filiol 2010, 758–761).

3.9 Vektorji in vrste napadov

DoS in DDoS

Napad DoS pomeni onemogočanje žrtvi ali uporabniku, da bi dostopala do določene storitve ali sistema tako, da se preobremeni sistem ali povezava med sistemom in uporabnikom s stalnim pošiljanjem zahtev ali paketov žrtvi. Namen napada ni uničenje sistema, temveč njegovo začasno onemogočenje. Obstajata dve poglavitni vrsti napadov DoS: takšni, ki preobremenijo storitve, in takšni, ki jih zaustavijo, napad pa se izvede na računalniške vire¹³, konfiguracijo informacij, stanje informacij, fizične mrežne komponente in komunikacijske kanale. Napad pogosto spremlja tudi dostava zlonamerne programske opreme, vir napada pa je običajno zavarovan s ponarejenim IP-naslovom. (Singh 2005).

¹³ Npr. diske, procesorske storitve, pasovno širino ...

Napad DDoS je združen napad na žrtev iz več virov, ki so običajno povezani v botnet. Napad je tako učinkovitejši, napadalca pa je težje odkriti.

Napad je mogoče preprečiti s pravilno vzpostavitev sistema oz. mreže. Prvi način preprečitve napada je omejitev sredstev, ki jih lahko določena vrsta prometa uporabi. To sicer prepreči napade, vendar pa lahko močno omeji promet, ki je sicer legitimen. Drugi način je preusmerjanje zlonamernega prometa v navidezen vmesnik, ki promet opusti. Takšen način preprečevanja napada sicer deluje, vendar še vedno porabi precej sredstev. Pravilna nastavitve sistema naj bi zlonameren promet enostavno opustila oziroma zablokirala. Sodobna strojna oprema ima ustrezne varnostne mehanizme že vgrajene (Tanase 2003).

Injekcija kode

Injekcija kode je termin, ki ga uporabljamo za opis napada, v katerem napadalec napadenemu sistemu pošlje kodo, ki jo ta nehote zažene. Takšni napadi so raznovrstni; eden od njih je pošiljanje skripte na spletno stran, običajno prek JavaScript, in sicer tako, da napaden strežnik zažene skripto, ki mu jo pošlje napadalec. Druga vrsta injekcije je injekcija SQL; napadalec lahko dostavi element SQL v strežnik, in če administrator strežnika ne validira stalno, se lahko ta SQL zažene in tako napadalcu omogoči zajem in spremembo podatkov, vzpostavitev administratorskih računov ipd. Možnih injekcij je še veliko, omejiti ali onemogočiti pa jih je vedno mogoče s pravilnim kodiranjem baz ali z orodji za njihovo zaščito (Austin 2010, 771–775).

Preplavljanje medpomnilnika

Med letoma 1995 in 2005 je bila največja nevarnost za informacijske sisteme napad, imenovan preplavljanje medpomnilnika¹⁴. Najbolj razširjeni programski jeziki proti tem napadom nimajo vgrajenih varnostnih mehanizmov, je pa takšen napad za napadalca relativno lahko izvesti. Cilj takšnega napada je podreditev privilegiranega programa. Napadalec prevzame nadzor nad njim in s tem tudi nad gostiteljskim sistemom (Cowan 1999).

¹⁴ Buffer overflow

Podreditev napadalec doseže tako, da preplavi medpomnilnik programa in povzroči, da ta prekorači svoje meje ter išče vire na drugih točkah spomina. Napadalec ob takšnem napadu spremeni parametre v okolici medpomnilnika tako, da ti vsebujejo ukaz, naj program dostopa do kode, ki jo je napadalec dodal ali pa zlorabil za namene prevzema sistema. Program tako začne izvajati neželene ukaze in povzroča napake, nedelovanje sistema ali pa kršitve varnosti sistema (Cowan 1999).

Danes večina programskih okolij vsebuje varnostne mehanizme za preverjanje izvajanja kode, ki preprečujejo tovrstne napade, vendar pa so bili ti pred desetletjem zelo nevarni in razširjeni. Eden izmed bolj znanih napadov je bil črv SQL slammer, ki je januarja 2003 za nekaj ur bistveno upočasnil celoten spletni promet, izrabil pa je varnostno pomanjkljivost v strežnikih MS SQL, za katero je podjetje Microsoft že izdalo popravek, a na številnih sistemih ta ni bil nameščen (BBC 2003).

Elektronska pošta

Najpogostejši način dostave zlonamerne programske kode je elektronska pošta. Poročila ugotavljajo, da po celotnem svetovnem spletu na mesec zaokroži več kot devet milijard elektronskih sporočil, od tega pa jih kot napade lahko opredelimo več kot 80 % (Bernik in Prislan 2012, 56). Kot ugotavlja poročilo enega izmed vodilnih svetovnih podjetij za informacijsko varnost McAfee (Mcafee 2011), lahko na primer ugotovimo, da je isti napadalec med letoma 2006 in 2011 na enak način napadel vsaj 72 organizacij, in sicer tako, da so zaposlenim v tej organizacij poslali elektronsko pošto s priponko. Ko so jo ti odprli, se je namestila programska oprema za oddaljen dostop do sistemov v organizacijah.

Podobno je bila uporabljena neželena elektronska pošta za dostavo trojanskega konja, imenovanega ZEUS, ki je deloval po principu keyloggerja in je v letu 2009 na več kot 10.000 okuženih računalnikih po vsem svetu zbiral podatke o uporabniških imenih, geslih, kreditnih karticah in podobnem. Programska oprema je bila na voljo za prodajo, njena cena pa je bila med 3000 in 4000 ameriški dolarji (Bernik in Prislan 2012, 58).

Napadi, značilni za nadzorne sisteme

Značilnost sistemov, kot so sistemi ICS in SCADA, je, da za izvajanje nadzora uporabljajo logične kontrolerje, ki niso računalniški sistemi, temveč le programabilne

točke. Ti predstavljajo precejšnjo nevarnost, če so fizično zajeti, saj lahko napadalec s takšnim dejanjem zagotovi ugotovitev načina delovanja omrežja, vključno z varnostnimi protokoli. Ta nevarnost je še posebej velika, če gre za točke, ki so povezane v brezžično mrežo. Proti takšnim napadom je seveda učinkovita fizična varnost, poleg tega pa čim manjša verjetnost, da si točka deli varnostne ključne s sosednjimi točkami. (Kifayat in drugi 2010, 527).

Še ena nevarnost za takšne sisteme je napad z vzporednim kanalom, ki v brezžičnem omrežju meri nihanja v signalih in tako s posebnimi protokoli omogoča razpoznavanje šifriranja in prenesenih podatkov. Proti takšnim napadom se je mogoče boriti z vzpostavitvijo naključnih nihanj v porabi električne energije, frekvenc procesorjev ter s pošiljanjem lažnih ukazov, razdeljenih ukazov in podobno (Kifayat in drugi 2011: 528).

3.10 Tehnični sistemi za izboljšanje informacijske varnosti

Nadzor dostopa

Nadzor dostopa zagotavlja, da do sistema dostopa za to pooblaščen oseb, storitev ali proces, ne pa tudi nepooblaščen. Razdelimo ga lahko v tri sklope: identifikacijo, avtentikacijo in avtorizacijo. Identifikacija je vzpostavitev identitete, avtentikacija pa potrditev, da je identiteta pravilna. Identifikacija in avtentikacija sta dejavnosti, ki ju uporabnik izvede proti gostiteljskemu sistemu, avtorizacijo pa izvede gostiteljski sistem proti uporabniku, kar pomeni, da mu odobri dostop (Dulaney in Easttom 2014).

Priporočljiva je avtentikacija z dvema mehanizmoma. Možni mehanizmi so trije:

- nekaj, kar posameznik ima, na primer certifikat;
- nekaj, kar posameznik je, na primer biometrični podatki;
- nekaj, kar posameznik ve, na primer geslo (Ramzan 2010, 442).

Sistem za zaznavanje vdora in protivirusni sistem

Eden izmed pomembnejših varnostnih mehanizmov za informacijske sisteme, tudi za sisteme SCADA, je sistem zaznavanja vdora. Sestavljen je lahko iz strojne opreme, programske opreme ali iz obeh komponent, deluje pa tako, da analizira aktivnost na gostiteljskem sistemu ali omrežju in zaznava zlonamerne dogodke, ki bi lahko

negativno vplivali na razpoložljivost, celovitost oziroma zasebnost omrežja ali računalnika. Sisteme za zaznavanje vdora lahko razdelimo po naslednjih merilih: glede na to, ali so osnovani na omrežju ali na gostiteljskem sistemu, glede na to, ali so aktivni ali pasivni, ali zaznavajo znane napade ali samo anomalije (Scarfone in Mell 2007, 9–127).

Sistemi, osnovani na omrežju, so običajno pasivni sistemi, ki nadzorujejo določen segment omrežja tako, da prestrežajo in ocenjujejo podatkovne pakete ter preprečujejo, da bi neprimerni paketi prišli do gostiteljskih računalnikov. V primeru velike obremenitve omrežja takšen sistem lahko ne bi prestregel vseh paketov in zato ne bi mogel nujno preprečiti napada. Takšen sistem prav tako ne bi mogel preprečiti in ustaviti šifriranega paketa, poleg tega pa ne more oceniti rezultata napada, čeprav ga zazna, zato je vsakič, ko sistem zazna napad, potrebno ročno ukrepanje osebja.

Sistemi, osnovani na gostiteljskem sistemu, zaznavajo in analizirajo informacije na posameznem računalniku, zato je mogoče od njih pridobiti več informacij o dogodkih, mogoče pa je tudi oceniti posledice posameznih napadov. Sistem je zmožen tudi razbiranja podatkov po tem ali pred tem, ko so šifrirani. Takšen sistem lahko analizira podatke glede na dnevnike operacijskih sistemov, zato lažje zazna vrsto napada in določi primeren odziv. Sistemi, osnovani na gostiteljskih sistemih, so torej bolj prilagodljivi, zahtevajo pa več sredstev in so zato večja obremenitev za računalniški sistem, na katerem tečejo, poleg tega pa so bolj ranljivi za napade DDoS.

Sistemi, ki zaznavajo znane napade, so sistemi, ki nadzorujejo dejavnost na omrežju oziroma računalniku in značilnosti te dejavnosti primerjajo z značilnostmi dejavnosti oziroma vzorcev znanih napadov. Ker takšen sistem prepozna vrsto napada, ima operater več informacij o njem, poleg tega pa so rezultati zanesljivejši, ker je manj lažnih alarmov. Seveda je pomanjkljivost, da sistem novih vrst napadov ne zaznava, poleg tega pa imajo napadi na sisteme SCADA drugačne značilnosti kot napadi na druge informacijske sisteme, ker so prilagojeni drugačnim protokolom.

Sistemi, ki zaznavajo anomalije, so po drugi strani sistemi, ki preučuje statistične podatke na omrežju ali gostiteljskem računalniku, in ko so ti podatki drugačni od pričakovanih, to prepozna kot verjeten napad. Podatki, ki jih preverja, so običajno npr. obremenitev procesorja, število neuspešnih prijav na sistem ipd. Takšen sistem

prepozna nove vrste napadov, vendar pa ne prepoznava napadov, ki spreminjajo parametre, ki jih sistem ne nadzoruje, poleg tega pa obstaja možnost lažnih alarmov.

Aktivni sistemi so sistemi, ki izvedejo določeno akcijo, ko zaznajo dogodek, npr. blokirajo omrežna vrata ali spremenijo sezname dovoljenega dostopa na omrežnem usmerniku ali požarnem zidu, da onemogočijo prenos podatkovnih paketov od IP-naslova morebitnega napadalca. Pasivni sistemi po drugi strani le zberejo podatke in jih posredujejo posamezniku, ki potem ukrepa. Ti podatki so npr. IP-naslov, od katerega prihaja napad, IP-naslov tarče, rezultat napada, orodje ali mehanizem napada ipd.

Pomembno je tudi, ali ti sistemi zbirajo podatke v realnem času ali pa v paketih po dogodku. Slednji so bili pogosti v preteklosti, saj sistemi niso bili dovolj zmogljivi, da bi podpirali analizo v realnem času (Krutz 2006, 100–101).

Požarni zid

Omrežni požarni zidovi so naprave, ki nadzorujejo pretok informacij med omrežji in jih po potrebi zaustavljajo. Medtem ko so bili v preteklosti požarni zidovi načeloma postavljeni na mejah omrežij – to je na točki, kjer je bila vzpostavljena povezava med omrežjem družbe in svetovnim spletom – je danes takšna oblika zavarovanja nezadostna, zato družbe uporabljajo požarne zidove tudi na drugih mestih (Scarfone in Hofman 2009, 11).

Razredi požarnih zidov so običajno sledeči (Stouffer in drugi 2011, 59–60):

- požarni zidovi, ki filtrirajo podatkovne pakete. Ti požarni zidovi so najosnovnejši. To so predvsem usmerjevalniki, ki vsebujejo funkcionalnost nadzora za systemske naslove seje komunikacije. V tej obliki požarni zidovi nadzorujejo tretjo plast modela OSI. Pregledajo namreč le osnovne informacije podatkovnega paketa (npr. IP-naslov pošiljatelja, port) in ga na podlagi postavljenih pravil posredujejo naprej ali zaustavijo. Takšni požarni zidovi imajo prednost, da so cenovno ugodni in imajo majhen vpliv na zmogljivost omrežja;
- požarni zidovi, ki nadzorujejo stanje povezave. Ta vrsta požarnega zida deluje tudi na plasti 4, saj poleg filtriranja podatkov nadzoruje tudi zgodovino prenosov in odprte povezave in lahko glede na te podatke določi, ali je

posamezen paket legitimen ali ne. Takšen tip zidu je varnejši in še vedno nudi dobro stopnjo zmogljivosti, je pa dražji in ga je težje nastaviti in upravljati kot prvi tip;

- požarni zidovi, ki nadzorujejo promet na nivoju aplikacije. Takšni požarni zidovi filtrirajo podatke glede na pravila aplikacij ali protokolov, poleg tega pa delujejo kot posrednik, kar pomeni, da uporabnika na različnih straneh zidu nimata vzpostavljene neposredne povezave. Nudijo visok nivo varnosti, vendar pa močno vplivajo na zmogljivost omrežja, kar je lahko v okoljih SCADA nesprejemljivo.

Težava požarnih zidov, ki jih uporabljajo družbe, ki imajo v omrežju sisteme SCADA, je, da če ti požarni zidovi niso postavljeni specifično za sisteme SCADA, niso primerni za protokole, ki jih ti sistemi uporabljajo, in zato ne morejo optimalno nadzorovati prenosa podatkov. Obstajajo tudi požarni zidovi, ki so konfigurirani tudi za protokole SCADA, vendar so novost in se širše ne uporabljajo (Krutz 2006, 63).

Arhitektura sistema omogoča postavitve požarnega zidu na več načinov. Če požarnega zidu ni, je sistem SCADA – v primeru, da ne deluje v fizično ločenem omrežju – lahko zavarovan samo tako, da je logično ločen od preostalega omrežja. To pomeni, da nadzorni sistemi delujejo na ločeni strojni opreми kot preostalo omrežje. Tako NIST ob vzpostavitvi povezave s preostalim omrežjem svetuje vsaj dokumentirane in na najmanjše število zmanjšane povezave. Seveda to še vedno predstavlja precejšnje tveganje, če napad na sistem SCADA poteka znotraj omrežja (Stouffer in drugi 2011, 61).

Priporočljiva je uporaba požarnega zidu med sistemom SCADA in omrežjem družbe. Če je vzpostavljena takšna povezava, je požarni zid najverjetneje konfiguriran tako, da omogoča najboljšo možno varnost za sistem SCADA in je nevarnost omejena na dva dejavnika. Prvi je sistem za zapisovanje zgodovine podatkov, ki je, če deluje v omrežju izven sistema SCADA, lahko ugrabljen ali posneman in lahko pošlje zlonamerne ukaze v omrežje. Če je v sistemu SCADA, pa mora biti zmožen komunikacije z vsemi računalniki v zunanjem omrežju prek ukazov SQL ali http in je ranljivejši za napade. Drugi dejavnik so lažni podatkovni paketi, npr. trojanski konj v obliki http, s katerimi bi operater lahko po nesreči okužil gostiteljski računalniški sistem (Stouffer in drugi 2011, 62–63).

Bistveno izboljšavo te arhitekture predstavlja uvedba t. i. demilitariziranega območja med omrežjem družbe in omrežjem sistema SCADA. To pomeni požarni zid s tremi namesto dvema povezavama in posebno omrežje, v katerem so nezavarovane ali deljene naprave, kot je datotečni strežnik. Tako neposredne komunikacijske poti med omrežjem družbe in omrežjem SCADA niso potrebne; vsaka pot se konča v DMZ, kamor je umeščena tudi zaščita pred zlonamerno programsko opremo. Možna je konfiguracija z enim požarnim zidom ali dvema, pri čemer je priporočljiva slednja, torej konfiguracija z enim požarnim zidom med omrežjem družbe in DMZ ter drugim med omrežjem sistema SCADA in DMZ (Stouffer in drugi 2011, 63–65).

VPN

Navidezno zasebno omrežje je vrsta vzpostavitve kriptografske tehnologije, ki omogoči zasebno in varno omrežno povezavo med sistemi in ki omogoča prenos med njimi na način, kot bi ga omogočala nezavarovana neposredna povezava. Za vzpostavitev takšne povezave uporablja tehniko vzpostavitve predora med dvema točkama ter določene varnostne procedure. Običajno se takšne povezave uporabljajo za razširitev omrežja družbe na oddaljene lokacije. Obstaja več vrst VPN-jev (Whitman in Mattord 2011, 282):

- VPN-ji, ki so vzpostavljeni prek najetih fizičnih povezav, ki jih ne uporablja nihče drug. Povezava temelji na zaupanju med družbo, ki ponuja omrežje, in družbo, ki to omrežje najema;
- VPN-ji, ki z uporabo varnostnih protokolov in šifriranja podatkov zagotavljajo varnost povezave prek javnega omrežja, npr. interneta;
- kombinacija obeh vrst VPN-jev, ki zagotavljajo zavarovano in šifrirano povezavo prek najetih povezav.

Varen VPN mora zagotavljati naslednje varnostne mehanizme (Whitman in Mattord 2011, 282):

- enkapsulacijo podatkovnih paketov, ki omogoči, da obe točki v omrežju uporabljata enake protokole za prenos podatkov prek javnega omrežja in so tako primerni za uporabo obeh sistemov;
- šifriranje podatkov, da so ti podatki varni med prenosom prek javnega omrežja;

- avtentikacijo oddaljenega računalnika in njegovega uporabnika, s čimer se prepreči dostop nepooblaščenim uporabnikom.

Obstajata dva načina povezave: transportni in predorski način. Prvi je vrsta povezave med enim računalnikom oz. uporabnikom in omrežjem, pri čemer je vsebina podatkov zaščitena, glava podatkov, torej npr. informacije o tem, kam je podatek namenjen, pa ne. Drugi način je način povezave med dvema omrežjema. Takšna povezava je varnejša, saj omogoča zavarovanje celotnega paketa podatkov, tudi glave (Whitman in Mattord 2011, 283–284).

Kriptografija in SSL/TSL

Kriptografija oz. šifriranje je način zagotavljanja varnega prenosa podatkov, saj so ti znani le pošiljatelju in prejemniku.

Poznamo dva razširjena načina šifriranja: simetrično šifriranje in asimetrično šifriranje z javnim ključem (Stavroulakis in Stamp 2011). Prvi način je uporabljen za povsem zasebni promet, saj gre za dogovorjen način šifriranje med dvema strankama¹⁵. Pri drugem gre za razširjen javni protokol šifriranja po modelu PKI, pri čemer moramo izpostaviti predvsem protokola SSL in TLS.

Transport Layer Security (TLS) in njegov predhodnik Secure Socket Layer (SSL) sta množično razširjena kriptografska protokola, namenjena varnosti komunikacije prek spleta, npr. za spletno bančništvo in oddaljen dostop do sistemov podjetij. Uporabljata asimetrično kriptografijo za avtentikacijo in zaupnost izmenjave ključev, simetrično šifriranje za izmenjavo podatkov in avtentikacijska gesla za integriteto podatkov (Dierks 2008, 4–6).

V modelu OSI se TLS/SSL začne v 5. plasti in deluje v 6. plasti. Proces prepoznavanja¹⁶ se z uporabo asimetrične kriptografije začne v 5. plasti. Tu se vzpostavijo nastavitve šifriranja in skupen ključ, nato pa se ta ključ uporabi za šifriranje podatkov v 6. plasti. (Dierks 2008, 4–6).

¹⁵ Ti načini so zelo raznoliki, npr. eliptična, kvantna, biokriptografija itd. (Stavroulakis in Stamp 2011, 21–174).

¹⁶ T. i. handshake

Protokola za avtentikacijo uporabnika običajno uporabljata certifikate javnih ključev, elektronske dokumente, ki uporabljajo digitalen podpis za povezavo javnega ključa z identiteto posameznika (Canetti 2004, 3–11).

3.11 Organizacijske rešitve varovanja kritične infrastrukture

Poleg tehničnih sistemov lahko opredelimo tudi organizacijske ukrepe, ki jih lahko organizacija izvede za izboljšanje informacijske varnosti. Sledi njihova opredelitev.

Obramba po globini

Strategija večplastne obrambe oz. obrambe po globini je koncept, ki se je prenesel iz strategije kinetičnega vojskovanja v strateško razmišljanje IKT-varnosti. Logika organiziranja obrambe pred kibernetскими napadi je tako podobna; gre namreč za organizacijo obrambe na več točkah in z več vidikov tako, da napadalec ob napadu izrabi čim več svojih zmogljivosti. Ob tem mora za dosego svojega cilja premagati veliko preprek (Cleghorn 2013, 144). NSA definira globinsko obrambo kot strategijo najboljših praks, ki se zanaša na inteligentno aplikacijo tehnik in tehnologij; te danes obstajajo zato, da se zagotovi dostopnost, celovitost in zaupnost podatkov. Gre za varnostno strategijo, ki naj bi zagotavljala ugodno razmerje med varnostnimi zmoglostmi ter ceno, zmogljivostjo in aplikacijskimi zmoglostmi sistemov.

Administrator naj bi obrambo postavil tako, da bi večplastni varnostni sistemi, ki se med sabo pokrivajo tako, da je podatkovni promet obravnavan večkrat naenkrat, odvrnili vsakdanjega napadalca od napada in preprečili večino napadov. Tisti napadi, ki so izvedeni, naj bi bili uspešno zaznani, administrator pa obveščen, da lahko pravočasno ukrepa. Kontrole naj se ne bi izvajale le na obrobju sistema, temveč tudi znotraj njega, saj so napadi znotraj sistema najuspešnejši (Cleghorn 2013, 144–145).

Strategija torej vsebuje priporočilo, da za zavarovanje sistema uporabi čim več različnih, tudi v tem delu opisanih sistemov, ki se med sabo prekrivajo in podpirajo. Poleg tega pa NSA svetuje tudi jasne politike ter redno usposabljanje in skrb za zadovoljstvo zaposlenih.

Nekateri avtorji menijo, da je pristop globinske obrambe neučinkovit in obsojen na dolgoročen propad, saj je strategija, ki je prevedena iz kinetičnega vojskovanja v kibernetični svet, pomanjkljiva. Končni namen globinske obrambe v kinetičnem svetu

je namreč protinapad, tega pa v kibernetskem svetu ne more biti, saj ne napadalec zelo redko organizirana skupina ljudi (Small 2011, 1–19). Tako bi bilo treba razmišljati ne samo o preprečevanju napadov, temveč tudi o zmanjševanju posledic vdorov, saj se ti vsekakor dogajajo. Treba bi bilo zagotavljati večje sodelovanje tako med napadenimi podjetji kot tudi med dobavitelji varnostne opreme s čim hitrejšim in učinkovitejšim širjenjem informacij (prav tam).

Lonci medu in rezultati njihove uporabe

Ena od komponent sistemov za zaznavanje vdorov je lahko sistem lonec medu oz. honeypot. To je na omrežju osnovan sistem za zaznavanje vdorov, ki se uporablja kot vaba za zaznavanje in zapisovanje vdorov. Načrtno je osnovan tako, da vdor vanj ne more biti legitimna dejavnost, zato je vsaka interakcija z njim lahko opredeljena kot napad. Z uporabo lonca medu lahko uporabnik odkriva metode napada na sistem in se s tem pripravlja na napade na dejanske sisteme. Idealno je lonec medu zasnovan tako, da napadalec ne more vedeti, da gre za vabo, saj popolnoma posnema dejanski sistem, ki je tarča napada. Običajno so sestavni del požarnega zidu. Glede na intenzivnost uporabe poznamo produkcijske in raziskovalne lonce medu. Prve uporabljajo predvsem podjetja, druge pa raziskovalne ustanove. Raziskovalni lonci medu lahko pridobijo bistveno več informacij, vendar pa bistveno bolj obremenijo sisteme in omrežja (Singh 2009).

Lonec medu je pasivna komponenta IDS-ja. Vhoden promet gre običajno v omrežje prek vhodnega sistema, npr. požarnega zidu, ki promet defragmentira in klasificira. Nato odpre vrata do sistema za zaznavanje vdora in pošlje podatke vanj. IDS preveri podatke in ugotovi, ali je promet legitimen ali ne. Če zazna podatke kot napad, jih pošlje v lonec medu, sicer jih posreduje v običajen tokokrog informacij (Singh 2009).

Obstajajo tudi konfiguracije z več različno pripravljenimi lonci medu, ki se združujejo v omrežja, imenovana honeynete¹⁷. Ti so v zadnjem obdobju vse bolj razširjeni zaradi večanja števila virtualnih sistemov (Wade 2011, 14).

Danes lahko identificiramo tri takšne projekte, ki so usmerjeni v varovanje sistemov SCADA:

¹⁷ Eden izmed takšnih primerov je odprtokodni projekt Honeyd, virtualno omrežje, ki simulira več različnih operacijskih sistemov hkrati.

- SCADA HoneyNet Project podjetja Cisco systems;
- Digital Bond honeynet;
- Team Cymru darknet.

Medtem ko prva dva projekta simulirata logične kontrolerje za delovne inštrumente v sistemih SCADA, je tretji le identificiral TCP-vrata, ki jih običajno uporabljajo sistemi SCADA, in zapisuje število vdorov. Prva dva projekta sta kot aplikacije na voljo za prosto prenašanje prek interneta.

Aplikacija drugega izmed teh projektov za magistrsko delo v ZDA (Wade 2011, 27–35) je prispevala ugotovitve, da je bilo v 31 dneh testiranja na sistem honeynet izvedenih skoraj 2 milijona napadov, velika večina prek krmilnikov UPnP. Zanimivo je, da napadi sami po sebi niso bili škodljivi, niti niso bili izvedeni z namenom neposrednega škodovanja, temveč zgolj za zbiranje podatkov. Napadi prek krmilnikov UPnP se namreč običajno uporabljajo za pridobitev administratorskih pravic na sistemu, napadov, ki bi izkoristili kakšno ranljivost prek MODBUS-a, pa ni bilo, prav tako napadalcev ni zanimala arhitektura sistema SCADA.

To je skladno s predhodno opisanimi ugotovitvami projekta Team Cymru darknet. Očitno je, da organizacije izvajajo risanje zemljevida obstoječe infrastrukture, torej se za zdaj ugotavlja njen obstoj, vsekakor pa ima zbiranje teh informacij določen namen.

3.12 Standardi in priporočila na področju varovanja informacij in SCADA

Odbor predsednika ZDA za varovanje kritične infrastrukture je leta 2002 izdal publikacijo, imenovano 21 Steps to Improve Cyber Security of SCADA Networks¹⁸. V tej publikaciji je navedenih 21 korakov za izboljšanje stanja varnosti sistemov SCADA. Ti koraki so sledeči (U.S. department of energy 2001, 3–9):

1. Identificirati je treba vse povezave do omrežij sistema SCADA in izvesti temeljito analizo tveganja, da bi ugotovili nujnost in tveganje vsake povezave v omrežje. Ugotoviti je treba tudi, kako dobro so te povezave zavarovane ter identificirati in oceniti vse notranje povezave, povezave s svetovnim spletom,

¹⁸ Ta publikacije je ena od del, ki so nastala kot posledica ukaza predsednika ZDA o varovanju kritične infrastrukture v informacijski dobi. Ta ukaz je predsednik G. W. Bush izdal manj kot mesec po terorističnih napadih na ZDA septembra 2001.

- naprave za brezžično omrežje, vključno s satelitskimi povezavami, povezave z modemi in povezave s poslovnimi partnerji, dobavitelji ali regulatornimi organi.
2. Odklopiti je treba vse nepotrebne povezave na omrežje sistema. Omrežje je treba izolirati, kolikor je to mogoče. Vsaka povezava na katerokoli omrežje pomeni dodatna tveganja, še posebej če ta povezava omogoča dostop do svetovnega spleta.
 3. Oceniti in zavarovati je treba vse preostale povezave na omrežje ter izvesti penetracijske teste in analize tveganja za vse preostale povezave do omrežja. Pridobljene informacije morajo biti sestavni del sistema upravljanja tveganj varnostne strategije. Treba je uvesti požarne zidove, sisteme za zaznavanje dostopa in druge primerne mehanizme. Vodstvo družbe mora razumeti in sprejeti odgovornost za vsako povezavo do omrežja.
 4. Omrežje je treba zavarovati tako, da se odstrani nepotrebne storitve. Strežniki, ki delujejo na omrežju, so lahko ranljivi za napade prek privzetih mrežnih storitev. Odstraniti oziroma onemogočiti je treba vse storitve, ki niso nujno potrebne. To je še posebej pomembno, kadar je omrežje sistema SCADA povezano z drugimi omrežji. Za vsako storitev oziroma funkcijo posebej je treba narediti analizo koristi in tveganj, s katero lahko ugotovimo, ali so koristi takšne, da so tveganja sprejemljiva.
 5. Lastniški protokoli niso zadostno zagotovilo varnosti. Varnost nekaterih omrežij je zasnovana predvsem na neznanosti protokolov, vendar to ni zadosten razlog za varnost, prav tako ne zanašanje na privzete tovarniške nastavitve. Dobavitelji opreme morajo priskrbeti vse podatke o morebitnih dostopnih točkah.
 6. Izvesti je treba vse varnostne funkcije, ki jih sistemi zagotavljajo. Nekateri, predvsem starejši sistemi SCADA, sploh nimajo varnostnih funkcionalnosti, zato morajo lastniki omrežij vztrajati, da dobavitelji nadgradijo sisteme SCADA s takšnimi funkcionalnostmi. Novejši sistemi sicer te funkcionalnosti imajo, vendar so ob inštalaciji izključene. Vse nastavitve je treba prilagoditi tako, da bodo zagotavljale najvišji nivo varnosti.
 7. Vzpostaviti je treba močan nadzor nad mediji, ki se uporabljajo kot zadnja vrata v omrežje SCADA. Če zadnja vrata obstajajo, jih je treba zavarovati z močno kontrolo dostopa. Idealno je, če se način dostopa zamenja z varnejšo metodo.

8. Vzpostaviti je treba sistem za notranje in zunanje zaznavanje vdorov in 24-urni nadzor dogodkov. Tak sistem mora biti del strategije, ki vsebuje opozarjanje sistemskih administratorjev na zlonamerno dejavnost, vzpostavljeni pa morajo biti tudi mehanizmi za učinkovito odzivanje na takšne dejavnosti. Dodatno je treba zagotoviti tudi zapisovanje dogodkov v dnevnike, da se lahko zagotovi sledenje.
9. Treba je izvesti tehnično revizijo naprav in omrežij SCADA, da bi lahko odkrili varnostne težave. Takšne revizije ne bodo rešile sistemskih problemov, odkrile pa bodo nepravilnosti v sistemih, ki bi jih napadalci zlahka izkoristili. Ko so napake odkrite in odpravljene, je treba revizijo izvesti ponovno.
10. Izvesti je treba fizično analizo vseh točk, ki so povezane v omrežje in oceniti njihovo varnost. Vsaka lokacija s povezavo v omrežje je namreč potencialna tarča napada, še posebno, če je ta točka daljinsko krmiljena in nezavarovana. Zagotoviti je treba primerno varovanje za preprečevanje nepooblaščenega dostopa. Nezavarovane točke z dostopom do omrežja niso sprejemljive.
11. Ustanoviti je treba ekipo za testiranje varnosti sistema in izvesti poskuse vdora. Takšna ekipa naj bo raznolika; poskusi naj ugotovijo vse možne točke, na katerih je mogoč vdor v sistem. Njene ugotovitve morajo biti del varnostne strategije.

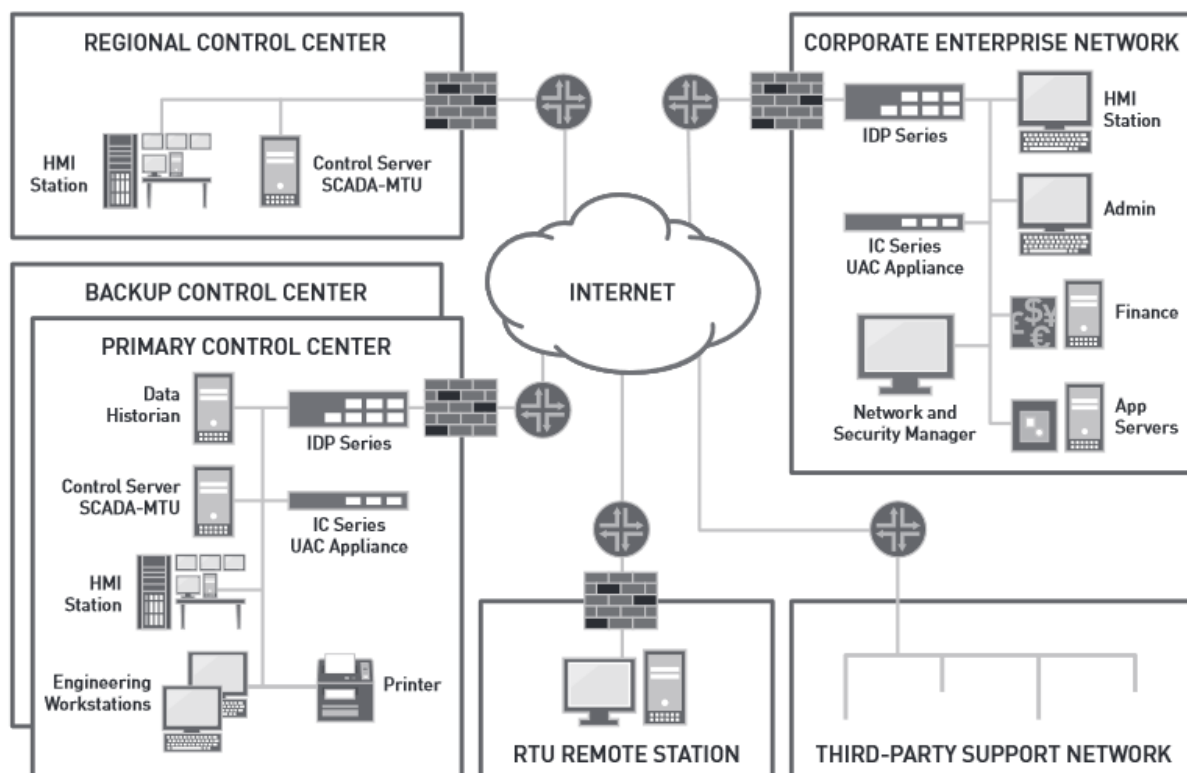
Zadnja točka je še posebej pomembna, ker je to najbolj kakovostna analiza varnosti sistema. Pregled šibkih točk omogočajo tudi sistemi za zaznavanje vdora, bolj kot izvedba pregleda pa je pomembna analiza podatkov. Takšen pregled bo namreč pokazal, katere naprave delujejo na omrežju, kakšne so njihove nastavitve in posodobitve programske opreme, katera omrežna vrata so odprta in se uporabljajo ter katere aplikacije in storitve se uporabljajo v omrežju. Takšen pregled, ki mora imeti podporo vodstva družbe, bo pokazal, katere možnosti lahko uporabijo morebitni napadalci. Orodja za prav takšno analizo so na voljo na internetu in jih lahko uporabi vsak posameznik z nekoliko znanja in želje (Kruz 2006, 101–102).

Preostale točke v publikaciji so usmerjene v upravljanje s tveganji na področju informacijske varnosti in so skladne s standardnimi pravili, ki so opisani v standardih v nadaljevanju. Predvsem gre za definiranje vlog, popis arhitekture, vzpostavitev procesa obvladovanja tveganj in strategije ter izvajanje revizij.

Načeloma se strokovna literatura s področja varovanja informacijskih sistemov na področju ICS strinja, da je najprimernejša varnostna arhitektura sistemov takšna, da morata biti nadzorno oz. krmilno okolje in preostali ekosistem organizacije v največji možni meri ločena (Knapp 2011, 31). Medtem ko je fizična ločitev danes praktično nemogoča, je potrebna čim bolj utrjena logična ločitev.

Slika 3.3 prikazuje logično ločitev poslovnega in ICS-omrežja. Nadzorni centri, poslovno okolje organizacije, oddaljene postaje in podporno omrežje so med seboj ločeni logično, saj so v različnih logičnih omrežjih, pri dostopu do vsakega pa je postavljen tudi požarni zid.

Slika 3.3 : Logična ločitev poslovnega in ICS-omrežja v omrežju WAN



Vir: Juniper networks (2010)

ANSI/ISA 99 - ANSI/ISA-62443

Skupina standardov ANSI/ISA-99 je proizvod skupine ISA (Byres 2012). Nanaša se specifično na varnost sistemov ICS, katerih nedelovanje bi lahko povzročilo nevarnost javnosti ali uslužbencem, izgubo javnega zaupanja, izpolnjevanje

zakonskih zahtev, izgubo lastniških ali zaupnih informacij, ekonomsko izgubo ali negativen vpliv na državno varnost (prav tam).

Pod sisteme ICS skupina razume tako programsko in strojno opremo kot tudi z njo povezane človeške, mrežne in strojne interakcije ter vmesnike. Fizična varnost ni vključena v model ISA.

Skupina standardov vnese v varovanje infrastrukture koncept območij in vodov. Območja definira kot skupino logičnih in fizičnih sredstev, ki si delijo skupne varnostne zahteve glede na dejavnike, kot je npr. kritičnost. Oprema v območju ima določeno zmožnost doseganja stopnje varnosti, in če ta stopnja ne doseže zahtev po varnosti območja, jo je treba ustrezno nadgraditi.

Komunikacija med območji mora potekati po opredeljenih vodih, ki služijo tudi za nadzor nad prometom podatkov ter se posledično uporabljajo tudi za varovanje pretoka podatkov in za blaženje razlik med varnostnimi zmožnostmi določenih območij.

Skupina standardov ne določa natančno, kako naj družba definira svoja območja in vode, temveč poda zahteve glede na ocenjeno nevarnost napada, pri čemer je nevarnost sestavljena iz možnosti in posledic.

Družba naj bi tako najprej identificirala operativna območja kot na primer skladiščenje, procesiranje ipd., nato pa naj bi ta območja razdelila na funkcionalne plasti, kot so na primer nadzorni sistemi in vmesniki. Nato naj bi opredelila nevarnost izpada območij, varnostne cilje, strategijo in povezave.

Primer takšne opredelitve je prikazan v prilogi 7.2. Po analizi in implementaciji potrebnih sprememb je treba redno preverjati učinkovitost rešitev. (Byres 2012, 1–10).

Družina ISO/IEC 27000

Vedno večja odvisnost od informacijsko-komunikacijskih tehnologij ter odprtost organizacij in povečevanje pomena informacij v sodobnem poslovanju pomeni potrebo po standardizaciji varovanja upravljanja varovanja informacijskih sistemov, zato je mednarodna organizacija za standardizacijo izdala rastočo družino

standardov ISO/IEC 27000, ki se nanašajo na upravljanje varovanja informacij (SIQ 2010).

Za razliko od predhodne družine standardov je ta bolj razširjena, saj se nanaša na vsa podjetja in je zato tudi manj specifična. Del te družine, ISO/IEC 27001 – sistemi upravljanja varovanja informacij – je mogoče presojati, zato je mogoča certifikacija.

ISO/IEC 27001 postavi naslednje zahteve:

- sistematičen pregled tveganj za informacije v družbi, pri čemer se upoštevajo grožnje, šibkosti ter posledice;
- načrtovanje in implementacija koherentnega in celovitega nabora kontrol in drugih oblik blaženja tveganj za tista tveganja, ki se opredelijo kot nesprejemljiva;
- sprejem celovitega sistema upravljanja, ki skrbi za to, da varnostne kontrole stalno delujejo skladno s pričakovanji.

Standard je skladen s sistemom kakovosti (ISO/IEC 2005).

Standardi NIST

NIST je ameriška neregulatorna agencija, ki deluje v okviru ameriške gospodarske zbornice. Njegov namen je razvoj znanstvenih meritev, standardov in tehnologij tako, da ti širijo ekonomsko varnost ZDA.

NIST izdaja tako priporočila kot standarde, vendar pa slednji niso osredotočeni na upravljanje tako kot predhodno opisana standarda, pač pa natančno opredeljujejo določene vidike informacijske varnosti in podajajo navodila za njihovo zavarovanje. Ti vidiki so na primer varnostno označevanje podatkovnih paketov, varnostne zahteve za kriptografske module, sistemi za overjanje ključev ipd. (NIST 2009). Priporočila so uporabnejša za vodstva podjetij, saj se ukvarjajo z varnostnimi politikami.

NIST uporablja kompleksnejši pristop do življenjskega cikla upravljanja kot ISO; NIST namreč dosledno opredeljuje štiri korake¹⁹, drugi odvisno od situacije korake prilagaja. Načeloma naj bi menedžment nevarnosti razdelili na planiranje, začetno fazo, razvoj in pridobitev, implementacijo, operativno in vzdrževalno fazo ter opustitveno fazo.

¹⁹ Načrtovanje, implementacija, nadzor in popravljanje

Vsaka organizacija naj bi na začetku upravljanja informacijske varnosti ustvarila in definirala program informacijske varnosti, v katerem se opredelijo sredstva, programska oprema, informacije in osebje, ki so vanj zajeti. Iz tega programa naj bi potem izhajale strateške usmeritve organizacije v zvezi z informacijsko varnostjo; določene naj bi bile zadolžitve in odgovornosti ter ukrepi za premostitev odstopanj med načrti in dejanskim stanjem.

Vsaka politika, ki izhaja iz programa, se mora osredotočiti na določeno področje. Pogosto mora biti posodobljena, njen namen, vloge in odgovornosti pa morajo biti jasne. Politika mora biti izražena kot pravilo. Vse politike naj bi imele vse potrebne dodatke za večjo jasnost, bile naj bi jasno vidne in dosledne, podpirati pa jih mora vodstvo. Vsaka politika mora biti izvedena v skladu z določenim življenjskim ciklom.

NIST izdaja publikacije, ki se nanašajo na varnost informacijskih sistemov v seriji SP 800. Primarno so te namenjene administratorjem in vodjem organizacij, ki delujejo v administraciji ali v podpori administracije ZDA. Te organizacije morajo izpolnjevati pogoje, podane v teh publikacijah ter pridobiti NIST-ovo certifikacijo in akreditacijo. V nadaljevanju bom analiziral delovni okvir, ki ga agencija postavi za oceno tveganj in varnosti informacijskih sistemov.

4 Razvoj orodja in aplikacija orodja

Po pregledu relevantnih teoretičnih izhodišč za ocenjevanje kibernetске varnosti elektroenergetske kritične infrastrukture sledi izdelava analitičnega orodja, ki bo takšno ocenjevanje omogočalo. Takšno orodje mora za svoj uspeh izpolnjevati določena načela, ki so opredeljena v nadaljevanju, najprej pa sledi pregled obstoječih evalvacijskih metod in orodij.

4.1 Pregled obstoječih orodij in metod

CRAMM

CRAMM je matrična, kvalitativna metoda ocenjevanja tveganj, ki jo je izdelala britanska agencija za komunikacije in telekomunikacije leta 1987. Metoda se za ocenjevanje tveganj uporablja po vsem svetu, ocenjevanje pa se izvede na nivoju upravljanja ter operativnega in tehničnega delovanja organizacij. Zahteva visok nivo sodelovanja in poznavanja sogovornikov, s katerimi se izvedejo strukturirani intervjuji. Je skladna s certificiranjem po standardu ISO 27000, vendar pa po sami metodi ni mogoče licenciranje ali certificiranje. Obstajata dve komercialno dostopni metodi, t. i. polna in hitra metoda (Cramm-Site 2014)

Metoda zajema pet zaporednih korakov:

- iniciacijo, izvedeno s strukturiranimi vprašalniki in intervjuji, pridobitvijo obsega in ciljev analize, strukturiranjem urnika in z uvajanjem sodelavcev, ki bodo izvajali ocenjevanje;
- identifikacijo in oceno vrednosti sredstev, pri čemer se pod sredstva razume tudi storitve procesiranja podatkov, torej ne zgolj fizična sredstva. Vrednost sredstev se oceni glede na vpliv na delovanje organizacije, ki bi ga imela kršitev zaupnosti, integritete dostopnosti in nezatajljivosti podatkov, ki jih ta sredstva omogočajo. Pri tem je vpliv na delovanje standardiziran in se meri v finančnih učinkih;
- oceno groženj in ranljivosti, pri katerih naročnik sam oceni, katere grožnje se bodo v analizi upoštevale. Ocena vseh grožnje na vseh sredstvih je namreč nesmiselna. Ob uporabi polne metode ocenjevalci izvajajo intervjuje s

tehničnim osebjem in njihove odgovore vpisujejo v programsko orodje, s katerim pridobijo stopnje tveganja. V primeru hitre metode ocenjevalci sami odgovarjajo na vprašanja;

- oceno tveganja, ki se pridobi z matematično metodo, ki združi grožnje, ranljivosti in vrednosti sredstev. Končen rezultat je, da ima vsako sredstvo t. i. varnostno zahtevo, ocenjeno od 1 do 7;
- ukrepe za preprečevanje tveganj, ki se izberejo iz vnaprej določenega nabora in se uporabijo glede na izvedeno analizo tveganj (SANS Institute 2002).

OCTAVE

OCTAVE je prilagodljiv, kvalitativen okvir za ocenjevanje kritičnih groženj, sredstev in ranljivosti in je kot takšen primeren za oceno ogroženosti. Na podlagi te je mogoče izdelati varnostne načrte, kontrole in politike. Z oceno organizacija lahko preveri, katera sredstva so kritična za njeno delovanje, kakšne so njihove ranljivosti, določi in oceni možne posledice za organizacijo, če pride do izpolnitve groženj, in izvede korektivne ukrepe za premostitev teh groženj in tveganj. Ocena deluje v naslednjih fazah:

- vzpostavitev meril merjenja tveganj;
- razvoj profilov informacijskih sredstev z njihovimi vsebniki;
- opredelitev problematičnih področij in scenarijev groženj;
- opredelitev in analiza tveganj;
- izbira pristopa k premostitvi tveganj.

OCTAVE uporabniku ponuja izdelane ocenjevalne liste in priporočila za izvedbo analize za vsako izmed teh področij, vendar pa mora organizacija sama izbrati obseg in določiti kritičnost za sredstva ter metode premostitve. To je namreč zgolj okvirno orodje, ki predpostavlja definirane procese, samostojno usmeritev delovanja, timsko delo in prilagodljive ukrepe v podjetju. Tako mora imeti organizacija že vzpostavljene ustrezne sisteme vodenja in poslovno kulturo, če želi uporabljati ta okvir (Alberts in Dorofee 2001 ter Caralli in drugi 2007).

Primer ocenjevalnega lista za tveganje informacijskega sredstva je prikazan v prilogi C.

Veliko publikacij, ki jih NIST izdaja, se nanaša na specifične kontrole informacijskih sistemov²⁰, ki so bile za izdelavo pričujočega orodja bistvenega pomena. Ta organizacija pa izdaja tudi delovni okvir za upravljanje tveganj v informacijski varnosti ter za njihovo oceno. Publikaciji sta v hierarhični strukturi – SP 800-37 je nadrejena SP-800-30; prva postavi delovni okvir, druga pa kontrole za analizo. NIST opredeli tri varnostne nivoje, ki so primerni za specifične organizacije, ter katere kontrole so ustrezne za kateri nivo.

Organizacija naj bi za izpolnitev zahtev delovnega okvira najprej kategorizirala informacijski sistem, ga opisala in orisala ter ga registrirala pri ustreznih internih ali eksternih organih. Nato naj bi identificirala in dokumentirala že obstoječe varnostne kontrole, zatem pa dopolnila seznam kontrol s kontrolami, ki jih še želi dodati. Izdelala naj bi tudi strategijo nadzora nad temi kontrolami, vse te korake zapisala v varnostni načrt ter pridobila podporo vodstva za načrt. Kontrole naj bi implementirala in implementacijo dokumentirala, nato pa preverila njihovo delovanje ter izvedla dodatne ukrepe za premostitev razlik med nominalnim in dejanskim stanjem. Naslednji korak je avtorizacija, certifikacija in akreditacija sistema, sledi pa stalen krog nadzora in korektivnih ukrepov. (NIST 2010)

SP 800-30 tveganja razdeli na namerna in nenamerna in jih kvantificira tako, da vsakemu tveganju, ki ga organizacija identificira, dodeli indeks tveganja v vrednosti med 0 in 100. Ta indeks je kompozitna ocena kvantificiranega značilnosti vira grožnje, relevantnosti, verjetnosti, ranljivosti sistema, verjetnosti uspeha in posledic napada. Publikacija ne priporoča skupnega indeksa, zgolj razdelitev po identificiranih tveganjih (NIST 2012).

Penetracijski testi

Medtem ko druge opisane metode v tem poglavju preverjajo varnostne kontrole sistemov, se penetracijski testi osredotočajo izključno na to, kaj ni vzpostavljeno, torej kako lahko napadalec vdre v informacijski sistem organizacije. Organizacija najame izvajalca penetracijskega testa, da vdre v njihov sistem (Allsopp 2009, 2).

Prav tako v nasprotju z drugimi metodami penetracijski testi ne uporabljajo le informacijskih sredstev, pač pa vsa mogoča sredstva na razpolago napadalcem.

²⁰ Glej npr. NIST SP 800-53

Tako lahko napadalec za zbiranje informacij uporabi socialni inženiring, lahko pa tudi fizično vdre v stavbo, zato je dogovor o obsegu testiranja v tem načinu testiranja izredno pomemben.

Del dogovora je tudi dogovor o nivoju predhodnega medsebojnega poznavanja napadalca in tarče. OSSTMM²¹ tako glede na nivo medsebojnega poznavanja definira šest vrst napadov:

- slepi napad: analitik napade tarčo brez predhodnega poznavanja njenih obrambnih zmogljivosti, tarča pa se pripravi na test s popolno vednostjo o njem. Ta napad je običajno namenjen preverjanju znanja izvajalca napada. Tem vrstam napada se običajno reče tudi etični heking, vojne igre ali igranje vlog;
- dvojno slepi napad: analitik napade tarčo brez predhodnega poznavanja tarče, tarča pa nima vedenja o tem, kdaj in kako bo napadena. Ta vrsta napada je namenjena tako preverjanju znanja napadalca kot tudi pripravljenosti naročnika na različne vrste napada. Ti testi so najpogostejši in so poznani tudi kot penetracijski testi oz. črni test;
- sivi test: analitik ob napadu delno pozna obrambne zmogljivosti in sredstva tarče ter popolnoma pozna njene komunikacijske kanale. Tarča je pripravljena na testiranje in pozna način napada. Napad je namenjen preverjanju učinkovitosti delovanja analitika. Ti testi se običajno imenujejo testi ranljivosti in jih izvedejo organizacije za samooceno obrambnih zmogljivosti;
- beli test: analitik napade tarčo z delnim poznavanjem obrambne zmogljivosti in sredstev tarče ter s popolnim poznavanjem njenih komunikacijskih kanalov. Tarča je obveščena o obsegu in času napada, ne pa tudi o vrsti ter načinu napada. Ta vrsta testa je namenjena tako preverjanju obrambnih zmogljivosti tarče kot zmogljivosti napadalca. Test je poznan tudi kot dvojno sivi test;
- tandemski oz. kristalni test: tako analitik kot tarča sta popolnoma pripravljena na test ter sta vnaprej dogovorjena o vseh podrobnostih. Takšen test preverja vzpostavljene kontrole in varnostne mehanizme tarče, ne pa potencialnih neznanih vrst in mehanizmov napada. Takšno preverjanje organizacija običajno izvede sama, analitik pa je običajno član organizacije;

²¹ The Open Source Security Testing Methodology Manual

- rdeča ekipa: napadalec je popolnoma pripravljen na napad, tarča pa ne ve, ne kdaj ne kako bo napadena. Namen tega testa je preverjanje, kako dobro je organizacija pripravljena na neznane vrste in načine napada (ISECOM 2010: 34).

NSA IAM in IEM

NSA IEM je pomemben, ker v nasprotju s številnimi drugimi modeli ponuja bolj jasno opredeljen model, ki je še vedno t. i. baseline approach. To pomeni osnovne smernice za lastno izdelavo modela ocenjevanja tveganj in odgovorov nanje, vendar pa jasno opredeli aktivnosti, ki so priporočene za uspešno izvedbo pregleda. NSA IEM je bil razvit na osnovi metodologije NSA IAM in je poleg metode za ocenjevanje državnih ustanov primeren tudi za zasebne uporabnike (Rogers 2005, 8–9).

IEM razdeli metodo evalvacije v tri faze: predevalvacijsko, evalvacijsko na lokaciji subjekta in poevalvacijsko fazo.

V prvi fazi preučevalec identificira sisteme in meje subjekta, nato opredeli arhitekturo sistemov, se uskladi glede pravnih vidikov pregleda, ustvari in uskladi pravila pregleda, se uskladi glede obsega pregleda ter pripravi načrt evalvacije in izvedbe.

Druga faza je sestavljena iz predhodnega pojasnila namena in poteka evalvacije, testiranja ter zaključnega sestanka.

Tretjo fazo sestavljajo končna analiza, svetovanje na podlagi opravljene analize, priprava strategije za večjo varnost, končno poročila in kasnejši intervju o tem, kako je subjekt implementiral varnostne izboljšave (Rogers 2005, 49–393).

Za namene tega dela je pomembna faza testiranja, ki je opredeljena v modelu. To sestavlja deset osnovnih aktivnosti:

- skeniranje portov, nizkonivojsko odkrivanje topologije omrežja, s katerim se izvedejo nadaljnje aktivnosti; ugotovi se, ali v omrežju obstajajo nedokumentirane priključene naprave;
- SNMP-skeniranje, odkrivanje krmilnikov omrežja in poizvedba, koliko informacije je mogoče odkriti s preprostimi poizvedbenimi ukazi;
- odkrivanje naprav na omrežju; na tej točki bi moral ocenjevalec imeti informacijo o vseh napravah, ki so v omrežju gostitelja;

- odkrivanje brezžičnih dostopnih točk ter ugotavljanje, ali je prek njih možen neposreden dostop do notranjega omrežja;
- odkrivanje ranljivosti s poskusi napadov, o katerih se predhodno dogovorita ocenjevalec in subjekt;
- ocena določenih gostiteljskih sistemov. Ocenjeni naj bi bili vsi kritični sistemi. Na tej točki se preverja varnostna konfiguracija s pomočjo določenih skript, ki simulirajo različne napade;
- analiza omrežnih naprav, predvsem dostopne točke omrežja;
- testiranje ustreznosti gesel;
- skeniranje specifičnih aplikacij, vnaprej dogovorjeno preverjanje določenih informacijskih rešitev, kot so poštni odjemalci, brskalniki ter lastne aplikacije;
- odkrivanje in poskušanje razbiranja prometa v omrežju (Rogers 2005, 182–187).

OSSTM

Open Source Security Testing Methodology je, kot je že razvidno iz imena, odprta metodologija za preverjanje operativne varnosti organizacije.

Metodologija je zaradi svoje odprtosti prosto dostopna, vendar pa mora presojevalec izvrstno poznati področje informacijske varnosti, če želi pridobiti realno sliko varnosti. Metoda je za to delo zelo pomembna tudi zato, ker se približa njegovi ideji, to je izdelava orodja, ki na koncu presoje poda indeks operativne varnosti informacijskega sistema organizacije.

S predpostavko, da bi imel prost dostop do informacijskega sistema organizacije, katere varnost presojam, bi vsekakor izbral to metodo. Poleg jasnega pregleda in smisla metodologije za razliko od številnih drugih metod namreč opredeli jasne kontrole, ki jih postavi v kontekst. Druge metode, npr. penetracijski testi, kot standard namreč ne opredelijo jasnih kontrol, spet druge, npr. CRAMM, pa te kontrole jasno opredelijo, vendar jih ne postavijo v kontekst. Rezultat metode je vrednost ocene tveganja (RAV), ki je izražena kot indeks v vrednosti od 0 do 100, pri čemer je 100 popolna varnost, 0 pa nikakršna.

Metoda kontrole groženj razdeli na dva dela: interaktivne, ki preprečujejo grožnjam, da bi vstopile v sistem, in procesne, ki nadzorujejo grožnje, ko so vstopile. Varnostni

cilji so razdeljeni skladno z modelom CIA, kontrole pa so razporejene logično, glede na to, katere cilje zasledujejo. Poleg kontrol operative varnosti metoda razčleni tudi pomanjkljivosti varnostnih sistemov, ki jih kontrole odkrivajo, kot posebno kategorijo presoje. Presojajo se trije kanali interakcije s sistemi: Telekomunikacijski in mrežni (COMSEC), človeški in fizični (PHYSSEC) ter brezžični (SPECSEC).

Metoda postavi 42 zahtev, ki jih morajo presojevalci izpolniti in ki so tako tehnične kot etične. Te zahteve skupaj s kontrolami odgovorijo na tri vprašanja: kako sistem deluje, kako se to delovanje razlikuje od pričakovanj vodstva in kako bi moral delovati. Poleg kontrol mora presojevalec ugotoviti tudi dejavnik vidnosti sistema, vstopne točke in razmerja zaupanja med potencialnimi tarčami²² (ISECOM 2010).

Poročilo, izdelano s to metodo, je predstavljeno na eni strani s končnim indeksom RAV; primer tega je predstavljen v prilogi 7.4.

4.2 Načela razvoja analitičnega orodja

Analitično orodje mora na podlagi opredeljenih normativnih in organizacijskih specifik slovenskega okolja in spoznanj, ki so nastala med izdelavo tega dela, izpolnjevati naslednja načela:

- univerzalnost: orodje mora biti uporabno tako za upravljavce omrežij kot za organizacije, ki proizvajajo električno energijo. To pomeni, da mora takšno orodje upoštevati specifiko elektroenergetskih omrežij. To predvsem pomeni, da mora upoštevati specifiko sistemov za nadzor proizvodnje in prenosa energije, preseči pa mora nadaljnje specifične organizacij, na primer velikosti, vrste sistemov za nadzor, institucionalno okolje itd. Eno od poglavij v nadaljevanju postavljenega vprašalnika se nanaša na sistema SCADA, vendar je treba opozoriti, da je ta sistem lahko imenovan tudi kako drugače, odvisno od njegove kompleksnosti in namena.
- minimalno sodelovanje: orodje mora upoštevati, da njegov uporabnik ne bo imel nujno popolnega sodelovanja organizacije oziroma da ta ne bo želela razkriti varnostno občutljivih informacij. Običajno organizacije, ki želijo ocenjevati varnost svojih informacijskih sistemov, za ta namen uporabijo

²² Ta zadnja razmerja so zelo pomembna, ker predpostavijo avtentikacijo. Sistema z vzpostavljenim razmerjem zaupanja med seboj ne izvajata avtentikacije, zato okužba enega pomeni okužbo drugega.

najete izvajalce ali interne vire, ki naročniku zagotavljajo zaupnost rezultatov. Tu gre za akademsko delo, katerega rezultati so javno dostopni, zato je orodje treba zasnovati tako, da iz njega ne bo razvidna zasnova varnostnih sistemov organizacij, ki se jih ocenjuje. Orodje predvsem ugotavlja, ali varnostni mehanizmi obstajajo ali ne in ali so skladni z uveljavljenimi standardi. Kljub predpostavki minimalnega sodelovanja vprašalnik predpostavlja iskrenost odgovorov predstavnikov organizacije;

- preverjanje višjih plasti: večina organizacij, ki se ukvarjajo s presojanjem varnosti kritične infrastrukture, zagovarja strategijo globinske obrambe. To pomeni, da so varnostne kontrole implementirane na več različnih plasteh IKT-infrastrukture. Zavedam se, da bi ob varnostnem preverjanju vseh plasti sistemov dobil popolno varnostno sliko, vendar pa bi bil vprašalnik, ki bi varnost ugotavljal tako natančno, dolg več sto tiskanih strani. Poleg tega na veliko večino vprašanj ne bi mogel pridobiti odgovora. Vprašalnik je zato izdelan za preverjanje varnostnih mehanizmov in politik za vsa področja na najvišjih ravneh;
- zaprtost: orodje namenoma ni zasnovano tako, da bi ga bilo mogoče prilagajati, saj je njegov namen primerjalno ocenjevanje kibernetске varnosti z metodo, ki je vedno identična. Večina orodij in sistemov certificiranja je kvalitativna, zato upoštevajo tudi specifikе organizacij. Poleg tega načeloma podajo okvir za implementacijo varnostnega sistema, ki je od organizacije do organizacije različen. To orodje je namenjeno tudi primerjanju sistemov in mora zato precej običajnih predhodnih korakov varnostnih presoj opustiti. Vprašanja so tako zaprta in karseda določna, nekatera pa so vseeno postavljena tako, da od predstavnikov organizacije zahtevajo mnenje o učinkovitosti določenih sistemov. Ta kompromis omogoča, da ocenjevalec pridobi oceno učinkovitosti varnostnega sistema, ne da bi zahteval varnostno občutljive podatke;
- specifičnost slovenskega normativnega okolja: precej priporočil, ki izhajajo iz različnih vprašalnikov, standardov in orodij, se nanaša na normativna okolja, ki takšne kontrole omogočajo. Tako je na primer eno izmed pomembnih priporočil, da organizacija osebo, ki bo opravljala varnostno kritična dela, pred zaposlitvijo varnostno preveri s pomočjo neodvisne institucije. V RS je mogoče zgolj preveriti informacije, ki jih je ta oseba javno objavila. Prav tako razen

redkih izjem ni mogoče uporabljati biometričnih avtentikacijskih mehanizmov ali snemati delovnih prostorov. Določene kontrole, ki sicer večajo varnost v RS, tako torej niso mogoče.

4.3 Sestava in delovanje orodja

Orodje je sestavljeno iz vprašalnika in ocene.

Vprašalnik vsebuje določna vprašanja, na katera so mogoči naslednji odgovori:

- da;
- ne;
- ne vem in
- ne smem/želim odgovoriti.

Odgovor »ne« razen določenih izjem vedno prinese 0 točk, odgovor »da« pa različno število točk, večje od 0. Točkovanje je določeno ob vprašanjih. Orodje razdeljuje oceno varnosti v štiri sklope:

- procesi (p);
- splošni sistemi (s);
- specifični sistemi (ss);
- ljudje. (lj).

Trije sklopi so standardni sklopi vsake poslovne arhitekture. Gre za medsebojno povezane ljudi, sisteme in procese, dodana pa je specifična kategorija nadzornih sistemov.

V vsaki izmed teh kategorij seštejemo zbrano število točk in ga delimo z največjim številom točk, nato pa ga množimo s številom 10. Matematično je indeks prikazan tako:

$$\Sigma_s = s/s_{\max} \times 10$$

Tako dobimo za vsako kategorijo indeks kakovosti varnostnega sistema za to kategorijo (p, s, ss, l), skupen indeks varnosti (I) pa dobimo tako, da seštejemo vse štiri indekse in dobljeno število delimo s številom 4. Matematično indeks brez v nadaljevanju prikazanih korakov prikažemo takole:

$$I = (\Sigma_p + \Sigma_s + \Sigma_{ss} + \Sigma_{lj})/4.$$

Rezultat grafično prikažemo s polarnim grafikonom.

Med vprašanji so tudi določena kontrolna vprašanja, označena s črko k; njihov namen je ugotavljanje kakovosti in zanesljivosti odgovorov. Vprašanja postavljajo določene v več vprašalnikih izpostavljene osnovne varnostne kontrole, ki morajo biti implementirane, če ima organizacija vzpostavljen učinkovit sistem varovanja informacij. Takšnih vprašanj je sedem; vsako pozitivno vprašanje prinese točko, skupaj seštete točke pa tvorijo dodaten indeks kakovosti odgovorov (K), prikazan na lestvici od 0 do 7. Rezultat 0 pomeni zelo nezanesljive, 7 pa zelo zanesljive odgovore.

$$K = \Sigma_k$$

Odgovori »ne vem« ter »ne smem/želim odgovoriti« so vključeni tako, da odgovor »ne vem« predpostavlja, da varnostna kontrola ni implementirana, torej je enak odgovoru »ne« »ne smem/želim odgovoriti« pa predpostavlja, da sta mogoča oba odgovora. To pomeni, da je končnemu rezultatu dodano povprečje možne razlike med doseženim in nedoseženim rezultatom ter razpon možnega rezultata. Če je torej v prvem sklopu možnih 32 točk in je dosežen rezultat 25 točk, za 5 točk pa je bil odgovor »ne smem/želim odgovoriti« (n), je rezultat torej 27,5 točke, mogoč razpon pa med 25 in 30 točk.

Končni indeks je torej matematično prikazan tako:

$$I = (\Sigma_p + n_p + \Sigma_s + n_p + \Sigma_{ss} + n_p + \Sigma_l + n_p)/4.$$

V končnem rezultatu prikažemo tudi najvišji ter najmanjši možen rezultat za vsak posamezen indeks ter oba grafično prikažemo.

$$I_{\min}(\Sigma_p + \Sigma_s + \Sigma_{ss} + \Sigma_{lj})/4.$$

$$I_{\max} = (\Sigma_p + n_{p\max} + \Sigma_s + n_{p\max} + \Sigma_{ss} + n_{p\max} + \Sigma_l + n_{p\max})/4.$$

Za namene tega dela bomo postavili mejo, povezano s potrjevanjem hipoteze pri 8, torej bomo pri vrednosti 8 ali več ugotovili, da kibernetске grožnje organizacije ne ogrožajo bistveno. Pri vrednostih, manjših od 8, bomo ugotovili, da jih bistveno ogrožajo.

Celoten vprašalnik je v prilogi 1.

4.4 Primera aplikacije orodja

Potek analize

Predstavnik prve organizacije, v kateri sem izvedel analizo, je sodelovanje zagotovil pod pogojem, da iz dela ni mogoče razbrati identitete organizacije, zato je njena predstavitev zelo otežena. Gre za podjetje, ki zadostuje vsem pogojem analize.

Intervju sem opravil z dvema osebama: oseba, odgovorna za varnostni sistem, je odgovarjala na vprašanja iz sklopov 1, 2 in 4, oseba, odgovorna za varnost nadzornega sistema, pa na vprašanja iz sklopa 3. Oba intervjuja sta bila izvedena 20. decembra 2013 in sta vsak posebej trajala okoli 45 minut, saj je prva oseba odgovarjala hitro, druga oseba pa je pri večini vprašanj zahtevala pojasnila ter preverjala interno dokumentacijo. Čeprav je prva oseba odgovarjala hitro, je bilo iz načina odgovarjanja mogoče sklepati, da so odgovori resnični.

Prejetih odgovorov »ne smem/želim povedati« je bilo presenetljivo malo; takšen je bil le en odgovor in še ta je bil v sklopu kontrolnih vprašanj. Tako prikaz razpona indeksa ni potreben.

Tudi predstavnik druge organizacije je privolil v sodelovanje pod pogojem, da njegova identiteta in identiteta organizacije nista razkriti. Tudi v tem primeru gre za podjetje, ki zadostuje pogojem analize. Na vsa vprašanja je odgovoril sam, intervju je bil izveden 16. februarja 2015 in je trajal eno uro. V tem primeru odgovorov »ne smem/ne želim povedati« ni bilo.

Rezultati

Glede na odgovore, ki so podani v prilogi, je analiza pokazala rezultate, kot sledi.

Prvo podjetje

1. procesi: 22/29;
2. sistemi: 29/31;
3. specifični sistemi (SCADA): 32/37;
4. ljudje: 22,5/24,5.

Zbrano število točk pri kontrolnih rezultatih je 6,5 od 7, kar pomeni, da obstaja velika verjetnost, da so kontrole vzpostavljene zanesljivo.

Indeksi po sklopih so torej:

$$p = 7,58$$

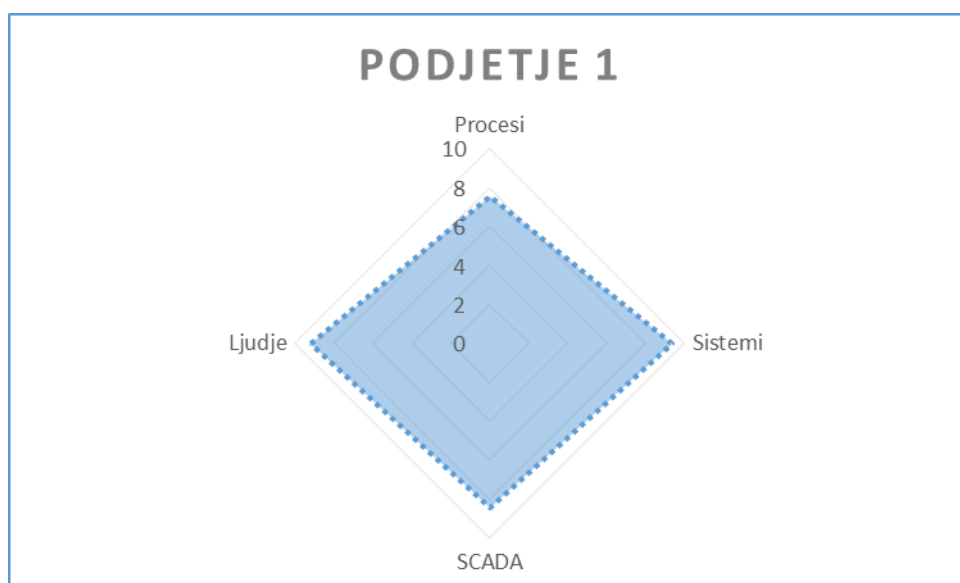
$$s = 9,35$$

$$ss = 8,45$$

$$lj = 9,18$$

Slika 4.1 prikazuje polarni grafikon indeksov za podjetje 1.

Slika 4.1: Polarni grafikon za podjetje 1



Skupni indeks, ki ga lahko pridobimo kot povprečje indeksov, pa je:

$$I = (p + s + ss + lj)/4 = (7,58 + 9,35 + 8,45 + 9,18)/4 = 8,64.$$

Drugo podjetje

1. procesi: 14/29;
2. sistemi: 16/31;
3. specifični sistemi (SCADA): 21,5/35;
4. ljudje: 9,5/24,5.

Zbrano število točk pri kontrolnih rezultatih je 3 od možnih 6, kar pomeni, da kontrole verjetno niso vzpostavljene zanesljivo.

Indeksi po sklopih so torej:

$p = 4,82$

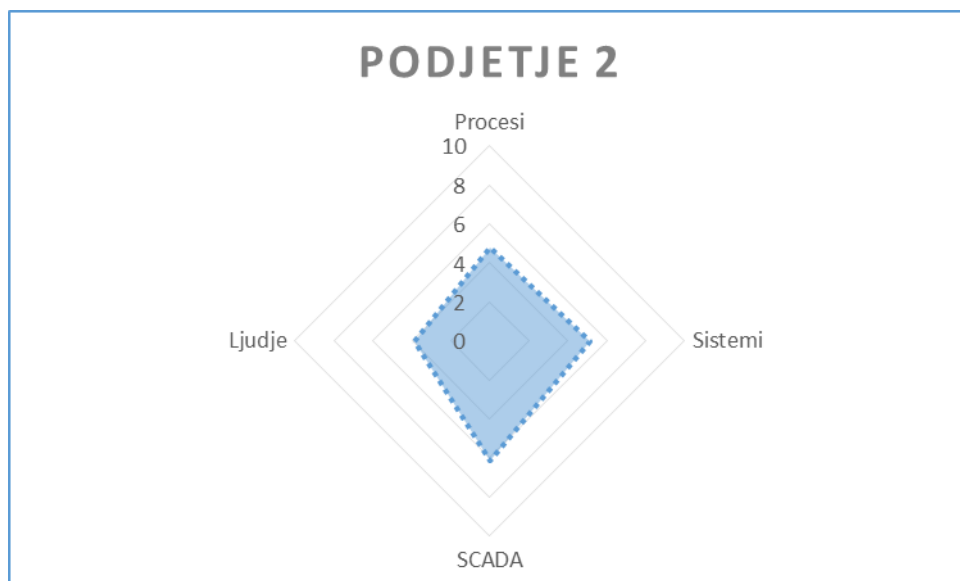
$s = 5,16$

$ss = 6,14$

$lj = 3,88$

Slika 4.2 prikazuje polarni grafikon indeksov za podjetje 2.

Slika 4.2: Polarni grafikon za podjetje 2



Skupni indeks, ki ga lahko pridobimo kot povprečje indeksov, pa je:

$$I = (p + s + ss + lj)/4 = (4,82 + 5,16 + 6,14 + 3,88)/4 = 5.$$

4.5 Interpretacija rezultatov in priporočila

Pri organizacija se pokaže izrazito nasprotje pri rezultatih. Ugotovimo lahko, da ima prvo podjetje sistem varovanja infrastrukture in informacij relativno dobro vzpostavljen, drugo podjetje pa ne, tudi kontrole, ki jih ima, verjetno niso vzpostavljene učinkovito. Ugotavljam, da je to najverjetneje povezano s financiranjem sistema, saj sta podjetji v izrazito različnih finančnih položajih.

Posebnih nasprotij med sklopi v prvem podjetju ne moremo zaznati. Največja razlika med doseženim številom točk po sklopih v prvem podjetju je 1,6, in sicer presenetljivo med procesi in sistemi. Podjetje ima vzpostavljeno kulturo procesnega vodenja, zato je nenavadno, da so najslabše ocenjeni prav procesi. Poleg tega je nepričakovan tudi rezultat, ki se nanaša na družbene vidike informacijske varnosti; ta

kategorija je namreč ocenjena višje od skupnega povprečja. Skupni indeks varnosti je pri prvem podjetju 8,64, kar pomeni, da je nad mejo, ki v orodju predstavlja bistveno ogroženost. Tako lahko ugotovimo, da kibernetске grožnje podjetja 1 ne ogrožajo bistveno.

Kot je razvidno iz priporočil, lahko identificiramo dva pomembna sklopa pomanjkljivosti: prvi je, da očitno zaposleni, ki se ukvarjajo z informacijsko varnostjo, pri svojem delu niso povsem samostojni in verjetno dokaj slabo koordinirajo svoje delo; drugi je, da je podjetje za informacijsko varnost sistema SCADA očitno razvilo svojo lastno metodologijo, ki v širšem okolju ni uveljavljena kot dobra praksa.

Pri podjetju 2 lahko ugotovimo, da ga kibernetске grožnje bistveno ogrožajo, saj je vrednost skupnega indeksa 5. Pri rezultatih je prišlo tudi do višjega odstopanja med največjo in najmanjšo vrednostjo, 2,26, tokrat pričakovano med varnostjo sistema SCADA in družbenimi vidiki informacijske varnosti. Zadnji indeks je najnižji, kar pomeni, da družbeni vidiki kibernetских groženj v podjetju 2 predstavljajo večji vir ogrožanja varnosti kot tehnični.

Iz aplikacije analitičnega orodja lahko za podjetje 1 izvedemo naslednja priporočila:

- vzpostaviti je treba s priznano metodologijo certificiran sistem neprekinjenega poslovanja;
- vzpostaviti je treba fizično in tehnično varovanje na vseh oddaljenih enotah;
- dokumentirati je treba vse procese, ki potekajo v organizaciji;
- osebe in organizacijske oddelke, ki funkcionalno pokrivajo področje fizične in informacijske varnosti ter varnosti nadzornih sistemov, je treba združiti v enotni služni ali skupni stalni delovni skupini;
- zagotoviti je treba, da so organizacijski oddelki in osebe, ki funkcionalno pokrivajo področje fizične in informacijske varnosti ter varnosti nadzornih sistemov (SCADA), v snovanju varnostnih politik in tehnik neodvisni od svojih neposredno nadrejenih, če ti niso člani ožjega vodstva ali vodje varnostne službe;
- vzpostaviti je treba kontrole, ki zagotavljajo, da je nemogoče zlorabljati računalniško opremo (uporaba za nezakonite namene), ne da bi bilo to ugotovljeno;

- izdelati je treba politiko arhiviranja podatkov, ki vsebuje klasifikacijo in roke hranjenja določenih vrst podatkov;
- potrebna je ponovna izvedba penetracijskega testa za sistem SCADA;
- oceno tveganj za varnostni sistem SCADA je treba dopolniti tako, da bo izdelana na podlagi uveljavljene metodologije;
- treba je izdelati varnostno oceno sistema SCADA skladno z uveljavljenimi smernicami in standardi oziroma metodologijo;
- vzpostaviti je treba politiko rednega preverjanja zadovoljstva zaposlenih;
- vzpostaviti je treba učinkovit proces odzemanja nepotrebnih delovnih sredstev posameznikom, ki so premeščeni na drugo delovno mesto.

Priporočila, ki izhajajo iz analize v podjetju 2, so sledeča:

- vzpostaviti je treba skladno s priznano metodologijo certificiran sistem vodenja (npr. ISO 9001);
- vzpostaviti je treba skladno s priznano metodologijo certificiran sistem varovanja informacij (npr. ISO 27001);
- vzpostaviti je treba skladno s priznano metodologijo certificiran sistem neprekinjenega delovanja (npr. ISO 22301);
- v organizaciji je treba določiti vodjo oz. menedžerja varstva informacij;
- vzpostaviti je treba politiko določanja občutljivosti informacij;
- izdelati je treba seznam kritičnih procesov in sredstev;
- izdelati je treba politiko testiranja varnostnih načrtov in načrtov neprekinjenega poslovanja;
- izdelati je treba analizo tveganj po priznani in uveljavljeni kvalitativni in kvantitativni metodi;
- izdelati je treba splošen katalog občutljivih informacij;
- dokumentirati je treba vse procese, ki potekajo v organizaciji;
- izdelati je treba načrt neprekinjenega poslovanja;
- izdelati je treba politiko obvladovanja računalniških računov;
- za dostop do domene je treba uvesti vsaj še en avtentikacijski mehanizem;
- zagotoviti je treba, da vse delovne postaje v organizaciji izpolnjujejo varnostno politiko;

- vzpostaviti je treba politiko obvladovanja dnevnikov varnostno pomembnih dogodkov; dnevnike je treba ustrezno zavarovati in preprečiti vpogled nepooblaščenim osebam;
- vzpostaviti je treba kontrole, ki zagotavljajo, da je nemogoče zlorabljati računalniško opremo (uporaba za nezakonite namene), ne da bi bilo to ugotovljeno;
- izdelati je treba politiko nadzora dostopa do sistemov;
- izdelati je treba splošno IKT-strategijo;
- izdelati je treba politiko obvladovanja programske opreme;
- izdelati ali vzpostaviti je treba standarde vzdrževanja in obvladovanja sprememb v sistemih;
- izdelati je treba politiko arhiviranja podatkov, ki vsebuje klasifikacijo in roke hranjenja določenih vrst podatkov;
- izdelati je treba politiko sledenja spremembam podatkov;
- izdelati je treba politiko odzivanja na varnostne incidente;
- izvesti je treba testiranje varnostne zanesljivosti omrežja s simulacij napada, prek interne »rdeče ekipe« ali prek najetega izvajalca;
- omrežje sistema SCADA je treba logično izolirati od preostalega informacijskega omrežja organizacije;
- izvesti je treba penetracijski test sistema SCADA;
- oceno tveganj za varnostni sistem SCADA je treba dopolniti tako, da bo izdelana na podlagi uveljavljene metodologije;
- izvesti je treba vajo, ki bi preverila delovanje načrta sistema SCADA;
- na ravni vseh posameznih točk sistema SCADA je treba vgraditi mehanizme za zaznavanje vdora;
- izvesti je treba oceno tveganj za omrežje SCADA, ki temelji na uveljavljeni metodologiji (npr. OICM);
- onemogočiti je treba, da bi uporabniki sisteme, ki so povezani v sistem SCADA, uporabljali za zasebne namene (npr. brskanje po spletu, e-pošta ipd.);
- onemogočiti je treba vse nepotrebne povezave v omrežje sistema SCADA;
- onemogočiti je treba vse nepotrebne storitve v omrežju SCADA;
- izdelati je treba varnostno oceno sistema SCADA skladno z uveljavljenimi smernicami in standardi oziroma metodologijo;

- za nadzorne sisteme v omrežju SCADA je treba uvesti vsaj še en dodaten identifikacijski mehanizem;
- izdelati je treba kodeks ravnanja oziroma etični kodeks uslužbencev;
- vzpostaviti je treba proces sledenja vsem identifikacijskim karticam, ključem, prenosnikom, službenim telefonom, sredstvom za oddaljen dostop ipd;
- vzpostaviti je treba učinkovit proces odvzemanja nepotrebnih delovnih sredstev posameznikom, ki so premeščeni na drugo delovno mesto;
- izvesti je treba varnostno usposabljanje, ki vsebuje zaznavanje in preprečevanje napadov s socialnim inženiringom za vse zaposlene;
- izvesti je treba test napada s socialnim inženiringom;
- izvesti je treba varnostne ukrepe, ki se nanašajo specifično na preprečevanje napadov s socialnim inženiringom;
- jasno je treba definirati naloge in odgovornosti vseh zaposlenih;
- uvesti je treba redno preverjanje delovanja varnostnih politik, ki se ukvarjajo z izdajanjem informacij osebja;
- uvesti je treba ukrepe, na podlagi katerih bo zagotovljeno razumevanje zaposlenih, da bodo v primeru kršenja varnostih politik verjetno sankcionirani;
- vzpostaviti je treba učinkovit sistem obveščanja zaposlenih o spremembah varnostnih politik.

5 Razprava in zaključek

5.1 Razprava

To delo je v prvem delu opredelilo temeljne koncepte in kontekstualiziralo njihovo razumevanje. Tako smo najprej razdelali razlikovanje med pojmom kibernetika in kibernetiko, nato pa ugotovili, da varnost elektroenergetske kritične infrastrukture ni predmet nacionalne ali mednarodne varnosti sama po sebi, temveč postane skozi proces sekuritizacije predmet societalne varnosti. Ob opredelitvi pojmov energetska in informacijska varnost pa smo lahko spoznali, da sta ta opredeljena s tehničnimi in ekonomskimi, manj pa s pojmi iz obramboslovnih in varnostnih ved. Bolj jasno opredeljen je pojem kritične infrastrukture, saj je vsem definicijam skupno, da jo opredelijo kot infrastrukturo, katere motenje bi bistveno vplivalo na delovanje družbe. Pomembna ugotovitev je, da je institucionalni okvir slovenske elektroenergetske kritične infrastrukture nominalno sicer dodelan, funkcionalno pa ne, predvsem zaradi neizpolnjenega namena družbe SODO, kar verjetno pomeni, da je samo zaradi tega dejstva ranljivost sistema višja, kot bi morala biti.

Delo veliko pozornosti nameni industrijskim sistemom za nadzor, torej ICS oz. SCADA, ki delujejo v enotnem informacijskem okolju, uporabljajo razširjene protokole, kot sta ethernet in TCP/IP, in so prek teh odprti v informacijsko okolje družb, ki si jih lastijo, nikdar pa niso bili zasnovani tako, da bi s temi parametri delovali varno. Njihova ranljivost je zato visoka, če jih upravitelji dodatno ne zavarujejo. To predstavlja težavo tako zaradi morebitnega padca zmogljivosti sistema kot tudi zaradi visokih stroškov tega. Ugotovili pa smo lahko, da danes že obstajajo protokoli za sisteme SCADA, ki si ponujajo določene, četudi zelo nepopolne varnostne mehanizme.

Po tem pregledu smo pregledali varnostne standarde in priporočila informacijske varnosti in poskušali najti takšne, ki so ustrezni tudi za sisteme SCADA. Ugotovili smo lahko, da tudi ti obstajajo, se pa ne razlikujejo bistveno od splošnih standardov informacijske varnosti. V nadaljevanju smo razčlenili taksonomijo zlonamerne programske kode ter vektorje in vrste napadov. Ugotovili smo, da so najučinkovitejši napadi tisti, ki so usmerjeni v uporabnike in ne takšni, ki so usmerjeni v tehnične sisteme. Slednji namreč ne kršijo vzpostavljenih varnostnih politik in protokolov, prvi pa delujejo bolj nedosledno. Ugotovili smo lahko, da številni avtorji tudi iz lastnih

izkušenj trdijo, da noben varnostni sistem ni učinkovit, če uporabniki sistema niso varnostno ozaveščeni. Na koncu konceptualno-teoretičnega okvirja smo pregledali še tehnične in organizacijske rešitve za izboljšanje informacijske varnosti, ob tem pa je bila predvsem pri tehničnih rešitvah pomembna ugotovitev, da se med seboj nominalno enakovredne rešitve med seboj močno razlikujejo. Tako na primer protivirusna aplikacija lahko deluje zgolj na podlagi znanih zapisov zlonamerne kode, kar danes pomeni neprimerno zaščito sistema. Ustreznejše so aplikacije, ki nudijo tudi hevristično zaznavanje zlonamerne kode.

V empiričnem delu smo opravili pregled obstoječih metod in delovnih okvirjev, ki se nanašajo na informacijsko varnost, ter ugotovili, da se med seboj močno razlikujejo, saj nekateri zahtevajo specifične kontrole točke, drugi pa postavijo zgolj okvir, na podlagi katerega bo upravitelj informacijskega sistema sam vzpostavil varnostne kontrole. Nekatere metode tudi način ocenjevanja varnosti prepustijo upravitelju, druge pa postavijo detajlna merila za določitev intervalnega indeksa. Takšen indeks sem poskušal ustvariti tudi sam in mi je (po lastnem mnenju) to tudi uspelo. S tem namenom sem ustvaril analitično orodje, ki se je izkazalo kot uporabno za nominalno oceno varnosti informacijskega sistema dveh gospodarskih družb, ki delujeta na področju slovenske elektroenergetske kritične infrastrukture.

ENISA ugotavlja, da se svet vsak dan sooči s 350.000 novimi variantami zlonamerne programske kode in da se je število opaženih napadov med letoma 2013 in 2014 podvojilo. Ogroženost se povečuje v desetih od 15 sklopov groženj (ENISA 2014: 14). Ta dva podatka nam povesta, da je varnost informacijskih sistemov, ki kot koncept obstaja že več kot 30 let, danes pomembnejša, kot je bila kadarkoli prej. Medtem ko se nenehno širi površina za možen napad in se diverzificirajo vektorji in tipi napadov, organizacije ugotavljajo, da ta varnost postaja tudi vse kompleksnejša. Po drugi strani lahko ugotovimo, da se ogroženost informacijskih sistemov ne veča bistveno. Pregled varnostnih incidentov nam namreč pove, da se kljub hitremu in opaznemu večanju števila napadov škoda, ki jo ti napadi povzročijo, ne veča bistveno (Valeriano in Maness 2015). Iz tega lahko sklepamo, da organizacije vlagajo v informacijsko varnost, po drugi strani pa so organizacije, ki tega ne počnejo, ogrožene vse bolj, kar je razvidno tudi iz rezultatov tega dela.

To delo je ponudilo orodje za nominalen pregled varnosti informacijskih sistemov v okoljih, ki uporabljajo sisteme SCADA, torej tudi sisteme, ki upravljajo ključno infrastrukturo na področju oskrbe z električno energijo. Nujno pa je treba poudariti, da takšen pregled ne zadostuje za kakovostno oceno varnosti informacijskih sistemov. Za to je namreč potreben natančen pregled, pri katerem ima presojevalec dostop do informacijskega sistema organizacije. Kot je na primer opredeljeno v standardih informacijske varnosti v družini ISO 27000, je potrebna vzpostavitev kontrol in politik, ob tem pa je družbi praktično prepuščena izbira, kako bo te kontrole vzpostavila. To je tako odvisno predvsem od kompetenc osebe ali organizacije, ki takšen sistem vzpostavlja. Enako velja za presojevalce po številnih drugih metodah, npr. penetracijskih testov, izvajalcev izobraževanj, nabave infrastrukturne opreme in podobno. Kot je vedno znova razvidno iz primerov prakse, veliko družb ne deluje proaktivno, če jih v to ne prisili institucionalni okvir in se odzovejo šele, ko pride do uspešnega napada. Primer tega je, ko se organizacija okuži s cryptolockerjem in plača več tisoč evrov za rešitev svojih podatkov, pri čemer bi bila enaka investicija zadostna za to, da bi se takšen napad lahko preprečil.

V svojem poklicu se vsakodnevno srečujem z varnostjo informacijskega sistema in ugotavljam, da so napadi z zlonamerno programsko kodo takšni, da jih sama tehnična zasnova sistema težko zajezi. Poleg tega je, kot je razvidno iz teoretičnega dela, vedno treba tehtati med varnostjo in možnostjo uporabe sistema. Ugotavljamo, da sta najpogostejša vektorja napada elektronska pošta in USB-ključki, ki jih zaposleni prinesejo od doma. Tu se moramo torej odločati: ali bomo filter elektronske pošte, ki deluje tako glede na zapise kot hevristično, nastavili tako, da zaposleni gotovo ne bodo dobivali pošte, ki vsebuje zaznane napade z ribarjenjem in s tem tvegali, da zaposleni občasno ne bodo dobili relevantne pošte, ali pa se bomo zanašali na zaposlene, da ne bodo odprli priponke v elektronski pošti, ki jo je filter spustil, ker ji ni določil dovolj visokega indeksa zaznanega napada (lahko gre na primer za povsem nov napad). Podobno se srečujemo z vprašanjem, ali bomo za zaposlene onemogočili uporabo USB-ključkov ali pa bomo pričakovali, da bo končna protivirusna aplikacija napad prestregla, ko bo zaposleni v računalnik vstavil USB-ključek. Problematična je predvsem elektronska pošta, saj ta predstavlja tveganje, ki je odvisno predvsem od zaznavanja uporabnika pošte. Tudi iz lastnih izkušenj ugotavljam, da so ti napadi vse bolj prepričljivi in kompleksni in da lahko tudi najbolj

izkušeni uporabniki nenamerno namestijo zlonamerno programsko kodo s klikom na priponko v e-poštnem sporočilu; ta je lahko na primer račun za komunikacijske storitve ali pa dobronamerno opozorilo varnostnega strokovnjaka, ki iz vašega naslova dobiva nenavadno veliko sporočil z virusi in vam pošilja varnostno poročilo.

Administratorji tako moramo razmišljati in delovati kompleksno ter dograjevati in dodatno plastiti varnostni sistem. Postavljati moramo logične in fizične prepreke na vseh korakih ter investirati v varnostni sistem. Tako smo v organizaciji, v kateri sem zaposlen, v zadnjem letu na področju varnosti vpeljali tri nove samostojne varnostne sisteme (požarni zid z vgrajenim IDS/IPS, sistem za nadzor mobilnih naprav in filter poštnega protokola SMTP), vseeno pa se srečujemo z uspešnimi napadi, predvsem zaradi neznanja uporabnikov ali pa celo zaradi njihovega odklanjanja vzpostavljenih varnostnih politik.

5.2 Potrditev hipotez

Prvo hipotezo za podjetje 1 potrdim, za podjetje 2 pa zavrnem. Nasprotno drugo hipotezo za podjetje 1 zavrnem, za podjetje 2 pa potrdim. Po eni strani je v prvem podjetju sistem varovanja infrastrukture in informacij vsaj nominalno dobro postavljen, organizacija pa tudi ustrezno vlaga v varnostno ozaveščanje svojih zaposlenih. Pri pregledu druge organizacije pa lahko ugotovimo, da sistema varovanja infrastrukture in informacij nima dobro postavljenega, po drugi strani pa so zaposleni po pričakovanjih največji dejavnik ogrožanja. Prvotni namen tega dela je bil, da bi to analizo izvedel na vsaj večini subjektov, ki delujejo v slovenskem elektroenergetskem sistemu, vendar se je izkazalo, da skoraj nobena organizacija ni želela sodelovati. Še pri predstavnikih, ki so v sodelovanje privolili, je bila privolitev pogojena z zagotovilom, da njihova identiteta ni razkrita. Če bi lahko izvedli analizo na vseh omenjenih organizacijah, bi lahko pridobili nominalni indeks zaščite celotnega slovenskega elektroenergetskega sistema. To bi ocenil kot precejšen znanstven prispevek k razumevanju varnosti slovenske kritične infrastrukture, na žalost pa se mora domet tega dela ustaviti pri izdelavi in primeru aplikacije orodja.

Veljavnost rezultatov lahko dodatno pretehtamo še s pregledom medijskih objav, ki bi omenjale varnostne incidente na področju elektroenergetske kritične infrastrukture; v Sloveniji jih še nismo zaznali, redki pa so tudi v tujini. Prvi kibernetiski napad v Evropi na ta segment kritične infrastrukture je bil zaznan v letu 2012. Šlo je za napad DDoS,

ki ni prizadel elektroenergetskega omrežja (Neslen 2012), iz česar lahko sklepamo, da kibernetski viri na splošno bistveno ne ogrožajo slovenske elektroenergetske kritične infrastrukture. Vsekakor pa bi bilo za zanesljivost te trditve treba analizirati vsa podjetja, ki sodelujejo pri upravljanju elektroenergetskega omrežja v Sloveniji.

Pomembno je tudi, v kakšnem splošnem varnostnem okolju deluje sistem, saj je gotovo, da bi ob koordiniranem in tehnično izpopolnjenem napadu napadalci lahko vdrli v vsak informacijski sistem in povzročili škodo, kar potrjuje primer Stuxneta. Nadalje je iz pričevanj Edwarda Snowdna povsem mogoče, da so informacijski sistemi, s katerimi upravljamo elektroenergetsko kritično infrastrukturo, že okuženi z zlonamerno programsko kodo, ki pa lahko zgolj pasivno zbira podatke ali pa je v stanju mirovanja in bi lahko njeno delovanje sprožili ob določenem dogodku.

5.3 Priporočila za nadaljnje raziskovanje

Poudariti je treba, da je za zanesljive rezultate za slovenski elektroenergetski sistem potrebna temeljitejša analiza. Orodje, predstavljeno v tem delu, bi lahko bilo primerno za izvajanje analize vrzeli, torej za primerjanje zaznane in dejanske stopnje varnosti. Tako bi lahko na primer za organizacijo aplicirali najprej to orodje, nato pa še analizo z metodologijo SSTM. Glede na moje poznavanje vsaj ene izmed teh dveh organizacij menim, da bi bila vrzel velika in bi lahko odprla vprašanje razmerja med zaznano in dejansko ogroženostjo sistema.

Pri izdelavi dela sem se moral zaradi nesodelovanja ustaviti pri zgolj dveh subjektih. Priporočim lahko, da bi aplicirali orodje še na vse preostale gospodarske družbe, ki delujejo na področju upravljanja slovenske elektroenergetske kritične infrastrukture. S tem bi namreč pridobili celovit nominalen pregled kibernetske varnosti na tem področju, kar bi bila lahko dobra iztočnica za priporočila za izboljšanje varnosti ter primerjave med sistemi. Iz nje bi lahko na podlagi drugih raziskav izvedli pomembne sklepe, kako dobro so informacijski sistemi teh družb zavarovani in kaj na to varnost vpliva.

Kot primer tega lahko odprem pomembno vprašanje, ki se je nakazalo po naključju; po javno dostopnih podatkih je organizacija, ki ima bistveno bolje organizirano informacijsko varnost v veliko boljšem finančnem položaju kot druga organizacija. Tako je ustrezno raziskovalno vprašanje, kako finančno stanje organizacije vpliva na

njeno organizacijo varnostnega sistema. To je še posebej pomembno, če gre za organizacijo, ki je opredeljena kot upravljavec kritične infrastrukture. Če bi se izkazalo, da sta finančno neugoden položaj in slaba informacijska varnost v kavzalnem razmerju, bi to po mojem mnenju odprlo prostor za pomemben premislek o tem, kako organizirati politiko obvladovanja takšnih organizacij, da ne bo ogroženo delovanje slovenske elektroenergetske kritične infrastrukture.

6 Literatura

- Abrams, Marshall in Joe Weiss. *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*. Dostopno prek: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf (12. junij 2015).
- Alberts, Christopher J. in Audrey J. Dorofee. 2001. *OCTAVE Criteria, Version 2.0*. Pittsburgh: Carnegie Mellon University. Dostopno prek: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2001_005_001_13871.pdf (09. april 2015).
- ARNES. 2015. *Poročilo o omrežni varnosti za leto 2014*. Dostopno prek: https://www.cert.si/wp-content/uploads/2015/05/Porocilo-o-omrezni-varnosti_2014.pdf (10. junij 2015).
- Austin, Thomas H. 2010. Designing a Secure Programming Language. V *Handbook of Information and Communication Security*, ur. Peter Stavroulakis in Mark Stamp, 433–448. New York: Springer.
- BBC. 2003. *Virus-like attack hits web traffic*. Dostopno prek: <http://news.bbc.co.uk/2/hi/technology/2693925.stm> (21. september 2013).
- --- 2012. *Flame malware makers send »suicide« code*. Dostopno prek: <http://www.bbc.co.uk/news/technology-18365844> (21. september 2013).
- Bernik, Igor in Kaja Prislan. 2012. *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede, univerza v Mariboru.
- Bhattacharyya, Debnath. 2008. The Taxonomy of Advanced SCADA Communication Protocols. *Journal of Security Engineering* 12 (6): 517–526.
- Byres, Eric J. 2004. *The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems*. Dostopno prek: <http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf> (21. september 2013).

- --- 2012. *Using ANSI/ISA-99 Standards to Improve Control System Security*. Dostopno prek: <http://www.tofinosecurity.com/downloads/589> (21. september 2013).
- Bohi, Douglas R. in Michael A. Toman. 1996. *The Economics of Energy Security*. Boston: Kluwer Academic Publishers.
- Boiten, Eerke in Julio Hernandez-Castro. 2014. *Interdisciplinary Research Centre in Cyber Security at the University of Kent in Canterbury second online survey*. Dostopno prek: <http://www.cybersec.kent.ac.uk/Survey2.pdf> (04. april 2015)
- Calder, Alan. 2005. *A business guide to information security*. London: Kogan Page.
- Canetti, Ran. 2004. *Universally Composable Signature, Certification, and Authentication*. Dostopno prek: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.79.4596&rep=rep1&type=pdf> (21. september 2013).
- Caralli, Richard A., James F. Stevens, Lisa R. Young in William R. Wilson. 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Pittsburgh: Carnegie Mellon University. Dostopno prek: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf (09. april 2015).
- Cleghorn, Lance. 2013. Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *Journal of Information Security* 4, 144–149.
- Cornell University Law School. 2015. *44 U.S. Code § 3542 – Definitions*. Dostopno prek: <https://www.law.cornell.edu/uscode/text/44/3542> (28. marec 2015).
- Cowan, Crispin, Perry Wagle, Calton Pu, Steve Beattie in Jonathan Walpole. 1999. *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*. Dostopno prek: <http://users.ece.cmu.edu/~adrian/630-f04/readings/cowan-vulnerability.pdf> (21. september 2013).
- Dierks, T. 2008. *The Transport Layer Security (TLS) Protocol*. Dostopno prek: tools.ietf.org/html/rfc5246 (21. september 2013).

- Dimesnional engineering. 2011. *The Risk of Social Engineering on Information Security: a Survey of it Professionals*. Dostopno prek: <http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf> (21. september 2011).

- *Direktiva sveta ES št. 114/2008 z dne 8. decembra 2008 o ugotavljanju določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite*. Dostopno prek: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:SL:PDF> (21. september 2013).

- Duggan, David P. *Penetration Testing of Industrial Control Systems*. Albuquerque: Sandia National Laboratories. Dostopno prek: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf (21. september 2013).

- Dulaney, Emmett in Chuck Eastomm. 2014. *CompTIA Security+ Study Guide: SY0-401*. Indiannapolis: John Wiley & Sons, Inc.

- ENISA. 2014. *Cramm-Site*. Dostopno prek: http://rm-inv.enisa.europa.eu/methods/m_cramm.html (16. oktober 2014).

- Erbschloe, Michael. 2005. *Trojans, worms and spyware*. Burlington: Elsevier Inc.

- Falliere, Nicholas, Liam O. Murchu in Eric CHien. 2011. *W32.Stuxnet Dossier*. Cupertino: Symantec Corporation. Dostopno prek: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (21. september 2013).

- Filiol, Eric. 2010. Viruses and Malware. V *Handbook of Information and Communication Security*, ur. Peter Stavroulakis in Mark Stamp, 433–448. New York: Springer.

- Goodchild, Joan. 2011. *The Ultimate Guide to Social Engineering*. Dostopno prek: <http://assets.csoononline.com/documents/cache/pdfs/Social-Engineering-Ultimate-Guide.pdf> (21. september 2013).

- Greeno, Cherri. 2003. Blackout crash injuries claim teen; He was hit on Speedvale Avenue on the night the power went out. *The Record* (25. avgust). Dostopno prek: <http://pqasb.pqarchiver.com/therecord/doc/355524939.html?FMT=ABS&FMTS=ABS:FT&type=current&date=&author=&pub=&edition=&startpage=&desc=> (21. september 2013).
- Gundert, Levi. 2009. Total gridlock. *Jane's intelligence review* 21 (11): 25–27.
- Gutmann, Barbara in Edward A. Roback. 1995. *An Introduction to Computer Security: The NIST Handbook*. Gatithersburg: National Institute of Standards and Technonolgy. Dostopno prek: <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf> (21. september 2013).
- Heylighen, Francis in Cliff Joslyn. 2001. Cybernetics and Second-Order Cybernetics. V *Encyclopedia of Physical Science & Technology* (3rd ed.), ur. Meyers, R.A., 2–24. New York: Academic Press).
- Hruska, Joel. 2014. *Synology NAS devices targeted by hackers, demand Bitcoin ransom to decrypt files*. Dostopno prek: <http://www.extremetech.com/extreme/187518-synology-nas-devices-targeted-by-hackers-demand-bitcoin-ransom-to-decrypt-files> (25. marec 2015).
- *Inštitut za slovenski jezik Frana Ramovša ZRC SAZU*. Dostopno prek: <http://bos.zrc-sazu.si/sskj.html> (21. september 2013).
- International energy agency. 2013. *Topic: Energy security*. Dostopno prek: <http://www.iea.org/topics/energysecurity/> (21. september 2013).
- ISECOM. 2010. *The Open Source Security Testing Methodology Manual*. Cardedeu: ISECOM Spain.
- ISO/IEC. 2005. *ISO/IEC 27001: 2005*. Ženeva: ISO Copyright office.
- Janczewski, Lech J. in Andrew M. Colarik. 2007. *Cyber warfare and cyber terrorism*. Hershey: Information science reference.
- Javna agencija RS za energijo. 2013. *Elektroenergetska podjetja*. Dostopno prek: <http://www.agen->

rs.si/sl/informacija.asp?id_informacija=870&id_meta_type=37&type_informacij= (21. September 2013).

- Juniper Networks. 2010. *Architecture for Secure SCADA and Distributed Control System Networks*. Dostopno prek: <http://www.juniper.net/us/en/local/pdf/whitepapers/2000276-en.pdf> (05. april 2015).

- Kalapatapu, Rao. 2004. *Scada protocols and communication trends*. Dostopno prek: <http://www.isa.org/journals/intech/TP04ISA048.pdf> (21. september 2013).

- Kaspersky Lab. 2012. *Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat*. Dostopno prek: http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat (21. september 2013).

- Kifayat, Kashif, Madjid Merabti, Qi Shi in David Llewellyn-Jones. 2010. *Security in Wireless Sensor Networks. V Handbook of Information and Communication Security*, ur. Peter Stavroulakis in Mark Stamp, 433–448. New York: Springer.

- Knapp, Eric D. 2011. *Industrial network security : securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*. Waltham: Elsevier.

- Krutz, Ronald L. 2006. *Securing Scada systems*. Indianapolis: Wiley Publishing.

- Liotta, Peter H. 2002. Boomerang Effect: The Convergence of National and Human Security. *Security Dialogue* 33(4): 473–488.

- Lukasik, Stephen J., Seymour E. Goodman in David W. Longhurst. 2003. *Protecting Critical Infrastructures Against Cyber – Attack*. New York: Oxford university press.

- Mabro, Robert. 2008. On the Security of Oil Supplies, Oil Weapons, Oil Nationalism and All That. *OPEC Energy Review* 32 (1): 1–12.

- Makhija, Jay. 2003. Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus. Dostopno prek:

http://www.ee.iitb.ac.in/~esgroup/es_mtech03_sem/sem03_paper_03307905.pdf (21. september 2013).

- Manjikian, Mary McEvoy. 2010. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* 54: 384–401.

- Matrosov, Alexandr, Eugene Rodionov, David Harley in Juraj Malcho. 2010. *Stuxnet Under the Microscope*. Dostopno prek: http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (21. september 2013).

- McAfee. 2011. *McAfee Threats Report: Second Quarter 2011*. Dostopno prek: <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf> (21. september 2013).

- McDonald, Matt. 2008. Securitization and the Construction of Security. *European Journal of International Relations* 2008 (14): 563–588.

- McMillan, Robert. 2010. *Siemens: Stuxnet worm hit industrial systems*. Dostopno prek: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142 (21. september 2013).

- Meserve, Jeanne. 2007. Sources: Staged cyber attack reveals vulnerability in power grid. *CNN*, 26. september. Dostopno prek: <http://edition.cnn.com/2007/US/09/26/power.at.risk/> (21. september 2013).

- Meše, Pavel. 2003. *Varnost v elektronskih komunikacijah in informacijski tehnologiji*. Ljubljana: Elektrotehniška zveza Slovenije.

- Ministrstvo za gospodarstvo. 2010a. *Energetska bilanca Republike Slovenije za leto 2010*. Dostopno prek: http://www.mg.gov.si/fileadmin/mg.gov.si/pageuploads/Energetika/Porocila/EBRS_2010.pdf (21. september 2013).

- --- 2010b. *Zbrana gradiva o reorganizaciji elektrodistribucijskih podjetij*. Dostopno prek: http://www.mg.gov.si/fileadmin/mg.gov.si/pageuploads/Energetika/Porocila/Reorganizacija_DIS.pdf (21. september 2013).
- Mitnick, Kevin D. 2002. *The art of deception*. Indianapolis: Wiley publishing.
- Møller, Bjorn (2004): *National, Societal and Human Security: Discussion – Case Study of the Israel-Palestine Conflict*. Dostopno prek: www.humsamf.au.dk/~bm/012_Moeller.pdf (21. september 2013).
- Moteff, John in Paul Parfomak. 2004. *Critical Infrastructure and Key Assets: Definition and Identification*. Dostopno prek: www.fas.org/sgp/crs/RL32631.pdf (21. september 2013).
- Naughton, John. 2012. How Flame virus has changed everything for online security firms. *The Guardian*, 17. junij. Dostopno prek: <http://www.theguardian.com/technology/2012/jun/17/flame-virus-online-security> (21. september 2013).
- Neslen, Arthur. 2012. *European renewable power grid rocked by cyber-attack*. Dostopno prek: <http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541> (12. junij 2015).
- New York Independent System operator. 2005. *Blackout August 14, 2003 Final Report*. Dostopno prek: http://www.nyiso.com/public/webdocs/media_room/press_releases/2005/blackout_rpt_final.pdf (21. september 2013).
- NIST. 2009. *Recommended Security Controls for Federal Information Systems and Organizations*. Dostopno prek: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (21. september 2013).
- --- 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems*. Dostopno prek: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf> (05. januar 2015)

- --- 2012. *Guide for Conducting Risk Assessments*. Dostopno prek: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (18. maj 2014).
- OECD. 2008. *Protection of »Critical Infrastructure« and the Role of Investment Policies Relating to National Security*. Dostopno prek: www.oecd.org/daf/inv/investment-policy/40700392.pdf (21. September 2013).
- Patton, Michael Q. 1987. *How to Use Qualitative Methods in Evaluation*. Thousand Oaks: Sage publications.
- Peltier, Thommas R. 2001. *Information Security Risk Analysis*. Boca Raton: Auerbach Publications.
- Pctools. 2013. *What is a Keylogger?* Dostopno prek: <http://www.pctools.com/security-news/what-is-a-keylogger/> (21. september 2013).
- Pfleeger, Charles P. in Shari L. Pfleeger. 2003. *Security in Computing*. Boston: Pearson Edicaton, Inc.
- Poulsen, Kevin. 2008. Did Hackers Cause the 2003 Northeast Blackout? *Wired Magazine* (29. maj). Dostopno prek: <http://www.wired.com/threatlevel/2008/05/did-hackers-cau> (21. september 2013).
- Prezelj, Iztok. 2000. *Varnost družbe kot večdimenzionalni pojav (oblikovanje metodološkega modela proučevanja ogrožanja varnosti)*. Magistrsko delo. Ljubljana: Fakulteta za družbene vede.
- --- 2009. Nacionalna kritična infrastruktura v Republiki Sloveniji. *Teorija in praksa* 4 (46): 464–484.
- ---, ur. 2010. *Kritična infrastruktura v Sloveniji*. Ljubljana: Fakulteta za družbene vede.
- Radvanovsky, Robert in Jacob Brodsky. 2013. *Handbook of SCADA/Control systems security*. Boca Raton: Taylor & Francis Group.

- Ramzan, Zulfikar. 2010. Phishing Attacks and Countermeasures. V *Handbook of Information and Communication Security*, ur. Peter Stavroulakis in Mark Stamp, 433-448. New York: Springer.
- Richards, Larry. 2007. *A Larry Richards Reader 1987–2007*. Dostopno prek: <http://polyproject.wikispaces.com/file/view/Larry+Richards+Reader+6+08.pdf> (21. september 2013).
- Riptech. 2001. *Understanding SCADA System Security Vulnerabilities*. Dostopno prek: <http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf> (21. september 2013).
- Robles, Rosslin John in Min-kyu Choi. 2009. Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems. *International Journal of of Grid and Distributed Computing* 2 (2): 27–34.
- Rossi, Peter H., Mark W. Lipsey in Howard E. Freeman. 1999. *Evaluation: a systemic approach*. Thousand oaks: Sage Publications.
- Sanger, David E. 2013. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*, 1. junij. Dostopno prek: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2 (21. september 2013).
- SANS institute. 2002. *A Qualitative Risk Analysis and Management Tool – CRAMM*. Dostopno prek: <http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83> (04. november 2014).
- --- 2005. *Security for Critical Infrastructure SCADA Systems*. Dostopno prek: <http://www.sans.org/reading-room/whitepapers/warfare/security-critical-infrastructure-scada-systems-1644?show=security-critical-infrastructure-scada-systems-1644&cat=warfare> (21. september 2013).
- Sauver, Joe St. 2004. *SCADA Security*. Dostopno prek: <http://pages.uoregon.edu/joe/scada/SCADA-security.pdf> (21. september 2013).

- Scarfone, Karen in Paul Hoffman. 2009. *Guidelines on Firewalls and Firewall Policy*. Gaithersburg: National Institute of Standards and Technology. Dostopno prek: <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf> (21. september 2013).
- Security incidents organization. 2009. *Quarterly report on cyber security incidents and trends affecting industrial control systems 3rd quarter 2009*. Dostopno prek: <http://www.securityincidents.net/docs/RISI%20Q1%202009%20Sample%20Analysis%20Report%20Sec.pdf> (21. september 2013).
- Sinclair, Timothy, ur. 1997. *Collins cobuild english dictionary*. London: HarperCollins Publishers.
- Singh, Abhishek. 2005. *Demystifying Denial-Of-Service attacks, part one*. Dostopno prek: <http://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one> (21. september 2013).
- Singh, Ram Kumar. 2009. Intrusion Detection System Using Advanced Honeypots. *International Journal of Computer Science and Information Security* 2 (1):1–9.
- SIQ. 2010. *ISO/IEC 27001:2005 sistemi vodenja varovanja informacij*. Dostopno prek: http://www.siq.si/ocenjevanje_sistemov_vodenja/storitve/sistemi_vodenja_varovanja_informacij/index.html (21. september 2013).
- Skywiper Analysis Team. 2012. *sKyWlper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks*. Budimpešta: Budapest University of Technology and Economics, Department of Telecommunications. Dostopno prek: www.crysys.hu/skywiper/skywiper.pdf (21. septeber 2013).
- Small, Prescott E. 2011. *Defense in Depth: An Impractical Strategy for a Cyber World*. Dostopno prek: <http://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896?show=defense-depth-impractical-strategy-cyber-world-33896&cat=assurance> (21. september 2013).

- Stouffer, Falco in Mell Scarfone. 2011. *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg: National institute of standards and technology.
- Svete, Uroš (2005): *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
- Svete, Uroš in Marjan Malešič. 2014. *Slovenija v ledenih okovih 2014 – odzivi in izzivi*. Ljubljana: Fakulteta za družbene vede.
- Swanson, Marianne in Barbara Guttman. 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Dostopno prek: <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf> (21. september 2013).
- Symantec Corporation. 2013. *Bot-infected Computers*. Dostopno prek: http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=bot_infected_computers (21. september 2013).
- Tanase, Matthew. 2003. *Closing the Floodgates: DDoS Mitigation Techniques*. Dostopno prek: <http://www.symantec.com/connect/articles/closing-floodgates-ddos-mitigation-techniques> (21. september 2013).
- Team Cymru. 2009. *Who is looking for your SCADA infrastructure?* Dostopno prek: <http://www.team-cymru.com/ReadingRoom/Whitepapers/2009/scada.pdf> (21. september 2013).
- The national security archive. 2013. *Update: Agent Farewell and the Siberian Pipeline Explosion*. Dostopno prek: <http://nsarchive.wordpress.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/> (21. september 2013).
- Total defense. 2013. *Global security advisor glossary*. Dostopno prek: <http://www.totaldefense.com/support/security-advisor/glossary.aspx#V>. (21. september 2013).
- U.S. department of energy. 2001. *21 Steps to Improve Cyber Security of SCADA Networks*. Dostopno prek: www.oel.netl.doe.gov/docs/prepare/21stepsbooklet.pdf (21. september 2013).

- United nations development programme. 1994. *Human development report 1994*. New York: Oxford university press. Dostopno na <http://hdr.undp.org/reports/global/1994/en/> (21. september 2013).
- Valeriano, Brandon in Ryan C. Maness. 2015. *The Coming Cyberpeace*. Dostopno prek: <https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace> (10. junij 2015).
- Voglar, Dušan, ur. 2000. *Enciklopedija Slovenije*. Drugi in štirinajsti zvezek. Ljubljana: Mladinska knjiga.
- Wade, Susan M. 2011. *SCADA Honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats*. Magistrsko delo. Ames: Iowa State University.
- Weiss, Gus W. 2007. *The farewell dossier*. Dostopno prek: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a14p.pdf> (21. september 2013).
- Whitman, Michael E. in Herbert J. Mattord. 2012. *Principles of Information Security*. Boston: Course Technology.
- Wiener, Norbert. 1964. *Cybernetics: or control and communication in the animal and the machine*. Cambridge, Mass.: M.I.T. Press
- Zetter, Kim. 2010. Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target. *Wired magazine*, 23. september. Dostopno prek: <http://www.wired.com/threatlevel/2010/09/stuxnet/> (21. september 2013).
- Zetter, Kim. 2012. Report: Obama Ordered Stuxnet to Continue After Bug Caused It to Spread Wildly. *Wired magazine*, 1. junij. Dostopno prek: <http://www.wired.com/threatlevel/2012/06/obama-ordered-stuxnet-continued/all/> (21. september 2013).

Priloge

Priloga A: Vprašalnik

Procesi

1. Ali ima organizacija skladno s priznano metodologijo certificiran:
 - a. Sistem vodenja?(2)
 - b. Sistem varovanja informacij?(2)
 - c. Sistem neprekinjenega delovanja?(2)
2. Ali je glavna poslovna stavba vašega podjetja varovana
 - a. Fizično?(1)
 - b. Tehnično?(1)
3. Ali so vse oddaljene enote v vašem podjetju varovane
 - a. Fizično?(0,5)
 - b. Tehnično?(0,5)
4. Ali v organizaciji obstaja oseba, določena kot vodja oz. menedžer varstva informacij?(1)
5. Ali ima organizacija izdelano splošno politiko varovanja informacij?(1)
6. Ali v organizaciji obstaja in se izvaja politika presojanja dokumentov varovanja informacij?(1)
7. Ali obstaja politika določanja občutljivosti informacij?(1)
8. Ali ima organizacija izdelano splošno varnostno politiko?(1)
9. Ali na ravni organizacije obstaja spisek kritičnih procesov in sredstev?(1)
10. Ali v organizaciji obstaja politika, ki določa, da morajo pogodbeni izvajalci izpolnjevati enake varnostne kriterije, kot zaposleni?(1)
11. Ali v organizaciji obstaja in se izvaja politika testiranja varnostnih načrtov in načrtov neprekinjenega poslovanja?(1)
12. Ali je sistem varovanja informacij zgrajen na podlagi opravljene analize tveganj?(1)
 - a. Ali je bila analiza izvedena po mednarodno uveljavljeni metodi? (0,5)
 - b. Ali je bila ta analiza tako kvalitativna, kot kvantitativna?(0,5)
13. Ali v organizaciji obstaja politika obvladovanja dostopanja do varnostno občutljivih podatkov?(1)

14. Ali v organizaciji obstaja splošen katalog občutljivih (tajnih, kritičnih, varovanih) informacij?(1)
15. Ali je za obvladovanje sistema varovanja informacij ves čas določena vsaj ena dežurna oseba? (1)
16. Ali ima organizacija izdelano politiko čiste mize in zaslona?(1)
17. Ali ima organizacija izdelane administrativne varnostne zahteve, ki vsebujejo označevanje, prenos, hrambo dokumentov ipd?(1)
18. Ali so vsi procesi dokumentirani?(1)
19. Ali ima organizacija izdelan načrt neprekinjenega delovanja?(1)
20. Ali so organizacijski oddelki in osebe, ki funkcionalno pokrivajo področje fizične in informacijske varnosti ter varnosti nadzornih sistemov (SCADA), združeni v enotni službi ali v skupni stalni delovni skupini?(1)
21. Ali so organizacijski oddelki in osebe, ki funkcionalno pokrivajo področje fizične in informacijske varnosti ter varnosti nadzornih sistemov (SCADA), v snovanju varnostnih politik in tehnik, neodvisni od svojih neposredno nadrejenih, če ti niso člani ožjega vodstva ali vodja varnostne službe? (2)

Sistemi

1. Ali obstaja in se izvaja politika glede avtentikacije za dostop do uporabniških računov?(1)
 - a. Ali ta politika določa, da morajo gesla izpolnjevati določene varnostne standarde?(0,5)
 - b. Ali ta politika določa, da se sistemi po krajšem obdobju neuporabe samodejno zaklenejo?(K)
2. Ali v organizaciji obstaja in se izvaja politika obvladovanja uporabniških računov?(1)
3. Ali je za dostop do domene potreben več, kot en avtentikacijski mehanizem?(1)
4. Ali zagotovo v omrežju organizacije ne obstaja računalnik, ki ne izpolnjuje varnostne politike?(1)
5. Ali med medmrežjem in notranjim omrežjem organizacije obstaja DMZ?(1)
6. Ali obstaja sistem za sledenje podatkovnega prometa med domeno in območjem izven domene?(1)
7. Ali je ob avtentikaciji uporabnik vedno enoznačno identificiran? (K)

8. Ali obstaja seznam uporabnikov, ki lahko uporabljajo oddaljen dostop do domene?(1)
9. Ali v organizaciji obstaja politika obvladovanja dnevnikov varnostno pomembnih dogodkov?(1)
 - a. Ali so ti dnevniki ustrezno zavarovani?(0,5)
 - b. Ali je dovoljen vpogled samo pooblaščenim osebam?(0,5)
 - c. Ali varnostni dnevniki vsebujejo naslednje podatke: tip, čas, kraj, vir, izid, identiteta izvajalca? (K)
10. Ali je uporabnikom onemogočeno zaganjanje datotek, ki niso skladne z varnostno politiko (npr preko e-mailov, usb ključkov)?(1)
11. Ali menite, da je nemogoče zlorabljeni računalniško opremo (uporaba za nelegalne namene), ne da bi bilo to ugotovljeno?(1)
12. Ali so za oddaljen dostop opredeljene varnostne zahteve sistema, iz katerega se ta dostop izvaja in ali se te zahteve preverjajo ob dostopu? (K)
13. Ali je mogoče do domene dostopati samo preko zasebnega omrežja, tj lastnih vodov ali VPN?(1)
14. Ali obstaja varnostna politika za oziroma so v varnostno politiko zajete tudi prenosne naprave (mobilni telefoni, tablični računalniki, dlančniki)?(1)
15. Ali obstaja politika, ki določa, do kakšnih spletnih strani imajo zaposleni dostop?(1)
16. Ali se varnostno občutljivi podatki ob pošiljanju izven podjetja ustrezno šifrirajo?(1)
17. Ali ima organizacija izdelano politiko sprejemljive rabe sistemov in povezav?(1)
18. Ali ima organizacija izdelano politiko nadzora dostopa do sistemov?(1)
19. Ali ima organizacija izdelano IKT strategijo?(1)
20. Ali ima organizacija izdelano politiko obvladovanja programske opreme?(1)
21. Ali ima organizacija izdelane standarde vzdrževanja in obvladovanja sprememb v sistemih?(1)
22. Ali ima organizacija izdelano arhitekturo omrežja s pojasnili?(1)
23. Ali ima organizacija izdelano politiko varnostnega kopiranja podatkov?(1)
24. Ali ima organizacija izdelano politiko arhiviranja podatkov, ki vsebuje klasifikacijo in roke hranjenja določenih vrst podatkov?(1)
25. Ali ima organizacija izdelano politiko sledenja spremembam podatkov?(1)

26. Ali ima organizacija izdelano politiko odzivanja na varnostne incidente?(1)
27. Ali je kdorkoli v organizaciji izrecno obveščen, ko se uporabniku sistemsko dvigne nivo uporabniških pravic? (K)
28. Ali je v celotnem omrežju nameščena protivirusna programska oprema?(1)
 - a. Ali ta programska oprema nadzoruje tudi prenosne naprave?(1)
 - b. Ali ta oprema preveri vse datoteke, vključno z elektronsko pošto s priponkami, ki vstopijo v omrežje organizacije?(0,5)
29. Ali v organizaciji obstajajo sistemi za zaznavanje vdora v omrežje?(1)
30. Ali so vse sistemske ure sinhronizirane? (K)
31. Ali ste že izvedli testiranje varnostne zanesljivosti omrežja s simulacij napada, preko interne "rdeče ekipe" ali preko najetega izvajalca?(2)

Sistemi-SCADA

1. Ali so delovne postaje, ki nadzorujejo sistem SCADA niso del domene?(1)
2. Ali je omrežje ICS oz. SCADA izolirano od omrežja družbe?(1)
3. Ali ste že izvedli penetracijski test za sistem SCADA? (1)
 - a. V zadnjih treh letih? (0,5)
4. Ima sistem SCADA lasten požarni zid?(1)
 - a. Če ne, ali je požarni zid podjetja postavljen tako, da je posebej prilagojen za sistem SCADA?(0,5)
5. Ali med omrežjem družbe in omrežjem SCADA obstaja DMZ?(1)
6. Ali je za nadzorni sistem SCADA zagotovljen rezervni sistem?(1)
7. Ali je izdelana varnostna politika specifično za sistem SCADA?(2)
 - a. Ali je ta politika skladna z varnostno politiko podjetja oz. ali jo izključno nadgrajuje? (0,5)
 - b. Ali temelji na oceni tveganj, izdelani na podlagi uveljavljene metodologije? (0,5)
 - c. Ali politika opredeli obseg in potrebe po varovanju informacij? (0,5)
 - d. Ali politika opredeli varnostne potrebe sistema? (0,5)
 - e. Ali politika postavi varnostno arhitekturo sistema in jo implementira? (0,5)
 - f. Ali se je izvedla presoja politike v zadnjih treh letih?(0,5)
8. Ali so kateri izmed delov sistema SCADA med seboj povezani z brezžičnimi povezavami (/)

- a. Če da, ali gre za povezave, ki so zavarovane bolje kot klasične WI-FI povezave? (1)
9. Ali obstaja načrt neprekinjenega delovanja za SCADO? (2)
- a. Ali je bil revidiran in ugotovljeno skladen s certificiranim sistemom menedžmenta? (0,5)
 - b. Ali se redno pregleduje in posodablja? (0,5)
 - c. Ali načrt zajema vse točke sistema? (0,5)
 - d. Ali ste z uporabniki že izvedli vajo, ki bi preverila delovanje načrta in ali je načrt deloval? (1)
10. Ali ima omrežje SCADA vgrajene mehanizme za zaznavanje vdora na ravni posameznih točk? (1)
11. Ali so arhitektura sistema in posamezne točke v njem v celoti dokumentirani? (1)
12. Ali imate izdelan varnostni načrt, ki vsebuje načrt odziva in lajšanja posledic napada na sistem SCADA? (1)
13. Ali ste kdaj izvedli oceno tveganj za omrežje SCADA, ki temelji na uveljavljeni metodologiji (npr. OICM)? (1)
14. Ali je na vseh SCADA nadzornih centrih zagotovljeno fizično in tehnično varovanje? (1)
15. Ali se ni mogoče povezati na sistem SCADA iz oddaljenega sistema brez avtentikacije? (1)
16. Ali je onemogočeno, da bi uporabniki sisteme, ki so povezani v sistem SCADA uporabljali za zasebne namene (npr. brskanje po spletu, e-maili ipd)? (1)
17. Ali imajo vsi sistemi, povezani v sistem SCADA nameščeno protivirusno programsko opremo? (1)
- a. Če določeni sistemi te opreme nimajo, pa bi njena namestitev oslabila delovanje sistema SCADA, ali so ti sistemi ustrezno izolirani in drugače zavarovani? (/0,5)
 - b. Ali je vsaka datoteka, ki pride v omrežje sistema SCADA varnostno pregledana? (0,5)
18. Ali so občutljive informacije, ki izvirajo iz sistema SCADA ob prenosu na druge sisteme ustrezno šifrirane in zavarovane? (1)
19. Ali so vse povezave v omrežje sistema SCADA identificirane? (1)

20. Ali so vse nepotrebne povezave v omrežje sistema SCADA onemogočene? (1)
21. Ali so vse nepotrebne storitve v omrežju onemogočene? (1)
22. Ali so vse varnostne funkcije, ki so privzeto vgrajene v sistem implementirane? (1)
23. Ali ste že izvedli varnostno oceno sistema SCADA skladno z uveljavljenimi smernicami oziroma standardi? (2)
 - a. V zadnjih treh letih? (0,5)
24. Ali komunikacija med točkami v sistemu SCADA poteka preko komunikacijskih vodov, ki so namenjeni izključno temu? (1)
25. Ali se varnostno zanimivi pojavi beležijo in shranjujejo? (1)
26. Ali je za nadzorne sisteme v SCADI za avtentikacijo potrebna več, kot ena vrsta avtentikacijskega mehanizma? (1)

Ljudje

1. Ali bi rekli, da zaposleni v oddelkih, ki se ukvarjajo z informacijsko varnostjo, niso preobremenjeni? (1)
2. Ali ima organizacija izdelan kodeks ravnanja oz. etični kodeks uslužbencev? (1)
3. Ali ima organizacija izdelano Organizacijsko shemo s popisom delovnih mest, njihovih nalog in zadolžitev? (1)
4. Ali obstaja in se izvaja politika rednega preverjanja zadovoljstva zaposlenih? (1)
5. Ali telefonski imenik zaposlenih ni javno objavljen? (1)
6. Ali je vsak nov zaposleni seznanjen z vsemi varnostnimi politikami podjetja, ustreznimi za njegovo delovno mesto? (1)
7. Ali je vzpostavljen proces sledenja vsem identifikacijskim karticam, ključem, prenosnikom, službenim telefonom, sredstvom za oddaljen dostop ipd? (1)
8. Ali je vzpostavljen učinkovit proces odvzemanja takšnih sredstev posameznikom, s katerimi je delovno razmerje prekinjeno? (1)
9. Ali je vzpostavljen učinkovit proces odvzemanja takšnih nepotrebnih sredstev posameznikom, ki so premeščeni na drugo delovno mesto? (1)

10. Ali je vzpostavljen učinkovit proces odvzemanja takšnih sredstev in onemogočanja računov posameznikom preden organizacija nespornostno prekine delovno razmerje? (1)
11. Ali obstaja politika komuniciranja z zunanjimi osebami? (1)
12. Ali ste v zadnjih treh letih izvedli varnostno usposabljanje za določene zaposlene? (1)
- a. Ali je to usposabljanje vsebovalo usposabljanje za zaznavanje in preprečevanje napadov socialnega inženiringa? (1)
13. Ali ste v zadnjih treh letih izvedli varnostno usposabljanje za vse zaposlene? (1)
- a. Ali je to usposabljanje vsebovalo usposabljanje za zaznavanje in preprečevanje napadov socialnega inženiringa? (1)
14. Ste že izvedli test napada s socialnim inženiringom? (1)
15. Ali ste v organizaciji izvedli kakšne ukrepe, ki se nanašajo specifično na preprečevanje napadov s socialnim inženiringom? (1)
16. Ali se je že zgodilo, da je kdo od zaposlenih, ki se ne ukvarja specifično z varovanjem informacij, ustrezni osebi poročal o slabostih pri varovanju? (0,5)
17. Ali bi rekli, da so varnostne politike dovolj poznane in razumljive, da zaposleni natančno razumejo, kakšne informacije lahko predajajo in kakšne ne? (1)
18. Ali bi rekli, da so vloge in odgovornosti delavcev jasno definirane? (1)
19. Ali redno preverjate delovanje varnostnih politik, ki se ukvarjajo z izdajanjem informacij osebja? (1)
20. Ali vodstvo organizacije v celoti spoštuje njene varnostne politike? (1)
21. Ali so za kršenje varnostnih politik definirane kazni? (1)
22. Ali ste že obravnavali primer, v katerem ste ugotovili kršenje varnostne politike? (/)
- a. Ali je oseba, ki je kršila varnostno politiko bila kaznovana(K)?
23. Ali zaposleni razumejo, da bodo v primeru kršenja varnostnih politik verjetno sankcionirani? (1)
24. Ali imate vzpostavljen učinkovit sistem obveščanja zaposlenih o spremembah varnostnih politik? (1)

Priloga B: Primer opredeljenega varnostnega območja po ANSI/ISA-99 (Byres 2010).

ZONE S₁

Zone Name: Unit 1 Hydrocracker Safety System

Definition of this Zone: This zone includes all safety integrity systems for the Unit 1 Hydrocracker.

Controlling Agency: Process Automation Department, SIS Team.

Zone Function: The systems in this zone provide safety functions to the Unit 1 Hydrocracker.

Zone Boundaries: The Safety Integrated System as defined by the Unit 1 Hydrocracker HAZOP.

Typical Assets: The Safety Integrated System controller, engineering station and communications hardware

Inheritance: This zone inherits attributes from Zone C₁ (Unit 1 Hydrocracker Basic Control System)

Zone Risk Assessment: This is a low to moderately secure zone with extreme consequences if breached.

- a) **Security Capabilities of Zone Assets:** All assets are assumed to be incapable of withstanding low level attacks (i.e. those launched by unsophisticated attackers or malware) on their availability or confidentiality. This is a result of the protocols in use and system design. Assets are assumed to be capable of withstanding medium level attacks (i.e. those launched by moderately sophisticated attackers or malware) on their integrity.
- b) **Threats and Vulnerabilities:** The vulnerabilities of this zone are assumed to be typical of legacy industrial control devices using MODBUS for communications. The principal threats are:
 - a. Network-based Denial of Service to SIS communications.
 - b. Internal or External unauthorized access to the SIS engineering station.
 - c. Spoofing of MODBUS/TCP control commands.
 - d. Spoofing of MODBUS/TCP responses to the process system.
 - e. Reprogramming of safety functions.
- c) **Consequences of a Security Breach:**
 - a. Loss of production >6 hrs from false trip of emergency shutdown system.
 - b. Loss of production <6 hrs due to loss of visibility to safety system.
 - c. Disabling/manipulation of emergency shutdown resulting in fatality or major community incident.
- d) **Business Criticality:** Extreme

Security Objective: To protect the integrity and availability of the Unit 1 Hydrocracker Safety System.

Acceptable Use Policy: I/O and Fieldbus communications is allowed to Zone P₁ (Unit 1 Hydrocracker Process). Read access to published data is allowed to approved systems in the Zone C₁ (Unit 1 Hydrocracker Basic Control System). All Write access to this zone is forbidden. All system management and programming functions shall be internal to this zone.

Inter-zone Connections: Conduits to this zone may be established from Zone C₁ (Unit 1 Hydrocracker Basic Control System) and from Zone P₁ (Unit 1 Hydrocracker Process).

Security Strategy: All connections to this zone must be controlled using type S conduits. Access to these systems must be approved by the Controlling Agency.

Change Management Process: All changes to this zone or any of its connecting conduits must follow the approved change management process of its corresponding Controlling Agency (see above). This includes, but is not limited to, the installation or replacement of equipment, modification of security policy, and exceptions to security policy or existing practices.

Priloga C: Ocenjevalni list za tveganje informacijskega sredstva orodja OCTAVE (Caralli in drugi 2007: 127).

Allegro Worksheet 10		INFORMATION ASSET RISK WORKSHEET				
Information Asset Risk	Threat	Information Asset	PBCD			
		Area of Concern	Denial-of-service attack against hospital network impedes the hospital's ability to electronically deliver bills to the insurance organizations. (PBCD must traverse Internet to reach insurance organizations.)			
		(1) Actor <i>Who would exploit the weakness?</i>	A hacker who wants to see if he can damage the hospital financially			
		(2) Means <i>How would the actor do it? What would they do?</i>	Uses DoS toolkit found on hacking website			
		(3) Motive <i>What is the actor's reason for doing it?</i>	Entertainment			
		(4) Outcome <i>What would be the resulting effect on the information asset?</i>	☐ Disclosure ☐ Modification		☐ Destruction ☒ Interruption	
		(5) Security Requirements <i>How would the information asset's security requirements be breached?</i>	The PBCD must be available for billing and collection activities.			
		(6) Probability <i>What is the likelihood that this threat scenario could occur?</i>	☐ High	☐ Medium	☐ Low	
	(7) Consequences <i>What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?</i>		(8) Severity <i>How severe are these consequences to the organization or asset owner by impact area?</i>			
	Continual attacks against hospital network add significant delays in the reimbursement process. Hospital must burn CDROMs with the data and messenger them to insurance services. Significant financial and productivity impacts.		Impact Area	Value	Score	
			Reputation & Customer Confidence	Med	4	
			Financial	High	12	
Productivity			High	9		
Safety & Health			Low	5		
Fines & Legal Penalties			Low	1		
		User Defined Impact Area				
Relative Risk Score					31	

Priloga Č: Primer lista s kalkulacijo indeksa RAV za informacijski sistem (ISECOM 2010: 69).

OPSEC

Visibility	1
Access	3
Trust	0
Total (Porosity)	4

CONTROLS

Class A		Missing
Authentication	7	0
Indemnification	0	4
Resilience	0	4
Subjugation	0	4
Continuity	0	4
Total Class A	7	16

Class B		Missing
Non-Repudiation	0	4
Confidentiality	0	4
Privacy	1	3
Integrity	0	4
Alarm	9	0
Total Class B	10	15

		True Missing
All Controls Total	17	31
Whole Coverage	42.50%	77.50%

LIMITATIONS

		Item Value	Total Value
Vulnerabilities	4	8.750000	35.000000
Weaknesses	5	5.000000	25.000000
Concerns	8	4.750000	38.000000
Exposures	0	5.025000	0.000000
Anomalies	0	4.250000	0.000000
Total # Limitations	17		98.0000

**OPSEC**

6.776361

True Controls

3.837843

Full Controls

4.986272

True Coverage A

20.00%

True Coverage B

25.00%

Total True Coverage

22.50%

**Limitations**

15.930239

Security Δ

-17.72

True Protection

81.13

Actual Security: 82.23

The raw calculation sheet for determining the balance between porosity, controls, and limitations.