Univerza v Mariboru

Fakulteta za varnostne vede

Sodobni aspekti informacijske varnosti

Urednika: Igor Bernik, Blaž Markelj

SODOBNI ASPEKTI INFORMACIJSKE VARNOSTI

Univerza v Mariboru

Fakulteta za varnostne vede

serija: Informacijska varnost

Sodobni aspekti informacijske varnosti

Urednika:
dr. Igor Bernik
Blaž Markelj

Avtorica stvarnega kazala:
dr. Sabina Zgaga

Lektorica:
Karin Pečnikar

Izdajatelj:
Fakulteta za varnostne vede, Univerza v Mariboru, Ljubljana

www.fvv.uni-mb.si

E-knjiga narejena:
marca 2013

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

659.2:004:351.78

SODOBNI aspekti informacijske varnosti [Elektronski vir] / avtorji Igor Bernik ... [et al.] ; urednika Igor Bernik, Blaž Markelj. - El. knjiga. - Ljubljana : Fakulteta za varnostne vede, 2013. - (Serija Informacijska varnost)

ISBN 978-961-6821-32-2 (ePub)
ISBN 978-961-6821-33-9 (mobi)
ISBN 978-961-6821-34-6 (pdf)

1. Bernik, Igor

265112320

Avtorske pravice

Vsebina

Varovanje občutljivih podatkov v informacijskih sistemih 5

Blaž Ivanc

Uvod 5
Koncepti večnivojske varnosti 6
Človeški viri – ključni element pri varovanju podatkov 9
Zaključek 11
Viri 12
O avtorju 13

Zagotavljanje učinkovitosti informacijske varnosti z merjenjem 14

Kaja Prislan

Uvod 14
Merjenje informacijske varnosti 15
Pogoji za učinkovitost 18
Ravni merjenja 20
Ključni indikatorji 21
Načini merjenja 22
Analiza in predstavitev podatkov 23
Sklep 25
Viri 26
O avtorju 27

Projekt vpeljave sistema za upravljanje informacijske varnosti v organizacijo 28

Klemen Vehar, Alenka Brezavšček, Tomaž Kern

Uvod ... 28
Sistem za upravljanje informacijske varnosti – SUIV ... 30
Model načrtovanja SUIV po standardu ISO/IEC 27003 ... 31
Pridobitev soglasja vodstva za začetek projekta vpeljave SUIV ... 32
Definiranje obsega in meja SUIV ter politike SUIV ... 33
Analiza zahtev v zvezi z informacijsko varnostjo ... 34
Ocena tveganja in oblikovanje predloga varovalnih ukrepov ... 35
Oblikovanje končnega načrta vpeljave SUIV ... 35
Izdelava projektnega načrta za vpeljavo SUIV ... 36
Zaključek ... 39
Viri ... 40
O avtorjih ... 41

Revidiranje sistemov upravljanja varovanja informacij 42

Mladen Terčelj, Boštjan Delak

Uvod ... 42
Kratek pregled standardov ... 43
ISO/IEC 27007:2011 ... 44
Namen standarda ... 44
Cilji standarda ... 45
Opis postopka revizije ... 45
Priprava programa revizije ... 45
Izvedba revizije ... 46
ISO/IEC 27006:2007 ... 47
Sinergija med ISO/IEC 27007:2011 in ISO/IEC 27006:2007 ... 47
COBIT ... 48
COBIT 5 ... 48
COBIT 5 – Varovanje informacij ... 50
Primer iz prakse ... 51
Razprava ... 52
Zaključek ... 53
Viri ... 54
O avtorjih ... 54

Strategija kibernetske varnosti in kibernetske obrambe v okviru slovenske strateške kulture 55

Adriana Dvoršak

Uvod ... 56
Dejavniki Slovenske strateške kulture ... 56
Oblikovanje države ... 58
Kolektivna identiteta ... 58
Pretvorba vrednot v nacionalne politike ... 58
Civilna družba ... 59
Odnos do mednarodnih norm ... 59
Odzivna strategija kibernetske varnosti in kibernetske obrambe ... 59
Razvoj mednarodnih norm in potrebe Slovenije ... 63
Zaključek ... 67
Viri ... 69
O avtorici ... 70

Kibernetska mimikrija kot kaznivo dejanje 71

Zoran Cunk

Uvod ... 71
Kibernetska mimikrija – sestavina igre, posla ali kaznivega dejanja ... 73
Posredna kibermimikrija in njene pojavne oblike ... 77
Neposredna kibermimikrija in njene pojavne oblike ... 80
Zaključek ... 82
Viri ... 82
O avtorju ... 84

Enkripcija digitalnih podatkov – sodobni problem digitalnega dokazovanja 85

Miha Šepec

Uvod ... 85
Enkripcija digitalnih podatkov ... 86
O TrueCrypt zaščiti na splošno ... 88
Kazenskopravni preiskovalni vidik ... 88
Zaključek ... 92
Viri ... 93
O avtorju ... 94

Možnosti izgube podatkov in kazenskopravne posledice 95

Blaž Markelj, Sabina Zgaga

Uvod ... 96
Računalništvo v oblaku in mobilne naprave ... 97
Raziskava ... 98
Kazenskopravne dileme nepazljive uporabe mobilnih naprav, ki povzroči izgubo zaščitenih podatkov ... 99
Relevantna kazniva dejanja ... 99
Izvršitveno ravnanje ... 105
Zaključek ... 106
Viri ... 108
O avtorjih ... 109

Varovalni mehanizmi e-banke z vidika uporabnosti, funkcionalnosti in enostavnosti 110

Lucija Tomšič Zupan, Bernik Igor

Uvod ... 110
Metode ... 111
Pregled varovalnih mehanizmov in njihova uporabnost ... 111
Varovalni mehanizmi in njihova odpornost na grožnje ... 112
Uporabnost, funkcionalnost in enostavnost uporabe varovalnih mehanizmov ... 113
Dosedanje raziskave na temo uporabnosti varovalnih mehanizmov e-banke ... 114
Možni pristopi k doseganju uporabne varnosti e-banke ... 117
Zaključek ... 118
Viri ... 119
O avtorjih ... 120

Trendi uporabe mobilnih naprav 121

Blaž Markelj, Igor Bernik

Uvod ... 121
Mobilne naprave in potencialne grožnje ... 123
Ravnanje mladih z mobilnimi napravami ... 124
Zaključek ... 128
Viri ... 129
O avtorjih ... 129

Zaščita industrijskih kontrolnih sistemov – obramba v globino 130

Blanka Strmšek

Uvod ... 130
Ranljivosti industrijskih kontrolnih sistemov ... 131
Definiranje obrambe v globino ... 134
Ljudje ... 134
Postopki ... 135
Tehnologija ... 136
Segmentacija omrežja, varnostna območja in kanali ... 136
Omrežna arhitektura IKS ... 137
Življenjski cikel obrambe v globino ... 138
Zaključek ... 140
Viri ... 141
O avtorju ... 142

Stvarno kazalo 143

Sabina Zgaga

Varovanje občutljivih podatkov v informacijskih sistemih

Blaž Ivanc

Pri obdelavi občutljivih podatkov se pogostokrat srečujemo z agentom grožnje, ki mu pravimo notranji sovražnik. Njegova aktivnost je vidna v obliki zlorab informacijskih sistemov in nespoštovanja pravil. Nevarnost predstavlja tudi delovanje zlonamerne programske kode, ki posledično izkorišča končnega uporabnika. Članek prikaže koncepte večnivojske varnosti in potrebo po kompetentnih človeških virih, ki so ključni element pri varovanju podatkov. Večnivojski varnostni sistemi so se začeli razvijati v obrambnih ustanovah, nekateri prilagojeni sistemi pa so rezultat aplikacijske osredotočenosti na delovne procese v obveščevalnih službah. Področje je predmet raziskav in razvoja že desetletja, nastale koncepte in spoznanja pa so informacijsko naprednejše države uporabljale že v devetdesetih letih prejšnjega stoletja za varovanje informacijske zasebnosti državljanov. Skupinsko delo in razpoložljivost strokovnjakov sta ključnega pomena v procesu vzpostavljanja in zagotavljanja informacijske varnosti. Poznavanje »učečega se nasprotnika« in njegovih zmožnosti za zlonamerna dejanja je ključno pri zavarovanju podatkov, zato so v članku predlagane tudi točke za izboljšanje zavarovanja podatkov v informacijskih sistemih.

KLJUČNE BESEDE: beleženje, informacijski sistemi, nivo dovoljenja, potreba po védenju, stopnja tajnosti, varovanje podatkov, večnivojski varnostni sistem

1 Uvod

Številne informacijske nesreče, ki v manjšem obsegu pridejo do medijev, za večino pa širša javnost ne izve, nakazujejo resnično stanje na področju informacijske varnosti. Za nedelovanje z informacijsko varnostjo povezanih dejavnikov lahko brez zadržkov okrivimo pomanjkanje izvornih znanj in nerazumevanje področja. Informacijska varnost je obsežno področje, ki zahteva timski pristop in z njim

širok nabor strokovnjakov različnih strok. Področje preseneti z eksponentno rastjo znanja, ki izjemno hitro zastari, kar je posledica interdisciplinarnega pristopa in velike težnje po odkrivanju novega.

Pri obdelavi občutljivih podatkov se velikokrat srečujemo z agentom grožnje, ki mu pravimo notranji sovražnik. Njegova aktivnost je vidna v obliki zlorab informacijskih sistemov in nespoštovanja pravil. Slednje je ranljivost, ki jo pogosto izkorišča socialni inženiring. V kontekstu tega članka lahko kot notranjega sovražnika upoštevamo tudi delovanje zlonamerne programske kode, ki posledično izkorišča končnega uporabnika.

V javnosti velikokrat zasledimo poudarjanje moči in kompleksnosti varnostnih mehanizmov, s čimer želijo upravljavci prikazati visoko tehnološko in upravljalno -ravnalno sposobnost varovanja podatkov. Žal nas vedno znova presenetijo nikoli prej javno predstavljene tehnike napadov, zlorabe mehanizmov zaupanja in odzivi, ki nastanejo zaradi razkritja informacij, ki so posledica kršenja osnov razvoja varnostnih mehanizmov. Wang, Wu, Wang in Le (2009) so izpostavili, da konvencionalni varnostni ukrepi niso osredotočeni na tveganja, povezana z varovanjem občutljivih informacij. Med ranljivosti, ki so pogosto spregledane, se uvrščajo kompromitacija dolgoročnih kriptografskih ključev in odsotnost premišljene kontrole dostopa pri skupinskem deljenju.

Področje večnivojske varnosti je predmet raziskav in razvoja že desetletja, nastale koncepte in spoznanja pa so informacijsko naprednejše države uporabljale že v devetdesetih letih prejšnjega stoletja za varovanje informacijske zasebnosti državljanov. Namen članka je prikazati koncepte večnivojske varnosti in potrebo po kompetentnih človeških virih, ki so ključni element pri varovanju podatkov. V članku so predlagane tudi spremembe za zagotovitev boljšega zavarovanja podatkov v informacijskih sistemih. Članek v drugem poglavju na kratko predstavi modele večnivojske varnosti in kratek pregled razvojnega dela, ki temelji na v poglavju predstavljenih modelih. Tretje poglavje predstavi potrebo po znanju, ki predstavlja temelj informacijske varnosti. Četrto poglavje je zaključek.

2 Koncepti večnivojske varnosti

Večnivojski varnostni sistemi so večini znani po hierarhiji varnostnih nivojev: interno, zaupno, tajno, strogo tajno. Pri tem je bistvena ločitev med nivojem dovoljenja in stopnjo tajnosti. Nivo dovoljenja sporoča najvišjo stopnjo tajnosti,

s katero ravna oseba, naprava ali se hrani in pregleduje v ustrezno zavarovanem območju. Nivo dovoljenja, ki se nanaša na osebo, odraža zaupanje, dodeljeno osebi, ki pridobi varnostno dovoljenje. Stopnja tajnosti se nanaša na občutljivost informacij v dokumentu in načeloma odraža potencialno škodo interesom države v primeru razkritja. Poleg hierarhičnih varnostnih nivojev, večnivojski sistemi pogosto uporabljajo še oznake skupin občutljivih informacijskih postavk. S tem je vzpostavljena dodatna omejitev. Ta koncept se lahko predstavi ločeno pod imenom večstranska varnost. Pogosto pa ta koncept srečamo združen z večnivojsko varnostjo. Tako je omogočeno izvajanje načela, ki mu pravimo »potreba po védenju« in ki onemogoča, da tudi oseba z najvišjo pravico dostopanja samovoljno pregleduje poljubne zapise v sistemu.

Večnivojski varnostni sistemi so se začeli razvijati v obrambnih ustanovah, nekateri prilagojeni sistemi pa so rezultat aplikacijske osredotočenosti na delovni proces v obveščevalnih službah. Koncepte večnivojske varnosti srečamo v različnih aplikacijah, kot so: komunikacijski protokoli, računalniška omrežja, sistemi upravljanja s podatkovnimi bazami in objektno orientirani sistemi.

Večnivojski varnostni sistemi morajo omogočati večuporabniško izvajanje in biti varni pred zlonamerno programsko kodo. Pri načinu izvajanja ločimo: namenski način, način najvišje varnosti sistema in način z večnivojsko varnostjo. V namenskem načinu se ne uporablja računalniških mehanizmov kontrole dostopa, temveč se neavtoriziran dostop do podatkov preprečuje z mehanizmi navzočimi v prostorih. Način najvišje varnosti sistema zahteva mehanizem dostopa do datotek, značilen za večuporabniške sisteme. Način z večnivojsko varnostjo zahteva uporabo kontrole dostopa, ki ustreza določilom večnivojske varnosti (Smith, 2006).

Zaupnost in integriteta sta glavni lastnosti, ki ju želimo zagotoviti v varnih računalniških sistemih. Zanje je značilna obvezna kontrola dostopa. Slednje pomeni, da sistem uveljavlja varnostno politiko neodvisno od uporabnikovih dejanj. Bell-LaPadula je bil prvi formalni večnivojski varnostni model, predstavljen leta 1973. To je dosledno oblikovan model, usmerjen na komponento zaupnosti. Model prek preproste varnostne karakteristike preprečuje branje objekta, označenega z višjim varnostnim nivojem, kot ga ima subjekt. Model prek dodatne karakteristike tudi preprečuje pisanje na nižjem varnostnem nivoji. Pri modelu je bila leta 1994 formalno dokazana možnost kompromitacije z uporabo zlonamerne programske kode in implementacijo prikritega kanala. Zhihong, Jianwei, Bailing in Feng (2011) menijo, da je šibkost modela njegova prevelika doslednost, ki se kaže

kot neprilagodljivost. Z vidika varovanja integritete podatkov predstavlja osnovo model Biba, predstavljen leta 1977. Model je praktično pretvorba standardnega modela zaupnosti Bell-LaPadula v model integritete. Med znane predstavnike modelov integritete spada tudi Clark-Wilsonov model. Model, ki združuje zahteve po zaupnosti in integriteti, predstavlja Lipnerjev model, ki je kombinacija modelov Bell-LaPadula in Biba. Združevanje zaupnosti in integritete srečamo tudi pri večstranskih modelih, kakršen je model kitajskega zidu. V tem modelu subjekti nimajo neposredno dodeljenih varnostnih dovoljenj (Stamp in Hushyar, 2006). Z večnivojsko varnostjo je povezanih še veliko drugih modelov. Omenjeni so zgolj osnovni modeli, ki so temelj za številne razširitve konceptov večnivojske varnosti.

Habib, Jaume in Morisset (2008) so predstavili možnost za primerjavo modelov za kontrolo dostopanja. Ker so modeli dokaj zapleteni, njihovo ogrodje pravzaprav predstavlja orodje za preučevanje modelov z vidika uvedbe in primerjave modelov. V študiji ugotavljajo, da so številne predstavitve politik kontrole dostopa v literaturi preveč površne. Izpostavijo manjkajoče formalne predstavitve. To je pogost razlog za kasnejši neuspeh pri delu na metodoloških smernicah in njihovih izvedbah.

Znani so nekateri poskusi vključevanja tveganja v sisteme kontrole dostopanja. Shaikh, Adi, Logrippo in Mankovski (2011) so kritizirali splošno znane modele za kontrolo dostopanja, saj ti ne upoštevajo negotovosti in tveganja pri določitvah dostopa. Zato kot nov prispevek, predstavijo dinamično izračunavanje vrednosti zaupanja in tveganja na posameznem paru subjekt/objekt. Ocena preteklega obnašanja temelji na zgodovini zbranih točk iz kazni in nagrad. Končne vrednosti tveganja in zaupanja so poleg omenjenega izračunane še iz varnostnega nivoja dostopa subjekta in nivoja občutljivosti objekta.

Gao, Xiao, Xu in Gao (2012) so v svoji predstavitvi prikazali razširjen model Bell-LaPadula na ravni varnega informacijskega sistema za deljenje informacij. Da kontrola dostopa predstavljenega sistema ustreza večnivojski varnosti, predstavijo nekatere nove interpretacije konceptov vgrajene v model Bell-LaPadula. Predstavljen informacijski sistem sestoji iz varnega računalniškega okolja, varnostno -upravljalnega središča, meje varovanega območja in varnega komunikacijskega omrežja. Varni informacijski sistemi morajo izpolnjevati številne zahteve, med drugim zahtevajo zanesljivo identifikacijo in avtentikacijo uporabnika ter varen prenos podatkov po omrežju, kar se doseže z uporabo šifrirne tehnologije. Wu, Le in Srinivasan (2008) so predlagali varen sistem za občutljive informacije, temelječ na enkratnih dinamičnih ključih, s čimer se izboljšata varnost komunikacije in avtentikacije. Sistem sestoji iz: enote za upravljanje izdajanja dinamičnih ključev,

enote za upravljanje občutljivih informacij in enote za upravljanje avtentikacije ter avtorizacije. Teoretično sistem omogoča varovanje, kljub kompromitaciji in ponuja zaznavanje ter preprečevanje prevar.

Pravilna zasnova in izvedba sistemov se zagotovita s testiranjem varnostno-kritičnih komponent. Temelj pri varnih informacijskih sistemih so: zaupanja vredna računalniška osnova, kontrola dostopa, identifikacija in avtentikacija, varnostna presoja in ocena. Varni informacijski sistemi zagotavljajo, da imajo samo pravilno avtorizirane osebe ali procesi, ki delujejo v njihovem imenu, pravico branja, pisanja, kreiranja in brisanja dokumentov (Zhihong, Bailing, Ye in Zhang, 2011).

3 Človeški viri – ključni element pri varovanju podatkov

Skupinsko delo in razpoložljivost strokovnjakov sta ključnega pomena v procesu vzpostavljanja in zagotavljanja informacijske varnosti. Ta se začne z ocenjevanjem tveganj in izvajanjem sprememb že v fazi zasnove sistema. Buckshaw, Parnell, Unkenholz, Parks, Wallner in Saydjari (2005) so izrazili potrebo po timskem pristopu za zagotavljanje potrebnih podatkov, ki so ključni za uspeh procesa ocene tveganj.Skupino, ki pri tem sodeluje, sestavljajo naslednji kadri:

- Strokovnjaki z znanjem na področju vsiljivcev, njihove motivacije in zmožnosti.
- Strokovnjaki z znanjem in izkušnjami s področja ranljivosti sistemov in metod izkoriščanja ranljivosti.
- Strokovnjaki, ki poznajo namensko uporabo sistema in prepoznajo, kako bodo napadi in protiukrepi delovali na poslanstvo sistema.
- Sistemski inženirji z znanjem zasnove sistemov in razumevanjem delovanja protiukrepov.
- Analitiki s področja varnostnih tveganj.

Da lahko govorimo o uporabni tehnologiji, mora ta imeti več lastnosti, kot so uporabnost, učinkovitost, robustnost in vsesplošna navzočnost (Goldberg, 2008). Kljub temu pa je tehnologija konstantno izpostavljena različnim napadom. Če želimo zagotavljati varnost, moramo tako ob zasnovi, kot tudi tekom celotnega življenjskega cikla sistema poznati ofenzivne informacijske tehnike, taktike in procedure. Temu se najbolj približamo z rednim spremljanjem znanstveno-

raziskovalnih študij in s skupinskim pristopom, ki edini omogoča sodelovanje oseb s potrebnim, a med seboj zelo različnim, naborom izvornih znanj.

Klasični večnivojski varnostni modeli niso najbolj primerni za uporabo v dinamičnih okoljih. Razlog je v statični varnostni politiki. Delovanje modelov je popolnoma skladno z varnostno politiko, ki je rezultat predhodno opravljenih analiz. Prav tako ni možnosti izklopa skladnosti z varnostno politiko ali njene prilagoditve vsakokratnim operativnim potrebam (Shaikh et al., 2011). Kljub temu so v razvitejših državah s področja informacijskih tehnologij poznane številne praktične uporabe konceptov, povezanih z večnivojsko varnostjo. Napredno varovanje osebnih podatkov v informacijskih sistemih so že v devetdesetih letih prejšnjega stoletja prikazale Nemčija, Nova Zelandija in Švica, katerih prakse so postale vzorčni primeri za druge države. Tako načelo »potrebe po védenju« že dolgo ni več zgolj v domeni obrambnih in obveščevalno-varnostnih organizacij. Slednje se, še posebej po terorističnih napadih leta 2001, srečujejo z načelom »potrebe po delitvi z ostalimi«, ki pa z vidika varovanja informacijske zasebnosti državljanov ni zaželeno. V Sloveniji se žal še vedno prepogosto srečujemo z nerazumevanjem, kaj točno pomeni načelo »potrebe po vedenju«. Posledično to onemogoča učinkovito vzpostavitev stanja, ki mu angleško pravimo »who knew«.

Urad informacijskega pooblaščenca je inštitucija z najvišjo stopnjo zaupanja v državi. Urad je precej izboljšal stanje na področju informacijske zasebnosti državljanov. Kljub temu stanje še ni zadovoljivo, odgovornost pa gre iskati v veliki razpuščenosti in neorganiziranosti upravljavsko-uravnalnih vidikov informacijske varnosti v državi. Zaradi prevelikega zanašanja na zaupanje in odsotnosti načela »potrebe po védenju« je varovanje osebnih podatkov z mehanizmom sledljivosti dostopa do podatkov popolnoma odpovedalo. Prav tako v današnjem času, ko se je potrebno za zasebnost boriti, različni dobronamerni priročniki, namenjeni mladim, nehote podajajo izkrivljeno sliko odgovornosti za informacijsko zasebnost državljanov. Zavarovanje osebnih podatkov je urejeno v 24. členu Zakona o varstvu osebnih podatkov (ZVOP-1). Kljub temu je problematika zavarovanja osebnih podatkov v informacijskih sistemih precejšen problem, zato je na tem mestu smiselno predlagati naslednje:

Obvezna uvedba načela »potrebe po védenju« v izbranih informacijskih sistemih.

Razlog: Notranjega sovražnika pri varovanju občutljivih podatkov v informacijskih sistemih predstavlja zaupanja vredna, pooblaščena oseba. Zakonodaja že

določa, da se nepooblaščenim osebam onemogoči dostop do občutljivih podatkov. Zato so ravno pooblaščene osebe tiste, ki predstavljajo agenta grožnje. Načelo »potrebe po védenju« onemogoča samovoljno pregledovanje zapisov s strani oseb, ki sicer imajo za to ustrezne dostopne pravice. Oznake skupin občutljivih informacijskih postavk na različnih varnostnih nivojih omogočajo, da subjekt z nižjim varnostnim dovoljenjem izloči uporabnika z višjim varnostnim dovoljenjem. Pogostokrat pa se izkaže, da je implementacija načela prezahteven organizacijski in logično-tehničen zalogaj. Omeniti velja, da je še vedno ponekod prisotna okoljsko specifična odsotnost posamičnih dostopnih pravic, ki jo nadomešča uporaba skupinskih delovnih pravic, kar je nedopustno.

Obvezna uporaba naprednejših metod za zaznavanje zlorab informacijskih sistemov ter obveščanje oseb v realnem času.

Razlog: Beleženje, ki omogoča učinkovito izvajanje nivoja sledljivosti, imenovanega »sledljivost dostopa do podatkov«, mora biti predmet inteligentnih analiz podatkov. Predhodno je potrebna uporaba namenskih rešitev za ugotavljanje zlorab informacijskih sistemov, saj se le tako zagotavlja uspešnost funkcije ter precej zmanjšuje možnost manipulacij po ugotovljenih kršitvah. Hkrati je potrebno uvesti obveščanje oseb, do katerih podatkov se je dostopilo, in sicer v realnem času prek elektronske pošte v vnaprej predpisani obliki.

Za varovanje podatkov v informacijskih sistemih je ključna uporaba mehanizmov, ki so zaradi stalne pojavnosti omenjene problematike stalno predmet raziskav in razvoja. Predstavljena sta zgolj dva predloga, ki bi precej izboljšala obstoječo problematiko. Priporočljivi bi bili še dodatni ukrepi, kot so: pametna sanacija zapisov, varnostni priporočilni sistem in specializirane predhodne, sprotne in povratne kontrole.

4 Zaključek

Kljub nezadostni skrbi za informacijsko varnost v večini organizacij, te obdelujejo občutljive podatke in udejanjajo že skoraj bizarno željo po zbiranju vseh mogočih podatkov. Za skrbnike informacijskih sistemov še vedno ne izbirajo ustreznih strokovnjakov, ki bi omogočal vsaj zadostno varovanje informacij. V državi se je nujno potrebno zavzeti za velik dvig varnostnih standardov. Hkrati je potreben

pritisk na izboljšanje različnih smernic, delovnih navodil in večjo resnost pri obravnavi nepravilnosti.

Varnostna vprašanja je potrebno presojati z vidika agentov grožnje, za kar pa je obvezen nabor izvornih znanj, seznanjanje z najnovejšimi dognanji in vrhunsko poznavanje nasprotnika. Glede na obravnavano tematiko avtor članka priporoča upravljavcem pomembnejših informacijskih sistemov vzpostavitev oddelkov za informacijsko varnost ali premik odgovornosti ven iz sektorja informatike. Glede na omejeno razpoložljivost ustreznih strokovnjakov bi veljalo premisliti o vzpostavitvi skupnega oddelka za informacijsko varnost v organizacijah, ki imajo podobno področje dela in so uvrščene v isto statistično regijo.

Viri

- Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M. in Saydjari, S. O. (2005). Mission Oriented Risk and Design Analysis of Critical Information Systems. Military Operations Research, 10 (2), 19–37.
- Gao, C., Xiao, C., Xu, X. in Gao, Y. (2012). Secure Information Systems: Extensions to BLP Model. Advances in information Sciences and Service Sciences, 4 (4), 58–65.
- Goldberg, I. (2008). Privacy-Enhancing Technologies for the Internet III: Ten Years Later. V Acquisti, A., Gritzalis, S., Lambrinoudakis, C., Vimercati, S. Digital Privacy: Theory, Technologies, and Practices. (3–18). Miami: Auerbach Publications.
- Habib, L., Jaume, M. in Morisset, C. (2008). A formal comparison of the Bell & LaPadula and RBAC models. Fourth International Conference on Information Assurance and Security. 3–8. Washington, DC: IEEE Computer Society.
- Shaikh, R. A., Adi, K., Logrippo, L. in Mankovski, S. (2011). Risk-based Decision Method for Access Control Systems. NinthAnnual International Conference on Privacy, Security and Trust. 189–192.
- Smith, R. E. (2006). Multilevel Security. V Bidgoli , H., Handbook of information security, volume 3 (972–986). New Jersey: John Wiley & Sons.
- Stamp, M. in Hushyar, A. (2006). Multilevel Security Models. V Bidgoli, H., Handbook of information security, volume 3 (987–997). New Jersey: John Wiley & Sons.
- Wang, X., Wu, X., Wang, Y. in Le, D. P. (2009). The Design and Implementation of a Sensitive Information System. V Fourth International Conference on Computer Sciences and Convergence Information Technology. 1174–1179.
- Wu, X., Le, P. D. in Srinivasan, B. (2008). Dynamic Keys Based Sensitive Information System. V Zhang, J. J. (ur.) 9th International Conference for Young Computer Scientists, 1895–1901.

- Zhihong, T., Bailing, W., Ye, Z. in Zhang, H. (2011). The Survey of Information System Security Classified Protection. V Zhu, M. (ur.) Lecture Notes in Electrical Engineering, 98, 975–980.
- Zhihong,T., Jianwei, Y., Bailing, W. in Feng, L. (2011). A Security BLP Model Used in Classified Protection System. IEEE Joint International Information Technology and Artificial Intelligence Conference, 211–215.

O avtorju

Blaž Ivanc, neodvisni raziskovalec, Jožef Stefan IPS.

Zagotavljanje učinkovitosti informacijske varnosti z merjenjem

Kaja Prislan

Informacijska varnost lahko učinkovito pripomore k izpolnjevanju organizacijskih ciljev zgolj v primeru, ko je kompatibilna z varnostnimi potrebami organizacije. Njeno prilagajanje pa je mogoče, če poznamo dejansko stanje različnih ravni, ki zajemajo uporabniške in tehnične informacijskovarnostne vidike. To lahko dosežemo s pomočjo merjenja, ki se priporoča organizacijam, ko želijo identificirati ključne pomanjkljivosti v varnostnem procesu in izbrati primerne kontrolne mehanizme za njihovo upravljanje. Merjenje je proces, ki je navadno finančno nezahteven, vendar je za njegovo uporabnost potrebna organiziranost in zavzetost za izvedbo ter njegovo ohranjanje. Postopki in načini merjenja so standardizirani in prilagodljivi heterogenim poslovnim področjem, pri čemer se njihova kompleksnost povečuje s ponavljajočimi se programi merjenja. Najpomembnejša faktorja, ki sta pogoja za uspešnost procesa, sta določitev varnostnih ciljev in objektov oz. izhodiščnih točk, od katerih je v nadaljevanju odvisen način merjenja oz. uporabljena merska metoda. Učinkovitost je odvisna tudi od načina predstavitve rezultatov in kontinuiranosti samega procesa, s katerim spremljamo razvoj in izboljšanja posameznih atributov informacijske varnosti. Na ta način zagotovimo racionalne odločitve in opozorimo na pomen in prispevek informacijske varnosti k organizacijski viziji.

1 Uvod

Nadziranje in upravljanje družboslovnih pojavov je tesno povezano z njihovim merjenjem. Pojasnjevanje dejanskega stanja različnih atributov družbe je omogočilo njen razvoj in napredek, saj smo skozi zgodovino tako ugotavljali, kaj in kako je mogoče nekaj izboljšati, popraviti ali na novo razviti. Dva izmed takšnih primerov sta kriminaliteta in odklonsko vedenje, ki predstavljata veliko grožnjo eni izmed osnovnih človekovih potreb, ki mora biti izpolnjena – varnosti. Razvoj sodobne tehnologije pa je omogočil selitev odklonskih ravnanj v kibernetski prostor, kjer

je glavna posledica deviantnih pojavov ogroženost informacijske varnosti. Tovrstna varnost je posebej pomemben atribut za poslovne entitete, saj je informacijski kapital, kot glavna tarča kibernetskih groženj, najpomembnejši faktor organizacijskega uspeha. Za zagotavljanje varnosti morajo organizacije zato stalno ocenjevati in posodabljati informacijsko varnostne sisteme, zaradi nenehnih sprememb pa se morajo prilagajati tudi obstoječim varnostnim razmeram v kibernetskem prostoru.

Stanje informacijske varnosti v organizacijskem okolju je pogojeno z različnimi dejavniki, pri čemer je varnost pred (kibernetsko) kriminaliteto le eden izmed pogojev za zagotavljanje celovite varnosti. Poleg tega igrajo veliko vlogo v tem procesu tudi tehnični, uporabniški in procesnopolitični vidiki varnosti, ki morajo biti medsebojno kompatibilni in povezani, da je mogoče doseči končni organizacijski cilj. Hkrati pa je tudi informacijska varnost zgolj posamičen vidik splošne varnosti v organizaciji, zato je nikoli ne smemo razumeti ločeno od celovitega varnostnega stanja. Ker pa je informacijska varnost v veliki meri odvisna od stanja v kibernetskem prostoru, ki je abstraktne narave, je tudi merjenje njenega stanja prilagojeno in specifično.

2 Merjenje informacijske varnosti

Merjenje informacijske varnosti se je eksponentno razvilo po letu 2000, ko so bile sprožene aktivne debate o načinih, vzrokih in uporabnosti takšnega merjenja. Danes se večina strokovnjakov strinja s tem, da je merjenje informacijske varnosti v organizaciji uporabno in zaželeno (Bartol, Bates, Goertzel in Winograd, 2009). Pravzaprav je proces merjenja postal eden izmed glavnih pogojev učinkovitega upravljanja varnosti v organizaciji. Finnan (2012) navaja, da mora imeti organizacija, ki želi biti dolgoročno uspešna, izoblikovano varnostno strategijo, ki temelji na poznavanju varnostnih groženj in aktivnih meritvah učinkovitosti informacijske varnosti. Nepravilne in neracionalne odločitve pa so navadno posledica neustreznih merskih postopkov ocenjevanja trenutnega stanja in odsotnosti informacij o tem (Centre for Internet Security [CIS], 2010).

Merjenje informacijske varnosti je proces, s katerim ugotavljamo, v kolikšni meri so izpolnjeni cilji informacijskovarnostne politike in koliko ti cilji pripomorejo k stanju celovite varnosti v organizaciji (SANS Institute, 2007). Moškon in Brezavšček (2009) navajata, da je potrebno sistem upravljanja z informacijsko varnostjo (ISMS)[1] stalno nadzirati in spremljati njegovo učinkovitost. V ta namen je

[1] Information Security Management System.

potrebno vzpostaviti ustrezen sistema merjenja, s katerim lahko spremljamo, ali obstoječi sistem služi svojemu namenu; hkrati pa tak sistem merjenja omogoča analizo učinkov načrtovanih izboljšav in proučevanje smiselnosti njihove uvedbe. Navadno takšen proces uporabljamo kot podporo odločitvenim procesom, saj lahko s pridobljenimi podatki razrešujemo različne dileme in ugotavljamo, kako varni smo oz. ali smo dovolj varni, ali so finančni viri pravilno razporejeni, kakšno je doseganje varnostnih zahtev ter standardov in katero mesto dosegamo v primerjavi z drugimi organizacijami (Turner-Rice, 2012 in Practical Software and System Measurement [PSM], 2005). S pojasnjevanjem takšnih in podobnih vprašanj ugotavljamo, kaj je še potrebno storiti, da bodo zastavljeni informacijsko varnostni cilji uresničeni. Pri tem si organizacije lahko pomagajo z normativno ureditvijo, ki določa zahteve po informacijski varnosti in mednarodnimi standardi, ki dajejo priporočila pri merjenju njihovega izpolnjevanja.[2]

Konvencija o kibernetski kriminaliteti, ki jo je z zakonom (MKKKDP, 2004) ratificirala tudi Slovenija, določa, da mora vsaka država pogodbenica s posameznimi zakoni urediti zahteve po varovanju zaupnih podatkov (16. čl.) in s tem zagotoviti ustrezno stopnjo informacijske varnosti. Splošen pravni akt, ki ureja to področje v Sloveniji je Zakon o varstvu osebnih podatkov (2007), ki v 24. členu določa, da morajo biti osebni podatki v organizacijah zavarovani z ustreznimi organizacijskimi, fizičnimi, programskimi in tehničnimi ukrepi, s katerimi se prepreči uničevanje, sprememba, izguba, nepooblaščena obdelava ali nesorazmerna uporaba takšnih podatkov. Natančnejše ukrepe zagotavljanja informacijske varnosti v nadaljevanju urejajo različni zakonski akti, ki obravnavajo posamezna (kritična) organizacijska področja, kot je npr. Zakon o elektronskih komunikacijah (2007). Ta določa, da morajo operaterji komunikacij z ustreznimi tehničnimi in organizacijskimi ukrepi zagotoviti čim manj moteno delovanje sistemov v primeru nesreč ali varnostnih incidentov (96. čl), analizirati tveganja, določiti kritične ranljivosti v sistemu (102. čl.) in jih zavarovati v skladu z notranjimi pravili. Določa tudi nadzor nad zagotavljanjem takšne varnosti sistemov in podatkov (141. čl) ter kazensko odgovornost pravnih oseb (151. čl.), ki takšne varnosti ne zagotovijo. Na podoben način so določene zahteve po informacijski varnosti v drugih področnih zakonih. Natančneje pa so ukrepi zagotavljanja varnosti in izvajanja revizij oz. nadzora nad ustreznostjo varnostnih mehanizmov navadno določeni z notranjimi pravili, ki morajo biti v skladu s splošnimi usmeritvami zakonodaje.

---

[2] Najpomembnejši standardi, ki jih je potrebno proučiti pri razvijanju programa merjenja informacijske varnosti, so NIST SP 800-55 (in njegova revizija), ISO/IEC 27001 in ISO/IEC 27004. Slednji je temeljni mednarodni standard, ki povzema smernice ISO/IEC 27001 in NIST SP 800-55 ter daje vladnim službam priporočila pri razvijanju programa merjenja.

Kljub temu, da obstajajo zakonske smernice, so večinoma splošne narave, zato so organizacije pri analiziranju ustreznosti in učinkovitosti informacijske varnosti prepuščene same sebi in lastnim zmogljivostim. Do danes še vedno ni konsenza o najprimernejših ukrepih, načinih in indikatorjih merjenja učinkovitosti. Ker gre pri merjenju informacijske varnosti za ugotavljanje zelo heterogenega in abstraktnega stanja (kibernetski prostor) pa obstajajo tudi dvomi v smiselnost, učinkovitost in realnost takšnega merjenja.

Večina skeptikov ne dvomi o teoretičnih predpostavkah merjenja, temveč se sprašujejo o zmožnostih izoblikovanja pravega merskega inštrumenta, ki bi meril dejansko stanje. Po njihovem mnenju je splošno stanje varnosti tehnologije trenutno preveč nepredvidljivo, da bi bilo merjenje lahko učinkovito in uporabno (Bartol et al., 2009). Dileme se kažejo tudi pri ustreznosti kvantitativnega prikazovanja kvalitativnih atributov (Mimoso, 2009), saj pri tem prihaja do močnih odstopanj od realnega stanja. Medtem pa Steven Bellowin (2006),[3] nasprotuje učinkovitosti merjenja varnosti programskih orodij, saj naj bi bila programska oprema že po svoji naravi ranljiva, varnostnim napakam, ki nastanejo pri zasnovi opreme in njeni implementaciji, pa se zato ne moremo izogniti. Po njegovem mnenju lahko v tem trenutku, glede na varnostno slabo zasnovane programe, merimo samo verjetnosti, medtem ko je merjenje dejanskega stanja informacijske varnosti vizija v prihodnosti.

Dileme povezane z merjenjem informacijske varnosti se odražajo tudi v trenutnem stanju, v katerem so se znašle organizacije, saj študije poročajo o stagnaciji poizkusov merjenja (Mimoso, 2009). Raziskava,[4] ki jo je izvedlo podjetje PwC v letu 2011 (Finnan, 2012) ugotavlja, da podjetja sicer aktivno razvijajo informacijsko varnost, vendar varnostne zmogljivosti podjetij nazadujejo od leta 2008. Vzporedno pa analiza[5], ki jo je izvedlo podjetje Sensage ugotavlja, da 65 odstotkov organizacij ne meri stanja informacijske varnosti oz. je to merjenje neučinkovito in neustrezno razvito. Trenutna varnostna situacija je zato asimetrična, saj lahko storilci za dosego svojih ciljev zlorabijo zgolj eno ranljivost, medtem ko morajo organizacije analizirati in zavarovati vse svoje ranljivosti (Info Security, 2011).

Kljub temu, da imajo kritiki dobre argumente, pa tudi brezbrižnost in nezainteresiranost za stanje informacijske varnosti nista primerna ukrepa. Informacijska

---

3 Varnostni strokovnjak iz Columbia University.

4 Globalno stanje informacijske varnosti (Global State of Information Security Survey), 9600 izpraševancev.

5 311 izpraševancev na RSA konferenci 2011.

varnost postaja vse pomembnejši faktor poslovnega uspeha, kibernetske grožnje pa se stalno razvijajo in spreminjajo, zato je potrebno vsaj poizkusiti slediti smernicam razvoja. Seveda pri merjenju informacijske varnosti, zaradi splošnosti in heterogenosti načinov, prihaja do večjih odstopanj od realnega stanja, kot pri drugih vrstah raziskovanj, vendar lahko ugotovitve močno pripomorejo k racionalnemu izboljšanju splošne varnosti v organizaciji.

2.1 Pogoji za učinkovitost

Odsotnost poenotenih merskih inštrumentov je logična posledica heterogenosti poslovnega okolja in organizacij nasploh, saj ima vsaka poslovna entiteta svoje zahteve, cilje, načine in možnosti. Vsaka organizacija mora zato pred izvedbo procesa analizirati ter upoštevati lastne zmogljivosti, v smislu časovnih, finančnih in kadrovskih virov. Glede na to lahko proces izvede sama, če pa tega ni zmožna, lahko odgovornost prenese na druge specializirane skupine. Zaradi pomanjkanja virov manjša podjetja veliko težje izvajajo enake programe merjenja kot večje ali bolj uspešne, vendar učinkovitost merjenja navadno ni odvisna od finančnih zmožnosti temveč neustrezne organizacije in neprimernih merskih postopkov.

Proces merjenja informacijske varnosti ni finančno zahteven program, ker imajo organizacije veliko podatkov, ki jih potrebujejo, že zbranih v različnih virih,[6] zato je potrebna racionalnost pri financiranju; izdatki naj ne bodo večji kot je vrednost končnega rezultata oz. izboljšanj. Pri tem je priporočljivo upoštevati tudi t.i. pravilo KISS[7] (ohranite sistem preprost), ki priporoča izogibanje kompleksnejšim študijam in izpostavlja potrebo po enostavnosti (Hinson, 2006). Iz tega sledi, da morajo biti varnostni cilji pred izvedbo procesa natančno določeni in izvedljivi, postopek pa se ne usmerja na področja, ki niso določena v ciljih.

Odločitev o načinu merjenja informacijske varnosti je odvisna od vsake posamezne organizacije, medtem ko smiselnost takšnega merjenja ne bi smela biti dilema. Vsekakor se moramo prilagoditi potrebam po varnosti, vendar je v primeru visoke ogroženosti zaupnih in za uspeh pomembnih informacij postopek potrebno izvesti, da lahko izboljšamo trenutno situacijo. Tudi v primeru, da je stanje varnosti zadovoljivo, je potrebno varnost stalno ocenjevati in posodabljati. Merjenje pa ni nujno tudi kompleksno ali heterogeno, saj organizacija meri zgolj tisto kar

---

6 Med takšne informacije štejemo npr. podatke o izdatkih za informacijsko varnost, povratne informacije strank, poročila o varnostnih incidentih ipd. (Hinson, 2006).

7 »Keep it simple, stupid ! «.

želi, pri čemer je lahko to celoten sistem ali zgolj posamezna ranljivost. Tudi načini merjenja so lahko različni, zato so odpori do takšnega postopka nesmiselni. Pogoj, ki ga organizacija mora izpolniti za učinkovitost merjenja, je zgolj močna zaveza za razvoj učinkovitega merskega inštrumenta, njegova implementacija in ohranjanje. Poznavanje informacijske varnosti je odvisno od konstantnega merjenja takšnega stanja, zato je potrebno procese ciklično ponavljati in jih medsebojno primerjati ter pojasnjevati. Govorimo o t.i. SMART[8] merjenju (SANS Institute, 2007), ki je specifično, izvedljivo in ponovljivo.

Proces merjenja informacijske varnosti je zelo podoben drugim raziskovalnim procesom, v splošnem pa je sestavljen iz osmih korakov[9] (Bartol et al., 2009):

- Razvijanje in posodabljanje merskega inštrumenta: izbira ciljev, identifikacija virov podatkov, analiza povezav med cilji in podatki ter razvoj merskega inštrumenta.
- Zbiranje podatkov iz razpoložljivih virov.
- Shranjevanje podatkov.
- Analiza podatkov: analiziranje, sintetiziranje, interpretiranje in pojasnjevanje.
- Poročanje ugotovitev: zapis in predstavitev ugotovitev ciljni skupini/naročniku.
- Uporaba informacij pri sprejemanju odločitev, razporejanju finančnih virov, določanju varnostnih prioritet in komunikaciji z vodstvenim kadrom.
- Odločitev o varnostnih mehanizmih in korektivnih ukrepih.
- Ocenjevanje in izboljševanje varnosti s kontinuiranim merjenjem.

S cikličnim ponavljanjem merskega procesa se povečujeta njegova zrelost in učinkovitost. Proces v osnovi ostaja enak, vendar se s kontinuiranostjo merjenja in izboljševanjem spreminjajo procesi in postopki, povečuje se količina dostopnih podatkov, merjenje postaja vse bolj standardizirano, podatke pa je lažje in hitreje zbrati.

---

8 Specific, measurable, attainable, repeatable, time-dependent.

9 Proces merjenja informacijske varnosti je podoben shemi PDCA kroga, kot ga priporočajo in opisujejo ISO standardi.

3 Ravni merjenja

Merjenje informacijske varnosti lahko poteka na različnih ravneh in je usmerjeno v različna področja. Slednja lahko opredelimo glede na časovni, razvojni ali procesni vidik. Od izbranega vidika so odvisni tudi načini merjenja, pridobivanja podatkov in analize, ki jih pri tem uporabimo.

S časovnega vidika je načrtovanje varnostne situacije proces, ki temelji na informacijah o preteklosti, da bi pridobili informacije za načrtovanje aktivnosti v prihodnosti, ob upoštevanju trenutne situacije, zmogljivosti in priložnosti. Podatke o preteklosti zbiramo z analizami prejšnjih rezultatov in ugotavljanjem zadovoljstva strank; trenutno stanje ugotavljamo z analiziranjem učinkovitosti, odzivnosti in postopkov okrevanja po varnostnih incidentih; medtem ko načrtujemo prihodnje ukrepe s pomočjo analiziranja tveganj, ozaveščenosti zaposlenih in želenih ciljev (PSM, 2005).

Z razvojnega vidika se proces deli glede na stopnjo razvoja in zmožnosti organizacije. Osnovni oz. začetni proces merjenja se osredotoča na določanje varnostnih ciljev ter ključnih indikatorjev; nadaljevalni procesi se osredotočajo na merjenje implementacije ukrepov in učinkovitosti kontrolnih mehanizmov; najbolj razviti modeli pa se usmerjajo v merjenje učinka informacijske varnosti na poslovni uspeh in kompatibilnost z organizacijskimi cilji ter vizijo (National Institut for Standards and Technology [NIST], 2008). Pri tem se z vsako stopnjo povečuje kompleksnost analiz in merskega inštrumenta.

S procesnega vidika je merjenje lahko usmerjeno na strateško, taktično ali operativno raven. Pri analiziranju strateških vidikov se osredotočamo predvsem na trenutno informacijskovarnostno politiko, odnos managementa in zavezo vodstva kot podporo varnostnemu programu. Na taktični ravni nas zanima razporeditev razpoložljivih virov in učinkovitost pri implementaciji varnostnih ukrepov. Merjenje na operativni ravni pa se usmerja na vsakodnevne aktivnosti povezane z upravljanjem groženj, ranljivosti in varnosti nasploh (Mahncke, McDermid in Williams, 2009). Pri tem je lahko objekt merjenja informacijske varnosti organizacija procesov, posamičen produkt ali postopek, celoten informacijski sistem ali njegov del, vedenje ljudi ali pa varnost kot celota (Savola, 2006).

Za zagotovitev učinkovitosti merjenja informacijske varnosti je delitev na posamezna področja smiselna rešitev, saj s tem natančno določimo objekt merjenja. Trije omenjeni vidiki pa so medsebojno povezani saj se z razvijanjem programa stopnjujejo ravni na posamezni stopnji. Začetni poizkusi so navadno usmerjeni

v pridobivanje informacij o preteklih operativnih aktivnostih. Nadaljevalni programi se usmerjajo na srednjo oz. taktično raven, kjer pridobivamo informacije o trenutnem stanju postopkov in njihove implementacije. Napredni programi, ki so produkt cikličnosti in stalnih izboljševanj, pa proizvajajo kompleksnejše ugotovitve, usmerjene v strateško raven, kjer sta glavna indikatorja uspeh organizacije in njena informacijskovarnostna politika. Načini merjenja v posamezni fazi so pri tem odvisni od objekta, ki ga analiziramo, zbiranje podatkov pa je pri tem navadno standardizirano.

3.1 Ključni indikatorji

Da bi se v čim večji meri izognili napakam in zmanjšali odstopanja od realnega stanja, je potrebno proces merjenja izvajati natančno, po vnaprej določenih korakih. Pri tem je najpomembnejši pogoj, od katerega je odvisna učinkovitost merjenja, predhodna določitev kriterijev merjenja oz. t.i. ključnih indikatorjev učinkovitosti[10] (Pironti, 2007). Z njihovo pomočjo določimo izhodiščne točke pri merjenju in primerjanju stanj, z njihovim poznavanjem pa je veliko lažje določiti tudi atribute, ki jih bomo dejansko merili. Indikatorje učinkovitosti je najlažje določiti s pomočjo informacijskovarnostnih ciljev, ki so zapisani v varnostni politiki organizacije. Na podlagi ciljev lahko določimo tudi varnostne ideale, h katerim stremi organizacija, s čimer je odločitev o objektu merjenja veliko lažja.

Primer varnostnih idealov za ameriške SCADA sisteme in način merjenja njihovega doseganja (McQueen, Boyer, McBride, Farrar in Tudor, 2008):

- Varnostna skupina popolnoma pozna kontrolne sisteme, identificira vsak zlonameren napad in takoj vzpostavi integriteto kontrolnega sistema po incidentu (primer merjenja: identifikacija pomanjkljivosti v varnostnih pregledih, pomanjkljivosti v sistemu detekcije groženj in čas okrevanja).
- Zlonamerna skupina sploh ni seznanjena s kontrolnimi sistemi organizacije (primer merjenja: izpostavljenost podatkov pri njihovem prenosu).
- Kontrolni sistemi so nedostopni zlonamernim skupinam, so popolnoma neranljivi in ne morejo povzročiti škode v primeru incidenta (primer merjenja: analiza dostopnosti sistema in truda pri napadu, čas razbijanja gesel, škoda v primeru najslabšega mogočega scenarija).

[10] KPI-Key Performance Indicator.

Iz tega sledi, da so ključni indikatorji učinkovitosti v tem primeru zaščiteni kontrolni sistemi, uspešne varnostne skupine in neuspešne zlonamerne skupine. Gre za splošne varnostne ideale, pri čemer so lahko v drugem organizacijskem okolju indikatorji drugačni ali bolj specifični, saj so odvisni od potreb in ciljev organizacije. Kadar ta ni povsem prepričana, katera področja zajeti v merjenje posameznega ideala ali ključnega indikatorja, si lahko pomaga tudi s priporočili različnih varnostnih strokovnjakov ali mednarodnih organizacij. V splošnem lahko organizacija meri vse, kar je mogoče zabeležiti s podatki, relevantnost posameznega objekta, sistema ali postopka pa je odvisna od prioritet organizacije.

4 Načini merjenja

Mednarodna organizacija CIS je sprejela konsenz o področjih merjenja informacijske varnosti; to so: aplikacije, spremembe, finance, grožnje, ranljivosti in varnostni popravki (CIS, 2010). O teh področjih lahko zbiramo najrazličnejše informacije. Lahko nas zanimajo odstotek kritičnih aplikacij in njihovi rezultati ob varnostnem testiranju. Za ugotavljanje položaja informacijske varnosti na lestvici pomembnosti je pomembna tudi razporeditev finančnih virov skozi celoten varnostni sektor. Eden izmed vidikov so grožnje, pri katerih nas zanima čas njihovega odkrivanja in čas okrevanja po incidentih, odstotek zlonamernih groženj (okužba z zlonamerno programsko opremo ali napad iz omrežja) in napak (malomarnost, nesreča, okvara) ter statistika požarnega zidu. Ugotavljamo lahko tudi ranljivosti na različnih področjih, od tehnološke do uporabniške, in čas za njihovo odkritje ter odpravo. Velik vpliv na stanje informacijske varnosti imajo spremembe procesov in tehnologije, njihovo sprejemanje in trajanje. Vir informacij so lahko rezultati varnostnih pregledov sistema ter statistika varnostnih popravkov s časovnega vidika (povzeto po: SANS Institite, 2010, Hinson, 2006, CIS, 2010). Pomembno je proučiti tudi varnost podatkov pri njihovem prenosu in izpostavljenosti zunanjim vplivom. Vse pogosteje pa se v merjenje informacijske varnosti vključuje tudi politika ravnanja z mobilnimi napravami in uporabe socialnih omrežij.

Posebna oblika merjenja informacijske varnosti so penetracijski testi, s katerim simuliramo realne scenarije napadov in vdorov v sisteme. Pri tem je ena skupina sestavljena iz strokovnjakov, katerih namen je penetrirati v sistem oz. omrežje določene žrtve, medtem ko je naloga druge ekipe minimizirati učinke teh napadov na varnostni sistem. S takšnimi testi lahko pridobimo natančne informacije o varnostnih procesih in ranljivostih v sistemu (Bartol et al., 2009).

Poleg tehničnih in postopkovnih vidikov v procesu ugotavljanja varnosti, vključujemo tudi uporabniški vidik, saj stanje informacijske varnosti ni odvisno samo od političnih in tehničnih ukrepov. Navsezadnje je ravnanje in vedenje ljudi ključni dejavnik, ki odloča, ali bodo tehnični ukrepi in politika zaživeli v praksi. Uporabniško raven informacijske varnosti ugotavljamo z merjenjem informacijskovarnostne ozaveščenosti zaposlenih, kot uporabnikov tehnologije v delovnem okolju. Pri tem je ozaveščenost kompleksen pojav, odvisen od znanja, vedenja in odnosa zaposlenih, kar je potrebno upoštevati tudi pri merjenju.

Model za merjenje informacijsko varnostneozaveščenosti zaposlenih po Kreuger in Kerneyu (2006) vključuje predpostavke o znanju, odnosu in obnašanju zaposlenih z vidika informacijske varnosti. Merjenje se osredotoča na to, kaj zaposleni vedo, kaj si mislijo in kako se obnašajo pri uporabi tehnologije in v primerih uresničenih informacijskih incidentov. Na podlagi rezultatov je možno izmeriti tudi indeks ozaveščenosti v različnih oddelkih, narediti mapo stanja ozaveščenosti in predlagati smernice za izboljšanje stanja varnosti v organizaciji. Pri merjenju teh treh atributov lahko uporabimo različne indikatorje. Merimo lahko dostope do nedovoljenih internetnih strani, neveljavne poskuse prijavljanja v sistem, incidente povezane s shranjevanjem nedovoljenih vsebin, poskuse dostopanja do nedostopnih informacij, incidente povezane z razkrivanjem in krajo zaupnih informacij ipd. Priporočila organizacije ISSA pa izpostavljajo še potrebo po merjenju disciplinskih postopkov, rezultatov testiranj zaposlenih in njihovo poznavanje informacijsko varnostne politike, kršitev pravil in ugotavljanje incidentov, ki so povzročeni s strani zaposlenih (Bartol et al., 2009).

Sprejem informacijsko varnostnih pravil je najbolj učinkovit, kadar smo poučeni o zmogljivostih in možnostih tistih, ki naj bi pravila upoštevali. Ob implementaciji sprejete politike pa mora organizacija s pomočjo različnih izobraževalnih programov, tečajev usposabljanja in testov preverjanja poskrbeti za njeno razumevanje in dosledno upoštevanje. Tako kot je potrebno periodično ocenjevanje in posodabljanje tehnologije in varnostnih mehanizmov, je potrebno preverjati in dopolnjevati tudi znanje o tem.

5 Analiza in predstavitev podatkov

Ne glede na raven merjenja (politično/tehnično/uporabniško) ali način, ki ga uporabimo pri zbiranju podatkov, so končni rezultat kvantitativni ali kvalitativni podatki, ki odražajo stanje varnosti. Navadno zbiramo kvantitativne podatke,

da lahko primerjamo rezultate, uporabimo formule za analize in spremljamo spremembe pri istih izhodiščnih točkah (PSM, 2005). ISO/IEC 27004 kot najpogostejše vire informacij oz. načine zbiranja informacij omenja intervjuje, anketne vprašalnike, revizijska poročila in poročila o varnostnih incidentih. V začetni fazi se podatki navadno zbirajo ročno oz. osebno, z razvojem programa pa lahko kompleksnejše podatke pridobimo s pomočjo avtomatiziranih orodij in modelov[11] (NIST, 2008). Pri merjenju informacijske varnosti pridejo v poštev različne merske lestvice, pri čemer se največkrat uporabljajo ordinalne (Bartol et al., 2009), saj z numeričnimi lestvicami lažje prioritiziramo različna tveganja in grožnje (PSM, 2005). Tudi rezultati merjenja se največkrat prikazujejo v numerični obliki (povprečja, odstotki ipd.), saj lahko z natančnimi merskimi lestvicami in točnimi numeričnimi prikazi zmanjšamo subjektivnosti pri merjenju (Mahncke et al., 2009).

Podatke, ki jih pridobimo s pomočjo merjenja, potem ko so shranjeni v primerni obliki, analiziramo s pomočjo različnih statističnih metod. Najpogosteje se za prikazovanje in pojasnjevanje informacij uporablja deskriptivna statistika ter linearne povezave med posameznimi atributi oz. spremenljivkami. Za napovedovanje stanja se lahko uporabljajo tudi multivariatne statistične metode, ki ugotavljajo bolj kompleksne povezave, vendar je tudi pri prikazovanju rezultatov potrebno imeti v mislih pravilo enostavnosti, saj je uspeh merjenja odvisen tudi od predstavitve podatkov. Pironti (2007) pri tem predlaga razčlenitev poročanja na tri ravni: za sistemske administratorje, menedžment in vodstvo, kjer se tehnična poglobljenost v rezultate zmanjšuje s posamezno ravnjo. Rezultati se navadno prikazujejo s pomočjo grafičnih orodij, kjer so mogoče primerjave različnih področij in informacij, hkrati pa je razumljivost prikazov večja. Poročila morajo biti časovno kontinuirana in ciklična, pri čemer je po mnenju Hinsona (2006) smiselno izdajati mesečna poročila vodjem oddelkov o varnostnih incidentih in škodi, četrtletna poročila najvišjemu menedžmentu odgovornemu za organizacijsko varnost, kjer se določajo ravni ogroženosti in ključni indikatorji ter letno visoko zaupno poročilo vodstvu o dosedanjih uspehih in pomanjkljivostih.

S pomočjo končnih informacij, ki so predstavljene na primeren način, lahko pri vodstvenem kadru vzbudimo zanimanje za informacijsko varnost. Veliko raziskav poroča o pomanjkanju virov za informacijskovarnostne potrebe organizacij,

[11] Pri izvajanju takšnih analiz imamo na voljo orodja, kot so COBIT (NIST), ISF orodja (ISF Benchmark, FIRM), DREAD Model (Microsoft) in metode kot npr. pričakovana letna izguba, analiza stroškov in koristi, analiza upravljanja s tveganji, penetracijski testi ipd.

zato lahko z opozarjanjem na ogroženost in tveganja povečamo podporo programom informacijske varnosti. Na podlagi rezultatov merjenja lahko vodstvo sprejema racionalne odločitve, ki temeljijo na točnih podatkih o dejanskem stanju. Informacije pridobljene s pomočjo merjenja pripomorejo k lažjemu odločanju glede upravljanja groženj, ki pretijo informacijski varnosti. Organizacija oz. menedžment lahko sprejme različne odločitve in ukrepe glede posameznih tveganj. Lahko npr. zmanjša verjetnost uresničenja grožnje/napada, popolnoma odpravi ranljivosti, zmanjša verjetnosti incidentov s sistemi detekcije, zmanjša posledice v primeru uresničene grožnje ali izboljša postopke okrevanja (PSM, 2005), lahko pa se odloči popolnoma prezreti določeno tveganje. Kadar ukrepi temeljijo na točnih podatkih so ti bolj učinkoviti, racionalni in izvedljivi, neželene posledice pa so manj verjetne, kar je tudi glavna prednost poznavanja in merjenja informacijske varnosti.

6 Sklep

Kakor vsak proces povezan z upravljanjem informacijske varnosti, je tudi njeno merjenje dinamičen proces, ki se mora stalno razvijati in posodabljati. Kljub zahtevam, ki morajo biti izpolnjene, za njegovo učinkovitost (kot npr. cikličnost, specifičnost, enostavnost, racionalnost ipd.) in oviram (abstraktnost, splošnost, subjektivnost pojavov) je merjenje informacijske varnosti izjemno fleksibilen proces, ki ga je mogoče prilagoditi razpoložljivim virom, obstoječim informacijam in informacijskovarnostnim ciljem. Tudi v primeru dilem ali neizkušenosti si organizacije pri načrtovanju in izvedbi procesa lahko pomagajo z različnimi priporočili, standardi, primeri dobre prakse in avtomatiziranimi orodji. Zaradi tega in prednosti, ki jih prinaša poznavanje informacijske varnosti (racionalne odločitve, smiselni ukrepi, večja podpora), je merjenje priporočljivo in zaželeno, predvsem kadar organizacija želi uskladiti stanje informacijske varnosti z mednarodnimi zahtevami, standardi in najpomembneje, z organizacijsko vizijo.

Kljub prednostim, ki jih prinaša takšno merjenje, pa je to področje, tako kot informacijska varnost nasploh, izjemno neurejeno in še vedno prepuščeno vsaki organizaciji zase. Za izboljšanje trenutnega stanja bi bilo smiselno zakonsko oz. politično urediti zahtevo po poročanju o stanju informacijske varnosti na nacionalni ravni. Takšen ukrep bi bil potreben predvsem za tista organizacijska področja, kjer je informacijska varnost rizičnega pomena, (npr. kritična infrastruktura in državni organi) in kjer so takšne direktive tudi dovoljene. Poleg tega bi bilo smiselno sprejeti

univerzalno terminologijo, povezano z merjenjem in informacijsko varnostjo, saj bi se s tem veliko lažje poenotili tudi merski inštrumenti. Čeprav je zaradi heterogenosti organizacijskega okolja izoblikovanje univerzalnega merskega modela nemogoče, pa bi bila potrebna večja prizadevanja v smeri razvijanja modelov za različne industrije in poslovne usmeritve. Nenazadnje pa je v slovenskem prostoru potrebno dvigniti zanimanje za merjenje informacijske varnosti, saj je to področje zaenkrat še nerazvito, medtem ko za poslovno uspešnost organizacij skriva veliko potenciala.

Viri

- Bartol, N., Bates, B., Goertzel, K. in Winograd, T. (2009). Measuring Cyber Security and Information Assurance. State-of-the-Art Report. Herndon: Information Assurance Technology Analysis Center [IATAC].
- Bellovin, S. (2006). On the Brittleness of the Software and the Infeasibilty of Security Metrics. Pridobljeno 10. 8. 2012 na https://www.cs.columbia.edu/smb/talks/brittle-metricon.pdf
- Centre for Internet Security [CIS]. 2010. The CIS consensus security metrcis. Pridobljeno 10. 8. 2012 na http://benchmarks.cisecurity.org/en-us/?route=downloads.metrics.
- Finnan, J. (2012). Measuring Information Security Effectiveness. Pridobljeno 7. 8. 2012 na http://www.ciozone.com/index.php/Security/Measuring-Information-Security-Effectiveness.html
- Hinson, G. (2006). Seven Myths about Information Security Metrics. ISSA Journal. Pridobljeno 15. 8. 2012 na http://www.noticebored.com/html/metrics.html
- Info Security (2011). Most Enterprises Poor at Measuring Information Security Effectiveness. Pridobljeno 8. 8. 2012 na http://www.infosecurity-magazine.com/view/16928/most-enterprises-poor-at-measuring-information-security-effectiveness/
- Kreuger, H. A. in Kerney, W. D. (2006). A Prototype for Assessing Information Security Awareness. Computers & Security, 25, 289-296.
- Mahncke, R. J, McDermid, D. C. in Williams, P. (2009). Measuring Information Security Governance within General Medical Practice. Australian Information Security Management Conference. Pridobljeno 10. 8. 2012 na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1008&context=ism
- McQueen, M., Boyer, W., McBride, S., Farrar, M. in Tudor, Z. (2008). Measurable Control System Security through Ideal Driven Technical Metrics. SCADA Security Scientific Symposium. Pridobljeno 15. 8. 2012 na http://www.inl.gov/technicalpublications/Documents/3881671.pdf
- Mimoso, M.S. 2009. Number-Driven Risk Metrics Fundamentally Broken. Pridobljeno 20. 8. 2012 na http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html#

- Moškon, S. in Brezavšček, A. (2009). Merjenje učinkovitosti sistema za upravljanje informacijske varnosti. Pridobljeno 20. 8. 2012 na http://www.fvv.uni-mb.si/dv2009/Zbornik/clanki/moskon_brezavscek.pdf
- National Institut for Standards and Technology [NIST]. (2008). NIST SP800-55 Rev.1 Performance Measurement Guide for Information Security. Pridobljeno 20 .8. 2012 na http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
- Pironti, J.P. (2007). Developing Metrics for Effective Information Security Governance. Information System Control Journal, 2, str. 1-5.
- Practical Software and System Measurement [PSM]. (2005). Security Measurement. PSM White Paper. Pridobljeno 12 .8. 2012 na http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf
- SANS Institute. (2007). A Guide to Security Metrics. Pridobljeno 10. 8. 2012 na http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55
- Savola, R. (2006). Measuring Information Security. IPLU worskshop. Pridobljeno 10. 8. 2012 na http://iplu.vtt.fi/digitalo/iplu_savola.pdf
- Turner-Rice, S. (2011). Who's Measuring Information Security Risk Anyway? Pridobljeno 22. 8. 2012 na http://www.tripwire.com/state-of-security/it-security-data-protection/whos-measuring-information-security-risk-anyway/
- Zakon o elektronskih komunikacijah [ZEKOM]. (2007). Uradni list RS, (13/07).
- Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih [MKKKDP]. (2004). Uradni list RS, (17/04).
- Zakon o varstvu osebnih podatkov [ZVOP-1]. (2007). Uradni list RS, (94/07).

O avtorju

Kaja Prislan, podiplomska študentka, Fakulteta za varnostne vede, Univerza v Mariboru.

Projekt vpeljave sistema za upravljanje informacijske varnosti v organizacijo

Klemen Vehar, Alenka Brezavšček, Tomaž Kern

Informacijska podpora poslovnim procesom je postala ključnega pomena pri učinkovitosti posameznih procesov. Ker je informacijska tehnologija v organizacijah izpostavljena različnim varnostnim tveganjem, je potrebno poskrbeti za ustrezen nivo informacijske varnosti. Tega zagotovimo z ustrezno vpeljanim sistemom za upravljanje informacijske varnosti – SUIV. Ker je vpeljava SUIV v organizacijo kompleksna aktivnost, je v prispevku prikazano, kako lahko s pomočjo napotkov standarda ISO/IEC 27003 in z uporabo računalniških orodij za projektno vodenje izdelamo plan vpeljave SUIV za določeno organizacijo.

KLJUČNE BESEDE: informacijski sistem, varnost, SUIV, ISO/IEC 27001, ISO/IEC 27003, projektni plan, PROSIS

1 Uvod

Glede na to, da je danes informacijska tehnologija že tako napredovala in je postala povsem nepogrešljiv del našega vsakdana, je potrebno razmišljati tudi o njeni varni uporabi.

Informacijski sistemi, ki se uporabljajo v organizacijah, so že nekaj časa nepogrešljiva hrbtenica vsake organizacije. Svojo nemoteno dosegljivost od kjer koli na svetu morajo zagotavljati z najvišjo stopnjo varnosti in zanesljivosti, hkrati pa morajo preprečevati neavtorizirane fizične in logične poskuse vdorov ali odtujitve informacij.

Neljubi dogodki, ki se uresničijo zaradi nepravilne rabe (zaradi nepoučenosti uporabnika) informacijske tehnologije in neustrezne varnostne politike, lahko povzročijo izpad in nedostopnost informacijskega sistema. Slednje lahko

onemogoči nemoteno izvajanje poslovnih procesov v organizaciji, kar zanjo pomeni izpad dohodka. Zato je potrebno zmanjšati možnosti, da bi do takih neljubih dogodkov, ki jih imenujemo tudi grožnje varnosti, sploh prišlo.

Da bi zagotovili stabilno delovanje informacijskega sistema in s tem omogočili nemoteno izvajanje poslovnih procesov v organizaciji, moramo varnosti informacijskega sistema nameniti dovolj pozornosti. Vse prevečkrat se namreč zgodi, da organizacije pomembnost dobre varnostne politike in izobraženost uporabnikov o pravilni rabi informacijskega sistema spoznajo šele takrat, ko je že prišlo do t.i. varnostnega incidenta.

Izsledki v literaturi kažejo na to, da zagotavljanje varnosti v velikih organizacijah zahteva sistematičen pristop, ki zahteva vpeljavo sistema za upravljanje informacijske varnosti (v nadaljevanju SUIV) (Brezavšček in Moškon, 2009). Kot navajata Calder in Watkins (2008), je vpeljava SUIV v določeno organizacijo nujna, saj se izpostavljenost grožnjam varnosti, ki pretijo zaupnosti, celovitosti in razpoložljivosti dobrin informacijskega sistema, vseskozi povečuje.

Vpeljava SUIV v organizacijo je kompleksna aktivnost. Sestavljena je iz več povezanih faz, ki so vsaka zase kompleksna in zahtevna. Proces vpeljave je zato potrebno čim bolj poenostaviti in ga razdelati na več aktivnosti znotraj posamezne faze. Procesni pristop pri vpeljavi SUIV omogoča, da se ta stalno izboljšuje tudi po vpeljavi. S stalnim preverjanjem in korektivnimi ukrepi namreč dosežemo to, da SUIV živi in diha z organizacijo ter tako dejansko služi svojemu namenu.

Pri vpeljavi SUIV so nam v veliko pomoč mednarodni standardi, ki so nastali na podlagi najboljših praks v različnih organizacijah. Napisani so dovolj ohlapno, da lahko njihovo vsebino prenesemo v organizacijo kakršne koli velikosti in dejavnosti. Vodilno vlogo na tem področju zavzema družina standardov 27000.

V pričujočem prispevku se bomo osredotočili na standarda ISO/IEC 27001 in ISO/IEC 27003. Standard ISO/IEC 27001 predpisuje zahteve za vpeljavo celovitega SUIV v organizacijo. Standard ISO/IEC 27003 pa se osredotoča na prvo fazo vpeljave SUIV, ki je faza načrtovanja. Ta faza je za vpeljavo celovitega SUIV ključnega pomena, saj je skrbno načrtovan SUIV predpogoj za njegovo učinkovito delovanje v prihodnosti. Standard ISO/IEC 27003 definira vse aktivnosti, ki jih je v organizaciji potrebno izvesti v fazi načrtovanja SUIV.

Zaradi številnih kompleksnih in medsebojno prepletenih aktivnosti, ki jih zahteva vpeljava SUIV v organizacijo, bomo v praksi dosegli večje uspehe, če bomo pri vpeljavi SUIV uporabili projektni pristop. Osnovo za uspešno izvedbo katerega

koli projekta pa predstavlja skrbno pripravljen in definiran projektni plan. V prispevku želimo prikazati, kako lahko s pomočjo obstoječih standardov in računalniških orodij za projektno vodenje pripravimo projektni plan vzpostavitve SUIV in s tem olajšamo kompleksnost vpeljave SUIV v organizacijo.

2 Sistem za upravljanje informacijske varnosti – SUIV

Če torej hočemo v organizaciji vzpostaviti željeni nivo informacijske varnosti in s tem zagotoviti stabilnost izvajanja poslovnih procesov, ki jih podpira informacijska tehnologija, moramo vpeljati ustrezen SUIV. Z vpeljavo SUIV želimo v organizaciji ustvariti varno okolje, v katerem neprestano skrbimo za udejanjanje in izboljševanje ukrepov zoper grožnje varnosti. Pri vpeljavi takega sistema je organizacijam v veliko pomoč mednarodni standard ISO/IEC 27001. Ta standard podaja specifikacije za SUIV, ki so pogoj za pridobitev certifikata skladnosti s standardom ISO/IEC 27001. Zajema organizacij ne glede na vrsto, velikost in značaj (npr. trgovinska podjetja, vladne agencije, neprofitne organizacije) (BS ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements, 2005). ISO/IEC 27001 uvaja procesni pristop upravljanja informacijske varnosti, ki temelji na štirih fazah Demingovega kroga:

- Faza 1: načrt vpeljave SUIV.
- Faza 2: uvedba SUIV.
- Faza 3: vzpostavitev sistema kontrol in nadzora nad delovanjem SUIV.
- Faza 4: analiza odstopanj SUIV in izvajanje korektivnih ukrepov.

Za vsako izmed naštetih faz ponuja standard ISO/IEC 27001 smernice in splošne principe, ki so pomembni za celovito vpeljavo SUIV v organizacijo (Brezavšček in Moškon, 2009). Z izvedbo teh štirih faz nastane celovit SUIV, ki organizaciji omogoča, da oceni tveganja in uvede ustrezne nadzorne mehanizme. Glavni namen nadzornih mehanizmov je zavarovanje informacij organizacije in preprečitev izgube ali zlorabe informacij (ISO 27001: Sistem vodenja varovanja informacij, 2012).

Pri vzpostavitvi SUIV je ključnega pomena prva faza, v kateri je potrebno pripraviti načrt vpeljave SUIV. Ker je ta faza zelo kompleksna (predvsem v velikih

organizacijah), zahteva izdelava načrta za vpeljavo SUIV projektni pristop. Kot pomoč za uspešno izdelavo projektnega načrta za vpeljavo SUIV je mednarodna organizacija za standardizacijo ISO izdala poseben standard ISO/IEC 27003, ki podaja natančna navodila, kako se v praksi lotiti izdelave takšnega načrta. Standard ISO/IEC 27003 predlaga, da se izdelava načrta za vpeljavo SUIV v organizacijo razdeli na pet povezanih faz, ki jih bomo podrobneje predstavili v nadaljevanju. Povedati je potrebno, da prva faza načrtovanja SUIV po standardu ISO/IEC 27003 ni zahteva standarda ISO/IEC 27001, je pa zelo priporočljiva, saj pove, kaj je namen in kakšni so cilji vpeljave SUIV v organizacijo.

3 Model načrtovanja SUIV po standardu ISO/IEC 27003

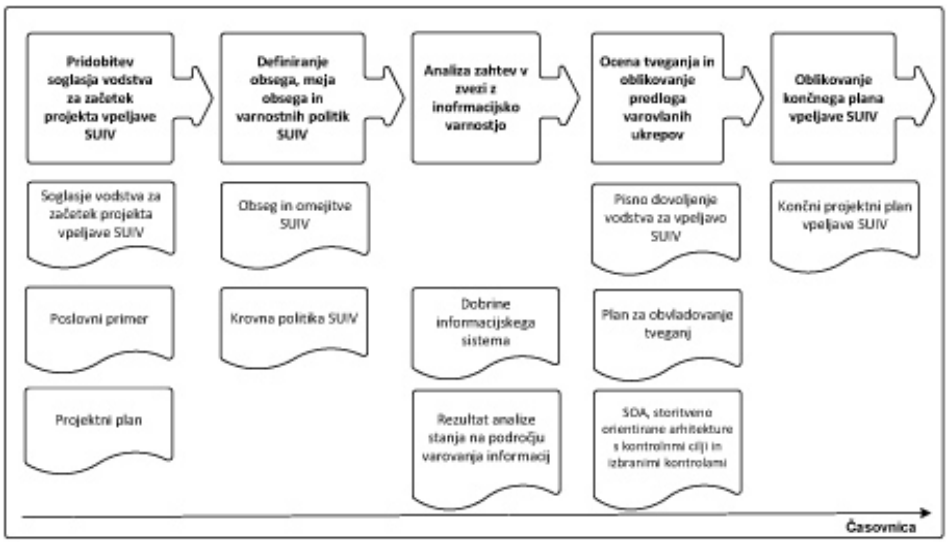
Načrtovanje vpeljave (kot prva faza vpeljave SUIV v organizacijo) je obsežen projekt, ki se ga moramo lotiti procesno, zato je tudi standard ISO/IEC 27003 razdeljen na pet faz, kot sledi: (ISO/IEC 27003:2010 Information Technology — Security Techniques — Information Security Management System Implementation Guidance, 2010):

- Faza 1: pridobitev soglasja vodstva za začetek projekta vpeljave SUIV.
- Faza 2: definiranje obsega politike, meja obsega in varnostne politike SUIV.
- Faza 3: analiza zahtev v zvezi z informacijsko varnostjo.
- Faza 4: ocena tveganja in oblikovanje predloga varovalnih ukrepov.
- Faza 5: oblikovanje končnega načrta vpeljave SUIV.

Vsaka izmed petih faz vsebuje več aktivnosti in nalog, ki morajo biti dokončane za uspešno izvedbo posamezne faze in za nadaljevanje naslednje faze. Tak način priprave načrta mora biti dobro premišljen in skrbno pripravljen, saj je dober načrt pogoj za uspešno vpeljavo celovitega SUIV.

Rezultati posameznih aktivnosti in nalog znotraj vsake od petih faz planiranja SUIV so s standardom predpisani dokumenti. Izvedba aktivnosti in nalog znotraj projekta zahteva svoj čas, vire (ljudi, opremo, material) in finančna sredstva, zato mora biti dobronačrtovana.

Na sliki 1 je grafično prikazanih vseh pet faz načrtovanja vpeljave SUIV po standardu ISO/IEC 27003. Prikazani so tudi ključni dokumenti, ki so rezultat aktivnosti in nalog znotraj posamezne faze.



Slika 1: Faze načrtovanja SUIV po standardu ISO/IEC 27003 in pričakovani rezultati posameznih aktivnosti (vir: ISO/IEC 27003, 2010)

Standard ISO/IEC 27003 priporoča, kako naj si sledijo faze načrtovanja vpeljave SUIV in tudi, kateri naj bodo dokumenti (rezultati) posameznih faz. Ker so posamezne faze zelo obsežne, se je treba načrtovanja vpeljave SUIV lotiti projektno. Napotkov za izdelavo projektnega načrta v standardu ne bomo našli, zato je to prepuščeno uvajalcem.

3.1 Pridobitev soglasja vodstva za začetek projekta vpeljave SUIV

Sprejetje odločitve o vpeljavi SUIV v neko organizacijo je povsem brezpredmetno, če s tem ne seznanimo vodstva in ne pridobimo njegove podpore. Vodstvo je tisto, ki se mora zavedati pomembnosti zagotavljanja varnosti informacijskega sistema. Prav tako se mora vodstvo zavezati, da bo podpiralo vpeljavo SUIV v vseh fazah njegovega nastanka in kasneje vzdrževanja. Poleg seznanitve je ključno tudi razumevanje nujnosti vpeljave SUIV. Sam projekt vpeljave zahteva tudi finančni vložek, ki pa ga v večini primerov lahko odobri le vodstvo. Osnovni namen prve faze je torej seznanitev vodstva s projektom vpeljave SUIV in pridobitev soglasja za njegov zagon po mednarodnem standardu ISO/IEC 27001. V prvi fazi si ustvarimo

sliko proučevane organizacije, zato je pri zbiranju podatkov ključno dobro poznavanje okolja, v deluje katerem organizacija. Pomembno je tudi dobro poznavanje vseh ključnih procesov, ki se vsakodnevno odvijajo v organizaciji.

Ker vpeljava SUIV ni enostavna in zahteva ogromen angažma udeleženih, je prva faza projekta osnova za vse naslednje. Na podlagi vseh podatkov, zbranih v prvi fazi, znamo identificirati trenutne varnostne pomanjkljivosti in jih ustrezno predstaviti vodstvu. Preden se lotimo prve faze, je nujno, da v organizaciji poiščemo osebo, ki bo zmogla zbrati vse informacije, ki jih bomo potrebovali v celotnem procesu vpeljave SUIV. Ta oseba mora imeti tudi dovolj visoka pooblastila in moč, da jo bodo ljudje jemali resno in ji pomagali pri zbiranju informacij, ki so ključne za zagon projekta vpeljave SUIV (Law Society of South Africa, 2011).

Aktivnosti znotraj prve faze pri načrtovanju SUIV so:

- začetno načrtovanje in posnetek obstoječega stanja,
- določitev ciljev in prednostnih nalog za vpeljavo SUIV,
- definiranje obsega SUIV,
- definiranje poslovnega primera in projektnega načrta,
- pridobitev soglasja in zavezanosti vodstva za začetek vpeljave SUIV.

3.2 Definiranje obsega in meja SUIV ter politike SUIV

Ko je vodstvo organizacije odobrilo zagon projekta vpeljave SUIV, se lotimo definiranja obsega SUIV. Določiti obseg SUIV pomeni odločiti, kaj znotraj in zunaj organizacije bomo varovali ter česa ne bomo varovali. Vse tisto, kar bo izključeno iz obsega SUIV, opredelimo kot izključitve, ki ne bodo zajete v naš sistem varovanja. Vse morebitne izključitve mora organizacija dodatno utemeljiti in navesti razloge za takšno odločitev. S stališča varnosti bi bilo najbolje, če bi v obseg SUIV lahko zajeli celotno organizacijo, vendar to pogosto, zaradi kompleksnosti povezav med poslovnimi procesi, ni izvedljivo (Rakovec, 2005). Priporočljivo je, da obseg SUIV omejimo na poslovna področja, ki so najbolj kritična za poslovanje, in ga kasneje postopno širimo z vključevanjem še preostalih področij poslovanja. S tem, ko bodo obseg in meje SUIV natančno določeni, se bo za vsako informacijsko dobrino vedelo, ali je v SUIV vključena ali ne. Na podlagi določitve obsega in meja SUIV opredelimo tudi politiko SUIV z vidika značilnosti poslovanja, organizacije, njene lokacije ter sredstev in tehnologije.

Druga faza pri načrtovanju SUIV je torej sestavljena iz petih aktivnosti, ki si sledijo tako:

- definiranje obsega politike in meja obsega z vidika značilnosti in organizacije poslovanja,
- definiranje obsega politike in meja obsega z vidika informacijskokomunikacijske tehnologije,
- definiranje obsega politike in meja obsega z vidika fizičnih lokacij,
- definiranje obsega politike in meja obsega za celoten SUIV,
- izdelava politike SUIV in pridobitev soglasja vodstva.

3.3 Analiza zahtev v zvezi z informacijsko varnostjo

Izvedba analize zahtev s področja informacijske varnosti v organizaciji je pomembna faza, saj v njej popišemo vse dobrine informacijskega sistema in trenutno stanje informacijske varnosti znotraj definiranega obsega SUIV. Trenutno stanje primerjamo z želenim stanjem in izberemo ustrezne metode za doseganje želenega. Informacije, ki jih pridobimo v fazi analize varnosti informacijskega sistema, služijo kot:

- vir informacij o trenutnem stanju v organizaciji,
- vir informacij o pogojih vpeljave SUIV,
- vir prečiščenih informacij o vseh objektih v sklopu proučevane organizacije,
- vir informacij o posebnih okoliščinah, na katere moramo biti še posebej pozorni,
- vir informacij o želenemu nivoju varovanja informacij,
- zbir vseh informacij v okviru definiranega obsega, ki so potrebne za vpeljavo in se nanašajo na del organizacije ali pa na celo organizacijo.

Tretja faza planiranja SUIV ima tri glavne aktivnosti, ki jih je potrebno narediti za uspešno izpeljano analizo zahtev v zvezi z informacijsko varnostjo. Te aktivnosti so:

- definiranje informacijskovarnostnih zahtev za SUIV,
- definiranje dobrin znotraj obsega SUIV,
- primerjava obstoječega stanja s cilji organizacije na področju informacijske varnosti.

3.4 Ocena tveganja in oblikovanje predloga varovalnih ukrepov

V četrti fazi planiranja SUIV ocenimo, katera so najbolj kritična tveganja pri varovanju informacij. Poleg njihove identifikacije in določitve njihove stopnje ogrožanja dobrin, zanje predlagamo varovalne ukrepe. Kot pomoč nam bo v tej fazi služil mednarodni standard ISO/IEC 27005, ki zagotavlja smernice za obvladovanje tveganja pri varovanju informacij. Cilj te faze je torej določiti metodologijo, po kateri bomo ocenjevali tveganja, jih analizirali in določili varovalne ukrepe za njihovo omejitev. Aktivnosti v sklopu te faze so:

- izvedba ocene tveganja,
- določitev varovalnih ukrepov za obvladovanje tveganj,
- pridobitev soglasja vodstva za vpeljavo in izvajanje SUIV.

3.5 Oblikovanje končnega načrta vpeljave SUIV

Zadnja, peta faza je namenjena oblikovanju končnega načrta vpeljave SUIV. Na podlagi tega načrta bo v proučevani organizaciji zagnan projekt vpeljave SUIV kot del faze »stori« Demingovega kroga. Pri oblikovanju končnega načrta vpeljave SUIV je potrebno celotno informacijsko varnost obravnavati s treh vidikov (tako kot je bilo to narejeno v drugi fazi, ko je bil definiran obseg SUIV): z vidika značilnosti poslovanja, z vidika IKT in z vidika fizičnih lastnosti organizacije. Rezultat te faze je končni načrt vpeljave SUIV v organizacijo. Peta faza planiranja SUIV je sestavljena iz naslednjih aktivnosti:

- oblikovanje načrta varovanja informacij z vidika značilnosti poslovanja organizacije,
- oblikovanje načrta vpeljave varovalnih ukrepov z vidika fizične in logične (IKT) varnosti,
- vzpostavitev sistema za vzdrževanje in izobraževanje v zvezi z SUIV,
- izdelava končnega plana vpeljave SUIV.

Na podlagi faz in aktivnosti, ki so bile predstavljene v tem poglavju, lahko izdelamo projektni načrt za vpeljavo SUIV. Za izdelavo projektnega načrta lahko uporabimo različna računalniška orodja. V nadaljevanju je prikazana izdelava projektnega načrta s pomočjo dveh računalniških orodij, PROSIS in Microsoft Project.

4 Izdelava projektnega načrta za vpeljavo SUIV

Pri izdelavi načrta vpeljave SUIV je zaradi njegove kompleksnosti in obsežnosti ključnega pomena uporaba projektnega pristopa. Projekti, ki se jih dnevno lotevamo v organizacijah, so lahko precej obsežni in v današnjih časih neobvladljivi brez ustrezne informacijske in dokumentacijske podpore (Kern, Roblek, Urh in Kokalj, 2008). Za izdelavo projektnega načrta SUIV je priporočljivo uporabiti dve računalniški orodji, in sicer:

- računalniški projektni sistem PROSIS,
- računalniški program Microsoft Project.

Projektni sistem PROSIS je namenjen predvsem vodenju in obvladovanju kompletne projektne dokumentacije, ki nastaja med procesi inicializacije, koncipiranja, planiranja, izvajanja in zaključevanja projekta. PROSIS je plod razvoja podjetja Protal d.o.o., programersko pa ga podpira podjetje 3K-IT d.o.o. (Protal, 2011).

Programski paket Microsoft Project je namenjen učinkovitemu vodenju projektov. Izdeluje ga podjetje Microsoft, ki je leta 2010 izdalo aktualno verzijo programa Microsoft Project 2010. Program uporabljajo projektni vodje, ki z njim planirajo in spremljajo realizacijo projekta. Uporabljajo ga še za določitev aktivnosti in nalog znotraj projekta ter za določitev njihovega zaporedja in trajanja. Nalogam znotraj aktivnosti se dodeli vire in sredstva, da se lahko spremlja stroške in sprotno realizacijo.

Vsak projekt, ki ga začnemo v PROSIS-u, začne svojo pot kot pobuda, ki na podlagi odobritev odgovornih oseb, nadaljuje svojo pot po sistemu, vse do odobritve projektneganačrta, izvajanja in zaključevanja projekta. Vsaka faza projektnega sistema PROSIS omogoča ustrezno dodeljevanje virov in spremljanje njihovih aktivnosti, povezanih s projektom. PROSIS je močno povezan s programskim orodjem Microsoft Office, saj se v nekaterih aktivnostih dopolnjujeta. Zato Microsoft Project uporabimo takrat, ko projektnemu načrt določamo:

- zaporedje nalog znotraj aktivnosti (mrežni diagram),
- oceno trajanja nalog znotraj aktivnosti (gantogram),
- oceno rabe virov – dodelitev potrebnih virov (ljudje, oprema, material) na posamezno nalogo znotraj aktivnosti in razporeditev virov.

Na podlagi priporočil standarda ISO/IEC 27003 in uporabe računalniških orodij za projektno vodenje nastane načrt zaporedja aktivnosti vpeljave SUIV. Zaporedje aktivnosti najlažje določimo s programom Microsoft Project, kjer imamo več možnosti določanja zaporedja aktivnosti in nalog znotraj posamezne aktivnosti. Nekatere naloge se lahko izvajajo vzporedno, nekatere pa morajo biti zaporedne, ker so med seboj časovno odvisne. To pomeni, da se mora najprej končati prva naloga, šele nato se lahko prične izvajati naslednja. Standard ISO/IEC 27003 predlaga, katere so tiste naloge, ki morajo biti predhodno končane, da lahko začnemo z izvajanjem naslednje naloge, zato to tudi upoštevamo. Zaporedje faz, aktivnosti in nalog znotraj posamezne aktivnosti je smiselno prikazati kot hierarhično strukturo aktivnosti projekta (WBS). To pomeni, da projekt členimo od najvišjega nivoja, ki ga predstavljajo faze, in nižje do aktivnosti in posameznih nalog projekta. Hierarhična struktura faz, aktivnosti in nalog je prikazana na sliki 2. Poleg tega so na tej sliki prikazane zaporedne številke nalog, ki morajo biti končane pred izvajanjem naslednje naloge.

ID	Ime faze, aktivnosti	Predecessors
0	**SUIV_PO1**	
1	**1. FAZA: PRIDOBITEV SOGLASJA VODSTVA ZA ZAČETEK PROJEKTA VPELJAVE SUIV**	
2	**Začetno planiranje in posnetek obstoječega stanja**	
3	Določitev korporativnih poslovnih ciljev	
4	Določitev, analiziranje in razumevanje poslovnih procesov	3
5	Zbiranje ključnih podatkov o značilnostih poslovanja organizacije, njeni lokaciji, dobrinah in tehnologiji	4
6	**Določitev ciljev in prednostnih nalog za vpeljavo SUIV**	
7	Identifikacija potreb po informacijski varnosti in ciljev zved z SUIV	3,4,5
8	Zbiranje informacij o specifičnih zakonskih predpisih in industrijskih standardih, vezanih na informacijsko varnost	7
9	**Definiranje okvirnega obsega SUIV**	
10	Določitev okvirnega obsega SUIV	7,8
11	Določitev vlog in odgovornosti za okvirni obseg SUIV	10
12	**Definiranje poslovnega primera in projektnega načrta**	
13	Izdelava poslovnega primera	10;11;7
14	Izdelava predloga projektnega plana	10;11;7
15	**Pridobitev soglasja vodstva in zavezanost vodstva za začetek vpeljave SUIV**	
16	Predstavitev projekta vpeljave SUIV vodstvu in pridobitev soglasja	13;14
17	1. FAZA Zaključena	16
18	**2. FAZA: DEFINIRANJE OBSEGA, MEJA OBSEGA SUIV IN VARNOSTNE POLITIKE SUIV**	
19	**Definiranje obsega in meja obsega z vidika značilnosti in organizacije poslovanja**	
20	Določitev obsega SUIV z vidika značilnosti poslovanja	16;10;7
21	Določitev organizacijske strukture v proučevani organizaciji	20
22	Identifikacija informacij, ki se izmenjujejo znotraj in zunaj definiranega obsega	20;21
23	Identifikacija poslovnih procesov in odgovornosti za informacijsko-dobrine znotraj in zunaj definiranega obsega	20;22
24	**Definiranje obsega in meja obsega z vidika IKT**	
25	Določitev meja obsega za IKT v proučevani organizaciji	16;10;20;23
26	Identifikacija informacijskega sistema in mrežne infrastrukture znotraj in zunaj obsega	25
27	**Definiranje obsega in meja obsega z vidika fizičnih lokacij organizacije**	
28	Določitev fizičnega obsega in meja obsega	16;10;20;25
29	Pridobivanje informacij o fizični lokaciji in geografskih značilnostih organizacije	28
30	**Definiranje obsega in meja obsega za celoten SUIV**	
31	Določitev obsega in meja obsega za celoten SUIV	20;25;28;10
32	**Izdelava politike SUIV in pridobitev soglasja vodstva**	
33	Izdelava politike SUIV	31;7;13;14
34	Pridobitev soglasja vodstva za politiko SUIV	33
35	2. FAZA Zaključena	34
36	**3. FAZA: ANALIZA ZAHTEV V ZVEZI Z INFORMACIJSKO VARNOSTJO**	
37	**Definiranje informacijskih varnostnih zahtev za SUIV**	
38	Zbiranje informacij o ključnih procesih, organizacijski strukturi, lokaciji in IKT v organizaciji	7,8,31,33
39	Definiranje zahtev po informacijski varnosti v organizaciji z vidika zaupnost, celovitost in razpoložljivost	38
40	Definiranje zahtev po informacijski varnosti z vidika specifičnih zakonskih predpisov ter pogodbenih poslovnih zahtev	39
41	Zbiranje informacij o znanih varnostnih ranljivostih v organizaciji	38
42	**Definiranje dobrin znotraj obsega SUIV**	
43	Identifikacija ključnih procesov v organizaciji	31,33,38,41
44	Identifikacija glavnih dobrin znotraj ključnih procesov	43
45	Klasifikacija glavnih dobrin znotraj ključnih procesov	44
46	**Primerjava obstoječega stanja s cilji organizacije na področju informacijske varnosti**	
47	Identifikacija stanja informacijske varnosti in obstoječih varnostnih kontrol v organizaciji	31,33,38,43,45
48	Dokumentiranje ocenjenih varnostnih pomanjkljivosti v organizaciji	47
49	3.FAZA Zaključena	48
50	**4. FAZA: OCENA TVEGANJA IN OBLIKOVANJE PREDLOGA VAROVALNIH UKREPOV**	
51	**Izvedba ocene tveganja**	
52	Izbira metode za izvedbo ocene tveganja	47
53	Izvedba ocene tveganja in dokumentiranje rezultatov	52
54	**Določitev varovalnih ukrepov za obvladovanje tveganj**	
55	Izbira varovalnih ukrepov za ocenjena tveganja	53
56	Izdelava načrta za obvladovanje tveganj	55
57	**Pridobitev soglasja vodstva za vpeljavo in izvajanje SUIV**	
58	Pridobitev podlastila vodstva za vpeljavo in izvajanje SUIV	13,14;31,33;53;55
59	Pridobitev soglasja vodstva za predlagana področja tveganja	58
60	Priprava izjave o uporabnosti SOA	59
61	4. FAZA Zaključena	60
62	**5. FAZA: OBLIKOVANJE KONČNEGA PLANA VPELJAVE SUIV**	
63	**Oblikovanje načrta varovanja informacij z vidika značilnosti poslovanja organizacije**	
64	Oblikovanje končne organizacijske strukture za varovanje informacij	11,31,33,38,44,53,55,58
65	Določitev načinov za dokumentiranje vzvezi z SUIV	31,33,58,64
66	Oblikovanje informacijske varnostne politike	7,13,14,31,33,39,44,53,64,65
67	Oblikovanje internih standardov in postopkov za delo v zvezi z informacijsko varnostjo	31,33,53,55,58,64,65,66
68	**Oblikovanje načrta vpeljave varovalnih ukrepov z vidika fizične in logične (IKT) varnosti**	
69	Določitev in dokumentiranje postopkov za vpeljavo izbranih varovalnih ukrepov	31,33,39,44,53,55,59
70	**Vzpostavitev sistema za vzdrževanje in izobraževanje v zvezi z SUIV**	
71	Oblikovanje načrta vodstvenih pregledov SUIV	31,33,58,66
72	Vzpostavitev programa za ozaveščanje, usposabljanje in izobraževanje s področja izvajanja SUIV	31,33,39,55,58,66,67
73	**Izdelava končnega plana vpeljave SUIV**	
74	Priprava končnega plana vpeljave SUIV	31,33,64,65,66,67,69,71,72
75	5. FAZA Zaključena	74

Slika 2: Zaporedje aktivnosti in nalog petih faz načrtovanja vpeljave SUIV z zahtevanimi predhodnimi nalogami (vir: lasten)

Sledi določitev trajanja posamezne aktivnosti. Vsaka aktivnost je sestavljena iz več nalog. Za vsako nalogo znotraj posamezne aktivnosti določimo, koliko časa bo trajala, kar navadno ocenimo na podlagi kompleksnosti posamezne naloge, na podlagi okvirne ocene razpoložljivosti virov, ki bodo dodeljeni posamezni nalogi, ali pa na podlagi preteklih izkušenj. Trajanje posamezne naloge lahko izrazimo z različnimi časovnimi enotami (ura, dan, teden itn.). Na podlagi vnesenih časov za naloge, program Microsoft Project oceni trajanje posamezne aktivnosti in faze, kakor tudi trajanje celotnega projekta vpeljave SUIV.

Naslednji korak je dodelitev virov za posamezne naloge znotraj planiranih aktivnosti. Organizacije se same odločijo, katere ljudi bodo angažirale pri teh naloga in v kolikšni meri. Tiste organizacije, ki zagotavljajo interno informacijsko podporo svojim poslovnim procesom, bodo k nalogam projekta dodelili več svojih zaposlenih. Organizacije, ki nimajo toliko internega znanja, pa bodo k nalogam povabile več zunanjih strokovnjakov. Tudi za planiranje virov lahko uporabimo program Microsoft Project.

Dodelitvi virov sledijo še ocene stroškov za posamezen vir. Stroške dela ljudi, ki opravljajo naloge znotraj posameznih aktivnosti, običajno določimo na podlagi urne postavke za posameznika. Določimo še ostale stroške opreme in materiala. Tako dobimo še stroškovno oceno celotnega projekta.

Rezultat je projektni načrt, ki ga mora pred izvedbo potrditi najvišje vodstvo v organizaciji. Po potrditvi gre projektni načrt v fazo izvedbe, ko se realizirajo vse načrtovane aktivnosti.

5 Zaključek

Vsak poslovni proces v organizacijah je tako ali drugače informacijsko podprt. To je zadosten razlog, da moramo poskrbeti tudi za ustrezno varnost informacijskega sistema, ki jo zagotovimo s pravilno vpeljanim in vzdrževanim sistem za upravljanje informacijske varnosti – SUIV. Poglavitno vprašanje, ki se ob tem zastavlja je, kako se lotiti planiranja vpeljave SUIV. Na to vprašanje smo poskušali odgovoriti v pričujočem prispevku.

V ta namen smo predstavili SUIV po standardu ISO/IEC 27001. Zaradi kompleksnosti planiranja SUIV, smo prikazali model načrtovanja vpeljave SUIV po navodilih standarda ISO/IEC 27003 v kombinaciji z dvema računalniškima orodjema. V prispevku je predstavljena vsaka izmed petih faz načrtovanja vpeljave

SUIV. Za izdelavo projektnega plana smo uporabili dve računalniški orodji, in sicer projektni sistem PROSIS ter program Microsoft Project. Rezultat je projektninačrt, ki je razdeljen na pet povezanih faz s po več aktivnostmi. Prikazani projektni načrt je mogoče preslikati na katero koli organizacijo, saj so prikazane faze in aktivnosti univerzalne. Organizacije se same odločijo, koliko virov in časa bodo namenile za aktivnosti v posamezni fazi v sklopu projekta vpeljave SUIV.

Z vpeljavo SUIV se v organizaciji vzpostavi celovit in kontinuiran proces, ki ga je potrebno stalno preverjati in izboljševati. Na ta način je zagotovljen ustrezen nivo informacijske varnosti, ki si ga želi vsaka organizacija v današnjem poslovnem okolju.

Viri

- ISO 27001: Sistem vodenja varovanja informacij. (15.8.2012). Bureau Veritas Slovenija. Pridobljeno 15.8.2012 na http://www.bureauveritas.si/wps/wcm/connect/bv_si/Local/Home/bv_com_serviceSheetDetails?serviceSheetId=13799&serviceSheetName=ISO+27001
- Brezavšček, A. in Moškon, S. (2009).Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. Nova vizija tehnologij prihodnosti. Pridobljeno 14.8.2012 na http://www.vris.si/default.asp?page_id=01KXBOKDZ501HE6KD7HO04
- BS ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements. (2005). London: British Standards Institution.
- Calder, A. in Watkins, S. (2008). A Manager's Guide to Data Security and ISO 27001/ ISO 27002 – 4th Edition. London: Kogan Page Ltd.
- ISO/IEC 27003:2010 Information Technology — Security Techniques — Information Security Management System Implementation Guidance. (2010).Ženeva:ISO copyright office.
- Kern, T., Roblek, M., Urh, B. in Kokalj, Š. (2008). Sistem za podporo vodenja in upravljanja projektov, Zbornik prispevkov 1. strokovnega posveta, »Informatika v sodobni družbi« (str. 51 – 59). Novo mesto: Univerzitetno in raziskovalno središče Novo mesto.
- Protal. (2011). Opis projektnega sistema Prosis. Pridobljeno 10.8.2012 na http://www.protal.si/index-2.html
- Rakovec, S. (2005).Varovanje informacij skladno s standardom BS 7799. Pridobljeno 11. 8. 2012 na http://www.cek.ef.uni-lj.si/magister/rakovec543.pdf
- Law society of South Africa. (2011). Information Security for South African Law Firms – LSSA Guidelines. Pridobljeno 15.8.2012 na http://www.lssa.org.za/upload/Information%20Security%20Guideline%202011%20v1_0%20110517.pdf

O avtorjih

Klemen Vehar je diplomirani organizator–menedžer in je zaposlen kot vodja informatike v podjetju Alpina, d.o.o., Žiri.

Alenka Brezavšček je zaposlena na Fakulteti za organizacijske vede Univerze v Mariboru. Dela kot visokošolska učiteljica UNI, docentka. Njeno znanstveno raziskovalno in pedagoško delo zajema področja statistike, stohastičnih procesov, zanesljivosti in razpoložljivosti sistemov ter varnosti informacijskih sistemov.

Tomaž Kern je doktor znanosti s področja organizacijskih ved, magister informatike in inženir strojništva. Je redni profesor na Fakulteti za organizacijske vede in pokriva področje poslovnih procesov in projektnega menedžmenta. Je prorektor za področje informatike na Univerzi v Mariboru, član senata Fakultete in član senata Univerze v Mariboru. Je predstojnik Laboratorija za projektni in procesni menedžment na Fakulteti za organizacijske vede. Vodi skupino raziskovalcev in deluje kot strokovnjak na področju poslovnih procesov in projektnega menedžmenta. Kot vodja ali sodelavec je uspešno zaključil več deset projektov v različnih slovenskih podjetjih in ustanovah ter v tujini. Je ustanovni član PMI Slovenija Ljubljana. Njegov bibliografski opus obsega več kot 340 znanstvenih in strokovnih prispevkov in člankov.

Revidiranje sistemov upravljanja varovanja informacij

Mladen Terčelj, Boštjan Delak

Varovanje informacij postaja eno od najpomembnejših poslovnih vprašanj, s katerimi se danes ukvarjajo organizacije. Zaskrbljenost glede varstva zasebnosti posameznika, občutljivih osebnih podatkov, občutljivih poslovnih podatkov, verodostojnosti in celovitosti poslovnih podatkov itn. zahteva uveljavitev novih zakonov in predpisov, ki bodo zagotovili, da bodo organizacije ustrezno obravnavale varnost lastnih podatkov in podatkov, ki so jim zaupani v upravljanje. Vse več je standardov in metodologij, ki opredeljujejo posamezne usmeritve in postopke za upravljanje in kontrolo področja varovanja informacij. Prispevek se osredotoča na to, da nam tudi standardi iz skupine ISO/IEC 27K, predvsem ISO/IEC 27007:2011 in ISO/IEC 27006:2007, lahko olajšajo pripravo in zlasti izvedbo revizije sistema upravljanja varovanja informacij (SUVI) tako, da se ohranjajo načela revidiranja. Po drugi strani pa je ISACA nadgradila tudi celovit pristop COBIT 5 s profesionalnim vodičem COBIT 5 for Information Security, ki je, tako kot standard ISO/IEC 27007:2011, tudi sodilo za revidiranje varovanja informacij in s tem SUVI.

KLJUČNE BESEDE: ISO/IEC 27007:20011, ISO/IEC 27006:2007, COBIT 5, revizija varovanja informacij

1 Uvod

Varovanje informacij postaja eno od najbolj pomembnih poslovnih vprašanj, s katerimi se danes srečujejo podjetja. Zaskrbljenost glede varstva zasebnosti posameznika, občutljivih osebnih podatkov, občutljivih poslovnih podatkov, verodostojnosti in celovitosti poslovnih podatkov itn. zahteva uveljavitev novih zakonov in predpisov, ki bodo zagotovili, da bodo podjetja ustrezno obravnavala varovanje lastnih podatkov in podatkov, ki so jim zaupani v upravljanje (Axelord, Bayuk in Schutzer, 2009). Obstaja več virov obveznosti za izpolnitev varnostnih zahtev: zakoni in podzakonski akti, skupne pravne obveznosti, pravila o dokazovanju, industrijski standardi, pogodbene obveznosti ter ne nazadnje dobre prakse.

V prvem delu prispevek predstavlja novosti, povezane z novim standardom ISO/IEC 27007:2011 – Informacijska tehnologija – Tehnike varovanja – Smernice za revizijo sistema upravljanja varovanja informacij (SUVI). Kot že samo ime pove, ta standard opisuje usmeritve za revizijo SUVI, kot ga za organizacije, ki imajo ta sistem certificiran, opredeljujejo zahteve po standardu ISO/IEC 27001:2005. V drugem delu prispevek opisuje ISO/IEC 27006:2007 – Informacijska tehnologija – Tehnike varovanja – Zahteve za organe, ki izvajajo presoje in postopke certificiranja SUVI. V tretjem delu pa sledi opis načrtovanja in pregleda sistema SUVI v omejenem obsegu, s pomočjo standarda ISO/IEC 27007:20011 v slovenskem podjetju, ki že ima certificiran SUVI po standardu ISO/IEC 27001:2005. Prispevek v četrtem delu na kratko predstavi novi COBIT 5 celovit pristop in še posebej področje COBIT 5 – Varovanje informacij. Na koncu je seznam nasvetov in usmeritev pri načrtovanju in izvedbi revizije SUVI po standardu ISO/IEC 27007:2011 za potencialne uporabnike v primeru notranje revizije in za izvajalce zunanje revizije.

Avtorja tega prispevka imata več deset let izkušenj v IS in večletne izkušnje s SUVI. Z novim standardom ISO/IEC 27007:2011 sta se spoznala teoretično. Njuna hipoteza je, da lahko standard ISO/IEC 27007:2011 ter druge ISO standarde učinkovito uporabimo pri reviziji SUVI v slovenskem prostoru.

2 Kratek pregled standardov

V prispevku so navedeni nekateri standardi po ISO/IEC[12]. V nadaljevanju je kratek pregled teh standardov.

#	Standard	Namen standarda
1	ISO/IEC 17021:2011	Standard vsebuje načela in zahteve za usposobljenost, doslednost in nepristranskost revizije in certificiranja organov, ki te dejavnosti opravljajo za sisteme vodenja vseh vrst.
2	ISO/IEC 19011:2011	Standard vsebuje napotke za revidiranje sistemov upravljanja, vključno s principi revidiranja, upravljanja revizijskega programa in izvedbo revizije sistemov upravljanja, kot tudi navodila za ocenjevanje usposobljenosti vseh, ki so vključeni v proces revidiranja.

[12] ISO/IEC – International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee.

3	ISO/IEC 27000:2009	Standard daje pregled in uvod v celotno družino ISO/IEC 27K standardov s področja SUVI. Standard vsebuje slovar temeljnih pojmov in definicij, ki se uporabljajo v vsej družini ISO/IEC 27K standardov.
4	ISO/IEC 27001:2005	Standard opredeljuje zahteve za vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema za upravljanje varovanja informacij (SUVI) v različnih organizacijah (npr. gospodarskih, vladnih, neprofitnih itn.).
5	ISO/IEC 27005:2011	Standard je podpora splošnim pojmom, opredeljenim v standardu ISO/IEC 27001:2005 in je namenjen pomoči za zadovoljivo izvajanje varovanja informacij, ki temelji na metodi upravljanja s tveganji.
6	ISO/IEC 27006:2007	Standard določa zahteve in daje navodila za akreditacijske in certifikacijske organe, ki izvajajo presojo in certifikacijo SUVI.
7	ISO/IEC 27007:2011	Standard vsebuje napotke za vodenje revizijskega programa SUVI, o izvedbi revizije, ter o usposobljenosti revizorjev za SUVI, poleg navodil, ki so vsebovana v ISO 19011.

Preglednica 1: Standardi ISO/IEC

Za to področje je objavljenih bolj malo znanstvenih prispevkov. Ma in Pearson (2005) sta ugotovila, da niso bile izvedene empirične raziskave za področje standarda varovanja informacij. Tashi in Ghernaouti-Hellie (2007) pa sta v svojem prispevku bolj predstavila varovanje informacij, pripadajoči standard ISO/IEC 27001:2005 ter povezavo na COBIT[13]. Standard ISO/IEC 2700/:2011 je dokaj nov in o njem še ni bilo objavljenih znanstvenih in raziskovalnih prispevkov.

3 ISO/IEC 27007:2011

3.1 Namen standarda

Standard ISO/IEC 27007:2011 (ISO/IEC, 2011) podaja smernice upravljanja in izvajanja revizijskega pregleda pri organizacijah, ki zagotavljajo skladnost z določili standarda ali pa že imajo certificiran SUVI po standardu ISO/IEC 27001:2005 (ISO/IEC, 2005). Hkrati standard podaja smernice za ustrezno kompetentnost in vrednotenje revizorjev v tesni povezavi s smernicami za revidiranje sistemov vodenja, ki so zapisane v standardu ISO 19011:2011 (SIST, 2011).

[13] COBIT – Control Objectives for Information and Related Technologies (Kontrolni cilji za informacijsko in sorodno tehnologijo).

Standard ISO/IEC 27007:2011 poleg sedmih poglavij vsebuje še prilogo – Praktične smernice za izvedbo revizije SUVI po zahtevah standarda ISO/IEC 27001:2005, vendar brez kontrol iz aneksa A tega standarda. Prva tri poglavja so namenjena obsegu, referencam na druge standarde ISO skupine ter definicijam. Pri tem se navedeni standard v celoti sklicuje na izraze in definicije, kot kot so zapisani v standardih ISO 19011:2011 in ISO/IEC 27000:2009. Naslednje poglavje pa konkretneje opredeljuje upravljanje s programom revizije. Poleg opredelitev, ki jih za to področje navaja standard ISO 19011:2011, določa, da mora biti program revidiranja SUVI izdelan na osnovi informacijskih tveganj revidirane organizacije.

3.2 Cilji standarda

Standard ISO/IEC 27007:2011 opredeljuje načela revidiranja, ki jih prav tako povzema po standardu ISO 19011:2011. Ta načela so integriteta revizorjev, spremljanje zakonskih zahtev, pazljivo podajanje sodb ob ugotovitvah pri reviziji, še posebno glede na vpliv, ki bi jih te imele pri njihovi implementaciji v revidirani organizaciji, obveznost razumljivega in sprotnega poročanja, poklicna skrbnost pri revidiranju samem, zaupnost oz. varovanje informacij, neodvisnost pri podajanju sklepov revizije in podajanje zaključkov na osnovi evidenc. Cilji revidiranja po standardu ISO/IEC 27007:2011 so zagotavljanje učinkovite izvedbe programa revidiranja. Cilji so odvisni od opredeljenih varnostnih zahtev revidirane organizacije, zahtev standarda ISO/IEC 27001:2005, nivoja izvajanje ukrepov varovanja informacij, ki se odražajo v varnostnih dogodkih, za katere ukrepi varovanja niso bili zadostni, v pojavnosti varnostnih incidentov ter s tem izkazane neučinkovitosti implementiranih ukrepov.

3.3 Opis postopka revizije

Postopek izvedbe revizije se, upoštevajoč določila standarda ISO/IEC 27007:2011, deli na dva osnovna koraka: na pripravo programa revizije in na izvedbo revizije.

3.3.1 Priprava programa revizije

Pri pripravi programa revizije je potrebno upoštevati kompetence, znanja in izkušnje izvajalcev. Vsekakor naj pri pripravi programa ne bi zanemarili možnosti razširitve obsega revizije, ki pa naj sloni na številu revidirancev po posamezni lokaciji, številu informacijskih sistemov, številu lokacij, njegovi odvisnosti od

kompleksnosti sistemov, kritičnosti procesov in pomembnosti informacij ter informacijskih sredstev, ki jih obsega SUVI. V programu je potrebno opredeliti še vire, potrebne za izvedbo revizije. Pri opredelitvi programa revizije mora vodja revizije uskladiti program z revidirano organizacijo ter članom revizijske skupine dodeliti obseg, cilje in predvsem kriterije za revizijo, ki jo bodo ti izvajali posamično. Vodja revizije naj izbere člane revizijske skupine, v kateri naj ne bi manjkali tudi tehnični strokovnjaki za posamezna področja. Vodja naj za revizijsko skupino opredeli metodo, po kateri bodo izvajali revizijo.

3.3.2 Izvedba revizije

Pri izvedbi revizije naj revizorji še pred njenim začetkom na lokaciji revidirane organizacije zberejo in pregledajo dokumentacijo SUVI, ki je relevantna za revidiranje v obsegu, kot je določen v programu revizije. Predhoden pregled dokumentacije vsekakor vpliva na pripravo delovnega gradiva revizorjev in na vodenje intervjujev.

Na uvodnem sestanku revizorji vzpostavijo kontakt s predstavniki revidirane organizacije. Poleg obojestranske osebne predstavitve, načina izvedbe in ciljev revizije naj še najmanj enkrat potrdijo že dogovorjen program revizije z vsemi udeleženci revidirane organizacije. Revizorji izvajajo revizijo z intervjuji, opažanjem v poslovnem okolju, pregledom in po potrebi z zbiranjem dokumentacije, predvsem zapisov, ki dokazujejo pravilnost oz. zapisano izvajanje ukrepov varovanja informacij. Revizorji naj ob morebitni ugotovitvi odstopanja od zakonskih določil, določil standarda varovanja informacij ali odstopanja od določil internih predpisov varovanja informacij vsakemu predstavniku revidirane organizacije takoj sporočijo svoje ugotovitve. Ob zaključku izvedbe revizije naj revizorji na zaključnem sestanku vsem sogovornikom, obvezno pa predstavnikom revidirane organizacije, navedejo vse ugotovitve ter nadaljnje postopke revidirane organizacije po prejemu vmesnega in končnega poročila o reviziji.

Kot praktičen primer revidiranja SUVI z uporabo standarda ISO/IEC 27007:2011 povzemava osnovne smernice za revidiranje, objavljene v petem poglavju – Odgovornost vodstva po standardu ISO/IEC 27001:2005.

Poleg določil v navedenem poglavju si revizorji pri zbiranju dokazil lahko pomagajo še s posameznimi specifičnimi določili standardov ISO/IEC 27005:2011 (SIST; 2011b), ISO/IEC 27006:2007 (ISO/IEC, 2007), ISO/IEC 17021:2011 (SIST; 2011a) in prilogo A standarda ISO/IEC 27001:2005.

Revizorji naj pri pregledu tega poglavja vključijo dokumente krovne varnostne politike, načrtovanje in zapise o obravnavanju zmanjšanja informacijskih tveganj, izobraževanja, internih presoj ter sklepe vodstva za navedena področja. Vključijo naj dokumente, ki opredeljujejo odgovornost posameznikov za informacijska sredstva ter dokumente, ki opredeljujejo vloge in odgovornosti posameznikov za izvajanje ukrepov varovanja informacij. Pregledajo naj poročila o analizah informacijskih tveganj in internih presojah. Opravijo naj tudi intervju z vodstvom organizacije, pooblaščencem za varovanje informacij in predstavnikom morebitnega varnostnega foruma v organizaciji. Pri pregledu naj ne pozabijo na pregled kompetenc posameznikov ter pri tem odločijo, katere dodatne kompetence naj bi imel posameznik za področje varovanja informacij in kako naj bi jih, z dodatnim izobraževanjem, dosegel.

4 ISO/IEC 27006:2007

Standard ISO/IEC 27006:2007 opredeljuje zahteve za organe, ki izvajajo presoje in postopke certificiranja SUVI po standardu ISO/IEC 27001:2005. Sestava tega standarda je podobna standardu ISO/IEC 27007:2011, vendar se pri opredelitvi osnovnih določil ta standard ne povezuje s standardom ISO 19011:2011, temveč s standardom ISO/IEC 17021:2011. Poleg vsebinsko podobnih določil s standardom ISO/IEC 27007:2011 pa ima ISO/IEC 27006:2007 priloge, ki jih prvi navedeni standard ne vsebuje. To sta na primer tabela, s katero se opravi analiza kompleksnosti in poslovne specifičnosti revidirane organizacije ter tabela za izračun časa, ki je potreben za izvedbo revizije. Standardu je dodana priloga smernic za pregled implementiranosti kontrol, ki so opredeljene v prilogi A standarda ISO/IEC 27001:2005. Te smernice za posamezne kontrole, zapisane v preglednici, opredeljujejo tip kontrole (organizacijska ali tehnična), nujnost ali le pogojno potrebo po računalniškem testiranju posamezne tehnične kontrole ter kratek opis postopka, ki naj ga izvede revizor ali s strani revizorja določeni izvedenec za pridobitev dokazil o implementiranem ukrepu za izpolnitev pogoja kontrole.

4.1 Sinergija med ISO/IEC 27007:2011 in ISO/IEC 27006:2007

Pri revidiranju SUVI zasledimo sinergijo ISO standardov, saj se z uporabo vseh določil standardov ISO/IEC 27007:2011 in ISO/IEC 27006:2009 ter ob dodatni, vendar omejeni uporabi določil drugih standardov skupine 27K, lahko v celoti

izvede revizija SUVI, postavljena po določilih standarda ISO/IEC 27001:2005 v različnih podjetjih in ustanovah v Sloveniji. Upoštevajoč določila obeh obravnavanih standardov, ISO/IEC 27007:2011 in ISO/IEC 27006:2007, ter dosledno uporabljajoč smernice iz prilog teh dveh standardov, revizorji lahko v celoti izvedejo revizijo SUVI, vzpostavljeno po standardu ISO/IEC 27001:2005.

5 COBIT

ISACA[14] je v sodelovanju z IT Governance Institute (ITGI) v zadnjih desetletjih razvijala COBIT. Razvijali in nadgrajevali so metodologijo in okvir za upravljanje in obvladovanje IT. Slovenski inštitut za revizijo je v sodelovanju z ISACA leta 2007 prevedel takratno verzijo COBIT 4.1 tudi v slovenski jezik[15].

V zadnjih nekaj letih so vzporedno s COBIT metodologijo razvili tudi komplementarna ogrodja za obvladovanje stroškov (ValIT) in tveganj (Risk IT). Zaradi vse večjega spoznanja, da organizacije varovanje informacij izvajajo v izolaciji od drugih procesov (ISACA, 2009), so v sodelovanju z univerzo v Južni Karolini (ZDA) – Marshall School of Business Institute for Critical Information Infrastructure Protection – razvili Business Model of Information Security (BMIS).

Metodologije in okviri, ki so nastajali vzporedno s COBIT, so zapolnjevali vrzeli različnih področij, kot so stroški, tveganja in varovanja informacij. Vendar so to samostojne celote, ki niso direktno povezane s COBIT. ISACA je v sodelovanju z ITGI nadgradila obstoječo metodologijo COBIT 4.1 z namenom vzpostavitve celovitega pristopa – okvirja (»framework«) obvladovanja IT v organizaciji (»Governance of Enterprise IT« (GEIT)) – COBIT 5.

5.1 COBIT 5

Cilji COBIT 5 so uspešno obvladovanje in upravljanje IT v organizaciji (ISACA, 2012). COBIT 5 temelji na družini produktov (preglednica 2), od katerih so nekateri že objavljeni, drugi pa so v razvoju in pripravi.

[14] ISACA – Information System Audit and Control Association.

[15] www.si-revizija.si

Področje	Naslov	Status
COBIT 5	COBIT 5 (Framework)	objavljen
COBIT 5 vodiči, ki omogočajo	COBIT 5 Enabling Processes	objavljen
	COBIT 5 Enabling Information	v razvoju
	ostali pomožni vodiči	www.isaca.org/cobit
COBIT 5 profesionalni vodiči	COBIT 5 Implementation	objavljen
	COBIT 5 for Information Security	objavljen
	COBIT 5 for Assurance	v razvoju
	COBIT 5 for Risk	v razvoju
	ostali profesionalni vodiči	www.isaca.org/cobit
COBIT 5 spletno okolje	COBIT 5 online collaborative environment	v razvoju

Preglednica 2: COBIT 5

COBIT 5 temelji na petih principih:

- ugoditi zahtevam deležnikov,
- pokrivati organizacijo od začetka do konca,
- uporabiti enoten celovit pristop,
- omogočati celovit pristop,
- ločiti obvladovanje od upravljanja.

Izvajalci so dejavniki, ki samostojno ali skupaj vplivajo tako, da bo nekaj delovalo – v primeru COBIT 5 je to obvladovanje in upravljanje IT. Izvajalci so:

- načela, politike in celoviti pristopi,
- procesi,
- organizacijska struktura,
- kultura, etika in vedenje,
- informacije,
- storitve, infrastruktura in aplikacije,
- ljudje, veščine in sposobnosti.

COBIT 5 poudarja ključna področja obvladovanja in upravljanja s poudarkom na procesih:

- Obvladovanje (voditi, ocenjevati, spremljati) s petimi procesi,
- Upravljanje (z 32 procesi), ki so razdeljeni na:
- načrtovati (APO – Align, Plan and Organize),
- graditi (BAI – Build, Acquire and Implement),
- izvajati (DSS – Deliver, Service and Support),
- spremljati (MEA – Monitor, Evaluate and Assess).

5.2 COBIT 5 – Varovanje informacij

Eden izmed profesionalnih vodičev iz družine produktov COBIT 5 je tudi COBIT 5 for Information Security. ISACA opredeljuje varovanje informacij (ISACA, 2012a) kot:

- »Zagotavljanje, da so informacije znotraj organizacije zaščitene pred:
  - razkritjem nepooblaščenih uporabnikov (zaupnost),
  - nepravilnimi spremembami (celovitost) in
  - nedostopnostjo, ko to zahtevamo (razpoložljivost).«

COBIT 5 for Information Security temelji na istih principih kot COBIT 5 celoviti pristop (ISACA, 2012a). Dokument je sestavljen iz treh delov. V prvem delu opisuje, kaj je to varovanje informacij in kako se COBIT 5 arhitektura prilagaja zahtevam varovanja informacij. Drugi del opisuje, kako se sedem izvajalcev COBIT 5 uporablja za vzpostavitev varovanja informacij. Tretji del opisuje, kako prilagodimo COBIT 5 for Information Security v okolje organizacije. Dokument ima tudi osem prilog, prvih sedem je namenjeno podrobnim smernicam za posamezne skupine COBIT 5 izvajalcev. Zadnja, osma priloga, podrobno opisuje preslikavo COBIT 5 for Information Security na nekatere preostale standarde varovanja informacij: ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISF[16] in NIST[17]. V COBIT 5 for Information Security (priloga osem) so posamezni COBIT 5

[16] ISF (Information Security Forum) – document ISF 2011 Standard of Good Practice for Information Security.

[17] NIST (National Institute for Information Security) document – NIST Guide for Assessing the Information Security Controls in Federal Information Systems and Organization – Special Publication 800-53A Revision 1.

procesi v obsežni preglednici povezani s posameznimi poglavji standarda ISO/IEC 27001:2005 ter tudi posameznimi kontrolami iz kontrolnega seznama priloge A standarda ISO/IEC 27001:2005.

6 Primer iz prakse

Kot praktičen primer pri revidiranja SUVI z uporabo standarda ISO/IEC 27007:2011 povzemava del revizijskega pregleda, v katerem sva uporabila osnovne smernice tega standarda za revidiranje poglavja 5 – Odgovornost vodstva po standardu, kot je v SUVI opredeljeno po standardu ISO/IEC 27001:2005.

Poleg določil v navedenem poglavju sva si pri zbiranju dokazil pomagala še s posameznimi specifičnimi določili standardov ISO/IEC 27005:2011, ISO/IEC 27006:2007, ISO/IEC 17021:2011 in prilogo A standarda ISO/IEC 27001:2005 ter pridobljeno Izjavo o primernosti – SOA.

Program revizije je bil usklajen, tako po obsegu kot vsebini oziroma revidiranih področjih med vodjo revizije in pooblaščencem za sisteme vodenja v organizaciji. Poleg navedenega je program revizije vseboval še časovne okvire za posamezna področja, dodeljen obseg za posameznega revizorja, ki naj bi nekatera področja revidiral samostojno, ter sogovornike s strani revidirane organizacije. Glede na poskusno revidiranje po novem standardu niso bili izbrani tehnični strokovnjaki za posamezna področja, kot to določajo smernice standarda.

Pred pričetkom revizije sva sledila smernicam, da naj revizorji, še preden začnejo revizijo na lokaciji revidirane organizacije, zberejo in pregledajo dokumentacijo SUVI, ki je relevantna za revidiranje v obsegu, kot je določen v programu revizije. Predhoden pregled dokumentacije vsekakor vpliva na pripravo delovnega gradiva revizorjev in na vodenje intervjujev.

Tako sva pridobila ter pregledala nekaj osnovnih dokumentov SUVI, in sicer »Poslovnik vodenja« za integriran sistem kakovosti in varovanja informacij, »Krovno varnostno politiko« in »Izjavo o primernosti – SOA[18]«.

Na uvodnem sestanku sva vzpostavila kontakt s predstavniki revidirane organizacije. Na njem smo, poleg obojestranske osebne predstavitve revizorjev in revidirancev, opredelili način izvedbe (vzorčenje) in cilje revizije ter znova potrdili že dogovorjen program revizije.

[18] SOA – Statement of Applicability.

Revizijo sva izvajala z intervjuji, opažanjem v poslovnem okolju, s pregledom in po potrebi z zbiranjem dokumentacije, predvsem zapisov, ki dokazujejo pravilnost oziroma zapisano izvajanje ukrepov varovanja informacij, kot so opredeljeni v internih predpisih organizacije in zbrani v Izjavi o primernosti – SOA. Posebej sva za zahtevo *5.1 – Zavezanost vodstva v SUVI vodila i*ntervjuje z vodstvom organizacije ter pregledala naslednjo dokumentacijo: sklep vodstva za SUVI; sklep o sprejetih ukrepih za zmanjšanje informacijskih tveganj; sklep o zadolžitvi pooblaščenih oseb za področje upravljanja varovanja informacij; zapisnike vodstva, v katerih je to obravnavalo področje varovanja informacij; sklep vodstvenega pregleda o nivoju sprejemljivih informacijskih tveganjih ter sklep vodstva o izvajanju ter rezultatih notranjih presoj SUVI. Za zahtevo *5.2. – Upravljanje sredstev v SUVI sva prav tako vodila intervjuje in pregledala dokumentacijo o stanju preventivnih in korektivnih ukrepov, ki so bili zapisani ob notranji ali zunanji presoji SUVI, opis delovnih mest glede na to, katere kompetence so potrebne za izvajanje posameznega opravil*a, ki kakor koli vplivajo na varovanje informacij, ter pregledala načrt in izvedbo izobraževanja za posameznika v organizaciji.

Ob vodenju intervjujev in pregledu dokumentacije sva vsakemu sogovorniku revidirane organizacije, ob morebitni ugotovitvi odstopanja od določil internih predpisov varovanja informacij ali v smislu izboljšanja prepisa, takoj sporočila svoje ugotovitve. V času revizije sva opravila še intervjuja s predstavnikoma vodstva za sisteme vodenja in varovanja informacij.

V času revizije nisva ugotovila odstopanj niti od zakonskih določb niti od internih predpisov, ki so osnova za izvajanje ukrepov zmanjšanja tveganj pri varovanju informacij.

Ob zaključku sva na zaključnem sestanku vsem sogovornikom navedla vse predloge, ki bi, ob dopolnitvi internih predpisov varovanja informacij, lahko izboljšali delovanje SUVI.

7 Razprava

Praktična izvedba revizije SUVI je pokazala, da revizor IS oziroma preizkušen revizor IS nima večjih težav pri načrtovanju in izvedbi revizije po novem standardu. Tako kot pri vsaki drugi reviziji se je potrebno ustrezno pripraviti in izbrati ustrezna sodila, s pomočjo katerih izvedemo revizijski pregled. Sodila so v tem primeru navedena v prilogah standarda ISO/IEC 27007:20011.

Ta revizijski pregled SUVI je bil poizkusen in ni vključeval tehničnih strokovnjakov v revizijski ekipi, kot to opredeljuje novi standard. Pregled je pokazal, da je možno s pomočjo standarda ISO/IEC 27007:2011 analitično pristopiti k načrtovanju samega pregleda in s pomočjo smernic tudi učinkovito izvesti pregled.

Z objavo celovitega pristopa COBIT 5 in še posebej z objavo profesionalnega vodiča COBIT 5 for Information Security smo revizorji informacijskih sistemov dobili komplementaren produkt za revidiranje varovanja informacij.

Po drugi strani se moramo revizorji IS spoznavati tudi z drugimi metodami, standardi, celovitimi pristopi, ki pokrivajo področje revidiranja, in ne samo uporabljati COBIT kot osnovo za vse. Dobro je, če ta spoznanja oziroma tudi druge metode, standarde in celovite pristope uporabljamo pri svojem delu. ISACA je samo ugotovila, da je potrebno COBIT povezovati z različnimi drugimi dobrimi praksami, standardi in celovitimi pristopi, saj z novo objavljeno družino COBIT 5, ISACA poizkuša zapolniti vrzeli, ki so nastale v zadnjem desetletju.

Samemu revizorju informacijskih sistemov oziroma vodji revizijskega pregleda je prepuščeno, katero smernice in sodilo bo uporabil pri načrtovanju in revizijskem pregledu SUVI.

8 Zaključek

Uporaba standardov ISO/IEC 27007:2011 in ISO/IEC 27006:2007 omogoča izvedbo celovite revizije SUVI. Ker je vsak začetek težak, bo s pridobivanjem izkušenj možno učinkovito izvesti celovito revizijo SUVI v organizaciji, ki je certificirana ali se pripravlja na certificiranje po ISO/IEC 27001:2005 ali pa naj bi bila skladna z zahtevami tega standarda. Po drugi strani nam ISACA ponuja metodo za revizijo varovanja informacij s pomočjo COBIT 5 for Information Security.

Možnosti za nadaljnje delo so v praktični izvedbi revizije sistema upravljanja varovanja informacij v organizaciji, ki ima ta sistem certificiran po ISO/IEC 27001:2005 s pomočjo celovitega pristopa COBIT 5 in COBIT 5 for Information Security.

Avtorja prispevka želiva izvesti revizijo v organizaciji, ki že ima certificiran SUVI po ISO/IEC 27001:2005 s pomočjo standardov ISO/IEC 27007:20011 in COBIT 5 for Information Security ter pripraviti analizo obeh pristopov. Rezultate te analize nameravava predstaviti prihodnje leto.

Viri

- Axelord,C.W., Bayuk, J.L. inSchutzer, D. (2009). Enterprise Information Security and Privacy. ArtechHouse, ISBN 978-1-59693-190-9
- ISACA. (2009). An Introduction to the Business Model of Information Security
- ISACA.(2012).COBIT 5 ISBN 978-1-60420-237-3
- ISACA.(2012a).COBIT 5 for Information Security ISBN 978-1-60420-255-7
- ISO/IEC. (2005). ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO/IEC. (2011). ISO/IEC 27007:2011 Information Technology – Security Techniques – Guidelines for Information Security Management System Auditing
- ISO/IEC. (2007). ISO/IEC 27006:2007 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management System
- Ma, Q. inPearson, J. M. (2005) ISO 1799: »Best Practices« in Information Security Management, Communications of the Association for Information Systems, Volume 15, Article 32, str. 577-591
- SIST. (2011). SIST EN ISO 19011:2011 Smernice za presojanje sistemov vodenja
- SIST. (2011a). SIST EN ISO/IEC 17021:2011 Ugotavljanje skladnosti – Zahteve za organe, ki presojajo in certificirajo sisteme vodenja (ISO/IEC 17021:2011)
- SIST. (2011b). SIST ISO/IEC 27005:2011 Informacijska tehnologija – Varnostne tehnike – Upravljanje tveganj informacijske varnosti
- Tashi, I. in Ghernaouti-Helie, S. (2007) ISO Security Standards as a Leverage on IT Security Management, Zbornik: Americans Conferences on Information Systems, http://aisel.aisnet.org/amcis2007/63 (dostop dne: 15.9.2012)

O avtorjih

Mladen Terčelj, univ. dipl. ing., CISM, PRIS, CIS-A; vodilni presojevalec sistema upravljanja varovanja informacij ISO/IEC 27001:2005; prokurist; VZHOD,Terčelj in drugi d.n.o.

dr. Boštjan Delak, CISA, PRIS, CIS; samostojni svetovalec; ITAD, Revizija in svetovanje, d.o.o. (član Sekcije upravljanja varovanja informacij pri Območni zvezi Ljubljana GZS).

Strategija kibernetske varnosti in kibernetske obrambe v okviru slovenske strateške kulture

Adriana Dvoršak

Namen prispevka je proučiti stanje nacionalnih politik na področju kibernetske varnosti in kibernetske obrambe in ga postaviti v perspektivo razvoja mednarodnih norm na področju kibernetske varnosti, kibernetskega bojevanja in informacijskega bojevanja v mednarodnih organizacijah. Avtorica obravnava strategijo kibernetske obrambe kot sestavni del širše strategije kibernetske varnosti. Nacionalna pravila kibernetske obrambe je nujno potrebno postaviti zaradi sprememb, ki jih doživlja pojmovanje kibernetskega prostora v mednarodnem okolju. Razlog za pisanje prispevka je potreba po drugačnem odnosu do kibernetske varnosti in obrambe. Uporabljeni sta deskriptivna in primerjalna metoda. Kibernetsko bojevanje povečuje nasilne in vojaške možnosti malih držav in nedržavnih akterjev, kot vedno bolj dosegljivo in realno sredstvo za doseganje zunanjepolitičnih ciljev. Zato se v mednarodnih odnosih povečuje število pobud za uravnavanje aktivnosti držav v kibernetskem prostoru. Namen teh pobud je preprečiti konflikte v kibernetskem prostoru med nacionalnimi državami, ne pa tudi med nedržavnimi akterji, ki niso predmet mednarodnih norm. Izhajajoč iz stanja nacionalnih politik sta ključna dejavnika za uspeh vzpostavljanje zmogljivosti za učinkovito upravljanje incidentov in ustrezna partnerstva za zagotavljanje teh zmogljivosti. Največja omejitev raziskave je omejen dostop do relevantnih državnih virov informacij in pomanjkanje tehničnega znanja za oceno resnosti stanja ogroženosti v Sloveniji. Praktična uporabnost prispevka je povečana sposobnost odločevalcev za oblikovanje koristnih partnerstev in doprinos k reševanju sodobnih mednarodnih groženj miru in varnosti. Raziskava prispeva k razumevanju motivov in dejavnosti malih držav za povečanje mednarodne kibernetske varnosti. Izvirnost prispevka je v analizi učinka, ki ga imata zunanja ali mednarodna prisila in nacionalna politična kultura na razvoj strategije kibernetske varnosti in kibernetske obrambe.

KLJUČNE BESEDE: kibernetska obramba, odločanje, partnerstva, strategija, strateška kultura

1 Uvod

Avtorica prispevka pojmuje postopke odločanja, po katerih nastaja strategija kibernetske varnosti, kot pomemben člen strateške kulture. Manjši del kibernetske varnosti predstavlja kibernetska obramba, ki je za razvite države vedno večji diplomatski, informacijski, vojaški in ekonomski izziv (European Parliament [EP], 2009). Družbene silnice kot so skupno prepričanje, predpostavke o (ne)varnosti, pripovedi, ki oblikujejo kolektivno identiteto in odnose do drugih skupin sooblikujejo strateško kulturo skupaj z varnostnimi cilji in sredstvi za doseganje teh ciljev. Strateška kultura v Sloveniji na začetku 21. stoletja temelji na nekaterih konkretnih dogodkih in sosledjih dogodkov: nastanku države, procesih vzpostavljanja kolektivne identitete, načinu, kako se vrednote skupnosti preoblikujejo v politiki, dejavnostih civilne družbe in sprejemanju mednarodnih norm. Na področjih kibernetske varnosti in obrambe slovenski avtorji ugotavljajo (Praprotnik, Podbregar, Bernik, in Ticar, 2012), da prevladuje občutek varnosti in nizkega varnostnega tveganja.

Slovenija ni razvila svoje velike strategije, ki bi združevala velike zunanjepolitične in vojaške cilje, njena zgodovinska izkušnja je močno vpeta v asimetrično delovanje in formalno so se spremenile strani v tej asimetriji šele pred kratkim, z vstopom v Severnoatlantsko zavezništvo. Izostruje se vprašanje, ali obstoji evropska strateška kultura v okviru Evropske unije in kako se razlikuje od strateške kulture Severnoatlantskega zavezništva, kar je bilo razvidno iz razhajanja med ZDA in EU glede urejanja kibernetskega bojevanja. Medtem, ko so se ZDA zavzemale za podpis pogodbe, podobne pogodbi o preprečevanju uporabe kemičnega orožja, so Evropejci v večji meri zagovarjali normativni pristop. Po terorističnem napadu 11. septembra 2001 so predvsem ZDA proučevale strateško kulturo nasilnih nedržavnih akterjev, ki združujejo teroristična dejanja s kibernetskim bojevanjem in s spletnim kriminalom. Funkcionalno je strategija kibernetske varnosti usmerjena k preprečevanju kibernetskega kriminala, strategija kibernetske obrambe pa k zagotavljanju integritete kritične infrastrukture. Pri obeh prepoznamo več dimenzij – nacionalno, evropsko in globalno, pri strategiji kibernetske obrambe pa še Severnoatlantsko.

2 Dejavniki Slovenske strateške kulture

Nedavni dogodki, povezani z izdelavo virusnih programov, namenjenih pridobivanju pomembnih informacij, razkrivajo informacijsko bojevanje, kakor ga pojmuje slovenska vojaška doktrina in ga popularno imenujejo cyberwarfare. Med

izrazoma informacijsko bojevanje in cyberwarfare obstojijo določene razlike (EP, 2009), vendar razčiščevanje osnovnih konceptov ni namen tega prispevka. Duqu, Stuxnet, Flame (Team Register, 2012) kažejo na to, da poteka intenzivno pridobivanje informacij o političnih procesih na Bližnjem vzhodu, kakor tudi o kritični infrastrukturi Irana. Proučevanje informacijskega bojevanja na Kitajskem in delovanja opozicijskih gibanj ter nasprotnikov avtoritarnih režimov v Severni Afriki prav tako kaže na razvejano državno sponzorirano dejavnost. Ti mednarodni dogodki so podžgali razpravo o nacionalnih in mednarodnih normah v kibernetskem bojevanju, nacionalnih strategijah in nacionalnih strateških kulturah ter o tem, kdo sploh so udeleženci v kiberentskem bojevanju in kakšne so njihove obveznosti po mednarodnem humanitarnem pravu. Posledično se odpirajo tudi razprave o varstvu zasebnosti in vlogi civilne družbe v globalnem upravljanju svetovnega spleta.

Nacionalne vojaške doktrine gradijo na uporabi kibernetskih zmogljivosti za pridobivanje informacij in kot podporo kinetičnim operacijam. Nekatere države vključujejo posebne načrte za informativne in politične operacije. Druge države povezujejo zmogljivosti v informacijskem bojevanju z obstoječim elektronskim bojevanjem (Lewis, Timlin, 2011). Razlike v vojaških doktrinah se pojavljajo zaradi razlik v nacionalnih strateških kulturah in različnega zgodovinskega razvoja. Preden si ogledamo elemente strategije kibernetske varnosti za majhno državo, si zelo na kratko oglejmo velike družbene silnice, ki oblikujejo strateško kulturo.

Začnimo s preprosto definicijo, ki je uporabna na ravni analize politik in pušča nekaj prostora za razpravo na akademski ravni: strateška kultura je niz skupnih prepričanj, predpostavk, pisnih in ustnih pripovedi, ki oblikujejo skupno identiteto in razmerja do drugih skupin in ki določa ustrezne varnostne cilje ter sredstva in vedenje za doseganje teh ciljev, kakršna izhajajo iz skupnih izkušenj (Johnson in Larsen, 2006).

Dejavniki strateške kulture oblikujejo vedenje, ki temelji na politični tradiciji, na zgodovini, na vrednotah in prepričanjih, na virih (v primeru strategije kibernetske varnosti predvsem gospodarskih, tehnoloških in znanstvenih), na velikih zgodbah, na konceptu obrambe, na geografskih značilnostih, na izkušnjah politične generacije in še na čem. Poleg splošnih dejavnikov moramo sprejeti tudi druga posebna prepričanja, kar velja predvsem za nedržavne akterje.

Strateška kultura v Sloveniji je utemeljena v naslednjih dejavnikih in konkretnih zgodovinskih dogodkih: nastanku in oblikovanju države ter kolektivne identitete, vzorcu spreminjanja vrednot skupnosti v posamične politike, vlogi in razvejanosti civilne družbe ter tudi v sprejemanju mednarodnih norm.

2.1 Oblikovanje države

Oblikovanje države je povezano s številnimi procesi in dogodki, ki so vodili v nastanek državne tvorbe. Kako je nastala Slovenija je obsežno izpričano na drugih mestih, pomembno pa je, kako se nastanek države odraža na varnostni kulturi.

2.2 Kolektivna identiteta

Vprašanje kolektivne identitete, ki presega meje nacionalne države, je pomembno pri ugotavljanju trdnosti mednarodnih zavezništev in pripadnosti mednarodnim procesom. S katero kolektivno identiteto se povezuje Slovenija, s kom razvija skupinsko pripadnost in kateri individualni občutki pripadnosti se razvijajo? Možni odgovori se nahajajo v verski identiteti (prevladujoča rimskokatoliška vera) in geografsko-političnih nadnacionalnih tvorbah kot je Evropska unija, posebej v njeni evrski skupini, na ostankih hladne vojne (NATO in izginuli Varšavski pakt) ter manj otipljivih kulturno-civilizacijskih prostorih kot so srednjeevropski prostor, sredozemska kultura, alpska kultura, slovanske kulture, Južni Slovani in narodi nekdanje Jugoslavije.

V političnem razvoju naroda in njegovi zavesti glede prihodnje politične usode igra pomembno vlogo nacionalna sposobnost usklajevanja zamišljenih političnih ciljev z ustreznimi sredstvi, orodji in postopki za njihovo doseganje. Lahko nacionalne elite dobijo podporo ljudstva za doseganje svojih političnih ciljev, za mednarodni uspeh? Ali obstajajo razlike med zamišljenimi in realnimi politikami in zakaj pride do prekinitev v prevajanju politike političnih elit v nacionalne politike? Razlike med zamišljenimi in realiziranimi politikami lahko izhajajo iz šibke interakcije med nacionalnimi elitami, kar pomembno oblikuje strateško kulturo in varnostne politike. Kot primer šibke povezanosti elit naj navedem incident z nezakonitim tehničnim prisluškovanjem sejam vlade ter varnostno občutljivim posedovanjem in posredovanjem pridobljenih informacij prek YouTuba (Praprotnik et al., 2012).

2.3 Pretvorba vrednot v nacionalne politike

Ozaveščanje in kritična introspekcija slovenskih elit bi vzpodbudila razmislek o tem, kako nacionalne vrednote postanejo nacionalne politike. V primeru, da se vrednote in politike institucionalno povezujejo samo v parlamentu, so zanemarjeni pomembni vidiki civilne družbe, relativno večji pomen pa pridobivajo mednarodne organizacije (EU, NATO) ki prek zakonodajnega telesa neposredno vplivajo na nacionalne politike. Članstvo v EU in NATO odpira vprašanje, v kakšnem obsegu

nacionalne politike ustrezajo nacionalnim vrednotam, saj obe organizaciji predpišeta veliko mednarodnih norm, ki se neposredno uporabljajo v notranjem pravnem redu. Na področju kibernetskega upravljanja, kibernetske varnosti in pravice do zasebnosti je potrebno računati s civilno družbo in s širšo politično javnostjo, saj je naivno verjeti, da se bosta sprijaznili z vlogo gledalcev političnih procesov.

2.4 Civilna družba

V kibernetskem upravljanju je civilna družba priznano pomemben akter in se še krepi v smeri prevzemanja večje politične vloge. Tudi zato je potrebna ena celovita strategija za varnost v kibernetskem prostoru, ki bi določala varnostne cilje države, gospodarstva in posameznikov. Civilna družba podpira ravnanje države pri zagotavljanju nacionalne varnosti, hkrati pa visoko na lestvico potreb postavlja varovanje zasebnosti in ohranjanje odprtih informacijskih in komunikacijskih omrežij. Morda se razlikuje od hierarhije vrednot pri določenih profesionalnih in političnih elitah.

2.5 Odnos do mednarodnih norm

Naslednja značilnost je sprejemanje globalnih in mednarodnih norm ter vpliv mednarodnih dogodkov na domačo politično razpravo o nacionalni varnosti. Priznati je potrebno, da Slovenija nikoli ni bila zares izolirana in da globalni trendi vplivajo na državo, tudi če ni udeležena v prvem valu tehnoloških, političnih in kulturnih sprememb. Vrednostni sistem in strateška kultura v Sloveniji nista naklonjena nasprotovanju velikim silam ali pobudam v okviru mednarodnih organizacij. Male države načelno podpirajo doseženi red in utrjujejo doseženo soglasje. Nekonfliktnost, celo nevidnost v mednarodnih odnosih, naj bi že stoletja veljala za dobro politično izbiro. Vendar pa se taka defenzivna drža hitro spremeni pri vseh družbenih slojih v krizi, ki neposredno ogroža narod. To je prav gotovo veljalo za mednarodno asertivnost med nastankom države v devetdesetih letih prejšnjega stoletja.

3 Odzivna strategija kibernetske varnosti in kibernetske obrambe

Odnosa do nacionalne in mednarodne varnosti se močno razlikujeta. Prvi je tesno povezan s slovensko državnostjo in je v zgodovinskem spominu aktivne

politične generacije še zelo živ. Drugi je v manjši meri prepoznan kot pomemben dejavnik strateške kulture, tako da ga v veliki meri oblikujejo mednarodne norme od zunaj. Ta pravica in odgovornost držav sooblikovati in upoštevati mednarodne norme vzbuja občutek lastne pomembnosti, saj so Slovenci šele pred kratkim pridobili pravico do nastopa v mednarodni skupnosti in obveznost prevzemanja mednarodnih obveznosti. Po drugi strani pa mednarodnimi konflikti in spori niso nekaj, kjer bi aktivno vključevanje Slovenije kar koli bistveno spremenilo, zato je v širši javnosti na splošno sprejemljivo, da se mednarodni varnosti namenjajo skromni nacionalni viri.

Za legitimnost udeležbe slovenskega osebja na mednarodni misiji je zelo pomembna moralna integriteta slovenskega osebja, spoštovanje človekovih pravic ter ustrezna udeležbe na podlagi odločitve Varnostnega sveta (VS) in mednarodnega prava. Lahko sklepamo, da bi bilo sodelovanje Slovencev v kateri koli kibernetski mednarodni operaciji podvrženo enaki javni presoji. To je tudi dodaten razlog, da vlada pristopi k pripravi celovite strategije kibernetske varnosti, saj legitimnost varnostnih in obrambnih ukrepov ne sloni le na odločitvah VS, temveč tudi na nacionalnih kazenskih zakonikih.

V zgodovini velikih držav, pa tudi nekaterih malih, starejših od Slovenije, so se izoblikovale tako imenovane velike strategije. Odgovarjajo na vsaj tri velika vprašanja:

- Kateri so osnovni nacionalni interesi?
- Katere zunanje sile jih ogrožajo?
- Kaj lahko nacionalni voditelji in politične elite storijo, da jih zaščitijo?

Zakaj Slovenija ni oblikovala tako jasne in preproste velike strategije ostaja neodgovorjeno. Še več, Nacionalna varnostna strategija prav tako ne daje odgovora na nobeno od teh treh vprašanj in posledično slovenska velika strategija za multipolarni svet v pogojih globalizacije še ni zastavljena.

Državnim akterjem v kibernetski obrambi se pridružujejo nedržavni akterji, nastajajo nova partnerstva na mednarodni ravni, spreminja pa se tudi narava partnerstev v državni varnosti. To dinamično dogajanje povzroča obstoječim varnostno-obrambnim strukturam dodatne in povsem nove obremenitve tako na konceptualni kot operativni ravni. Ena izmed takih novosti je pojav nevidnih in nepredvidljivih nasprotnikov, na primer anonimnih posameznikov, skupin

hektivistov, proksijev in vohunov. Strateška kultura je bila v preteklosti omejena na ravnanje nacionalne države, v kibernetskem prostoru pa imamo igralce, ki bi jim komaj pripisali kako strateško kulturo, jasen namen, hierarhično organizacijo ali profesionalizacijo. V tem smislu se varnostno-obrambni podsistem z jasnimi pisnimi pravili in z močno hierarhično organizacijo srečuje s svojim nasprotjem. Zahodne strateške kulture se srečujejo z akterji, ki ne igrajo po do zdaj znanih pravilih in jih tudi ni mogoče analizirati z metodami, učinkovitimi pri preganjanju klasičnega organiziranega kriminala, vstajnikov, demonstrantov ali nasilnežev. Vztrajnosti strateških kultur bi lahko pripisali iskanje modelov upravljanja kibernetskih konfliktov na osnovi oboroževalne tekme in hladne vojne. Avtorica prispevka meni, da stopnja dosežene globalizacije preprečuje nastanek dveh relativno izoliranih blokov ali nastanek bipolarne globalne ureditve. Podrobneje je logiko hladne vojne v kibernetskem prostoru obravnaval Jospeh Nye (Nye, 2006), oživitev nekaterih orodij, kot je rdeči telefon med predvidoma ameriškim in kitajskim predsednikom, pa zagovarjajo starejši ameriški vplivneži.

Spletni kriminal in kibernetske napade izvajajo posamezniki z močno izraženimi osebnostnimi lastnostmi, vrednotami in cilji. Občutek nepravičnosti je zanje odločujoč motivacijski dejavnik, ostalih dejavnikov strateške kulture pa nanje ne bi mogli aplicirati. Nedržavni akterji v kibernetskem prostoru ne delujejo po pravilih strateške kulture, za boljše razumevanje vedenje nedržavnih akterjev v kibernetskem prostoru bo potrebno razviti nove metode. Kadar prihaja do državno sponzoriranih kibernetskih napadov, so analize strateških kultur, obstoječih vojaških doktrin, taktike zavajanja in podobnega nadvse koristne. Omenjeni Duqu, Stuxnet in Flame sledijo geopolitični situaciji na Bližnjem in Srednjem Vzhodu, kakor tudi logiki slepilnih manevrov, ki jih uporabljajo nacionalne vojske (Team Register, 2012).

Ko se ozremo na nanizane elemente slovenske strateške kulture in upoštevamo, kako delujejo kriminalci, hektivisti in nacionalne države, nam postane jasno, da bo slovenska kibernetska strategija predvsem odzivna in ne proaktivna. Proaktivna bi bila v primeru, da je namen strategije izkoristiti kibernetski prostor za povečanje mehke moči države.

Vedenje udeležencev v kibernetskih konfliktih (Schreier, 2012) povratno vpliva tudi na nacionalne cilje kibernetske obrambe. Vodenje ofenzivnega kibernetskega bojevanja izpostavlja razlike med NATO-vo strateško kulturo in strateško kulturo Evropske unije. Med njima lahko pričakujemo osnovne razlike v ciljih in namenih, razumevanju pravične vojne, upravičenosti preventivnega udarca, kar

so tudi vzroki za nastanek razlik med obrambnimi in napadalnimi strategijami. Avtorica predpostavlja, da ofenzivne kibernetske strategije, kakršno so sprejele ZDA, ne moremo nekritično posnemati v malih državah Evropske Unije. Prav tako male države in države v razvoju težko nekritično sledijo mednarodnim priporočilom, saj v njih ni upoštevana sposobnost posamične države, da učinkovito izkoristi svoje vire. Razen tega Wamala (International Telecommunication Union [ITU], 2011) s priporočili v priročniku ITU vzbuja vtis precejšnjega birokratizma in z veliko lahkoto preskoči vse dejavnike strateškega kulture, kar nas mora znova odvrniti od avtomatskega zasledovanja priporočil.

Majhen, pa vendar pomemben del strateške kulture predstavljajo institucije, ustanovljene za sprejemanje odločitev na nacionalni ravni, ki odločitve sooblikujejo s pomočjo demokratičnih pravil in s podeljevanjem legitimnosti. V teh institucijah se oblikuje postopek odločanja, določa se predmet odločitve, opravi se formalni sprejem odločitev, pridobivajo se potrebne informacije, sprejemajo se kompromisi, dogaja se proces učenja ali vzpostavi povratna zanka med odločitvijo in stanjem, ki nastopi kot posledica te odločitve. Avtorica prispevka pojmuje kot pomemben element strateške kulture postopke odločanja, ki so relevantni pri kibernetski obrambi: formulacija problema, ozaveščanje in postopki v primeru, da elite ne zaznavajo resnosti problema, oblikovanje politik, vključno z uvedbo varnostno obrambnih strategij, zakonodajni postopek na področju telekomunikacij in/ali nacionalne varnosti, kot tudi odločitve, ali bodo mednarodne norme sprejete ali prezrte. Praktična uporabnost prispevka je tudi v tem, da je moč preveriti, kako obstoječe institucije na področju kibernetske varnosti podpirajo ali ovirajo ukrepe, ki jih sprejemajo politični in vojaški odločevalci. Premislek o vlogi institucij nas tudi postavi pred vprašanje, katera institucija je v Sloveniji pristojna za dajanje pobude za pripravo kibernetske strategije.

Porast spletnih napadov celo v večji meri kot informacijsko bojevanje izpostavlja nove nedržavne akterje, ki v oboroženih spopadih med organiziranimi vojskami sploh ne nastopajo. Posamezniki, ki so postali pomembni za kibernetsko varnost in obrambo, niso predmet mednarodnega prava. Hektivistov, patriotskih hekerjev, spletnih aktivistov, organiziranega kibernetskega kriminala, teroristov in drugih avtonomnih akterjev mednarodno pravo ne obravnava. Nadalje ti posamezniki niso seznanjeni z vojaško etiko, z zakoni nevtralnosti, nimajo jasne namere ali vojaškega cilja, ne upoštevajo pravil delovanja hierarhičnih organizacij, zato mednarodno pravo in klasične vojaške doktrine malo ali nič ne vplivajo nanje. Avtorica prispevka meni, da lahko kljub temu prepoznamo skupni tehnični motiv v ozadju kibernetskih napadov. Gre za pridobivanje dostopa do sistemov

ali informacij, pomembnih za nacionalne gospodarske in strateške cilje. V ožjem smislu gre za motiv namernega napada na zaupnost, integriteto in razpoložljivost informacijske komunikacijske tehnologije v določeni državi, pri čemer pa ne analiziramo raznolikih motivacijskih dejavnikov, ki stojijo za napadom.

Narava kibernetskega kriminala in pripadajočih pravnih vprašanj presega nacionalne meje, zato so države zainteresirane za oblikovanje mednarodnih norm v okviru mednarodnih organizacij. ZN in NATO se osredotočajo na dejavnosti povezane s pravili kibernetske vojne, zato je težišče globalnega dogovora potrebno videti v ZN, ne le v NATU ali skupini držav G20.

Pri oblikovanju mednarodnih norm pogosto prevladuje skupina držav, vodilno vlogo pa prevzemajo ZDA (International Strategy for Cyberspace, 2011). Zanje na začetku 21. stoletja (še) velja, da imajo za razliko od vplivne skupine BRICS realno sposobnost vodenja v globalnih zadevah. Na področju kibernetskega bojevanja ZDA veliko napora vlagajo v bojevanje s pravom – v originalu »lawfare«, in v poenotenje v NATU, ker v ZN domnevno naj ne bi prišlo do učinkovitega dogovora zaradi načela ena država en glas. Del ameriških teoretikov opušča željo po mednarodni pogodbi, podobni tisti, o neširjenju kemičnega orožja, saj ji že dolgo nasprotujejo evropski uradniki (EP, 2009).

4 Razvoj mednarodnih norm in potrebe Slovenije

Mednarodne norme (Melzer, 2011) in kodeksi (Maurer, 2011) stopajo v ospredje mednarodnih odnosov tudi s prizadevanji ITU za razširitev pogodbe med 193 članicami prek telekomunikacijskega področje tudi na splet in na preprečevanje konfliktov med državami v kibernetskem prostoru. Trenutno se v mednarodni skupnosti pojavljajo dvomi o pravilnosti vodenje ofenzivne kibernetske vojne zaradi kritik uporabe škodljive kode Flame. Obrambne dejavnosti so sprejemljivejše za širše občinstvo, za katerega prav tako ni mogoče reči, da odobrava postopno vedno bolj intenzivno in vsiljivo ameriško primerjanje kibernetskih aktivnosti Kitajske s hladnovojnimi aktivnostmi. Mednarodna javnost nasprotuje inkriminiranju spletnega in »offline« vedenja posameznikov. Vsesplošni nadzor spletnih aktivnosti krši človekove pravice in pravico do zasebnosti, čemur nasprotujejo mnoge nevladne organizacije in pri tem uživajo moralno in materialno podporo civilne družbe. Kaznovanje kršitev pravic intelektualne lastnine v velikem obsegu ne uživa podpore javnosti in nepopularnost ukrepov je že spremenila politično

pokrajino v Evropi s pojavom Evropske piratske stranke. Državne institucije ne spremljajo odnosa slovenske civilne družbe do omenjenih vprašanj, ga pa zato v večji meri nevladne organizacije za e-upravljanje, e-demokracijo in podobno.

Opredelitev Sveta Evrope v Konvenciji o kibernetski kriminaliteti (Council of Europe, 2001) je dovolj prožna za širši premislek o kibernetski varnosti, saj obravnava tehnologijo, ki presega tradicionalne računalniške sisteme. Definicija vključuje mobilno telefonijo, ki ima zmogljivosti za proizvodnjo, obdelavo in prenos podatkov, omogoča dostop do interneta, pošiljanje e-pošte in pošiljanje priponk.

Kibernetska varnost pomeni zaščito pred namernimi napadi, poškodbami in dostopom omrežij, računalnikov, programov in podatkov. Obravnava elektronskih dokazov o napadu je predmet nacionalnih kazenskih zakonodaj, kar smo že omenili v primeru mednarodnega kazenskega prava in mednarodnih norm na področju komunikacijske tehnologije. Spomniti velja, da zahodni pravni sistemi ne poznajo preventivnega kaznovanja, do kazni pride potem, ko je bilo kaznivo dejanje storjeno in ko je bila izrečena pravnomočna sodba pred pristojnim sodiščem. Za razliko od kibernetske varnosti kibernetska obramba pomeni zaščito kritične infrastrukture, kazenska zakonodaja pa se bo verjetno nekoliko razlikovala od zakonodaje, ki se nanaša na kibernetski kriminal ali klasično kriminaliteto. Ogrožanje varnosti kritične infrastrukture bi lahko bilo deležno posebne obravnave v nacionalnem pravu podobno kot teroristične dejavnosti.

Mednarodna telekomunikacijska unija ITU je pripravila orodje za samoocenjevanje nacionalne kibernetske varnosti in za ocenjevanje dejavnosti, ki vodijo k oblikovanju strategije kibernetske varnosti (ITU, 2009). Predlagano izhodišče za strategijo kibernetske varnosti je opredelitev vloge informacijskih in komunikacijskih tehnologij v državi, to je v gospodarstvu, v nacionalni varnosti, v kritični infrastrukturi in v civilni družbi. ITU v samoocenjevalnem orodju državam predlaga, da nadaljujejo z identifikacijo groženj in ranljivostjo IKT. Naslednje priporočene naloge so oblikovanje politike kibernetske varnosti, izvajanje strategije, postavljanje časovnega okvirja, metrike in odnosa do regionalnih in mednarodnih dejavnosti.

V Sloveniji je zelo pomembno poudariti nacionalne cilje kibernetske varnosti, ki so primarni, kar se v postopkih upravljanja pogosto spregleda oziroma se kot primarne postavijo mednarodne strategije, katerim so slovenske potrebe podrejene. Nacionalne strategije postanejo odziv na mednarodne grožnje, ki s slovenskim položajem nimajo prav dosti skupnega. Tak odnos do strategij v strateški kulturi kaže, da je država premalo proaktivna in ne določa lastnih ciljev.

V nadaljevanju je predstavljena hrbtenica nacionalne strategije kibernetske varnosti in kibernetske obrambe. Postavljena je kot zaporedje nalog prilagojenih potrebam malih držav, konkretno Slovenije. Kot vir je uporabljeno orodje za samoocenjevanje Mednarodne telekomunikacijske unije (ITU, 2009).

Razlog za nacionalno ukrepanje:

- Ugotovi stanje nacionalne politike na področju kibernetske varnosti.

Udeležene institucije:

- Opredeli ključna ministrstva in institucije, ki so najbolj odgovorni za kibernetsko varnosti in opiši njihove naloge.
- Opredeli druge udeležence s pristojnostmi na področju kibernetske varnosti in opiši njihove naloge.

Organizacija kibernetske varnosti:

- Katere organizacijske strukture vplivajo na razvoj politike kibernetske varnosti? Opiši delovanje teh struktur in kako se vanje vključujejo novi udeleženci.
- Katere organizacijske strukture operativno zagotavljajo kibernetsko varnost? Opiši delovanje teh struktur in kako se vanje vključujejo novi udeleženci.

Sodelovanje med javnim in zasebnim sektorjem:

- Opredeli cilje in oblike sodelovanja med javnim in zasebnim sektorjem.
- Opredeli cilje in oblike zaupnega sodelovanja med javnim in zasebnim sektorjem.

Zmogljivosti za upravljanje incidentov:

- Ugotovi, kje v državni upravi so zmogljivosti za upravljanje incidentov.
- Opredeli in določi cilje v upravljanju incidentov.

Pravni okvir:

- Opredeli cilje za posodobitev zakonodaje o informacijski družbi, o kibernetski kriminaliteti in o obrambi, da bodo v podporo nacionalnemu ukrepanju.

Strateška kultura in povratne informacije:

- Opredeli in določi cilje za nadgrajevanje nacionalne varnostne kulture.
- Ugotovi, kako dokončati in razširiti nacionalno strategijo.
- Preglej finančne zahteve in vire za vsak element nacionalne strategije.
- Ugotovi časovni okvir za izvajanje zahtev.
- Izvajaj meritve in znova presojaj cilje.

Če povzamemo in razložimo osnovne pristojnosti in odgovornosti pri pripravi strategije, ugotovimo, da so vlade odgovorne za pripravo strategije kibernetske varnosti in kibernetske obrambe. Oborožene sile so odgovorne za opredelitev ciljev in ustreznih ukrepov za doseganje varnosti kritične infrastrukture, za razvoj kibernetske obrambe in za nadgradnjo doktrine, kjer se ta nanaša na informacijsko bojevanje. Vlade so tudi odgovorne za identifikacijo in uspeh javno-zasebnih partnerstev ter za omogočanje sodelovanja vseh zainteresiranih strani.

Če združimo navedene naloge in jih prenesemo na slovensko situacijo, ugotovimo, da je potreben razvoj na dveh področjih. Eno je povsem konceptualno, drugo pa upravljalsko. O konceptih »cyber defense« in »cyber crime« (Council of Europe 2011), se bosta morala izreči slovenska obrambna in varnostna stroka, politika in javna uprava pa sprejeti odločitve glede delitve pristojnosti in odgovornosti, kakršne lahko predvidimo na osnovi naštetih nalog v orodju ITU. Na upravljalski ravni bo potrebno natančno proučiti razpoložljive človeške vire in skrbno pretehtati odločitev, da se ob CERT-u ustanovi še CERT za računalniška omrežja v javni upravi in CERT za kritično infrastrukturo, ki bi bil na Ministrstvu za obrambo. MORS je odgovoren za koordinacijo varovanja kritične infrastrukture, pravno-formalno pa je bil v njem ustanovljen le Svet za informacijsko varnost. Zelo priporočljivo je, da Ministrstvo za obrambo jasno določi in objavi organizacijsko strukturo komunikacijske varnosti v obliki preprostega grafikona, tudi za namere odvračanja kibernetskih napadov, v angleščini »deterrence«. CERT MORS bi lahko v majhni državi kot je Slovenija prevzel vlogo upravljanja

incidentov in postal odgovoren za zaščito omrežij kritične infrastrukture, usklajevanje vseh aspektov informacijskega bojevanja vključno s psihološkimi operacijami in za sodelovanje z domačimi in tujimi partnerji. Na tej točki avtorica priporoča, da so zmogljivosti za upravljanje incidentov usmerjenim proti kritični infrastrukturi, prav tako v domeni CERT MORS. S tem bi se izognili razdrobljenosti virov (znanje, ljudje in denar). Nadalje avtorica na upravljalski ravni priporoča sodelovanje z najetimi strokovnjaki, saj so človeški viri v majhnih držav preskromni, da bi oblikovali učinkovite vojaške kibernetske enote in jim zagotovili ustrezno usposabljanje ekskluzivno v vojaške namene. Kot zadnji člen v sintezi, avtorica priporoča, da se Svet za informacijsko varnost pooblasti za avtonomno sodelovanje s partnerji na nacionalni ravni, s čimer bi zmanjšali birokratske ovire v komuniciranju in odločanju.

5 Zaključek

Izhajajoč iz slovenskih okoliščin sta najpomembnejša dejavnika uspeha nacionalne strategije kibernetske varnosti vzpostavitev učinkovitih zmogljivosti za upravljanje incidentov in ustrezna javno-zasebna partnerstva. S stališča mednarodne politologije je nekoliko zaskrbljujoča razvejanost in intenzivnost partnerstev v primerjavi z dejavnostmi v ostalih primerljivih državah članicah NATA, OECD in EU: »Slovenska vojska sodeluje pri razvoju nacionalne strategije in razvoju koncepta kibernetske obrambe le z dvema predstavnikoma v delovni skupini. Za zdaj pa ne razpolaga s sredstvi za razvoj lastnih zmogljivosti.« (Čaleta in Rolih, 2011) Avtorica priporoča, da prednostne naloge nacionalne varnosti za obdobje 2012–2016 upoštevajo poročila o spletnih grožnjah v mednarodni skupnosti in da Svet za nacionalno varnost preveri ustreznost nacionalnih politik glede na poročila o spletnih grožnjah iz mednarodnega okolja. Nekatere od prednostnih nalog bi se lahko nanašale na izboljšano razumevanje položaja za krizno upravljanje v EU, združevanje aktivnosti v odnosu do EU in NATA, kot sta združevanje nacionalne pomorske in zračne varnosti v evropski varnosti in združevanje kibernetske obrambe v pomorski in zračni varnosti v NATU.

Ena glavnih ugotovitev raziskave je, da je potrebno sinergijske učinke med kibernetsko obrambo in kibernetsko varnostjo načrtovati in učinkovito nadzirati v Svetu za nacionalno varnost. Ta organ je odgovoren tudi za začetek procesa oblikovanja strategije in daje pobudo za njeno oblikovanje ustreznim organom. Avtorica predlaga širitev članstva Sveta za nacionalno varnost na druge zainteresirane

deležnike v zasebnem sektorju. V njegovo pristojnost spadajo pomembna politična vprašanja, kot je odločitev, ali bo obrambo pred kibernetskim napadom izvajala Slovenija na nacionalni ravni ali bo zaprosila za pomoč mednarodne organizacije. Kot zamišljeno v kibernetski politiki NATA (NATO, 2011), zavezništvo zagotavlja usklajeno pomoč v kibernetski obrambi, če je kateri koli zaveznik žrtev kibernetskega napada. Tovrstna kolektivna obramba je predmet odločitve Severnoatlantskega sveta. Slovenski uradni zahtevek NATU bi moralo odobriti zakonodajno telo, to je parlament, prav tako kot v klasičnem ogrožanju varnosti. Vsak kibernetski napad, pri katerem bi sodelovali slovenski državljani, potrebuje parlamentarno odobritev, podobno kot katera koli druga mednarodna misija in pod pogojem, da Slovenija dosega minimalne standarde za sodelovanje v mednarodni misiji. Posledično avtorica zagovarja stališče, da se pravila kibernetskega bojevanja izvajajo iz vojnega prava, predvsem ius in bello, ius ad bellum.

Izhajajoč iz predpisov in zahtev, ki jih na članice naslavljata NATO in EU, velja eksplicitno izpostaviti zaključno ugotovitev raziskave, da je slovensko strategijo potrebno zasnovati na nacionalnih ciljih kibernetske obrambe. Podrejeno strategiji pa tudi pravno-formalno vzpostaviti CERT MORS in čim prej opredeliti kritično infrastrukturo, čeprav celoten seznam verjetno ne bo javno dostopen. Vpoklic rezervne sestave z ustrezno usposobljenostjo in spretnostmi ni izključen. Zaradi te možnosti se bo potrebno sistematično lotiti bitke za talente in odkriti, kje je največja koncentracija talentov in sposobnosti – na univerzah, v zasebnih varnostnih družbah, v zasebnih razvojnih podjetjih ali kje drugje.

Civilna družba kot determinanta strateške kulture igra pomembno vlogo pri vzpodbujanju vrednot na področju nadzora kibernetskega prostora, pri odnosu do tehnologije in v modernizaciji družbe. V odnosu do regije kot akterja v globalnem upravljanju pa bodo Evropejci in Slovenci morali premisliti, kakšna je evropska strateška kultura in kakšen koncept globalne varnosti podpira: bipolarno ureditev z nasprotujočima poloma ZDA in Kitajsko, multilateralizem v Varnostnem svetu ali dogovore izven organov mednarodne skupnosti v skupinah držav kot so G8, G20 in ad hoc koalicije. Katero pot bo izbrala kot najustreznejšo, je odvisno tudi od trdnosti evropskih institucij in od tega, kje se bo nahajala moč v nadaljevanju evropske integracije: v Evropskem svetu oziroma med vladama Nemčije in Francije ali v Skupni zunanji in varnostni politiki oziroma ali bo Velika Britanija pripravljena prenesti institucionalni položaj zmagovalne sile v 2. svetovni vojni na evropske institucije. Med obstoječimi alternativami malim državam najbolj ustrezata multilateralizem in verodostojna Skupna zunanja in varnostna politika (Zanders, 2009).

Civilna družba z nezaupanjem spremlja spodbujanje zasebnega sektorja k policijskemu nadzorovanju spleta, v angleščini »internet policing«, zanjo patruljiranje na spletu ni sprejemljivo. Ideja varnosti je najtesneje povezana z obstoječimi in preteklimi politikami in je prepletena s prevladujočimi vrednotami nacionalnega varnostnega aparata. Deibert navaja, da je po drugi strani civilna družba največkrat povezana s spoštovanjem pravic, demokracije, raznolikosti in odprtosti. Patruljiranje na spletu se opravičuje z varnostjo skupnosti, pri čemer v Sloveniji še ni jasno, v kolikšni meri civilna družba podpira več državne varnosti na škodo zasebnosti posameznika. Občutljivost glede državljanskih svoboščin ima korenine v izkušnji avtoritarnega nadziranja komunikacij; preroško so jo opredmetili pisci Ustave.

Med regionalnimi aktivnostmi so pomembne dejavnosti na področju informacijske družbe, sodelovanje policije v Europolu (EC3 v Hagu), sodelovanje nacionalnih CERT-ov (ENISA v Heraklionu), in Natov Center odličnosti za kooperativno kibernetično obrambo (CCD COE v Talinu). Poleg nacionalnih strateških kultur in strateških kultur nasilnih nedržavnih akterjev, bomo morali upoštevati še strateško obnašanje Evropske unije – Kakšna je njena kolektivna identiteta in katere vrednote se spreminjajo v politike?

Razvoj mednarodnih norm in povečanje števila mednarodnih omrežnih incidentov z državnimi sponzorji silita nacionalne odločevalce in zakonodajalce k oblikovanju kibernetskega varnostnega sistema, ki bo omogočal državam, da sodelujejo v mednarodnih dejavnostih. Nacionalne elite so odgovorne za pobudo razvoja lastnih kibernetskih sposobnosti in s tem za razvoj kibernetske moči države. Kratkoročno in oprijemljivo pa gre za vzpostavljanje nacionalnih zmogljivosti za obvladovanje mrežnih incidentov, ki se bodo lahko vključevale v mednarodne skupine.

Viri

- Council of Europe. (2001). Konvencija o kibernetski kriminaliteti. Uradni list RS, št. 17/2004, 4205-4224. Pridobljeno 12.9.2012 na http://www.uradni-list.si/_pdf/2004/Mp/m2004062.pdf.
- Council of Europe. (2011). Cybercrime and Cyber Security Strategies: Report. Pridobljeno 12.9.2012 na http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/WS3_a_seger_strategies.pdf.
- Čaleta D., Rolih G.(2011). Cyber Security in the Operation of Critical Infrastructure – An Analysis of the Situation in the Field of Slovenian Defence. Sodobni vojaški izzivi,13(3).
- Deibert R. (2012). Towards a cyber security strategy for global civil society? Pridobljeno 12. 9. 2012 na http://giswatch.org/sites/default/files/gisw_- _towards_a_cyber_security_strategy.pdf.

- European Parliament. (2009). Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU: Study. Pridobljeno 12. 9. 2012 na http://www.evi.ee/lib/cyber.pdf
- International Strategy For Cyberspace. Prosperity, Security, and Openness in a Networked World. (2011). Pridobljeno 20. 6. 2012 na http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
- International Telecommunication Union. (2011). ITU National Cyber Security Strategy Guide. Pridobljeno 20. 6. 2012 na http://www.itu.int/ITU-D/cyb/cyber security/docs/ITUNationalCyber securityStrategyGuide.pdf.
- International Telecommunication Union. (2009). Self Assessment Toolkit. Pridobljeno 20. 6. 2012 na http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf.
- Johnson L., Larsen J. (2006). Comparative Strategic Cultures. Pridobljeno 12. 9. 2012 na http://www.fas.org/irp/agency/dod/dtra/syllabus.pdf.
- Lewis J. A., Timlin K. (2011). Cyber Security and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization. Pridobljeno 20. 6. 2012 na http://unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.
- Maurer T. (2011). Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security. Pridobljeno 20. 6. 2012 na http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.
- Melzer N. (2011). Cyberwarfare and International Law. Pridobljeno 12. 9. 2012 na http://unidir.org/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf.
- NATO. (2011). Defending the Networks. The NATO Policy on Cyber Defense.
- Nye J.S. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly 5(4): 18-38. Pridobljeno 12. 9. 2012 na http://www.au.af.mil/au/ssq/2011/winter/nye.pdf.
- Praprotnik G., Podbregar I., Bernik I,. Ticar B. (2012) A Slovenian Perspective on Cyber Warfare. Cyber Conflict. Competing National Perspectives, Edited by Daniel Ventre, CNRS, France. V izhajanju.
- Schreier, F. (2012). On Cyberwarfare. Pridobljeno 20. 6. 2012 na http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf
- Team Register. (2012). Source Code Smoking Gun Links Stuxnet AND Flame. Pridobljeno 20. 6. 2012 na http://www.theregister.co.uk/2012/06/12/stuxnet_flame_links_discovered_by_security_researchers/.
- Zanders J.P. (2009). What Role For CFSP? Pridobljeno 20. 6. 2012 na http://www.iss.europa.eu/uploads/media/Report_cyber_security_1_.pdf

O avtorici

Adriana Dvoršak, mag. mednarodnih odnosov, Institut NOVUM, Ljubljana.

Kibernetska mimikrija kot kaznivo dejanje

Zoran Cunk

Računalniške sisteme vedno pogosteje uporabljamo za komuniciranje. Kibernetska mimikrija kot izrazna oblika človeške mimikrije pri komuniciranju med uporabniki računalniških sistemov v kibernetskem prostoru se pojavlja tudi z namenom izvrševanja kaznivega dejanja. Tako posredna kot neposredna kibernetska mimikrija lahko s svojimi pojavnimi oblikami prehajata čez črto dovoljenega na področje potencialnega kaznivega dejanja, hkrati pa odpirata vprašanje opredelitve prepovedane kibernetske mimikrije v prihodnosti. Slovenija ima v svoji kazenskopravni zakonodaji opredeljena kazniva dejanja, ki izpolnjujejo zahteve Konvencije o kibernetski kriminaliteti in ki jih je z določili KZ-1 mogoče opredeliti kot nedovoljeno in sankcionirano kibernetsko mimikrijo. Omejili smo se na kibernetsko mimikrijo pri kaznivem dejanju, ob strani pa smo pustili prav tako pomembno kibernetsko demimikrijo, ki tudi lahko izpolnjuje vse znake kaznivega dejanja. Čeprav smo se pri obravnavi problema kibernetske mimikrije kot kaznivega dejanja osredotočili na računalniške sisteme kot sredstva komunikacije v kibernetskem prostoru, je mogoče ugotovitve smiselno uporabiti tudi pri obravnavi drugih (mobilnih, socialnih) omrežjih, ki omogočajo stalno povezljivost in komunikacijo.

KLJUČNE BESEDE: kibernetski prostor, komunikacija, (ne)posredna kibernetska mimikrija, kaznivo dejanje

1 Uvod

Pogačnik obravnava inteligentnost človeka kot sposobnosti živih bitij za obdelovanje informacij na način, ki je zanje nov (Pogačnik, 1995). Pri definiranju bistvenih revolucionarnih pridobitev umskih sposobnosti, kot četrto mentalno revolucijo v procesu antropogeneze človeka, opredeljuje zunanje obdelovanje informacij (računalnik) ter človeka te dobe imenuje človeka informacijske dobe (ibid.).

Temeljna značilnost informacijske tehnologije, kot pojavnega znanilca informacijske dobe, je kompleksnost celote postopkov in naprav za oskrbovanje uporabnika s potrebnimi podatki. Računalniški sistemi so v informacijski dobi bistveni proizvodi informacijske tehnologije. V nadaljevanju bomo računalniški sistem obravnavali v skladu z definicijo Konvencije o kibernetski kriminaliteti (v nadaljevanju Konvencija) (2004), ki jo je skupaj z Dodatnim protokolom h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v računalniških sistemih (v nadaljevanju Dodatni protokol h Konvenciji), ratificirala tudi Slovenija. Tako je računalniški sistem vsaka naprava ali skupina med seboj povezanih ali soodvisnih naprav, od katerih ena ali več samodejno obdeluje podatke s pomočjo programa (a alineja 1. točke Konvencije).

Področja uporabe računalniških sistemov so dobesedno brezmejna, (vedno bolj) pogosto pa jih uporabljamo tudi za komuniciranje. Komunikacija kot proces sporočanja in sprejemanja informacij oz. izmenjava informacij med ljudmi je za človeka tako pomembna, da ga lahko imenujemo »hommo communicus« (Trček, 1994). Hommo communicus uporablja za večanje hitrosti in učinkovitosti prenosa informacij s hkratno zahtevo po usklajevanju in povezovanju informacij z različnih področij, s tem pa tudi komuniciranja na različnih ravneh, prav računalniške sisteme in to pogosto v t.i. kibernetskem prostoru (cyberspace). Kibernetski prostor na splošno opisuje nematerialno okolje, ki ga računalniški sistemi ustvarjajo in vzdržujejo (Pahor, 2002). Tako okolje je npr. okolje elektronske pošte, v katerem se ljudje med seboj pisno sporazumevajo, ali pa svetovni splet (internet). Zgolj za ponazoritev pomembnosti komuniciranja po internetu naj navedemo, da je internet postal uporaben medij v tolikšni meri, da je postala družba od njegovega delovanja do določene mere celo odvisna (Bratuša, 2006). Ob tem je potrebno poudariti, da kibernetski prostor omogoča tako glasovno besedno, glasovno nebesedno (pošiljanje sporočil prek fonetike in parajezika), neglasovno besedno (sporočanje s pisavo) in nebesedno neglasovno (slike, sončki) komunikacijo, in to v posebnem – umetno ustvarjenem okolju. Kibernetski prostor lahko udeležencem zagotavlja tudi virtualno realnost. Osnovni značilnosti te virtualne realnosti sta t.i. virtualni prostor, ki udeležencem omogoča, da so med procesom komunikacije na geografsko ločenih lokacijah, hkrati pa od uporabnika ne zahteva, da je namen sodelovanja v komunikaciji oblikovan vnaprej, ampak je lahko ta namen povsem nov in se pojavi šele v virtualni realnosti (Praprotnik, 2003).

Praprotnik (2003) ugotavlja, da računalniško posredovana komunikacija oz. vsaj nekateri njeni partikularni tipi »… udeležencem omogočajo anonimnost; v anonimni komunikaciji se lahko predstavijo tako, kot se želijo, torej si ustvarijo

novo, tako imenovano virtualno identiteto.« Ne glede na to ali je ustvarjanje nove identitete varovalo za zagotavljanje informacijske zasebnosti ali pa sredstvo, s katerim bo uporabnik bodisi preslepil, prevaral in/ali celo izkoristil uporabnika (oziroma informacije o njem), s katerim računalniško komunicira, pa lahko trdimo, da za to uporabniki računalniške komunikacije uporabljajo v kibernetskem prostoru tudi določen način »izkrivljanja« realnosti – mimikrijo. Mimikrija (ang. mimicry – posnemanje) je pojav v zoologiji: rastline in živali se po obliki, z varovalno barvo ali vedenjem prilagodijo okolici (rastlini ali živali) in se tako prikrijejo sovražniku ali ga prestrašijo Tako npr. užitne živali postanejo neužitne, roparice plen, nenevarne vrste pa posnemajo nevarne vrste (Leksikon Sova, 2006). Znanstveniki so začeli preučevati mimikrijo živali v 19. stoletju v porečju Amazonke. Ugotovitve na področju naravoslovnih ved so hitro utrle pot preučevanju mimikrije v družboslovju. Tako igra mimikrija posebno vlogo v diskurzu filozofije, jezikoslovja, literature in psihoanalize (Becker, Doll, Wiemer in Zehner, 2008). Prehod iz naravoslovja nakazuje tudi bistveno razliko pri obravnavi mimikrije živali in človeške mimikrije. Smrke (2002), ki je pri nas utrl preučevanje družbene – človeške mimikrije, poudarja, da je živalska mimikrija predvsem (čeprav ne vedno izključno) v območju genetike, medtem ko je človeška mimikrija predvsem (pa tudi ne vedno izključno) v območju kulture. Glede na dejstvo, da kulturo sestavljajo samo tisti človekovi izdelki in dejanja, ki so povnanjeni, objektivno materializirani (Flere, Marjanović in Markov, 1992), kultura nedvomno vsebuje tudi izrazno področje kibernetske mimikrije.

2 Kibernetska mimikrija – sestavina igre, posla ali kaznivega dejanja

Tomc (2000) ugotavlja, da se človek med bitji s kulturo odlikuje po zavestnem polaščanju prostora in časa. Kot drugo in novejšo (za telesnim prostorom) raven doživljanja prostora opredeljuje doživljanje socialnega prostora drugih (ibid.). Ena od oblik doživljanja socialnega prostora drugih je nesporno tudi kibernetski prostor, ki tako predstavlja kulturni medij, s katerim konstruiramo (kibernetsko) socialno skupnost. V našem primeru kibernetsko okolje kot prostorsko in časovno specifično definirano okolje omogoča/vzpodbuja/zahteva določeno vrsto človeške mimikrije – kibernetsko mimikrijo. Kibernetska mimikrija je pojavna oblika človeške mimikrije. Človeška mimikrija je tako delovanje posameznika ali različnih družbenih skupin, v katerih se skuša z različnimi oblikami pretvarjanja

povečati možnost uspeha oz. zmanjšati možnosti neuspeha v družbenem ali naravnem okolju (Smrke, 2007). Znanstveniki poudarjajo, da je za pravilno obravnavo človeške mimikrije (torej tudi kibernetske), nujno potrebno ločevati nekatere druge oblike človeškega pretvarjanja. Najpogosteje prihaja do zamenjave mimikrije z mimezo. Pojem mimeze, ki se je sicer prvič pojavil v 5. stoletju p.n.š., je tako prvenstveno močneje povezan s telesom in njegovim zunanjim videzom, v novejšem času pa je še močneje povezan z oponašajočo reprezentacijo slike (Becker idr., 2008). Novak (2007) posebej poudarja, da je treba razlikovati med posnemanjem (gr. mimesis) in mimikrijo kot pretvarjanjem, saj samo posnemanje še ni namerno pretvarjanje v smislu prevare, ker ne pomeni nujno odvisnosti od drugih. Na to napotuje tudi Smrke (2007), saj jasno opredeli, da posnemanje (imitacija) ni mimikretična akcija. Posnemovalec s svojim delovanjem ne meri na noben naravni ali človeški/družbeni subjekt, ki naj bi bil v vlogi operaterja in zatorej ni njegov namen v očeh nekega operaterja vzbuditi določeno zamenjavo z določenim modelom (ibid). Smrke pa tudi jasno ločuje oz. povezuje mimikrijo in simulacijo. Če je simulacija umetno ustvarjanje določenih situacij, da bi se v pogojih kontroliranih dejavnikov/parametrov raziskalo določene možne učinke določenih delovanj v umetnem okolju, govorimo o nemimikretični simulaciji, če pa to izvedemo v realnem svetu, lahko govorimo o mimikretični simulaciji (ibid).

Becker idr. (2008) za človeško mimikrijo ugotavljajo, da se pri njenem obravnavanju ves čas pojavljajo vprašanja različnih konceptov identitete, podobnosti, namembnosti, uporabnosti mimikrije. S tem vnašajo v obravnavo napetost med uporabo prisile za zagotovitev vnaprej določenih zakonitosti človeškega delovanja in upoštevanjem polja človeške svobode. To pa nesporno velja tudi za kibernetsko mimikrijo. Ugotavljali smo že (Cunk, 2011 in 2012), da uveljavljena filozofska disciplina – etika, in v okviru nje izoblikovana informacijska etika (Johnsonova (2001) govori celo o »virtualni etiki«), ne ustrezata sliki dejanske uporabe v vsakdanjem življenju. Zato številne civilnopravne norme s svojo zgodovinsko utemeljeno funkcijo varstva uporabnika informacijske tehnologije kot posebej zaščitenega udeleženca ustvarjanja, uporabe in hranjenja podatkov in informacij, določajo minimum pravic informacijske zasebnosti. Kibernetska mimikrija torej lahko krši določena etično-moralna stališča družbe, kateri uporabnik pripada. Lahko pa tudi izpolnjuje zakonsko opredeljene določbe, ki so v končni fazi (s pravnomočno sodbo sodišča) opredeljeni kot najtežje kaznivo ravnanje – kaznivo dejanje. Z osredotočenostjo na obravnavo kibernetske mimikrije kot kaznivega dejanja (v nadaljevanju kibermimikrije), lahko opredelimo naslednje vloge in elemente mimikretičnega odnosa kibermimikrije (prirejeno po Smrke, 2007):

- kibermimik je tisti akter mimikretičnega odnosa/akcije, ki skuša kot uporabnik računalniškega sistema s komunikacijo v kibernetskem prostoru iz takšnih ali drugačnih razlogov vzbuditi vtis o enakosti/istosti z določenim modelom z namenom doseganja določenega mimikretičnega cilja;
- operator je tisti akter, ki mu je namenjeno kibermimikovo delovanje;
- model je stvaren ali nestvaren pojav, ki ga kibermimik posnema;
- mimem je celota več posamičnih posredovanih informacij kibermimika operatorju, ki jim pravimo signal, s katerimi poskuša kibermimik pri operatorju vzbuditi zamenjavo z modelom; in
- mimikretičen cilj je cilj, ki ga želi doseči kibermimik in je njemu večinoma bolj ali manj jasen, prikrit pa bi naj bil operatorju.

Poudariti je potrebno, da vsaka kibernetska mimikrija kot zavestno človekovo dejanje ni kazenskopravno sankcionirana (torej ni kibermimikrija). Ob tem pa je potrebno upoštevati, da se ravno pri potencialnih kaznivih dejanjih kibermimikrije operator lahko nahaja tudi v vlogi:

- igralca v kibernetski igri, ki že vnaprej ali v sami igri predvideva in dovoljuje kibernetsko mimikrijo kot bistven element igre. Kibernetsko igro v tem primeru lahko označimo kot vsako urejeno dejavnost, ki je sama sebi namen in ne stremi k neki koristni modifikaciji realnega (Benveniste, 2001). Strehovec (2003) opisuje bistvene lastnosti internetske igre opazovane s stališča tradicionalne teorije iger, ki pa jih lahko opredelimo tudi kot lastnosti kibernetske igre: bistvena je njihova ločitev od vsakdanjega življenja, izločitev iz njegovega prostora in časa in prehod na igrišče kot prav posebno strukturiran prostor igre in v intenzivni čas igrinega dogajanja. Kibernetska igra naj bi tako s svojo negotovostjo in rizičnostjo, ki sodita v današnjo kulturo, uporabniku priskrbela tudi pakete dražljajev izjemne negotovosti, tveganja in zgoščenih naključnih situacij (ibid.).
- Hommo oeconomicusa v procesu gospodarjenja, ko zasleduje le racionalno obnašanje (tako kibermimika kot operatorja). Pri popolnoma racionalnem obnašanju obeh ekonomskih subjektov bosta torej oba delovala premišljeno, brez upoštevanja čustev, navad in predsodkov ter težila k uresničitvi zastavljenih ciljev, praviloma z izhodiščem na svojih sebičnih nagibih. Osnovni kriterij doseganja cilja je torej ekonomski kriterij. Pri vsem tem ekonomsko

mimikrijo opredelimo kot doseganje ali poizkušanje doseganja ekonomskih ciljev z mimikretično akcijo (Smrke, 2007). Smrke tudi poudarja, da ekonomska teorija že vključuje ključni pojem, ki se tiče mimikrije – pojem informacijske asimetrije. Določen ekonomski vidik cilja mimikrije pa opredeljuje tudi Novak (2007), ki kot bistveno lastnost mimikrije določa njeno prekoračenost obstoječih meja. Hkrati trdi, da je mimikrija posledica inflacije, ker človek posnema druge zaradi določene koristi oz. profita, hkrati pa z mimikrijo posameznik (ne)upravičeno spoznava drugo bit kot svojo.

KZ-1 (2008) opredeljuje kaznivo dejanje kot človekovo protipravno dejanje, ki ga zakon zaradi nujnega varstva pravnih vrednot določa kot kaznivo dejanje in hkrati določa njegove znake ter kazen za krivega storilca (člen 16. KZ-1). Kibermimik izpolnjuje elemente kaznivega dejanja s kibernetsko mimikrijo, ko v razraščajočem se kibernetskem prostoru izvaja (Smrke, 2007):

- Katero koli mimikrijo področij človeškega delovanja (ekonomskega, političnega, zdravstvenega itn.), katerih medij pojavljanja oz. izražanja je kibernetski, in
- povsem specifično mimikrijo, ki se nanaša na različne mimikretične tehnike delovanja kibernetskih virusov, hekerstva ipd.

Da je kibernetska mimikrija kazenskopravno sankcionirana, morajo biti izpolnjene naslednje bistvene vsebinske značilnosti kibermimikrije:

- Operatorjev status oškodovanca v postopku kibernetske mimikrije: Ne glede na dejstvo, ali je kibermimik storil kaznivo dejanje, ki se preganja na zasebno tožbo, na predlog oškodovanca ali je kaznivo dejanje uradno pregonljivo, je za ustrezen zaključek kazenskega postopka izredno pomembna sama odločitev operatorja, ali ga je kibermimik s kaznivim dejanjem oškodoval. Oškodovanec je oseba, ki ji je bila s kaznivim dejanjem kršena ali ogrožena katera koli njena osebna ali premoženjska pravica (144. člen ZKP, 2004). Poudariti je potrebno, da je vsaj pri kaznivih dejanjih, ki se preganjajo na zasebno tožbo in pri kaznivih dejanjih, ki se preganjajo na predlog, bistvena izrazna oblika statusa oškodovanca – podana ovadba. Nekoliko drugače je na področju kaznivih dejanj, ki so uradno pregonljiva. Praviloma se ta dejanja preganjajo tudi takrat, ko jih pristojni državni organ zazna samoiniciativno in sproži ustrezni postopek. V praksi pa se tudi zgodi, da se postopek, ker se operator ne prepozna v vlogi oškodovanca, zaključi v »dobro« kibermimika.

- Neločljivo povezano z obravnavo statusa oškodovanca operatorja pa je tudi kibermimikovo (ne)spoštovanje bistvenega kriterija – vrednot družbe, ki jih ta zaščiti z določili kazenskega prava. Kibermimikove aktivnosti, sicer izvedene v skladu z jasno postavljenimi pravili in kriteriji igre ali gospodarjenja, lahko z izpolnjevanjem elementov tridelnega koncepta splošnega kaznivega dejanja – človekovega voljnega ravnanja, ki izpolnjuje bit kaznivega dejanja, protipravnosti in storilčeve krivde – določijo kibermimikrijo kot točno določeno kaznivo dejanje. Ob tem je potrebno tudi upoštevati, da človekovo resnično bit oblikuje zgradba njegovega značaja, ki predstavlja resnični vzgib njegovega vedenja, da pa se njegovo vedenje (lahko) razlikuje od njegovega značaja (Fromm, 2004). Takrat pa njegovo vedenje le delno odslikava njegovo bit, ki je navadno le krinka, ki jo nosi zaradi njegovih lastnih namenov (ibid.). Ravno kibernetski prostor pa kibermimiku omogoča velike možnosti za drugačno prikazovanje njegove prave biti – ne samo virtualne podobe, temveč tudi njegovega motiva za izvedbo mimikrije.

Poseben problem pa pri dokazovanja kaznivega dejanja predstavlja »dešifriranje« kibermimikove virtualne identitete. Završnik (2009) poudarja, da se pri obravnavi t.i. kibernetskih kaznivih dejanj, več ne moremo naslanjati na biometrijo, kjer je telo edino relevantno za identifikacijo in avtentikacijo subjekta (storilca), saj v kibernetskem prostoru telesa ni in je pomemben le posameznikov digitalni dvojnik. Če torej prenesemo že omenjeno Smrketovo definicijo človeške mimikrije na področje kibermimikrije, jo torej lahko izrazimo kot izrazno obliko človeške mimikrije, ki predstavlja tako delovanje posameznika ali različnih skupin (kibermimik), ki upravljajo z računalniškim sistemom v specifičnem družbenem okolju – kibernetskem prostoru, v katerem se skuša z različnimi oblikami pretvarjanja povečati možnost uspeha oz. zmanjšati možnosti neuspeha izvedbe kaznivega dejanja. Kibermimikova mimikrija je tako pri teh kaznivih dejanjih lahko uperjena posredno na operatorja (prek računalniškega sistema, ki ga ta uporablja) ali pa je (z računalniškim sistemom) namenjena neposredno operatorju (direktnemu komuniciranju).

2.2 Posredna kibermimikrija in njene pojavne oblike

Kot posredno kibermimikrijo lahko opredelimo (praviloma) naklepna ravnanja kibermimikov, ki v modelu nezainteresiranega uporabnika kibernetskega prostora poskušajo oz. izvedejo iz svojega (oz. tistega, ki ga uporabljajo) računalniškega sistema v kibernetski prostor (redkeje točno določenemu operaterju) mimikretično

akcijo in v računalniški sistem (ne)identificiranega operatorja, prenesejo mimem z zatajenim signalom, ki prikriva operatorju namero kibermimika o trajnem ali začasnem vstopu in namestitvi programa v kibernetski prostor oz. računalniški sistem operatorja, s funkcijo prestreznika iskanih informacij o operatorju.

Praviloma poznamo dve možnosti prikritja signala operatorju, in sicer:

- operatorjev računalniški sistem operaterju sploh ni prikazoval mimema – celote zatajenega signala, ali pa jih operater ni zaznal (mimem sestavljajo izključno zatajeni signali – skupek disimulacij);
- operator je prejel mimem, ki je poleg mimikretičnih signalov (simulacij neškodljivih sporočil), vseboval tudi zatajene signale (skupek disimulacij – računalniškega programa), ki so omogočili »domovanje« mimema v računalniškem sistemu.

To dejavnost izvaja kibermimik čimbolj ali v celoti prikrito. Čeprav je kot prvenstven mimikretičen cilj kibermimika nakazan računalniški sistem oz. kibernetski prostor operatorja, pa je to zgolj navidezno. Kibermimika zanimajo bolj ali celo samo arhiv/dejavnosti/aktivnosti operatorja, kot prinašalci koristnih informacij o operatorju. Torej »o svojem domovanju (navzočnosti/odsotnosti) slepi« računalniški sistem in s tem posredno operaterja.

Bistvene oblike kazenskopravne kibermimikrije je mogoče razbrati iz dela kazenskega materialnega prava Konvencije (2004) (Naslov 1 Konvencije), ki obravnava kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov. Iz tega dela Konvencije je mogoče opredeliti, katera so tista naklepna posredna kibermimikova dejanja, ki jih je mogoče opredeliti kot kaznива dejanja. Ta so:

- protipraven dostop: neupravičen vstop v računalniški sistem ali njegov del (2. člen Konvencije);
- protipravno prestrezanje: neupravičeno prestrezanje nejavnih prenosov računalniških podatkov s tehničnimi sredstvi do računalniškega sistema, od njega ali v njem, vključno s prestrezanjem elektromagnetnega sevanja računalniškega sistema, s katerim se taki računalniški podatki prenašajo (3. člen Konvencije);
- motenje podatkov: poškodovanje, izbris, poslabšanje, spreminjanje ali oviranje računalniških podatkov (4. člen Konvencije);

- motenje sistemov: resno, neupravičeno oviranje delovanja računalniškega sistema z vnosom, prenosom, poškodovanjem, izbrisom, poslabšanjem, spreminjanjem ali oviranjem računalniških podatkov (5. člen Konvencije); in
- zloraba naprav: z namenom zlorabe za storitev kaznivih dejanj protipravnega dostopa, protipravnega prestrezanja, motenja podatkov in motenja sistemov, izdelovanje, prodaja, dajanje v uporabo, uvažanje, distribuiranje ali zagotavljanje na drug način:
  - naprav, vključno z računalniškimi programi, zasnovanih ali prilagojenih predvsem za storitev zgoraj navedenih kaznivih dejanj,
  - računalniških gesel, kod ali podobnih podatkov, ki omogočajo dostop do računalniškega sistema ali katerega koli njegovega dela (6. člen Konvencije).

Kazniva dejanja, ki jih s tem stori kibermimik, spadajo med t.i. kazniva dejanja, povezana z integriteto informacijskega sistema in podatkov ter sodijo v področje kibernetske kriminalitete v ožjem smislu. Kibernetska kriminaliteta v ožjem smislu tako vključuje kriminaliteto, ki ogroža informacijsko in omrežno varnost, objekt kazenskopravnega varstva pa so informacijski sistemi in računalniški podatki (Završnik, 2007). V Sloveniji lahko med kazniva dejanja, ki sodijo v kibernetsko kriminaliteto v ožjem smislu, uvrstimo:

- Napad na informacijski sistem po 221. členu KZ-1(2008) (kot izhodiščno kaznivo dejanje zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov z različnimi oblikami protipravnega dostopa, protipravnega prestrezanja, motenja podatkov in motenja sistemov).
- Vdor v poslovni informacijski sistem po 237. členu KZ-1 (kot specialno obliko predhodnega kaznivega dejanja, t.i. industrijsko vohunstvo).
- Zlorabo osebnih podatkov po 2. in 5. odstavku 143. člena KZ-1 (obravnava naklep pri storitvi sicer drugega temeljnega kaznivega dejanja, kjer pa je namen vdora pridobitev osebnih podatkov).
- Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje po 306. členu KZ-1 (kot pripravljalno dejanje, vendar opredeljeno kot samostojno kaznivo dejanje).

Sodna praksa sicer kaže, da je odkritih in procesuiranih kaznivih dejanj kibernetske kriminalitete v ožjem smislu relativno malo, nedvomno pa je ob teh podatkih o gibanju kaznivih dejanj nujno potrebno upoštevati veliko območje neraziskanih in neodkritih kaznivih dejanj (Cunk, 2011 in 2012).

2.3 Neposredna kibermimikrija in njene pojavne oblike

Kot neposredno kibermimikrijo lahko opredelimo (praviloma) naklepno usmerjena (merijo na točno določenega uporabnika) ali neusmerjena (ne merijo na posebnega uporabnika) ravnanja kibermimikov, s katerimi poskušajo izvesti oz. izvedejo iz svojega (oz. tistega, ki ga uporabljajo) računalniškega sistema, v kibernetski prostor (redkeje točno določenemu operaterju) mimikretično akcijo in s pomočjo računalniškega sistema (ne)identificiranega operaterja, prenesejo mimem z mimikretičnim signalom, ki vsebuje dezinformacijo o mimiku ali mimikretičnem cilju. Medtem ko je pri posredni kibermimikriji kibermimik prikrival svojo navzočnost in zainteresiranost za lastnosti operatorja, ter se zato osredotočil na računalniški sistem z namenom prikritja odkrite in neposredne komunikacije, pa bo v primerih neposredne kibermimikrije računalniški sistem uporabljal »le« kot sredstvo za prikaz modela operatorju in torej za vidno/udejanjeno »neposredno« obliko prenosa mimikretičnega signala.

Iz omenjene Konvencije (2004) je prav tako mogoče opredeliti, katere so bistvene izhodiščne oblike kazenskopravne kibernetske mimikrije, ki jih je mogoče opredeliti kot kazniva dejanja neposredne kibermimikrije:

- Kazniva dejanja, povezana z računalnikom: računalniško ponarejanje, računalniška goljufija (Naslov 2 Konvencije).
- Kazniva dejanja, povezana z otroško pornografijo (Naslov 3 Konvencije).
- Kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic (Naslov 4 Konvencije).
- Kazniva dejanja razširjanja rasističnega in ksenofobičnega gradiva v računalniških sistemih, rasistična in ksenofobična grožnja, rasistična in ksenofobična grožnja ter zanikanje, hujše zmanjševanje pomena, odobravanja ali zagovarjanje genocida ali hudodelstev zoper človečnost (Dodatni protokol h Konvenciji).

Konvencija opredeljuje le nekatera kazenskopravno prepovedana pojavna dejanja kibermimikov. Upoštevati pa moramo, da je navedenih delitev kaznivih

dejanj iz področja kibernetske kriminalitete v širšem smislu več. Za ponazoritev si poglejmo delitev kibernetske kriminalitete, kot jo opredeljuje Yar (2006): politični haking in kibernetski terorizem, virtualno piratstvo, kibernetske goljufije, ilegalna, škodljiva in žaljiva ravnanja od sovražnega govora do otroške pornografije, kibernetsko zalezovanje in pedofilija. Ob tem je potrebno poudariti, da nastajajo vedno nove oblike možnih grupacij posameznih kaznivih dejanj s skupnimi značilnostmi (npr. kazniva dejanja kibernetskega medvrstniškega nasilja ipd.). Kakor koli že, kazniva dejanja, ki jih z neposredno kibermimikrijo stori kibermimik spadajo med t.i. kazniva dejanja, pri katerih je cilj ali sredstvo informacijsko komunikacijska tehnologija in sodijo v področje kibernetske kriminalitete v širšem smislu. Pri kibernetski kriminaliteti v širšem smislu so objekti kazenskopravnega varstva izredno heterogeni: poleg varstva elektronskih komunikacijskih omrežij in podatkov, lahko vanjo uvrstimo vsa kazniva dejanja, ki so izvršena zoper informacijski sistem ali z njegovo pomočjo, kjer je informacijski sistem orodje ali tarča kaznivega dejanja (Završnik, 2007).

Dandanes je uporaba računalniških sistemov že nuja v vsakdanjem življenju, in sega na vsa področja človeškega udejstvovanja. Ravno zaradi tega je mogoče trditi, da računalniške sisteme lahko uporabljajo kibermimiki za izvedbo prav vsake pojavne oblike kaznivega dejanja. Na to opozarja že Smrke (2007) v opredelitvi definicije izpolnjevanja elementov kaznivega dejanja s kibernetsko mimikrijo (»… katero koli področje človeškega delovanja«). V »najbolj blagi« obliki mimikrije opredelimo sicer še kot sredstvo potencialno nekaznivih oblik pripravljalnih dejanj, ki pa kasneje lahko bistveno pripomorejo k dokazovanju naklepa kibermimika za storitev kaznivega dejanja. Zato lahko med kazniva dejanja, ki sodijo v kibernetsko kriminaliteto v širšem smislu, poleg že opredeljenih in navedenih kaznivih dejanj iz konteksta kriminalitete v ožjem smislu, uvrstimo prav vsa kazniva dejanja iz KZ-1 (2008). Tudi tista, ki jih sicer opredeljujemo kot kazniva dejanja, t.i. splošne kriminalitete (npr. umor, rop, vlom ipd.). Glede na kibermimikov namen uporabe računalniškega sistema za izvedbo kaznivega dejanja bi lahko razdelili kazniva dejanja na kazniva dejanja, pri katerih:

- je računalniški sistem komunikacijsko sredstvo (npr. za komunikacijo različnih udeležencev pri kaznivem dejanju);
- računalniški sistem omogoča izvedbo pripravljalnih dejanj – (npr. spremljanje pogostosti ali vsebine informacij (sem na dopustu, ni več »prometa«));
- je računalniški sistem sredstvo za izvedbo kaznivega dejanja (npr. spravljanje operatorja v zmoto pri goljufiji, uporaba za ponarejanje listin ipd.).

3 Zaključek

Završnik (2007) ugotavlja, da je informacijska tehnologija človeštvu prinesla veliko koristi, hkrati pa so vzniknile tudi nove oblike kriminalitete. Pri kibernetski kriminaliteti lahko igra kibermimikrija pomembno oz. celo odločilno vlogo. Ob tem je potrebno upoštevati bistveno značilnost kibermimikrije – virtualno identiteto. Kibernetski prostor nedvomno omogoča uporabniku, da svoj jaz nenehno spreminja v skladu z načelom: »Sem takšen, kakršnega me želite.« To Fromm (2004) opredeljuje kot temeljno značilnost ljudi s tržnim značajem. Ta izraz povezuje tudi z odtujenim značajem, katerega bistvena značilnost je odtujenost od dela in samega sebe. Zanimivo pa je, da kot temeljno značilnost takšne osebe opisuje njeno kibernetično vero, s katero je človek (uporabnik) naredil sebe za boga, ker je pridobil tehnične zmožnosti za »drugo stvarjenje« sveta (ibid.). Dokler ima takšno poveličevanje sebe še pozitivno izrazno vlogo v igri in potencialno še pri gospodarskem poslu, pa je takrat, ko vodi v izvajanje kaznivih dejanj, popolnoma nesprejemljivo in nedovoljeno. Na to posebej dobro opozarja terminologija, ki jo pri obravnavi tega problema uporabljajo znanstveniki: informacijsko bojevanje, tretja svetovna vojna ipd. Znanje, pojavne oblike in značilnosti kibernetskega prostora omogočajo raznovrstnost izvedb kaznivih dejanj, naloga zakonodajalca pa je, da njihove značilnosti vpelje v kazensko procesno in kazensko materialno pravo. Pri vsem tem pa je potrebno upoštevati, da je sprejemanje zakonov neke vrste umetnost oz. veda, ki pa zahteva učenje in nadaljnje izpopolnjevanje (Igličar, 2012). To še posebej pride do izraza pri razmišljanju in izmenjavi mnenj strokovnjakov in znanstvenikov o tem, ali je smiselno opredeliti kaznivost nekaterih dejanj, oz. razmišljanju o možni sistematični izpustitvi dejanja iz cone kriminalnosti zaradi statusa in teže dejanja, ravno na področju kibernetske kriminalitete.

Kakor koli, še vedno je potrebno upoštevati dejstvo, da kazensko pravo kot ultima ratio societatis ne more biti primarni mehanizem za reševanje tega problema in se torej vseeno moramo vrniti k izhodiščnim pravilom (so)bivanja in usklajevanja ter potrjevanja »pravilnosti« kibernetske mimikrije, ki jih opredeljujejo etika in princip (so)odgovornosti. Navedeno pa predstavlja pomemben in velik izziv za prihodnost na tako pomembnem in pogosto uporabljenem področju človeškega (so)bivanja – v kibernetskem prostoru.

Viri

- Becker, A., Doll, M., Wiemer, S. in Zehner, A. (2008). »Einleitun«, in: dies.(Hg), Mimikry.
- Gefahrlicher Luxus zwischen Natur und Kultur, 7-27. Schliengen: Etition Argun.

- Benveniste, E. (2001). Igra kot struktura. Koper: Hyperion.
- Bratuša, T. (2006). Hekerski vdori in zaščita. Ljubljana: Pasadena.
- Cunk, Z. (2011). Kazenskopravni vidik varstva integritete informacijskega sistema in podatkov v Sloveniji: obdobje 2000-2009. Pravna praksa, 8 (3. 3. 2011), II-VIII.
- Cunk, Z. (2012). Slovenija in informacijska zasebnost ter kibernetska kriminaliteta v ožjem smislu v letih 2000-2010. V: I. Bernik in G. Meško (ur). Zbornik prispevkov konference Informacijska varnost: odgovori na sodobne izzive. Ljubljana: Fakulteta za varnostne vede. Pridobljeno 5. 7. 2012 na http://www.fvv.uni-mb.si/KonferencaIV/zbornik.html.
- Flere, S., Marjanović, M. in Markov, S. (1992). Uvod v sociologijo. Ljubljana: ČT Ur. list RS.
- Fromm, E. (2004). Imeti ali biti. Ljubljana: Vale-Novak.
- Igličar, A. (2012). Problemi zakonodajne politike. Pravna praksa, leto 31/1048, št. 26.
- Johnson, D.G. (2001). Computer Ethics (3rd Edition). New Jersey: Prentice-Hall, Inc. A
- Division of Pearson Education Upper Saddle River.
- Kazenski zakonik (KZ-1). (2008). Uradni list RS, štev. 55/2008 s spremembami in dopolnitvami.
- Konvencija o kibernetski kriminaliteti. (2004). Uradni list RS, MP 17/2004. Pridobljeno 18. 11. 2010 na www.soe.si/sl/dokumenti_in_publikacije/konvencije/185.
- Leksikon Sova. (2006). Ljubljana: Mladinska knjiga.
- Novak, B. (2007). Kaj pomeni mimikrija na področju edukacije? Pridobljeno 5. 7. 2012 na www.geocities.ws/nlpmojster/mimikrija.rtf.
- Pahor, D. (2002). Leksikon računalništva in informatike. Ljubljana: Pasadena.
- Pogačnik, V. (1994). Pojmovanje inteligentnosti. Radovljica: Didakta.
- Praprotnik, T. (2003). Skupnost, identiteta in komunikacija v virtualnih skupnostih. Ljubljana:
- Institutum Studiorum Humanitatis – Fakulteta za podiplomski humanistični študij.
- Smrke, M. (2002). Stare vešče – nova luč: religijske oblike družbene mimikrije v pogojih družbene tranzicije. Teorija in praksa let. 39/2, str. 170-181.
- Smrke, M. (2007). Družbena mimikrija. Ljubljana: Fakulteta za družbene vede.
- Strehovec, J. (2003). Umetnost interneta: umetniško delo in besedilo v času medmrežja. Ljubljana: Študentska založba.
- Tomc, G. (2000). Šesti čut: Družbeni svet v kognitivni znanosti. Ljubljana: Znanstveno in publicistično središče (Zbirka Sophia).
- Trček, J. (1994). Medosebno komuniciranje in kontaktna kultura. Radovljica: Didakta.
- Yar, M. (2006). Cybercrime and Society. London: SAGE Publications.

- Zakon o kazenskem postopku (ZKP). (2004). Uradni list RS, št. 63/2004 s spremembami in dopolnitvami.
- Završnik, A. (2007). Problemi kibernetske kriminalitete, V A. Šelih (ur.), Sodobne usmeritve kazenskega materialnega prava, 453-493. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

O avtorju

Zoran Cunk, univ. dipl. ekonomist, mag. znanosti s področja Ekonomije in poslovnih ved, višji kriminalistični inšpektor, Sektor kriminalistične policije Policijske uprave Maribor.

Enkripcija digitalnih podatkov – sodobni problem digitalnega dokazovanja

Miha Šepec

V prispevku obravnavamo enkripcijo digitalnih podatkov. Prikažemo enostavni postopek enkripcije digitalnih podatkov s programom TrueCrypt – brezplačnim programom z izredno kvalitetnim enkripcijskim algoritmom.

Namen prispevka je predstaviti težave, ki jih digitalna enkripcija povzroča kazenskemu pravu in organom pregona pri preiskovanju kaznivih dejanj. Glavni problem enkripcije je v dejstvu, da so na ta način zavarovani podatki praktično nedostopni preiskovalcem kaznivih dejanj – ti fizično ne morejo do podatkov, tudi če imajo sodno odredbo, ki jim to dovoljuje.

Do podatkov bi bilo sicer mogoče priti, če bi osumljena oziroma obdolžena oseba izdala geslo, s katerim so podatki zavarovani, vendar pa slovenska zakonodaja tega ne omogoča. Digitalni podatki, zaščiteni s TrueCrypt metodo bodo tako ostali nedotakljivi za preiskovalce kaznivih dejanj, s tem pa bo kazenski pregon potencialnih kaznivih dejanj izredno otežen, če ne praktično nemogoč.

V prispevku podajamo nekatere teoretične in praktične ugotovitve ter predlagamo spremembo kazenske zakonodaje, s katero bi organom pregona omogočili dostop do digitalnih podatkov, zaščitenih z enkripcijo, in s tem olajšali kazenski pregon kaznivih dejanj, povezanih z digitalnimi podatki.

1 Uvod

Živimo v digitalni družbi, v kateri so informacije in podatki ključnega pomena. Z željo po tajnosti informacij so se začeli razvijati enkripcijski programi, ki posamezniku omogočajo zaščito njegovih podatkov – ti postanejo nedostopni in nedosegljivi nepooblaščenim osebam. S tega vidika je enkripcija podatkov družbi potrebna in dobrodošla. Temna plat enkripcije pa se pokaže v kazenskih postopkih, ko ta organom pregona prepreči dostop do digitalnih podatkov, do katerih so upravičeni na podlagi sodne odredbe.

Termin »enkripcija« izhaja in angleške besede »encryption«, ki pomeni konverzijo podatkov v šifrirno obliko (»ciphertext«), ki je nerazumljiva nepooblaščenim osebam (Techtarget.com, 2006). Slovar informatike (Islovar, 2012) pojem »enkripcija« enači s pojmom »šifriranje« – to pa opredeli kot postopek, pri katerem se z uporabo šifrirnega algoritma in šifrirnega ključa čistopis spremeni v tajnopis. Temu nasproten je postopek dešifriranja (ang. »decryption«), ki je postopek, pri katerem se tajnopis z uporabo šifrirnega algoritma in šifrirnega ključa spremeni v čistopis.

Pojmi kodiranje, šifriranje in enkripcija se v tujih virih uporabljajo kot sinonimi. Kljub vsemu, naj bi med njimi obstajale nekatere razlike glede nivoja konverzije. Tako naj bi se pojem šifriranje nanašal predvsem na črkovno konverzijo besedil (črka A je B, črka B je C itn.). Pojem dekodiranje pa naj bi se nanašal tudi na konverzijo fraz, pomenov, itn. (beseda ptič pomeni letalo ipd.) (Techtarget.com, 2006). Dejstvo je, da kazenskopravni in informacijski strokovnjaki (Clough, 2010; Barett, 1997) danes za kodiranje digitalnih podatkov uporabljajo pojem »enkripcija« oz. v izvirniku »encryption«, zato bomo ta termin uporabljali tudi v tem prispevku.

V nadaljevanju nas bo predvsem zanimalo, kako enkripcija deluje, kakšni so njeni varnostni vidiki in kakšne probleme lahko povzroča organom kazenskega pregona pri preiskovanju kaznivih dejanj, povezanih z digitalnimi podatki.

2 Enkripcija digitalnih podatkov

Enkripcija je seveda stara že prav toliko kot človeška komunikacija. Z razvojem komuniciranja je človek začel razvijati tudi metode, kako komunikacijo zaščititi pred osebami, katerim vsebine niso bile namenjene.

Enkripcijo digitalnih podatkov (Data Encyption Standard – DES) je leta 1974 razvil IBM, leta 1977 pa so jo ZDA prevzele kot državni standard za šifriranje digitalnih podatkov. Idejo digitalne enkripcije je IBM začel razvijati, ko so od bančnega sektorja dobili navodila, da naj pripravijo zaščito za transakcije na bančnih avtomatih (s tem naj bi se preprečilo nepooblaščeno dvigovanje denarja). V letu 1976 je Državna Varnostna Agencija ZDA (National Security Agency – NSA) na podlagi IBM-ovega standarda razvila modificirano verzijo enkripcije, ZDA pa so jo prevzele, kot uradni zvezni informacijsko-enkripcijski standard (imenovan FIPS) (Coppersmith, 1994). S potrditvijo NSA je ta enkripcijski standard hitro prodrl v akademske in vojaške informacijske sisteme na mednarodni ravni.

Jedro enkripcije predstavlja enkripcijski algoritem, ki temelji na enkripcijskem ključu (najbolj pogosti so 128-bitni in 256-bitni ključi). Algoritem predrugači strukturo digitalnega podatka, tako da ta postane nerazumljiv, če oseba nima gesla, s katerim je bil podatek zakodiran (geslo se neposredno veže na enkripcijski ključ) (Frazier, 2011).

Z razvojem informacijske družbe se je potreba po šifriranju podatkov neizmerno povečala. Posamezniki so želeli zaščititi osebne podatke, podjetja pa gospodarske skrivnosti in patente. Enkripcija digitalnih podatkov je tako postala nujno potrebna oblika zaščite za razvijajočo se informacijsko družbo. Zato so se pojavili različni enkripcijski programi (npr. TruCrypt, IronKey, Bitlocker, Guardian Edge ipd.), ki posameznikom in podjetjem omogočajo zaščito njihovih podatkov.

Enkripcija digitalnih podatkov s kvalitetnim enkripcijskim ključem zdaj velja za enega najbolj zaščitenih in najtežje zlomljivih varnostnih mehanizmov. Z enkripcijo digitalnih podatkov samo po sebi seveda ni nič narobe – celo nasprotno, podjetja lahko na ta način zaščitijo svoje digitalne baze in zaupne informacije. Tako zavarovani podatki bodo tudi v primeru vdora v sistem podjetja za storilca neuporabni, saj ta brez enkripcijskega gesla ne bo imel dostopa do njih. Enkripcija je tako v današnji družbi izredno pomemben element varnosti vsakega podjetja, ki hrani svoje gospodarske skrivnosti ali posluje v digitalni obliki.

Z enkripcijo zaščiteni podatki bodo varni pred vsakršno zlorabo s strani nepooblaščenih oseb, ki bi lahko kakor koli pridobili dostop do podatkov podjetja ali posameznika. Dejstvo je tudi, da digitalnih podatkov, ki so kakor koli dostopni prek omrežja, ni mogoče zaščititi fizično (recimo z varnostnikom), saj je dostop do takih podatkov mogoč v nefizični obliki (npr. z vdorom v informacijski sistem). Posamezniki in podjetja morajo zato poseči po digitalni obliki zaščite, ki varuje podatke ravno v primeru, da jih nepooblaščena oseba pridobi na digitalni način.

Digitalna enkripcija pa se lahko izkaže za izredno problematično pri preiskovanju kaznivih dejanj, ko storilec kaznivega dejanja zakodira digitalne dokaze z enkripcijsko metodo, zaradi česar so tako zavarovani digitalni dokazi neuporabni in nedosegljivi računalniškim forenzikom in preiskovalcem kaznivih dejanj.

V zadnjem času se pojavljajo velike pravne dileme, kako pridobiti digitalne podatke iz informacijskih sistemov, ki so zaščiteni z enkripcijskim programom. Teh je na tržišču več vrst, nivo njihove zaščite pa je odvisen od enkripcijskega ključa, ki ga vsebujejo. V tem prispevku se bomo osredotočili le na en enkripcijski program – TrueCrypt, ki zaradi izredne učinkovitosti preiskovalnim organom povzroča številne težave.

2.1 O TrueCrypt zaščiti na splošno

TrueCrypt je brezplačen program, dostopen na internetu, s pomočjo katerega lahko vsaka informacijsko ozaveščena oseba z enkripcijo zaščiti določene podatke na informacijskem sistemu – mogoče je zaščititi tudi celoten sistem. TrueCrypt temelji na tehnologiji Advanced Encryption Standard z 256 bitnim enkripcijskim ključem, ki ga je ameriški zvezna varnostna agencija (NSA) razglasila za primernega za zaščito tudi najbolj tajnih dokumentov (Krumpar, 2012) – gre torej za nezlomljiv algoritem, ki ga ne morejo obiti niti skupine najboljših forenzičnih ekspertov. To je bilo lepo razvidno iz primera brazilskega bankirja Daniela Dantasa, osumljenega bančnih goljufij. FBI, ki je sodeloval z brazilsko policijo, namreč ni bil sposoben predreti TrueCrypt zaščite na nosilcih podatkov, ki so jih Dantasu zasegli med hišno preiskavo (Layden, 2010). FBI je neuspešno poskušal predreti TrueCrypt zaščito celih 12 mesecev, nakar so preiskovalci obupali. Informacijski sistem, zaščiten s TrueCrypt metodo bo torej organom pregona nedostopen, kljub sodni odredbi, ki jim ta pregled dovoljuje.

Zato so preiskovalci predlagali avtorjem TrueCrypt programa, da naj v program vdelajo stranska vrata, ki naj bi v izrednih primerih omogočala preiskovalcem, da obidejo TrueCrypt zaščito (torej v smislu administratorskega univerzalnega gesla, ki bi odklenil zaščito v primeru kazenskih zadev), vendar pa so jih avtorji programa zavrnili s trditvijo, da tega ne bodo nikoli storili, saj bi s tem nasprotovali sami ideji (zaščita podatkov), zaradi katere so program sploh naredili (TrueCrypt, 2012). Taka zahteva državnih institucij bi vsekakor bila sporna z vidika ustavnih določb o svobodnem podjetništvu – seveda ob upoštevanju, da enkripcijski programi, kot je TruCrypt, v bistvu niso bili izdelani za prikrivanje kaznivih dejanj, temveč za zaščito tajnosti podatkov. To, da se programi zlorabljajo za kriminalne namene, pa so seveda stranski pojavi digitalnega razvoja. A po drugi strani je treba priznati, da bi bila vgraditev stranskih vrat v enkripcijske programe najbolj preprosta rešitev, s katero bi organi pregona lahko dostopali do tako zaščitenih digitalnih dokazov.

2.2 Kazenskopravni preiskovalni vidik

Preden se lotimo problematike TrueCrypt zaščite s kazenskopravnega vidika, je treba predstaviti preiskovalni ukrep, s katerim organi pregona pridobivajo digitalne podatke.

Zakon o kazenskem postopku (ZKP, 2011) ureja zaseg, zavarovanje in preiskavo elektronske naprave v členih 219.a in 223.a, ločeno od klasične preiskave. Člena

sta bila uvedena z novelo zakona ZKP-J leta 2009 in zajemata sodobna preiskovalna dejanja, namenjena digitalnih dokazom. Digitalni podatki se bodo torej pridobivali na podlagi omenjenih členov Zakona o kazenskem postopku.

Člen 219.a je umeščen v ZKP (2011) pod poglavje Hišna in osebna preiskava, s čimer se namiguje, da bodo elektronske naprave in nosilci digitalnih podatkov praktično vedno zaseženi v okviru teh dveh dejanj. Tako prvi odstavek člena 219.a ZKP določa, da se preiskava elektronskih in z njimi povezanih naprav ter nosilcev elektronskih podatkov, zaradi pridobitve podatkov v elektronski obliki, lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke, na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti ali prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali tiste, ki jih je mogoče uporabiti kot dokaz v kazenskem postopku.

Preiskava se opravi na podlagi vnaprejšnje privolitve imetnika elektronske naprave ali na podlagi pisne odredbe sodišča, za katero zaprosi tožilec.

V praksi bo to videti tako, da bodo organi pregona osumljenca seznanili s pisno odredbo sodišča, nato bodo zasegli odrejene nosilce digitalnih podatkov (trdi diski, USB ključi, DVD-ji, »druge pametne naprave« itn.). Preiskava se vedno opravlja na identičnih kopijah, ki jih naredijo preiskovalci (ne preiskuje se torej na zaseženem nosilcu). Težava seveda nastane, če je digitalni podatek zaščiten s TrueCrypt metodo.

Preiskovalni sodnik lahko tudi na ustni predlog državnega tožilca izda ustno odredbo za preiskavo elektronske naprave. To je praktično edina možnost pridobitve elektronskih podatkov iz računalniškega sistema, ki je v celoti zaščiten s TrueCrypt metodo. Ideja je, da bi policisti vdrli v zaprte prostore, medtem ko bi storilec uporabljal informacijski sistem – ta naj medtem ne bi bil zaščiten. Seveda se bodo načrti preiskovalcev podrli že takoj, ko bo storilec izklopil informacijski sistem – ob vnovičnem zagonu bo ta zopet pod TrueCrypt zaščito. Prav tako bo ukrep popolnoma nesmiseln, če storilec hrani podatke na zaščitenem USB ključu ali drugem nosilcu podatkov (kar bo pogosto v praksi), ki je stalno pod TrueCypt zaščito (storilec ima nosilec na varnem mestu, ga ne uporablja in ne odklepa).

Problematičnost določbe petega odstavka člena 219.a ZKP (2011) je tudi, da zahteva pogoj obstoja neposredne in resne nevarnosti za varnost ljudi ali premoženja, kar pa pogosto ni podano. Izredno nizka je namreč možnost, da bi organi pregona zalotili storilca v času, ko bi npr. izvrševal napad na informacijske sisteme določenih državnih ustanov, ki skrbijo za splošno varnost ali premoženje ljudi

(npr. napad na informacijski sistem komunalnih ustanov, prek katerega bi storilec izpustil nepredelane kanalizacijske odpadke v reko, v kateri bi se kopali ljudje, ali bi jo uporabljali za pitno vodo). Organi pregona bodo informacije o kaznivem dejanju pridobili šele po končanem kaznivem dejanju, ko ne bo več neposredne in resne nevarnosti za varnost ljudi ali premoženja, takrat pa bo lahko storilčev računalnik že pod varno zaščito TrueCrypt.

Zapisali smo že, da so podatki zaščiteni s TrueCrypt metodo, v praksi nedosegljivi še tako izkušeni forenzični ekipi. Je potem do teh podatkov sploh mogoče priti ali se zaradi nedosegljivosti štejejo za neobstoječe?

Vsekakor se ne štejejo za neobstoječe, saj podatki obstajajo – le za organe pregona so nedosegljivi. Vprašanje nastopi, kako naj zakonodaja organom pregona omogoči dostop do digitalnih dokazov oz. ali je to sploh mogoče doseči z zakonsko ureditvijo?

Nekoliko radikalna, a v praksi relativno učinkovita, je metoda, ki jo uporablja Združeno Kraljestvo v skladu z Zakonom o ureditvi preiskovalnih pooblastil (Regulation of Investigatory Powers Act, 2000). V tretjem oddelku je določeno, da posebno samostojno kaznivo dejanje, s predpisano kaznijo zapora do dveh let, stori, kdor ne posreduje organom pregona zahtevanih šifrirnih ključev za dostop do informacijskega sistema. Kaznuje se lahko tudi obdolženec, osumljenec ali družinski član, ki ve za šifrirni ključ. Prvi odmevni primer te ureditve se je zgodil leta 2007, ko so morali, pod grožnjo dveletne zaporne kazni, šifrirna gesla predati zagovorniki živalskih pravic (Ward, 2007).

Slovensko pravo v šestem odstavku člena 219.a ZKP (2011) vsebuje podobno zahtevo, da mora imetnik oz. uporabnik elektronske naprave omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če tega ne stori, se lahko zapre do izročitve predmetov ali do konca kazenskega postopka, vendar največ za mesec dni. Vendar pa določba ne velja za osumljenca, obdolženca ali osebo, ki ne sme biti zaslišana kot priča – torej osebe, ki bodo te ključe pogosto imele. Prav tako naša določba po ZKP predstavlja le kazen za neupoštevanje sodne odredbe, ne pa za samostojno kaznivo dejanje.

Taka ureditev izhaja iz privilegija zoper samoobtožbo, ki je ustavno priznana pravica vsakega obdolženca v kazenskem postopku. V ZDA so obdolženci zaščiteni s petim amandmajem ameriške ustave, ki preprečuje, da bi se od obdolžencev zahtevalo kakršno koli sodelovanje z organi pregona – kar vključuje tudi posredovanje šifrirnih ključev. Sodni precedens, ki to potrjuje glede šifrirnih ključev, je

ZDA proti John Doe iz leta 2012, v katerem je sodišče odločilo, da obdolženec ni dolžan tožilstvu predati gesel za odklep njegovega računalniškega sistema.

Kljub spoštovanju človekovih pravic, svoboščin in privilegijem v kazenskem postopku take ureditve ne moremo podpirati. Dejstvo je, da je enkripcija elektronskih podatkov novost, s katero se je pravo šele začelo srečevati. Togo vztrajanje na tradicionalnih metodah, ko se srečujemo z novodobnimi tehnologijami, pa je včasih lahko pogubno. Če obdolženca ne moremo »prisiliti«, da nam izda šifrirni ključ, potem elektronskih podatkov, za katere vemo, da so na njegovem sistemu, ne moremo pridobiti. Tu se omenja, da gre za hud poseg v zasebnost posameznika – vendar je ta pravičen, ko imajo organi pregona za to odrejen sodni nalog. Prav tako sodobno kazensko pravo omogoča odvzem DNK obdolženca, kar velja za hujši poseg v posameznikovo zasebnost, kot pregled njegovih digitalnih vsebin.

Po analogiji lahko vzameno tudi primer sefa, ki si ga lasti obdolženec. Organi pregona bodo lahko s silo (ali s posebnimi kemičnimi sredstvi) odprli sef, če imajo za to sodno odredbo, in to kljub temu, da jim obdolženi ne sporoči kombinacije sefa. Značilnost digitalnega kodiranja s programom TrueCrypt pa je, da te zaščite ni mogoče predreti na noben način. Tako zakodirani podatki so za organe pregona povsem nedostopni. Digitalna enkripcija je pojav, s katerim se pravo do sedaj še ni srečalo. Zelo skrbno je treba preučiti, kako bomo do nje pravno pristopili, saj lahko z uveljavljanjem tradicionalnih pravnih pogledov zaščitimo storilce določenih kaznivih dejanj do te mere, da bo kazenski pregon zoper njih postal praktično nemogoč. Digitalna enkripcija je tako neke vrste neprebojni sef za elektronske podatke in dokaze. Predstavljajmo si hipotetičen primer, da ima nekdo na vrtu pred hišo zgrajen trezor, velik kot garaža, iz neuničljivih elementov – trezorja torej ne bi bilo mogoče na noben način odpreti ali uničiti (tudi ne z eksplozivom, kemikalijami itn.). Lastnik tega trezorja bi nato ubil svojo ženo in njeno truplo ter morilsko sredstvo zaprl v trezor, katerega kombinacijo bi poznal le on. Če predpostavimo, da bi soseda sporočila policiji, da je slišala prepir in videla moža, kako nekaj nosi v trezor, kako bi lahko organi pregona prišli do trupla in orožja v trezorju? Brez trupla in orožja bi imeli le posredni dokaz v obliki pričanja sosede, ki vsekakor ni dovolj za obsodilno sodbo kaznivega dejanja (podobno imamo pri kibernetskih kaznivih dejanjih posredne dokaze, kaj se je verjetno zgodilo, oprijemljive dokaze pa je potrebno najti v informacijskem sistemu obdolženca).

Nekakšen zakonodajni ukrep, po katerem bi lahko organi pregona pridobili gesla, ki bi jim omogočala dostop do tako zavarovanih (šifriranih) vsebin, se zato zdi primeren.

V primeru, da kazenska zakonodaja predvidi (po vzoru Združenega Kraljestva) posebno samostojno kaznivo dejanje neizdaje šifrirnega gesla, se lahko pojavi težava, da bo storilec preprosto zatrjeval, da je geslo pozabil – kar predpostavlja njegovo malomarnost. Omenjeno kaznivo dejanje je po sodobni kazenskopravni doktrini lahko le naklepno (ne gre namreč za ogroževalno kaznivo dejanje, poleg tega pa tudi sama bit kaznivega dejanja v tem primeru zahteva naklep). Dokazovanje, da storilec geslo pozna in ga naklepno noče izdati, je lahko izredno težavno.

Drugi mogoč pristop je v obliki posrednega dokazovanja in prek dokaznih virov, ki se nahajajo drugje, kot na informacijskem sistemu obdolženca ali osumljenca. Tako bo mogoče prek internetnega ponudnika pridobiti sledi, da so se z določenega informacijskega sistema pridobivali podatki z določene medmrežne FTP povezave, za katero se ugotovi, da ponuja otroško pornografijo. Med hišno preiskavo lahko organi pregona zasežejo nosilce podatkov (DVD-ji, USB ključi), na katere si je storilec presnel nezakonito gradivo (če je to zakodirano, se zopet znajdemo v že navedeni dilemi). Prednost tega pristopa je vsekakor ta, da se dokazi zbirajo zunaj digitalne sfere storilca – tako pridobljeni podatki pa niso praktično nikoli zaščiteni z enkripcijo.

3 Zaključek

Digitalni dokazi bodo v prihodnosti kazenskega prava imeli vedno večjo vlogo. Vedno več kaznivih dejanj bo povezanih z informacijskimi sistemi in vedno bolj pogoste bodo preiskave teh. Če želi kazensko pravo slediti razvoju tehnologije, se mora tudi samo stalno razvijati in dopolnjevati, obenem pa upoštevati, da tradicionalni pravni pristopi ne bodo vedno pravilni in primerni za prihajajoče informacijske tehnologije. Nazoren primer tega je enkripcija digitalnih podatkov, s katero se kazensko pravo pravzaprav še ni temeljito spopadlo. Prevzeto tradicionalno stališče, da obdolženec zaradi privilegija zoper samoobtožbo, ni dolžan sporočiti policiji šifrirnih gesel za dostop do podatkov v njegovem informacijskem sistemu (kljub sodni odredbi, ki to dovoljuje), se bo lahko izkazalo za usodno v marsikateri kazenski zadevi kibernetskega ali klasičnega kriminala v prihodnosti.

Ena od mogočih rešitev glede računalniške enkripcije (ki je sicer sama po sebi izredno sporna z ustavnega vidika), je opredelitev posebnega samostojnega kaznivega dejanja neizdaje šifrirnih gesel organom pregona, ki te zahtevajo na podlagi sodne odredbe. Alternativna rešitev se kaže v posrednem dokazovanju in zbiranju digitalnih dokazov, kar sicer ni ustavno sporno, a je v praksi bistveno manj učinkovito.

Sami zagovarjamo rešitev po vzoru Združenega Kraljestva, po kateri bo posebno samostojno naklepno kaznivo dejanje izvršila oseba, ki bo poznala, a ne bo želela izdati enkripcijskega gesla za elektronsko napravo, za katero bodo organi pregona imeli sodno odredbo za preiskavo. Kljub ustavni spornosti, je ukrep v današnji informacijski družbi potreben. Argumentacijo za tako ureditev vidimo tudi v trenutni zakonski odreditvi odvzema DNK vzorca obdolženca – ta se je sodni odredbi dolžan podrediti, poleg tega pa odvzem DNK vzorca predstavlja večji poseg v zasebnost posameznika kot preiskava elektronske naprave. Alternativna in pravno bolj čista rešitev bi bila zakonska ureditev, po kateri bodo morali izdelovalci enkripcijskih programov v te vstaviti stranske univerzalne ključe, ki bi lahko obšli zaščito v primerih kazenskih preiskav. Ali se izdelovalce v to lahko prisili, je ločeno (in zopet ustavno sporno) vprašanje, prav tako pa je vprašljivo, ali ne bi potem uporabniki posegli po starejših verzijah enkripcijskih programov, ki teh obhodnih univerzalnih ključev ne vsebujejo.

Kazensko pravo vsekakor sledi razvoju informacijske tehnologije in pričakujemo lahko, da bo tako tudi v prihodnosti. Z vidika dokaznega prava si upamo trditi, da bo ravno na tem področju največ sprememb in polemik v kazensko-procesnem dokaznem pravu. Pravo tu pravo ne sme biti pretirano rigidno in bo moralo začeti dopuščati določene izjeme pri sicer ustaljeni ustavni dogmatiki, sicer bo pregon kaznivih dejanj, povezanih z informacijskimi sistemi, postal pretirano otežen, če ne že skoraj nemogoč.

Viri

- Barrett N. (1997). Digital Crime, Policing the Cybernation. Michigan: Kogan Page.
- Clough J. (2010). Principles of Cybercrime. Cambridge: Cambridge University Press.
- Coppersmith, D. (1994). The Data Encryption Standard (DES) and Its Strength Against Attacks. IBM Journal of Research and Development, 38(3), 243–250. Pridobljeno 8. 9. 2012 na: http://web.archive.org/web/20070615132907/http://www.research.ibm.com/journal/rd/383/coppersmith.pdf
- Encryption – Definition (1. 7. 2006). Techtarget.com. Pridobljeno 22.8.2012 na: http://searchsecurity.techtarget.com/definition/encryption
- Fraizer R. E. (5. 4. 2011). Data Encyption Techniques. Pridobljeno 9. 9. 2012 na: http://www.mrp3.com/encrypt.html
- Krumpar I. (2012). Državno tožilski vidik problematike digitalnih dokazov. V Dvoršek A. in Frangež D. (ur.) (2012). Digitalni dokazi, kazensko pravni, kriminalistični in informacijsko-varnostni vidiki (str. 54 – 56). Ljubljana: Fakulteta za varnostne vede.

- Internetna stran programa TrueCrypt (1. 9. 2012). TrueCrypt.org. Pridobljeno 11.7.2012 na: http://www.truecrypt.org/
- Islovar – terminološki slovar informatike (2012). Slovensko društvo Informatika. Pridobljeno 11. 8. 2012 na: http://www.islovar.org/
- Layden J. (28. 6. 2010). Brazilian Banker's Crypto Baffles FBI. Theregister.co.uk. Pridobljeno 22. 7. 2012 na: http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out/
- Slovar slovenskega knjižnega jezika (2000). Inštitut za slovenski jezik Frana Ramovša ZRC SAZU. Pridobljeno 10. 11. 2011 na: http://bos.zrc-sazu.si/sskj.html
- Regulation of Investigatory Powers Act 2000. Parlament Združenega Kraljestva, zakon sprejeto 28. julija 2000 z novelami do leta 2010, Združeno Kraljestvo. Pridobljeno 11. 5. 2012 na: http://www.legislation.gov.uk/ukpga/2000/23
- Ward M. (20. 11. 2007). Campaigners Hit by Decryption Law. BBC News UK. Pridobljeno 30. 5. 2012 na: http://news.bbc.co.uk/2/hi/technology/7102180.stm
- Zakon o kazenskem postopku, uradno prečiščeno besedilo (ZKP-UPB4). Uradni list RS, št. 32/2007 z dne 10. 4. 2007 z novelami ZKP-I, Uradni list RS, št. 68/2008 z dne 8. 7. 2008, ZKP-J, Uradni list RS, št 77/2009 z dne 2. 10. 2009 in ZKP-K, Uradni list RS, št. 91/2011 z dne 14. 11. 2011.
- ZDA proti John Doe (23. 2. 2012). Pritožbeno sodišče v Floridi, opravilna številka D.C. Docket No. 3:11-mc-00041-LAC, Združene Države Amerike. Pridobljeno 22. 5. 2012 na: http://www.ca11.uscourts.gov/opinions/ops/201112268.pdf

O avtorju

Miha Šepec, univ. dipl. pravnik in univ. dipl. varstvoslovec, doktorski kandidat kazenskega prava na Pravni fakulteti Univerze v Mariboru. Asistent za kazensko pravo na Fakulteti za varnostne vede Univerze v Mariboru in na Evropski Pravni fakulteti v Novi Gorici.

Možnosti izgube podatkov in kazenskopravne posledice

Blaž Markelj, Sabina Zgaga

Časi ločevanja podatkov na zasebne in službene so mimo. Razlog tiči v vedno bolj razširjenih modernih mobilnih napravah in računalništvu v oblaku. Pri slednjem je, ko gre za javni oblak, skoraj nemogoče določiti fizično lokacijo podatkov. Samodejno se nam zastavlja vprašanje, zakaj ljudje potem uporabljamo takšno tehnologijo. Odgovor je zelo enostaven: zaradi racionalizacije stroškov ter hitrejšega, bolj fleksibilnega in enostavnejšega obvladovanje informacijske tehnologije. Ko govorimo o fleksibilnosti dostopanja do podatkov v oblaku, ne moremo mimo mobilnih naprav. Ti predstavljajo nepogrešljivo sredstvo za izvajanje dnevnih opravil ter dostopanje do podatkov. Mobilno napravo lahko primerjamo z (mobilnim) terminalom, ki smo ga nekoč v preteklosti uporabljali za prikazovanje informacij (nekaj jih je tudi hranil). So pa uporabniki nekdaj vedeli, kje dejansko so spravljeni njihovi podatki, danes pa zdaj zaradi mobilnosti vedno bolj izginjamo nadzor nad podatki. Še večjo težavo predstavlja mešanje različnih tipov podatkov na mobilni napravi in dostopanje do različnih tipov oblakov. Uporabnik lahko mobilno napravo uporablja ali za zasebni ali poslovni namen in dostopa tako do javnega oblaka, ki ga uporablja za zasebne potrebe, kot do zasebnega oblaka, kjer so spravljeni korporativni podatki, ki so lahko različno varnostno klasificirani. Mešanje različnih vrst podatkov poveča možnost razkritja ali odtujitve varnostno občutljivih informacij.

Uporabniki mobilnih naprav so lahko kazensko odgovorni, če svoje mobilne naprave ne uporabljajo skrbno in povzročijo neko prepovedano posledico. Zaradi vse bolj množične uporabe mobilnih naprav in predvsem zaradi ne dovolj pazljivih uporabnikov, se pojavlja veliko vprašanj na kazenskopravnem področju, in te obravnavamo v drugem delu tega prispevka. Med drugimi sta pomembni vprašanji: (1) za katera kazniva dejanja uporabnik mobilne naprave sploh lahko odgovarja na ravni inkriminacije oz. zakonske znake katerih kaznivih dejanj je izpolnil s svojim ravnanjem, in (2) na kakšen način lahko izvrši kaznivo dejanje (s storitvijo ali opustitvijo).

KLJUČNE BESEDE: pametni mobilni telefoni, informacijska varnost, kazenska odgovornost, mladi

1 Uvod

Moderna tehnologija je dodobra spremenila naše delovanje. Mobilnost tehnologije je spremenila, kako komuniciramo, sprejemamo odločitve in dostopamo do informacij. Vsekakor pa je spremenila načine in vrste podatkov (osebni, javni, tajni itd.) katere dnevno delujemo. Zaradi čedalje večjega števila uporabnikov mobilnih naprav in računalništva v oblaku, ki to tehnologijo uporabljajo tako za zasebne kot službene namene, se je meja med zasebnim in službenim tako rekoč zabrisala. Mobilne naprave, še posebej mobilni telefoni, so iz dneva v dan bolj uporabne. Vedno več je ljudi, ki jih uporabljajo kot nadomestek za svoj osebni računalnik. Zaradi uporabne inovativnosti in možnosti neprekinjenega dostopa do interneta, mobilne naprave z lahkoto prepričajo vsakega uporabnika. Študentje (mladi) jih uporabljajo kot nenadomestljiv pripomoček za vzdrževanje neprekinjene komunikacije, zaposleni pa jih uporabljajo še za hranjenje in obdelovanje informacij, potrebnih za sprejemanje vsakodnevnih odločitev. Računalništvo v oblaku, še posebej javni oblak, postaja vedno bolj pomemben »prostor«, kamor uporabniki odlagajo svoje podatke oz. ga uporabljajo za elektronsko pošto in kot sredstvo za neprestan dostop do podatkov s svojo mobilno napravo. Računalništvo v oblaku je postalo vroča téma pogovorov informatikov in predstavnikov informacijske varnosti. Storitve v oblaku lahko definiramo kot souporabo računalniških resursov prek interneta, pri čemer uporabnik za upravljanje ne potrebuje veliko računalniškega znanja oz. uporabniku preprosto ni potrebno skrbeti za upravljanje sistema, njegova skrb je zgolj, kako in za kaj ga bo uporabljal (Glavač, 2009). Ideja oblaka ni nova, je pa danes s pomočjo naprednejših internetnih povezav in informacijske tehnologije bolj dostopna. Za preprostega uporabnika je najbolj dostopen javen oblak. S hitro razvijajočimi mobilnimi telefoni – število uporabnikov narašča iz dneva v dan narašča – je pot do podatkov v javnem oblaku sila enostavna. Danes že težko najdemo mobilni telefon, ki ne bi omogočal stalnega dostopa do interneta. S preskokom iz »statičnega načina dela«, pri katerem smo uporabljali navadne računalnike, terminale in strežniške sisteme, katerih fizična lokacija nam je bila znana, v »dinamičen način dela«, pri katerem uporabljamo računalništvo v oblaku (fizična lokacija, ki je odvisna od vrste oblaka, nam velikokrat ni znana) in imajo pomembno vlogo mobilne naprave (mobilni telefoni, tablični računalniki, prenosniki itn.), je postalo zagotavljanje informacijske varnosti bistveno težje. Zato je zelo pomembno, da se tega zavemo tudi uporabniki in upoštevamo dinamičnost tudi, ko premišljujemo o varovanju podatkov ter vzpostavljanju in uporabi informacijskih zaščit. Ne razvijajo pa se zelo hitro samo mobilne naprave ter računalništvo v oblaku, ampak tudi številne grožnje, ki pretijo uporabnikom teh

tehnologij. Ob nevestni uporabi teh tehnologij se lahko uresniči katera od groženj in posledice so lahko tudi odtujitev podatkov (ti so lahko osebni, službeni, tajni, poslovni itn.). V drugem delu članka se zato sprašujemo o kazenskopravni odgovornosti posameznika za posledice (npr. izguba podatkov) nevestne uporabe, o potencialno kaznivih dejanjih in načinih njihovega izvrševanja.

2 Računalništvo v oblaku in mobilne naprave

Pri računalništvu v oblaku je glavni poudarek na optimizaciji informacijskih resursov in s tem povezanim zmanjševanjem stroškov. Podjetje TechNavio je objavilo poročilo o trenutni in predvideni prihodnji rasti storitve računalništva v oblaku; navedli so možnost 42 odstotnega povečanja števila uporabnikov med letoma 2010 in 2014 (Infiniti Research Limited, 2011). Hiter razvoj informacijske tehnologije in dostopnejše ter hitrejše spletne povezave nam omogočajo, da lahko s mobilnim telefonom pregledujemo vse pomembnejše novice dneva, opravimo poslovanje z banko, pregledamo elektronsko pošto, na voljo pa so nam še druge storitve (Guillimein, 2009). Povezovanje mobilnega telefona z različnimi internetnimi storitvami je s pomočjo računalništva v oblaku za uporabnika veliko preprostejše in predvsem cenejše. Povezovanje mobilnih naprav s pripadajočo programsko opremo z aplikacijami v oblaku je čedalje pogostejše. Sprašujemo se, ali je resnično mogoče v vsakem trenutku priti do podatkov? Ob razmišljanju o storitvah, ki nam jih omogoča oblak, ne moremo mimo vprašanja o informacijski varnosti. Odgovoriti pa bo treba tudi na vrsto vprašanj o zasebnosti podatkov, shranjenih v oblaku.

Velika količina podatkov, ki je na voljo v vsakem trenutku, je shranjena v korporativnih informacijskih centrih in/ali v računalniškem oblaku. S pomočjo naprednih mobilnih naprav in pripadajoče programske opreme dokaj enostavno dostopamo do korporativnih podatkov (npr. elektronska pošta, dokumenti, poizvedovanje po bazah ipd.). Zaradi hitrosti poslovnih procesov in sprejemanja pomembnih odločitev je nujno imeti hiter in učinkovit dostop do informacij. Pomembno je poskrbeti za informacijsko varnost, saj so od tega odvisni razpoložljivost in integriteta podatkov ter zaupanje v informacije, poslovne procese in odločitve, ki jih sprejema in predstavlja organizacija.

Ideja informacijske tehnologije in oblaka kot storitve izvira že iz časov terminalov in zaprtih, med seboj nepovezanih korporativnih omrežij. S hitrim razvojem tehnologije prenosa podatkov po različnih omrežjih in mobilnih napravah,

predvsem pa zaradi visokih stroškov nakupa informacijske tehnologije in storitev, je znova oživela zamisel računalništva v oblaku. Podjetja se čedalje pogosteje odločajo za oblak, ker jih je gospodarska kriza prisilila k zmanjševanju stroškov informatike. Podjetja virtualni prostor oz. oblak, kjer lahko uporabljajo storitve informacijske tehnologije in sistema, vidijo kot priložnost za zmanjšanje stroškov nakupa in vzdrževanja lastne informacijske tehnologije ter dostopa do vedno novejših različic programske opreme (Rodier, 2011). Oblak pa predstavlja tudi informacijsko tveganje. Elektronska pošta, odlaganje dokumentov, baze podatkov in dodatna nadomestna lokacija so le nekatere storitve, ki jih lahko podjetja zakupijo pri ponudnikih prostora v njihovem oblaku. Storitve oblaka so lahko razdeljene zaradi večje prilagodljivosti storitev in informacijske varnosti ter glede na želje uporabnikov. Podjetja lahko z lastnimi kadri in varnostnimi metodami (gesla, enkripcija podatkov, redundanca ipd.) skrbijo za lasten, zasebni oblak. Ta se navadno nahaja znotraj korporativnega omrežja, medtem ko za javni oblak ne poznamo natančne fizične lokacija – nahaja se pač na internetu. Javni oblak nam omogoča, da lahko podjetje ali organizacija prenese vse svoje potrebe po informacijski tehnologiji na internet. Hibridni oblak je kombinacija zasebnega in javnega oblaka. Pomembni podatki so shranjeni v zasebnem oblaku znotraj korporativnega omrežja, medtem ko izkoriščajo programsko opremo javnega oblaka (Glavač, 2009).

3 Raziskava

Decembra 2011 je bila med študenti narejena raziskava z naslovom Zavedanje groženj mobilnim napravam. Namen raziskave je bil pridobiti ustrezne informacije o zavedanju in poznavanju groženj, ki pretijo mladim uporabnikom, predvsem študentski populaciji, pri uporabi mobilnih naprav; o njihovem poznavanju delovanja in uporabi varnostnih zaščit. Študentje so namreč bodoči kader, ki bo deloval v organizacijah. Raziskava je bila narejena s pomočjo spletnega vprašalnika, ki je bil decembra 2011 tri tedne objavljen na spletnem portalu »1ka« (www.1ka.si). Informacija o raziskavi je bila študentom posredovana prek elektronske pošte, spletnih socialnih omrežij in z osebnim povabilom. Zbrani podatki so bili analizirani z orodjem SPSS. V analizo je bilo zajetih 281 vprašalnikov. Nekateri vprašalniki niso bili izpolnjeni v celoti, zato se je pri posameznih vprašanih vzorec populacije spreminjal. Med anketiranci je bilo največ takih, ki so bili stari od 21 do 25 let, sledi starostna skupina do 20 let. Med anketiranci je bilo 61,5 odstotka žensk in 63,2 odstotka takih, ki imajo že zaključeno srednješolsko izobrazbo.

Vzorec, SN = 216	N	%
Samo za zasebne potrebe	126	58,3
Za zasebne in tudi službene potrebe	56	25,9
Za zasebne in službene potrebe	31	14,4
Za službene in delno tudi zasebne potrebe	1	0,5
Samo za službene potrebe	2	0,9

Tabela 1: Namen uporabe pametnega telefona

Tabela 1 prikazuje, v kakšne namene študentje uporabljajo mobilne telefone. Ni presenetljiv podatek (glede na populacijo anketiranih), da največji odstotek (58,3 %) študentov mobilni telefon uporablja v privatne namene. Je pa zanimiv podatek, da skoraj 26 odstotkov vprašanih uporablja mobilni telefon (poleg privatnih namenov) občasno še za službene namene. Hkrati pa 14,4 odstotka vprašanih uporablja mobilni telefon tako za zasebne kot poslovne namene. Glede na populacijo, ki ji pripadajo sodelujoči v anketi, lahko rečemo, da se trditev o izginjanju meje med zasebnim in privatnim, ki smo jo postavili že v začetku članka, uresničuje že pri mlajših uporabnikih, to je študentih. Študentje so tisti, ki bodo v naslednjih letih delovali v podjetnih, zato je zelo pomembno, da razumemo njihovo delo z podatki, mobilnimi napravami in računalništvom v oblaku. Pomembno je razumeti njihovo delovanje v dinamičnem svetu komunikacij. Podatki iz raziskave nam prikazujejo, katere vrste podatkov študenti hranijo na mobilnem telefonu. Največ jih hrani GSM številke in slike, tem sledijo seznami kontaktov in video vsebine. Vse to nakazuje, da ima največ vprašanih na mobilnem telefonu shranjene osebne podatke. To nam še dodatno potrjuje domneve o tem, za kaj študentje uporabljajo mobilne napravoe. Je pa zanimiv odstotek tistih, ki imajo na mobilnem telefonu shranjene še službene podatke (naslovi, datumi službenih potovanj, elektronski naslovi) ter certifikate. Ob uresničitvi katere koli od groženj so lahko ogroženi vsi ti podatki.

4 Kazenskopravne dileme nepazljive uporabe mobilnih naprav, ki povzroči izgubo zaščitenih podatkov

4.1 Relevantna kazniva dejanja

V zvezi z neprimerno uporabo mobilnih naprav in oblaka si je mogoče zamisliti vsaj dva kazenskopravna konkretna dejanska stanova. Po prvem, uporabnik

s pomočjo svoje mobilne naprave vdre v tujo napravo, da bi si pridobil določene podatke. V tem primeru je uporabnik sam uporabil svojo mobilno napravo kot orodje za izvršitev vdora v tujo mobilno napravo. V drugem konkretnem dejanskem stanu pa uporabnik ne skrbi zadostno za varnost svoje mobilne naprave in tretja oseba to izkoristi ter prek uporabnikove naprave (z namestitvijo malwarea ali virusa) vdre v tujo mobilno napravo. V tem primeru je torej tretja oseba uporabnika in njegovo mobilno napravo uporabila in izkoristila za izvršitev vdora v tuj informacijski sistem in za pridobitev naprave.

Glede na predvidena konkretna dejanska stanova sta relevantni dve skupini kaznivih dejanj iz Kazenskega zakonika-1 (KZ-1).[19] Prva skupina kaznivih dejanj je opredeljena z vsebino podatkov, ki jih uporabnik pridobi z vdorom v tujo mobilno napravo ali jih neupravičeno razkrije, in ne z vrsto mobilne ali druge informacijske naprave. Tako imamo opravka s štirimi vrstami podatkov: z osebnimi podatki, (uradno, vojaško) tajnostjo, poklicno skrivnostjo in poslovno skrivnostjo. Specialno definicijo teh podatkov najdemo ali v KZ-1 ali pa v pravnih aktih z matičnih področij.

Poslovna skrivnost je tako po noveli KZ-1B[20] definirana s KZ-1, pred tem pa je bila relevantna definicija iz Zakona o gospodarskih družbah.[21] V skladu s KZ-1 so poslovna skrivnost listine in podatki, ki so z zakonom, statutom, pravili ali drugim splošnim aktom ali odredbo pristojnega organa ali druge upravičene osebe razglašeni za industrijsko, bančno ali drugo poslovno skrivnost in so tako pomembni, da so z njihovo izdajo očitno nastale ali bi lahko nastale hujše škodljive posledice. Ta definicija v bistvu ustreza definiciji poslovne skrivnosti iz splošnejšega ZGD.[22]

Za razliko od poslovne skrivnosti je tajni podatek definiran s področno zakonodajo, in sicer z Zakonom o tajnih podatkih. Tajen podatek je tako dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije, znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost

19 Kazenski zakonik-1, Ur. l. RS, 55/2008, 66/2009, 91/2011.

20 Ur. l. RS, 91/2011.

21 39. člen Zakona o gospodarskih družbah-1, Ur. l. RS, št. 65/2009, 33/2011, 91/2011.

22 236. člen KZ-1.

državnih organov Republike Slovenije, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno. Bistveno je, da je podatek določen za tajnega s strani pooblaščene osebe, ker bi z njegovim razkritjem nepoklicani osebi nastale, ali bi očitno lahko nastale, škodljive posledice za varnost države ali za njene politične ali gospodarske koristi.[23]

Podatek za opredelitev relevantnega kaznivega dejanja je lahko tudi poklicna skrivnost.[24] To je vsak podatek, ki ga oseba pridobi pri opravljanju poklica. KZ-1 kot take osebe našteva zagovornika, odvetnika, zdravnika, duhovnika, socialnega delavca in psihologa, seveda pa imajo dolžnost varovati poklicno skrivnost vse osebe, ki opravljajo poklic (Deisinger, 2002: 145).

In ne nazadnje, podatek, s katerimi upravljajo organizacije z mobilnimi napravami, je lahko tudi osebni podatek.[25] Tudi tega KZ-1 ne definira, ampak je definicijo mogoče najti v Zakonu o varstvu osebnih podatkov-1,[26] v skladu s katerim je osebni podatek kateri koli podatek, ki se nanaša na posameznika, ki je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa ne glede na obliko, v kateri je izražen.[27]

KZ-1 na te definicije podatkov navezuje ustrezna kazniva dejanja neupravičenega razkritja ali pridobitve podatkov. Vsaka vrsta podatka ima v KZ-1 predpisano ustrezno kaznivo dejanje. Tako je na primer v KZ-1 opredeljeno kaznivo dejanje izdaje in neupravičene pridobitve poslovne skrivnosti, ki ga izvrši vsakdo, kdor neupravičeno v nasprotju s svojimi dolžnostmi glede varovanja poslovne skrivnosti sporoči ali izroči komu podatke, ki so poslovna skrivnost, ali mu kako drugače omogoči, da pride do njih, ali jih zbira z namenom, da jih izroči nepoklicani

23 2., 10. in 11. člen Zakona o tajnih podatkih.

24 142. člen KZ-1.

25 143. člen KZ-1.

26 Ur. l. RS, št. 94/2007.

27 6. člen Zakona o varstvu osebnih podatkov-1.

osebi.[28] Kako mora biti poslovna skrivnost varovana in kdo jo je dolžan varovati, pa KZ-1 ne določa. To določi gospodarska družba s sklepom, s katerim tudi opredeli, kateri podatek je poslovna skrivnost[29] in kako naj se ta podatek varuje z vidika informacijske varnosti.

Podobno je opredeljeno kaznivo dejanje izdaje tajnih podatkov,[30] ki ga izvrši uradna oseba[31] ali druga oseba, ki v nasprotju s svojimi dolžnostmi varovanja tajnih podatkov sporoči ali izroči komu tajne podatke ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke, zato da jih izroči nepoklicani osebi. Tudi tu KZ-1 ne določa načina varovanja tajnih podatkov, ampak je to urejeno z Zakonom o tajnih podatkih in številnimi podzakonskimi predpisi.[32] V skladu s tem zakonom mora vsaka organizacija sprejeti ustrezne sisteme in postopke varovanja tajnih podatkov, ki ustrezajo določeni stopnji tajnosti in onemogočajo njihovo razkritje nepoklicanim osebam, na podlagi predpisov.[33] S tega vidika je posebej relevanten predpis Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, ki ureja tudi vidik informacijske varnosti tajnih podatkov. Če tisti, ki je dolžan varovati tajnost, naklepno krši te dolžnosti, določene z zakonodajo in pravilniki organizacije, in s tem povzroči neupravičeno razkritje tajnega podatka, izvrši kaznivo dejanje izdaje tajnih podatkov.

KZ-1 opredeljuje tudi kaznivo dejanje neupravičene izdaje poklicne skrivnosti, ki ga izvrši vsakdo, ki neupravičeno izda skrivnost, za katero je izvedel kot zagovornik, odvetnik, zdravnik, duhovnik, socialni delavec, psiholog ali kot kakšna druga oseba pri opravljanju svojega poklica.[34] Način varovanja tudi tu ni določen v KZ-1, ampak v področnih predpisih, ki urejajo določen poklic.

Zlorabo osebnih podatkov po 143. členu KZ-1 pa izvrši vsakdo, kdor brez podlage v zakonu ali v osebni privolitvi posameznika, na katerega se osebni podatki nanašajo, osebne podatke, ki se obdelujejo na podlagi zakona ali osebne privolitve

28 1. odst. 236. člena KZ-1.

29 1. odst. 40. člena Zakona o gospodarskih družbah.

30 260. člen KZ-1.

31 Glej 99. člen KZ-1.

32 Na primer Uredba o varovanju tajnih podatkov, Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, itn.

33 38. in 40. člen Zakona o tajnih podatkih.

34 2. odst. 142. člena KZ-1.

posameznika, posreduje v javno objavo ali jih javno objavi.[35] Zakon o varstvu osebnih podatkov-1 ureja način varovanja osebnih podatkov in predpisuje, da so upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov ter v svojih aktih predpisati postopke in ukrepe za zavarovanje osebnih podatkov ter določiti osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.[36] Ti akti morajo seveda zajemati tudi vidik informacijske varnosti teh podatkov, če upravljavci uporabljajo mobilne naprave.

Po drugi strani pa pride v poštev tudi kazenska odgovornost za katero izmed »računalniških« kaznivih dejanj. KZ-1 določa dve taki kaznivi dejanji; napad na informacijski sistem in zloraba poslovnega informacijskega sistema. Kaznivo dejanje napada na informacijski sistem[37] je uvrščeno v poglavje o kaznivih dejanjih zoper premoženje in izvrši ga vsakdo, ki neupravičeno vstopi ali vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, ali kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema.[38]

Kaznivo dejanje vdora v poslovni informacijskega sistema[39] pa je uvrščeno v poglavje o kaznivih dejanjih zoper gospodarstvo in njegova opredelitev je ožja in bolj specialna, saj KZ-1 zahteva, da gre za neupravičen vstop ali vdor v poslovni informacijski sistem ob opravljanju gospodarske dejavnosti.[40] To kaznivo dejanje tako izvrši samo tisti, ki pri gospodarskem poslovanju neupravičeno vstopi ali vdre v informacijski sistem ali ga neupravičeno uporablja tako, da uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema ali neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem, da bi sebi ali komu drugemu pridobil protipravno premoženjsko korist ali drugemu povzročil

35 1. odst. 143. člena KZ-1.

36 25. člen Zakona o varstvu osebnih podatkov-1.

37 221. člen KZ-1.

38 1. in 2. odst. 221. člena.

39 237. člen KZ-1.

40 10. točka 1. odst. 99. člena KZ-1: »Vsaka dejavnost, ki se opravlja proti plačilu na trgu, vsaka dejavnost, ki se za dogovorjeno ali predpisano plačilo opravlja poklicno ali organizirano.«

premoženjsko škodo.[41] Pri tem kaznivem dejanju je torej treba dokazati naklep pridobiti protipravno premoženjsko korist in opravljanje gospodarske dejavnosti ob izvrševanju tega dejanja.

Glede na to, da imamo opravka s kar nekaj kaznivimi dejanji, se seveda najprej zastavi vprašanje razmerja med temi kaznivimi dejanji, oziroma vprašanje stekov, in to na dveh ravneh;

- razmerje med različnimi vrstami podatkov in posledično med ustreznimi kaznivimi dejanji neupravičene pridobitve ali razkritja teh podatkov[42] ter
- razmerje med ustreznimi kaznivimi dejanji neupravičenega razkritja ali pridobitve podatkov na eni strani in »računalniškimi« kaznivimi dejanji[43] na drugi strani.

Na vprašanje, ali gre za pravi ali navidezni stek med različnimi kaznivimi dejanji neupravičene pridobitve ali razkritja podatka, ki ga je mogoče subsumirati pod poslovno skrivnost, osebni podatek, uradno tajnost in/ali poklicno skrivnost, je mogoče odgovoriti posredno. Najprej se je po mojem mnenju treba odločiti, katera lastnost podatka je močnejša in pomembnejša. Z navideznim stekom tako ostane le odgovornost za neupravičeno razkritje ali pridobitev tega podatka. Izjema bi obstajala le v primeru, da KZ-1 pri določeni vrsti podatkov nekega ravnanja ne inkriminira (na primer neupravičena pridobitev poklicne skrivnosti ni inkriminirana v KZ-1), kjer je po mojem mnenju treba dati prednost odgovornosti za neupravičeno ravnanje z drugo vrsto podatkov, kjer ravnanje je inkriminirano. Tako je po mojem mnenju kaznivo dejanje neupravičene izdaje poklicne skrivnosti tako splošno kaznivo dejanje, da v primeru, če gre za razkritje podatka, ki je hkrati poklicna skrivnost na eni strani in poslovna skrivnost ali tajni podatek na drugi strani, storilec odgovarja za specialno kaznivo dejanje izdaje poslovne skrivnosti ali tajnega podatka, (Deisinger, 2002:146) ne pa tudi za izdajo poklicne skrivnosti. Tudi osebni podatek je po mojem mnenju specialen v razmerju do tajnega podatka.

Po drugi strani pa je treba tudi odgovoriti na vprašanje, ali storilec s tem, ko z vdorom v (poslovni) informacijski sistem neupravičeno pridobi ali razkrije podatek,

41 1. odst. 237. člena KZ-1.

42 142., 143., 236. in 260. člen KZ-1.

43 221. in 237. člen KZ-1.

ki ga je mogoče uvrstiti v eno izmed zgornjih kategorij,[44] odgovarja le za neupravičeno razkritje ali pridobitev določenega podatka ali le za vdor v (poslovni) informacijski sistem ali pa za obe kaznivi dejanji hkrati. Ker gre za napad na različne pravne vrednote (varovanje določenih vrst podatkov na eni strani in premoženje oziroma delovanje gospodarskih subjektov na drugi strani), bi bilo po mojem mnenju treba uporabiti pravi stek med obema vrstama kaznivih dejanj. Storilec bi torej moral odgovarjati za obe kaznivi dejanji (relevantno kaznivo dejanje iz 237. ali 221. člena in kaznivo dejanje iz 142., 143., 236. ali 260. člena KZ-1).

4.2 Izvršitveno ravnanje

Pri kaznivem dejanju neupravičene izdaje poklicne skrivnosti KZ-1 določa storitveno inkriminacijo.[45] Enako velja za inkriminacijo kaznivega dejanja zlorabe osebnih podatkov,[46] izdaje in neupravičene pridobitve poslovne skrivnosti[47] ter izdaje tajnih podatkov[48] na eni strani, in vdora v informacijski sistem[49] ter vdor v poslovni informacijski sistem na drugi strani.[50]

Kljub temu, da vse inkriminacije določajo le storitvena izvršitvena ravnanja, pa so na podlagi splošnega dela KZ-1 kaznive tudi opustitve, ki v enaki meri privedejo do enake prepovedane posledice; bodisi do neupravičene pridobitve ali razkritja varovanih podatkov bodisi do vdora v (poslovni) informacijski sistem. Odgovornosti za pravo opustitev po 17. členu KZ-1 torej ni, ker zakonodajalec ni določil nobenega opustitvenega izvršitvenega ravnanja, mogoča pa je odgovornost za neprave opustitve. Za nepravo opustitev gre, ko storilec povzroči prepovedano posledico s tem, ko ne prepreči njenega nastanka. V takem primeru se storilec kaznuje za opustitev, če je imel dolžnost preprečiti nastanek prepovedane posledice in če je opustitev za nastanek take posledice enakega pomena kot storitev (Bavcon et al., 2009: 155).[51] Storilec odgovarja za nepravo opustitev takrat, kadar

[44] po opravljeni analizi stekov, seveda

[45] 1. odst. 142. člena KZ-1.

[46] Glej vse odstavke 143. člena KZ-1.

[47] 236. člen KZ-1.

[48] 260. člen KZ-1.

[49] 237. člen KZ-1.

[50] 221. člen KZ-1.

[51] 3. odst. 17. člena KZ-1.

je povzročil prepovedano posledico s svojo pasivnostjo oziroma z opustitvijo ravnanj, ki bi jih glede na svoj položaj dolžan opraviti. V vsakem primeru odgovornosti za neprave opustitve je treba dokazati, da je imel storilec v razmerju do oškodovanca garantno dolžnost in garantni položaj.

V našem primeru torej uporabnik mobilne naprave s svojo pasivnostjo in opustitvijo dolžnostnih ravnanj varovanja določenih podatkov omogoči razkritje teh podatkov. Odgovornost za neprave opustitve pride v poštev v primeru, ko je uporabnik mobilne naprave dolžan varovati tajnost določenih podatkov, pa opusti dolžnost varovanja s tem, ko ne skrbi primerno za varnost svoje mobilne naprave. Temelj varovalne garantne dolžnosti je v tem, da je uporabnik predhodno prevzel pravno dolžnost varovati določene podatke. Ti podatki torej predstavljajo odvisno kazenskopravno dobrino, ki jo je uporabnik dolžan varovati zaradi svojega pravnega položaja, hkrati pa je prišlo tudi do dejanskega prevzema oblasti nad to dobrino, tako da jo je storilec imel možnost in sposobnost varovati (Bavcon, 2009: 161). To je pomembno zato, ker relevantna kazniva dejanja iz KZ-1[52] določajo, da jih lahko izvrši samo nekdo, ki jih je dolžan varovati. V tem delu gre torej za posebna kazniva dejanja, t.j. pravi delictum proprium, saj osebe brez te zahtevane lastnosti ne morejo izvršiti teh kaznivih dejanj (Bavcon, 2009: 193). Drugače pa velja za neupravičeno pridobitev teh podatkov. Pri teh izvršitvenih ravnanjih je bistvo inkriminacije ravno v tem, da varovane podatke pridobi nekdo, ki ni upravičen do njih in ki jih posledično tudi ni dolžan varovati.

Hkrati lahko najdemo še dodatni vir, tokrat nadzorstvene garantne dolžnosti. Mogoče je utemeljiti, da je mobilna naprava nevarna stvar v oblastnem območju uporabnika (Bavcon, 2009: 162), ki jo je uporabnik dolžan primerno nadzorovati in skrbeti za njeno varnost in za to, da ne postane orodje za izvrševanje kaznivih dejanj s strani tretje osebe. Ker to stališče precej širi cono kriminalnosti, moram opozoriti, da gre v tej fazi le za temelj garantne dolžnosti in da to seveda ne pomeni, da bo v vsakem primeru uporabnik odgovoren za kaznivo dejanje in da so v vsakem primeru izpolnjeni vsi elementi kaznivega dejanja. Tukaj gre le za vprašanje obstoja prvega elementa kaznivega dejanja (bit inkriminacije z ravnanjem), obstoj vseh ostalih elementov kaznivega dejanja pa je šele treba ugotoviti. Predvsem bo vprašljiva uporabnikova krivda, oziroma odgovor na vprašanje, ali uporabniku lahko očitamo, da je bil v skrbi za varnost svoje mobilne naprave tako malomaren, da mu lahko pripišemo odgovornost za kaznivo dejanje.

[52] Izjema je zloraba osebnih podatkov.

5 Zaključek

Razvoj in uporaba mobilnih naprav ter računalništva v oblaku se ne bo ustavil, kvečjemu ravno nasprotno. To dokazujejo tudi že omenjen raziskave. Tudi v prihodnosti lahko pričakujemo vedno večjo uporabo omenjenih tehnologij na eni strani in na drugi vedno več modernih groženj, ki bodo posamično ali v kombinaciji (Markelj in Bernik, 2011) ogrožale podatke in naprave. Posamezniki se bodo morali zavedati pomena varovanja mobilnih naprav in podatkov, v nasprotnem primeru bodo potencialne žrtve zlorab mobilnih naprav, odtujitve podatkov in kibernetske kriminalitete. Na dojemanje slednjega imajo velik vpliv tudi mediji (Meško in Bernik, 2011), zato je izobraževanje uporabnikov v središču varovanja podatkov in moderne tehnologije. Samo z izobraževanjem in ozaveščanje uporabnikov mobilnih naprav o naprednih tehnologijah in grožnjah, ki jim pretijo, ter njihovih posledicah, lahko dosežemo zadosti visoko raven varnosti. Rezultati raziskave – nekateri podati iz nje so bili omenjeni v tem članku – so nam jasno prikazali, katere vrste podatkov uporabniki hranijo na svojih mobilnih napravah, kako ravnajo z njimi in s kakšnimi nameni jih uporabljajo. Uporabniki se bodo morali odločiti, s kakšnimi podatki bodo upravljali s pomočjo mobilnih naprav, in podatkom določiti »vrednost« oz. oceniti škodo, ki bi nastala, če bi jih izgubili. To pomeni, da morajo uporabniki odločiti, katere podatke bodo shranjevali in obdelovali na mobilni napravi in v oblaku ter katere bodo prenašali prek različnih internetnih povezav. Varnostna rešitev kot je enkripcija bi morala postati standard, drugače (v primeru uresničitve katere od groženj) lahko uporabnik postane žrtev in je hkrati še kazensko odgovoren za izgubo določenih podatkov.

Razširjenost uporaba mobilnih naprav odpira več zanimivih kazenskopravnih vprašanj. Načeloma velja, da splošni del KZ-1 zadošča tudi za obravnavo različnih vprašanj v zvezi z odtujitvijo podatkov prek uporabnikove mobilne naprave, zlasti glede načina izvršitve relevantnih kaznivih dejanj. Menimo, da trenutno veljavna kazenska zakonodaja v zadostni meri omogoča vzpostavitev kazenske odgovornosti tako za aktivno nedopustno pridobitev določenih podatkov prek mobilne naprave, kakor tudi za uporabnikovo nezadostno aktivnost v smeri zaščite njegove mobilne naprave, ki je posledično zlorabljena za pridobitev podatkov, ki predstavljajo zaščitene podatke po inkriminacijah iz posebnega dela KZ-1. S tem KZ-1 predstavlja zadostno podlago za uporabnikovo kazensko odgovornost za neprave opustitve, saj uporabnika lahko utemeljimo kot garanta varovalne garantne dolžnosti v razmerju do določenih vrst podatkov, če je bil dolžan varovati te podatke.

Glede kaznivih dejanj, za katera bi uporabnik lahko odgovarjal, se najprej na ravni biti inkriminacije zastavi vprašanje stekov, saj imamo opravka z dvema vrstama relevantnih kaznivih dejanj; KZ-1 ureja dve povsem »računalniški« kaznivi dejanji in štiri kazniva dejanja nedopustnega razkritja in/ali pridobitve določenih vrst podatkov, zato bodo morala sodišča v tem primeru najprej odločiti o razmerju med tema skupina kaznivih dejanj, kasneje pa še o razmerju med posameznimi vrstami podatkov. Menimo, da je v prvem primeru treba uporabiti pravi stek, v drugem primeru pa je treba upoštevati, kateri podatek je specialen in tako storilec lahko odgovarja samo za neupravičeno razkritje in/ali pridobitev takega podatka.

Vprašanje relevantnih inkriminacij, stekov med njimi ter način njihove izvršitve pa predstavljajo le nekaj izmed kazenskopravnih vprašanj, ki se odpirajo ob vse bolj razširjeni uporabi mobilnih naprav.

Zdi se, da se morata s povečevanjem možnosti uporabe mobilne naprave povečati tudi zavedanje in odgovornost njihovih uporabnikov oziroma lastnikov. Pogosteje ko neko napravo uporabljamo in bolj ko je naprave dostopna in razširjena v praksi, manj imamo možnosti, da se kot uporabniki uspešno sklicujemo, da se nismo zavedali potencialnih možnosti za zlorabo ter da nismo poznali možnosti zaščite in je zato nismo uporabljali. Ker postajajo posledice nepazljivosti in neznanja čedalje hujše, je nujen premislek o kazenskopravnih vidikih in posledicah (neustrezne) uporabe mobilnih naprav.

Viri

- Bavcon, L., Šelih, A., Korošec, D., Ambrož, M. in Filipčič, K. (2009). Kazensko pravo, splošni del. Ljubljana: Uradni list.
- Deisinger, M. (2002). Kazenski zakonik s komentarjem, posebni del. Ljubljana: GV založba.
- Glavač, Z. (2009). Računalništvo v oblaku in virtualizacija (Diplomsko delo). Maribor: Fakulteta za elektrotehniko, računalništvo in informatiko.
- Guillemin, A. (2009). Mobile Applications Transform the Financial Adviser. Practice Management Solutions, 10.
- Infiniti Research Limited. (2011). Global Cloud System Management Software Market 2010-2014. Pridobljeno 7. 9. 2011 na http://www.marketresearch.com/Infiniti-Research.
- Juniper Networks (2011). Malicious Mobile Threats Report 2010/2011. Pridobljeno 10. 9. 2011 na http://www.juniper.net/us/en/dm/interop/go.
- Kazenski zakonik, Ur. L. RS, 63/1994, 70/1994, 23/1999, 40/2004.

- Kazenski zakonik-1, Ur. L. RS, 55/2008, 66/2009, 91/2011.
- Lookout (2010). Zlonamerna koda nad zasebnost uporabnikov mobilnikov Android. Racunalniske-novice.com. Pridobljeno 07.09.2011 na http://www.racunalniske-novice.com/novice/mobilna-telefonija/google/zlonamerna-koda-nad-zasebnost-uporabnikov-mobilnikov-android.html.
- Markelj, B., Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. V Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. Konferenca Dnevi slovenske informatike, Portorož, Slovenija, 18.-20. 4. 2011. Ljubljana: Slovensko društvo Informatika.
- Meško, G. in Bernik, I. (2011). Cybercrime: awareness and fear: Slovenian perspectives. V: N. Memon and D. Zeng (ur.). 2011 European Intelligence and Security Informatics Conference [Electronic source]. Athens, 12.-14. 11. 2011 (str. 28-33).
- Rodier, M. (2011). The Year Of Compliance And The Cloud. Wall Street & Technology, 29 (2), 26.
- Zakon o gospodarskih družbah, Ur. L. RS, št. 65/2009, 33/2011, 91/2011.
- Zakon o tajnih podatkih, Ur. L. RS, št. 50/2006, 9/2010, 60/2011.
- Zakon o varstvu osebnih podatkov, Ur. L. RS, št. 94/2007.
- Završnik, A. (2005). Kibernetična kriminaliteta – (kiber)kriminološke in (kiber)viktimološke posebnosti »informacijske avtoceste«. Revija za kriminalistiko in kriminologijo, 248-260.
- Završnik, A. (2007). Kazniva dejanja s področja kibernetske kriminalitete. V A. Šelih (ur.) Sodobne usmeritve kazenskega materialnega prava (str. 453-492). Ljubljana: Inštitut za kriminologijo.

O avtorjih

dr. Sabina Zgaga, univ. diplomirana pravnica, docentka za kazensko pravo na Fakulteti za varnostne vede.

Blaž Markelj, univ. diplomirani organizator – informatik, predavatelj za informacijsko varnost na Fakulteti za varnostne vede.

Varovalni mehanizmi e-banke z vidika uporabnosti, funkcionalnosti in enostavnosti

Lucija Tomšič Zupan, Igor Bernik

Prispevek opredeljuje vrste varnostnih elementov v e-bančništvu, njihov vpliv na uporabnost in enostavnost uporabe rešitev. Prispevek prikazuje težave, ki se v praksi pojavljajo zaradi neustrezno uporabljenih varnostnih mehanizmov. S premišljeno uporabo varnostnih mehanizmov se varnost e-bančnih storitev poveča pod pogojem, da vpeljani varnostni mehanizmi ne vplivajo na zmanjšanje uporabnosti in enostavnosti uporabe e-bančnih storitev. Učinki neustreznih varovalnih mehanizmov, ki od uporabnika zahtevajo nadpovprečno dobro poznavanje informacijskih tehnologij in so nepraktična, neživljenjska, lahko ustvarijo učinek, ki je v nasprotju z vpeljanim varovalnim mehanizmom. Podan je opis priporočljivih točk pozornosti pri vpeljavi varovalnih mehanizmov, ki jih narekujejo dobra praksa, izkušnje stroke in rezultati raziskav na tem področju. Ugotovitve prispevka so pomembne za nadaljnji razvoj, saj so smernice za snovalce in naročnike rešitev ter regulatorje e-bančništva. Prikazane zahteve pri vpeljavi varovalnih mehanizmov v e-bančnih storitvah služijo kot osnova za nadaljnje ukrepe poslovnih bank in ponudnikov rešitev pri načrtovanju spletnega in mobilnega bančništva. Pri načrtovanju e-bančnih rešitev je potrebno nameniti posebno pozornost funkcionalnosti bančnih storitev in enostavnosti uporabe, zato bi morala biti evalvacija rešitev z vidika uporabnosti in funkcionalnosti sestavni element v procesu načrtovanja in izdelave rešitev.

KLJUČNE BESEDE: e-bančništvo, varovanje, mehanizmi, avtentikacija uporabnikov, avtorizacija transakcij

1 Uvod

Pri današnjih zlorabah elektronskega bančništva igra veliko vlogo organizirani kibernetski kriminal. Posamični napadi so napredovali v dobro organizirana kazniva dejanja organiziranih skupin (Zupan in Vodopivec, 2010). Nove metode organiziranega kriminala zahtevajo tudi prilagajanje policijske dejavnosti (Lukman in Bernik, 2012). V zadnjem obdobju je slovenska policija (2012) zaznala povečano dejavnost kriminalnih združb, ki so napadle več uporabnikov e-bank (na-

padi na pametne kartice, ki so bile puščene v računalniški opremi podjetij in napad na uporabnike SKB e-banke s pomočjo preusmerjanja na lažne strežnike (SKB, 2012, Slovenska policija, 2012). Večino on-line napadov se še vedno izvede s pomočjo napadov, ki izkoriščajo naivnost uporabnikov, slabo zaščitene računalnike ali zastarelo aplikativno rešitev za izvajanje storitev e-bančništva, ki jo banke niso nadgradile, kljub znanim napadom (Moeckel, 2010). Razlog za neustrezno nadgrajene e-bančne rešitve je najverjetneje v tem, da banke še niso postale tarča napada oz. napadi niso presegli kritične točke, na kateri je vrednost investicije manjša od stroškov povzročene škode. Večina držav EU je sprejela zakonodajo (tudi Slovenija), po kateri morajo banke v primeru realizirane grožnje (uspešnega napada in odtujitve sredstev) kriti nastalo škodo. Zakonska določila se spreminjajo v prid zaščite uporabnika, saj mu je banka dolžna povrniti ukradena sredstva v znesku nad 150 EUR (ZPlaSS, 2011), vendar pod pogojem, da je uporabnik upošteval priporočila banke. V primeru, da pride do realizacije škode, je potrošnik tisti, ki mora dokazati, da ni ravnal malomarno oz. je uporabil vse varnostne ukrepe, ki jih je predpisala banka. Po našem mnenju so razlogi za nepravilno uporabo storitev e-banke v pomanjkljivem tehničnem znanju uporabnikov. Slednje pa vodi tudi v tveganje zlorabe oz. nastanek škode. Trenutno tako banke kot regulatorji ne namenjajo dovolj pozornosti področju uporabnosti, funkcionalnosti in enostavnosti uporabe rešitev. Praksa kaže, da uporabniki pogosto ne uspejo dokazati, da njihova dejanja niso bila naklepna ali plod malomarnosti (ZPS, 2010). Študija, ki jo je izvedel Guardian Analitics (2011) je pokazala, da v kar 60 % primerov uporabniki niso dobili povrnjenih sredstev v primeru zlorabe e-banke.

2 Metode

Uporabljena je bila opisna metoda na podlagi pregleda literature, ustreznih študij in praks, ki se ukvarjajo z uporabnostjo sistemov e-bančništva. Uporabljena je bila primerjalna metoda posameznih mehanizmov z vidika uporabnosti, enostavnosti uporabe in funkcionalnosti, ki daje celovit pregled uporabnosti in varnosti elektronskega bančništva. Na podlagi raziskav in analiz preteklih raziskav je mogoče izvesti sistematično ocenjevanje varnostnih ukrepov z vidika uporabnosti.

3 Pregled varovalnih mehanizmov in njihova uporabnost

Z naraščanjem števila uporabnikov in groženj e-bančništvu se implicitno povečujejo potrebe po varnem in uporabniku prijaznem e-bančništvu. Zahteve po varovanju računalniške opreme, ki jih banke postavljajo uporabnikom, so obsežne in kompliciranе, zato je utemeljeno vprašanje, ali jih uporabniki sploh razumejo.

Uporabnik mora pri uporabi spletne banke upoštevati številna navodila banke za uporabo varne računalniške opreme s primernimi zaščitnimi programi in skrbno varovati avtentikacijske elemente za dostop do banke. V nadaljevanju opisujemo varovalne mehanizme ter njihovo odpornost na grožnje ter uporabnost z vidika funkcionalnosti, enostavnosti in sistemske neodvisnosti.

3.1 Varovalni mehanizmi in njihova odpornost na grožnje

Varovalne mehanizme v grobem delimo na identifikacijo in avtentikacijo uporabnika ter avtorizacijo transakcije. V EU so bile številne oblike varovalnih mehanizmov uvedene kot odgovor na pojavljanje novih groženj. Tabela 1 ponazarja odpornost trenutno vpeljanih varovalnih mehanizmov na najbolj aktualne oz. pogoste grožnje. Podatki v tabeli so bili pridobljeni s proučitvijo predhodnih študij in znanih napadov.

Grožnja	Identifikacija uporabnika				Avtentikacija uporabnika			Avtorizacija transakcije				
		Digitalno potrdilo		EMV CAP	Geslo	OTP	Varnostno vprašanje	Brez	OTP	iTAN-ni povezave s transakcijskimi podatki	mTAN-povezava s transakcijskimi podatki (SMS)	Avtorizacijska koda - (EMV-CAP)
		na disku	na pametnem mediju									
Ribarjenje	x	x			x		x	x				
Zvabljanje	x	x			x	x	x	x	x	x		
Mož v sredini	x	x	x		x		x	x	x	x	x	
Mož v brskalniku	N/A	N/A	N/A	N/A	N/A	N/A	N/A	x	x	x	x	

Tabela 1: Prikaz odpornosti varovalnih mehanizmov na aktualne grožnje e-banki (vir: lasten)

Varnostni mehanizem (dvofaktorska avtorizacija z EMV-CAP), ki je trenutno priznan kot najbolj učinkovit obrambni mehanizem proti vsem novejšim oblikam napadov (ribarjenje[53], izvabljanje[54], MitM[55], MitB[56]), pa že kaže tudi svoje slabosti, saj:

[53] Ribarjenje (phishing) je eden od najpogostejših napadov na e-bančništvo, pri katerem v običajnem scenariju napadalec uporabniku pošlje elektronsko sporočilo, ki uporabnika skuša zvabiti na lažno stran banke, in to pod pretvezo, da se mora zaradi preverjanja podatkov ali aktiviranja računa vnovič prijaviti in opraviti preveritev. Če uporabnik na lažni spletni strani vnese svoje podatke, jih napadalec kasneje lahko izkoristi za prijavo v e-banko in krajo sredstev z računa.

[54] Zvabljanje (pharming) je vrsta napada, pri katerem se v sistemu domenskih imen uporabnika preusmeri na lažno spletno mesto z namenom kraje in zlorabe uporabnikovih avtentikacijskih elementov oz. kraje identitete.

[55] Mož v sredini (napad man-in-the-middle ali MitM) je vrsta napada, pri katerem se prevarant postavi na točko v omrežju med uporabnikom in strežnikom banke ter spreminja podatke o računu in prometu ali odtuji avtentikacijske podatke uporabnika.

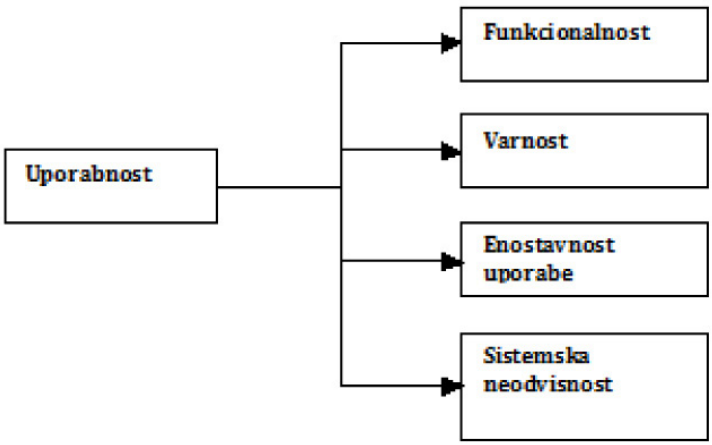
[56] Mož v brskalniku (man-in-the-browser ali MitB) je vrsta napada, pri katerem trojanski konj okuži spletni brskalnik tako, da ta lahko spreminja spletno stran ali vsebino transakcije ali izvede plačilno transakcijo brez vednosti uporabnika.

- otežuje enostavnost rabe (uporabniki ne razumejo tehnologije, varnostnih zahtev in zamenjujejo korake oz. vrstni red avtentikacijskih elementov, ki jih morajo uporabiti v posameznem koraku);
- onemogoča fleksibilnost (uporabniki niso več mobilni). Mobilnost je na splošno problem in preveč oglaševana prednost, saj je uporabnik primoran delati na zaupanja vredni napravi, ki mora biti skladna z enakimi varnostnimi standardi kot domači računalnik – javni računalniki (cybercaffe ipd.) tako ne pridejo v poštev. Problem je sicer rešljiv z vpeljavo mobilnih naprav, vendar pa so te izpostavljene drugim/dodatnim tveganjem;
- podaljšuje čas uporabe, čas za izvedbo prijave, transakcije;
- ima lahko nepremišljena raba dvofaktorske avtentikacije (primer EMV-CAP) negativne učinke, v ekstremnem primeru pa lahko ogrozi celo človeška življenja (Drimer, Murdoch in Anderson, 2009).

Na podlagi zgornjih ugotovitev bankam in razvojnim podjetjem svetujemo, da pred uvedbo podrobneje analizirajo izkušnje bank, ki so že uvedle podobne rešitve ter pripravijo ustrezne strategije. Bankam, ki so že uvedle tovrstno tehnologijo, pa priporočamo, da pozorno analizirajo in proučijo potencialne napake in težave uporabnikov (npr. s pomočjo analize trendov in podatkov, ki jih zbira uporabniška podpora). Nadalje je mogočih več pristopov, ki so opisani v poglavju 3.3.

3.1 Uporabnost, funkcionalnost in enostavnost uporabe varovalnih mehanizmov

Uporabnost e-banke je skupek funkcionalnosti, varnosti, enostavnosti uporabe in sistemske neodvisnosti. Varnost e-banke igra osrednjo vlogo tudi pri zaupanju komitentov, po nekaterih raziskavah celo vpliva na odločitev uporabnika o tem, ali bo izbral določeno banko. Nekatere raziskave (Hussain, Brganza in Morabito, 2007; Munoz-Leiva, Luque-Martínez, in Sanches-Fernandez et al., 2010) tudi kažejo, da sta tako uporabnost kot varnostna rešitev med ključnimi dejavniki uspeha pri vpeljavi in zaupanju uporabnikov v e-banke. Po raziskavi (Hussain et al., 2007) je uporabnost na prvem mestu po pomembnosti, varnost e-banke pa na drugem. Številne raziskave nakazujejo, da sta varnost in uporabnost povezani oz. da šibka uporabnost aplikacije zmanjšuje varnost sistema (Weir, Douglas, Carruthers in Mervyn, 2009; Alzomai Alfayyadh, Audun in McCullagh, 2008). V slovenskem prostoru je bil zaznan trend stagnacije v prenovi varnostnih mehanizmov e-bank (Zupan in Bernik, 2012).



Slika 1: Soodvisnost varnosti, uporabnosti, funkcionalnosti, enostavnosti uporabe in sistemske neodvisnosti (vir: lasten)

Težava današnjih e-bančnih sistemov je v tem, da mnogi niso doživeli celovite prenove, temveč so se z leti dograjevali. S pojavom novih groženj so se na obstoječe rešitve dodajali dodatni varovalni mehanizmi, ki pa hromijo uporabnost in funkcionalnost rešitev ter podaljšujejo čas, ki ga uporabnik potrebuje za izvedbo transakcije. Takšne rešitve imajo za uporabnike številne neželene posledice, predvsem zmanjšanje uporabnosti, fleksibilnosti, udobja in nenazadnje tudi varnosti. Na drugi strani sta fleksibilnost in varnost med pogostimi prednostmi, ki jih banke oglašujejo pri uporabi e-bančništva, kar pa je zavajanje uporabnikov (Mannan in Oorschot, 2007).

3.2 Dosedanje raziskave na temo uporabnosti varovalnih mehanizmov e-banke

S področjem uporabnosti varovalnih mehanizmov za avtentikacijo uporabnikov v e-bančnih rešitvah se je ukvarjalo veliko avtorjev. Avtorji Weir (et al., 2009), Mannan (et al., 2007), Alzomai (et al., 2008), Hertzum (et al., 2004) ter Gunson, Marshall, Morton in Jack (2011) v svojih študijah ugotavljajo naslednje:

- Varnostni mehanizmi, ki niso uporabniku prijazni, zmanjšujejo varnost e-banke.
- Glavnina uporabnikov ni pripravljena žrtvovati uporabnosti in enostavnosti na račun varnosti e-banke.

- Dvofaktorske metode z vidika uporabnosti niso najbolje ocenjene (število korakov, število varnostnih kod).
- Naprave za izdelavo varnostnih kod so zaradi njihove velikosti neprimerne za prenašanje in zmanjšujejo mobilnost uporabnikov.
- Večina napak se naredi pri uporabi naprav, ki nimajo intuitivnih uporabniških vmesnikov.
- Zahteve in priporočila bank glede zagotavljanja varnega okolja e-banke so za povprečnega uporabnika prezahtevni (upravljanje požarnih zidov; nameščanje protivohunske in protivirusne programske opreme; uporaba e-banke le na opremi, ki je skladna z visokimi varnostnimi določili, je redno nadgrajevana z varnostnimi popravki in ustrezno protivirusno opremo).
- Od uporabnikov se pričakuje, da ima nadpovprečno dobro tehnično znanje (preverjanje veljavnosti strežniškega certifikata, ocenitev ali je na napravo nameščena vohunska programska oprema, proučevanje sporazumov o programski opremi).

Alzomai in soavtorji (2007) so tudi ugotovili, da večine zahtev, ki so jo jih svojim strankam postavile kanadske banke, ne morejo izpolniti niti nadpovprečno informacijsko pismeni uporabniki. V študiji nakazujejo, da je stanje pri povprečnem uporabniku e-banke še slabše. V raziskavi, ki so jo naredili Weir in njegovi sodelavci (2009) so med drugim preverjali ali bodo uporabniki opazili, da je bil pri izvedbi transakcije zamenjan ciljni račun (vrsta napada znana kot MitM spada med naprednejše oblike napada). Z eksperimentom so pokazali, da večina uporabnikov zamenjave ciljnega računa ni opazila. Varnostni problem, ki izhaja iz tega, da uporabniki ne opazijo podrobnosti transakcije, je problem uporabnosti, ne tehnične varnosti (Alzomai et al., 2007), zato so omenjeni avtorji tudi mnenja, da je v takih primerih potrebno povečati funkcionalnost varovalne rešitve (ki bo npr. zagotovila, da uporabnik ne bo spregledal zamenjave ciljnega računa) in ne nujno spremeniti varnostnih mehanizmov.

Avtorji Hertzum, Jørgensen in Nørgaard (2004), Alzomai (2008) in Lampson (2009) v predhodnih študijah ugotavljajo, da kompliciranе varnostne rešitve pri uporabnikih povzročijo, da ti:

- zaobidejo kontrole,
- ignorirajo varnostna opozorila, ker jih ne razumejo ali jih je preveč,

- napačno uporabljajo rešitev,
- prenehajo uporabljati rešitev.

V drugih študijah (Mannan et al., 2007) je bil ugotovljen razkorak med percepcijo uporabnikov in bank o tem, kako se deli odgovornost za varnost. Uporabniki so prepričani, da bi morale banke poskrbeti za ustrezno varnost oz. od bank pričakujejo, da bodo poskrbele za varnost sistemov.

Banke zagovarjajo stališče, da se odgovornost za varnost e-banke deli med uporabnike in banko. Mannan oporeka temu prepričanju, saj ugotavlja, da pričakovanja banke, da bodo uporabniki uspeli izpolnjevati vse varnostne zahteve, niso realne. Banke predpostavljajo, da je odgovornost za preverjanje pravilnosti avtorizacijskega sporočila na strani uporabnika, a če je velik delež uporabnikov nezmožen uporabiti metodo pravilno, bi morale banke znova oceniti svojo domnevo (Alzomai et al., 2008).

E-banka je primerno uporabna le, če so izpolnjeni vsi dejavniki oz. so primerno zagotovljeni njeni sestavi; funkcionalnost[57], enostavnost uporabe[58], varnost[59], sistemska neodvisnost[60] in posledično tudi mobilnost uporabnika. Tabela 2 prikazuje ocene uporabnosti in operativne stroške posameznih varovalnih mehanizmov. Podatki v tabeli so bili deloma pridobljeni iz proučitve predhodnih študij, deloma pa po oceni avtorjev.

---

57 **Funkcionalnost** rešitve je v kontekstu varovalnih mehanizmov e-banke definirana, kot nabor učinkovitih mehanizmov, skladnih z varnostnimi cilji, ki jih želimo doseči pri doseganju nivoja zaščite e-banke.

58 **Enostavnost uporabe** vključuje razumljivost, intuitivnost uporabljenih varovalnih mehanizmov za končnega uporabnika ter enostavnost pomnjenja uporabljenih postopkov in korakov za uporabnika. Pomembno je tudi, da se jih uporabniki hitro in brez večjih naporov naučijo pravilno uporabljati tako, kot je bilo predvideno s strani načrtovalcev rešitev.

59 **Varnost** e-banke predstavlja nabor varovalnih mehanizmov, ki jih e-banka mora vsebovati, da je dosežen primeren nivo varnosti in zaščite glede na trenutno aktualne grožnje e-banki.

60 **Sistemska neodvisnost je lastnost var**ovalnega mehanizma, ki omogoča njegovo uporabo na poljubnem informacijskem sistemu. Kot taka, uporabnikom omogoča mobilnost oz. geografsko neodvisnost.

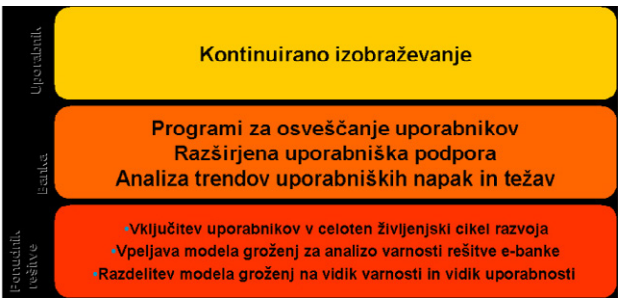
Avtentikacija/avtorizacija	Uporabnost					Operativni stroški
	Funkcionalnost	Mobilnost uporabnika	Sistemska neodvisnost	Enostavnost uporabe	Varnost	
Uporabniško ime in geslo za enkratno uporabo	S	V	S	V	N	N
Digitalno potrdilo na disku za identifikacijo	N	N	S	S	N	S
Digitalno potrdilo na pametnem mediju za identifikacijo	S	N	N	S	V	S
Digital certificate for transaction authorization	V	S	S	S	V	V
EMV-CAP za identifikacijo	S	S	S	S	V	V
EMV-CAP za avtorizacijo transakcije	S	S	S	N	V	V
Digitalno potrdilo za identifikacijo na mobilni napravi	V	V	N	S	V	S
SMS za avtorizacijo transkacije	S	V	N	N	S	S

Tabela 2: Prikaz ocene uporabnosti in stroškov posameznega varovalnega mehanizma e-banke (vir: lasten)

3.3 Možni pristopi k doseganju uporabne varnosti e-banke

K zagotavljanju večje uporabnosti in varnosti e-banke je mogoče pristopiti na različnih nivojih. Te pristope v grobem delimo na (Tomšič Zupan in Bernik, 2012):

- vključitev uporabnikov v celoten razvojni življenjski cikel (načrtovanje in testiranje),
- vpeljavo modela groženj (OWASP, 2012),
- razdelitev modela groženj z vidika varnosti in uporabnosti,
- uporabo programov za ozaveščanje uporabnikov,
- vpeljavo zaupanja vrednih naprav in
- razširitev uporabniške podpore.



Slika 2: Pristopi k povečanju uporabnosti rešitev na različnih nivojih

Pri vpeljavi varovalnih mehanizmov e-banke morajo tako načrtovalci in razvojniki (ponudniki) rešitev e-bank kot tudi banka proučiti vpliv na uporabnost in funkcionalnost rešitev, z namenom slediti varnostnim ciljem in preprečitvi zlorabe.

4 Zaključek

Na podlagi predhodnih študij in prakse ocenjujemo, da banke nimajo ustreznih povratnih informacij o tem:

- ali so uporabniki sposobni izpolniti vse naštete zahteve,
- kakšne so dejanske kompetence uporabnikov,
- kako uporabniki razumejo varnostne zahteve,
- kako varnostni mehanizmi vplivajo na enostavnost njihove uporabe in
- ali so uporabniki pripravljeni še naprej uporabljati e-banko.

Rešitev problema je v rednem izvajanju postopkov analize tveganj s strani razvojnih kadrov ter vključitvijo uporabnikov v proces analize, testiranje in verificiranje aplikacije. Da bi banke lahko zagotavljale varne, a tudi uporabne rešitve, morajo nujno vzpostaviti postopke in mehanizme za pridobivanje povratnih informacij uporabnikov. Banke bi morale uveljaviti sistematično pridobivanje povratnih informacij, predvsem pa premisliti, kako in katere podatke bodo pridobivale (npr. prek centra za pomoč uporabnikom) in jih v nadaljevanju sistematično analizirale. Na podlagi analize strukturiranih podatkov bi morale prilagoditi rešitve e-banke, pripraviti ustrezna navodila ter izobraževanja, z namenom zmanjšanja napak in možnosti napadov. Avgustovski primer (Slovenska policija, 2012) je konkretno nakazal problematiko pomanjkljivo izvedenih scenarijev ogroženosti že v fazi analize in oblikovanja/načrtovanja rešitev, kot tudi neučinkovito ozaveščanje uporabnikov. Ozaveščanje uporabnikov je še vedno eno ključnih področij pri uspešnem zagotavljanju varnosti. Pri sedanjem načinu dela nismo opazili, da bi banke od svojih uporabnikov zbirale povratne informacije o tem, ali so se seznanili z vsemi njihovimi zahtevami in priporočili glede pričakovane varnostne zaščite. Priložnosti za banke vidimo tudi v vpeljavi sistemov za e-učenje, saj se je prav to izkazalo kot ekonomična možnost informiranja velikega števila ljudi, poleg tega pa ponuja tudi različne oblike preverjanja pridobljenega znanja oz. pošiljanje povratne informacije. Opisani pristop je lahko predvsem v korist bankam, da zmanjšajo tveganja in se bolje pripravijo na prihodnje grožnje.

Na področju evalvacije uporabnosti rešitev e-bančništva in ozaveščanja uporabnikov zaznavamo največji primanjkljaj, hkrati pa največjo priložnost in tveganje, zato ocenjujemo, da je nadaljnje raziskovanje tega področja nujno.[61]

Viri

- AlZomai, M. Alfayyadh, B. Audun, J., McCullagh, A., (2008), An Experimental Investigation of the Usability of Transaction Authorization in Online Security Systems, Conferences in Research and Practice in Information Technology (CRPIT), Vol 81.
- Drimer S., Murdoch S.J., in Anderson R. (2009) Optimised to Fail: Card Readers for Online Banking, pridobljeno 5. 12. 2011 na: http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf.
- Gunson, N., Marshall, D., Morton, H., Jack, M., (2011), User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking, Computers & Security, Volume 30, Issue 4, June 2011, Pages 208–220.
- Guardian Analitics, (2011), Business Banking Trust Study, Ponemon Institute, pridobljeno 14.8.2012 na: http://www.guardiananalytics.com/index.php
- Hertzum, M., Jørgensen, N., Nørgaard, M., (2004), Usable Security and e-Banking; Ease of Use vis-a-vis Security, Australasian Journal of Information Systems, Vol 11, št. 2.
- Hussain, M., Brganza A., Morabito V, (2007), A Survey of Critical Success Factors in e-Banking : An Organizational Perspective, European Journal of Information systems, 16, 511-524.
- Lampson, B., (2009), Usable Security: How to Get it, Communications of the ACM, Vol. 52, št. 11, 25-27.
- Lukman, M., Bernik, I., (2012), Kibernetski napadi na sisteme kritične infrastrukture – pregled najpogosteje uporabljenih tehnik in zadnji trendi digitalnih groženj, Konferenca informacijske varnosti, januar 2012, Ljubljana.
- Mannan, M., Oorschot, P C Van (2007), Security and Usability: The Gap in Real-World Online Banking, New Security Paradigms Workshop (NSPW), New Hampshire.
- Moeckel, C., Abdallah, A.E., (2010), Sixth International Conference on Information Assurance and Security, IEEE.
- Muñoz-Leiva, F., Luque-Martínez, T., Sanches-Fernandez, J., How to Improve Trust Toward Electronic Banking, Online Information Review, Vol. 34 Iss: 6 pp. 907 – 934, pridobljeno 14. 6. 2012 na http://dx.doi.org/10.1108/14684521011099405
- OWASP, (2012), Application Threat Modeling, pridobljeno 10. 9. 2012 na: https://www.owasp.org/index.php/Application_Threat_Modeling

61 Za podrobnejšo analizo uporabnosti in varnosti e-banke preberite prispevek, ki je bil predstavljen na konferenci »Criminal Justice and Security in Eastern and Central Europe«, (Tomšič Zupan, Bernik, 2012).

- Slovenska policija, (2012), Ste se po uporabi odjavili iz sistema elektronskega bančništva? Policija svetuje varno uporabo spletnih storitev, pridobljeno dne 2. 8. 2012 na: http://www.policija.si/index.php/novinarsko-sredie/index.php?option=com_content&view=article&id=63863
- SKB, Priporočila za varno uporabo spletnega bančništva, (2012), pridobljeno dne 21. 8. 2012 na: http://www.skb.si/opozorilo
- Tomšič Zupan, L., Bernik I., (2012), e-banking Security vis-a-vis Usabitliy, Functionality and Ease of Use, Criminal Justice and Security in Central and Eastern Europe, September, Ljubljana.
- Weir, C. S., Douglas, G., Carruthers, M., Mervyn, J. (2009), User Perceptions of Security, Convenience and Usability for e-banking Authentication Tokens, Computers & Security, 28, 47-62.
- Zahid, N., Mujtaba, A., Riaz, A., (2010), Consumer Acceptance of Online Banking, European Journal of Economics, Finance and Administrative Sciences.
- Zakon o plačilnih storitvah in sistemih [ZPlaSS], (2009, 2011) Ur.l. RS, št. 58/2009 , Ur.l. RS, št. 34/2010, 9/2011-ZPlaSS-B
- Zveza potrošnikov Slovenije, (2010), pridobljeno 25. 8. 2012 na: http://www.zps.si/osebne-finance/varnost-placil/oskodovanje-potrosnikov-pri-uporabi-spletne-banke.html?Itemid=666
- Zupan, L., Bernik I., (2012), Zahteve za varovanje e-bančnih storitev – izzivi varovanja, Konferenca informacijske varnosti, pridobljeno 7. 6. 2012 na: http://www.fvv.uni-mb.si/KonferencaIV/zbornik/Zupan_Bernik.pdf.
- Zupan, L. in Vodopivec T. (2010); Vloga revizorja informacijskih sistemov pri zagotavljanju varnosti in kakovosti e-bančnih storitev, 14. Konferenca revizorjev informacijskih sistemov, Zbornik str.161-201

O avtorjih

Lucija Tomšič Zupan, od leta 2006 certificirani vodja informacijske varnosti (CISM), od leta 2010 interna revizorka bančnih informacijskih sistemov.

Igor Bernik, prodekan za izobraževalno dejavnost, vodja katedre za informacijsko varnost na Fakulteti za varnostne vede, Univerza v Mariboru.

Trendi uporabe mobilnih naprav

Blaž Markelj, Igor Bernik

Mobilne naprave zaradi naprednega tehnološkega razvoja in preproste uporabe predstavljajo pomemben segment v procesu digitalnih komunikacij in so ena izmed najpogosteje uporabljenih možnosti za dostop do kibernetskega prostora. Neprestana dosegljivost in možnosti izmenjevanja podatkov so za mlade ključni elementi uporabe mobilnih naprav.

Pomembna vidika uporabe mobilnih naprav sta informacijska varnost in varno ravnanje z mobilno napravo, za kar je potrebno poznavanje/zavedanje groženj in mogočih varnostnih rešitev. Skozi proces izobraževanja/ozaveščanja je potrebno vzpostaviti višjo stopnjo informacijske varnosti pri uporabi mobilnih naprav.

Tako vzpostavimo ravnotežje med vplivom groženj, poznavanjem, uporabo varnostnih rešitev in potrebno stopnjo varnosti. Rezultati opravljene raziskave kažejo, da študentje slabo poznajo celovito delovanje mobilnih naprav in pripadajoče programske opreme. Ogroženi so, ker se ne zavedajo groženj ter ne poznajo in/ali ne uporabljajo obstoječih varnostnih rešitev in ker z napravami ne ravnajo vestno. Zanimivo je dejstvo, da se njihovo poznavanje groženj ustavi pri standardnih grožnjah, ki so znanje že iz preteklosti, medtem ko novodobnih groženj, ki pretijo uporabnikom mobilnih naprav, mladi ne poznajo. Enako velja za varnostne rešitve, pri katerih je za uporabnike problem celo uporaba preprostih varnostnih rešitev, ki jih omogočajo že mobilne naprave same. V prispevku bodo predstavljeni nekateri rezultati in predlagane smernice nadaljnjega razvoja informacijske varnosti pri uporabi mobilnih naprav med študenti.

KLJUČNE BESEDE: grožnje, mobilne naprave, informacijska varnost, mladi

1 Uvod

Sodobno družbeno okolje od posameznika zahteva neprestano dosegljivost in možnost hitrega dostopa do informacij. Tudi potreba po ažurnih informacijah iz dneva v dan narašča, to pa se odraža v potrebi po neprestanem dostopu do kiber-

netskega prostora. V preteklosti je komunikacija med mladimi potekala z medosebnimi stiki v živo, danes pa se spoznavanje in komunikacija vse bolj selita v kibernetski prostor. Socialna omrežja, internetne strani, namenjene spoznavanju in druženju, ter številni programi za povezovanje omogočajo enostavno in hitro komuniciranje. Danes že kratka nedostopnost do družabnih omrežij, spleta in drugih komunikacijskih kanalov mladim predstavlja nesprejemljivo dejstvo. O tem priča tudi podatek, da se število uporabnikov interneta dnevno povečuje, ravno tako pa se povečuje tudi razmerje med stacionarnim in mobilnim internetom, in sicer v prid slednjega (comShore, 2011).

V zanosu novosti, ki jih prinašajo mobilne naprave[62], pogosto pozabljamo na vidik (informacijske) varnosti. Uporabnikov mobilnih naprav ne omejuje njihovo neznanje, saj lahko te naprave veliko stvari naredijo avtomatsko (npr: iskanje brezžičnih omrežij, posodabljanje programske opreme itn.). Vprašati pa se je treba, ali si to sploh želimo, če upoštevamo varnostni vidik. Ali zaupamo avtomatiziranemu sistemu upravljanja naprave, pri čemer kot njeni lastniki in uporabniki dejansko ne vemo, kaj se dogaja v ozadju?

Splet in virtualno okolje ponujata številne prednosti, istočasno pa tudi nevarnosti (Bernik in Prislan, 2012). Dnevno lahko beremo o različnih novih grožnjah, ki pretijo uporabnikom mobilnih tehnologij, kar dokazujejo tudi vse raziskave na to temo (npr. Mcafee, 2012). Grožnje, ki lahko odtujijo podatke iz naše mobilne naprave, se izkoristijo za vdor v korporativne informacijske sisteme in posameznika posledično naredijo žrtve ali storilca kibernetske kriminalitete. Motivi za kibernetsko kriminaliteto so različni (Dimc in Dobovšek, 2010), na to, kako kibernetsko kriminaliteto dojemajo uporabniki, pa močno vplivajo mediji (Meško in Bernik, 2011).

Za preprosto uporabno mobilnih tehnologij resnično ni potrebno veliko znanja, če pa si želimo varnosti, je potrebno imeti določeno znanje in se zavedati nevarnosti. V nadaljevanju obravnavamo navade in namene uporabe mobilnih naprav med študentsko populacijo ter njihovo poznavanje groženj, ki pretijo mobilnim napravam, prikazano pa bo tudi, kako se je mogoče zaščititi pred temi grožnjami.

---

62 Med mobilne naprave uvrščamo predvsem naprave, ki imajo prilagojene operacijske sisteme kot so iOS, Android, BlackBerry OS, Windows mobile in so prenosljive. Vse naprave, ki se lahko prenašajo in imajo dostop do kibernetskega prostora omogočeno brez fizične povezave, pa se lahko uvrsti v to kategorijo (tudi prenosniki, prenosne igralne konzole, industrijski čitalci, ...).

2 Mobilne naprave in potencialne grožnje

V zadnjih letih se je prodaja mobilnih naprav izjemno povečala. O tem pričajo številne raziskave. Samo v prvem četrtletju leta 2012 je bilo na območju Zahodne Evrope prodanih 28,2 milijona pametnih mobilnih telefonov (IDC, 2012). Tudi predvidevanja prihodnosti obetajo povečanje obsega prodaje. Organizacija IDC (2012) napoveduje, do bo do konca leta 2012 prodaja pametnih mobilnih telefonov zrasla do številke 686 milijonov, do leta 2015 pa do 982 milijonov. Po raziskavi CEE Telco Industry Report, ki jo je izvedla organizacija GfK Group (2011) in je zajela 15 držav Srednje in Vzhodne Evrope, je Slovenija po uporabi pametnih mobilnih telefonov vodilna, saj kar 27,8 odstotka uporabnikov mobilne telefonije uporablja pametni mobilni telefon, sledijo ji Turčija z 23,7 odstotka in Litva z 18,5 odstotka. Raziskava, ki jo je objavila organizacija comShore (2011), je zajela pet evropskih držav. Merili so povprečno 3-mesečno uporabo, njihove ugotovitve pa jasno kažejo, da so najpogostejši uporabniki mobilnih naprav stari od 25 do 34 let, sledijo uporabniki v starostni skupini od 35 do 44 let. Navedene številke ne presenečajo, saj mobilne naprave s svojim inovativnim pristopom k delu, zmogljivostjo in priročnostjo z lahkoto prepričajo uporabnike.

Prek brezžičnih povezav (WiFi) ali mobilnega omrežja (2G, 3G in LTE tehnologij prenosa podatkov) je mogoče neprestano dostopati do interneta. To dejstvo je zelo pomembno, saj nam premik iz »stacionarnega« v »dinamično« delovanje omogoča neprestan dostop do informacij in možnost komunikacije v vsakem trenutku. S pomočjo raznovrstne programske opreme lahko pošiljamo oz. sprejemamo sporočila, komuniciramo prek različnih kanalov (Facebook, Skype itn.) ali brskamo po spletu.

Glede velikega povečanja števila uporabnikov mobilnih naprav ne smemo mimo dejstva, da ravno tako narašča tudi število groženj, ki pretijo uporabnikom. Te lahko delujejo samostojno ali kombinirano. S stališča informacijske varnosti (ne)varna uporaba mobilnih naprav in vse dotične programske opreme lahko poveča možnost uresničitve groženj, pa naj si bodo to okužba s škodljivo programsko opremo, kraja osebnih podatkov ali druge zlorabe. Številne raziskovalne organizacije v določenih časovnih intervalih poročajo o spremembah oziroma pojavih novih groženj v digitalnem svetu. Hitro lahko potegnemo vzporednice z rezultati raziskav, ki sta jih opravila podjetje Lookout (2011) in Juniper (2011), ki prikazujeta drastično povečanje različnih groženj.

3 Ravnanje mladih z mobilnimi napravami

Zaradi boljšega vpogleda v namen in način uporabe pametnih mobilnih telefonov ter poznavanje groženj in možnih zaščit med populacijo študentov je bila decembra 2011 narejena raziskava z naslovom »Zavedanje groženj mobilnim napravam«. Raziskava je bila izvedena s spletnim vprašalnikom, objavljenim na spletnem portalu »1ka« (www.1ka.si). Informacija o raziskavi je bila študentom posredovana prek elektronske pošte, spletnih socialnih omrežij in z osebnimi povabili. Zbrani podatki so bili analizirani z orodjem SPSS. V analizo je bilo zajetih 281 vprašalnikov. Nekateri vprašalniki niso bili izpolnjeni v celoti, zato se je pri posameznih vprašanih vzorec populacije spreminjal. Med vprašanimi je bilo največ starih med 21 in 25 let, sledi starostna skupina do 20 let, med njimi je bilo 61,5 odstotka žensk in 63,2 odstotka takih, ki imajo že zaključeno srednješolsko izobrazbo.

S pomočjo spletnega vprašalnika smo ugotavljali, koliko študentov ima mobilni telefon in kako ga uporablja. Rezultati so pokazali, da skoraj vsi študenti (99,65 %) uporabljajo mobilni telefon. Velik delež je tudi takih, ki poleg mobilnega telefona, uporabljajo še dodatno mobilno napravo, najpogosteje tablični računalnik.

Na vprašanje o pogostosti uporabe določenih storitev, ki jih omogoča mobilna telefonija, so vprašani lahko izbirali odgovore na Likertovi lestvici z možnimi odgovori: Ne uporabljam, Poznam, vendar ne uporabljam, Imam nameščeno, vendar je ne uporabljam, Uporabljam le občasno, Uporabljam. Z namenom boljše preglednosti rezultatov, smo združili posamezne rubrike in predstavljamo rezultate za področji Ne uporabljam in Uporabljam.

Tabela 1 prikazuje storitve na mobilnih telefonih, ki so med anketiranimi bolj popularne (jih uporabljajo) in katerih storitve ne uporabljajo. Največ vprašanih je povedalo, da uporabljajo mobilno napravo za namene fotografiranja, pisanja sporočil in brskanja po internetu; najmanj pa jih uporablja mobilno bančništvo in odlaganje dokumentov v spletna odlagališča. Sredino po uporabnosti oz. neuporabnosti predstavljajo storitev sinhronizacije stikov in koledarja ter avtomatsko iskanje brezžičnih dostopnih točk. Ugotovitve potrjujejo dejstva, ki smo jih navedli v uvodu, da mladina mobilne telefone v prvi vrsti najpogosteje uporablja kot sredstvo za neprestano komuniciranje (pisanje sporočil, brskanje po internetu, uporaba socialnih omrežij itn.).

Storitve na mobilnem telefonu	Storitev uporabljam
Fotografiranje (n = 211)	92,89 %
Pisanje sporočil (n = 211)	92,42 %
Brskanje po internetu (n = 216)	88,89 %
Poslušanje glasbe (n = 214)	75,70 %
Uporaba socialnih omrežij (n = 214)	66,82 %
Pregledovanje dokumentov (n = 213)	65,26 %
Navigacija (n = 212)	61,79 %
Posodobitev programske opreme telefona (n = 213)	58,69 %
Sinhronizacija elektronske pošte (222)	55,86 %
Nameščanje različnih brezplačnih aplikacij (igre, različni pripomočki ipd.) (n = 215)	55,35 %
Igranje iger (n = 216)	54,63 %
Priklop na market (OVI, Android Market, App Store itn.) in prenos ter nameščanje različne dodatne programske opreme (n = 213)	52,58 %
Avtomatsko iskanje brezžičnih dostopnih točk (n = 214)	51,87 %
Sinhronizacija stikov (n = 216)	47,69 %
Sinhronizacija koledarja (n = 215)	46,51 %
Programska oprema za komunikacijo (Skype, Google+ idr.) (n = 211)	45,50 %
Avtomatski priklop na odprto dostopna brezžična omrežja (n = 215)	45,12 %
Online pregledovanje dokumentov (n = 214)	40,65 %
Nalaganje foto vsebine na splet (n = 215)	33,02 %
Online poslušanje glasbe (n = 215)	30,23 %
Nalaganje video vsebine na splet (n = 214)	24,30 %
Online igranje iger (n = 216)	21,76 %
Nalaganje glasbe na splet (n = 213)	19,25 %
Odlaganje podatkov v oblak (Dropbox, SkyDrive itn.) (n = 211)	15,64 %
Mobilna banka (bančno poslovanje) (n = 214)	8,88 %

Tabela 1: Pogostost uporabe storitev na mobilnem telefonu

Poleg tega, da smo študente spraševali, s kakšnim namenom uporabljajo mobilni telefon, nas je zanimalo tudi, kako dobro poznajo grožnje in ali uporabljajo varnostne rešitve za telefone. Najbolj poznana grožnja med študenti je kraja, (te možnosti se je zavedalo 89,4 odstotka anketiranih), sledijo virusi (83,1 odstotka) in bluetooh vdori ter sledenje. To kaže, da študenti najbolje poznajo tiste grožnje, ki jih že nekaj časa dobro pozna tudi širša javnost, vendar je bolj zaskrbljujoče dejstvo, da zelo slabo poznajo modernejše oblike groženj (malware, rootkit, spyware), ki jih je

v zadnjem obdobju vedno več. Če nam zgoraj omenjeni rezultati omogočajo vpogled v to, kako dobro uporabniki poznajo grožnje, ki pretijo njihovim mobilnim telefonom, ostane vprašanje, kako se tem grožnjam izogniti oz. Zaščititi se pred njimi.

Uporabniki (tudi mladi, ki običajno še ne dostopajo do korporativnih in strogo zaščitenih podatkov) imajo možnost zaščititi svoje podatke na mobilni napravi s pomočjo orodij za enkripcijo. Enkripcija je učinkovita zaščita le, če je ključ, s katerim kriptiramo podatke, ustrezen. Kriptira se lahko le del podatkov na mobilni napravi, celotni sistem ali zgolj podatki, ki se prenašajo v kibernetski prostor; pri tem pa enkripcija s svojim delovanjem (kriptiranjem in dekriptiranjem) ne sme zavirati delovanje mobilne naprave. Gilaberte (2004) opisuje načine in logaritme, ki so primerni za določen način enkriptiranja podatkov. Istočasno lahko uporabniki pri prijavljanju v visoko varovane portale (banka, internetna pošta, v zadnjem času tudi Facebook in Gmail ter drugi) ali prenosu rizičnih podatkov na mobilno napravo povečajo stopnjo varnosti s pomočjo uporabe varnejšega protokola prenosa podatkov »https« in avtentikacije, s pomočjo certifikatov, kasnejše enkripcije in dekripcije podatkov (uporaba SSL-ja) ter uporabe VPN[63]-ja. Za samo preverjanje verodostojnosti pri dostopanju do omenjenih portalov so v pomoč različna identifikacijsko-varnostna digitalna potrdila. Pri prijavljanju v sistem mobilne naprave ali določenega informacijskega okolja se lahko uporabniki zaščitijo še z močnimi gesli. Vsekakor se je treba vprašati, koliko sami pripomoremo k zaščiti naših mobilnih naprav in podatkov.

S tem namenom smo študentom zastavili vprašanje o uporabi različnih zaščit na mobilnih telefonih. Tabela 2 prikazuje možne varnostne rešitve, ki lahko zavarujejo pametni mobilni telefon in podatke na njem pred različnimi grožnjami. Največ vprašanih uporablja PIN kodo za SIM in PIN kodo za dostop do aplikacij. Vendar je že odstotek drugih zelo nizek, kajti omenjeno varnostno rešitev pozna skoraj 50 odstotkov (49,3 %) vprašanih, vendar jo uporablja zgolj 29,5 odstotka. Zanimivo je tudi dejstvo, da vprašani ne poznajo bolj sofisticiranih varnostnih rešitev, kot so enkripcija podatkov, vzpostavitev VPN povezave itn. To si lahko razlagamo na dva načina: prvič, mladi se ne zavedajo dovolj groženj, ki jim pretijo, in ne vedo dovolj o varnostnih rešitvah; in drugič, mladi nekaterim varnostnim rešitvam, kljub temu da jih poznajo, ne zaupajo dovolj, da bi jih uporabljali oz. se ne počutijo dovolj ogrožene, kar je razvidno iz rezultatov, predstavljenih v nadaljevanju.

63 VPN – Virtual Private Network (navidezno zasebno omrežje).

Varnostne rešitve	Uporabljam	Poznam, vendar ne uporabljam	Ne poznam
PIN za SIM kartico	89,6 %	9,9 %	0,5 %
PIN za dostop do aplikacij na pametnem telefonu	29,5 %	49,3 %	21,3 %
Enkripcija podatkov	26,0 %	41,2 %	32,8 %
Avtentikacija ob uporabi določenih funkcij	21,4 %	56,8 %	21,8 %
Oddaljeno brisanje vsebin	20,3 %	50,2 %	29,5 %
Antivirusna zaščita	19,5 %	44,4 %	36,1 %
VPN povezava	13,0 %	43,3 %	43,8 %
Arhiviranje vsebin pametnega telefona	6,8 %	40,8 %	52,4 %
Centralni nadzor pametnega telefona (določanje politike uporabe)	6,8 %	40,8 %	52,4 %
Omogočeno sledenje pametnega telefona v primeru kraje	6,3 %	40,5 %	53,2 %
Izobraževanje	5,8 %	54,4 %	39,8 %

Tabela 2: Uporaba varnostnih rešitev za pametne mobilne telefone

Tabela 3 prikazuje raven zaupanje uporabnikov v varnostne rešitve. Največ anketiranih zaupa v PIN kodo za SIM kartico, kot je razvidno iz tabele 2. Najmanjši je odstotek uporabnikov, ki zaupajo v možnosti oddaljenega brisanja vsebin in VPN povezave, hkrati pa je iz tabele 2 lepo razvidno tudi, da se jim zdita ti dve funkciji najmanj uporabni.

Varnostne rešitve	Zaupam
PIN za SIM kartico	84,21 %
PIN za dostop do aplikacij na pametnem telefonu	70,60 %
Antivirusna zaščita	66,58 %
Omogočeno sledenje pametnega telefona v primeru kraje	65,08 %
Izobraževanje	64,39 %
Enkripcija podatkov	62,37 %
Avtentikacija ob uporabi določenih funkcij	58,97 %
Arhiviranje vsebin pametnega telefona	55,03 %
Centralni nadzor pametnega telefona (določanje politike uporabe)	53,32 %
VPN povezava	52,82 %
Oddaljeno brisanje vsebin	47,95 %

Tabela 3: Zaupanje uporabnikov mobilnih telefonov v varnostne rešitve

Število uporabnikov mobilnih naprav se povečuje in se bo povečevalo tudi v prihodnosti, kljub različnim grožnjam, ki predstavljajo nevarnost za uporabnikove podatke in podatke, do katerih dostopa s pomočjo mobilne naprave. Uporabniki smo sami odgovorni za to, da se pred temi grožnjami ustrezno zaščitimo, naj bo to z različnimi tehničnimi in programskimi zaščitami ali tako, da se izobražujemo, krepimo ozaveščenost in zavedanje o obstoju in delovanju groženj ter možnostih zaščite. Vsekakor je najboljša kombinacija obojega. V prvi vrsti se je potrebno dobro seznaniti z novimi tehnologijami, dodobra spoznati njihovo delovanje in nato pregledati nevarnosti ter možnosti zaščite. Znanje je bistvenega pomena pri zoperstavljanju grožnjam. S pregledom rezultatov in njihove interpretacije, lahko ugotovimo, da je trenutno glavni problem pomanjkanje znanja o varni uporabi mobilnih naprav ter poznavanja posameznih segmentov njihovega delovanja in vse relevantne programske opreme, tudi varnostnih rešitev ter groženj. Izobraževanje je vedno v središču vzpostavljanja informacijske varnosti, tudi ko gre za mobilne naprave – seveda v kombinaciji z različnimi tehnično-programskimi rešitvami.

4 Zaključek

Rezultati raziskave kažejo, kako mladi ravnajo z mobilnimi napravami. Na eni strani smo zaznali velik odstotek uporabnikov storitev mobilne telefonije, na drugi pa slabo poznavanja varnostnih ukrepov in nizko stopnjo zaupanja v varnostne rešitve.

Na podlagi predstavljenega menimo, da smernice pri uporabi mobilnih naprav niso dobre in jih bo potrebno spremeniti. Uporaba obstoječih varnostnih rešitev mora postati stalnica, predvsem pa se je treba intenzivno usmeriti v izobraževanje in ozaveščanje uporabnikov.

Varnostne rešitve ne morejo zaščititi mobilne naprave pred grožnjami, če jih uporabniki ne poznajo, in še posebej ne, če jih ne uporabljajo. Uporabnik se mora že ob nakupu mobilne naprave poučiti o tem, kako ta deluje, o posameznih nastavitvah ter o varnem povezovanju v različna omrežja za dostop do interneta. Pri uporabi mobilnih naprav moramo predvsem upoštevati informacijsko-varnostna priporočila ter uporabljati obstoječe varnostne ukrepe. Številne organizacije dnevno opozarjajo uporabnike različnih mobilnih naprav na raznovrstne grožnje, zato je nujno, da se posameznik redno seznanja z njimi.

Viri

- Bernik, I. in Prislan, K. (2012). Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem. Ljubljana: Fakulteta za varnostne vede Univerze v Mariboru.
- comScore. (2011). V Europe, Apple iOS Eco System Twice the Size of Android When Accounting for Mobile Phones, Tablets and Other Connected Media Devices. Pridobljeno 18. 2. 2012 na http://www.comscore.com/Press_Events/Press_Releases/2012/1/Nearly_50_Percent_of_Internet_Users_in_Europe_Visit_Newspaper_Sites
- Dimc, M. and Dobovšek, B., Perception of Cyber Crime in Slovenia, Journal of Criminal Justice and Security, 2010, 4, 378-396.
- IDC. (2012). IDC – Press Release. Pridobljeno 10. 8. 2012 na http://www.idc.com/getdoc.jsp?containerId=prUK23507512
- GfKGroup. (2011). CEE Telco Industry Report 2011. Pridobljeno 6. 2. 2012 na http://www.gfk.com/group/press_information/press_releases/008894/index.en.html
- Juniper Networks (2011). Malicious Mobile Threats Report 2010/2011. Pridobljeno 10. 9. 2011 na http://www.juniper.net/us/en/dm/interop/go
- Lookout. (2011). Lookout Mobile Threat Report. Pridobljeno 10. 9. 2011 na https://www.mylookout.com/mobile-threat-report
- Meško, G. in Bernik, I. (2011). Cybercrime: Awareness and Fear: Slovenian Perspectives. V: N. Memon and D. Zeng (ur.). 2011 European Intelligence and Security Informatics Conference [Electronic source]. Atene, 12.-14. 9. 2011 (str. 28-33).
- Mcafee. (2012). McAfee Threats Report: Third Quarter 2012. Pridobljeno 15. 10. 2012 na http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

O avtorjih

Blaž Markelj, univerzitetni diplomirani organizator–informatik, predavatelj informacijske varnosti na Fakulteti za varnostne vede, Univerze v Mariboru.

Igor Bernik, prodekan za izobraževalno dejavnost, vodja katedre za informacijsko varnost na Fakulteti za varnostne vede, Univerza v Mariboru.

Zaščita industrijskih kontrolnih sistemov – obramba v globino

Blanka Strmšek

V poslovnem okolju je dostop do informacij ključnega pomena za dolgoročno konkurenčno prednost. Poleg vseh koristi, ki jih prinaša nova tehnologija, prinaša tudi nove grožnje in izzive za zaščito informacij. Ni optimalne rešitve za boj proti grožnjam, ampak je to skupek več posameznij rešitev. Večina jih sicer služi svojemu namenu, vendar so nepopolne in navadno same po sebi ne zagotavljajo zadostne zaščite. Namen tega prispevka je predstaviti smernice za boljšo zaščito industrijskih kontrolnih sistemov (IKS). IKS so del kritične infrastrukture. Zaradi kompleksnosti in vse večje povezljivosti teh sistemov, narašča število varnostnih težav in z njimi povezanih tveganj. Za učinkovito zaščito pred kibernetskimi napadi se je za uporabno izkazala večplastna zaščita sistemov. Obramba v globino je večplastni varnostni pristop, ki uporablja več različnih načinov kontrole, metod in tehnik za zaščito pred fizičnimi in kibernetskimi napadi. Posamezna plast sama po sebi ne zagotavlja zadostne zaščite, vendar pa v medsebojni povezavi predstavlja pomemben zaščitni ukrep. Prispevek je namenjen varnostnim menedžerjem, vodjem informacijske tehnologije (IT), sistemskim administratorjem, inženirjem ter vodstvom podjetij, da bi razumeli in prepoznali prednosti večplastne zaščite njihovih sistemov.

KLJUČNE BESEDE: kritična infrastruktura, industrijski kontrolni sistemi, kibernetska varnost, ranljivosti, obramba v globino.

1 Uvod

Industrijski kontrolni sistemi (IKS) so računalniško podprti sistemi, ki se uporabljajo v številnih panogah za spremljanje in nadzor občutljivih procesov in fizičnih funkcij. Opravljajo vitalne funkcije v kritični infrastrukturi, npr. v energetiki, jedrski industriji, informacijski in telekomunikacijski tehnologiji, kemični industriji, pri zagotavljanju vodnih virov in prehrane, prometu ter javni administraciji. Vključujejo sisteme za nadzor in upravljanje industrijskih procesov (SCADA),

porazdeljene nadzorne sisteme (DCS) in programabilne logične krmilnike (PLK) (NIST Special Publication 800-82, 2011).

IKS so zaradi svoje kompleksnosti in povezanosti s poslovnim ter zunanjim omrežjem izpostavljeni vse večjemu tveganju za kibernetske napade. Njihove ranljivosti so izpostavljene vedno bolj motiviranim in visoko kvalificiranim napadalcem, kar dokazujejo nedavni napadi na IKS (Stuxnet[64], Flame[65]). Nevarnosti ne predstavljajo samo napadi od zunaj, temveč v veliki meri tudi od znotraj. Okvare, izpad sistema ali prekinitve delovanja bi lahko resno vplivale na zdravje in varnost ljudi ali na poslovanje podjetja, s tem pa na njegovo finančno stanje in morebitno izgubo. Načrtovanje in implementacija rešitev za zaščito IKS zahteva dober premislek in celovit pristop k varnosti. Za učinkovito zaščito IKS pred kibernetskimi napadi je potrebnih več protiukrepov. Ta prispevek obravnava večplastni varnostni pristop – obrambo v globino – ki zagotavlja najvišjo mogočo varnost v organizaciji. V nadaljevanju bodo predstavljene ranljivosti in s tem povezani vektorji napadov. Opredelili bomo obrambo v globino in predstavili tri ključne dejavnike: ljudi, postopke in tehnologijo.

2 Ranljivosti industrijskih kontrolnih sistemov

Preden nadaljujemo, bi rada opredelila še nekaj osnovnih pojmov, kot so ranljivosti in grožnje. Shirey (2007) opisuje ranljivost kot pomanjkljivost ali šibkost v načrtovanju, implementaciji in delovanju sistema ter upravljanju, ki lahko krši varnostno politiko sistema. Grožnja je opredeljena kot vsaka morebitna okoliščina, zmožnost, ukrep ali dogodek, ki lahko ogrozi varnost in povzroči škodo. To pomeni, da je grožnja potencialna nevarnost, ki lahko izkoristi ranljivosti. Grožnje, ki pretijo kontrolnim sistemom, izhajajo iz različnih virov, vključno s terorističnimi skupinami, nezadovoljnimi zaposlenimi in zlonamernimi vsiljivci (United States Government Accountability Office, 2005). Zaradi kompleksnosti sodobnih IKS obstaja veliko ranljivosti, kot tudi vektorjev napada. V študiji, ki so jo izvedli na

[64] Stuxnet – črv napada Simensove SCADA sisteme (WinCC/PCS 7), ki se uporabljajo za nadzor in krmiljenje industrijskih procesov. Črv se širi prek lokalnega omrežja in izmenljivih naprav. Stuxnet je zelo izpopolnjena zlonamerna koda, ki lahko spreminja kodo na posebnih programabilnih logičnih krmilnikih (Kako nevaren je pravzaprav Stuxnet?, 2012).

[65] Flame – zlonamerni program za prisluškovanje in krajo informacij. Omogoča zelo raznolike metode vohunjenja, med drugim prestrezanje omrežnega prometa, prestrezanje tipkovnice, zajemanje zaslonske slike, snemanje in posredovanje zvočnih zapisov pogovorov uporabnikov računalnika, ne da bi se ti tega zavedali (Huš, 2012).

podlagi prijavljenih varnostnih incidentov iz podatkovne baze RISI, kaže, da izhajajo varnostni problemi IKS iz treh glavnih virov. Prvi problem je, da so ti sistemi zelo lahka tarča (zaradi pomanjkanja omrežne robustnosti, varnostnih popravkov ali protivirusnih posodobitev). Drugi problem je, da so tudi brez neposredne povezave z internetom še vedno dostopni prek več različnih dostopnih točk (daljinsko vzdrževanje/diagnostične povezave, strežniki historian in strežniki sistema za upravljanje proizvodnje (MES), serijske povezave, brezžični sistemi, mobilni prenosniki, naprave USB). Kot zadnji problem navajajo slabo omrežno segmentacijo (Byres, 2011). Razumevanje ranljivosti IKS in s tem povezanih vektorjev napadov je bistvenega pomena za oblikovanje učinkovite strategije za zmanjšanje tveganj. Ti vključujejo (U.S. Department of Homeland Security, 2009):

- stranska vrata in luknje v omrežnem perimetru (ali DMZ);
- ranljivosti v skupnih protokolih (npr. napadi na OPC/DCOM);
- napade na kontrolni sistem prek področne naprave;
- napade na zbirke podatkov ob pomoči vrivanja SQL (angl. SQL injection);
- komunikacijske ugrabitve (angl. *communications hijacking*) in napade človek-v-sredini (angl. *man-in-the-middle).*

Varnostne incidente povezane z IKS lahko razdelimo v tri kategorije (NIST Special Publication 800-82, 2011):

- Namerni ciljno usmerjeni napadi – pridobivanje nepooblaščenega dostopa do datotek, DOS napadi ali e-poštne prevare in podobno. Primer namerno usmerjenega napada je črv Stuxnet, ki je bil odkrit junija 2010.
- Nenamerni varnostni incidenti – črvi, virusi ali odpovedi sistema, ki lahko povzročijo neposredno škodo z nepredvidljivimi posledicami, kakršno je na primer povzročil črv Slammer.[66]
- Nenamerni notranji varnostni dogodki – vključujejo različne proizvodne okvare in zastoje, ki so posledica nepravilnosti in zapletov med testiranjem varnosti.[67]

[66] Slammer – omenjeni črv je leta 2003 prizadel jedrsko elektrarno Davis-Besse v Ohiu v ZDA, kar je povzročilo večurno prekinitev delovanja nadzornega sistema jedrske elektrarne.

[67] Podjetje za distribucijo zemeljskega plina je najelo podjetje za varnostno svetovanje, da bi opravili penetracijsko testiranje poslovnega omrežja. Varnostno podjetje si je drznilo iti na del omrežja, ki je neposredno povezan s sistemom SCADA. Penetracijski preizkus je zablokiral sistem SCADA, zaradi česar je bila za štiri ure onemogočena distribucija plina.

Povezovanje omrežij vodi do ranljivosti, ki zmanjšuje varnost organizacije in izpostavlja kontrolne sisteme kibernetskim grožnjam. Prehod na standardne komercialne produkte (npr. operacijski sistemi Windows), odprte protokole (npr. TCP/IP) in uporabo interneta ima pozitivne in negativne učinke. Na pozitivni strani ta prehod omogoča dostop do novih in bolj učinkovitih načinov komunikacije in bolj zanesljivih podatkov. Na negativni strani pa je IKS izpostavljen novim vrstam groženj, ki lahko zelo povečajo verjetnost za napad (U. S. Department of Homeland Security, 2009). Tudi v NIST Special Publication 800-82 (2011) so izpostavili, da je sprejetje odprtih komunikacijskih protokolov (npr. OPC), tehnologij z znanimi ranljivostmi, povezanosti kontrolnih sistemov z drugimi omrežji, negotovih in šibkih povezav (oddaljen dostop) ter razširjene razpoložljivosti tehničnih informacij o kontrolnih sistemih, prispevalo k povečanju tveganja kontrolnih sistemov. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT, 2012) opozarja na vse večje tveganje zaradi informacij o nastavitvah kontrolnih sistemov dostopnih prek interneta, ranljivosti in orodij za izkoriščanje ranljivosti[68] ter povečanega zanimanja za izvedbo napadov na kontrolne sisteme s strani hektivističnih skupin. Napadi na IKS postajajo vse bolj dovršeni in številčni, kar dokazuje poročilo o kibernetskih napadih na kontrolne sisteme, ki ga je izdelal ICS-CERT (2011) v obdobju od 2009 do 2011. S pomočjo analize ugotovitev o odzivih na incidente, poročil o incidentih in rezultatov so določili skupne trende varnostnih pomanjkljivosti v okoljih kontrolnih sistemov. Ugotovili so, da največjo varnostno vrzel tako predstavljajo ljudje, postopki in tehnologija.

Iz ugotovitev zgoraj izhaja, da so danes kontrolni sistemi ranljivi bolj kot kdaj prej. Največjo ranljivost tako predstavljajo uporaba standardnih komercialnih produktov in odprtih protokolov, povečana povezljivost, negotove povezave, prosto dostopne informacije o IKS, ter v zadnjem času povečano zanimanje za napade na IKS in uporaba orodij za izkoriščanje ranljivosti. Lahko ugotovimo, da nasprotniki napadajo iz več smeri, gre za notranje ali zunanje napadalce, zato potrebuje organizacija uvedbo zaščitnih mehanizmov na različnih lokacijah, da se upre različnim vrstam napadov.

[68] Hekerji spretno izkoriščajo iskalna orodja, ki omogočajo iskanje IKS dostopnih prek interneta (npr. SHODAN).

3 Definiranje obrambe v globino

Obramba v globino je v osnovi vojaška strategija s temelji v zgodnji zgodovini človeštva. Osnovno prepričanje je, da je bolje, da obramba zaustavi napad, kot da povzroči napredek napadalca. V okviru računalništva pa gre za pristop, ki ga je zasnovala National Security Agency kot celovit pristop k informacijski in kibernetski varnosti. Je koncept zaščite računalniškega omrežja z uporabo več mehanizmov zaščite. V primeru odpovedi enega obrambnega ukrepa, drugi še naprej zagotavljajo zaščito pred napadom. Za kritično infrastrukturo je dosleden in zanesljiv pristop k informacijski varnosti bistvenega pomena (Trusted Information Sharing Network, 2007). National Security Agency (2000) in Trusted Information Sharing Network (2007) opredeljujeta obrambo v globino kot uravnotežen in usklajen pristop ljudi, postopkov in tehnologije. Strategija uporablja različne ukrepe, ki lahko upočasnijo in preprečijo nedovoljene aktivnosti proti kontrolnim sistemom. Takšen pristop poveča verjetnost, da se grožnje pravočasno odkrijejo, in se prepreči, da bi dosegle svoj cilj. Obramba v globino poveča varnost kontrolnih sistemov in zaščiti sistem pred notranjimi ali zunanjimi grožnjami (Bradley, 2012). En sam varnostni proizvod, tehnologija ali rešitev ne more ustrezno zaščititi IKS, zato je potrebnih več kontrol ali varnostnih slojev. Tudi, če bi imeli teoretično 100-odstotno varen požarni zid, ki bi ščitil pred vsemi napadi iz interneta, ta ne more zaščititi pred notranjimi napadalci ali fizičnimi napadi (Axelsen, 2005). Če povzamemo, obramba v globino je koncept informacijske varnosti z več varnostnimi sloji zaščite v okolju IKS. Koncept zagotavlja, da odpoved ene varnostne kontrole ali izkoriščene ranljivosti ne ogrozi sistema. Trije ključni dejavniki so pomembni za uspešen program kibernetske varnosti IKS, in sicer ljudje, postopki in tehnologija. Nagnjeni smo k temu, da se zanašamo na tehnologijo, da bi nas obvarovala, ampak sta druga dva vidika prav tako pomembna.

4 Ljudje

Ljudje so najšibkejši člen v organizaciji in varnost je učinkovita le toliko, kolikor je učinkovit njen najšibkejši člen (Roy, 2004). Tudi Victor Hazlewood (2006) ugotavlja, da so ljudje najbolj kritična kategorija, zato jih postavlja v prvo linijo obrambe. Poudarja pomen njihove odgovornosti, vlog, varnostne politike, usposabljanja in ozaveščenosti. Pomemben dejavnik v razvoju celovite varnostne strategije je odziv na varnostne incidente, ki vključuje proaktivne ukrepe in načrt za krizno stanje. Kot navaja Urso (2011), sta podpora višjega menedžmenta in njegova

obveza, da bo osebje usposobljeno za vloge, ki jih imajo pri ohranjanju kibernetske varnosti IKS, dva od prvih korakov pri vzpostavitvi dobrega kibernetskega programa. Ključnega pomena sta usposabljanje zaposlenih in ozaveščenost o pomenu usposabljanja in izobraževanja, z dodatno pozornostjo na kibernetski varnosti poslovanja, posodobitvah, smernicah in novih grožnjah. To lahko prispeva k zmanjšanju nesreč, ki nastanejo, zgolj zaradi pomanjkanja kibernetske ozaveščenosti. Pravi, da se doseganje informacijske varnosti začne z jasnimi usmeritvami vodstva organizacije. Temu morajo slediti učinkovita varnostna politika, postopki, razdelitev vlog in dolžnosti, usposabljanje ključnih kadrov ter osebna odgovornost. To vključuje vzpostavitev fizične varnosti ter varnostne ukrepe za nadzor in spremljanje dostopa do objektov in kritičnih elementov informacijsko-tehnološkega okolja. Varnostna politika, ki velja posebej za okolje IKS mora zajemati (Byres in Cusimano, 2012): izmenljive medije, upravljanje s popravki, upravljanje s protivirusno programsko opremo, upravljanje sprememb, varnostne kopije in obnovo ter odziv na incidente. Organizacija potrebuje postopke, varnostne standarde in smernice za izvajanje varnostne politike. Varnostna politika in standardi, ki veljajo za IT okolje, pogosto niso uporabni ali prirejeni za okolje IKS. Avtorja priporočata razvoj posebnih dokumentov, ki opisujejo politiko podjetja, standarde in postopke za varnost IKS. Seznanitev z varnostnimi predpisi in standardi, ki veljajo za industrijo, zagotavlja trdno podlago za razvoj varnostne politike, standardov in postopkov organizacije, kakršen je npr. ANSI/ISA-99.00.01–2007 (2007) – gre za niz standardov, ki obravnavajo kibernetsko varnost za industrijsko avtomatizacijo in kontrolne sisteme.

5 Postopki

Postopki definirajo in uveljavljajo standardizirane ukrepe, ki se uporabljajo za razvoj in zagotavljanje vsakodnevne varnosti (Trusted Information Sharing Network, 2007). Ukrepi, ki jih je predlagala National Security Agency (2000) vključujejo: vzdrževanje varnostne politike, obvladovanje sprememb v informacijski tehnologiji, varnostni popravki, posodobitve protivirusne zaščite, vzdrževanje seznama za nadzor dostopa, zagotavljanje storitev upravljanja s ključi, izvajanje varnostne ocene sistema, odzivanje na trenutne grožnje, pripravljenost na napad, ustrezno opozarjanje in odzivanje ter okrevanje in obnova. Urso (2011) poudarja, da je pomembno vzpostaviti učinkovite postopke in smernice za ravnanje, ki vpliva na varnost organizacije (kot je uporaba pomnilniških ključev USB), in obnovo po katastrofi v primeru uspešnega napada (vključno z odzivanjem na

varnostne incidente, začasnimi ukrepi za vzdrževanje poslovanja in analizo po varnostnem incidentu).

6 Tehnologija

Danes je na voljo široka izbira tehnoloških rešitev, ki zagotavljajo informacijsko varnost. Da se zagotovi in uporabi dobra tehnologija, mora organizacija vzpostaviti učinkovito politiko in postopke. Ti morajo vključevati: varnostno politiko, informacijsko varnostna načela, varnostno arhitekturo in standarde, merila za informacijsko varnost proizvodov, nakup izdelkov, ki so potrjeni s strani zaupanja vrednih oseb, in smernice za konfiguracijo. Tudi najboljši razpoložljivi varnostni proizvodi imajo svoje pomanjkljivosti. Samo vprašanje časa je, kdaj bo nasprotnik našel ranljivost in jo izkoristil. Učinkovit protiukrep je uporaba več mehanizmov obrambe med napadalcem in njegovim ciljem. Vsak od teh mehanizmov mora predstavljati edinstveno oviro za nasprotnika. Poleg tega mora vsak od njih vključevati tako ukrepe za zaščito kot za odkrivanje. To prispeva k povečanju tveganja (odkritja) za nasprotnika, obenem pa zmanjša možnosti za njegov uspeh (National Security Agency, 2000). V nadaljevanju bodo predstavljeni tehnološki ukrepi za zaščito omrežja IKS, ki vključujejo segmentacijo omrežja in dobro načrtovanje omrežne arhitekture.

7 Segmentacija omrežja, varnostna območja in kanali

Omrežja IKS so danes bolj kompleksna kot kdaj prej. Sestavljena so iz več sto ali celo več tisoč posameznih naprav. Žal pa je načrtovanje teh omrežij še vedno pomanjkljivo in pogosto ne vključuje koraka segmentacije omrežja. Posledično se lahko težave, ki izvirajo v enem delu omrežja, hitro razširijo tudi na druga področja (Byres, 2011). Najpomembnejši korak za izboljšanje varnosti IKS je segmentacija omrežja, ki razdeli sistem na različna varnostna območja in uvaja več plasti zaščite za izolacijo najbolj kritičnih delov sistema. Poskrbi za večnivojsko zaščito pomembnih sredstev (Byres in Cusimano, 2012).

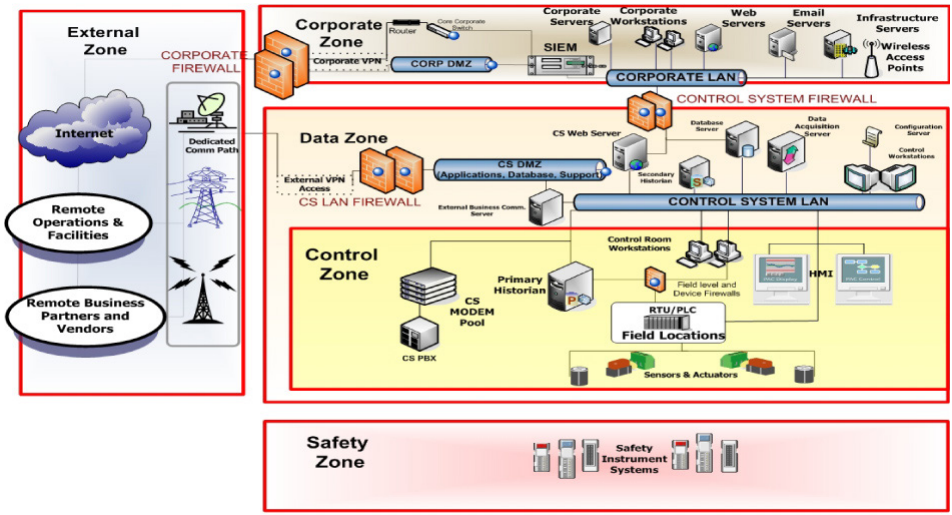
S pomočjo območij in kanalov lahko ločimo in izoliramo različne podsisteme IKS. ANSI/ISA-99.00.01–2007 (2007) opredeljuje območje, kot skupino logičnih ali fizičnih sredstev, ki imajo podobne varnostne zahteve. Kanali so poti v omrežje,

prek katerih se prenašajo podatki med temi območji. Obstajajo lahko tudi območja znotraj območij ali podobmočja, ki zagotavljajo večplastno obrambo. Byres in Cusimano (2012) pravita, da se oblikovanje območij in kanalov začne z določitvijo skupin naprav s podobnim delovanjem in podobnimi varnostnimi zahtevami. Na primer, objekt se najprej razdeli na operativna področja, kot so skladiščenje materialov, predelava, izdelava itn. Znotraj teh področij se lahko naredi delitev na funkcionalne plasti, kot so vmesniki človek/stroj (angl. human machine interface – HMI), PLK in varnostni sistemi. Naslednji korak je raziskati vse poti v omrežje, prek katerih se prenašajo podatki med temi območji, to so omrežni kanali. Mogoče jih je logično organizirati v skupino informacijskih tokov znotraj in tudi zunaj območja. Ko so kanali in njihove varnostne zahteve opredeljene, sledi zadnja faza, to je izvajanje ustreznih varnostnih mehanizmov (požarni zidovi, IDS -ji itn.). Najbolj kritična sredstva morajo biti v najvišjem varnostnem območju. U. S. Department of Homeland Security (2009) deli arhitekturo IKS na več območij (zunanje, poslovno, proizvodno/podatkovno, kontrolno in varnostno območje) glede na osnovne funkcije (Slika 1). Predstavljena so tudi tveganja za vsako od teh območij.

8 Omrežna arhitektura IKS

NIST Special Publication 800-82 (2011) priporoča, da se pri načrtovanju omrežne arhitekture IKS, loči kontrolno omrežje od poslovnega. Z ločitvijo omrežij, varnostne težave na poslovnem omrežju ne bi smele vplivati na omrežje IKS. Če mora biti omrežje povezano, se priporoča le minimalno število povezav (če je možno, le ena), ki morajo iti prek požarnega zidu in DMZ. DMZ je ločen omrežni segment in je neposredno povezan s požarnim zidom. Zunanjim povezavam je treba dovoliti le minimalen dostop prek požarnega zidu. Podane so dobre varnostne smernice za postavitve požarnih zidov in ustvarjanje varnostne arhitekture IKS. Dokument je dobra osnova za ustvarjanje večplastne obrambe. U. S. Department of Homeland Security (2009) pravi, da se razvoj strategije obrambe v globino začne z analiziranjem arhitekture IKS in izbiro varnostnih tehnologij. Natančna in dobro dokumentirana arhitektura omogoči organizaciji dobro varnostno ozaveščenost, uvajanje učinkovitih varnostnih protiukrepov in lažje razumevanje varnostnih incidentov. Priporočajo omrežno arhitekturo, ki vključuje uporabo več požarnih zidov, oblikovanje demilitaliziranega območja (DMZ) in sistemov za odkrivanje (IDS) ter preprečevanje vdorov (IPS), skupaj z učinkovito varnostno

politiko, programi usposabljanja in mehanizmi za odzivanje na incidente (SIEM). Slika 1 prikazuje večplastno arhitekturo IKS, razdeljeno na območja.



Slika 1: Obramba v globino – priporočena varnostna arhitektura (U. S. Department of Homeland Security, 2009)

Iz navedb zgoraj izhaja, da imajo tudi najboljši razpoložljivi varnostni proizvodi svoje pomanjkljivosti. Torej je samo vprašanje časa, kdaj bo nasprotnik našel ranljivost in jo izkoristil. Učinkoviti protiukrepi za omrežno varnost so uporaba več mehanizmov obrambe med napadalcem in njegovim ciljem, dobro zasnovana omrežna arhitektura ter segmentacija omrežja na območja in kanale, kot je prikazano na Sliki 1. Vsak od teh mehanizmov mora predstavljati edinstveno oviro za nasprotnika.

9 Življenjski cikel obrambe v globino

Obramba v globino ni enkraten cilj, ampak je nenehen proces ocenjevanja ranljivosti omrežja, posodabljanja varnostne politike in uvajanja novih tehnologij v življenjskem ciklu razvoja in vzdrževanja obrambe v globino (Linton, 2010). Tudi Byres in Cusimano (2012) pravita, da je treba varnost IKS redno spremljati in ohranjati. To vključuje številne dejavnosti, npr. posodobitve protivirusnih podpisov,

nameščanje varnostnih popravkov, spremljanje sumljivih dejavnosti itn. Za zagotavljanje optimalne varnosti je pomembno redno pregledovanje in ocenjevanje sistema, kot tudi posodabljanje varnostnih kontrol z najnovejšimi standardi in najboljšimi praksami. Standardi ANSI/ISA-99 zagotavljajo okvir za doseganje in vzdrževanje varnostnih izboljšav skozi življenjski cikel, ki združuje razvoj, izvajanje, spremljanje in nenehno izboljševanje. Zagotavljajo najboljšo prakso za razvoj in uvajanje politike ter tehnoloških rešitev, za reševanje varnostnih vprašanj v kontrolnih sistemih (Byres, 2011). Trusted Information Sharing Network (2007) opredeljuje obrambo v globino kot nenehen proces, ki zahteva stalne izboljšave, večjo natančnost in vedno boljše razumevanje okolice (Slika 2). Obramba v globino se začne z vzpostavitvijo konteksta, ki je nujen za razvoj trdnega okvira. Zahteva se temeljito razumevanje ciljev organizacije, informacijskih sredstev in sistemov ter groženj za vsako od njih. Naslednji korak je analiza tveganja okolja, ki vključuje zunanje in notranje grožnje. Poudarek je na identifikaciji, analizi in oceni groženj, tveganj ter ranljivosti, s katerimi se organizacija trenutno sooča. Vzpostavitev obrambe v globino predstavlja okvir za izvajanje kontrole upravljanja, ljudi, procesov in tehnologije. Bistvenega pomena je, da so sestavni deli obrambe v globino redno spremljani in pregledovani. Varnostne grožnje se nenehno spreminjajo, zato mora organizacija prilagajati obrambo v globino spremembam v okolju, da bi ostala učinkovita. Podpora višjega menedžmenta je nujna, da se kibernetski program lahko ohranja skozi celotno organizacijo, vse od upraviteljev sistema do vodstva organizacije.

Slika 2: Življenjski cikel strateškega izvajanja obrambe v globino (Trusted Information Sharing Network, 2007)

10 Zaključek

IKS so vse pogostejša tarča hekerjev in kibernetskih teroristov. Napadi so vse bolj dovršeni in tradicionalni varnostni pristop – uporaba požarnih zidov v kombinaciji z protivirusno programsko opremo – ni zmožen zaščiti pred današnjimi kibernetskimi grožnjami. Zato potrebujemo obrambo v globino, ki zaščiti okolje IKS s pomočjo več plasti zaščite, kar povečuje vložen čas in trud zlonamernih napadalcev, ki želijo prodreti v sistem in morajo pri tem premagati številne ovire. To bo zaščitilo IKS pred naraščajočim številom ranljivosti in izpostavljenosti informacijske tehnologije v kritični infrastrukturi. Kibernetska varnost iz vidika obrambe v globino ni le uvajanje posebnih tehnologij za preprečevanje določenih tveganj. Izvajanje učinkovite strategije obrambe v globino zahteva celovit pristop in pritisk na vse vire v organizaciji, da se zagotovi učinkovita raven zaščite, pri čemer je nujna podpora vodstva organizacije. Pomembno načelo obrambe v globino je doseganje informacijske varnosti, ki zahteva osredotočenost na ljudi, tehnologijo in postopke. Veliko organizacij se osredotoča predvsem na tehnološke rešitve, čeprav so vložki v ljudi in postopke prav tako nujni za zaščito kritične infrastrukture in premoženja. Pomemben korak za izboljšanje omrežne varnosti IKS je uporaba več mehanizmov obrambe med nasprotnikom in njegovim ciljem, dobro zasnovana omrežna arhitektura ter segmentacija omrežja na območja in kanale. Obramba v globino zahteva učinkovito varnostno politiko, postopke, usposabljanje in ozaveščenost osebja ter učinkovito spremljanje. Gre za nenehen proces, ki zahteva stalne izboljšave, redno pregledovanje in ocenjevanje sistema, kot tudi posodabljanje varnostnih kontrol z najnovejšimi standardi in najboljšimi praksami, ki obravnavajo kibernetsko varnost za industrijsko avtomatizacijo in kontrolne sisteme.

Ker obstaja veliko ranljivosti v IKS, ki se razlikujejo tudi glede na proizvajalca, ni enotne rešitve za vse sisteme. Vsak sistem je potrebno analizirati in prilagoditi smernice ter rešitve za vzpostavitev obrambe v globino. Prav tako ni enotnega standarda, iz katerega lahko izhaja obramba v globino, ampak je to skupek več standardov, smernic in tehničnih priporočil. Za zmanjšanje varnostnih tveganj na sprejemljivo raven, morajo uporabniki razviti in izvajati obrambo v globino. Ta naj temelji na standardih ANSI/ISA-99, ki predstavljajo dober okvir za segmentacijo omrežja, NIST SP 800-82, ki ponuja temeljit pregled nad IKS, njihovo ranljivostjo in grožnjami, ter drugimi industrijskimi standardi. Standardi zagotavljajo najboljšo prakso za razvoj in vzpostavitev varnostne politike ter tehnoloških rešitev za reševanje varnostnih vprašanj v življenjskem ciklu IKS.

Viri

- ANSI/ISA–99.00.01–2007. (2007). Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models. Pridobljeno 19. 8. 2012 na http://www.isa.org/filestore/expo/2009/PressKit/Information%20about%20ISA/Membership/Samples%20of%20Free%20ISA%20Standards%20and%20Technical%20Papers/ANSI%20ISA%2099-00-01%20%202007.pdf.
- Axelsen, L. (2005). Hacking as Approach to Defense in Depth. Pridobljeno 20. 7. 2012 na https://www.giac.org/paper/gsec/4386/hacking-approach-defense-in-depth/10726.
- Byres, E. (2011). Revealing Network Threats, Fears: How to Use ANSI/ISA-99 Standards to Improve Control System Security. Pridobljeno 22. 8. 2012 na http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=84829.
- Byres, E. in Cusimano, J. (2012). 7 Steps to ICS and SCADA Security. Pridobljeno 22. 8. 2012 na http://www.isssource.com/wp-content/uploads/2012/02/022912WP-7-Steps-to-ICS-Security-v1.0.pdf.
- Hazlewood, V. (2006). Defense-In-Depth, An Information Assurance Strategy for the Enterprise. La Jolla, CA: San Diego Supercomputer Center Security Technologies.
- ICS-CERT. (2011). ICS-CERT Incident Response Summary Report. Pridobljeno 15. 8. 2012 na http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf.
- ICS-CERT. (2012). ICS-ALERT-12-046-01- Increasing Threat to Industrial Control Systems. Pridobljeno 15. 8. 2012 na http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01.pdf.
- Linton, H. (2010). Cyber Security for Industrial Applications. Pridobljeno 20. 7. 2012 na http://www.garrettcom.com/techsupport/papers/cyber_security_industrial_applications.pdf.
- NIST Special Publication 800-82. (2011). Guide to Industrial Control Systems (ICS) Security. Pridobljeno 18. 8. 2012 na http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.
- National Security Agency. (2000). Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments. Pridobljeno 20. 7. 2012 na http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
- Bradley, A. (2012). Industrial Security Best Practices. Milwaukee: Rockwell Automation, Inc.
- Roy, M. (9. 6. 2004). Humans Still Weakest Security Link. InternetNews.com. Pridobljeno 20. 7. 2012 na http://www.internetnews.com/security/article.php/3366211/Humans+Still+Weakest+Security+Link.htm
- Shirey, R. (2007). Internet Security Glossary, Version 2(RFC4949). Pridobljeno 20. 7. 2012 na http://www.rfc-editor.org/rfc/rfc4949.txt.

- Trusted Information Sharing Network. (2007). Defence in Depth. Barton Act: Commonwealth of Australia.
- United States Government Accountability Office. (2005). Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, GAO-05-434. Washington D.C.: Diane Publishing.
- Urso, J. (2011). Defense in Depth: It's More than Just the Technology. Pridobljeno 22. 8. 2012 na http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=85573.
- U.S. Department of Homeland Security. (2009). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Pridobljeno 20. 7. 2012 na http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf.
- Kako nevaren je pravzaprav Stuxnet? (5. 7. 2012). Računalniške novice. Pridobljeno 20. 7. 2012 na http://www.racunalniske-novice.com/novice/dogodki-in-obvestila/kako-nevaren-je-pravzaprav-stuxnet.html.
- Huš, M. (29. 5. 2012). Flame stokrat kompleksnejši od Stuxneta. Slo-tech.com. Pridobljeno 20. 7. 2012 na https://slo-tech.com/novice/t520052.

O avtorju

Blanka Strmšek, podiplomska študentka, Fakulteta za varnostne vede, Univerza v Mariboru.

Stvarno kazalo

A

android 108–109, 122, 125, 129

aplikacija 7, 22, 49, 97, 113, 118, 125–127

avtentikacija 8, 9, 77, 110, 112–114, 126, 127

avtorizacija 7, 9, 28, 110, 112, 126

avtorska pravica 80

B

brezžično omrežje 122–125, 132

C

celovitost informacij 78, 79

certificiranje 43, 44, 47, 53, 54, 120

certifikat 30, 99, 115, 126

civilna družba 56–59, 63, 64, 68, 69,

COBIT 24, 42–44, 48, 49, 50, 53, 54

Č

človekove pravice 14, 60, 63, 91

človeški vir 5, 6, 66, 67

D

delovno okolje 23, 52

dešifriranje 77, 86, 126

digitalna baza 87
digitalni podatek 77, 85–89
digitalno dokazovanje 85, 89, 90, 92, 93
digitalno potrdilo 126
dinamični ključ 8
disciplinski postopek 23
dobre prakse 25, 53, 113
državna uprava 65
dvofaktorska metoda 112, 113, 115

E

e-bančništvo 110–120
elektronska pošta 11, 64, 72, 96–99, 112, 124, 125, 132
elektronski dokazi 64, 87–90, 92, 93
enkripcija 6, 85–88, 91–93, 98, 107, 126, 127
Evropska unija 56, 58, 61–63, 69

F

Facebook 123, 126

G

garantna dolžnost 106, 107
geslo 85, 87, 88, 90, 92, 93, 98, 126
Gmail pošta 126
grožnja 5, 6, 11, 12, 14, 18, 22, 24, 25, 29, 30, 64, 67, 80, 96, 97, 109, 111, 112, 116, 118, 121–123, 125, 126, 128, 130, 131, 133–135, 139, 140
GSM številka 99

H

heker 62, 76, 83, 133, 140

hektivist 61, 62, 133

I

identifikacija uporabnika 8, 9, 112, 126

indikator učinkovitosti informacijske varnosti 17, 21–24

industrijski kontrolni sistem 130, 131, 135, 140

industrijski standardi 42, 140

informacijska tehnologija 9, 10, 14, 17, 22, 23, 28, 30, 33, 34, 43, 54, 63, 72, 93, 95–98, 107, 110, 113, 122, 128, 130, 131, 133–135, 140

informacijska varnost 5, 6, 9–12, 14–20, 22–30, 31, 34, 35, 39, 40, 54, 66, 67, 95–98, 102, 103, 109, 121–123, 128, 134, 135, 140

informacijska zasebnost 5, 6, 10, 73, 74, 83

informacijski pooblaščenec 10

informacijsko bojevanje 55–57, 61–63, 66–68, 82, 129

industrijsko vohunstvo 79

informacijskovarnostni cilj 15, 21, 25

integriteta informacijskega sistema 7, 21, 56, 63, 79, 83

integriteta podatkov 8, 97

interdisciplinarnost 6

internet 23, 64, 69, 72, 75, 83, 78, 92, 94, 96–98, 107, 122–126, 128, 132, 133

interni podatki 6

intervju 24, 46, 47, 51, 52, 123

izobraževanje 20, 23, 29, 35, 47, 52, 58, 62, 88, 98, 107, 118–121, 124, 127–130, 134, 135, 137, 140

izvabljanje 117

K

kazen 63, 64, 75, 76, 95

kazenska odgovornost 16, 75, 76, 81, 95, 97, 103, 107

kazenska odgovornost pravnih oseb 16

kazenski postopek 76, 84, 85, 88–91, 93, 94

kazenski pregon 85, 86, 91

Kazenski zakonik 83, 100, 108

kaznivo dejanje 71, 73–82, 85–93, 95, 97, 99–111

kemično orožje 56, 63

kibermimik 75–81

kibernetska kriminaliteta 15, 16, 27, 56, 62–64, 66, 69, 71, 72, 77, 79–84, 91, 92, 107, 109, 110, 122, 129

kibernetska mimikrija 75, 77, 78, 80–82

kibernetska obramba 55–57, 60, 61, 63, 65–69, 112, 130, 131, 134, 137–140

kibernetska varnost 55–57, 59, 60, 62, 64–67, 69, 130, 134, 135, 140

kibernetski konflikt 55, 61, 63

kibernetski prostor 7, 12, 15, 17, 55, 59, 61, 63, 68, 71–78, 80, 82, 98, 121, 122, 126

kibernetski terorizem 81, 129, 140

kibernetsko bojevanje 55–57, 61, 63, 68

kibernetsko zalezovanje 81

koda 5, 6, 7, 63, 86, 87, 91, 92, 108, 109, 126, 127, 131

komuniciranje 67, 71–73, 77, 78, 83, 86, 96, 116, 122–125

komunikacijski protokol 7, 133

kontrola 6–9, 11, 14, 20, 21, 22, 30, 42, 44, 45, 47, 51, 74, 115, 130–135, 137, 139, 140

kontrola dostopa 6, 7, 8

kontrolni sistem 21, 22, 130–135, 139, 140

Konvencija o kibernetski kriminaliteti 16, 27, 64, 69, 71, 72, 78–80, 83

korporativno omrežje 97, 98, 122
kriminaliteta 14–16, 27, 64, 66, 69, 71, 72, 79–84, 107, 109, 122, 129
kriptografski ključ 6
kritična infrastruktura 25, 56, 57, 64, 66–68, 119, 130, 134, 140
krivda 76, 77, 106
krovna varnostna politika 47, 51

L

lažni strežnik 111, 112

M

malware 5–7, 22, 63, 100, 108, 119, 123, 125, 131
mednarodna misija 60, 68
mednarodna organizacija 22, 31, 55, 58, 59, 63, 68
Mednarodna telekomunikacijska unija 64
mednarodne norme 55–57, 59, 60, 62–64, 69
mednarodni standardi 16, 29, 30, 32, 35
merjenje informacijske varnosti 14–27
merska lestvica 24
Ministrstvo za obrambo 66
MitB 112
MitM 112, 115
mobilna naprava 22, 95–101, 103, 106–109, 113, 121–124, 126, 128
mobilni telefon 64, 95–97, 99, 123–128
mobilno bančništvo 110, 125

mobilno omrežje 71, 122, 123
motenje podatkov 78, 79
motenje sistemov 79

N

nacionalna politika 55, 58, 59, 65
nacionalna varnost 59, 60, 62, 64, 66, 67
napad na informacijski sistem 89, 90, 103
nosilec elektronskih podatkov 88, 89, 92

O

obdelava osebnih podatkov 5, 6, 11, 16, 64, 102, 103, 107
oblak 95–99, 107, 108, 125
obramba v globino 130, 136, 134, 137–140
obrambna ustanova 5, 7, 10, 60, 61
obveščevalna služba 5, 7, 10, 100
ocena tveganja 9, 30, 31, 35, 138, 139
odklonsko vedenje 14, 15
odlaganje dokumentov 96, 98, 124, 125
omrežje 7, 8, 22, 66, 87, 88, 112, 122, 123, 125, 126, 128, 131–134, 136–138, 140
opustitev 95, 96, 97
osebni podatek 10, 16, 24, 27, 42, 77, 79, 96, 97, 99, 101–106, 109, 123
oškodovanec 76, 77
otroška pornografija 80, 81, 92
ozaveščanje 20, 23, 29, 35, 47, 52, 58, 62, 88, 98, 107, 118, 119, 120, 121, 124, 127–129, 130, 134, 135, 137, 140

P

pametni mobilni telefon 89, 95, 99, 123, 124, 126, 127
pedofilija 86
penetracijski test 22, 24, 132
PIN koda 126, 127
podatkovna baza 7, 132, 137
poklicna skrivnost 100–105
pooblaščenec za varovanje informacij 47
poslovna skrivnost 100–104
poslovni podatek 42
poslovni proces 28–30, 33, 39, 41, 42
požarni zid 22, 115, 134, 137, 140
pravice intelektualne lastnine 63
preiskava elektronske naprave 88–90, 92, 93
prevencija 52, 61, 64
pripomočki za kaznivo dejanje 79, 96
pripravljalno dejanje 79, 81
prisluškovanje 58, 131
privilegij zoper samoobtožbo 90, 91, 92
protipraven dostop 78, 79, 101, 103–106, 108
protipravno prestrezanje 78, 79, 131
protivirusna zaščita 115, 127, 132, 135, 138, 140

R

računalniška goljufija 80, 81
računalniški forenzik 87, 88, 90
računalniški sistem 7, 64, 71, 72, 75, 77–81, 89, 91, 130

ranljivost sistema 6, 9, 16, 17, 19–22, 25, 64, 130–134, 136, 138–140
razpoložljivost informacij 97, 133
revizija sistema 16, 24, 42–48, 51–54
revizor 44–48, 51–53, 120
ribarjenje 112

S

sanacija zapisov 11
Severnoatlantsko zavezništvo 56, 58, 61, 63, 68, 69, 70
sinhronizacija 124, 125
Skype 123, 125
SMS sporočila 116, 123–125
socialno omrežje 22, 71, 98, 122, 124, 125
sodba 64, 74, 91
sodišče 64, 74, 89, 91, 94, 108
sodna odredba 85, 88–93
spletni kriminal 56, 61,
spletni napad 62
standard ISO/IEC 27001 16, 28, 29, 30–32, 39, 40, 43–48, 50, 51, 53, 54
standard ISO/IEC 27003 28, 29, 31, 32, 37, 39, 40
standard ISO/IEC 27006 42–44, 46, 47, 48, 51, 53, 54
standard ISO/IEC 27007 42–48, 51–54
statistika 12, 22, 24, 41
strateška kultura 55–62, 64, 66, 68, 69
Svet za informacijsko varnost 66, 67
Svet za nacionalno varnost 67

Š

šifrirni algoritem 86

šifrirni ključ 86, 90–92

škoda 7, 21, 24, 69, 103, 107, 111, 131, 132

T

tajni podatek 5, 6, 7, 85, 86, 88, 96, 97, 100, 101, 102, 104, 105, 106, 109

terorizem 10, 56, 63, 64, 81, 129, 131, 140

U

uporabnik 5–8, 11, 23, 28, 29, 43, 50, 71–75, 77, 80, 82, 90, 93, 95–100, 106–119, 121–123, 126–128, 131, 140

USB ključ 89, 92, 132, 135

V

varnostna politika 7, 10, 15, 21, 23, 28, 29, 31, 47, 51, 58, 68, 128, 131, 134–136, 140

varnostna situacija 17, 20

varnostna strategija 15, 55–57, 59–62, 64–68, 113, 132, 134, 137, 140

varnostne rešitve 107, 113, 115, 121, 125–128, 130

varnostni ideal 21, 22

varnostni incident 16, 18, 20–25, 29, 45, 55, 58, 65, 67, 69, 132–138

varnostni popravek 22, 115, 132, 135, 139

varnostni sistem 5–7, 15, 22, 69, 137

Varnostni svet 60

varnostno opozorilo 115, 120

varnostno tveganje 9, 28, 56, 140
varovalni ukrep 31, 35
vdor v poslovni informacijski sistem 79, 103–105, 122
vdor v sistem 22, 28, 79, 83, 87, 100, 103–105, 122, 125, 137
večnivojska varnost 5–8, 10, 136
virtualni prostor 14, 15, 17, 55, 59, 61, 63, 68, 71–78, 80, 82, 98, 121, 122, 126
virus 56, 76, 100, 115, 125, 127, 132, 135, 138, 140
vohunska programska oprema 115
vojaška doktrina 56, 57, 61, 62
vrednost tveganja 8

Y

YouTube kanal 58

Z

Zakon o elektronskih komunikacijah 16, 27
Zakon o kazenskem postopku 84, 88–90, 94
Zakon o varstvu osebnih podatkov 10, 16, 27, 101, 103, 109
zasebnost 5, 6, 10, 42, 57, 59, 63, 69, 73, 74, 83, 91, 92, 97, 108, 109
zaseg elektronske naprave 87–89, 92
zaupni podatki 16, 18, 23, 63, 78, 79, 87
zavarovanje elektronske naprave 88
zlonamerna programska koda 5–7, 22, 63, 100, 108, 119, 123, 125, 131
zloraba informacijskega sistema 5, 6, 11, 17, 30, 79, 103, 112
zloraba osebnih podatkov 79, 102, 105, 106

Univerza v Mariboru

Fakulteta za varnostne vede

S Fakulteto za varnostne vede sodelujejo: