Kibernetični terorizem - sodobna varnostna grožnja informacijskim sistemom

Kaja Prislan, študentka magistrskega študija, Fakulteta za varnostne vede, Univerza v Mariboru
Igor Bernik, Univerza v Mariboru, Fakulteta za varnostne vede

Namen in cilj prispevka
Informacijski sistemi so temeljna podporna komponenta, brez katere sodobne organizacije ne morejo dosegati zastavljenih ciljev. Da jih lahko zavarujemo se moramo grožnjam zoperstavljati. Mednje spada tudi kibernetični terorizem, ki spretno izkorišča zmožnosti in pomanjkljivosti računalniških in spletnih storitev.
Namen prispevka je predstaviti kibernetični terorizem, ki se jo zaveda le malo organizacij in predstaviti njihov način razumevanja in zoperstavljanja tej obliki.

Metodologija
Izvedena je bila raziskava med različnimi organizacijami v obliki ankete za ugotovitev njihovega načina razumevanja in zoperstavljanja tej obliki grožnje, za proučitev narave pojava kibernetičnega terorizma pa je bila uporabljena deskriptivna metoda. Za pridobivanje podatkov in oblikovanje spoznanj o resnosti kibernetičnega terorizma bom uporabila strokovno literaturo domačih in tujih avtorjev ter internetne vire, ki se nanašajo na področje tematike.

Ugotovitve in omejitve
Omejitve se kažejo predvsem v nerazumevanju pojava tovrstnega terorizma, ki se ga v javnosti večkrat zmotno zamenjuje s klasičnimi napadi na informacijske sisteme. Terorizem pa je medtem zavzel obliko s katero lahko z minimalnim naporom in znanjem povzroči katastrofalne posledice in ogrozi obstoj sleherne organizacije. Metode in tehnike takšnega napada se ne razlikujejo od načinov delovanja klasičnih storilcev računalniške kriminalitete. Da lahko nek napad klasificiramo kot teroristični mora zato stremeti k političnim ali socialnim spremembam z namenom povzročiti strah med širšo javnostjo. Najpogostejši napadi so uperjeni v informacijske sisteme in kritično infrastrukturo. Posledice terorističnega napada na informacijski sistem organizacije se največkrat kažejo v ekonomski škodi, povzroči pa lahko tudi poškodbe ali smrt osebja. Tako kot v klasičnem modelu upravljanja s tveganji tudi tukaj grožnje in potrebe po zavarovanju klasificiramo glede na posledice, ki jih kibernetični teroristični napad lahko povzroči. Zavarovanje pred tovrstno kibernetično grožnjo je torej nujno, a odvisno od vsake organizacije posebej.

Izvirnost
V Sloveniji takšne raziskave še ni bilo izvedene, zatorej se bodo organizacije lahko seznanile s pomanjkljivostmi pri dojemanju kibernetičnega terorizma kot grožnje in se tako ustrezno prilagodile spremembam.

Ključne besede: kibernetični terorizem, informacijska varnost, tveganja, grožnje, zoperstavljanje

1 Uvod

V digitalnem obdobju, kateremu smo priča, je informacijski sistem osnova vsake organizacijske strukture. Zavarovanje lastnega podpornega sistema, je nujno potrebno za neprekinjeno in posledično uspešno poslovanje vsake organizacije. Da lahko takšen sistem sploh zavarujemo, moramo natančno proučiti strukturo le-tega, prepoznati njegove ranljivosti in grožnje, ki mu pretijo. Grožnje informacijskemu sistemu pa so najrazličnejše, od kraje podatkov do pregrevanja strojne opreme. Mednje spada tudi novodobna oblika terorizma, ki izkorišča, napada in uporablja kibernetični prostor.

Kibernetični terorizem predstavlja načrten, politično motiviran napad na informacijo, računalniški sistem, računalniške programe in podatke (Pollitt, 1997). Da lahko napad klasificiramo pod kibernetični terorizem mora biti zasnovan tako, da povzroči strah in vpliva tako na celotno družbo kot na oblast (Rogers, 2003). Dejstvo pa je, da računalniki ne morejo direktno ubiti ali poškodovati osebo, vendar pa obstajajo posredna tveganja fizičnih okvar in neposredna tveganja ekonomskih poškodb. Lahko pa se računalniki povežejo z drugimi napravami, ki imajo fizično zmožnost povzročiti smrt ali poškodbo. Kadar računalnike poimenujemo/uporabimo kot orožje, se moramo zavedati, da so njihova dejanja posredna (Pollitt, 1997). Kljub temu pa so lahko posledice, katastrofalne, včasih celo večje, kot pri klasičnem napadu teroristov.

Pomembnost informacije in sposobnost dostopa do nje, prenosa in dejanja na podlagi le-te, je narasla do te stopnje, da je upravljanje poslov brez računalnika ali spleta nedoumljivo. Medtem, ko se viša vrednost računalniške infrastrukture, se vrednost razdora te infrastrukture prav tako povečuje. Finančne posledice so ena stvar, vendar je lahko psihološki vpliv prekinitve spleta in informacijskih sistemov, še bolj uničevalen (Coleman, 2003), saj računalniki nadzirajo sisteme kritične infrastrukture, kot je dobava električne energije, komunikacija, letalski promet in finančne usluge. Organizacije jih uporabljajo za shranjevanje vitalnih informacij, od zdravniških kartotek, poslovnih planov do kazenskih evidenc (Pollit, 1997). Razkritje ali uničenje takšnih zaupnih podatkov lahko organizacijo stane posla. Le-te se torej morajo zavedati najpogostejših oblik napadov teroristov, da se pred njimi sploh lahko zavarujejo.

Najbolj prepoznavna in najpogostejša oblika kibernetičnega terorizma je napad na informacijski sistem, katerega glavni cilj je sprememba ali uničenje vsebine elektronskih datotek, računalniških sistemov ali materiala, ki ga le-ta vsebuje. Druga oblika napadov teroristov pa je usmerjena na uničenje ali poškodovanje kritične informacijske infrastrukture. Sem so vključeni napadi na strojno in programsko opremo, kjer je stranska posledica tudi uničenje podatkov. Tretja kategorija tovrstne oblike terorizma pa zajema uporabo interneta in informacijskih sistemov za izvedbo klasičnega terorističnega napada (Ballard, Hornik in McKenzie, 2004).

Kibernetični terorizem se torej po metodah in tehniki ne razlikuje od drugih zlonamernih napadov na informacijski sistem, zaradi česar se v laični javnosti pogosto tudi najbolj navadne in enostavne napade poimenuje kot terorizem. A vendar med njimi obstaja razlika. Ta se kaže v motivaciji, ki žene klasične storilce računalniške kriminalitete-hekerje in teroriste, ki izkoriščajo splet za dosego svojih ciljev. Slednji si prizadevajo za dosego enakih končnih posledic, kot klasični teroristi, to so politične in socialne oz. družbene spremembe. Medtem pa hekerji in crackerji izkoriščajo varnostne vrzeli v informacijskih sistemih zaradi najrazličnejših razlogov. Najpogosteje gre za željo po dokazovanju, velikokrat pa tudi za iskanje in opozarjanje na varnostne vrzeli. Neredko delujejo tudi po naročilu. V tej točki lahko pride do stika med slednjimi in teroristi, kadar so le-ti hekerjem pripravljeni ponuditi zadostno količino finančnih virov za izvršitev kibernetičnega napada na informacijski sistem vladnih institucij, večjih

korporacij ali sistem kritične infrastrukture. Hekerji v tem primeru ne zasledujejo političnih ciljev, temveč je glavni razlog premoženjski (Furnell in Warren, 2004).
Kljub temu, da kibernetični terorizem obstaja odkar obstaja internet, pa si strokovnjaki s tega področja še vedno niso enotni glede škode, ki jo le-ta lahko povzroči. Znano pa je, da se tovrstni napadi teroristov največkrat kažejo v ekonomski škodi, posredno pa se lahko ob optimalnih pogojih, kadar gre za napad na kritično infrastrukturo pomembno za oskrbo ljudi, posledice kažejo tudi v poškodbah ali smrti ljudi. Teroristi spletne storitve sicer izkoriščajo tudi za druge potrebe, kot je npr. načrtovanje, koordiniranje, oglaševanje, rekrutiranje, propaganda in zbiranje finančnih sredstev, vendar pa so direktni napadi, zaradi razvoja tehnologij, na informacijske sisteme vse pogostejši. Zaskrbljujoče je že samo dejstvo, da internet uporablja več kot 26% svetovne populacije (Internet World Stats, 2010), od tega več milijonov ljudi njegove zmožnosti izkorišča za zlonamerna dejanja. Zoperstavljanje kibernetičnemu terorizmu je torej nujno potrebno za zavarovanje tako finančnega kot tudi informacijskega premoženja organizacije na mikro in makro ravni države. Iz tega je možen sklep, da je kibernetični terorizem sodobna varnostna grožnja vsem informacijskim sistemov. Najbolj izpostavljene in ranljive točke teh sistemov so informacije in komunikacije, električno omrežje, plin in olje (shranjevanje, transport, pridobivanje), bančništvo in finance, transport, sistemi za oskrbo ljudi z vodo in vladne storitve. Da bi se zavarovale te točke pred napadi jih je potrebno čim bolj fizično omejiti od interneta in informacijskih sistemov, kolikor je to mogoče, prav tako pa ustrezno usposobiti ljudi, ki upravljajo s tovrstnimi sistemi (Embar-Seddon, 2004: 19). Za protiukrepe so zadolžene tako organizacije kot tudi država. Slednje se morajo zavedati, da so klasični protiteroristični ukrepi proti novodobni obliki terorizma neuspešni (Collin, 2005). Zavzeti morajo novejše pristope, za to pa je nujno potrebno natančno poznati sovražnika. Temu pa se morajo približati tudi organizacije, saj privatni poslovni center predstavlja kar 85% celotnega spleta (Seifert, 2004). O varnosti nekega sistema pa se vedno govori, da je sistem varen toliko kolikor je varen najšibkejši člen. Slabo zavarovana podjetja, ki ne prenesejo udarca ob varnostnem incidentu, ogrozijo vso varnost in trud države in globalne skupnosti. Da bi se lahko organizacije učinkovito zavarovale pred tovrstno grožnjo se analizi sistema in upravljanju s tveganji ne morejo izogniti. Postopek upravljanja s tveganji na tem področju se bistveno ne razlikuje od klasičnega. Vsekakor so posledice najpomembnejši faktor, ki prispeva k odločitvi ali se bo sistem pred tovrstno grožnjo zavaroval in kako. Za zagotavljanje čim večje informacijske varnosti (kajti absolutna varnost ni mogoča), morajo organizacije natančno proučiti lastno infrastrukturo in grožnje, ki le-tej pretijo. Ali mednje uvrščajo tudi kibernetični terorizem je povsem odvisno od vsake organizacije posebej, kot je tudi odvisen sam način upravljanja s tveganji.
Ker pa je kibernetični terorizem sodobna oblika grožnje, je organizacijam še relativno neznan pojav. To stopnjuje tudi dejstvo nizke ogroženosti in nezanimivosti Republike Slovenije za potrebe teroristov. Seveda pa se bo to v prihodnosti spremenilo, saj terorizem v virtualnem svetu zahteva veliko manj napora kot klasični. In če se želimo ustrezno zoperstaviti prihajajočim grožnjam se je pred njimi potrebno zavarovati že zdaj. Tudi v tem primeru velja, da je preventiva veliko bolje kot kurativa. Avtorja sva s pomočjo usmerjenih intervjujev, ki sva jih izvedla v 20 različnih slovenskih organizacijah (večjih, manjših, v zasebnem in javnem sektorju), želela ugotoviti, kakšno je stanje razumevanja te oblike grožnje v komercialnem okolju. Namen raziskave je narediti pregled in primerjavo med organizacijami v slovenskem prostoru, glede njihovega načina dojemanja kibernetičnega terorizma, načina zavarovanja pred njim in ukrepi ter grožnjami, ki jih pričakujejo v prihodnosti.

2 Ugotovitve

Ob ugotavljanju kako organizacije razumejo pojem kibernetični terorizem, kar polovica izprašanih organizacij meni, da je to zlonamerni napad na informacijski sistem z namenom kraje in okvare podatkov. V grobem to sicer drži, vendar pa so izpustile glavno komponento, ki pravzaprav definira sam terorizem-politična motivacija z namenom povzročiti strah. Bistvo pojava je tako razumela le osmina (15%) udeleženih v raziskavo. Nerazumevanje tovrstne grožnje je zaskrbljujoče ravno, zaradi njenega porasta in zmožnosti povzročiti katastrofalno poslovno škodo. Verjetno je napačno dojemanje kibernetičnega terorizma posledica neizkušenosti pri soočanju s to problematiko. Vsekakor pa gre nerazumevanje pripisati tudi pomanjkanju izobraževanja in ozaveščanja, o tovrstni računalniški kriminaliteti, uporabnikov in zaposlenih.
Glede na napačno razumevanje pojava kibernetičnega terorizma je razumljivo, da kar 2/3 izprašanih organizacij kibernetični terorizem pojmuje kot grožnjo enako vsem ostalim. Organizacije, ki so pred tem razumele bistvo pojava pa ga uvrščajo med nepomembne grožnje, kar je prav tako razumljivo, predvsem zaradi neizkušenosti pri soočanju s to problematiko. Meniva, da je tovrstna oblika terorizma trenutno manj pereča oblika groženj informacijskih sistemov, bo pa v prihodnosti vse pogostejša in bolj sofisticirana. Organizacije naj se zato posvetijo izobraževanju na področju razumevanja in zaščite pred virtualno teroristično grožnjo.
Pri navajanju škode, s časovnega, premoženjskega in psihološkega vidika, ki bi jo kibernetični terorist lahko povzročil z napadom na njihov informacijski sistem, so organizacije podajale zelo različne odgovore. To je najverjetneje posledica razlik v velikosti, dejavnosti, organiziranosti in zaščiti informacijskih sistemov med udeleženimi v raziskavi. Večje organizacije z večjim premoženjskim kapitalom bi ob isti zaščiti kot manjše organizacije neverjetneje utrpele večjo premoženjsko škodo. Ob slabši zaščiti pa bi tudi manjša organizacija lahko bila deležna večje škode kot, druga večja in bolj zaščitena. S časovnega vidika je povprečje izgube razpoložljivosti sistema več kot 9 dni. Vendar pa rezultati niso povsem zanesljivi, saj je čas okrevanja povsem odvisen od načinov zaščite lastnega informacijskega sistema. Od le-tega pa je prav tako odvisna premoženjska škoda, ki so jo organizacije v povprečju navedle več kot 50.000 €, odkloni tako v premoženjskem in časovnem vidiku pa so preveliki, da bi lahko govorili o zanesljivosti teh podatkov. So pa zanesljivi podatki o psiholoških posledicah, ki bi pri tovrstnem napadu nastale. Organizacije se strinjajo, da bi bila izguba kredibilnosti v poslovnem okolju med partnerji in strankami najočitnejša posledica. Nekatere so navedle še izgubo posla, kot morebitno psihološko škodo, ki pa bi najverjetneje sledila, preveliki premoženjski izgubi.
Kljub začetnemu nerazumevanju tovrstne kibernetične grožnje pa se vse izprašane organizacije strinjajo, da njihov informacijski sistem še ni bil tarča terorističnega napada. Dejstvo je primerljivo s stopnjo ogroženosti Slovenije pred terorizmom. Zaenkrat je območje Slovenije dokaj varno in stabilno, saj je za terorizem še neraziskano in nezanimivo območje. To dejstvo pa se lahko že jutri spremeni, saj so spremembe v mednarodnem in družbenem okolju nepredvidljive, kar prinaša nepredvidljivost in nestabilnost transnacionalnih groženj. Kmalu bosta tako lahko katerakoli slovenska organizacija in njen informacijski sistem, postala tarča virtualnega terorističnega napada.
Skladno z odgovori o resnosti grožnje kibernetičnega terorizma, ko je večina izprašanih organizacij to grožnjo enačila z ostalimi grožnjami njihovemu informacijskemu sistemu, se tako pred njim tudi zavarujejo. Skoraj 2/3 organizacij se pred kibernetičnim terorizmom zaščiti enako kot pred ostalimi grožnjami. To vrsto grožnje ne obravnavajo posebej, temveč jo enačijo z vsemi ostalimi, kar se torej odraža na zaščiti pred terorističnimi napadi. Posebnih mehanizmov varovanja in okrevanja se ne poslužujejo, iz česar sledi, da za potrebe zaščite pred kibernetičnim

terorizmom uporabljajo splošen pristop. To je pravzaprav smiselno, saj teroristi, v kibernetičnem prostoru uporabljajo enake tehnike in metode kot storilci klasične računalniške kriminalitete. Zavarovanje pred hekerskimi vdori je torej uporabno za zaščito pred terorističnimi. Menimo pa, da bi bilo potrebno bolje poznati samo naravo in zmožnosti takšnega pojava, kajti golo enačenje z ostalimi grožnjami vodi v nevarno ignoranco. Z boljšim razumevanjem sposobnosti kibernetičnega terorizma, bi lahko izboljšali lastno zaščito in hitreje odpravljali posledice tudi ob vdoru klasičnih storilcev.

Kljub temu, da večina organizacij kibernetični terorizem ne dojema kot resno grožnjo in ga enači z ostalimi grožnjami njihovim informacijskim sistemov, pa skoraj vse izprašane organizacije menijo, da se bodo teroristi vse pogosteje posluževali koristi informacijskih in spletnih storitev za dosego zastavljenih političnih ciljev. Iz tega sledi, da se organizacije zavedajo sprememb v informacijskem okolju, tako na ravni groženj le-temu, kot na ravni zaščite. Informacijska tehnologija je integriran del sodobne družbe, brez katere organizacije ne morejo uspešno in konkurenčno poslovati. Tega se zavedajo tudi njihovi nasprotniki, ki lahko z ustreznim znanjem, zaradi trenutne nezadostne zaščite, z minimalnim naporom predrejo varnostne ovire in onesposobijo njihove sisteme. Zavedanje o rasti nevarnosti tovrstne grožnje kaže na visoko stopnjo varnostne kulture.

Skoraj polovica organizacij pa občuti tudi večjo izpostavljenost in ranljivost pred kibernetično obliko terorizma. Najverjetneje je to posledica visoke stopnje zanašanja in odvisnosti poslovanja od informacijske tehnologije. Čeprav so izpostavljene tudi pred klasičnimi napadi pa je verjetnost napada v fizični obliki manj verjetna, kot tista preko informacijskega sistema. Z informacijsko tehnologijo so organizacije povezane z drugimi organizacijami in državami kar ustvarja mednarodno medmrežje. Dostop do sistema z oddaljene lokacije je tako veliko bolj privlačen in enostaven, kot fizična prisotnost na samem kraju, še posebej ob upoštevanju dejstva, da je Slovenija trenutno manj zanimiva država s terorističnega vidika. Organizacije, ki se čutijo bolj izpostavljene pred klasično obliko terorističnega napada, pa so manj odvisne od informacijske tehnologije oz. le-ta ni ključnega pomena za uspešno poslovanje.

Pri navajanju bodočih varnostnih groženj informacijskim sistemov so organizacije podajale najrazličnejše odgovore. Vse pa menijo, da nevarnost leži v transformaciji že znanih groženj (kraja podatkov, vdori v sisteme, ipd) v bolj napredne in sofisticirane oblike. Najbolj ogrožena naj bi bila razpoložljivost informacijskih sistemov. Že zdaj poznamo izredno domišljene načine vdiranja in onesposabljanja sistemov, ki pa bodo v prihodnosti še bolj napredni. Nove oblike groženj je težko napovedovati, saj je prihodnost izjemno nepredvidljiva in nestabilna, ravno zaradi stalnih sprememb, vsekakor pa bodo le-te povezane z novimi napravami in storitvami. Vsakršna tehnologija ima svoje pomanjkljivosti, ki jih ljudje z ustreznim znanjem in motivacijo zlahka izkoristijo. Vsekakor se bodo razvile tudi metode in tehnike socialnega inženiringa, kar bo storilcem olajšalo pridobivanje podatkov. Pri odgovorih je zanimivo, da organizacije menijo, da je grožnja v prihodnosti tudi nesposobnost delovanja klasičnih sistemov, zaradi vse večje odvisnosti od tehnologije. Zaradi le-tega in medsebojne povezanosti in soodvisnosti med informacijskimi sistemi in tehnologijo bodo najverjetneje vse pogostejši tudi verižni efekti-kolaps sistemov enega za drugim.

Več kot polovica izprašanih organizacij meni, da bodo grožnje v prihodnosti bolj nevarne kot sedanje. Meniva, da to drži, saj se bo z razvojem strukture in metod groženj njihova resnost in nevarnost samo še stopnjevala. Grožnje bodo v prihodnosti torej vse bolj grozile obstoju, poslovanju in delovanju informacijskih sistemov, kar pa nujno ne pomeni, da bodo organizacije pred njimi bolj ogrožene. Tako kot se razvijajo in spreminjajo grožnje se spreminja in izboljšuje tudi zaščita pred njimi. Razlika je le v tem, da razvoj groženj ni odvisen od organizacij, le-te se

razvijajo skladno s spremembami v mednarodnem, družbenem in tehnološkem okolju, medtem pa je zaščita informacijskih sistemov popolnoma odvisna od volje organizacij. Le-te morajo poskrbeti, da se ogroženost in ranljivost njihovih informacijskih sistemov ne bo povečala temveč se bo prilagajala prihajajočim varnostnim grožnjam.
Za povečevanje informacijske varnosti je moč storiti veliko. Skoraj polovica organizacij pa največ pozornosti namenja izobraževanju in ozaveščanju tako uporabnikov podatkov in sistemov, kot zaposlenih, ki z njimi upravljajo. Preventiva je vsekakor najpomembnejši del dolgoročne odprave varnostne problematike, vendar pa so tudi drugi ukrepi izjemno pomembni za obvarovanje pred varnostnimi grožnjami informacijskim sistemov. Mednje vsekakor spada tudi nenehno spremljanje novosti tako na področju razvijanja groženj, kot posodabljanja obrambnih mehanizmov. Vpeljevanje le-teh v informacijsko strukturo vsekakor pomeni dvig ravni zaščite in varnosti, za formalno potrditev le-tega pa se lahko odločijo tudi za certificiranje informacijskega sistema s standardom ISO 27001.
Organizacije menijo, da se pred kibernetičnemu terorizmu lahko izognejo na enak način kot se zavarujejo pred ostalimi grožnjami informacijskim sistemom. To je sicer skladno z odgovori, da se zavarujejo pred njimi na enak način, vendar pa menimo, da se je izogniti takšnemu pojavu izjemno težko. Uporabniki in zaposleni lahko storimo vse, da bi ranljivost informacijskih sistemov zmanjšali na najmanjšo možno mero, vendar je to vse kar lahko storimo. Izognemo se mu lahko le tako, da informacijskega sistema sploh nimamo. Ko ga enkrat imamo, so kljub vsem zaščitam in varnostnim ukrepom prisotne določene ranljivosti, ki jih bodo ljudje z ustrezno stopnjo znanja in motivacije lahko izkoristili.

3 Sklep

Kibernetični terorizem, kot ena izmed najnovejših groženj informacijskim sistemom, se zaradi podobnosti v načinu delovanja in obliki, v javnosti velikokrat zamenjuje za klasično računalniško kriminaliteto. To so potrdile tudi ugotovitve izpeljane iz raziskave v slovenskih organizacijah na področju informacijske varnosti. Zaključujeva tako, da je kibernetični terorizem za organizacije novejši in zato neznan pojav. V večini organizacije tovrstno grožnjo enačijo z ostalimi in se skladno s tem, tako tudi zavarujejo. Zaščita pred teroristično grožnjo informacijskim sistemom se ne razlikuje od zaščite pred ostalimi grožnjami, saj je zanje sistem upravljanja s tveganji na tem področju popolnoma enak kot za ostala tveganja. Morda bi škoda, povzročena ob napadu na informacijski sistem organizacije povečala zanimanje za takšno obliko terorizma, vendar pa organizacije še niso bile tarča takšnega napada, zato je ugotavljanje morebitne škode na tem področju zelo oteženo. Kljub nizki stopnji ogroženosti slovenskih organizacij pred terorizmom, pa večina teh meni, da so bolj ranljive in izpostavljene kibernetičnemu, kot fizičnemu napadu teroristov. Najverjetneje je to posledica visoke stopnje odvisnosti od informacijske tehnologije, ki je tarča teroristov v virtualnem svetu. Zaradi povečevanja te odvisnosti in nezmožnosti poslovanja brez spletnih in računalniških storitev, organizacije v prihodnosti pričakujejo povečano aktivnost teroristov v informacijskem in komunikacijskem okolju. Prav tako menijo, da se bodo že obstoječe grožnje, zaradi sprememb v informacijskem in tehnološkem okolju še razvijale in postale bolj sofisticirane, zaradi navezanosti organizacij na tehnologijo pa bo škoda ob uspešnem napadu vse večja. Zavedanje organizacij o prihajajočih nevarnostih, kaže na visoko stopnjo varnostne kulture, zato na tem mestu največ pozornosti pri izogibanju grožnjam in povečevanju informacijske varnosti, posvečajo preventivnim ukrepom. Kljub nezadostnemu razumevanju narave terorizma v virtualnem prostoru, meniva, da so organizacije na dobri poti doseganja zadostne stopnje ozaveščenosti in pripravljenosti soočanja z najnovejšo virtualno

grožnjo informacijski varnosti. Izogniti se ji tako ali tako ne moremo, kajti odvisnost organizacij od informacijske tehnologije je prevelika. Največ kar na tej točki lahko naredijo, je pripraviti čim boljši postopek okrevanja in obnavljanja v primeru varnostnega incidenta, prav tako pa o grožnjah ozavestiti vse uporabnike sistema in njegove upravljavce.

4 Literatura

Ballard, J.D., Hornik, J.G. in McKenzie, D. (2004). Technological Facilitation of Terrorism.V A. O'Day (ur.), Cyberterrorism (str. 39-66). Aldershot: Ashgate Publishing Limited.

Coleman, K. (2003). Cyber Terrorism. Pridobljeno 23.1.2010, na http://www.directionsmag.com/article.php?article_id=432

Collin, B.C. (2005). 11th annual international symposium on criminal justice issues. Pridobljeno 23.1.2010, na http://afgen.com/terrorism1.html

Embar-Seddon, A. (2004). Cyberterrorism. V A. O'Day (ur.), Cyberterrorism (str. 11-21). Aldershot: Ashgate Publishing Limited.

Internet World Stats. (2010). Internet usage statistics. Pridobljeno 10.4.2010, na http://www.internetworldstats.com/stats.htm

Pollitt, M.M. (1997). Cyberterrorism - Fact or Fancy? Pridobljeno 23.1.2010, na http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Rogers, M. (2003). The psychology of Cyber-Terrorism. V S. Andrew (ur.), Terrorists, victims and society : psychological perspectives on terrorism and its consequences (str. 77-91). Chichester: Wiley.

Seifert, J.W. (2004). The effects of September 11, 2001, terrorist attacks on public and private information infrastructure: a preliminary assessment of lessons learned. V A. O'Day (ur.), Cyberterrorism (str. 289-306). Aldershot: Ashgate Publishing Limited.