Korporativna varnost

ICS
Institut za korporativne varnostne študije

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!

Letnik 2012, september • št. 1



Obvladovanje tveganj skozi perspektivo mednarodnega korporativnega okolja

g. Andrej Podvršič,
Director of Security, Du Pont International of Europe, Middle East & Africa

Korporativno varnostni manager leta 2011

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

Prvim desetim strankam, ki se bodo javile na elektronski naslov: *miran.vrsec@novapanorama.si* ponujamo brezplačno uro varnostnega svetovanja na temo kako optimizirati investicije v varnostni sistem in tekoče stroške financiranja varnostnega sistema?

IZVIRNA MISEL

Profesionalni in celovit varnostni sistem v podjetju odločilno prispeva k povečanju pozitivnih poslovnih izidov ter k dvigu kulture, konkurenčnih prednosti in ugledu podjetja (M. Vršec).

PRAVA IZBIRA

Nova Panorama, d. o. o. je ob sodelovanju vrhunskih varnostnih strokovnjakov usposobljena izvajati varnostni inženiring, to je varnost od A do Ž oziroma t. i. "varnost na ključ". Gre za vzpostavljanje integralnih varnostnih sistemov na projektni način, z integracijo varovanja v sisteme vodenja kakovosti z uvajanjem varnostnih standardov ter z upoštevanjem dobre prakse. Konkretni projektni proizvod je izdelava in implementacija varnostnega elaborata.

Storitve in produkti Nova Panorama, d. o. o. naročniku oziroma uporabniku zagotavljajo uvedbo varnostno in ekonomsko upravičenega varnostnega sistema, ki vzpostavlja ustrezno preventivo, opozorilni sistem in proces obvladovanja ranljivosti, ogroženosti, sprememb, tveganj in izrednih dogodkov.

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

- Načini (oblike) svetovanja
- Posnetek in analiza stanja
- Intervjuji in vprašalniki
- Ocene ogroženosti
- Varnostni elaborati
- Pravilniki, načrti, navodila

Integralni varnostni sistemi (celovito varovanje)

- Varnostna funkcija
- Varnostna politika
- Varnostna strategija
- Pravna podlaga
- Organiziranost in status varovanja
- Področja varnosti
- Civilna zaščita
- Varnostni menedžment
- Varnostni režim
- Alarmni in odzivni sistem
- Strokovni nadzor
- Portfelj zavarovanj

Varovanje oseb in premoženja

- Varovanje ljudi premoženja
- Prevoz in varovanje denarja ter drugih vrednostnih pošiljk
- Varovanje javnih zbiranj
- Izvajanje sistemov tehničnega varovanja

Kakovost in varnost

- Integracija varovanja v ISO 9000:2000
- Varnostni standardi
- Presojevalci kakovosti varovanja

Krizno vodenje (krizni menedžment)

- Objektivna potreba po načrtovanju kriznega vodenja
- Poslovanje na rezervni lokaciji

IZOBRAŽEVANJE

Varnostni menedžment

- Obvladovanje poslovnih in varnostnih tveganj ("risk management")
- Usposabljenje kriznega štaba
- Varnostna služba – usposobljenost varnostnikov za naloge varovanja podjetja
- Varnostna kultura in poslovna etika
- Usposabljanje za nadzornike
- Scenariji obvladovanja izrednih dogodkov





Korporativna varnost

Spoštovane bralke, spoštovani bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
dr. Denis Čaleta

Trženje:
ICS-Ljubljana
info@ics-institut.si
Aljoša Kandžič
aljosa.kan@ics-institut.si
Andrej Kovačič
andrej.kovacic@ics-institut.si

Oblikovanje in DTP:
Robert Mostar

Tisk:
Schwarz print d.o.o.

Datum izida
september 2012

Izvod revije je brezplačen

Naslovnica:
123RF Limited

ISSN 2232-6170

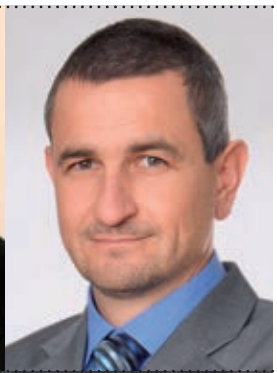
Objavljeni prispevki in njihova vsebina odraža mnenja in stališča avtorjev ter predstavljajo v celoti njihovo odgovornost.

Pred vami stoji nova strokovna revija, ki pokriva področje korporativne varnosti in s tem zapolnjuje prostor, ki je bil do sedaj v Sloveniji skoraj neobdelan. To nam ustvarjalcem te revije na eni strani daje edinstveno priložnost, da zaorjemo ledino in na novo pozicioniramo korporativno varnost kot zelo pomembno področje delovanja naše družbe, na drugi strani pa to pred nas postavlja odgovornost velikih pričakovanj strokovne in laične javnosti, da bodo vsebine, ki jih bo revija ponujala zanimive, poučne in dovolj raznovrstne, da bodo vsi našli del svojih pričakovanj. Živimo namreč v zapletenem dinamičnem okolju, kjer varnost, kot osnovna človeška potreba, še zdaleč ni sama po sebi umevno dejstvo. Varno okolje je za nemoten razvoj družbe in tudi organizacij, ki delujejo v tem okolju, postalo dobrina za katero se moramo ustrezno truditi. Management je v organizacijah javnega in zasebnega okolja danes postavljen pred pomembno dilemo in sicer kako z resursi, ki jih ima na voljo, ustrezno obvladati tveganja, katerim je izpostavljena njihova organizacija. V tem globalnem okolju neprestane tekmovalnosti in konkurenčnosti so ti ukrepi še toliko bolj pomembni, saj si s sistemskim pristopom in inovativnostjo na področju obvladovanja tveganj lahko zagotoviš določeno prednost pred konkurenco ali pa preprosto nimaš možnosti za preživetje. S tega stališča je za strateški management pomembna sposobnost zavedanja, da popolne varnosti ni mogoče zagotoviti, temveč, da se skozi različne sistemske mehanizme vedno znova odvija proces tehtanja in iskanja ustreznega razmerja med razpoložljivimi viri in stopnjo obvladovanja tveganj do te mere, da osnovni procesi v organizacijah potekajo nemoteno. V tem okviru kadrovski potencial organizacije, tudi skozi prizmo obvladovanja tveganj, na eni strani predstavlja njen najmočnejši člen na drugi strani pa tudi največje tveganje, katerega lahko učinkovito upravljamo samo s kontinuiranim vzpostavljanjem ustreznega okolja s poudarkom na ustrezni organizacijski in varnostni kulturi. Nove tehnološke rešitve, ki v vse večjem obsegu temeljijo na komunikacijsko-informacijski podpori so dejstvo in realnost, ki so postale stalnica in nujni predpogoj za normalno delovanja družbe kot celote. S temi procesi pa se pojavljajo pomembne varnostne dileme varovanja zasebnosti, informacij, osebnih podatkov in drugih pomembnih dejavnikov.

Na vsa in še druga vprašanja bomo ustvarjalci revije "Korporativna varnost" polagali ustrezno pozornost skozi odpiranje dilem in tudi podajanje določenih rešitev, novih spoznanj in dobrih praks.

Za ustrezno kakovostno raven revije pa ste pomembni tudi vi spoštovane bralke in bralci, sponzorji, znanstveniki, strokovnjaki in druga zainteresirana javnost saj lahko s svojimi mnenji, vprašanji, predlogi in tudi z dobrimi praksami in spoznanji iz vaših okolij, bistveno pripomorete k vsebinski rasti revije in nenazadnje tudi področja korporativne varnosti. Samo skupaj smo močnejši, kar se odraža tudi skozi osnovno poslanstvo Slovenskega združenja korporativne varnosti "**Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!**".

Doc. dr. Denis Čaleta
Glavni urednik

INTERVJU
mag. Miran Vršec in doc. dr. Denis Čaleta
soustanovitelja Instituta za korporativne varnostne študije, ICS-Ljubljana

POT DO USPEHA INSTITUTA ZA KORPORATIVNE VARNOSTNE ŠTUDIJE-ICS TLAKOVANA S TRDIM IN SISTEMATIČNIM DELOM 5



INTERVJU
g. Andrej Podvršič
Director of Security, Du Pont International of Europe, Middle East & Africa

OBVLADOVANJE TVEGANJ SKOZI PERSPEKTIVO MEDNARODNEGA KORPORATIVNEGA OKOLJA 12



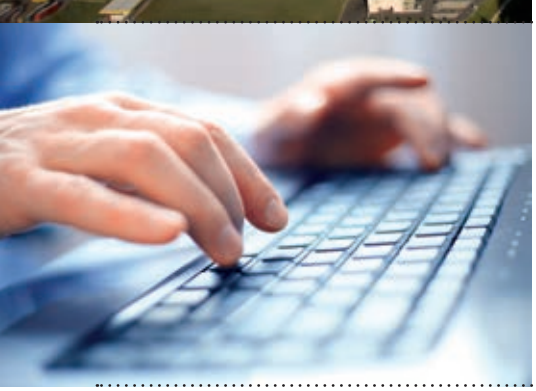
INTERVJU
g. Domen Pirkmajer,
korporativno varnostni manager, TE-TOL

KORPORATIVNO VARNOSTNI MANAGER LETA 2011 16



KORPORATIVNA VARNOST – KONKURENČNA PREDNOST GORENJA, D.D.

Varnost je za poslovno uspešnost Gorenja ena izmed pomembnih poslovnih funkcij. Kot korporativno varnost označujemo vse aktivnosti v družbi, s katerimi opredeljujemo in izvajamo potrebne sistemske ukrepe za obvladovanje varnostnih tveganj. 27



SISTEM UPRAVLJANJA VAROVANJA INFORMACIJ V ORGANIZACIJAH Z VIDIKA KORPORATIVNE VARNOSTI

Popolnoma jasno nam je, da je ustrezna informacijska infrastruktura postala odločilen dejavnik, ki pripomore k uspehu organizacije. Hkrati se vse bolj zavedamo pomembnosti varovanja informacij, ki mora postati del življenjskega cikla v razvoju in vzdrževanju informacijskih sistemov. 39

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije-ICS*

INTERVJU
mag. Miran Vršec in doc. dr. Denis Čaleta
soustanovitelja Instituta za korporativne varnostne študije, ICS-Ljubljana

POT DO USPEHA INSTITUTA ZA KORPORATIVNE VARNOSTNE ŠTUDIJE-ICS TLAKOVANA S TRDIM IN SISTEMATIČNIM DELOM

»Odsotnost zavedanja strateškega managementa o pomenu celovitih pristopov do obvladovanja tveganj v organizacijskih okoljih ima za slovensko gospodarstvo izredno negativne posledice. Te posledice so še toliko izrazitejše v obdobju gospodarske krize, kjer načeloma preživijo samo tisti, ki ustrezno obvladujejo tveganja, katerim je izpostavljeno delovanje njihovih organizacij in so s tem na izredno zahtevnem tržišču konkurenčnejši in bolj prilagodljivi od svojih neposrednih tekmecev« trdita Vršec in Čaleta.

Institut za korporativne varnostne študije ICS-Ljubljana vedno bolj postaja referenčna institucija v Sloveniji in tudi v regiji na področju korporativne varnosti. Ste zadovoljni s prehojeno potjo?

Čaleta: Nihče ni pričakoval tako velikega uspeha in tako pomembne vloge, ki jo danes ima Institut za korporativne varnostne študije v Sloveniji in tudi v širšem mednarodnem prostoru. Vse to je bilo doseženo s trdim in predanim delom vseh sodelavcev ICS-Ljubljana. Veliko pa je na uspeh vplivalo tudi dejstvo, da je bilo področje korporativne varnosti do sedaj relativno slabo raziskano in nesistemsko obravnavano. Vse to je botrovalo k temu, da so bile ideje in aktivnosti ICS-Ljubljana zelo pozitivno sprejete, tako v gospodarskem okolju kakor tudi v okolju javne uprave. Osnovno poslanstvo dvigovanja zavedanja o pomenu obvladovanja varnostnih tveganj je namreč povezano z vsakim organizacijskim okoljem ne glede na to ali gre za javno ali zasebno okolje.

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha! *"Ab uno disce omnes (po enem spoznaj vse)"*.

Vršec: Ustanovitelja inštituta in nekateri najožji sodelavci inštituta smo temelje za ustanovitev inštituta gradili nekaj let. Ko smo začutili pravi trenutek, smo združili znanja in izkušnje in ustanovili inštitucijo, katere primarni cilj je razvoj korporativne varnosti v lokalnem in globalnem okolju. Tudi tokrat so nam skeptiki in ostali, ki niso verjeli v našo idejo na ves glas zatrjevali, da je petelin spet zakikirikal prekmalu, pa vendar smo bili prepričani, da je to edini pravi način organiziranega delovanja za dose-

*avtor je član Slovenskega združenja korporativne varnosti

ganje zastavljenega cilja. Ko sedaj, po dobrih dveh letih delovanja inštituta pogledam nazaj, lahko s ponosom ugotovim, da je petelin zakikirikal pravi čas. Dejstvo je, da smo uspeli v tem času organizirati več strokovnih dogodkov (posvetov, konferenc, okroglih miz, strokovnih srečanj in drugih dogodkov) kot vse ostale strokovne inštitucije v Republiki Sloveniji skupaj, obenem pa smo uspeli našo idejo plasirati tudi v regijo, na kar smo še posebej ponosni. V teh kriznih časih sem še posebej ponosen tudi na dejstvo, da smo ves dosedanji razvoj uspeli financirati z lastnimi finančnimi sredstvi in lastnimi kadrovskimi resursi.

Kateri so tisti dejavniki, ki bi jih posebej izpostavili?

Vršec: Kot sem že dejal, je ključ uspeha v specifičnih in interdisciplinarnih znanjih sodelavcev inštituta, ki predstavljajo tudi gonilno silo inštituta. Pri tem je pomembno izpostaviti dejstvo, da vsa znanja in izkušnje temeljijo tudi na več deset letnem delu posameznih strokovnjakov in ekspertov inštituta v gospodarskem in javnem okolju. Izdelani elaborati, študije, analize, raziskave in ostale projektne naloge ter znanstveno in strokovno raziskovalno delo, ki je marsikateri organizaciji, tako v javnem, kot zasebnem sektorju, prinesla toliko koristi, so dokaz, da imamo izdelan model, ki organizacijam pomaga pri optimizaciji obvladovanja tveganj ter povečevanju njihove konkurenčnosti v javnem in poslovnem okolju v katerem delujejo. Vsekakor je pomembno poudariti tudi povezovalno vlogo inštituta, ki v Združenju za korporativno varnost povezuje in združuje znanja in izkušnje strokovnjakov z različnih okolij in področij korporativne varnosti.

V okviru ICS-Ljubljana deluje tudi Slovensko združenje za korporativno varnost. Kakšna je dodana vrednost tega združevanja?

Čaleta: Slovensko združenje korporativne varnosti predstavlja izredno pomemben del našega delovanja in mu prav zaradi tega namenjamo posebno pozornost. Združenje že skozi svoja temeljna izreka, ki se glasita »**Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!**« in »**Ab uno disce omnes (po enem spoznaj vse)**«, ponazarja tisto osrednje poslanstvo. Namreč to združevanje predstavlja odlično okolje za izmenjavo mnenj, dobrih praks in predvsem prenos novih spoznanj iz raziskovalnih dognanj v prakso operativnega okolja. Poznamo namreč dve obliki članstva in sicer redno članstvo, kjer so člani strokovnjaki posamezniki in korporativno članstvo, kjer so člani združenja organizacije iz javnega in zasebnega okolja. V svojem okviru imamo namreč najpomembnejše organizacije, ki upravljajo s pomembnimi infrastrukturnimi področji od energetike, prometa pa vse do informacijsko komunikacijskega področja. Posebej pa me veseli, da so svoj interes po sodelovanju našle tudi pomembne javne institucije, katere še posebej predstavljata Urad Informacijske pooblaščenke in Urad RS za varovanje tajnih podatkov. To namreč dokazuje, da je omenjeno združevanje tista ustrezna oblika, ki v danem trenutku ponuja neke nove kvalitete in obseg sodelovanja, v katerem se lahko združuje širok spekter posameznikov in organizacij, ki so neposredno in posredno povezane s korporativno varnostjo in s tem tudi potrebnim zavedanjem po učinkovitem obvladovanju tveganj.



Ena od pomembnih dejavnosti ICS je izvajanje izobraževanja in organizacija mednarodnih in nacionalnih konferenčnih dogodkov. Kaj v Slovenski prostor prinašajo ti dogodki?

Čaleta: Tem aktivnostim v ICS-Ljubljana posvečamo veliko pozornost, saj smo mišljenja, da ti konferenčni in posvetovalni dogodki v slovensko okolje prinašajo neka nova znanja in pristope, ki so nujni, da se bo dolgoročno zavedanje strateškega managementa in drugih upravljalskih struktur v naših organizacijah začelo dvigovati na višjo raven. Zelo pomembno je namreč zavedanje, da je celovit pristop vzpostavljanja organiziranega sistema delovanja korporativne varnosti nujen in osnoven predpogoj za nemoteno in varno delovanje vsake organizacije. Na teh dogodkih s pomočjo vrhunskih predavateljev ponujamo aktualne vsebine, organiziramo pa tudi okrogle mize, kjer so naši udeleženci najpomembnejši odločevalci v korporativnem in javnem okolju, ter s tem prenašamo nova znanja in zavedanje na naše udeležence posvetov in konferenc, kakor tudi preko tega izobražujemo strateški management, ki na okroglih mizah sodeluje v obliki aktivne udeležbe razpravljalcev. Pomemben del te zgodbe predstavljajo tudi naši mednarodni dogodki, kjer velja še posebej izpostaviti našo tradicionalno mednarodno konferenco »Dnevi korporativne varnosti«, ki vsako leto v marcu predstavlja največji tovrstni dogodek v regiji JV Evrope.



Tudi na področju raziskav in razvoja izvajate pomembne korake. Menite, da je znanstveni pristop tisti pravi, ki bo veljavo področja korporativne varnosti in celovitega obvladovanja tveganj dvignil na višji nivo?

Čaleta: Danes se brez sistematičnega znanstvenega pristopa ni mogoče predstavljati razvoja tako pomembnega področja kot je korporativna varnost. Znanstvena spoznanja pridobljena skozi raziskovalne projekte, so tista nujna podlaga na katerih se lahko gradi nove pristope in mehanizme, ki bodo v teh zahtevnih konkurenčnih in finančnih okoliščinah organizacijam, katere bodo obvladovanju tveganj namenile ustrezno pozornost, prineslo določeno konkurenčno prednost pred tekmeci in s tem tudi uspešnejše in učinkovitejše poslovanje. V okviru ICS-Ljubljana deluje raziskovalna skupina, ki je vpisana v razvid raziskovalnih skupin Agencije Republike Slovenije za raziskave in razvoj, pridobili pa smo tudi vse ustrezne akreditacijske postopke za vpis v raziskovalno bazo Nato in EU agencij. V vsakem projektu pa je naše osnovno vodilo, da znanstvena spoznanja kasneje prenašamo v prakso in v tem okviru je ravno Slovensko združenje korporativne varnosti tisto okolje, kjer se to še kako učinkovito izvaja z odličnimi rezultati.

Skupaj s Fakulteto za podjetništvo-GEA College razvijate podiplomski magistrski program »management korporativne varnosti«. Nam lahko poveste kaj bo glavna vrednost tega programa?

Čaleta: Študijski program Management korporativne varnosti je študijski program visokošolskega izobraževanja po drugi bolonjski stopnji, ki smo ga razvili v sodelovanju med ICS-Ljubljana in GEA College-Fakulteto za podjetništvo. Predstavlja namreč inovativni pristop interdisciplinarno zastavljenega podiplomskega študija, ki zajema široko paleto predmetov in področij poslovnih in varnostnih ved ter ostalih vsebinskih sklopov, kot so: ekonomija, finance, pravo, informatika, management, elementi nadzora, varnostni standardi, okoljski vidiki, katera so nujno potrebna za managerja korporativne varnosti. Magistrski program »Management korporativne varnosti« obsega znanja, ki so potrebna za obvladovanje procesov celovitega načrtovanja in izvedbe procesov integralne varnosti

v podjetjih in drugih organizacijah v domačem in mednarodnem okolju. Temelji na znanstveno–raziskovalnih dosežkih družboslovnih, podjetniških in naravoslovnih ved. Osrednji cilj je izobraziti managerje in strokovnjake s področja korporativne varnosti, ki bodo imeli široko poslovno znanje in perspektivo ter dobro razumevanje globalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja. Bistvo tega je pripraviti diplomante, da bodo sposobni spremljati trende zagotavljanja integriranih varnostnih rešitev v gospodarskem in poslovnem okolju ter okolju javne uprave.
Poseben pomen bo namenjen ravno povezavi med znanstveno raziskovalnimi spoznanji in realnim okoljem. V tem okviru bodo v okviru programa gostovali pomembni poslovneži, znanstveniki in strokovnjaki, najboljšim študentom pa bo omogočena tudi praksa v mednarodnem korporacijskem okolju in seveda zaposlitev.

ICS izvaja zelo aktivno mednarodno sodelovanje. Nam lahko zaupate kašni so nadaljnji načrti na tem področju.

Čaleta: V ICS in Slovenskem združenju korporativne varnosti smo bili eni izmed ustanoviteljev mednarodne asociacije s področja korporativne varnosti z nazivom SE European Corporate Security Association (SECSA). Omenjena mednarodna asociacija predstavlja možnost združevanja nacionalnih asociacij in strokovnjakov na širši mednarodni ravni. To sodelovanje je zelo pomembno iz večjih vidikov, naj omenim samo nekaj tistih najpomembnejših, kot so skupno nastopanje na področju razvoja in raziskav, organizacija mednarodnih dogodkov, izmenjava dobrih praks in novih spoznanj ter nazadnje najpomembnejši dejavnik, ki se odraža v dejstvu, da omenjena asociacija na mednarodni ravni zastopa interese strokovnjakov in naročnikov varnostnih storitev v razmerju do zakonodajalcev in ponudnikov neposrednih varnostnih storitev na tem zahtevnem dinamičnem tržišču.
Vršec: Razvojne dejavnosti inštituta so vsekakor usmerjene tudi v mednarodni prostor. V fazi zagona smo delovali po načelu »Razmišljaj globalno, deluj lokalno«, saj je bil primaren interes postavitev trdnih temeljev za dolgoročen razvoj inštituta. V posameznih fazah nadaljnjega razvoja inštituta bomo vse več aktivnosti usmerjali v razvoj dejavnosti inštituta v mednarodnem okolju po načelu »Razmišljaj globalno, deluj globalno«. Prenos mednarodnih dobrih praks in vključevanje v mednarodne raziskovalne projekte in študije je po naši oceni nujni pogoj za razvoj in uvajanje novih sodobnih rešitev v sisteme obvladovanja tveganj na korporativnem nivoju. Zavedamo se namreč preprostega dejstva, da se morajo lokalni trgi vse bolj odpirati globalnim ponudnikom, lokalni ponudniki pa prilagajati svoje delovanje globalnim potrebam in konkurentom. S tega vidika morajo organizacije v svoje poslovne procese uvajati filozofijo korporativne varnosti in obvladovati tveganja s sodobnimi orodji in pristopi na vseh ravneh delovanja organizacije. To filozofijo smo upoštevali tudi pri razvoju in pripravi našega magistrskega programa »Menedžment korporativne varnosti«, ki ga nameravamo izvajati tudi v mednarodnem okolju in s tem zagotoviti prenos znanj in dobrih praks tudi na področju izobraževanja. ICS se poleg navedenega vse bolj vključuje tudi v mednarodne raziskovalne projekte financirane s strani različnih evropskih inštitucij in na ta način razvijati nove rešitve na različnih področjih korporativne varnosti.

Izvajate tudi svetovalne projekte, kjer so vaši uporabniki predvsem gospodarski subjekti. V tem okviru ste razvili nekaj novih produktov, ki v našem prostoru veljajo za popolnoma novi pristop. Nam lahko navedete nekaj primerov tega sodelovanja?

Vršec: Naš najbolj udaren produkt, če lahko temu tako rečem, je izdelava varnostnih elaboratov in študij na podlagi katerih naročnikom s pomočjo lastne metodologije pomagamo prepoznati stopnjo ranljivosti, ogroženosti in varnostnih tveganj, jim analizirati varnostno okolje in tveganja ter jim pripraviti strokovne podlage za vzpostavitve integralnega varnostnega sistema, ki na celovit način zaznava in obvladuje tveganja, ki se pojavljajo v poslovnem procesu organizacije. Ob tej priliki bi rad izpostavil tudi izvajanje izobraževanj po naročilu s katerim zaposlenim v posameznih organizacijah plasiramo potrebna znanja za dvig njihove varnostne kulture in zavesti, s tem pa posredno vzpostavimo optimalne samovarovalne mehanizme, s katerimi zaposleni s svojim preventivnim delovanjem že v osnovi obvladujejo večino varnostnih tveganj, ki se pojavljajo v posameznih fazah poslovnega procesa. V fazi razvoja imamo tudi storitve nadzora nad delovanjem varnostnih sistemov vzpostavljenih v posameznih organizacijah, ki bodo zaradi svoje specifične metodologije in izvedbe zagotavljale ključne informacije o delovanju varnostnih sistemov ter pripomogle k uvajanju stalnih izboljšav v sisteme varovanja s tem pa tudi optimalnejšemu obvladovanju tveganj.

Katera področja bodo po vašem mnenju v bodoče potrebna podrobnejše strokovne in vsebinske obravnave predvsem če razmišljamo z vidika normativne in vsebinske ureditve, z vidika ustvarjanja novih dodanih vrednosti in tudi z vidika celovitejšega obvladovanja tveganj na operativnem in strateškem (nacionalnem) nivoju ?

Vršec: Po moji oceni bo potrebno v bodoče še več pozornosti posvečati optimizaciji finančnih vložkov v sisteme obvladovanja tveganj po metodi »Cost/Benifit«, tako z ekonomskega, kot tudi strokovnega vidika. Vsekakor bo potrebno pri izgradnji oziroma posodobitvah varnostnih sistemov vse bolj upoštevati globalne vidike ogroženosti in njihov vpliv na delovanje organizacij v lokalnem in globalnem okolju. Pri tem si lahko pomagamo z uvajanjem sodobnih menedžerskih orodij in standardov upravljanja in obvladovanja tveganj na vseh ravneh organizacije. Potrebno bo tudi urediti status varnostnega menedžmenta v sleherni organizaciji, ter določiti jasna merila za ocenjevanje stopnje tveganj in ukrepe za njihovo obvladovanje. Dejstvo je namreč, da sistemsko obvladovanje tveganj na korporativnem nivoju organizacijam prinaša konkurenčne prednosti in zanesljivejše delovanje poslovnih procesov, kar posredno vpliva tudi na dobro ime in status blagovne znamke na trgu. Skladno z zahtevami evropske unije bo potrebno urediti obvladovanje tveganj v subjektih, ki so del kritične infrastrukture ter poenotiti zakonodajo v delu, ki tako ali drugače nalaga organizacijam urejanje in obvladovanje različnih vrst tveganj. Ključno pri vsem tem pa je, da se prenovijo dodiplomski in podiplomski izobraževalni programi ter vzpostavijo pogoji za realno zaposljivost novo nastajajočih korporativnih varnostnih managerjev tako v javnem, kot tudi v zasebnem sektorju. ■

Avtor: Doc. dr. Milan Vršec / Inštitut za korporativne varnostne študije-ICS*



VLOGA KORPORATIVNE VARNOSTI

Ob izidu prve številke revije »Korporativna varnost« je umestno, da opredelimo vlogo korporativne varnosti v procesih korporativnega upravljanja gospodarskih in drugih subjektov. Gre za fenomen varnosti v industriji in gospodarstvu kjer se ustvarja nova vrednost na bazi upravljanja poslovnih procesov, sredstev, kapitala, informacij, komunikacij in človeških virov.

Upravljanje vsega tega uspešno funkcionira le, če je dosledno uvedena tudi funkcija upravljanja varnosti v najširšem, torej korporativnem smislu. V bistvu gre za upravljaje izrednih dogodkov v preventivnem in represivnem (odzivnem) pogledu. Izredni dogodki večjega in velikega obsega zagotovo vnesejo v vsakodnevno relativno mirno delo, obratovanje, poslovanje in življenje nemir, preplah, strah, negotovost, tveganje, ali celo šok, paniko, grozo in obup. Situacija je toliko hujša, če državne institucije, gospodarske družbe in civilne organizacije niso na kaj takega pripravljene. Med izredne dogodke velikih razsežnosti in posledic uvrščamo: potrese, povodnji, orkane, tornade, ciklone, viharje, obilne padavine, letalske, rudniške, železniške, delovne in cestnoprometne nesreče, večje vlome, roparske napade, teroristična dejanja, »električne mrke«, razlitja nevarnih snovi v morje, vodovje ali v zemljo (ogrožanje podtalnice), velike gozdne požare in požare ter eksplozije na industrijskih objektih in objektih z velikim številom ljudi (poslovne zgradbe, kinodvorane, gostinski lokali, hoteli, gledališča, športna igrišča, vlaki, avtobusi), itd. Posledice vsakega izrednega dogodka so praviloma neugodne, ker se izražajo v materialni, finančni, poslovni, človeški in moralni škodi in hkrati izgubi. Če so materialne, finančne, poslovne, obratovalne (proizvodne) in človeške posledice šokantne, opredelimo tak dogodek kot havarijo oziroma katastrofo za prizadete organizacije in ljudi. Vsak izredni dogodek velikega obsega je treba razreševati po načrtih varovanja, načrtih evakuacije ter kriznih načrtih oziroma načrtih odzivanja na katastrofe. Če državni, gospodarski ali civilni subjekti ne dajejo dovolj pozornosti na celovito obvladovanje tveganj in sprememb in hkrati na varnostne in nadzorne mehanizme je večja ali manjša verjetnost, da bo kaj ušlo nadzoru in da se bo zagotovo v nekem preseku časa zgodilo kaj šokantnega. Zato je treba na eni strani imeti pregled nad viri in vzroki izrednih dogodkov (ocena ogroženosti in tveganj), na drugi strani pa pregled nad realnimi, potencialnimi in prikritimi posledicami, torej nad neposrednimi in stranskimi škodami in izgubami zaradi izrednih dogodkov. Na tej točki se prične razvijati sodobna paradigma o upravljanju korporativne varnosti, ki je v tuji literaturi kar solidno obdelana. Tako bo potrebno tudi pri nas intenzivneje proučevati, raziskovati in razvijati vse segmente korporativne varnosti, kar je ena od poglavitnih usmeritev Inštituta za korporativne varnostne študije in Slovenskega združenja korporativne varnosti.

Integralna in integrirana varnost, varnostna politika

Korporativna varnost temelji na dveh prepoznavnih karakteristikah. To sta integralna (celovita) varnost ter integrirana (notranje povezana) varnost. Integralna varnost je skupek vseh relevantnih varnostnih področij v družbi, ki so: varstvo pred naravnimi in drugimi nesrečami, varstvo pred industrijskimi nesrečami, varstvo pred požari, varstvo okolja (zemlje, zraka, vode), zaščita in reševanje (CZ), varnost in zdravje pri delu, varstvo osebnih in tajnih podatkov, varovanje informacijskih sistemov, varovanje intelektualne lastnine in poslovnih skrivnosti, varovanje arhivov, fizično in tehnično varovanje ljudi in premoženja ter varovanje ugleda in konkurenčnih prednosti (z uporabo poslovnih orodij kot sta benchmarking in business intelligence). V sklopu celovite varnosti pa se mora razviti integrirana varnost, to je povezanost med posameznimi (prej omenjenimi) var-

*avtor je član Slovenskega združenja korporativne varnosti



nostnimi področju, ki morajo biti vpeta v sistem vodenja kakovosti po ISO 9001:2008. To mora biti razvidno iz krovne varnostne politike in izvedenih varnostnih politik ter iz notranjih aktov - pravilnikov, navodil, načrtov, organizacijskih predpisov in poslovnikov kakovosti. Za implementacijo teh dokumentov mora poskrbeti management organizacijskih enot, varnostni management in službe, ki upravljajo s človeškimi viri.

Ranljivost, ogroženost, varnostna tveganja, varnostni sistem

Temeljni motivi za upravljanje korporativne varnosti so ranljivost in ogroženost premoženja, kapitala, vrednot in osebja ter iz tega izvirajoča varnostna in druga tveganja. Tu je še zakonodaja, ki določa pravila igre pri vzpostavljanju učinkovitih varnostnih in nadzornih mehanizmov. Vsaka korporacija, koncern, poslovni sistem in gospodarska družba je ranljiva zaradi številnih slabosti in vrzeli v poslovnih procesih ter v nadzornih in varnostnih mehanizmih, kar povzroča nesreče in olajša dostop za kriminalne, teroristične in druge napade. Poleg tega se gospodarski subjekti soočajo s konkretnimi grožnjami in izrednimi dogodki, ki jih je treba - s pomočjo zgodnjega opozorilnega sistema - zaznati in preprečiti, v primeru nastanka pa učinkovito razrešiti posledice in vzpostaviti poslovne procese v prvotno (normalno) stanje. Gre torej za obvladovanje varnostnih tveganj, ki so največkrat sestavni del poslovnih, finančnih, ekonomskih, tržnih, logističnih in drugih tveganj. Kajti obvladovanje varnostnih tveganj je sestavni del doseganja visoke ravni korporacijske odgovornosti. To še posebej velja za gospodarske družbe, poslovne sisteme, in podjetja, ki predstavljajo evropsko in nacionalno kritično infrastrukturo – energetika, transport, zdravstvo, prehrana, voda, telekomunikacije, bančništvo idr. Zato je organiziranost varnostnih sistemov zlasti v sektorjih kritične infrastrukture pokazatelj nivoja kakovosti in učinkovitosti korporativne varnosti. V proces upravljanja in obvladovanja tveganj pa je nujno razviti tudi ustrezni zavarovalni portfelj z zavarovalnicami, ki uravnoteži stroške, škode in izgube kot posledice izrednih dogodkov.

Upravljanje tveganj nastanka izrednih dogodkov pa je ena od sodobnih korporacijskih funkcij, s katero se morajo ukvarjati lastniki, upravljavci, management, nadzorniki in projektni managerji.

Varnostni management, varnostni standardi

Varnostni management je glavni upravljavec korporativne varnosti. Začne se s krovnim varnostnim managerjem, ki je neposredno odgovoren vodstvu organizacije in je v bistvu predstavnik vodstva za korporativno varnost. Na srednji in operativni ravni sledijo varnostni managerji odgovorni za posamezna varnostna področja ter za varnostno operativo (fizično in tehnično varovanje, odzivanje na alarmne situacije itd.). Zlasti v sektorjih kritične infrastrukture mora varnostni management imeti posebno vlogo, kompetence in odgovornost v oblikovanju varnostnih politik, varnostnih sistemov in varnostnih režimov na varovanih območjih gospodarskih in drugih subjektov. Varnostni management je potemtakem omembe vreden človeški vir, ki mora imeti besedo na top ravni upravljanja, vodenja in odločanja. Lastniki, upravljavci in nadzorniki se namreč morajo zavedati, da je varnostni managemnent kompetenten in usposobljen za upravljanje korporativne varnosti. Tako mora varnostni management –



ob podpori vodstva - poskrbeti tudi za upravljanje korporativne varnosti v kriznih okoliščinah in v tem okviru tudi za neprekinjeno delovanje varnostnega sistema; in sicer po konceptu standarda BS 25999 in ISO/IEC 27000. Prav tako mora varnostni management poskrbeti za uvajanje nacionalnih in evropskih varnostnih standardov kot so SIST BS 5979, ISO 14001+EMAS, OHSAS 18001, HACCP in mnogih drugih varnostnih standardov, ki krojijo kakovost integralnih varnostnih sistemov.

Sklepna beseda

Inštitut za korporativne varnostne študije, v njegovi sestavi pa tudi Slovensko združenje korporativne varnosti, postajata prepoznavna v nacionalnem in mednarodnem okolju. Postopno večanje članstva združenja, vsakoletne mednarodne konference, mesečni nacionalni strokovni posveti na aktualne teme, publiciranje knjižnih del, soustanavljanje mednarodnih sorodnih institucij ter izgradnja mreže nacionalnih in mednarodnih povezav, daje inštitutu in združenju realno osnovo, da postavlja merila za raziskave in za razvoj korporativne varnosti v sektorjih kritične infrastrukture in v širšem gospodarstvu. Krizno stanje ne sme biti ovira temveč vzpodbuda za izboljšanje varnostnih in nadzornih mehanizmov v procesih korporativnega upravljanja. ■



Avtor: Denis Čaleta / Inštitut za korporativne varnostne študije-ICS, Ljubljana*

INTERVJU
g. Andrej Podvršič
Director of Security, Du Pont International of Europe, Middle East & Africa

OBVLADOVANJE TVEGANJ SKOZI PERSPEKTIVO MEDNARODNEGA KORPORATIVNEGA OKOLJA

Uspešen korporativni varnostni manager potrebuje znanja s področja razumevanja in obvladovanja varnostnih tveganj, obenem pa je enako pomembno razumevanje in poznavanja »businessa«.

Trenutno opravljate zelo pomembno funkcijo korporativno varnostnega managerja v svetovni multinacionalni korporaciji DuPont de Nemours International Sars. Prosim, če kratko opredelite kaj vse spada v obseg vaše odgovornosti.

V našem podjetju, ki ima svoje sedež za Evropo, Bližnji vzhod in Afriko v Ženevi, sem Direktor varnosti za omenjeno regijo od leta 2004. V moji pristojnosti je varnost zaposlenih, proizvodnje in drugih dejavnosti ter zaščita informacij. Za ilustracijo naj povem, da smo globalna korporacija s približno 70 000 zaposlenimi in delujemo v več kot 90 državah. V regiji, ki je v moji pristojnosti, pa je zaposleno več kot 18 000 ljudi in prisotni smo v več kot 40 državah - od Karačija v Pakistanu do Cape Towna v Južni Afriki. Prihodek v letu 2011 je znašal 38 milijard US $. Sorazmerni s temi dimenzijami so tudi varnostni izzivi, s katerimi se dnevno soočamo. V zadnjih letih ogromno časa posvečamo varovanju intelektualne lastnine, kriznemu menedžmentu, varnostni oceni naših tržišč in pa predvsem osebni varnosti naših zaposlenih. Varnostno osveščanje in usposabljanje naših zaposlenih je ena izmed glavnih prioritet, saj s tem vnašamo varnostno kulturo in zavest v vse nivoje korporacije. Dandanes je lahko le varnostno osveščena korporacija ali organizacija uspešna na konkurenčnem trgu in še posebno v teh težkih, nepredvidljivih časih.

Varnostno osveščanje in usposabljanje naših zaposlenih je ena izmed glavnih prioritet, saj s tem vnašamo varnostno kulturo in zavest v vse nivoje korporacije.

Je celovit pristop do obvladovanja tveganj po vaši oceni nujno potreben za učinkovito poslovanje organizacije?

Dandanes je izredno težko uspešno poslovati na globalni sceni brez obladovanje vseh mogočih rizikov, vključno z varnostnimi tveganji. Ti postajajo ključni element strateških odločitev na najvišjih nivojih korporativnega managmenta. Varnostna situacija širom po svetu se na žalost ne izboljšuje, ravno nasprotno. Laična in strokovna javnost se soočata s poplavo informacij o raznih kriznih dogajanjih iz vseh koncev sveta. Pravilno razumevanje in objektivna ocena varnostnih tveganj je za korporacije ključnega pomena. Le tako lahko pripravimo ustrezne ukrepe za obladovanje teh varnostnih tveganj in s tem zmanjšamo riziko, s katerim se korporacija sooča. Na tej

*avtor je član Slovenskega združenja korporativne varnosti



podlagi se nato sprejemajo tako pomembne strateške odločitve kot so na primer vstop na nerazviti trg, lansiranje novih proizvodov, kakor tudi enostavne, dnevne odločitve kot so sklepanje pogodb s poslovnimi partnerji v bolj rizičnih delih sveta.

Že v nacionalnem okolju ste opravili celo vrsto strateško pomembnih funkcij, med drugim ste bili Svetovalec za varnost Predsednika Vlade, Generalni direktor Slovenske policije, Slovenski konzul v ZDA, bil pa ste tudi prvi slovenski diplomant na akademiji FBI v ZDA. So ta znanja nudila zadostno podlago za učinkovito delo korporativno varnostnega managerja v svetovni korporaciji?

Brez dvoma so mi pridobljena znanja in pa izkušnje, ki sem jih pridobil z opravljanjem teh funkcij zelo pomagala, ko sem konkuriral za to delovno mesto. Kot vsak drug poklic, čeprav bi to raje opisal kot poslanstvo, zahteva tudi naše delovno področje nenehno izobraževanje in usposabljanje. Priča smo bliskovitemu razvoju na vseh področjih. Žal pa se tega napredka poslužuje tudi »nasprotna stran«, na primer pri industrijski špijonaži. Zato se mora vsak varnostni manager redno izpopolnjevati in usposabljati, kajti le tako je lahko uspešen pri svojem delu. Pomemben je tudi »networking« in ravno zato so združenja kot je Slovensko združenje korporativne varnosti in European Institut of Corporate Security Management, pomembna na področju izobraževanja in pridobivanju ter izmenjave izkušenj.

Prosim vas, če nam lahko podrobneje predstavite umeščenost korporativne varnosti v izvajanje celovitih procesov mednarodne korporacije DuPont.

Organizacijsko se korporativna varnost v DuPontu umešča v Pravni oddelek in »Chief Security Officer«, ki je korporativni varnostni direktor za celotni DuPont, administrativno odgovarja »Senior VP - General Councel«, funkcionalno pa direktno CEO. Kot regionalni direktor administrativno odgovarjam »General Councel«, funcionalno pa »Chief Security Officer«. Sama organizacijska umeščenost in linijska odgovornost sta pomembni, saj to omogoča dostop do managerjev, ki sprejemajo ključne odločitve.
Seveda pa sama organizacijska umeščenost in linijska odgovornost sama po sebi nista zadosti. Vsak varnostni manager mora tudi razumeti kako korporacija funcionira in posluje. DuPont je zelo raznolika korporacija z vsestranskim porfeljem in lahko samo povem, da se po 9 letih še vedno učim in spoznavam naše podjetje. Uspešen korporativni varnostni manager postaneš le, če si lahko predstaviš zamišljene varnostne ukrepe v luči »Return of Investement« (povračilo vloženih sredstev). To je govorica argumentov in številk, zato pogosto poudarjam, da sodi v opis del in nalog korporativnega varnostnega menedžerja tudi delo »sales and marketing«, saj moraš svoje zamisli ustrezno »prodati« potencialnemu internemu »kupcu« storitev. V številnih podjetjih se korporativna varnost tretira kot strošek, medtem ko jo mi promoviramo kot srednjeročno in dolgoročno investicijo, ki se lahko obrestuje v povečanem dobičku. Kot primer lahko navedem uspešen pregon ponarejevalcev naših proizvodov, kar se nam posledično povrne v povečanem tržnem deležu in seveda dobičku.

Kako so po vašem mnenju pomembne ključne informacije korporacije v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču. Ali temu področju v DuPontu namenjate veliko pozornosti?

Varnostne informacije in njihova realna ocena so ključnega pomena v vsaki korporaciji in organizaciji. Kot sem že omenil, nam razumevanje varnostnih trendov omogoča optimizacijo naših resursov in pomaga pri pomembnih dolgoročnih in kratkoročnih odločitvah. Proces ocene varnostnih tveganj poteka dnevno in to lahko opravljamo samo s kvalitetnimi informacijami, zato se poslužujemo zunanjih partnerjev, ki so specializirani za tovrstno dejavnost.



Verjetno še vedno redno spremljate stanje na področju korporativne varnosti v slovenskem okolju. Kako bi ocenili zavedanje strateškega managementa v slovenskih podjetjih o pomenu korporativne varnosti in učinkovitega obvladovanja tveganj?

Po resnici povedano, sem do nedavnega spremljal bolj z daljave, ker žal v preteklosti nisem imel toliko stika s slovenskimi kolegi. To se je spremenilo pred kratkim, saj sem postal član Slovenskega združenja korporativne varnosti in tudi marčevska konferenca mi je omogočila srečanje s številnimi kolegi, kar je samo po sebi potrditev, da se tudi naša podjetja prebujajo in začenjajo razumeti pomen korporativne varnosti. Sam na zadevo gledam sirše in sicer v smislu priložnosti. Slovenija je še vedno zelo varna država in to je vrednota, ki jo mednarodne korporacije in organizacije zelo cenijo. Ženeva je sedež številnih mednarodnih korporacij in organizacij in ocenjujem, da bi tudi Slovenija s svojo geopolitično situacijo, ustrezno davčno stimulativno politiko in relativno nizkimi fiksnimi stroški ter ugodnimi varnostnimi razmerami, lahko privabila številne mednarodne korporacije in organizacije.

Kaj bi svetoval kako izboljšati stanje splošnega zavedanja o pomenu učinkovitega obvladovanja tveganj?

Varnost postaja dandanes privilegij in v Sloveniji smo deležni tega v veliki meri, ker ocenjujem, da je naša država še vedno zelo varna. Osebno menim, da je prihodnost v partnerstvu med javnim sektorjem zagotavljanja varnosti in zasebnim, tudi korporativnim varnostnim sektorjem. Popolnoma se zavedam, da oba sektorja delujeta na različnih ekonomskih principih, vendar bo čas pokazal, da je ta simbioza nujno potrebna za uspešno obladovanje varnostnih tveganj. S tem bomo tudi pripomogli k splošnemu osveščanju in vrednotenju varnosti. Potrebno bo le določiti pravila igre, saj vsi na koncu stremimo k istemu cilju in sicer da se davkoplačevalci počutijo varni.
Pri tem vidim pomembno vlogo profesionalnih združenj kot je na primer Slovensko združenje korporativne varnosti, ki omogoča svojim članom izmenjavo izkušenj in promovira varnost kot eno izmed temeljnih vrednot današnje družbe.

Institut za korporativno varnostne študije-ICS izvaja pomembne aktivnosti na področju ozaveščanja vodilnega managementa o pomenu obvladovanja tveganj, kot predpogoja za učinkovito delovanje organizacij. Kako vi osebno ocenjujete te aktivnosti?

Osebno pozdravljam delovanje Inštituta za korporativne varnostne študije, saj je za ozaveščanje vodilnega managementa potreben organiziran in argumentiran pristop, katerega pa korporativni menedžerji sami ne zmoremo in tu omenjeni Inštitut igra pomembno vlogo, če ne celo ključno.

V zaključni fazi je tudi podiplomski magistrski program »management korporativne varnosti«, ki ga v soorganizaciji pripravljata Institut za korporativne varnostne študije-ICS in GEA College-Fakulteta za podjetništvo. Menite, da je to prava pot za upravljanje stroke in predvsem za izobraževanje strokovnjakov s področja korporativne varnosti v Republiki Sloveniji in tudi širše v regiji?

V zadnjem času je veliko diskusije kakšna znanja in izkušnje potrebuje uspešen korporativni varnostni manager in menim, da omenjeni magistrski študij z opravljanjem prakse v korporacijah ponuja pravi odgovor. Uspešen korporativni varnostni manager potrebuje znanja s področja razumevanja in obladovanja varnostnih tveganj, obenem pa je enako pomembno razumevanje in poznavanja »businessa«. Kombinacija teh znanj, prakse in dobrega »networka« je odgovor, ki ga iščemo in ga po mojem mnenju, ta študij tudi ponuja. Z zanimanjem bom spremljal razvoj tega projekta in želim obilo uspeha, saj je potreba po tovrstnem kadru čedalje večja in brez dvoma bodo tudi druge korporacije več kot zainteresirane. ■

Novi magistrski program 2. stopnje

MANAGEMENT KORPORATIVNE VARNOSTI

geacollege
Fakulteta za podjetništvo

ICS
Institut za korporativne varnostne študije

»Študij, ki je privlačen, koristen in vam lahko spremeni življenje«

- predavanja bodo skrbno izvajali največji strokovnjaki na področju korporativne varnosti
- veliko število gostujočih predavateljev, ter s tem zagotavljanje implementacije praktičnih spoznanj v izobraževalni proces
- sodelovanja v aktivnostih Slovenskega združenja korporativne varnosti (konference, posveti in neposredni obiski različnih organizacijskih okolij)
- visoko zaposljivost naših študentov v nacionalnem in mednarodnem okolju
- neposredna podpora pri zagotavljanju službe najboljšim študentom
- za najbolj uspešne študente zagotovitev izvajanja neposredne prakse v okolju mednarodnih korporacij
- širok nabor znanja tudi za delo na različnih nivojih korporativnega upravljanja

PRIHODNOST PRIPADA PODJETNIM!

Vzemi usodo v svoje roke in ustrezno obvladuj tveganja v svoji poslovni karieri!

GEA COLLEGE
Tel.: +386 1 5881 300
E-naslov: podiplomski@geacollege.si
www.gea-college.si

ICS Ljubljana
Tel.: +386 31 312 819
E-naslov: info@ics-institut.si
www.ics-institut.si

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije-ICS*

INTERVJU
g. Domen Pirkmajer,
korporativno varnostni manager, TE-TOL

KORPORATIVNO VARNOSTNI MANAGER LETA 2011

Slabo plačano varnostno osebje predstavlja resno grožnjo varnostnemu sistemu podjetja, ki ga varuje. Tega dejstva bi se moral zavedati vsak naročnik!

Svoje delo izvajate kot korporativno varnostni manager v Termoelektrarni Toplarni Ljubljana (TE-TOL). Nam lahko poveste katera so ključna področja vaših pristojnosti?
Področja, za katera sem, kot vodja službe za varnostni sistem pristojen in odgovoren (na to besedo radi pozabimo), so predvsem: fizično varovanje, tehnično varovanje, varovanje tajnih podatkov in organizacija ter delovanje civilne zaščite. Seveda se spogledujem tudi z informacijsko varnostjo podjetja, ekološko varnostjo, zaščito poslovnih skrivnosti in osebnih podatkov, vendar ta področja varnosti niso neposredno v moji pristojnosti, zato ne moremo govoriti o korporativnem varnostnem managiranju, ki ima vsa področja varnosti pod eno streho.

TE-TOL predstavlja del kritične infrastrukture na področju energetskega sektorja. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?
Zakaj je proizvodnja električne energije in toplote umeščena v kritični infrastrukturni podsektor, ni potrebno razlagati. Kompleksnost in razvoj družbe naraščata, kar se odraža tudi na povečevanju prepletenosti in povezanosti kritične infrastrukture. Lahko rečemo, da so sektorji kritične infrastrukture kritično soodvisni: denimo, bančni sistemi in informacijski sistemi ne morejo delovati, če ne delujejo energetski sistemi, transportni sistemi ne morejo delovati, če ne delujejo informacijski sistemi ... Vse večja soodvisnost infrastrukturnih sektorjev pomeni večjo ranljivost kritične infrastrukture kot celote, kar posledično pomeni ranljivost družbe.



Dejstvo je, da se je o kritični infrastrukturi na konceptualni in operativni ravni začelo govoriti predvsem v luči terorističnega ogrožanja. Zadnji, večji teroristični napadi v New Yorku, Madridu in Londonu, so imeli za tarčo objekte kritične infrastrukture. Vemo pa, da grožnje kritični infrastrukturi predstavljajo tudi in predvsem napake, ki so posledica pomanjkljivosti v sistemu in so posledica notranjih vzrokov ter nesreče, ki se navadno zgodijo zunaj proučevanih ali prizadetih sis-

Zaradi prej omenjene soodvisnosti pa se je potrebno zavedati, da se kljub normalnemu poslovanju TE-TOL lahko zgodi, da državljani ostanejo brez toplotne ali električne energije, če pride do razpada distribucijskih omrežij, katerih upravljalec ni TE-TOL.
Zato pogrešam aktivnejšo vlogo države, ki bi morala poskrbeti vsaj za smernice pri zaščiti kritične infrastrukture, predvsem pa za celovit in usklajen pristop v vseh kritičnih infrastrukturnih sektorjih.

*avtor je član Slovenskega združenja korporativne varnosti

temov. Vendar te grožnje so obstajale tudi pred omenjenimi terorističnimi napadi. Zdrava podjetja, ki se zavedajo pomembnosti zanesljivosti delovanja primarnega procesa, so te grožnje prepoznala, jih identificirala in se nanje ustrezno odzvala. Na ta način so povečala sposobnost preživetja.Verjamem, da je med njimi tudi TE-TOL.
Seveda so koraki za obvladovanje tveganj zelo kompleksni, trajajo več let ter zahtevajo veliko truda in poguma. V grobem obsegajo aktivnosti za zaščito podjetja pred dejanskimi, potencialnimi in prikritimi grožnjami. To so varnostne politike, varnostni koncepti, varnostni elaborati, strategije, preprečevanje destabilizacijskih pojavov (motnje, nesreče, napadi) in odziv, ko se ti pojavijo. Tu gre za ocenjevanje tveganj in groženj, načrtovanje, usposabljanje, vzpostavitev mehanizmov za odločanje v kriznih razmerah, vzpostavitev in vzdrževanje informacijskih, varnostnih, logističnih in drugih podpornih sistemov, dvigovanje ravni organizacijske in varnostne kulture med zaposlenimi ...



Je po vašem mnenju zavedanje o pomenu učinkovitega obvladovanja tveganj dovolj prisotno pri strateškem managementu organizacij?
Ko se ozremo na pogorišče vseh propadlih podjetij in če je bistvo varnostnega sistema podjetja, da zagotavlja zanesljivo in neprekinjeno delovanje primarnega procesa, lahko rečemo, da so ta podjetja propadla, ker je odpovedal njihov varnostni sistem. Očitno, se strateški management ni zavedal pomena celovitega obvladovanja tveganj. Glede na število podanih kazenskih ovadb pa je v kar nekaterih propadlih podjetjih ravno strateški management predstavljal največje varnostno tveganje.

Je vlaganje v izobraževanje kadrovskih potencialov organizacij lahko tista potrebna kvaliteta, ki tudi na področju varnostnega zavedanja, loči uspešna podjetja od povprečnih?
Izobraževanje in usposabljanje zaposlenih na področju varnosti je tako, kot na vseh ostalih področjih, danes bolj potrebno, kot kdaj koli prej. Razmah in razvoj informacijske tehnologije sta za seboj potegnila vrsto novih varnostnih tveganj, ki se jih zaposleni ne zavedajo. Če k temu dodamo še ravnanje s tajnimi podatki, osebnimi podatki in poslovnimi skrivnostmi, je tveganje, da bo šlo tu kaj narobe,še večje.Ko pa k temu priključimo še varstvo pred požarom, okoljsko varstvo in varstvo pri delu, vidimo, da se zaposleni znajde v zelo negotovem položaju, če organizacija ne poskrbi za njegovo usposabljanje tudi na teh področjih. V praksi se pogosto dogaja, da delodajalec uvede vrsto internih aktov, zaposlene pa prepusti subjektivni razlagi napisanih določil. To privede do improvizacije izvajanja teh določil, negativnega odnosa zaposlenih do začrtanih varnostnih izboljšav in stresa. Če s primerom razumevanje težave poenostavim in situacijo preslikam na prodajalca in kupca, izpade to približno takole; ko kupimo nov gospodinjski aparat, vrtno kosilnico ali avto, pričakujemo, da bodo zraven priložena navodila za pravilno, učinkovito in varno uporabo kupljenega izdelka. Če navodil ni priloženih ali če niso napisana v slovenskem jeziku, se jezni odpravimo k prodajalcu in le to od njega zahtevamo. Iz tega izhaja, da je izobraževanje in usposabljanje tudi pravica in ne samo dolžnost, ki je zaposlenemu pogosto odvzeta. Če zadevo pogledamo z vidika prodajalca, vidimo, da je tudi njemu v interesu, da navodila za pravilno, učinkovito in varno uporabo priloži izdelku. Tako se izogne jeznim kupcem, ki se po navodila vračajo. Ob pravilni uporabi izdelka je delo z novo napravo enostavno in učinkovito, o tem pa bodo uporabniki veselo pisali na forumih. Priložena navodila o varnem ravnanju z napravo bodo posledično privedla do zmanjšanja delovnih nesreč in posledično tudi do zmanjšanja števila tožb. Logika je zelo enostavna, kljub temu pa je v marsikaterem podjetju področje izobraževanja in usposabljanja odrinjeno na stranski tir. Pomanjkanje denarnih sredstev je v zadnjem času priročen izgovor za neodgovorne delodajalce, a jih to ne opravičuje. Lahko bi organizirali interna usposabljanja, ki so ob pravilni pripravi in izvedbi lahko celo bolj učinkovita od eksternih, saj so naravnana na konkretno delovno okolje, v katerem zaposleni delujejo, vzpostavi pa se tudi bolj pristen odnos med odgovornimi in zaposlenimi. Podjetja, ki svoje zaposlene cenijo in se zavedajo pomena izobraževanja in usposabljanja, so na pravi poti, ki dviguje nivo organizacijske in varnostne kulture med zaposlenimi ter predstavlja za podjetje konkurenčno prednost.

Kako pristopate k zagotavljanju fizičnega in tehničnega sistema varovanja glede na pomanjkanje kadrovskega potenciala. Nam lahko v grobem predstavite vaš model izbire zunanjih izvajalcev za določen segment fizičnega varovanja, ki v Republiki Sloveniji vsekakor velja za primer dobre prakse, vloge naročnika kot dobrega gospodarja, ki za svoj vložek dobi ustrezen nivo varnostne usluge.
Kot vsaka storitev, se tudi storitve fizičnega varovanja ponujajo na trgu varnostnih storitev. Tisti, ki se z varnostjo profesionalno ukvarjamo, se »krvne slike« zasebnega varovanja, ki kaže na slab ugled panoge v javnosti, na nezakonito izvajanje nosilcev licenc in na nizko tržno vrednost poklica, še kako zavedamo. Vendar, če velja, da se ponudba izoblikuje na podlagi povpra-



ševanja, moramo naročniki varnostnih storitev velik del krivde za takšno stanje pripisati sebi.
Slabo, če sploh, plačano varnostno osebje predstavlja resno grožnjo varnostnemu sistemu podjetja, ki ga varuje. Tega dejstva bi se moral zavedati vsak naročnik!
Torej, če je grožnja identificirana, jo je potrebno obravnavati in se nanj ustrezno odzvati. Moj odziv je bil v postavitvi modela, ki zagotavlja socialno varnost in ustrezne delovne pogoje najetemu varnostnemu osebju. Strah, da bo zaradi tega ponudbena cena višja, je bil odveč, saj se je v našem primeru cena celo znižala.
Model postavlja ceno kot vrednoteni pogoj v razmerje. Glede na obseg in zahtevnost pogodbenih del smo v TE-TOL to razmerje postavili 60:40. Od stotih možnih točk prinese najnižja ponudbena cena 60 točk, najvišja plača varnostnika pa 40 točk. V našem primeru so bile štiri različne plače za štiri različno zahtevna delovna mesta, ki so vsaka prinesle največ 10 točk. Model se lahko prilagaja glede na specifiko potreb naročnika varnostnih storitev. Bistveno je, da določimo minimalno možno ponujeno plačo in jasno navedemo, kaj je v tej plači zajeto. Tako se izognemo raznim akrobacijam in sprenevedanjem, ko je treba izbranemu ponudniku plače nakazati varnostnemu osebju. Seveda pa je potrebno v samem razpisu enako skrb posvetiti ostalim zahtevam, ki jih dosežemo s postavitvijo obveznih in prednostnih pogojev. Model nam omogoča, da nadzorujemo komponento, na katero do sedaj nismo imeli vpliva, je pa bistvena za kakovostno izvajanje varnostnih nalog. To so plače najetega varnostnega osebja. S tem najetemu varnostnemu osebju pokažemo, da nam ni vseeno za njihov socialni položaj, da cenimo njihovo delo in da so pomemben del v verigi varnostnega sistema, kateremu pripadajo. Vse to se nam obrestuje v motiviranosti in samoiniciativnosti varnostnega osebja pri delu. Predvsem pa s tem pridobimo pripadnost varnostnega osebja do podjetja, ki ga varuje. Zgodi se, da je varnostnik bolj pripaden podjetju ki ga varuje, kot svojemu delodajalcu. Cena? Manj dobička za delodajalca, višje plače varnostnega osebja in dvig kvalitete varnostnih storitev za naročnika.

Ste tudi eden od ustanovnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s področja korporativne varnosti potrebna in lahko prinesejo v naš prostor dodatno kvaliteto, ki smo jo predvsem na strani naročnikov močno pogrešali?
Menim, da je vsako združevanje ljudi, ki jih vežejo enaki interesi, dobro. Pravzaprav je za človeka kot socialno bitje to naravno in samo po sebi umevno. Tako je tudi slovensko združenje korporativne varnosti združilo ljudi z enakimi oziroma podobnimi interesi. Časi, v katerih živimo in evolucija varnostnih groženj postavljajo pred korporativne varnostne managerje in ljudi, ki se z varnostjo profesionalno ukvarjamo, vse večje in zahtevnejše izzive.
Eksplozija varnostnih groženj na eni strani in zmanjševanje varnostnih proračunov na drugi, sta dejstvi, kateri od varnostnega managerja zahtevata veliko znanja, prilagodljivosti in inovativni pristop, da bo sposoben zagotoviti zadovoljiv nivo varnosti. Prav tu vidim bistvo delovanja slovenskega združenja korporativne varnosti. Paleta strokovnjakov, ki prihaja iz različnih delovnih okolij in obvladuje različna področja varnosti, je iz meseca v mesec bolj pisana. V njej se skriva ogromno znanja, dobrih praks in inovativnih pristopov, ki so jih člani pripravljeni deliti z ostalimi.Verjamem, da je združenje s svojim aktivnim delovanjem prineslo dodano vrednost v vsa podjetja in organizacije, iz katerih prihajajo naši člani.

V letu 2011 vam je pripadel prestižni naziv »korporativno varnostnega managerja leta 2011«, ki ga vsako leto podeljuje Slovensko združenje korporativne varnosti. Kaj vam osebno pomeni ta laskavi naziv?
Vsakdo na svoji delovni poti potrebuje signale, da gre njegovo delo v pravo smer. Predvsem pa je spodbudno, da nekdo to ceni in opazi. To mi daje vso potrebno energijo za prihajajoče izzive, ki postajajo vedno večji in zahtevnejši. Resnica je, da smo vsi člani združenja zmagovalci, saj je največja nagrada biti del ekipe, ki premore toliko znanja in osebnih kompetenc. ■

Avtor: mag. Milan Tarman / Urad Republike Slovenije za varovanje tajnih podatkov*



OBVLADOVANJE INFORMACIJ – KORELACIJA VAROVANJA TAJNIH PODATKOV IN POSLOVNIH SKRIVNOSTI

V moderni družbi varnostnih tveganj in groženj je potrebno ob sistematičnem pristopu na področju varnosti posvetiti posebno pozornost tudi obvladovanju informacij. Varnost je mogoče v teh primerih razumevati, kot splet varnostnih ukrepov in postopkov, potrebnih za zaščito, sledljivost in preventivo zlorabe informacij.

V praksi se dokazuje, da je v tesnem in konstantnem sodelovanju pristojnih državnih organov za varovanje tajnih podatkov z ostalimi usposobljenimi inštitucijami korporacijske varnosti in poslovnimi subjekti mogoče uspešno varno obvladati informacije in se zoperstavljati številnim poskusom nepooblaščenega dostopanja. Pomembno je tudi multilateralno in bilateralno sodelovanje zlasti pri izmenjavi strategij in dobrih praks.

V primerih, ko so poslovni subjekti v pogodbenem odnosu z državnimi organi, ki bi jih zavezoval k varovanju tajnih podatkov, ravnajo ustrezno predpisom s predmetnega področja. Ustrezna strategija in posledično ukrepi za varovanje informacij so namreč ključni za uspešno delo tako v izmenjavi informacij med državnimi subjekti samimi, med javnim in zasebnim sektorjem kot tudi med poslovnimi subjekti.

Namen prispevka je prikazati pomen obvladovanja informacij kot obvladovanja enega izmed varnostnih tveganj. Vsebino predstavljeno v treh vsebinskih delih začenjam v prvem delu s krajšo predstavitvijo pristopa in sistema države k varovanju tajnih podatkov. Nadaljujem v drugem delu s predstavitvijo pristopov k varovanju poslovnih skrivnosti. Vsebina tretjega dela pa je korelacija omenjenih pristopov z izzivi in rešitvami za prihodnost.

Številni poslovni subjekti pa na podlagi dobro postavljenega sistema in dobrih praks varovanja tajnih podatkov države uporabljajo podobne modele pri varovanju svojih poslovnih skrivnosti, ker je le-to eden predpogojev za učinkovitost, produktivnost in konkurenčnost.

Predstavitev varovanja tajnih podatkov

Za organizacijsko, strokovno in drugo pomoč pri delovanju vlade ter usklajevanje dela ministrstev je Vlada Republike Slovenije leta 2002 ustanovila Urad Vlade Republike Slovenije za varovanje tajnih podatkov, ki spremlja stanje na področju določanja in varovanja tajnih podatkov in skrbi za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja tajnih podatkov v državnih organih, organih lokalnih skupnosti, pri nosilcih javnih pooblastil ter v gospodarskih družbah in organizacijah, ki pridobijo ali razpolagajo s tajnimi podatki. Prav tako skrbi za izvrševanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju tajnih podatkov.

*avtor je član Slovenskega združenja korporativne varnosti



Ključna delovna področja so:

Osebna varnost - pomeni, da so vse osebe, ki dostopajo do tajnih podatkov zaradi opravljanja nalog ali funkcije na svojem delovnem mestu, ustrezno varnostno preverjene. To pomeni, da se v postopku varnostnega preverjanja osebe preveri lojalnost, zanesljivost in verodostojnost osebe, in sicer z namenom, da se osebi izda ali da oseba zadrži dovoljenje za dostop do tajnih podatkov. V postopku varnostnega preverjanja se obravnavajo vidiki, ki zadevajo osebnostni značaj, in okoliščine, ki bi lahko povzročile nastanek potencialnih varnostnih problemov.

Fizična varnost - glavni cilj je odvrniti, preprečiti in/ali odkriti nepooblaščene dostope do tajnih podatkov. Fizična varnost je sestavljena iz različnih postopkov in ukrepov varovanja; organizacijskih, varnostno-tehničnih in mehanskih ter postopkov in ukrepov fizičnega varovanja. Vsi našteti dejavniki so med seboj tesno povezani, zato je učinkovitost celotnega sistema fizične varnosti tajnih podatkov odvisna od učinkovitosti njegovih posameznih elementov. Pri odločanju o tem katera stopnja fizične varnosti je potrebna se upoštevajo različni dejavniki; stopnja tajnosti in vrsta podatkov, ki se varujejo, njihova količina, oblika in način hranjenja, ocena ogroženosti ter stopnja varnostne kulture pri zaposlenih.

Dokumentacijska varnost - tajni podatek je lahko označen s stopnjo tajnosti INTERNO, ZAUPNO, TAJNO ali STROGO TAJNO. Dokumentacijska varnost opredeljuje enoten sistem določanja in označevanja tajnih podatkov, prenosa, razmnoževanja, evidentiranja, uničevanja in arhiviranja ter postopka ob zlorabi tajnega podatka.

Informacijska varnost - obsega določanje in uporabo ukrepov za zaščito tajnih podatkov, ki se obdelujejo, shranjujejo in prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov.
Informacijska varnost vsebuje tako ukrepe varovanja tajnosti v računalniških sistemih, oziroma računalniško varnost - COMPUSEC (varnost strojne opreme, varnost programske opreme in varnost programsko-strojne opreme), kot ukrepe varovanja tajnosti v komunikacijskih sistemih, oziroma komunikacijsko varnost - COMSEC (varnost prenosnih sistemov - TRANSEC, varnost kriptografskih metod in naprav - CRYPTOSEC, varnost pri elektromagnetnem sevanju elektronskih naprav - EMSEC). Med omenjene ukrepe sodi tudi odkrivanje, dokumentiranje in zoperstavljanje vsem oblikam groženj, usmerjenim tako proti tajnim podatkom, kot proti sistemom, ki tajne podatke obravnavajo.

Industrijska varnost - sprejem ukrepov za varovanje tajnih podatkov med gospodarskimi družbami in organizacijami v primerih, ko naročila in dodeljevanje naročil vsebujejo tajne podatke. Industrijska varnost pomeni uporabo varnostnih ukrepov in postopkov za preprečevanje, odkrivanje in povrnitev izgube ali prenehanje ogrožanja tajnih dokumentov, s katerimi razpolaga izvajalec ali podizvajalec med pogajanji pred dodelitvijo in med izvajanjem tajnega naročila oziroma tajnega podnaročila.

Usposabljanje - za organe in organizacije UVTP izvaja osnovno in dodatno usposabljanje s področja varovanja tajnih podatkov. Osnovno in dodatno usposabljanje v organih in organizacijah lahko izvajajo izvajalci (osebe ali organizacijske enote), ki jih določi predstojnik.

Pristopi k varovanju poslovnih skrivnosti

Na podlagi ustreznega postavljenega sistema in dobrih praks varovanja tajnih podatkov države uporabljajo številni poslovni subjekti, kot uvodoma omenjeno podobne modele pri varovanju svojih poslovnih skrivnosti, kot enega osnovnih pogojev za učinkovitost, produktivnost in konkurenčnost. V poslovnem svetu pa podjetja, ki na področju varovanja poslovnih skrivnosti ne uživajo ugleda in zaupanja,

V praksi imajo redki poslovni subjekti zadostne lastne dovolj strokovne resurse za ustrezno postavitev in vzdrževanje učinkovitega sistema varovanja poslovnih skrivnosti.

redko dosegajo poslovne uspehe. Z vidika ekonomičnosti je zato smotrno sodelovanje s specializiranimi usposobljenimi subjekti in inštitucijami korporacijske varnosti. Sistem varovanja poslovnih skrivnosti je potrebno ustrezno umestiti v celovit varnostni sistem, postavitev le-tega pa omogoča poslovno varnostno svetovanje, katerega kvalitetno izvajajo uveljavljene mednarodno priznane inštitucije z ustreznimi referencami.

Poslovno varnostno svetovanje se namreč lahko izvaja v več različnih oblikah:

Posnetki in analize stanja varnostnih sistemov - vsako poseganje v prenovo oziroma v posodobitev varnostnega sistema zahteva temeljit posnetek, analizo in oceno obstoječega varnostnega sistema. To je v bistvu prva faza prenove, posodobitve ali projektiranja celovitega varnostnega sistema. Da bi prišli do nabora potrebnih podatkov in informacij je potrebno opraviti operativni varnostni pregled območij, zgradb, prostorov, opreme, procesov, logistike in določene dokumentacije. Poleg tega je treba proučiti zakonodajo, notranje akte, standarde, ogroženost, varnostna tveganja in dobro prakso ter pridobiti informacije (intervjuji in vprašalniki) od kompetentnih ljudi v podjetju, zlasti vodstva in odgovornih oseb za posamezna področja varnosti. Pri analizi zbranih podatkov pa je treba uporabiti ustrezne kvalitativne in kvantitativne metode. Gre za profesionalni pristop k posnetku in oceni stanja, ki ga podjetje kot naročnik tovrstnih storitev lahko opravi le ob angažiranju zunanjih (neodvisnih) varnostnih strokovnjakov ali podjetja, ki se ukvarja z varnostnim inženiringom.

Intervjuji in vprašalniki - sestavni del posnetka stanja je tudi izvedba poglobljenih razgovorov ali intervjujev z vodstvom podjetja, z odgovornimi osebami za posamezna področja varnosti (varnostni management) in s strokovnjaki (informatiki, razvojniki, analitiki, raziskovalci). Kot dodatni pripomoček za pridobivanje podatkov se največkrat uporabi tudi vsebinsko ustrezen anketni vprašalnik, ki ga je treba obdelati z multivariantnimi statističnimi metodami. Če uporaba teh metod - zaradi nizkega števila podatkov - ni možna, se uporabijo analitične metode kvalitativne narave.

Ocenjevanje ogroženosti - ocena ogroženosti je, poleg varnostne politike in upravljanja s tveganji, na področju varnosti nepogrešljiv krovni dokument celovitega varnostnega sistema. Osnovni pokazatelj ocene ogroženosti se poda v obliki matrike ogroženosti, v kateri se na 10-stopenjski lestvici oceni 16 vrst ogroženosti, in sicer: ogroženost od naravnih nesreč, požarna, eksplozijska in ekološka ogroženost, ogroženost (tveganja) na delovnih mestih, kriminalna, teroristična, vohunska. informacijska, komunikacijska, sabotažna, stavkovna, prometna, logistična, konkurenčna in tehnično-tehnološka ogroženost ter ogroženost zaposlenega osebja. Vsaka vrsta ogroženosti se ponazori grafično in opisno. Sestavni del ocene ogroženosti je predlog varnostnih ukrepov, ki jih varnostna in druge službe ter zunanji izvajalci (outsourcing) izvajajo na podlagi ustreznih dokumentov (pravilnikov, načrtov, navodil, pogodb). Ocena ogroženosti je lahko samostojni dokument, ali pa je sestavni del varnostnega elaborata.

Varnostni elaborati - varnostni elaborat nastane na podlagi celovitega (temeljitega) posnetka in analize stanja, zajemati pa mora naslednje vsebinske dele: predstavitev naročnika, projektni pristop, posnetek in analizo stanja, oceno ogroženosti, ugotovitve, obvladovanje varnostnih tveganj in sprememb, predlog varnostnih izboljšav, prioritete, uvajanje varnostnih standardov, terminski plan, finančno konstrukcijo (potrebna sredstva za varnostne izboljšave), način implementacije varnostnega elaborata, potrebni odzivi vodstva, priporočila vodstvu. Izdelava varnostnih elaboratov je lahko eden od načinov poslovno-varnostnega svetovanja, ali pa se naročnik odloči, da se angažira usposobljen zunanji izvajalec za vzpostavitev integralnega (celovitega) varnostnega sistema. To pa pomeni, da se v prvi fazi izdela varnostni elaborat, v drugi fazi – ko vodstvo elaborat odobri - pa se pristopi k implementaciji elaborata. Implementacija elaborata pomeni realizacijo vseh predlaganih varnostnih izboljšav, ki se (izhajajoč iz dosedanje prakse) nanašajo pretežno na posodobitev in optimizacijo fizičnega in tehničnega varovanja, na dograditev aktivne požarne zaščite, na posodobitev pristopne kontrole in protivlomne zaščite, na izpeljavo izboljšav varovanja podatkov, informacij in poslovnih skrivnosti, na dograditev notranjih ak-





tov (pravilnikov, načrtov in navodil) in na usposabljanje varnostnega osebja in zaposlenih.

Dokumenti varovanja - naročniku storitev se pojasni katere dokumente varovanja (pravilnike, načrte in navodila) mora imeti po zakonu in katere bo domnevno treba izdelati na podlagi morebitnih kasnejših ugotovitev. V nadaljevanju se predstavi metodika (strukturo in vsebino) izdelave posameznih aktov in problematiko v zvezi s tem. Iz dosedanje prakse je razvidno, da so podjetja šibka zlasti v pripravah nekaterih pravilnikov in navodil, nadalje v načrtovanju fizičnega in tehničnega varovanja, načrtovanju in izvajanju evakuacije, načrtovanju obvladovanja izrednih dogodkov, obvladovanju alarmnega in odzivnega sistema ter v načrtovanju neprekinjenega obratovanja in poslovanja v kriznih razmerah (krizni management).

Strokovna mnenja - na podlagi zahtevkov varnostnih in pravosodnih organov, kakor tudi odvetnikov in ostalih zainteresiranih izdajamo strokovna mnenja, ki jih izdelajo najboljši strokovnjaki z akademskimi in praktičnimi izkušnjami. Strokovno mnenje je praviloma izdelano v pisni obliki, podkrepljeno z grafičnimi elementi. Po potrebi in na željo naročnika strokovno mnenje podrobneje obrazložimo na predstavitvi, ki je lahko obogatena tudi z realnimi primeri in praktičnim prikazom. Izdajajo se samo strokovna mnenja, ki so vsebinsko povezana s ponudnikom storitev in temeljijo na znanstvenih dognanjih in strokovnih rešitvah večkrat preverjenih v praksi.

Le v okvirih tovrstno izvedenega procesa je mogoče tudi ustrezno umestiti sam sistem varovanja poslovnih informacij v določenem poslovnem subjektu.

Sinergije navedenega ob ustreznem pristopu in implementaciji dejansko pomenijo doseganje ugleda in zaupanja pri poslovanju, učinkovitost, produktivnost in konkurenčnost ter boljše poslovne rezultate.

Korelacija varovanja tajnih podatkov in poslovnih skrivnosti

V okviru oblik poslovnega varnostnega svetovanja je mogoče nato v določenem poslovnem subjektu določiti model varovanja poslovnih skrivnosti, ki vsebuje tudi elemente področij varovanja tajnih podatkov: osebno, fizično, dokumentacijsko, informacijsko in industrijsko varnost ter usposabljanje.

Varovanje tajnih podatkov in poslovnih skrivnosti ter trend naraščanja s tem povezanih varnostnih tveganj je realnost - izziv, kako uspešno zagotavljati varovanje tajnih podatkov in poslovnih skrivnosti. To je prav gotovo eden največjih izzivov držav in poslovnih subjektov v želji zavarovati podatke zaradi zakonskih ali poslovnih razlogov pred nepoklicanimi osebami.

Tudi na tem področju namreč velja pregovor Winstona Churchilla: »**Attitude is a little thing that makes a big difference**« (v prevodu: Odnos je majhna stvar, ki pomeni veliko razliko). Naj zaključim ta prispevek s spoznanjem, da ostaja naslovna tema aktualna – še več, v današnjem svetu je praktično nujnost intenzivno in kooperativno sodelovanje s pristojnimi organi in inštitucijami v odgovor gornjemu izzivu.

Viri

- Churchill Winston, http://www.brainyquote.com/quotes/authors/w/winston_churchill.html#LPVI1hm2vgCdLvye.99, 5.7.2012.
- Inštitut za korporativne varnostne študije ICS, http://www.ics-institut.si/, 7.7.2012.
- Sklep o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Ur. l. RS, št. 6/02).
- Urad za varovanje tajnih podatkov - informacije na spletni strani, http://www.uvtp.gov.si/, 4.7.2012.
- Zakon o tajnih podatkih (Ur. l. RS, št. 50/06 in spremembe ter dopolnitve). ■

Avtor: mag. Miran Vršec / Inštitut za korporativne varnostne študije-ICS, Ljubljana*



KOLUMNA
miran.vrsec@ics-institut.si

STANJE NA PODROČJU GOSPODARSKE IN INDUSTRIJSKE VARNOSTI V REPUBLIKI SLOVENIJI – DILEME IN IZZIVI

Gospodarsko in industrijsko varnost v Republiki Sloveniji zagotavljajo različni subjekti javnega in zasebnega sektorja. Nacionalne interese in nacionalno varnostne cilje opredeljuje Resolucija o strategiji nacionalne varnosti, ki zaradi vpetosti Slovenije v EU, NATO in druge pomembne mednarodne organizacije upošteva določila mednarodnega prava in določa delovanje nacionalno varnostnega sistema po njihovih načelih. Ko govorimo o gospodarski in industrijski varnosti je pomembno poudariti, da strategija med ključne akterje zagotavljanja notranje varnosti uvršča tudi varnostne službe in organizacije zasebnega prava pri tem pa poudarja tudi razvoj javno-zasebnega partnerstva. Pomemben poudarek je dan tudi varovanju kritične infrastrukture in izboljšanju kakovosti varovanja premoženja na vseh ravneh. Na nacionalnem nivoju je torej prepoznana pomembna vloga tako subjektov zasebnega varovanja, kot tudi drugih organizacij pri zagotavljanju notranje varnosti, prav tako pa je nakazana potreba o določitvi in ustrezni zaščiti kritične infrastrukture, kot ključne infrastrukture za nemoteno delovanje države v kriznih razmerah. Ko govorimo o kritični infrastrukturi gre navsezadnje za vseevropski projekt vzpostavljanja sistema obvladovanja tveganj v subjektih, ki so ključnega pomena za delovanje države in življenje prebivalstva v kriznih oziroma kritičnih razmerah.

Tako je zamišljeno na nacionalnem in nadnacionalnem nivoju. Kakšno pa je dejansko stanje v praksi?

Področje gospodarske in industrijske varnosti v Republiki Sloveniji v pretežni meri obvladuje sektor zasebnega varovanja, v katerem trenutno deluje okoli 120 zasebnih varnostnih podjetij s preko 7.000 zaposlenimi. Če k tej številki prištejemo še ostalo osebje, ki skrbi za varnost po podjetjih na tak ali drugačen način, lahko ugotovimo, da na tem področju aktivno deluje okoli 9.000 ljudi. Število zaposlenih v sektorju zasebnega varovanja se ja tako že praktično izenačilo s številom zaposlenih v Ministrstvu za notranje zadeve (vključujoč tudi Policijo) ter Ministrstvu za obrambo (vključujoč tudi Slovensko vojsko). V letu 2011 je bil sprejet nov Zakon o zasebnem varovanju, ki je prinesel kar nekaj novosti, ki vsekakor pozitivno vplivajo na dvig zakonitosti in kakovosti izvajanja storitve zasebnega varovanja, kljub temu pa z zniževanjem vstopnih pogojev za pridobitev posameznih licenc zasebnega varovanja omogoča lažji vstop novim igralcem na trg zasebnega varovanja, kar bo po moji oceni vsekakor negativno vplivalo na kakovost in zakonitost varovanja. Upam, da ti negativni vplivi ne bodo prevladali nad pozitivnimi vplivi, ki jih je vpeljal novi zakon. Ključni problem, ki ga vidim v Republiki Sloveniji na področju zasebnega varovanja pa ni v zakonodaji kot taki, temveč predvsem v neurejenem statusu varnostnega menedžmenta, tako na eni strani pri subjektih zasebnega varovanja, kot na drugi strani tudi pri uporabnikih (kupcih) zasebnega varovanja,

*avtor je član Slovenskega združenja korporativne varnosti



nadalje v pomanjkanju sistemskega in strokovnega nadzora nad izvajalci zasebnega varovanja, v neustreznih in zastrelih programih izobraževanja tako na dodiplomskem, kot tudi na podiplomskem nivoju in ne nazadnje tudi na slabi organiziranosti in povezanosti varnostnih menedžerjev zaposlenih pri uporabnikih (kupcih) zasebnega varovanja. Ob tem bi rad še posebej opozoril na pomanjkanje sistemskega pristopa k obvladovanju tveganj v organizacijah, saj izgradnja varnostnih sistemov temelji predvsem na pavšalnih ocenah tveganj in ne na konkretnih ocenah ogroženosti, ranljivosti in varnostnih tveganj, zato vzpostavljeni varnostni sistemi in uvedene varnostne rešitve ne prinašajo pričakovane dodane vrednosti in učinkov glede na vložena sredstva. Po moji grobi oceni je zaradi navedenih problemov in neurejenega stanja v Republiki Sloveniji cca. 1.500 varnostnikov preveč. S celovitim pristopom in izdelavo realnih ocen ogroženosti, ranljivosti in varnostnih tveganj bi na nivoju Republike Slovenije v organizacijah, ki najemajo storitve zasebnega varovanja, lahko na letnem nivoju prihranili cca. 25 mio EUR, ki bi jih lahko investirali v posodobitve varnostnih sistemov in dvig učinkovitosti varnostnih rešitev ter na ta način posredno vplivali tudi na zmanjšanje kriminalitete v Republiki Slovenije ter dvig konkurenčnosti slovenskega gospodarstva v lokalnem in globalnem okolju.

> Zasebno varovanje ima predvsem status outsourcing (pogodbenega najema) storitev, ki po teoriji lahko organizacijam, katere najemajo tovrstne storitve povzroča še dodatna tveganja. Ko razmišljamo o statusu zasebnega varovanja nikakor ne moremo in ne smemo govoriti o strateškem nivoju obvladovanja tveganj, vsaj ne v situaciji v kateri se trenutno nahaja slovenski trg zasebnega varovanja in vsi z njim neposredno povezani akterji.

Ko razmišljamo o gospodarski in industrijski varnosti se je namreč potrebno zavedati dejstva, da subjekti zasebnega varovanja obvladujejo le določen del tveganj v organizacijah, kjer izvajajo svojo dejavnost in delujejo le na določenem, predvsem operativnem nivoju obvladovanja tveganj v organizacijah. V Republiki Sloveniji se tega dejstva vse premalo zavedamo, saj še vedno prevladuje prepričanje, da je zasebno varovanje tisto, ki lahko uporabnikom v večji meri ponudi vse rešitve na področju obvladovanja tveganj in pri reševanju tekoče varnostne problematike.

Dejstva so povsem drugačna. Ranljivost, ogroženost in varnostna tveganja lahko učinkovito obvladujemo le, če jih obravnavamo na strateškem nivoju in v organizacijo uvajamo filozofijo korporativne varnosti, ki temelji na metodološkem in celovitem prepoznavanju ranljivosti, ogroženosti in tveganj, na razvoju varnostnega menedžmenta, krepitvi poslovne etike in varnostne kulture, na izgradnji notranjega pravnega reda in izdelavi dokumentov varovanja, na uvajanju standardov varovanja, na sistematičnem izobraževanju, usposabljanju in izpopolnjevanju, na celovitem in strokovnem nadzoru in na uvajanju stalnih izboljšav v sistem varovanja in obvladovanja tveganj. Gre torej za vzpostavitev integralnega varnostnega sistema, ki na vseh nivojih organizacije zagotavlja učinkovito upravljanje s tveganji. Da bi dosegli nakazane usmeritve moramo v Sloveniji najprej prenoviti programe izobraževanja na dodiplomskem in podiplomskem nivoju, zakonsko urediti status (pristojnosti in odgovornosti) varnostnega menedžerja in odgovornost poslovodstva sleherne organizacije, kot to denimo določa zakonodaja s področja požarne varnosti in varstva in zdravja pri delu ter v zakonodaji jasno opredeliti notranji pravni red in dokumente varovanja, ki bodo sistemsko urejali področje obvladovanja in upravljanja z varnostnimi tveganji. ■

Avtor: dr. Dušan Marinčič / direktor podjetja DR DM d.o.o.*



POMEN CELOSTNIH ANALIZ ZA USPEŠNO POSLOVANJE

Za začetek 21. stoletja je značilna demokratizacija informacij, tehnologije in financ. Zaradi vedno večje negotovosti pri reševanju ekonomskih razmer, je potrebno iskati nove metode in orodja za enakomeren družbeni razvoj.

Pričujoči članek razkriva uporabo sodobne analitične metodologije pri razumevanju globalnih varnostnih odklonov, ki posledično vplivajo tudi na korporativno varnost in neprekinjeno poslovanje. Po koncu »hladne vojne« je politična znanost opredelila varnost kot nek skupek političnih, ekonomskih, zdravstvenih, okoljevarstvenih, kriminalnih, vojaških, informacijskih družbenih razsežnosti ter ostalih oblik groženj sodobni družbi. Uravnovešena interakcija med vsemi naštetimi družbenimi razsežnostmi predstavlja celostno varnost ali »varnost v njeni celotni podobi«.

Za razumevanje stanja celostne varnosti določene družbe, so potrebne celostne družbene analize, ki zahtevajo skrbno selekcijo geografskih/okoljskih, demografskih, ekonomskih, političnih in socialnih spremenljivk na ravni občine ali province. Vse z namenom, da bi lahko izmerili lokalne zmogljivosti izbrane politične entitete za trajnostni razvoj ali za družbeno obnovo v celoti. Občine ali province morajo s svojo funkcionalno strukturo zagotavljati blaginjo prebivalstvu. Sistem varnosti predstavlja tako posameznikom, skupinam, korporacijam in družbam na splošno, sredstvo za pridobivanje sposobnosti obvladovanja nepričakovanega in zaščito notranjih vrednot. Varnost pomeni obrambo proti zunanjim in notranjim grožnjam, ter socialno-ekonomsko blaginjo znotraj posamezne družbe.

S pomočjo sistemskega pristopa je možno razumevanje začetnih potencialov družbenih razsežnosti na določenem območju interesa. Za pravilno oceno tveganja in oceno razvitosti določene lokalne skupnosti, je potrebno najprej določiti funkcionalna in družbena področja analize. Lahko so povezana s predmeti tveganj, z območji tveganj in sposobnostjo lokalne skupnosti, da predvidi možne varnostne grožnje, s tem pa zmanjšuje lastno ranljivost. Ranljivost lokalne skupnosti je v stalni korelaciji z zmožnostjo upravljanja s kompleksnimi varnostnimi odkloni, in s tem tudi s stopnjo preživetja določene populacije. Lokalne skupnosti z zadovoljivo stopnjo ranljivosti lahko definiramo kot sposobne in prilagodljive. Najprimernejša metoda je multivariatna analiza lokalne zmogljivosti, z analizo skupin in faktorsko analizo, ki raziskovalcu dopuščajo definicijo tipologije občin ali provinc, glede na skupine spremenljivk. Omenjena metodologija je bila prvič uporablje-

> Da bi lahko v celoti razumeli raven lokalne zmogljivosti razvoja za trajnostni družbeni razvoj, je nujno poznavanje aplikativnega celostnega pristopa določeni družbi in s tem povezano načrtovanje najprimernejših varnostnih in poslovnih ukrepov.

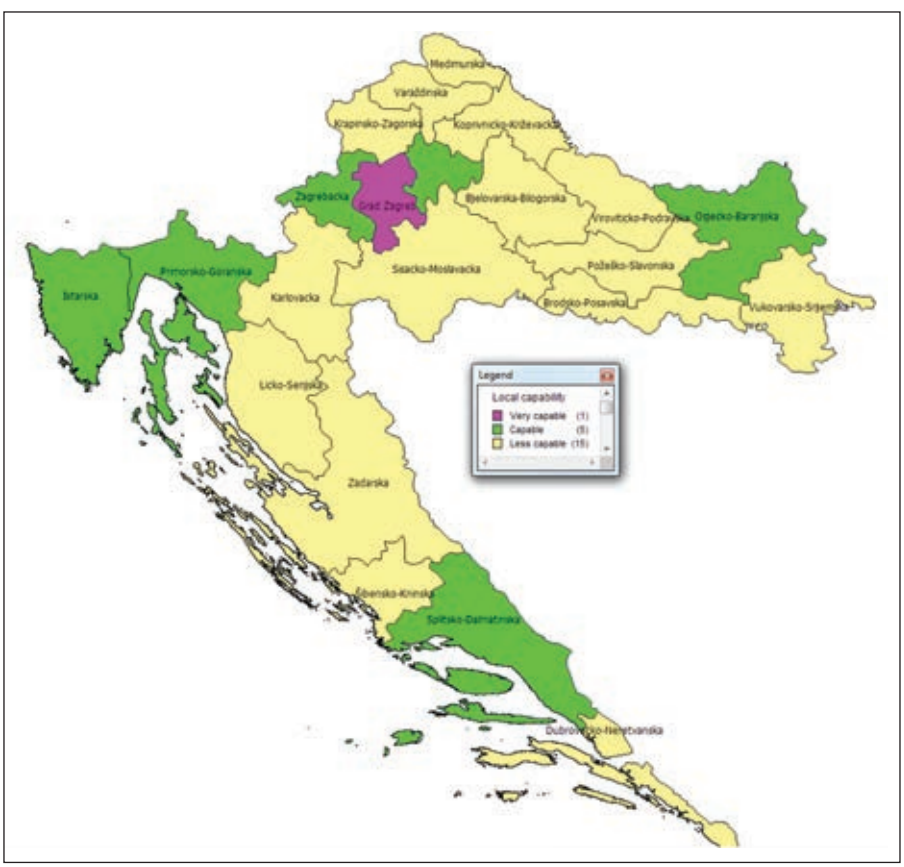
na za oceno družbenih razmer na območju kriznega odzivanja, kot sta Afganistan in Kosovo.

Glavni motiv za nadaljevanje tovrstnih raziskav je bila tudi raziskovalna radovednost, če se enaka metodologija lahko uporabi za korporativno varnost in za oceno tveganja v primeru novih investicij v določeni državi oziroma regiji. Na zahtevo naročnika, ki je želel preveriti lastno poslovno odločitev, smo izdelali multivariatno analizo Hrvaške na ravni županij. V nadaljevanju se je projekt na posa-

*avtor je član Slovenskega združenja korporativne varnosti

mični ravni osredotočil na razvoj turizma na otoku Krk, ter posebej na območje občine Malinska-Dubašnica s proučitvijo njenega prostorskega načrta.

Da bi lahko dobili vpogled v možnost prihodnjega vlaganja v turistične kapacitete otoka Krk, je bilo naprej potrebno izmeriti lokalne zmogljivosti županij Republike Hrvaške. Multivariatna analiza je pokazala, da so županije Hrvaške razdeljene na tri skupine, in sicer: v prvi zelo zmogljivi skupini je bila ena županija - Zagreb, v drugi zmogljivi skupini je pet županij, in v tretji manj zmogljivi skupini se nahaja ostalih 15 županij Hrvaške (glej sliko).



Druga skupina petih zmogljivih županij (zelena barva), izrazito pozitivno izstopa na področju turizma, v primerjavi z ostalimi skupinami. Tretja skupna manj zmogljivih (rumena barva) je pod povprečjem na vseh področjih družbenega razvoja. To pomeni, da kar 71% županij Hrvaške potrebuje pomoč centralne oblasti za dvig lokalne zmogljivosti, za normalen družbeni razvoj. Faktorska analiza je pokazala da sta ključna dva faktorja, turizem in splošni družbeni razvoj. Iz tega izhaja, da ima turizem na Hrvaške strateški značaj, med katerimi izstopa Splitsko-Dalmatinska in Primorsko-Goranska županija.

Glede na zahteve se je projekt osredotočil na Primorsko-Goransko županijo, kjer ima največ nočitev Mali Lošinj, z 1.722.917 nočitvami. Otok Krk s 759.433 nočitvami, ima kar 56% manj turističnih nočitev, v primerjavi z Malim Lošinjem. Zaradi tega je Krk na 6.mestu po številu turističnih nočitev v Primorsko-Goranski županiji. Občina Malinska-Dubašnica je v istem obdobju gostila 448.554 turistov, od tega samo mesto Malinska 399.194 turistov.

Z uporabo sodobne analitične metodologije se lahko omogoča korporacijam/podjetjem razumevanje poslovnega okolje in socialne dinamike, z namenom oblikovanja primerne korporativne politike in korporativne družbene odgovornosti.

Cilji nadaljnjega razvoja turizma na otoku Krk mora biti v soglasju z različnimi interesnimi skupinami prebivalcev in otoških organizacij. Za investitorja je pomembno, da z vlaganjem v turizem na otoku Krk uspešno posluje in istočasno kaže družbeno odgovornost do zunanjega okolja. Torej cilj turističnega razvoja na otoku Krk, mora biti v soglasju z dolgoročnimi interesi prebivalstva otoka Krk. To vsekakor predstavlja največje tveganje investicije ali posameznega projekta, saj je potrebno dolgotrajno usklajevanje želja in potreb obeh strani. Pri vsem tem, je potrebno spoštovati obstoječe prostorske ureditve (anekse) občin otoka Krk, kot tudi ostale dolgoročne socialne, ekonomske, okoljske in turistične cilje razvoja v prihodnje.

Z uporabo sodobne analitične metodologije se lahko omogoča korporacijam/podjetjem razumevanje poslovnega okolje in socialne dinamike, z namenom oblikovanja primerne korporativne politike in korporativne družbene odgovornosti. Podjetje/naročnik je tisti, ki je odgovoren za prepoznavanje in upravljanje s koordinacijo vseh funkcionalnih delov podjetja, ki vključujejo splošno varnost, kontinuiranost in varnost posameznika znotraj podjetja. Proces globalizacije je prisilil podjetja, da v okolju vedno večjega tveganja, morajo širše razumeti interakcijo med družbenimi razsežnostmi, z namenom, da bi lahko ocenili faktor investicijskega tveganja in oblikovali strateško-operativne načrte poslovanja.

Glede na multivariantno analizo in GIS prikazom najprimernejših poslovnih odločitev, skušamo torej poleg dobrega poslovanja tudi transparentno izboljšati življenjske pogoje tamkajšnjega prebivalstva. S tem ne delujemo samo poslovno ampak tudi družbeno odgovorno, kjer posledično prebivalstvo podpira naše poslovne rezultate v njihovem domačem okolju. Iz tega vidika multivariantna analiza omogoča selekcijo izbranih občin ali provinc, na podlagi lokalne zmogljivosti, ter omogoča poglobljeno izdelavo oceno tveganja v določeni regiji izbrane države. ■

Avtorja: Zdenko Hriberšek, Direktor Gorenje, d.d. - Varovanje*,
Alma Ribič, mag.var., Gorenje, d.d. - Varovanje





KORPORATIVNA VARNOST – KONKURENČNA PREDNOST GORENJA, D.D.

Varnost je za poslovno uspešnost Gorenja ena izmed pomembnih poslovnih funkcij. Kot korporativno varnost označujemo vse aktivnosti v družbi, s katerimi opredeljujemo in izvajamo potrebne sistemske ukrepe za obvladovanje varnostnih tveganj.

Za osnovni koncept korporativne varnosti v družbi Gorenje, d.d. in njen pomen za zagotavljanje varnosti v Skupini Gorenje smo na področju korporativnega upravljanja uveljavili visoke standarde, ki jih dosledno spoštujemo, izvajamo in nenehno nadgrajujemo skladno z dobrimi praksami na podlagi lastnih izkušenj in izkušenj drugih. Odprtost je že leta ena naših temeljnih vrednot, ki je prepoznana tudi v okolju. Skupina Gorenje s šestdesetletno zgodovino izdeluje tehnološko dovršene in energetsko učinkovite ter vrhunsko oblikovane gospodinjske aparate. Svojo ponudbo dopolnjujemo z lastnim proizvodnim programom kuhinjskega pohištva in kopalniške opreme ter dokupnega programa, v zadnjih letih pa svoje aktivnosti krepimo tudi v segmentih ekologije, energetike in storitev. Osrednja lokacija za proizvodnjo velikih gospodinjskih aparatov je v Velenju, svoje proizvodne obrate pa imamo tudi drugod v Sloveniji, v Srbiji, na Češkem in Finskem.

Sledimo implementaciji in uporabi poslovno-varnostnih standardov v vseh procesih. Proizvodni in poslovni procesi se v Gorenju izvajajo v skladu s sistemom vodenja kakovosti po standardu ISO 9001:2008. Poslujemo tudi skladno z zahtevami sistema varnega in zdravega dela po standardu OHSAS 18001 in s sistemom varnega okolja po standardu 14001+EMAS. Prav tako so v uporabi še mnogi drugi standardi, kot npr. 27001 za varovanje informacij, ISO 10002:2004 zadovoljstvo strank, navodila za reševanje pritožb, standardi zasebnega varovanja, itd.

V globalnem okolju in ob hitrih spremembah je Gorenje izpostavljeno velikim tveganjem. Le-ta analiziramo in poskušamo odkrivati nova, kar omogoča ustrezno odločanje in nadzorovanje tveganj. Korporativna varnost v Gorenju zajema vse oblike ranljivosti, ogroženosti in tveganja ter obvladovanje le-teh. Nevarnosti in različna tveganja vplivajo na učinkovitost in uspešnost poslovanja, zavedamo pa se, da lahko pomenijo resno ogroženost našega poslovnega sistema in njegovih procesov.

Gorenje je v svojem obstoju in delovanju podvrženo različnim oblikam zunanjih in notranjih nevarnosti, ki pa lahko neugodno vplivajo na procese, s tem pa tudi na poslovne rezultate. Kot učinkovito preventivno sredstvo obvladovanja neželenih ogrožanj in nevarnosti za ljudi ter premoženje družbe imamo vzpostavljeno celovito varovanje, t.i. integralni varnostni sistem, ki zajema varnostno politiko, zunanjo in notranjo pravno podlago, načrt varovanja, oceno ogroženosti in tveganj, zaščito zaupnih podatkov, informacij, znanja, informacijsko varnost, sklenitev ustreznega zavarovanja zaposlenih in premoženja, varnostno kulturo, varnost in zdravje pri delu, ekološko varnost, požarno varnost, lastno službo varovanja s fizičnim in tehničnim varovanjem, civilno zaščito z ekipo PP. Potrebno je omeniti tudi nadzorno funkcijo skozi kontroling družbe. Cilj korporativne varnosti je zagotavljanje delovanja integralnega varnostnega sistema. Za celotno zaokrožitev integralnega varnostnega sistema nam manjka lastni varnostno nadzorni center (VNC), ki ga sicer v Gorenju imamo, vendar ni v skladu z zahtevanimi standardi (SIST BS 5979, idr.). Že vrsto let obvladujemo dogodke s pogodbenim VNC. Tu se nam seveda na eni strani zastavlja vprašanje o neodvisnosti upravljanja z varnostnimi alarmi in intervencijami ter obvladovanjem izrednih dogodkov, na drugi pa glede upravičenosti investicije oziroma profitabilnosti lastnega VNC.

*avtor je član Slovenskega združenja korporativne varnosti



Z vzpostavljenim integralnim varnostnim sistemom zagotavljamo v Gorenju varnost do stopnje, ki je primerna za ohranjanje funkcij družbe ter varnosti ljudi in premoženja, podatkov, tehnologije, znanja, itd. pred odtujevanjem, uničenjem ali poškodovanjem. Seveda tu lahko govorimo tudi o poslovni varnosti, kjer gre za zagotavljanje pravnih, informacijskih, funkcionalnih in organizacijskih dejavnosti za zagotovitev nemotenega poslovanja družbe. Varnostna politika družbe usmerja in vodi družbo v strokovno in učinkovito varovanje ljudi in premoženja, podatkov, znanja, tehnologije in drugih dobrin. Z njo je tako vzpostavljen sistem uresničevanja varne družbe, katere varnost lahko merimo s stopnjo njene potencialne sposobnosti za odzivnost na tveganja z nevarnostmi, s katerimi se Gorenje nenehno srečuje v svojem okolju. Z lastno varnostno politiko smo predvideli potencialna tveganja in grožnje, določili smo mehanizme za obvladovanje tveganj ter opredelili cilje varovanja, s katerimi so seznanjeni tako zaposleni v družbi kot tudi njeni lastniki. Z nenehnim razvojem varnostne politike in stalnimi izboljšavami ter izobraževanjem zaposlenih v Varovanju, kakor tudi v Gorenju zagotavljamo ustrezno stopnjo nivoja korporativne varnosti.

Na stanje varnostnega sistema v Gorenju vplivajo zunanji in notranji dejavniki. Med notranjimi vzroki motenja varnostnega sistema v Gorenju so najpogostejši: delovne nezgode, izlitje nevarnih snovi, zastrupitve, tatvine, vlomi, nezadovoljstvo zaposlenih, stavka, goljufije, iznos znanja, zaupnih – razvojnih podatkov in informacij, vdori v IS, itd., med zunanjimi pa so predvsem državna regulativa, politični ukrepi, splošno gospodarsko stanje, cene surovin in materiala, sabotaže, kazniva dejanja, podkupljivost strokovnjakov, zunanji vdori v informacijske procese prodajne mreže Gorenja, itd. Zaposleni v Gorenju dojemamo varnost predvsem kot dobrino, ki je nujno potrebna za zagotavljanje nemotenega izvajanja delovnih procesov. Ta notranji pomen varnosti močno vpliva tudi na naše kupce, poslovne partnerje, zunanje sodelavce, dobavitelje in druge, ki seveda z razumevanjem našega varnostnega koncepta in ureditve prispevajo k še večji varnostni kulturi družbe. Naš vrhnji menedžment kot tudi varnostni menedžment se zaveda, da je tudi v prihodnje potrebno vzdrževati vzpostavljeni varnostni sistem in ga z ustreznimi mehanizmi nadgrajevati ter s tem zagotavljati pogoje za zmanjšanje škod in izgub. Trditev, da ni nič tako dobro, da ne bi lahko bilo še boljše, je glede na politiko Gorenja in njeno vlogo med proizvajalci bele tehnike v svetu nekaj kar je že dolgo prisotno, poznano in upoštevano. Zato je vloga razumevanja in izvajanja korporativne varnosti na vseh področjih in nivojih še toliko bolj pomembna. ■

... da bo vaš spanec miren in premoženje varno ...

... we protect your property and assure you peaceful sleep ...



NOVA GENERACIJA PRALNIH IN SUŠILNIH STROJEV.

NOVE TEHNOLOGIJE. UltraWHITE in UltraSOFT senzacija za vselej odlično negovano perilo.

reddot design award
winner 2012

gorenje
www.gorenje.si

Avtor: Jelenko Vidic / Slovensko združenje korporativne varnosti



RAVNANJE S TVEGANJI

Ravnanje s tveganji skozi prizmo predstavitve posamezne aktivnosti tega zahtevnega procesa strateškega managementa v organizacijah. Spoznanja in ugotovitve iz vsakodnevne prakse, ter rezultati različnih raziskav na to temo, ugotavljajo, da je v gospodarskih organizacijah premalo vedenja in znanja o orodjih, metodah in tehnikah ocenjevanja tveganj.

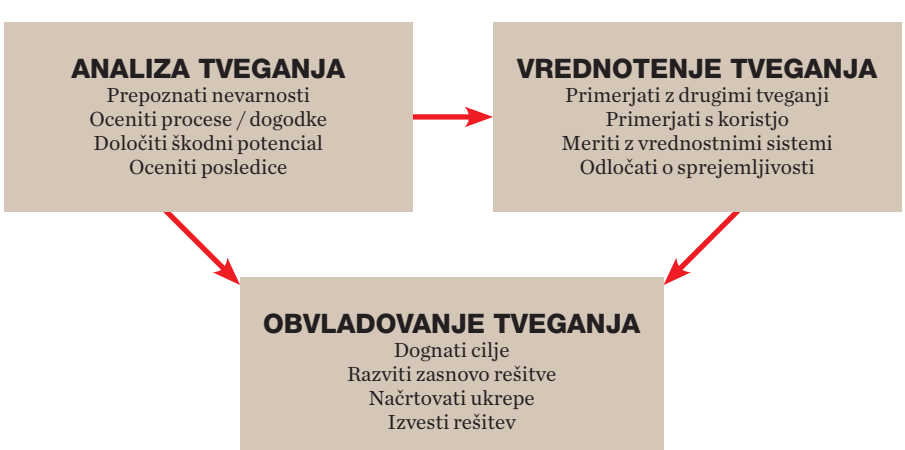
Orodja lastnikov in managementa za učinkovito ocenjevanje tveganj v organizacijah

Ravnanje s tveganji je v svetu vključeno v različne poslovodne modele, tehnike ter orodja pri upravljanju in vodenju podjetij, poslovnih sistemov, koncernov in korporacij. Zaradi poenotenega pristopa je posebej (Risk management) obravnavano v nekaterih nacionalnih in mednarodnih standardih, ter vključeno tudi v drugih standardih, ki opisujejo sisteme vodenja za različna področja**.** Proces ravnanja s tveganji je torej sestavni del strateškega vodenja podjetja, s katerim podjetje metodološko pristopi k obravnavi tveganj in njihovem obvladovanju.

Za vzpostavitev in implementacijo procesa ravnanja s tveganji obstoja kar nekaj znanih in v praksi uporabljenih metod ter strokovnih usmeritev na različnih področjih, s katerimi si pomagamo pri obvladovanju tveganj. Zanj je odgovorno poslovodstvo, vendar pa se v praksi ugotavlja, da se managerji (odločevalci) pogosto s tem nočejo ukvarjati, ker imajo dovolj težav s tekočimi problemi (»tukaj in sedaj«). Tako mnogokrat prepuščajo iskanje rešitev osebju na nižjem nivoju odločanja in/ali izvajanja, ki pa običajno ni dovolj kompetentno (izobraženo, usposobljeno,...) za izdelavo učinkovitih rešitev in zato teži k poenostavitvam (ker ne zna, ne zmore ali noče), da le zadovolji zahtevam (managementa, predpisov, standardov). Pogosto se pri tem pojavi problem, ko je treba za analizo in ocenjevanje ranljivosti, ogroženosti in tveganj izbrati eno ali več ustreznih metod in tehnik, pa iz množice kvalitativnih in kvantitativnih ne znamo izbrati. To bomo, na kolikor se da razumljiv način, poskušali predstaviti v naših prispevkih.

Kako pristopiti k obravnavi tveganj?

Če povzamemo Heinimanna (1998 v Đurović, 2005), je moderna obravnava tveganja sestavljena iz analize, vrednotenja in obvladovanja tveganja. Vsebinsko dajejo *analize tveganj* zgolj informacijo o velikosti pričakovanega vzročno-posledičnega učinka. *Ocena* je najboljše možno dognanje obsega nevarnosti, škodnega potenciala in tveganja (v primeru, da ti parametri ne morejo biti določeni z izračuni ali meritvami), *presoja* pa pomeni ugotovitev in določitev dejanskega stanja (v zvezi z nevarnostmi je to ponavadi *ocena).* Presoja družbeno-političnega pomena tveganj je naloga *vrednotenja tveganj. Obvladovanje tveganja* pa ureja način ravnanja v tveganih situacijah (**slika 1**).



Slika 1: Trije deli moderne obravnave tveganja (Heinimann, 1998 v Đurović, 2005).



Po Kienholzu (1998, prav tam) je *analiza (ocena, presoja) tveganja* sistematičen postopek označitve in kadar je možno tudi kvantifikacije verjetnosti nastopa in škodnega potenciala; *vrednotenje tveganja* pomeni presojo o sprejemljivosti iz analize tveganja pridobljenih znanj s pomočjo individualnih ali kolektivnih kriterijev (t. j. apliciranje vrednostnega sistema na dejansko stanje) in odgovarja na vprašanje »Kaj se sme zgoditi?«; *obvladovanje tveganja* opisuje ravnanje z znanimi nevarnostmi ter tveganji na temelju izidov analize in vrednotenja tveganja, ki se izvaja: preventivno, reaktivno in pasivno. Cilj obvladovanja tveganja je najvišja možna efektivnost (mera za stopnjo doseženosti cilja, brez upoštevanja porabe sredstev) in eficienca (razmerje med doseženim delovanjem ukrepa in porabljenimi sredstvi). *Komunikacija pri tveganju* pa je interaktivna izmenjava informacij in mnenj o tveganjih med udeleženci, oblastjo in strokovnjaki (z izbiranjem med možnostmi na temelju enakopravnega odločanja).

Kot analizo tveganja opisuje Flaker (1994:189-195), je to postopek, ki ga počnemo v vsakdanjem življenju tako rekoč neprenehoma, čeprav se tega ne zavedamo vedno; ko prečkamo cesto, kupujemo avto, se zaposlimo v novi službi, ..., in tako naprej. Poglavitna značilnost postopka analize je, da poskuša ločeno opredeliti in oceniti (a) grožnjo in (b) nevarnost, ki jo grožnja prinaša. Poskušajmo analizo tveganja predstaviti z njegovim primerom (v okviru spodaj).

Primer:

Bananin olupek je **grožnja**; **nevarnost**, ki nam grozi, pa je, da nam na njem spodrsne in pademo. Grožnja je torej nujen pogoj, da smo izpostavljeni nevarnosti, ne pa tudi zadosten pogoj, da se nam kaj pripeti. Se pravi: da nam spodrsne na bananinem olupku, mora biti olupek na tleh, vendar pa dejstvo, da je olupek na tleh,še ne pomeni, da nam bo na njem spodrsnilo. Oceniti moramo torej, kolikšna je **verjetnost**, da se nevarnost uresniči, če se ji izpostavimo s tveganim vedenjem. Verjetnost nevarnosti je **tveganje**, ki smo mu izpostavljeni, in tista količina, ki nas pravzaprav zanima. Nevarnost ima **status dogodka** in je statistično izmerljiva in izrazljiva. Grožnja pa nima tega statusa, (še) ni dogodek, ampak je le **okoliščina** (pogoj), da se lahko dogodek zgodi. Količinsko pa lahko izrazimo tudi resnost in gostoto grožnje (več ko je bananinih olupkov na tleh, večja je verjetnost, da se bo dogodek – nevarnost – zgodil. Grožnja je torej ***ključ*** za razumevanje nevarnosti. Vključi nas v svet nevarnosti in obratno, vključi nevarnost v naš življenjski svet (proaktivno ali reaktivno). Ko na tleh opazimo bananin olupek, ta vsaj za hip ustvari situacijo tveganja, v kateri se bomo odločili bodisi, da se ji izognemo (po navadi), bodisi, da se z njo kontrolirano in športno soočimo (bolj redko). Ali: ko treščimo po tleh, se ozremo in vidimo bananin olupek, se naše presenečenje uokviri v ugotovitev, da smo padli na bananinem olupku.

Kot analizo tveganja opisuje Flaker (1994:189-195), je to postopek, ki ga počnemo v vsakdanjem življenju tako rekoč neprenehoma, čeprav se tega ne zavedamo vedno.

Izbor orodij, metod in tehnik ocenjevanja nevarnosti, ogroženosti, ranljivosti ter tveganj

V globalnem in dinamičnem poslovnem okolju je za nemoteno delovanje organizacije učinkovito obvladovanje tveganj postalo ključni dejavnik za uspešnost, učinkovitost in navsezadnje za preživetje. Tisti menedžerji, ki se tega dejstva ne zavedajo, na žalost izgubljajo konkurenčno tekmo oziroma je njihovo podjetje dolgoročno obsojeno na stagnacijo ali celo propad (Čaleta, 2012). V svetovni praksi se za ocenjevanje tveganj, odvisno od dejavnikov, uporabljajo različni modeli. Pri izboru posameznega modela, metode ali tehnike je treba, glede na njihovo uporabnost, natančnost, omejitve, sprejemljivost metodologije in alternativne metodologije, modele in tehnike analiziranja, upoštevati velikost, dejavnost, politike, procedure, procese, zahteve in potrebe organizacije. Vsaka organizacija, mora glede na svoje specifike ter prepoznane grožnje, nevarnosti, ranljivosti in tveganja, izbrati zase najustreznejši pristop.

V tem članku najprej primeroma prikazujemo različne kvalitativne in kvantitativne tehnike in raziskovalne oziroma preiskovalne metode, ki jih podaja Sklet (2002) za raziskovanje, preiskovanje in prognoziranje nesreč (**tabela 1**). Uporabne so tudi za natančnejše analiziranje in ocenjevanje nevarnosti, ogroženosti, ranljivosti in tveganj ter posameznih dejavnikov vrednotenja in merjenja. V nadaljevanju pabo prikazano kako standard ISO/IEC 31010 (Risk management – risk assessment technique) tehnike ocenjevanja tveganj razvršča v različne skupine.

Sklepno

Pri procesu ravnanja s tveganji gre za izredno pomembno miselnost in delovanje managementa, ki se nanaša na pozitiven in kreativen pristop k obvladovanju tveganj, in s tem k preprečevanju škod in izgub (loss prevention). S tega vidika je ravnanje s tveganji sestavni del vseh sodobnih podjetniških in poslovnih funkcij ter procesov ter je vir dodatne koristi za lastnike in druge interesne skupine. Brez ustreznega izbora notranjih in zunanjih strokovnjakov ter uporabe različnih kvalitativnih in kvantitativnih metod, pa ne moremo govoriti o resnosti pristopa, saj je le to garant za uspešen in učinkovit spopad s tveganji ter njihovim obvladovanjem.

Viri

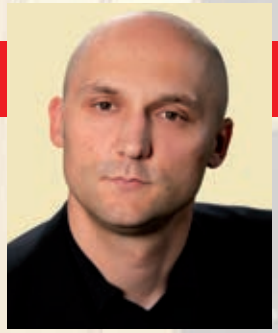
- Čaleta, D. (2012). Grožnje so del našega vsakdanjika. Interviju. Nedeljski dnevnik, 6. maj 2012, str.14.
- Đurović, B., Ribičič, M., Mikoš, M. (2005). RHDM postopek analize potencialne ogroženosti zaradi odlomne nevarnosti. Geologija, 48/1, str. 33-51, Ljubljana, 2005.
- Flaker, V. (1994). Analiza tveganja, Socialno delo, let. 33, št.4.
- Tušek, B. in Žager,L. (2004). Vloga notranjega revizorja pri ocenjevanju tveganj in ravnanju z njimi. Revizor, 14,2, 2004, str. 7-23.
- Sklet, S. (2002). Methodsforaccidentinvestigation. Pridobljeno dne 23.5.2012 na: http://www.ntnu.no/ross/reports/accident.pdf.

[1] Nekateri prevodi morda niso najbolj ustrezni, zato so v oklepaju podane kratice izvornih imen, npr.: FTA (FaultTreeAnalysis), AAM (AccidentAnatomymethod), itd. ■

ANALITIČNE TEHNIKE	PREISKOVALNE METODE
Bistvene analitične tehnike	Metoda anatomije nesreč (AAM) Analiza akcijskih napak (AEA) Analiza razvoja nesreč in ovir(AEB) Analiza vrednotenja sprememb (CE/A) Logični diagram vzroka in posledice(CELD) Drevesna metoda vzročnosti(CTM) Drevesna analiza napak(FTA) Analiza nevarnosti in operativnosti(HAZOP) Sistem stopnjevanja človeške učinkovitosti(HPES) Analiza človeške zanesljivosti-drevo dogodkov(HRA-ET) Več vzročno, sistemsko usmerjeno preiskovanje incidentov(MCSOII) Multi linearno zaporedje dogodkov (MES) Drevesna analiza tveganj napak upravljanja (MORT) Sistematična tehnika analize vzrokov (SCAT) Načrtovanje časovnega zaporedja dogodkov(STEP) Sistem preiskovanja temeljnih vzrokov incidentov (TRIIS) Tehnika operativnega pregleda (TOR) Analiza varnosti pri delu (WSA)
Diagram in analiza dogodkov ter vzročnih dejavnikov (ECFCA) Analiza ovir (BA) Analiza sprememb (CA) Analiza temeljnih vzrokov (RCA)	
Kompleksne analitične tehnike	
Drevesna analiza napak (FTA) Drevesna analiza tveganj napak upravljanja (MORT) Drevesna analiza ocenjevanja projekta (PET)	
Specifične analitične tehnike	
Analiza človeških dejavnikov (HFA) Integrirana matrika dogodkov nesreč (IAEM) Analiza možnih napak in njihovih učinkov (FMEA/FMECA) Analiza nevarnosti programske opreme (SHA) Analiza pogostih (skupnih) vzrokov napak (CCFA) Analiza prikritih okoliščin (SCA) 72-urno profiliranje Analiza materialov in struktur (MSA) Znanstveno modeliranje (ScM) (npr. za nesreče, ki vključujejo kritičnosti in atmosfersko razpršitev)	

Tabela 1: Analitične in preiskovalne tehnike in metode[1] (prirejeno po: Sklet, 2002).

Avtor: Andrej Kovačič, dipl. varstvoslovec / Slovensko združenje korporativne varnosti



VIDEONADZOR V IGRALNIŠTVU

Z razvojem tehnologije in s povečanjem igralniških procesov je videonadzor v zadnjih dveh desetletjih močno prisoten tudi v igralništvu. Videonadzor v igralnicah in igralnih salonih ima pomembno vlogo pri zagotavljanju njune korporativne varnosti in pri legitimnosti izvajanja posebnih iger na srečo.

Uvod

S tehnološkim razvojem in s povečanjem igralniških procesov je videonadzor v zadnjih dveh desetletjih prisoten tudi v igralništvu. Sistem internega nadzora, ki so ga v igralnicah izvajali pred pojavom videonadzora je z njegovo uvedbo odpravil določene pomanjkljivosti. Pravno podlago za uvedbo videonadzora v igralništvu ureja Zakon o igrah na srečo, ki zavezuje koncesionarje[1], da morajo predpisati podroben način izvajanja avdio videonadzora. V igralnicah[2] in igralnih salonih[3] se mora zagotoviti neprekinjen videonadzor vseh procesov prirejanja posebnih iger na srečo. V igralnicah so zaradi poslovanja z vrednostnimi žetoni in z gotovino na igralnih mizah večje možnosti za nastanek škodnih pojavov, čeprav dogodki kažejo, da so na "udaru" tudi igralni saloni. Videonadzor v igralnicah in igralnih salonih ima pomembno vlogo pri zagotavljanju njune korporativne varnosti in pri legitimnosti izvajanja posebnih iger na srečo. V članku bo predstavljena služba za videonadzor in sicer, kako bi morala biti organizirana in umeščena v integralnem varnostnem sistemu, kajti koncesionarji na različne načine urejajo to področje. V igralniških okoljih, kjer so nadzorni in varnostni pristopi ohlapni se dogaja, da se zaradi pomanjkljivosti v delovanju tega sistema pojavljajo težave, ki so povezane z goljufijami in ostalimi prevarami. Dotaknil se bom tudi igralniških procesov, kjer na operativni ravni obstajajo tveganja za nastanek škodnih pojavov.

Služba za videonadzor

Zaradi občutljivosti dela in možnih zlorab je področje videonadzora potrebno posebne obravnave. Tam, kjer se management zaveda pomena in odgovornosti službe, je z vidika varnosti in zaščite integritete zaposlenih uveljavljen profesionalen pristop. V izogib dodatnim težavam pri opravljanju dela v tej službi, je zagotovo boljši pristop, če se izvaja načelo neznane identitete zaposlenih. To načelo pa je realno le, če se ga upošteva v začetni fazi odpiranja igralnice. Nadzorna soba in ostali prostori službe morajo biti ločeni od igralnice, kar v praksi pomeni ločen vhod od ostalih zaposlenih in gostov igralnice. Zaradi "gledanja pod prste" in drugih posebnosti, služba ni ravno priljubljena med nadzorovanimi, kar se lahko izraža z različnimi pritiski ali grožnjami. Služba za videonadzor je samostojna organizacijska enota, specializirana za izvajanje nadzora igralniških procesov. Njena naloga je opazovanje in spremljanje igralniških procesov, sistematično pregledovanje in analiziranje, vrednotenje ugotovitev in informacij ter njihovo poročanje vodji službe ali korporativno varnostnem managerju[4]. Odvisno od velikosti igralnice je njuna naloga, da z vednostjo glavnega direktorja, odpravljata varnostno in postopkovno problematiko v delovnih procesih z vodji ostalih služb. Za področje videonadzora je odgovoren vodja ali korporativno varnostni manager, ki organizira in pripravlja programe za usposabljanje ter izvaja nadzor nad nalogami in aktivnostmi zaposlenih. Ker imajo zaposleni v tej službi celoten pregled nad varnostno sliko igralnice in zaradi občutljivosti dela je zelo pomemben preverjen izbor kadra, sledijo ustrezna usposobljenost, motiviranost ter sistemski in prostorski pogoji za delo. Odgovornost zaposlenih v tej službi je visoka, kajti pri delu ni sprejemljivo spreminjati odločitve. Potrebna je tudi prisotnost in zavedanje strokovne etike. Slovenska praksa kaže, da je izbor kadra mogoč iz že zaposlenih v igralnici ali od zunaj. Za profesionalen nivo formiranja službe je vsekakor boljši drugi način. Za izvajane internega usposabljanja potrebuje služba svojo učilnico[5]. Poznamo osnovno in specialistično usposabljanje, pri čemer ima svojo težo širok spekter znanja, od poznavanja igralniških

Tam, kjer se management zaveda pomena in odgovornosti službe, je z vidika varnosti in zaščite integritete zaposlenih uveljavljen profesionalen pristop.

*avtor je član Slovenskega združenja korporativne varnosti



procesov, zakonodaje in nadzora, do psihologije igralcev. Pri osnovnem usposabljanju gre za pripravo novincev za samostojno delo, medtem ko gre pri specialističnem usposabljanju za nadgradnjo znanja s področja, ki ga posameznik v osnovi najbolje obvlada. Več, kot ima služba internega znanja, lažje znotraj službe razjasni marsikatero sumljivo situacijo ter odpravi težave, ki se pojavljajo. Profesionalna organiziranost službe in ustrezna usposobljenost ter skrbno načrtovanje dela je ključnega pomena za boj proti goljufijam in ostalim deviantnim pojavom. Pri tem je seveda pomembno poznavanje tipičnih skupin igralcev in tistih, ki z vidika videonadzora spadajo v rizično skupino. Tako je mogoče pravočasno ukrepati in preprečiti ali zmanjšati že nastalo škodo. Z videonadzorom se omogoča tudi reševanje kontestacij[6], zaplete na igralnih avtomatih ter opozarjanje oz. odpravljanje napak v delovnih procesih. Vse informacije, ki izhajajo iz videonadzora, morajo biti verodostojne, saj v nasprotnem primeru služba izgublja ugled in kredibilnost. Z vidika službe je zelo pomembno, če ima služba svojega inštruktorja, ki je strokovnjak za celoten spekter iger na igralnih mizah s poznavanjem trikov in prevar in IT strokovnjaka, ki pokriva informacijsko varnost in obvladuje ostale interne sisteme. Ta posameznika sta poleg primarne usposobljenosti za delo še dodatno specializirana za omenjena področja, sledita njihovim novostim ter v internih usposabljanjih širita znanje med ostale zaposlene. Za pridobitev dovoljenja za delo v tej službi, je potrebna licenca za internega nadzornika, ki jo izdaja pristojna komisija pri Ministrstvu za finance RS.

Goljufije in ostali deviantni pojavi

Varnostna tveganja, ki v smislu goljufij in ostalih deviantnih pojavov pretijo igralnicam in igralnim salonom prihajajo tako od igralcev, kot od zaposlenih ter v njihovi navezi. Med udeleženci posebnih iger na srečo in glede na psihološke podobe igralcev so najbolj nevarni tisti, ki iščejo načine, da bi pridobili dobitke na nepošten način in ki so pri svojem početju disciplinirani. Takšne igralce lahko poimenujemo "profesionalni goljufi na dolgi rok", saj obiskujejo številne igralnice in jih je zelo težko odkriti, ker s prigoljufanimi zneski ne izstopajo. Pri ostalih profesionalnih goljufih, ki s svojim nepoštenim početjem hočejo iz igralnice odnesti velike vsote denarja, pa je samo vprašanje časa, kdaj bodo odkriti. Goljufi imajo premišljen in sistematičen način obiskovanja igralnic, kajti zelo redko se zadržijo več kot dan ali dva v eni. Za poslovanje igralnic so nevarni tudi števci kart[7] pri igri Black Jack, ki sicer ne spadajo med goljufe, vendar potrebujejo poseben strateški pristop[8]. Ker gre za zahtevno tehniko štetja, ni ravno veliko igralcev, ki bi na ta način lahko vplivali na potek igre. Pri notranji varnostni problematiki in nepoštenosti zaposlenih v igralnicah je tako, da ti izkoristijo možnosti, ker imajo dostop do sredstev. Pohlep in zadolženost ter ostale stiske pripeljejo tudi do nepoštenih in škodnih ravnanj. Nepošteni zaposleni, ki imajo dostop do denarja, do vrednostnih žetonov in dostop do pomembnih informacij, predstavljajo dodatna tveganja. Tako prihaja do sodelovanja med zaposlenimi in gosti igralnice, kjer z t.i. navezo povzročajo škodo igralnicam. Z vidika videonadzora so pomembni odgovori na vprašanja in sicer; kdo ima povod za goljufije; kdo ima možnost in dostop do sredstev ter kdo ima finančne potrebe in razloge zanje. Glede na dejstvo, da je v vseh igralniških procesih mogoče izvesti goljufije in ostale škodne pojave, je dober nadzor v igralnicah izjemnega pomena. Na operativni ravni so tveganja povsod, kjer gre za manipulacijo z denarjem, pri prenosu gotovine, pred štetjem gotovine, z igralnimi žetoni in s promocijskimi lističi do ostalih bonusov za goste. Tako poznamo goljufije in prevare povezane z igralnimi mizami, na igralnih avtomatih, pri blagajniško/trezorskem poslovanju,



marketingu in gostinstvu. Iznajdljivosti nepoštenih in pohlepnih zaposlenih ter goljufov nikoli ne bo zmanjkalo. Predvsem slednji se poslužujejo tako rokohitrskih spretnosti, kot raznih tehnološko razvitih pripomočkov in naprav, s katerimi vplivajo na potek igre. Znani so primeri pri igri Caribbean Poker in Punto Banco, ko so goljufij uporabili posebna očala, da so videli označene karte ter mikro kamere, ki so jih imeli vgrajene v mobilnih telefonih, torbicah, v prstanih, verižicah in broškah. Za igralnice in igralne salone je pomembno preventivno delovanje, ko pa pride do škodnih primerov, morajo ti biti čimprej odkriti, kajti zneski v tovrstnih pojavih nikakor niso zanemarljivi. Primeri škodnih dogodkov iz tujine namreč kažejo, da ti dosegajo milijonske vsote. Za boljši nadzor nad igranjem igralnih naprav bi bil potreben videonadzor iger, kar pomeni, da bi imele igralne naprave že v osnovi vgrajeno kamero. Glede na register dogodkov[9] je mogoče ugotoviti, da je največ škodnih primerov v igralništvu povezanih z igrami na igralnih mizah (Ameriška ruleta, Caribbean poker, Black Jack, Punto Banco, craps – igra s kockami) in sicer 58 %, sledijo igralni avtomati z 20 %, blagajniško/trezorsko poslovanje s 15 % ter ostali dogodki (ropi, ponarejeni denar v obtoku, tatvine) s 7 %.

Zaključek

Menim, da so primeri goljufij in ostali škodni dogodki v igralništvu dober pokazatelj, da je služba za videonadzor zelo pomemben segment pri zagotavljanju korporativne varnosti v igralnicah in igralnih salonih. Omenjena tveganja pri izvajanju igralniških procesov in statistika škodnih dogodkov kažejo, da teh procesov ni dobro prepuščati naključju in da je proaktivni nadzor še kako pomemben. Management sodobnih igralnic se zaveda, da profesionalni pristop k organiziranosti službe za videonadzor zagotovo prinaša pozitivne rezultate. Pri upoštevanju omenjenega so investicije v sisteme za potrebe službe in usposabljanja brez dvoma upravičene in smiselne. Zaradi splošne strategije pri obvladovanju goljufij je zelo pomembno sodelovanje z ostalimi službami znotraj igralnice, z inšpektorji iger[10] in varnostno službo. Za dobro sodelovanje med omenjenimi službami je potreben poseben pristop in razumevanje managementa, kajti dogaja se, da ta niso ravno na visoki ravni. Pomembni so postopki in pretok informacij v primerih, ko se sumijo goljufije in ostali škodni dogodki. Koristne so tudi informacije in izmenjava dobre prakse med vodji službe za videonadzor iz drugih igralnic ter širitev sodelovanja v mednarodni prostor. Zmogljivosti takšnega sodelovanja odpirajo dodatne možnosti za zmanjševanje in preprečevanje goljufij in ostalih prevar, ki se pojavljajo povsod, ne glede na velikost igralnice. Sodelovanja prinašajo koristi in dodano vrednost vsem, managementu, ki je na najvišjem nivoju odgovoren za varnost in službam, ki skrbijo za nadzor in zagotavljajo varnost v igralništvu.

1 Koncesionar je poslovni subjekt, ki je imetnik dovoljenja oz. koncesije za prirejanje posebnih iger na srečo v igralnicah in igralnih salonih.

2 V igralnici / casinoju se izvajajo posebne igre na srečo tako na igralnih mizah in sicer s krupjeji pri t.i. živi igri ter z igralnimi napravami/avtomati.

3 V igralnem salonu se izvajajo posebne igre na srečo samo z igralnimi napravami/avtomati. Samostojni saloni nimajo specializirane osebe/operativca, ki bi se ukvarjal s področjem videonadzora. Smiselna bi bila združitev funkcije z osebo odgovorno za varnost, ki pozna igralniške procese in ima ustrezno licenco ter je usposobljen za delo z video nadzornimi sistemi.

4 Pri načelu neznane identitete je njuna vloga drugačna, kot pri inšpektorjih v videonadzoru.

5 Gre za specializiran prostor v sklopu videonadzora, kjer je mogoče za namene usposabljanja izvajati igre na igralnih mizah in igralnih avtomatih.

6 Gre za spore med igralci pri igri na igralnih mizah in ko je potrebno z analizo video posnetkov ugotoviti dejansko stanje ter ga sporočiti inšpektorju iger, ki v igralnici ureja zadeve z igralci.

7 So igralci, ki lahko z določeno tehniko štetja visokih in nizkih kart premagajo igralnico.

8 Gre za metode in tehnike, ki jih igralnice uporabljajo proti števcem kart.

9 Register škodnih dogodkov avtorja članka, ki vsebuje primere goljufij, tatvin in ostalih prevar v igralništvu na podlagi zaprtih in odprtih virov.

10 Osebe, ki v igralnici neposredno izvajajo nadzor nad igralniškimi procesi. ■

Avtor: Gregor Oset / dipl. varstvoslovec, detektiv*

DETEKTIVSKA DEJAVNOST IN KORPORATIVNA VARNOST

Ko razmišljamo o korporativni varnosti in o detektivski dejavnosti, ki jo detektivi večinoma opravljamo za podjetja, ne govorimo o dveh različnih stvareh, temveč dveh zelo povezanih stvareh. Glede na naravo detektivske dejavnosti in potrebe, za katere se uporablja, bi jo lahko umestili v del varnostne funkcije podjetja.

S prepletenostjo varnostne funkcije z drugimi, kot so kadrovska, pravna, informacijska, logistična, računovodska in druge funkcije, lahko ugotovimo, da se detektivska dejavnost enako prepleta z vsemi funkcijami podjetja kot varnostna funkcija, poleg tega pa v svojem bistvu podjetjem pomaga do varnosti v različnih pomenih oziroma oblikah (glej sliko 1). Detektivska dejavnost je tako lahko pomemben element korporacijske varnosti.

Zakon o detektivski dejavnosti (ZDD-1, Ur. l. RS št. 17/2011) jo razloži s to definicijo: "Detektivska dejavnost je zbiranje, obdelava, posredovanje podatkov in informacij ter svetovanje na področju preprečevanja kaznivih ravnanj, ki ga za naročnikove potrebe opravlja po tem zakonu detektiv, ki ima izdano licenco in izpolnjuje pogoje v skladu s tem zakonom." Že iz drugega dela definicije vidimo, da je detektivska dejavnost lahko neposredno vpeta v osnovno varnostno funkcijo v smislu varovanja oseb in premoženja, saj vključuje „...svetovanje na področju preprečevanja kaznivih ravnanj...". Vpetost detektivske dejavnosti v praktično vse funkcije podjetja, kadar za to obstaja potreba, pa kaže prvi in osnovni del definicije, ki je: „detektivska dejavnost je zbiranje, obdelava, posredovanje podatkov in informacij..." Točne informacije so namreč potrebne v celotnem poslovanju posameznega podjetja.

Tako smo ugotovili, da bi glede na pomen, ki ga detektivska dejavnost ima za podjetje, če je le-to prepoznalo njeno koristnost in jo zna uporabiti, le-to lahko uvrstili k varnostni funkciji podjetja. Samo zbiranje informacij, kar je osnovno področje dela v okviru detektivske dejavnosti, sicer največkrat ni neposredno povezano z varovanjem v ožjem pomenu besede, je pa najpogosteje povezano z varnostjo v širšem pomenu.

V smislu zgornjega razmišljanja o detektivski dejavnosti kot delu varnostne funkcije podjetja bi lahko tudi razumeli eno izmed bistvenih sprememb, ki jih je prinesel nov Zakon o detektivski dejavnosti iz leta 2011. Medtem, ko smo po prejšnji zakonodaji detektivi svojo dejavnost opravljali kot svoboden poklic, bodisi individualno, bodisi v detektivski družbi (ki je bila lahko samo osebna, ne pa tudi kapitalska družba), je ZDD-1 iz leta 2011 prinesel v zvezi s tem nekaj sprememb. Detektivom je prinesel želeno možnost organiziranja detektivske družbe kot kapitalske družbe, tako da ni več omejitev v zvezi z ustanavljanjem detektivske družbe kot npr. družbe z omejeno odgovornostjo. ZDD-1 pa v svojem tretjem členu, ki opredeljuje obliko dela detektivov, poleg detektivske dejavnosti kot svobodnega poklica, določa tudi možnost, da lahko detektivsko dejavnost opravlja pravna ali fizična oseba, ki ima:

- kot poslovni subjekt v Poslovnem registru Slovenije vpisano detektivsko dejavnost;
- v delovnem razmerju detektiva in
- zavarovano odgovornost za škodo.

Tako je ZDD-1 omogočil opravljanje detektivske dejavnosti podjetjem pod pogojem, da imajo registrirano poizvedovalno dejavnost, zaposlenega detektiva in zavarovanje odgovornosti v skladu s tem zakonom. Tako lahko dejansko v skladu s pozitivno zakonodajo vsako podjetje, ki izpolnjuje navedene pogoje, opravlja detektivsko dejavnosti oziroma v okviru podjetja le-to opravlja detektiv(i), ki je (so) zaposlen(i).

Če gre za večje podjetje ali korporacijo, bi imel detektiv nedvomno veliko nalog tudi znotraj svojega podjetja, in bi v praksi opravljal storitve (tudi) za lastne potrebe oziroma potrebe svojega delodajalca. Še vedno sicer obstajajo določila, za kaj se lahko detektivska dejavnost uporablja in kakšni so pogoji (detektiv lahko zbira podatke le na podlagi pisnega pooblastila in v okviru pooblastila ter za točno določene naloge), tako da nikakor ne moremo govoriti o kakršnemkoli „vohunu" v podjetju, res pa je, da bi lahko napisali nov članek o tem, ali je bolje uporabiti „svojega" detektiva ali zunanjega izvajalca, ki ga notranji ne poznajo. V zvezi s tem pa je tako treba upoštevati osnovno izhodišče pri detektivskem delu, da je vsaka situacija različna in je

*avtor je član Slovenskega združenja korporativne varnosti



Če preidemo na praktične vidike detektivske dejavnosti in na povezanost z različnimi poslovnimi funkcijami podjetij, lahko začnemo pri kadrovski funkciji podjetja. S to funkcijo je namreč povezano vsekakor v javnosti najbolj izpostavljeno detektivsko delo, najbrž pa tudi eno izmed najpogostejših detektivskih opravil v Sloveniji.

treba vedno znova presojati tveganja in možnosti za uspeh.

ZDD-1 je sicer žal izpustil možnost zbiranja podatkov o kandidatih za zaposlitev (v okviru pisnega soglasja kandidata), čeprav sem prepričan, da je to lahko eno izmed pomembnih orodij za omejevanje tveganja v procesu odločanja pri zaposlovanju novih kadrov. Še tako usposobljen kandidat za delovno mesto, bodisi da gre za vodstvena delovna mesta ali pa tudi za nižja delovna mesta, ni nujno dober kandidat, če je možno ugotoviti, da ima težave s poštenostjo in dobronamernostjo (npr. ugotovljene tatvine pri nekdanjem delodajalcu, nagnjenost k zlorabam poslovnih skrivnosti ipd.). Kot je že omenjeno, v novem zakonu možnosti za preverjanje kandidatov za zaposlitev ni več, je pa pogosto opravljanje poizvedb in zbiranja informacij v zvezi z zlorabami pravice do zadržanosti z dela zaradi bolezni ali poškodbe, zlorabah uveljavljanja pravice do povračila stroškov prevoza na delo in z dela, dela pod vplivom alkohola (ali prepovedanih drog) ter o drugih disciplinskih kršitvah in kršilcih. S kadrovsko funkcijo je povezano tudi zbiranje podatkov o spoštovanju konkurenčne prepovedi, pa tudi o spoštovanju konkurenčne klavzule, ki se, tako kot v določeni meri tudi druge kadrovske stvari, navezuje tudi na pravno funkcijo podjetja. V isto področje bi lahko tudi uvrstili vročanje, saj se za podjetja pogosto vročajo pisanja zaposlenim po Zakonu o pravdnem postopku.

V Sloveniji je namreč dokaj običajno detektivsko delo pridobivanje informacij o dolžnikih in njihovem premoženju ter o dokaznem gradivu in dejstvih, potrebnih za zavarovanje ali dokazovanje pravic in upravičenj stranke pred sodišči, drugimi pravosodnimi organi in drugimi organi oziroma organizacijami, ki v postopkih odločajo o teh pravicah.

Tako lahko detektiv s svojim delom, najsi gre za pridobivanje podatkov iz uradnih evidenc, ali za terensko zbiranje informacij, bistveno pripomore k uspešnosti pravne funkcije podjetja, saj le-tej zagotavlja potrebne informacije za zagotovitev uspešnosti postopkov, bodisi kadrovskih, izvršilnih ali odškodninskih tožb. Zavedati se je namreč treba, da zanašanje le na podatke, ki jih pridobi sodišče, ni optimalno, saj se dejansko stanje pogosto razlikuje od podatkov v različnih evidencah. Glede na to, da se lahko detektiv z dolžnikom pogovarja tudi o tem, kdaj in kako bo dolg poravnan (ni namreč nujno, da so pridobljeni podatki le za sodni postopek), pogosto prispeva tudi k uspešnosti finančne funkcije podjetja, saj lahko zaradi hitrejših poplačil dolžnikov, bodisi fizičnih bodisi pravnih oseb, ali s pomočjo dobljenih sodnih postopkov (tožb), izboljša finančni tok v podjetju. Poleg tega se pri dolžnikih

Precej pogosta je lahko detektivska dejavnost tudi kot del pravne in finančne funkcije podjetja.

velikokrat srečujemo tudi z goljufivimi nameni le-teh, kar je tudi potrebno pravočasno prepoznati in tudi tukaj so lahko prave informacije še kako pomembne. Da gre pri neplačilih pogosto tudi za namerno goljufijo, bodisi navadno ali poslovno, potrjuje tudi izjava enega izmed odvetnikov, ki mi je ravno dan pred pisanjem članka dejal, da ga stranke večinoma sprašujejo, kako naj ne plačajo. Ob uspešnem pridobivanju podatkov v zvezi s poslom in vzroki za neplačilo je marsikdaj tudi možnost hitrejšega poplačila dolžnika, namesto da se le čaka na uspešnost izvršilnega postopka.

O podjetjih imamo sicer običajno dostopnih kar nekaj podatkov. V Sloveniji so od maja dostopni finančni podatki vseh podjetij, ki so za preteklo leto oddala svoje podatke Ajpesu. Te podatke lahko imamo za relativno ažurne, v določenih primerih pa so lahko tudi zelo zastareli, saj je lahko dogajanje v podjetju v tem letu povsem drugačno, kot v preteklem. V preteklosti je bilo namreč mnogo podjetij, ki so par let gradila svoje bilance z namenom, da so lahko na njihovi podlagi izpeljala poslovne goljufije v letu, ko dejansko svoje dejavnosti niso več opravljala. Tako je lahko pomembno tudi preverjanje poslovnih partnerjev, kar se izvaja tako v Sloveniji, kot tudi v tujini.

V proizvodno tehnični in razvojni funkciji so različna tveganja in sicer od tatvin v postopku proizvodnje, bodisi polizdelkov ali celotnih produktov, do izgube pomembnih tehničnih in razvojnih podatkov, ki lahko pomeni znaten, včasih tudi usoden udarec za podjetje. Vse te situacije so stvar korporativne varnosti in urejenosti varnostnega področja v podjetju, varnostni manager pa lahko na podlagi svoje ocene vključi detektiva bodisi pri preprečevanju tveganja, ali pa pri ugotavljanju in dokazovanju že nastale škode in preprečevanju novih škod.

Čeprav detektivi tudi v skladu z ZDD-1 lahko pridobivamo informacije o uspešnosti in poslovnosti poslovnih subjektov, menim, da ta del še ni dovolj uveljavljen v miselnosti poslovne sfere v povezovanju z dojemanjem detektivske dejavnosti. Mnogo tujih korporacij ima detektivsko dejavnost vključeno tudi v tržno funkcijo podjetja, saj se zavedajo, kakšnega pomena je sodelovanje z dobrim poslovnim partnerjem, ki trži njihove produkte ali storitve in kaj lahko pomeni sodelovanje s slabim poslovnim partnerjem, pri čemer ni nujno govora le o plačilni nedisciplini, temveč tudi o drugih neželenih vplivih na podjetje, od slabega slovesa do potencialnih oblastnih posegov oziroma sankcij raznih institucij.

Predvsem pri mednarodnem poslovanju vsako podjetje ne more vedno enostavno in pravilno oceniti potencialnega poslovnega partnerja na drugem kontinentu, je uporaba poizvedb v zvezi s poslovnostjo posameznega subjekta lahko izredno pomembna.

Glede na to, da ni nujno, da je naročnik detektivskih storitev vodstvo podjetja, je mogoče tudi pridobivanje informacij o vodstvu, saj je lahko naročnik detektivske storitve lastnik podjetja, če sumi, da poslovodstvo krši svoje obveznosti. S strani lastnikov slovenskih podjetij sicer sam ne opažam mnogo teh primerov, sem pa že imel primere s tujimi lastniki podjetij, pa tudi na primer s strani tujega stečajnega upravitelja, ki ga je zanimalo, kam se je prodal stroj iz neke tovarne v Sloveniji, ki je bila v tuji lasti. Glede na mnoga oškodovanja upnikov v okviru prisilnih poravnav in stečajnih postopkov lahko z dokaj veliko verjetnostjo predvidevam, da je na tem področju bilo in še vedno je veliko prostora za pridobivanje podatkov, ki bi jih stečajni upravitelji lahko koristno uporabili v svojih postopkih.

V zaključku prispevka, v katerem sem poskušal skozi prikaz dejanskega stanja detektivskega dela orisati uporabnost in pomen te dejavnosti v okviru korporacijske varnosti na splošno, bi rad poudaril, da je pri informacijah običajno pomembno, da so čim bolj točne in tudi pravočasne, za to pa je tudi potrebno, da se jih pravočasno pridobi. Prav zaradi tega je uspešnost našega dela lahko večja, če varnostni manager prepozna uporabnost detektivskega dela do te mere, da se zaveda, kdaj je smiselno v reševanje situacij, s katerimi se srečuje, vključiti detektivske storitve in na kakšen način, da bo sodelovanje čim bolj uspešno. ■



Slika 1. Varnostna funkcija v podjetju kot poslovnem sistemu (Vršec,1993) (rdeča črtkana črta predstavlja detektivsko dejavnost, ki je (občasen) del varnostne funkcije podjetja).

Avtor: Marko Potokar / državni nadzornik za varstvo osebnih podatkov,
Urad informacijskega pooblaščenca*



SISTEM UPRAVLJANJA VAROVANJA INFORMACIJ V ORGANIZACIJAH Z VIDIKA KORPORATIVNE VARNOSTI

Popolnoma jasno nam je, da je ustrezna informacijska infrastruktura postala odločilen dejavnik, ki pripomore k uspehu organizacije. Hkrati se vse bolj zavedamo pomembnosti varovanja informacij, ki mora postati del življenjskega cikla v razvoju in vzdrževanju informacijskih sistemov.

Varovanje informacij pojmujemo kot zaščito le-teh pred raznovrstnimi grožnjami. S tem se zagotovi neprekinjeno poslovanje, zmanjša poslovno tveganje ter doseže kar največji dohodek iz naložb in poslovnih možnosti. Če preletimo zahteve, ki jih določajo zakoni, predpisi in standardi, bi lahko celo rekli, da je v nekaterih okoliščinah varnost podatkov pomembnejša od podatkov samih.
Pri elektronskem poslovanju lahko kot bistvene zahteve za zagotavljanje konkurenčne prednosti navedemo pravočasen in natančen dostop do podatkov, neprekinjeno razpoložljivost sistemov, varno hranjenje poslovnih in zaupnih podatkov (osebni podatki strank, podatki o transakcijah, plačilnih in kreditnih karticah ipd.), potrebo po hitrem razvoju novih sistemov in kot pomembno prodajno pot tudi ponujanje izdelkov in storitev preko interneta. Elektronsko poslovanje je omogočilo nove poslovne poti, ki se zanašajo na učinkovit program za varovanje informacij, s katerim si lahko podjetje pridobi zaupanje strank.
Zakonodaja in regulativa, tako vladna kot industrijska, se še naprej razvijata in skušata zaščititi potrošnike in podjetja, ki poslujejo elektronsko. Pri nas sta poleg ostalih (ZEPEP, ZASP, kazenski zakonik, Zakon o tajnih podatkih, ZVDAGA idr.) najbolj odmevna Zakon o varstvu osebnih podatkov, ki predpisuje organizacijske, tehnične in pravne postopke in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi osebnih podatkov ter varnostni standard ISO/IEC 27001/2, ki med drugim podaja zahteve po preverjanju istovetnosti uporabnika, kontroli dostopa ter zagotavljanju razpoložljivosti in celovitosti podatkov.

Sistem upravljanja varovanja informacij (SUVI)

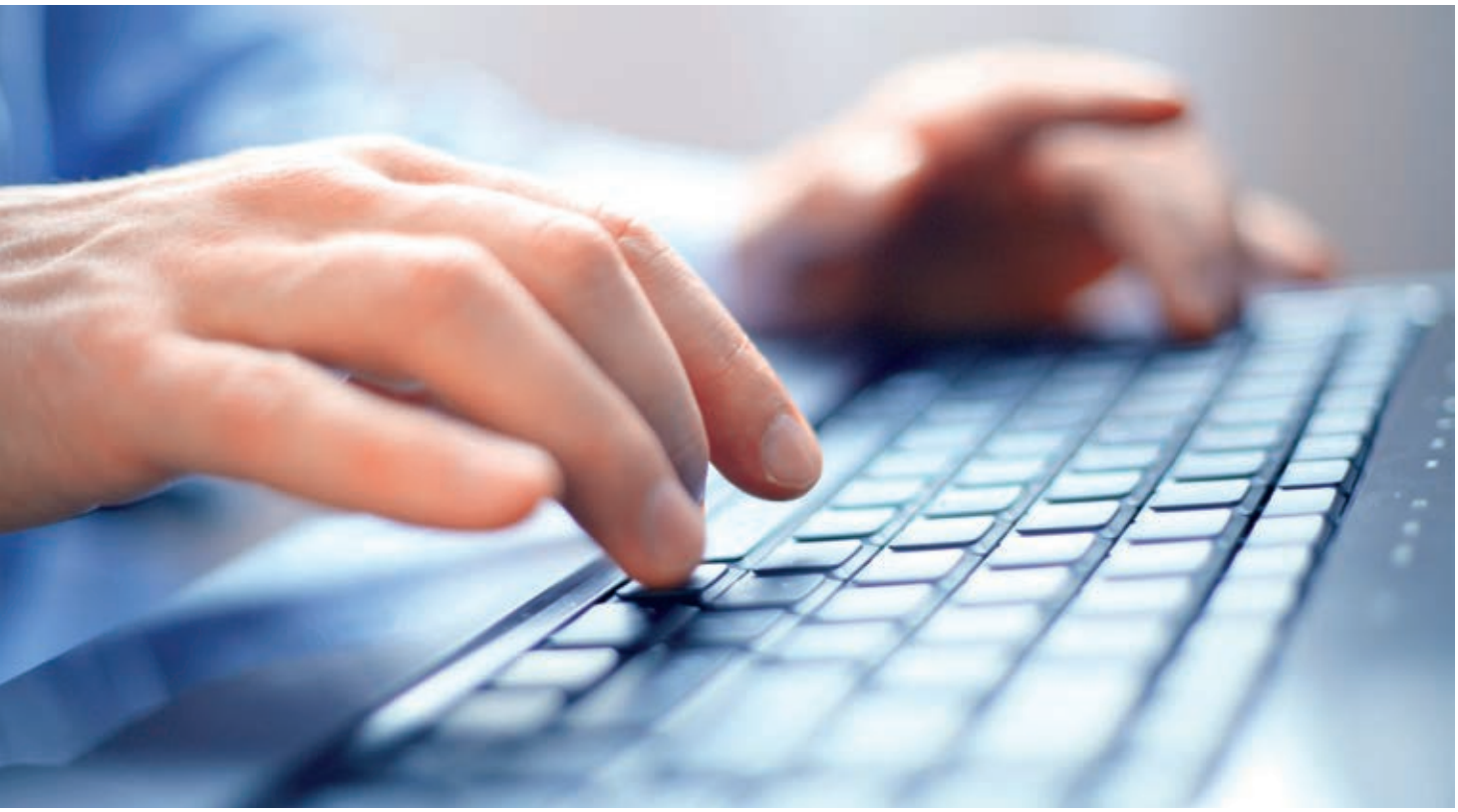
Pri uveljavljanju varnostnih zahtev oziroma vpeljavi sistema upravljanja varovanja informacij (SUVI) mora organizacija prepoznati svoje varnostne potrebe. Kodeks najboljše prakse ISO/IEC 27002 navaja tri glavne vire varnostnih zahtev:

-ocena tveganja, s katero prepoznamo grožnje, ki ogrožajo sredstva organizacije, ovrednotimo ranljivost in verjetnost pojava ter predvidimo možne posledice,
-niz načel, ciljev in poslovnih zahtev za obdelavo informacij, ki jih razvije organizacija v podporo svojim poslovnim procesom,
-zahteve, ki jih določajo zakoni, statuti, predpisi in pogodbe ter jih morajo izpolnjevati organizacija, njeni poslovni partnerji in okolje v katerega je umeščeno poslovanje organizacije.

SUVI kot proces

Pri upravljanju varovanja informacij se srečamo s procesnim pristopom. Upravljanje je proces, ki ima vhode in ima 'procesni del', ki le-te pretvarja v izhode. Proces varovanja informacij popišemo z znanim krogom PDCA (**P**lan, **D**o, **C**heck, **A**ct), ki zagotavlja nenehno nadzorovanje in izboljševanje procesa varovanja informacij. S procesnim pristopom se pravzaprav srečamo že pri vzpostavitvi sistema upravljanja varovanja informacij. Pri

*avtor je član Slovenskega združenja korporativne varnosti



analizi tveganj. Začnemo namreč s popisom informacijskih virov, ki jih nato umeščamo znotraj procesov. Seveda moramo pri tem popisati in določiti tudi ustrezne procese, v katerih sodelujejo opredeljeni informacijski viri. Pri tem ni vedno najboljši način, da izhajamo iz organizacijske sheme organizacije. Včasih je bolj smotrno procese oblikovati glede na vsebino, glede na izvajanje posameznih funkcij znotraj organizacije. Seveda pri tem ne smemo pozabiti na določitev lastnikov posameznih procesov. Šele ko smo opredelili procese sledi popis informacijskih virov, njihovo razvrščanje in umeščanje v procese. Nadaljujemo seveda z ocenjevanjem tveganj, katerega del je tudi vrednotenje virov, določitev ranljivosti in groženj ter opredelitev višine posameznih tveganj. Sledi obravnava tveganj, katere cilj je zmanjšanje nesprejemljivih tveganj na raven, določeno s kriterijem sprejemljivosti. Zmanjševanje dosežemo z izbiro ustreznih nadzorstev, lahko pa tudi z zavarovanjem tveganj pri zavarovalnici ali s prenosom tveganj na drugo osebo. Sledi izjava o primernosti, v kateri navedemo katera nadzorstva (kontrole) varnostnega standarda ISO/IEC 27001 smo pokrili in katere ne ter zakaj. Sledi izdelava načrta obravnave tveganj, ki predstavlja formalni načrt za uvajanje ukrepov za zmanjševanje tveganj. V njem med drugim opredelimo odgovornosti za obravnavo tveganj, prioritete, cene ukrepov, potrebne nove tehnologije, potrebno delo za vpeljavo in izobraževanje ter terminski rok izvedbe. Rezultati obravnave tveganj samo opredeljujejo, katera nadzorstva potrebujemo, v načrtu obravnave pa podrobneje opredelimo in ovrednotimo izbrano možnost obravnave tveganja. Ugotoviti želimo natančno, kako bomo zmanjšali tveganje in koliko nas bo to stalo. Cena morda zahteva ponovno potrjevanje upravljanja. Obravnava tveganj, ki je bila na prvi pogled najprimernejša, tako ni najustreznejša in jo moramo izboljšati ali spremeniti. Vrnemo se na točko obravnave. V tem primeru uporabimo krog izboljševanja (PDCA) za doseganje pričakovanih ciljev upravljanja. In vse skupaj se zavrti v nov krog.

Na upravljanje varovanja informacij lahko torej gledamo kot na vzpostavitev in vzdrževanje sistema za zagotavljanje usklajenosti strategije varovanja informacij s poslovnimi cilji organizacije in skladnosti z veljavnimi zakoni in predpisi. Tako je pri vzpostavitvi SUVI potrebno identificirati obstoječe in možne pravne in druge regulatorne zadeve, ki vplivajo na varovanje informacij in oceniti njihov vpliv na poslovanje organizacije.

Vloge in razmerja v procesu SUVI

Varnost oziroma zaščito informacij pred raznimi grožnjami dosežemo z vpeljavo ustreznih kontrol oziroma nadzorstev, ki obstoječa tveganja zmanjšajo na sprejemljivo raven. Seveda morajo biti izbrana taka nadzorstva, ki so v skladu z državnimi in mednarodnimi zakoni in predpisi. ISO/IEC 27002 kot ključna nadzorstva (z zakonskega vidika), ki so pomembna za organizacijo navaja zaščito podatkov in varstvo osebnih podatkov, zaščito organizacijskih zapisov in pravico do zaščite intelektualne lastnine.

Kot glavni in odgovorni za uspešno in učinkovito upravljanje SUVI, mora imeti upravljavec varovanja informacij (angl.: **C**hief **S**ecurity **O**fficer) po-

leg specifičnih znanj (kot so znanja s področja standardov za upravljanje varovanja informacij, poznavanje metodologije oblikovanja in izvajanja standardov, poznavanje metodologije izvajanja varovanja in nadzorov, poznavanje strategije poslovanja in poslovne politike podjetja, poznavanje IT področja ipd.) tudi znanja s pravnega področja. Ker upravlja tudi z zagotavljanjem skladnosti z zakonodajo in ostalimi pravnimi zahtevami v zvezi z varovanjem informacij, mora poznati pravne in regulatorne zadeve povezane s prenosom podatkov, šifriranjem, varovanjem osebnih podatkov, upoštevanjem avtorskih pravic, varovanjem poslovnih skrivnosti itd.

Seveda upravljavec informacijske varnosti praviloma nima formalne izobrazbe pravne smeri, ampak je veliko 'raje' izobražen s področja t.i. tehničnih ved (računalništvo, informatika ipd.). Tudi njegova predhodna profesionalna kariera je najpogosteje vijugala po virtualnih poteh računalniških in informacijskih svetov, ne pa v gozdovih zakonov in pravil ter njihovih interpretacij.

Ker je iluzorno pričakovati, da bo upravljavec varovanja informacij popoln strokovnjak na vseh področjih (in s tem tudi na pravnem), si lahko zamislimo, da si pri svojem delu, ki zadeva pravno področje, pomaga z nasveti in komentarji pridobljenimi s strani ustreznih strokovnih oseb oziroma služb. Tako se v trikotniku CEO/CIO/CSO pojavi še ogljišče LO (angl.: **L**aw-**O**ffice; slov.: pravniška pisarna), ki v obstoječe odnose (ki so po definiciji konfliktni) pristavi še svoj lonček interesov. Tako vloga upravljavca varovanja informacij postane še kanček težja, saj je ponavadi on tisti, ki pred vodstvom podjetja (CEO, CIO) zastopa tudi interese pravne službe. Tako postane upravljavec informacijske varnosti v očeh CEO in CIO še bolj moteč element v procesu doseganja ciljev organizacije: v informacijski sistem organizacije je ponavadi potrebno vgraditi še kakšno 'nepotrebno' varnostno funkcionalnost, kar seveda za seboj potegne dodatne stroške; hkrati je potrebno sprejeti še kakšno popravljeno varnostno politiko (če že ne napisati nove), s tem pa ponavadi posežemo v obstoječe organizacijske odnose in pravila ter tako povzročimo še nezadovoljstvo zaposlenih.

V takem okolju je toliko bolj pomembno zavedanje, da je za organiziranost, nadzor delovanja, zagotavljanja virov in razvoj celovitega upravljanja z informacijskimi tveganji odgovorno najvišje vodstvo organizacije, ki določa politiko ter cilje in je odgovorno za nadzor nad delovanjem sistema in koordinacijo vseh področij. Vodstvo organizacije tudi načrtuje in zagotavlja vse potrebne vire (človeške, finančne, materialne, informacijske), vključno s primerno infrastrukturo in delovnim okoljem, za učinkovito delovanje sistema. Za samo izvedbo politike in načrtov pa je seveda operativno odgovoren upravljavec varovanja informacij, v okviru danih možnosti, virov in sredstev.

Tako je še toliko bolj pomembno, da se s strani vodstva izražena zavezanost in podpora varovanju informacij kot pomembni poslovni aktivnosti organizacije, zapiše tudi v krovni varnostni politiki organizacije.

Spremljanje delovanja SUVI

Spremljanje vpeljanega SUVI je eden izmed najpomembnejših vidikov zagotavljanja varnosti informacijskih virov, čeprav mu navadno v zaključevanju procesa varovanja posvečamo premalo pozornosti. Ponavadi po vpeljavi varnostnih nadzorstev, ki izhajajo iz analize informacijskih tveganj, organizacije domnevajo, da je proces varovanja zaključen. Pri tem pa pozabljajo, da vpeljana nadzorstva zahtevajo neprestano spremljanje, ki zagotavlja, da leta delujejo in bodo še naprej delovala na zahtevan in pravilen način. Usmerjenost v nadzor nad učinkovitostjo izvajanja sistema vodenja varovanja informacij se kaže v zahtevi standarda ISO/IEC 27001, da je potrebno vzpostaviti in vzdrževati dokumentirane postopke za načrtovanje in izvajanje **notranjih presoj**, ki morajo postati sestavni del vsakega programa vzpostavitve, vzdrževanja in razvoja sistema vodenja varovanja informacij.

Vpeljana varnostna nadzorstva lahko delujejo učinkovito le pod pogojem njihovega preverjanja v realnem poslovnem življenju. Pri spremljanju varnostnega sistema je potrebno aktivnosti preverjanja sistematično načrtovati, odkrivanj zastarelih varnostnih nadzorstev oziroma tistih, ki delujejo v neskladju s predvidenimi zahtevami pa ne prepuščati naključju.

V prvi fazi spremljanja SUVI gre za zagotavljanje ustrezne funkcionalnosti varnostnih nadzorstev, kasneje pa tudi za spremljanje učinkovitosti ali šibkosti storitev in vpeljanih zaščit. Spremljanje vpeljanega varnostnega sistema naj bi take šibkosti odkrilo in omogočilo ustrezne akcije za odpravo oziroma izboljšanje le-teh.

Standard ISO/IEC 27001 zajema spremljanje vpeljanega SUVI v tako imenovani fazi *preveri (Check)*, kjer določa načine njegovega spremljanja. Faza *preveri* zagotavlja akcije za uspešno delovanje varnostnih nadzorstev, opis postopkov za upravljanje in delovanje teh nadzorstev in opis procesov za sprotno pregledovanje tveganj glede na spremembe tehnologije ali pojavitev novih groženj. Prihodnje spremembe je možno predvidevati le ob pozornem spremljanju tehnologije, poslovnih zahtev in pojavu novih groženj in tveganj. V krogu PDCA sodi torej notranja presoja v fazo *preveri*, hkrati pa, upoštevajoč popravne ukrepe, ki iz nje izhajajo, tudi v fazo *ukrepaj (Do)*.

Poleg notranje presoje obstajajo še drugi načini preverjanja, kot so: *rutinsko preverjanje, samoupravljalni postopki* in *vodstveni pregledi*. Pri *rutinskem preverjanju* gre za izvajanje spremljanja SUVI kot del običajnega poslovnega procesa, na primer preverjanje, da ne pride do nenamernih ali nepooblaščenih sprememb v nastavitvah, podatkih in podobno. *Samoupravljanje* je vrsta nadzora, ki omogoča zaznavo kakršne koli napake med delovanjem opreme ali izvajanjem nekega procesa, namen *vodstvenih pregledov* pa je, da se najmanj enkrat letno preveri, ali je SUVI učinkovit, možnosti za njegove izboljšave in morebitne dodatne ukrepe.

Zaključek

Pogosto v strokovni literaturi pri definiciji varnostnega sistema naletimo na navedbo, da varnostni sistem sestavljajo naslednje komponente: pravila in postopki, tehnologija in človek (ljudje). Pravila predstavljajo okvir sistema, postopki opišejo procese, tehnologija zagotavlja (pravzaprav podpira) skladnost s pravili, človek pa postopke izvaja.

Imejmo pa v mislih, da ima v tem razmerju človek globljo in širšo vlogo. Kot izvajalec je sestavni del (element) varnostnega sistema, obenem pa je tudi tvorec pravil, postopkov in tehnologije. Glede na to, da je celoten varnostni sistem prežet s človekovim (ne)delovanjem lahko trdimo, da je človek bistvena komponenta varnostnega sistema. ■

SOLARNI MODULI BAUER

Podjetje Solar Tehnik d.o.o. zastopa priznanega nemškega proizvajalca solarnih modulov Bauer, ki daje velik poudarek kakovosti in učinkovitosti, vse od izbire materiala pa do proizvodnje in dobave. Solarni moduli so tekom proizvodnje izpostavljeni zahtevnim testom za preverjanje kakovosti materiala in izdelave. V Bauerjevem lastnem logističnem centru se opravi naključen preizkus modula, ki je pripravljen za odpremo. Omenjeni nemški proizvajalec dela na tem področju že dobrih 27 let, kar je med drugim tudi garancija za kakovost proizvodov.

Lastnosti solarnih modulov Bauer:

- 10 let garancije za izdelek,
- garancija za zmogljivost – najmanj 90 % več kot 10 let in najmanj 80 % preko 25 let,
- zagotovljen pozitiven učinek tolerance (+3 %) izhodiščne moči za vse serijske modele Bauer,
- pred strogimi okoljskimi vplivi jih ščiti obloga iz ojačenega stekla in EVA folije, na zadnji strani pa je obloga PET folije,
- visoko kakovost zagotavljajo parni preizkusi, preizkusi izpostavitve različnim obremenitvam in simulacija menjalnih ciklov spreminjanja temperature,
- pred vsako odpremo strokovnjaki preizkusijo naključno izbran modul, kot to predpisujejo IEC 61215, IEC 61730-1, -2: 2004 in EN 61730-1, -2: 2007,
- članstvo v PV krogu zagotavlja tudi ekološko deponiranje zastarelih modulov,
- različni certifikati, od TUV, MCS, UL do VDE,RAL odvisno od serijskega modela



Solarni moduli Bauer so plod vrhunske nemške tehnologije in priznane evropske kvalitete.

ULIČNE SOLARNE SVETILKE

Inženirji podjetja Solar Tehnik d.o.o. so razvili ulične solarne svetilke, ki prejemajo energijo za razsvetljavo preko njihovih solarnih modulov. Čez dan se omenjene svetilke polnijo s solarno energijo, ponoči pa se ta energija uporablja za razsvetljavo, torej delujejo neodvisno od distributerja električne energije.

Lastnosti uličnih solarnih svetilk STS-30/90 LED

- svetlo in zanesljivo, brez oskrbe z električno energijo,
- svetilnost je cca 150 W halogenske luči,
- solarni moduli: mono-kristalni silicij (kaljeno steklo) zagotavljajo visoko kakovost in dolgo življenjsko dobo – cca. 25 let,
- mikroprocesor optimiziran za polnjenje baterije in nadzor razsvetljave,
- nadzorni sistem razsvetljave je zlahka dostopen.
- visoka kakovost 12 V baterij, brez vzdrževanja, dolga življenjska doba,
- prenapetostna zaščita in nizko stanje baterije,
- maksimalno obratovanje tudi v oblačnem vremenu,
- razred energijske učinovitosti: A+++ ,
- praktično brez vzdrževanja – solarne celice je potrebno le občasno očistiti z vodo.



Podjetje Solar Tehnik d.o.o. bo v času od 12. do 18. septembra razstavljalo solarne module Bauer in ulične solarne svetilke na sejmu MOS v Celju. Vljudno vabljeni!

Avtor: Blaž Ivanc / vodja razvoja Elmar d.o.o., Žalec*



UPORABA DREVESA NAPADOV PRI VAROVANJU ZASEBNOSTI

Pojem zasebnost še nikoli ni bil tako izpostavljen, kot je v današnjem času. Kljub številnim raziskavam s področja zasebnosti so nekateri avtorji mnenja, da je premik k zaostritvi zahtev po varovanju zasebnosti še vedno premajhen.

Z razvojem informacijskih tehnologij, porastom informacijskih sistemov in povezovanjem podatkovnih baz je informacijska zasebnost postala precej izmuzljiv pojem. Če predpostavimo, da je izguba zasebnosti podobna enosmerni funkciji ter da je vsak informacijski sistem teoretično ranljiv, se bo zavest o varovanju zasebnosti v prihodnje še stopnjevala. Namen članka je predstaviti uporabnost metode drevesa napadov pri varovanju zasebnosti.

Internet Engineering Task Force [IETF] (2007) definira grožnjo kot potencial za kršitev varnosti, ki obstaja, ko je prisotna okoliščina, sposobnost, akcija ali dogodek, ki bi lahko ogrozil varnost in povzročil škodo. Reddy in ostali (2008) predstavijo metodologijo sedmih različnih groženj zasebnosti:
Povezljivost – omogoča napadalcu, da uspešno loči, če so zapisi (lahko pa tudi osebe, sporočila, aktivnosti ...) med seboj povezani ali ne.

Razpoznavnost – omogoča, da napadalec uspešno identificira predmet (npr. osebo), na katerega se nanaša zapis ali sporočilo. Razpoznavnost je grožnja anonimnosti.
Nezmožnost zanikanja – napadalec zbere dokaze, s katerimi onemogoči zanikanje nasprotne strani, da nekaj ni bilo narejeno, izrečeno ...
Odkrivanje – napadalec uspešno ugotovi, če nek predmet zanimanja obstaja ali ne.

Za zagotavljanje zasebnosti pri hrambi podatkov uporabljamo različne varnostne ukrepe, kot so šifriranje, nadzor dostopa in varnostno beleženje. Vsi ti ukrepi pa so konstantno podvrženi različnim napadom. Z uporabo metod za modeliranje napadov lahko izboljšamo varovanje zasebnosti pred obstoječimi in nastajajočimi grožnjami.

Razkritje informacij – razkritje občutljivih informacij posameznikom, ki ne bi smeli imeti dostopa do njih.
Nepoznavanje vsebine – uporabnik nevede razkrije preveč osebnih podatkov, kar omogoča napadalcu, da enostavno pridobi uporabnikovo identiteto, ali se ne zaveda zastarelosti in nepravilnosti shranjenih podatkov.
Neskladnost pravil in soglasij – lahko pripelje do razkritja občutljivih informacij, ker ni zagotovila, da se bo res ravnalo v skladu s predhodno predstavljenimi varnostnimi pravili.

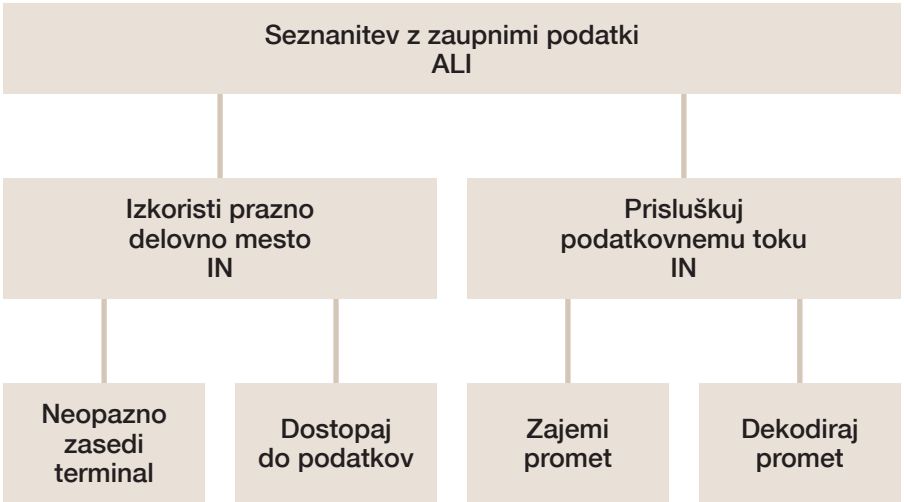
Grožnja zasebnosti, kakršna je razpoznavnost, lahko nastane kot posledica procesne napake, kljub zasnovi nekega postopka, ki načeloma zagotavlja zasebnost posameznika, lahko napadalec s podatkovnim rudarjenjem identificira predmet, ki se ga je želelo skriti. Whalen (2012) ugotavlja, da je odstranjevanje določenih občutljivih podatkov pogostokrat nezadostno, da bi dosegli anonimnost posameznika.

Razkritje informacij je temeljna grožnja zasebnosti, ki bo kasneje obravnavana v članku. Pri izvedbi te grožnje je tarča lahko proces, podatkovni tok ali hramba podatkov. Hramba podatkov je pogosta tarča napadov in izpostavljena različnim varnostnim grožnjam. Kotzanikolaou in Douligeris (2007) razdelita varnostne grožnje hrambe podatkov na: razkritje podatkov, sprememba podatkov, neavtoriziran dostop do podatkov, ilegalna raba podatkov, predolga hramba podatkov in pomanjkanje odgovornosti.

Modeliranje z metodo drevesa napadov

Drevo napadov se uvršča med formalne metode za modeliranje napadov (Camtepe, Bulent, 2007). Metoda se lahko uporablja v različne namene, vendar je največkrat prisotna za ocenjevanje obstoječe varnostne politike. Namen drevesa napadov je z analizo

*avtor je član Slovenskega združenja korporativne varnosti



Slika 1. Primer grafične predstavitve drevesa napadov.

ugotoviti ključne dejavnike, ki vplivajo na varnost in sprejem potrebnih varnostnih ukrepov (Li in ostali 2010). Drevo napadov predstavimo grafično ali tekstovno. Koren drevesa predstavlja glavni cilj napadalca, vmesna vozlišča podcilje, končna vozlišča ali listi pa dejanja, ki jih napadalec izvede za uresničitev cilja. Vozlišča, ne pa tudi listi, imajo dve »boolovi« operaciji: konjunkcija (IN) in disjunkcija (ALI). Vozlišča pod korenom drevesa tako predstavljajo sredstva za dosego glavnega cilja. Pri uporabi modela je potrebno razmišljati izven enostavnih okvirov obravnave napadov, četudi je zato napad obsežen, zahteva visoko specializacijo v obliki znanja in uporabo nevsakdanjih tehničnih orodij, kakor tudi, če izvedba napada predstavlja zajeten finančni zalogaj. Drevo napadov omogoča modularno oblikovanje in s tem razdelitev posameznih delov drevesa med več analitikov (Edge, 2007). Višje ležeča vozlišča je smiselno oblikovati skupaj, medtem ko se zaradi potreb po vrhunskem znanju posamezni deli oblikujejo s strani specializiranega analitika. Povezovanje modulov v kompleksno drevo napadov se ponovno izvede s timskim delom.

Slika 1 prikazuje primer grafične predstavitve drevesa napadov z glavnim ciljem seznanitve z zaupnimi podatki v neki ustanovi. Drevo ima dva podcilja. Uspešna izvedba enega izmed njih zadosti pogoju glavnega cilja. Skladno z metodologijo beremo liste od leve proti desni: pri izbiri prisluškovanja prometu mora napadalec najprej zajeti paketke in nato izvesti dekodiranje prometa.

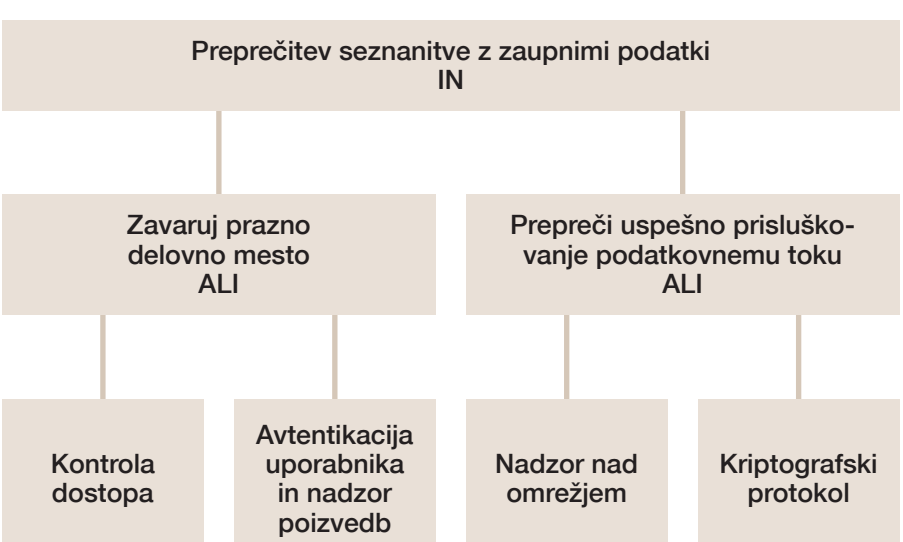
Drevo napadov je temeljno orodje za izdelavo scenarija napada, s katerim se prikaže proces napada in uporabljene tehnike (Eom in ostali 2008). Za sestavo scenarija napada poleg drevesa napadov potrebujemo še vzorec napadov. Slednji predstavlja ogrodje za izvedbo določenih vrst napadov in seznanitev z metodami, ki jih je mogoče uporabiti za izkoriščanje ranljivosti.
Pri modeliranju napadov moramo upoštevati notranjega in zunanjega sovražnika. Strokovno mu v razširjenem pomenu pravimo agent grožnje. Zanj je značilno predvsem, da ima na voljo zmogljivosti in jasen namen. Agenta grožnje lahko med drugim predstavljata računalniški virus ali logična bomba. Raziskave kažejo, da je na prvem mestu po številu incidentov ravno zlonamerna programska koda. Slednje je zaskrbljujoče, saj rezultati temeljijo na odgovorih informatikov, ki incidente zaznavajo predvsem s komercialnimi varnostnimi produkti, katere z uporabo razpoložljivih orodij uspešno zaobide že neizkušen napadalec. Prav tako ni jasno, kakšne so bile dejanske posledice takšnega incidenta.

Pregled metrik in izboljšav

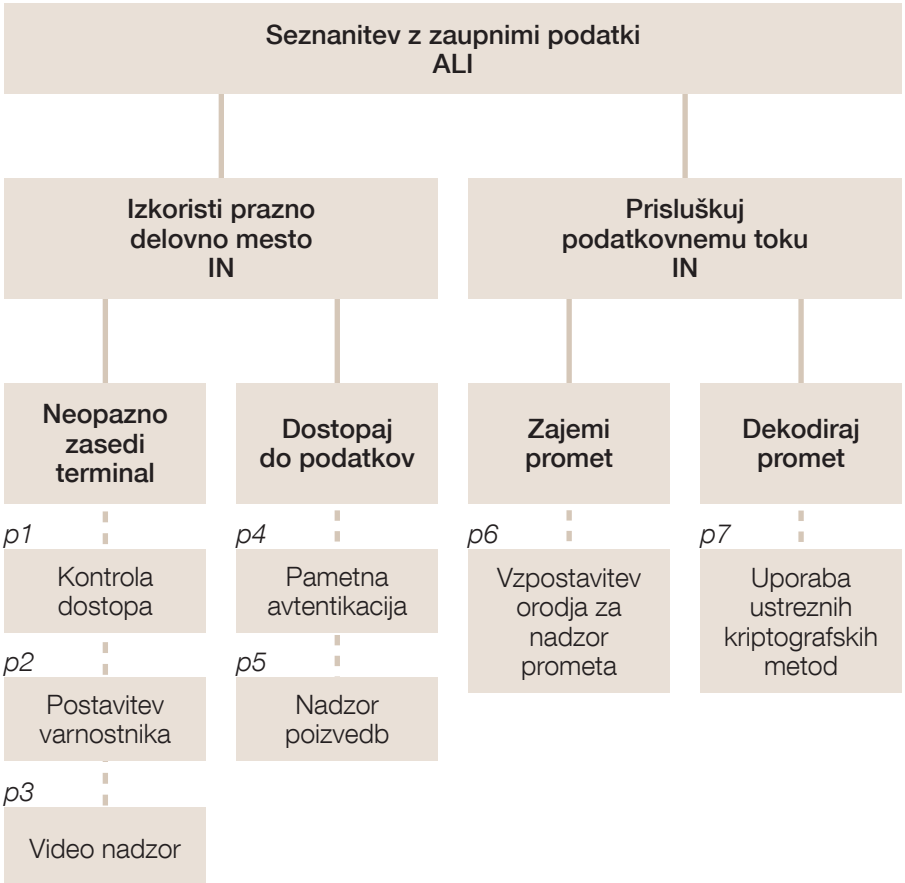
Edge (2007) ter Bistarelli in ostali (2006) opišejo drevo zaščite (ang. *protection tree*) in drevo obrambe (ang. *defense tree*), ki temeljita na predhodno izdelanem drevesu napadov. Drevo zaščite ima strukturo drevesa, katerega cilj v korenu drevesa in dejavnosti v končnih vozliščih se ujemajo z drevesom napadov, vendar tako cilji kot dejanja v končnih vozliščih izhajajo iz vidika zaščitnih ukrepov. Razlika med drevesoma je najbolje vidna v logičnih izrazih vmesnih vozlišč. Cilji vozlišč v drevesu napadov, ki zahtevajo izvedbo končnih vozlišč s pogojem IN, so uspešno onemogočeni, ko se jih zaščiti že za eno izmed dejanj končnih vozlišč. Obratno velja za vozlišča, katerih cilji so v drevesu napadov doseženi z eno od navedenih dejavnosti.

Drevo obrambe se sestavi tako, da se na končna vozlišča drevesa napadov doda niz protiukrepov.

Edge (2007) predstavi matriko, ki jo dodeli končnim vozliščem, vrednosti atributov ostalih vozlišč pa izračuna iz podatkov potomcev vozlišč, skladno z vnaprej določenimi pravili. Metrika vsebuje sledeče atribute:



Slika 2. Drevo zaščite, pripravljeno na podlagi slike 1.



Slika 3. Primer drevesa obrambe na podlagi drevesa napadov iz slike 1. Protiukrepi so označeni s p1–p7.

- **Verjetnost** – verjetnost, da bo zaščitni ukrep ustavil napadalca. Vrednost atributa je določena s strani analitika ob uporabi preteklih podatkov ali s strokovno oceno.
- **Strošek** – strošek izvedbe zaščitnega ukrepa, ki je podan v želeni enoti, največkrat v denarni valuti.
- **Vpliv** – parameter zasede vrednost med 1 in 10 odvisno glede na to, kakšen vpliv na sistem ima uspešna izvedba ofenzivne operacije v določenem vozlišču. Analitik za določitev vrednosti uporabi ustrezno tabelo z opisi vplivov na sistem in določitvijo vrednosti.
- **Tveganje** – vrednost tveganja v vozlišču se izračuna, ko so podane predhodno opisane vrednosti atributov. Izračun normalizirane vrednosti tveganja je potreben za primerjanje vrednosti atributa tveganja med vozlišči.

Drevo obrambe lahko obogatimo s kazalcema »donosnost varnostne naložbe« ROSI (ang. *return on security investment*) in »donosnost napada« ROA (ang. *return on attack*).

Sklep

Predstavljeni model drevesa napadov ilustrira uporabnost metode za prepoznavo problemov pri varovanju zasebnosti že med samo zasnovo sistemov ter oceno ranljivosti obstoječih mehanizmov varovanja zasebnosti. Današnje probleme pri varovanju zasebnosti bi uspešno odpravili, če bi prenehali čakati na pojav kršitve zasebnosti in reševati posledice, ko se kršitev že pojavi. Rešitev predstavljata usmerjenost v preprečevanje nastanka incidentov ter sistemska vgradnja mehanizmov varovanja zasebnosti.
Drevo napadov ima določene omejitve. Z njim lahko prikažemo zgolj tiste napade, ki so znani analitiku, ki modelira določen segment napadov. Model prav tako težko zajame dinamiko napadov in zato zahteva konkretne izkušnje pri izdelavi analiz.
Čeprav so nekateri avtorji mnenja, da bi moralo biti varovanje zasebnosti ključno pri informacijskih sistemih v organizacijah, ki obdelujejo občutljive osebne podatke, pogoste situacije zlorab in ugotovljene varnostne pomanjkljivosti ne govorijo temu v prid. Zato bi bila pri načrtovanju in preverjanju sistemskega varovanja zasebnosti priporočljiva redna uporaba metode za modeliranje groženj in napadov, kakršna je drevo napadov.

Viri

- Bistarelli, S., Fioravanti, F., Peretti, P. (2006). Defense trees for economic evaluation of security investments. *The First International Conference on Availability, Reliability and Security,* 416–423.
- Camtepe, A., Bulent, Y. (2007). Modeling and Detection of Complex Attacks. *Third International Conference on Security and Privacy in Communications Networks and the Workshops,* 234–243.
- Edge, K. (2007). The Use of Attack and Protection Trees to Analyze Security for an Online Banking System. *Proceedings of the 40th Hawaii International Conference on System Sciences,* 144b–144b.
- Eom, J.H., Han, Y.J., Park, S.H., Chung, T.M. (2008). Active Cyber Attack Model for Network system's Vulnerability Assessment. *International Conference on Information Science and Security,* 153–158.
- Internet Engineering Task Force. (2007). *Internet Security Glossary, Version 2.* Pridobljeno 6.3.2012 na http://tools.ietf.org/html/rfc4949
- Kotzanikolaou, P., Douligeris, C. (2007). Privacy Threats of Data Retention in Internet Communications. *18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 1–4.
- Li, W., Huang, J., You W. (2010). Attack Modeling for Electric Power Information Networks. *International Conference on Power System Technology*, 1–5.
- Reddy, K., Venter, H.S., Olivier, M., Currie, I. (2008). Towards Privacy Taxonomy-Based Attack Tree Analysis for the Protection of Consumer Information Privacy. *Sixth Annual Conference on Privacy, Security and Trust,* 56–64.
- Whalen, T. (2012). This Time, It's Personal: Recent Discussions on Concepts of Personal Information. *IEEE Security & Privacy,* 10, 77–79. ■

Avtor: Boris Milič / Vodja RNC-Ljubljana, DARS*



NADZOR IN UPRAVLJANJE PROMETA NA SLOVENSKIH AVTOCESTAH

DARS-ovim upravljavcem prometa videonadzor služi le kot eden izmed mnogih podsistemov, s pomočjo katerih upravlja promet na avtocestah in hitrih cestah v Sloveniji. DARS-ove kamere, teh je na območju slovenskih avtocest preko 1300, služijo predvsem za spremljanje prometa in ne posameznih vozil, ali celo voznikov.

Ko na avtocestnem priključku opazimo obvestilno tablo z napisom »VIDEONADZOR PROMETA«, smo se znašli na območju izvajanja videonadzora upravljavca slovenskih avtocest, družbe DARS d.d.. Mogoče beseda »nadzor« ni ravno prava. V osnovi je video sistem upravljavca avtocest zasnovan tako, da prepoznava registrskih tablic praktično ni mogoča, razen z nekaterimi določenimi novejšimi kamerami, pod posebimi pogoji. Bistvo je namreč v tem, da DARS ni prekrškovni organ in kljub temu, da marsikdaj opazi kršitve cestnoprometnih predpisov, povzročitelje ne more kaznovati. Še več: tudi kršitelje, ki jih »ujamejo« stacionarni radarji, postavljeni ob avtocesti, niso DARS-ovi, ampak z njimi upravlja policija. Le-ta tudi obravnava kršitelje in izdaja plačilne naloge. Tako pridobljena sredstva gredo direktno v proračun. Žal tudi posnetki najhujših prometnih prekrškov prej omenjenih kamer, večinoma ne zadoščajo za dovolj natančno prepoznavo storilcev in kaznovanje.

Upravljanje prometa

Množično uporabo sodobnih avtocest in hitrih cest v Republiki Sloveniji so spodbudile svetovna globalizacija, strmo naraščanje števila cestnih vozil ter posledično prometa. Pripomoglo je tudi »podiranje« državnih mej vzhodnih držav, ter posledično porast tranzitnega prometa in potrebe državljanov Slovenije po varnejši, udobnejši in hitrejši vožnji, ki jim jo nudijo avtoceste. K množični uporabi avtocest v Sloveniji je močno prispevala tudi uvedba relativno poceni vinjet za vsa vozila, do največje dovoljene mase 3500 kilogramov. Pri tem je potrebno opozoriti na to, da se je uvedba vinjet zgodila praktično čez noč, brez predhodne, oziroma sočasne odstranitve ovir, kot so danes velikokrat omenjane cestninske postaje. Druga plat medalje množične uporabe avtocest je, da ta množičnost uporabe, negativno vpliva na prometno varnost. Tako so za doseganje in ohranitev visokega nivoja prometne varnosti na avtocestah potrebne dodatne aktivnosti. Ena izmed najpomembnejših nadzorovano vodenje in upravljanje prometa. Kot vse razvite avtocestne države v Evropi, tudi Slovenija upravlja s prometom na avtocestah preko nadzornih centrov in v njih zaposlenih operaterjev. Le-ti s svojim delom upravljavca prevzemajo nase velike obremenitve in odgovornosti. To se kaže predvsem v zagotavljanju pretočnosti prometa in ob hitrem in učinkovitem »reševanju« izrednih dogodkov.

> Bistvo je namreč v tem, da DARS ni prekrškovni organ in kljub temu, da marsikdaj opazi kršitve cestnoprometnih predpisov, povzročitelje ne more kaznovati.

Razvoj nadzornih centrov

Ustanavljanje prvih nadzornih centrov (NC) za vodenje in nadzor prometa na slovenskih avtocestah in hitrih cestah, sovpada z izgradnjo prvih avtocestnih predorov po letu 1992.

*avtor je član Slovenskega združenja korporativne varnosti

Njihovem ustanavljanju je botrovala predorska oprema, ki je omogočala in zahtevala daljinsko upravljanje. Oprema, vgrajena v te predore, je tako prvič omogočila daljinsko upravljanje s predorsko prometno signalizacijo in videonadzor prometa v predorih. Prvi takšen center se je odprl na Hrušici za potrebe upravljanja predora Karavanke. Nekaj let kasneje sta mu sledila še dva nadzorna centra, Slovenske Konjice in Ljubljana. NC Slovenske Konjice je takrat prevzel upravljanje predora Pletovarje in predora Golo rebro, NC Ljubljana pa predora Golovec. Predorska oprema, s katero so takrat upravljali operaterji je bila, gledano iz današnjega zornega kota, nezahtevna in enostavna. Kljub temu je omogočala, za tiste čase hitro in učinkovito, ter predvsem relativno varno upravljanje in nadzor predorov. Omenjeno predorsko opremo so takrat sestavljali skromen video nadzor, semaforji in znaki spremenljive vsebine, ter meritve vidljivosti in koncentracije ogljikovega oksida CO. V vsakem nadzornem centru je bilo zaposlenih pet operaterjev, ki so zagotavljali delo centra 24 ur na dan in 365 dni na leto. Posebnih zahtev in kriterijev za zasedbo delovna mesta operaterjev ni bilo, v veliki meri so se na ta delovna mesta prerazporejali delavci z določenimi delovnimi omejitvami. To je le dokaz, da se ljudje marsikdaj ne zavedamo možnosti, ki nam jih nudijo nove tehnologije, predvsem pa jih ne znamo optimalno izkoristiti.

Nadzorni centri v Sloveniji danes

Danes se izvaja upravljanje z avtocestami in delno hitrimi cestami na področju Slovenije iz štirih regionalnih nadzornih centrov (RNC) in podpornega nadzornega centra (NC). Področja, ki ga pokrivajo posamezni centri in lokacije centrov so prikazani na sliki št. 1. Regionalni nadzorni centri za področje avtocest v Republiki Sloveniji so:

- RNC Kozina;
- RNC Ljubljana;
- RNC Vransko;
- RNC Slovenske Konjice;
- NC Hrušica (podporni nadzorni center)

Vir: (Interno DARS d.d., 2012)
Slika 1. Področje dela in lokacije nadzornih centrov na AC in HC v Sloveniji.



Značilnosti dela v nadzornih centrih

Osebje nadzornega centra 24 ur/dan in 365 dni/leto, s pomočjo različnih sistemov in naprav upravlja promet na pripadajočem delu avtoceste in hitre ceste. Prvenstvene naloge operaterjev so pravočasno zaznavanje dogodkov, ki negativno vplivajo, ali bi vplivali na prometno varnost, ter pravilna in strokovna uporaba vseh razpoložljivih sredstev, za potrebe zagotavljanja pretočnosti in prometne varnosti. Intenziteta dela operaterjev je neenakomerna in odvisna od dogajanja na cesti. Na pojav izrednih dogodkov operaterji večinoma ne morejo neposredno vplivati, lahko pa jih s pravočasnim zaznavanjem in ukrepanjem, v veliki meri omilijo in preprečijo. Pravočasno obveščanje udeležencev na oviro v prometu, nemalokrat prepreči nalete vozil, ki so na avtocestah, zaradi visokih hitrosti, nemalokrat vzrok za hude prometne nesreče. Pri tem je pomembno, da udeleženci upoštevajo obvestila in opozorila v obliki prometne signalizacije. Zaradi obilice sistemov in naprav, ki se nahajajo v nadzornih centrih in omejenega števila operaterjev, morajo le-ti ob sočasnosti večih izrednih dogodkov, pogosto izbrati in določiti prioriteto dogodka, ki ga bodo prvenstveno obravnavali. V osnovi pa je hierarhična lestvica pomembnosti naslednja:

Predori

- ITS sistemi na mostovih, viaduktih, razcepih...
- Odprta trasa avtoceste oziroma hitre ceste

Seveda je to le osnovna delitev, ki ne zajema lokacije in intenzitete dogodka, števila in klasifikacije udeleženih vozil, dolžine predora, nevarnosti, ki ga izredni dogodek predstavlja za okolico in ostale udeležence in še mnogo posrednih in neposrednih vzrokov. Zaradi vsega opisanega in pogosto nepredvidljivosti cestnega prometa, je nemogoče v naprej natančno predpisati ukrepe za takšne in podobne primere.

Regionalni nadzorni center Ljubljana

Regionalni nadzorni center Ljubljana upravlja avtocestni odsek dolžine 230 kilometrov. Na tem odseku se nahaja:

- 10 daljinsko upravljanih predorov in pokritih vkopov,
- Preko 250 viaduktov, mostov, nadvozov, podvozov,
- 350 video kamer,
- 260 SOS mest za klic v sili,
- Sistem za nadzor in vodenje prometa v dolžini 16 kilometrov,
- Vremenske postaje,
- Sistem za samodejno prepoznavanje vozil z ADR,
- Spremenljiva več pomenska LED signalizacija,
- Daljinsko nadzirana in upravljana razsvetljava razcepov in priključkov,
- 2 avtocestni bazi in 2 izpostavi avtocestnih baz,
- Cestninski postaji,
- Državni mejni prehod.

Operaterji v regionalnem nadzornem centru Ljubljana izvajajo vrsto različnih nalog, potrebnih za nemoteno delovanje vseh razpoložljivih sistemov in varno, ter tekoče odvijanje prometa. V grobem se te naloge lahko razdelijo na:

- Spremljanje in uporabljanje vseh računalniških aplikacij SCADA za upravljanje in nadzor sistemov,
- Vizualno spremljanje in upravljanje video nadzornih in video detekcijskih kamer,
- Tekoče in sprotno posodabljanje podatkov v aplikaciji Kažipot,
- Komuniciranje in obveščanje,

Izredni dogodki so odvisni od številnih vzrokov, od katerih so najpogostejši vremenski pojavi, gostota prometa, obnovitvena dela in polna luna.



Avtocestni predori v Sloveniji

Na slovenskem avtocestnem omrežju je trenutno 43 predorov, skupne dolžine 37.417 metrov. Omenjena dolžina predstavlja seštevek vseh predorskih cevi. Najdaljši, najstarejši in zaradi dvosmernega prometa v le eni sami cevi tudi najnevarnejši predor v Sloveniji, je predor Karavanke. S svojo dolžino 7.864 metrov povezuje dve državi (Slovenija – Avstrija) solastnici s tem, da je slovenski del dolg 3.450 metrov. Enocevni predori so nevarni predvsem zaradi nevarnosti čelnih trkov in zaradi nezmožnosti umika udeležencev na varno v primeru požara. Vsi ostali avtocestni predori v Sloveniji so dvocevni, med temi je najdaljši z 2.931 metri predor Trojane. Kot posebnost velja omeniti še ljubljanska predora Golovec in delno predor Šentvid, ki sta edina tripasovna predora. Po številu prometa v Sloveniji prednjači predor Golovec, ki je v letu 2011 dosegel povprečni letni dnevni promet (PLDP) preko 63.000 vozil.

Predorska oprema je vključno s predorsko signalizacijo večinoma novejšega datuma, zato mnogo voznikov ne pozna in se ne zaveda njenega pomena. To je opaziti predvsem pri starejših voznikih, marsikdaj pa tudi pri mnogih ostalih. Današnja tehnologija nam omogoča mnoge tehnične in napredne rešitve, ki jih pogosto vgrajujemo v predore. Žal pa vse te novosti niso učinkovite, če jih vozniki ne razumejo, ne poznajo in nenazadnje ne upoštevajo. Svoje znanje v zvezi z varno vožnjo skozi predor in pravili varne vožnje po avtocesti, si lahko preverite na spletnih straneh DARS-a.

Pravilno ravnanje ob izrednem dogodku, še posebej to velja za predor, rešuje življenja!

Zaključek

Z vsemi inteligentni transportni sistemi, spremenljivo cestno signalizacijo ter predori in tehnološko zapleteno predorsko opremo, še vedno upravlja človek. Zaradi cestnega prometa, ki je »živa« zadeva, na katerega vplivajo mnoge spremenljivke in neznanke, je to upravljanje zelo zahtevno in pogosto nepredvidljivo. Približati se cilju »nič mrtvih« v prometnih nesrečah na avtocestah je mogoče le z dobro usposabljenimi operaterji in tehnološko dovršeno prometno-varnostno opremo. Seveda morajo/mo temu ustrezno slediti tudi vozniki. Dokler se bodo pojavljala vprašanja kot: »Ali res moram ustaviti pred rdečo lučjo na semaforju v predoru?«, kot se je pojavilo nedolgo tega, bomo še zelo daleč od tega cilja. ■



Avtor: ddr. Robert Brumnik / METRA Inženiring d.o.o.*



DIGITALNI VOHUNI

Ob vseh raznovrstnih interesih in metodah, se danes večina vohunske dejavnosti odvija v gospodarske namene. Vidimo lahko, da se je tudi obveščevalna dejavnost prilagodila sodobnim časom informatike, digitalizacije in elektronike.

V smislu obveščevalne dejavnosti, je 20. in 21. stoletje, obdobje avtomatičnega pridobivanja, analize, interpretacije in uporabe informacij. Tako naj bi obveščevalne službe v prihodnje oblikovale elektronske baze, v katere bi uvrščale svoje obveščevalne izdelke, uporabniki pa bi med slednjimi sami izbirali ustrezne informacije. Evropska unija (EU) te aktivnosti opravlja že vsaj od l. 1996, teroristični napadi l. 2001 pa so to samo pospešili. Predlogi za povečanje nadzora in mednarodno sodelovanje na tem področju, so bili pripravljeni že pred 11. septembrom l. 2001.

Vohunstvo danes

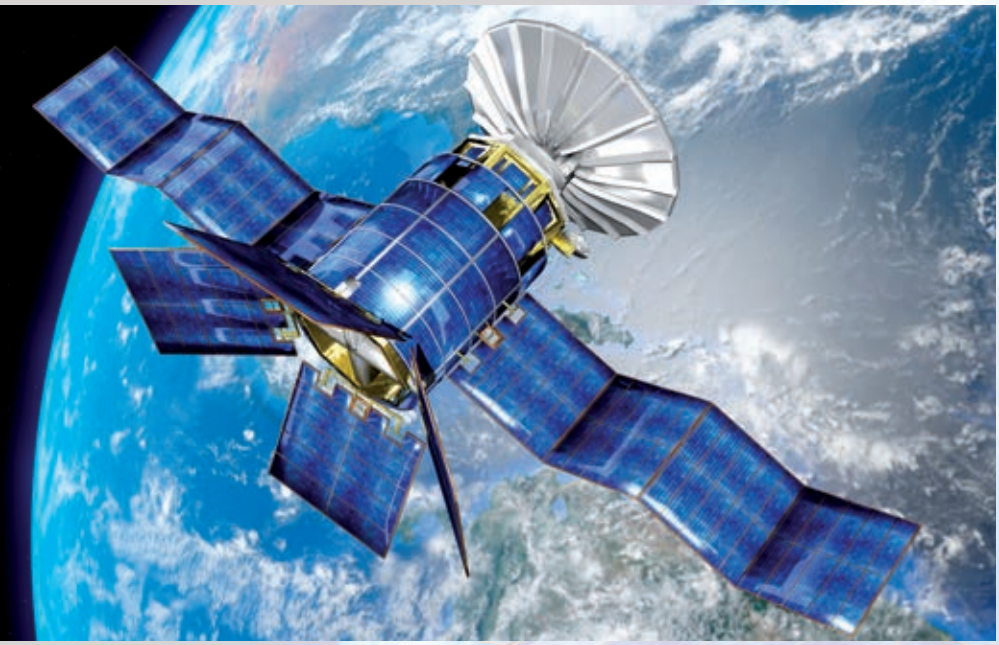
Na spletu lahko najdemo seznam omrežij (Cryptome, 2011), ki naj bi bila kakorkoli povezana, ali so pod kontrolo ameriške varnostne službe NSA (National Security Agency). ZDA so l. 1994 sprejele zakon za telefonske komunikacije (Digital Telephony Act), po katerem bi morali proizvajalci telekomunikacijske opreme puščati varnostne luknje zaradi nadzora. Prisluhe in nadzore torej vršijo različni državni nadzorni organi. Poleg tega, nas na internetu nadzirajo tudi velike korporacije. Zavedati se moramo torej tudi možnosti sodelovanja teh korporacij z državnimi organi, ki jim odstopajo naše podatke. V ZDA primer takšnega sodelovanja razkriva tožba organizacije za elektronske svoboščine proti telekomunikacijskemu podjetju, ki je NSA nezakonito omogočili dostop do podatkov o ameriških uporabnikih telefonije in interneta. Znan je tudi primer kitajskih oporečnikov, ki so jih identificirali in zaprli na podlagi podatkov, ki so jih kitajske oblasti pridobile od ameriške korporacije Yahoo. Tudi Google se je v preteklosti že uklonil cenzorskim pritiskom Kitajske v namenu pridobivanja obveščevalnih podatkov. V zadnjem času pa je Facebook najbolj strašljiva vohunska naprava, ki jo je človeštvo kadarkoli naredilo. Na enem mestu združuje podatke o ljudeh, njihovih odnosih, imenih, naslovih, lokaciji, komunikacijah, sorodnikih in vse to je dostopno ameriškim obveščevalcem (Assagne, 2012). Obstoječo nadzorovalno tehnologijo, ki je bila vzpostavljena za namene zakonitega nadzora, pa lahko zlorabijo tudi kriminalne ali teroristične združbe. Tipična primera sta bili prisluškovalni aferi v Grčiji in Italiji. Telefonske centrale imajo namreč celo vrsto funkcionalnosti za izvajanje prisluhov. V Grčiji je napadalcem (verjetno kakšna tajna služba, lahko pa tudi kriminalna združba) uspelo izrabiti varnostno ranljivost v modulu telefonske centrale, namenjene zakonitemu prisluškovanju. Več kot pol leta so prisluškovali okoli 100 politikom, med drugim tudi predsedniku vlade (Kovačič, 2007).

Elektronska orodja v obveščevalni in protiobveščevalni dejavnosti

Osnovni namen elektronskega izvidovanja je pridobivanje podatkov, ki bi bili koristni v primeru zagotavljanja nacionalne varnosti. Operacije elektronskega izvidovanja so (Polmar in

V zadnjem času pa je Facebook najbolj strašljiva vohunska naprava, ki jo je človeštvo kadarkoli naredilo. Na enem mestu združuje podatke o ljudeh, njihovih odnosih, imenih, naslovih, lokaciji, komunikacijah, sorodnikih in vse to je dostopno ameriškim obveščevalcem (Assagne, 2012).

*avtor je član Slovenskega združenja korporativne varnosti



Allen, 1998):
- zbiranje podatkov o nasprotnikovi obrambi (vrsta in položaji vojaških enot, radarjev, protiletalskih sistemov itd.),
- zbiranje podatkov o pomembnih postavitvah ali objektih nasprotnika in
- prisluškovanje nasprotnikovim komunikacijam.

Elektronska obveščevalna dejavnost (ELINT)

Segment obveščevalne dejavnosti, ki za zbiranje obveščevalnih informacij uporablja elektronska sredstva, imenujemo elektronska obveščevalna dejavnost ELINT. ELINT zajema več metod in sicer: SIGINT, TELINT, COMINT, zbiranje podatkov s seizmološkimi, radiološkimi, kemičnimi in drugimi meritvami (MASINT) in zbiranje podatkov o nasprotnikovi aktivnosti s uporabo radarjev (RADINT). Ta vrsta izvidovanja je doživela posebno hiter razvoj v obdobju hladne vojne in je danes v sodobnih nacionalno varnostnih sistemih nepogrešljiv element zagotavljanja kakovostnih informacij.

Nadzor nad telekomunikacijami

Zakonito nadzorovanje elektronskih komunikacij v Sloveniji, pomeni ukrep nadzora elektronskih komunikacij in zajema zakonito prestrezanje ter kontrolo in zavarovanje dokazov, vseh oblik komuniciranja v javnem komunikacijskem omrežju. Izvajajo ga pristojni organi v skladu z zakonom, ki ureja kazenski postopek, obrambo ali z zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo.

Vohunjenje preko mobilnih naprav in omrežij

Ob standardnih postopkih prestrezanja telefonskih klicev preko mednarodnih sistemov zvez (SOVA) in prestrezanja telefonskih klicev preko operaterjev (policija), se lahko omejimo na dva osnovna načina prestrezanja mobilnih komunikacij. Prvi način je z namestitvijo ustrezne vohunske programske opreme v mobilni telefon, s pomočjo katere lahko potem oseba dejansko popolnoma kontrolira dohodne in odhodne klice osebe, sms sporočila ter zvočno dogajanje okoli druge osebe. Za namestitev vohunske opreme, mora biti telefon osebi dostopen, da lahko naloži program. Poznana tehnika za vohunjenje v mobilnih omrežjih je tudi analiza pogovorov na pametnih telefonih, ki uporabljajo Googlov operacijski sistem, Android. Soundminer je trojanski konj, ki zaznava telefonske klice v avtomatska bančna sporočila oz. telefonsko banko in zazna, kdaj klicatelj sporoči banki številko bančne kartice. Proti omenjenemu načinu vohunjenja se lahko zaščitimo z orodjem Soundcomber (Schlegel, 2011).

IMSI (International Mobile Subscriber Identity) lovilec

Lovilec IMSI številk, je naprava za prepoznavanje, sledenje in prisluškovanje mobilnim telefonom, ki poteka na tak način, da uporabnik in tudi operater to zelo težko opazita. Leta 1996 je nemško podjetje Rohde&Schwarz iz Münchna predstavilo prvi IMSI Catcher GA090. Zamisel je bila prvotno namenjena identifikaciji naročnika, ki posreduje IMSI. S pomočjo mobilnega operaterja, je bilo mogoče ugotoviti, povezano telefonsko številko (Strobel, 2007).
Leta 1997 je nasledil GA900, ki omogoča, da klicatelj opravi telefonski klic preko mobilne postaje, brez vključitve v bazno postajo GSM omrežja. Pri prepoznavanju IMSI, ima vsak mobilni telefon zahtevo za optimizacijo sprejema. Če obstaja več baznih postaj vpisanega operaterja omrežja dostopen, bo vedno izbral tistega, z najmočnejšim signalom.

Elektronski agenti - Echelon

Sateliti lahko prisluškujejo vsem mogočim komunikacijam, računalniki znajo pretvoriti govor v zapisano besedilo in celo odstraniti nepomembno besedilo, tako da ostanejo le obveščevalni podatki. Tehnika pa je celo tako napredovala, da lahko en sam elektronski agent, v enem dnevu pridobi več ključnih informacij, kot nekaj najspretnejših operativcev na terenu. Echelon je sistem, ki so ga Američani skupaj z zavezniki razvijali več kot 20 let (Campbell, 2000). Echelon je ime, ki označuje svetovno razširjeno signalno-obveščevalno in analitično mrežo, ki jo upravlja skupnost imenovana UKUSA. UKUSA je združenje petih držav in sicer Velike Britanije, ZDA, Kanade, Avstralije in Nove Zelandije (Campbell, 1999). Ideja sistema Echelon ne pomeni osredotočenost na posameznika, področje obdelave (slika 1) je celoten telekomunikacijski sistem. Vse telekomunikacije, ki potekajo prek satelitov, mikrovalovnih zvez ali prek kablov[1], položenih na dnu morja, je mogoče nadzorovati.

Kriptoanaliza (primer GSM omrežja)

Kriptoanaliza; izvor besede gre verjetno iskati v grščini. Grška beseda kryptós pomeni skrito, beseda analýein pa



sprostiti ali odvezati. Kriptoanaliza je študija metod za pridobivanje pomena kodiranih informacij brez dostopa do skrivne informacije, ki bi jo v normalnem primeru potrebovali. To navadno pomeni iskanje skrivnega ključa. Kriptoanaliza označuje tudi poskuse zaobiti varnosti drugih tipov šifrirnih algoritmov in protokolov na splošno (Stergaršek, 2006). Digitalno telefonsko omrežje GSM uporablja vrsto kriptografskih protokolov kot so A3, A5 in A8, s katerimi poskuša zagotoviti določen nivo varnosti. Velika večina GSM operaterjev uporablja pri protokolu A3 in A8 algoritem COMP12814. Napad na A5 je potreben, če želi napadalec prisluškovati pogovorom v GSM omrežju, na A3 in A8 pa, če želi opraviti kloniranje SIM kartice. Če povzamem: napadi na GSM omrežja so možni in so tudi dejansko prisotni. Seveda pa je dandanes moderna kriptografija visoko presegla kriptoanalizo, saj obstaja kar nekaj kriptosistemov, ki jih ni mogoče zlomiti. Po drugi strani pa ne smemo pozabiti na druge učinkovite metode, kot so prestrezanje, uporaba fizične sile, bočni napadi, mobilni virusi, kvantni računalniki[2] itd.

Pogled v prihodnost

Znanstvene publikacije v vezi s prihodnostjo obveščevalne in protiobveščevalne dejavnosti, pogosto omenjajo tehnologije za elektronski nadzor človeških možganov. Seveda pa te zadeve niso neka novost, saj se s tem znanstveniki ukvarjali že v l.1941 (National Security Agency, 1997). V skupini SIGINT obstajajo orodja, ki omogočajo zaznavanje, prepoznavanje in spremljanje bio-električnega polja neke osebe na daljavo. SIGINT ima možnost neinvazivnega spremljanja podatkov v človeških možganih na daljavo. Z digitalnim dekodiranjem so izzvani potenciali pri 30-50 Hz, 5 mW elektromagnetnega sevanja v možganih. Daljinski nevronski nadzor (RNM, daljinsko spremljanje bio-električne informacije v človeških možganih) je postal končni sistem nadzorovanja. Uporablja ga omejeno število za to usposobljenih agentov ameriških obveščevalnih služb. Seveda pa ameriške obveščevalne službe v razvoju in uporabi teh prijemov niso osamljen primer.

Zaključek

Ob vseh teh raznovrstnih interesih in metodah, se danes večina vohunske dejavnosti odvija v gospodarske namene (Podbregar, Ivanuša in Lipičnik, 2007). V prispevku smo zajeli le nekaj možnosti elektronskega vohunjenja. Vidimo lahko, da se je torej tudi obveščevalna dejavnost prilagodila sodobnim časom informatike, digitalizacije in elektronike. Sateliti in namenska informacijska oprema omogočajo pogled na zemljo, tudi če jo prekrivajo oblaki, če sneži ali je noč. Z uporabo infrardečih žarkov, radarjev in naprednih senzorjev, je mogoče kar iz vesolja zaznati zelo majhne objekte. Zakaj bi torej še rabili agente, da fotografirajo objekt, če pa ga lahko vidimo iz vesolja? In, če temu dodamo še brezpilotna letala, opremljena z vsemi mogočimi vohunskimi napravami, potem res ni potrebe, da po klasičnih metodah vohunstva, še pošiljamo v nevarnost ljudi.

Viri

- Assagne, J. (2011). WikiLeaks revelations only tip of iceberg. *Russia Today*. Pridobljeno 24.05.2011 na http://www.rt.com/news/wikileaks-revelations-assange-interview/
- Campbell, D. (2000). Inside Echelon: *The history, structure und function of the global surveillance system known as Echelon*. Pridobljeno 25.05.2012 na http://echelononline.free.fr/documents/dc/inside_echelon.htm
- Campbell, D. (1999). *Development of surveillance technology and risk of abuse of economic information*. Pridobljeno 23.05.2012 na http://www.fas.org/irp/program/process/docs/98-14-01-2en.pdf
- Cryptome. (2011). *Nadzorovana omrežja: NSA*. Pridobljeno 04.06.2011 na http://cryptome.org/nsa-ip-update9.htm; http://cryptome.org/info/
- Kovačič, M. (2007). Intervju. Pridobljeno 19.05.2012 na http://www.mladina.si/dnevnik/13-07-2007-intervju/
- National Security Agency (1997). Covert operation of the U.S. *Nexus Magazine*. Pridobljeno 15.5.2012 na http://www.bibliotecapleyades.net/ciencia/echelon/echelon02.htm
- Podbregar, I., Ivanuša, T. in Lipičnik, M. (2007). Razsežnosti gospodarskega vohunstva v 21. Stoletju-primer gospodarskega vohunstva s pomočjo trojanskega konja. V B. Lobnikar (ur.), *Zbornik povzetkov: 8 slovenski dnevi varstvoslovja: Varnost v sodobni družbi groženj in tveganj* (str.6). Ljubljana: Fakulteta za varnostne vede.
- Polmar, N. in Allen, T. B. (1998). Spy book: *The encyclopedia of espionage*. New York: Random house.
- Richelson, J. (1999). *The U.S. intelligence community.* Boulder: Westview Press.
- Rockland: Syngress Publishing.
- Strobel, D. (2007). *IMSI Catcher.* Seminararbeit, Ruhr-Universität, Bochum.
- Stergaršek, E. (2006). *Kriptoanaliza.* Porazdeljeni informacijski sistemi in celovitost podatkov, Seminar na podipl. Študiju.
- Schlegel, R. (2011). Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. Pridobljeno 5.4.2012 na http://www.cs.indiana.edu/~kapadia/papers/soundcomber-ndss11.pdf

[1] Obstajata dva načina prestrezanja informacij, ki potujejo preko podmorskih kablov; če pogledamo, kako potekajo podmorski kabli, vidimo, da znaten del teh kablov pride do ameriškega ozemlja, ali pa gredo v Kanado, Avstralijo ter Veliko Britanijo. Ko torej kabli pridejo iz morja, lahko agencije, ki se ukvarjajo z ELINT, prestrežejo podatkovne tokove. V Angliji, je postavljena zemeljska ELINT postaja, nedaleč od vozlišča britanskega telekoma. Manj zanesljiva pa je varianta, ko podmornica v bližini kabla postavi prisluškovalno napravo.

[2] Kvantni računalnik je naprava, ki računa s superpozicijami kvantnih stanj. Pri kvantnih računalnikih se operira z valovnimi funkcijami, ki so edine primerne za opis stanj, zato lahko v kratkem času izvede milijarde računskih operacij. ■

Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij.
Skozi združenje člani organizirano uresničujejo osebne in poslovne interese na področju korporativne varnosti.

Namen združenja je uresničevanje interesov članstva, ki so:

- združevanje znanja, izkušenj, interesov in razvojnih pogledov,
- pospeševanje razvoja izobraževanja in usposabljanja,
- razvoj mednarodno primerljivih korporativnih varnostnih standardov,
- izboljšanje kakovosti storitev na področju zagotavljanja korporativne varnosti,
- razvoj korporativnega varnostnega managementa,
- razvoj varnosti kot vrednote, ki izboljšuje pogoje dela in dviguje motivacijo.

»Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!«

»Ab uno disce omnes (po enem spoznaj vse)«

Članstvo v združenju je prostovoljno. Združenje ima redne, korporativne in častne člane.

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih strokovnih srečanjih;
- popusti pri nakupu izdanih publikacijah ICS, Ljubljana;
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS-Ljubljana;
- popusti pri oglaševanjih in postavitev logotipa na spletno stran ICS-Ljubljana
- popusti pri članarinah za strokovne člane, ki prihajajo iz vrst organizacij katere so korporacijski člani združenja (korporacijski člani);

Več informacij je dostopnih na spletnih straneh www.ics-institut.si ali www.ics-institut.com.

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

TelekomSlovenije
Zanesljivo vsepovsod POŠTA SLOVENIJE
gorenje Gorenje, d.d.
LUKA KOPER Port of Koper
SIEMENS
TE-TOL
MIŠKA 20 let FMC Group
INFORMACIJSKI POOBLAŠČENEC
DARS
REISSWOLF secret. service.
univerzitetni klinični center ljubljana

Avtor: mag. Gregor Garb / Slovensko združenje korporativne varnosti



KORUPTIVNOST V ZASEBNEM SEKTORJU

Obstoj korupcije[1] v javnem sektorju že dolgo ni več tabu. V ospredje, in še posebej v povezavi z globalno ekonomsko in finančno situacijo, pa vse bolj prihaja zavedanje o koruptivnosti, tudi v zasebnem sektorju.

Da je pojav korupcije vedno bolj razširjen in problematiziran, kaže tudi poročilo, v katerem je Služba Evropske komisije za javnomnenjske raziskave Eurobarometer predstavila rezultate javnomnenjske raziskave o dojemanju in izzivih notranje varnosti v posameznih državah in na ravni celotne EU. Raziskava se je izvajala v obdobju od junija do novembra leta 2011, v njo je bilo vključeno 26.840 anketiranih državljanov EU, od tega 1024 iz Republike Slovenije.

Po mnenju državljanov EU zaseda korupcija peto mesto (18%) med največjimi izzivi notranje varnosti posameznih držav. Za razliko od EU zaseda korupcija v Sloveniji prvo mesto (47%) med največjimi izzivi. Visoke deleže dobiva dojemanje korupcije tudi v Romuniji (56%), Litvi (42%), Grčiji (39%), Češki (38%) in Španiji (37%), medtem, ko je dojemanje korupcije skoraj neznaten izziv notranje varnosti, predvsem v skandinavskih državah (Danska in Finska – 2% in Švedska – 3%).

Vir: http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf, z dne 24.6. 2012

Iz raziskave je moč razbrati, da predstavlja korupcija večji izziv notranje varnosti med »novimi« (12) članicami EU (29%), medtem ko je med »starejšimi« (15) članicami EU, tovrsten izziv umeščen v spodnjo tretjino (15%).

Kot izziv notranje varnosti na ravni EU se korupcija uvršča na šesto

Kaj je po vaši oceni najpomembnejše tveganje za nacionalno varnost?



Legenda: odprti tip odgovorov

mesto (15%). Kot najvišji izziv so jo ovrednotile Španija (35%), Romunija (30%), Slovenija in Grčija s po 29%. Pričakovano so jo ponovno najnižje ovrednotile skandinavske države. Kar 40% vprašanih je mnenja, da na visoko stopnjo korupcije vpliva prevelika povezanost gospodarstva in politike, kjer sta razloga predvsem neukrepanje politikov (36%) in netransparentnost pri porabi javnih sredstev (33%).

pravne države. Za Republiko Slovenijo lahko zaključimo, da je problem korupcije posledica specifičnosti slovenske tranzicije, zgodovinskih okoliščin, krize vrednot in pomanjkanja oziroma nespoštovanja predpisov ter partikularnega individualizma predvsem pri vrednotenju varnosti. Dejstvo namreč je, da je korupcija posledica določenega stanja, ki je premosorazmerna s šibkostjo institucij pravne države.

evropski ravni (Sporočilo za medije Evropske komisije v: KPK vestnik, 2012)

Dejstvo namreč je, da je v smislu preprečevanja s prisilnimi normami in ukrepi možno regulirati le del aktivnosti, daleč večji pomen in učinek pa imajo aktivnosti, za katere se odloči, predpiše, obveže in nenazadnje tudi realizira sam zasebni sektor.

Kaj je po vašem mnenju najpomembnejše tveganje za varnost državljanov EU?



Legenda: odprti tip odgovorov

Vir: http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf, z dne 24.6. 2012

Raziskava je tudi pokazala, da ima korupcija v Sloveniji naraščajoči trend (74%), le 3% pa menijo, da se je korupcija zmanjšala. Kar 78% vprašanih se popolnoma strinja, da je korupcija velik problem, le 5% pa se s to trditvijo ne strinja (KPK vestnik, 2012). Pri tem je potrebno upoštevati, da raziskava meri izključno percepcijo razširjenosti korupcije, kar pa ne pomeni nujno dejanske stopnje korupcije v posamezni državi oziroma na ravni EU. Na ta način se kaže tudi stopnja zaupanja/nezaupanja v politiko in delovanje institucij

Dobljeni rezultati s področja dojemanja razsežnosti korupcije kažejo na to, da je korupcija problem sistemskih razsežnosti tako posameznih držav kot tudi celotne EU. S ciljem preprečevanja korupcije, je Evropska komisija v letu 2011 sprejela protikorupcijski sveženj, v katerem je države članice pozvala k večji osredotočenosti na korupcijo. Z namenom doslednega spoštovanja ukrepov je vzpostavila poseben mehanizem EU za spremljanje in ocenjevanje, v kratkoročnem obdobju pa bo predložila tudi zakonske predloge glede kaznivih dejanj povezanih s korupcijo, reformo predpisov o javnem naročanju in o strožji politiki na področju boja proti goljufijam na

Kljub temu je država oziroma mednarodno okolje proaktivno pristopilo k preventivnemu delovanju in s ciljem vzpodbude zasebnemu sektorju ponudilo vrsto preventivnih ukrepov za preprečevanje korupcije, kot so: (1) krepitev sodelovanja med organi pregona in zasebnimi podjetji, (2) razvoj standardov in postopkov za zagotovitev integritete podjetij, vključno s kodeksi etike in preprečevanjem konflikta interesov, (3) krepitev transparentnosti v postopkih ustanavljanja in sodelovanja pravnih oseb v gospodarstvu, (4) preprečevanje zlorab v reguliranju dejavnosti zasebnih podjetij, zlasti na področju subvencij in raznih dovoljenj, (5) preprečevanje konflikta interesa med aktivnostmi nekdanjih ali aktualnih javnih uslužbencev in dejavnostmi pravnih oseb v zasebnem sektorju, (6) zagotavljanje zadostnih notranjih nadzornih postopkov ter (7) inkriminacija vseh oblik nepravilnega ali nepopolnega knjiženja poslovnih

Kot vidimo so se države na pojav korupcije odzvale predvsem z represivnimi, kazenskopravnimi ukrepi, medtem ko je preventivno delovanje skoraj v celoti prepuščeno zasebnemu sektorju.



dogodkov (UNCAC, 2003). V podporo preventivnemu delovanju je pristopila tudi Republika Slovenija in s prejetjem Zakon o integriteti in preprečevanju korupcije v letu 2011, Komisiji za preprečevanje korupcije v 12. členu, določilo pristojnost in nalogo sodelovanja pri krepitvi integritete[2] in preprečevanju ter odpravljanju tveganj za korupcijo v javnem in zasebnem sektorju kakor tudi izvajanje strokovnih nalog v zvez s pripravo in izdelavo načrtov integritete in pripravo ukrepov za preprečevanje korupcije za uporabnike iz zasebnega sektorja.

Kot že omenjeno pa bo uspešnost preventivnega delovanja odvisna predvsem od pristopa gospodarskih subjektov zasebnega sektorja, ki se bodo na izziv potencialne oziroma dejanske korupcije odzvali šele, ko bo slednji identificiran kot dejanski problem. Teorija pozna pet možnih načinov preventivnega strateškega pristopa[3] k preprečevanju korupcije. Izbor pa je, poleg odločitve vodstva, odvisen tudi od velikosti podjetja, njegove ekonomske moči, položaja na trgu, temeljnih značilnosti njegovih poslovnih partnerjev, pravnega sistema, v katerem deluje ipd.

Namesto zaključka lahko ugotovimo, da absolutne zakonitosti oziroma rešitve ni. Le zavestne odločitve vodstva k načrtnemu pristopu prepoznave, oblikovanja in vzdrževanja individualnega in kolektivnega kodeksa etičnega ravnanja, poudarjanje poštenosti, pravičnosti, transparentnosti in legalnosti postopkov v notranjem in zunanjem poslovanju s temeljno zahtevo, da bo vse omenjeno postalo običajni in vsakodnevni sestavni del delovnih procesov, bo gospodarske subjekte zasebnega sektorja ohranilo »čiste«.

Viri:

- EUROBAROMETER. http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf, z dne 24. 6. 2012
- Kos, D. Kako preprečevati korupcijo v gospodarstvu ?. V: Dobovšek, B. (ur.). Korupcija v gospodarstvu. Policija, Uprava kriminalistične policije, Ljubljana, 2004, str. 23-34.
- KPK vestnik. Komisija za preprečevanje korupcije, št. 12, marec 2012.
- UNCAC, UN Convention against Coruption. http://www.unodc.org/unodc/en/treaties/CAC/, z dne 27. 6. 2012.
- Zakon o integriteti in preprečevanju korupcije (ZIntPK-UPB2), Uradni list RS, št. 69/2011.

[1] Zakon o integriteti in preprečevanju korupcije v svojem četrtem členu, korupcijo opredeljuje kot »vsako kršitev dolžnega ravnanja uradnih in odgovornih oseb v javnem ali zasebnem sektorju, kot tudi ravnanje oseb, ki so pobudniki kršitev ali oseb, ki se s kršitvijo lahko okoristijo, zaradi posredno ali neposredno obljubljene, ponujene ali dane oziroma zahtevane, sprejete ali pričakovane koristi zase ali za drugega«.

[2] Integriteta je »pričakovano delovanje in odgovornost posameznikov in organizacij pri preprečevanju in odpravljanju tveganj, da bi bila oblast, funkcija, pooblastilo ali druga pristojnost za odločanje uporabljena v nasprotju z zakonom, pravno dopustnimi cilji in etičnimi kodeksi« (četrti člen ZIntPK-UPB2).

[3] »Nojeva taktika«, »Odisejeva taktika«, »Verižna taktika«, »Denarna taktika« in »Taktika celovitega ukrepanja« (Kos, 2004, str. 29-30). ■

Družba za upravljanje in vzdrževanje nepremičnin

JAXMA

Že 10 let sledimo poslovnim odnosom,
ki temeljijo na vrednotah

Zaupanje Kakovost Varnost

- ☑ Upravljanje in vzdrževanje več-stanovanjskih sosesk
  po meri naročnika – sledimo konceptu varne in urejene soseske
- ☑ Čistilni servis
- ☑ Kompletna storitev upravniško-vzdrževalnih in servisnih del
  za lastnike in najemnike poslovnih prostorov
- ☑ Urejanje okolice
- ☑ Pluženje snega
- ☑ Obnove objektov.

www.jaxma.si jaxma@siol.net

Detektivske storitve za prave odločitve!

DETEKTIV
GREGOR OSET
DeZRS lic. št. 109
+386 41 602 771

Zbiramo potrebne informacije:

- **o poslovnih subjektih (due dilligence),**
- **o dolžnikih** in njihovem premoženju (za uspešno izvršbo ali poravnavo) in
- informacije, ki jih potrebujete **v sodnih in drugih postopkih.**

Opravljamo preiskave v zvezi s kadrovskimi zadevami (alkotesti, kontrole bolniških, preiskava tatvin na delovnem mestu, kršitve konkurenčne prepovedi idr.) ter opravimo **osebno vročitev.**

Za slovenske in tuje zavarovalnice opravljamo preiskave zavarovalniških goljufij in zberemo potrebne informacije za odločanje likvidatorjev.

W: www.detektiv-oset.si E: info@detektiv-oset.si M: +386 41 602 771

Zanesljivo že sedem let - v Sloveniji in po svetu!

Avtor: Domen Pirkmajer / korporativno varnostni manager v TE-OL*



INTERNATIONAL FIRE AND SECURITY EXHIBITION AND CONFERENCE (IFSEC) 2012 V BIRMINGHAMU

IFSEC že skoraj štirideset let ostaja največji svetovni dogodek na področju varnosti. S svojo tradicionalno in prestižno vlogo predstavlja barometer svetovne varnostne industrije, ki ga v povprečju obišče 25.000 varnostnih strokovnjakov. Tudi letos je svoje storitve in produkte na ogled postavilo preko 650 vodilnih proizvajalcev, dobaviteljev in distributerjev varnostne opreme iz več kot stotih držav.

Varnostne rešitve in najboljše prakse

Posebnost varnostne industrije je, da ji svetovna gospodarska kriza ni prišla do živega, prej nasprotno, saj evolucija varnostnih grožen narekuje kontinuiran razvoj varnostnih inovacij, ki branžo ženejo naprej. Napisano potrjuje tudi zadnje poročilo izdano s strani Plimsoll Publishing, ki navaja, da bo prodaja v varnostnemu sektorju,v naslednjih desetih letih, zrasla za 64,5%. Celoten varnostni trg pa je v zadnjem letu zrasel iz $27,6 milijard na $28,7 milijarde. V povprečju se je prodaja povečala za 2,7%, večja podjetja pa so v povprečju zabeležila 4,6% rast.

Značilnost letošnjega varnostnega dogodka je bila, da je kar 95% vseh razstavljenih produktov, vezanih na CCTV, temeljilo na IP tehnologiji in ne več na analogni. To pomeni, da je tudi angleški trg, kljub vsem pomislekom, sprejel IP tehnologijo, kot neizogibno dejstvo, ki bo narekovalo prihodnost video nadzornih sistemov. Videli smo velik napredek pri izdelkih, ki v lanskem letu še niso bili izpopolnjeni. Predvsem gre za kamere z visoko ločljivostjo in tako imenovane multi-megapixel kamere, ki jih odlikujejo napredne slikovne funkcije.

Značilnost letošnjega varnostnega dogodka je bila, da je kar 95% vseh razstavljenih produktov, vezanih na CCTV, temeljilo na IP tehnologiji in ne več na analogni.



Naslednja stvar, ki jo je vredno omeniti je, da so proizvajalci IP kamer stopili korak naprej in začeli množično sodelovati s ponudniki sistemskih in softwerskih rešitev. To bo razveselilo predvsem kupce, ki jim kompatibilnost naprav predstavlja velike težave.

Velik preboj na varnostno tržišče je uspel podjetjem, ki razvijajo termovizijske kamere, ki lahko delujejo povsod, kjer se med procesom opazovanja prenaša temperatura. Infrardeče sevanje se spreminja v vid-

*avtor je član Slovenskega združenja korporativne varnosti



Bistvena prednost termovizijskih kamer je, da so neobčutljive na vremenske razmere, kot so tema, megla, dež ali sneg.

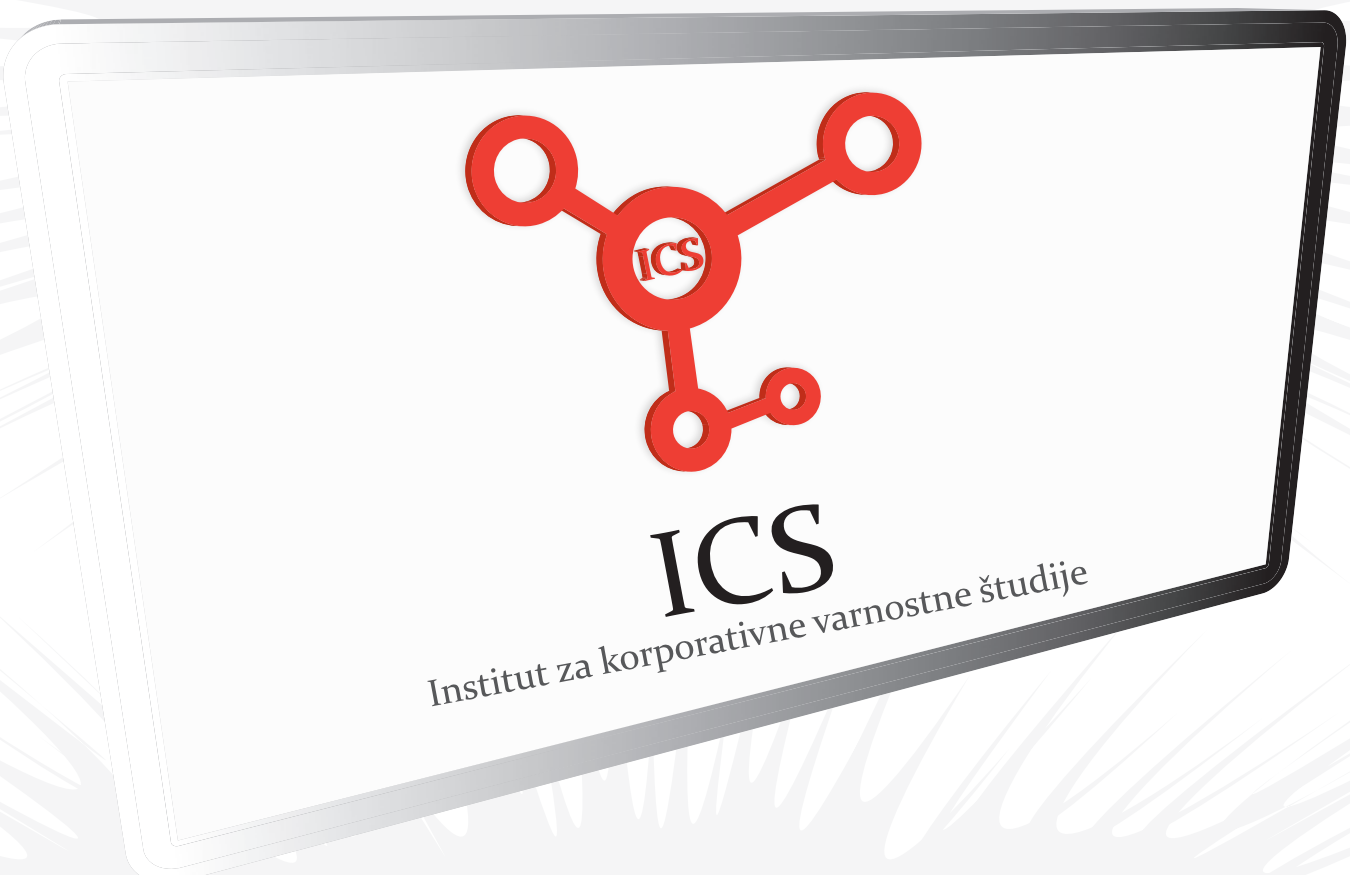
no sliko na kameri. Bistvena prednost termovizijskih kamer je, da so neobčutljive na vremenske razmere, kot so tema, megla, dež ali sneg.

Pravo smer razvoja termovizijskih kamer je nagradila tudi komisija za izbor najboljših varnostnih inovacij v kategoriji CCTV Camera Equipment of the Year. Laskavi naslov je pripadel podjetju Pelco by Schneider Electric Sarix Thermal Imaging.

Pa poglejmo še ostale letošnje nagrajence po kategorijah:

- CCTV Camera Equipment of the Year: Pelco by Schneider Electric - Sarix Thermal Imaging
- CCTV System of the Year (excluding cameras and lens): Ipsotek - Tag and Track
- Intruder Alarm or Exterior Deterrent Product of the Year: Visonic - PowerMaster-30 G2
- Physical Security Product of the Year: Mul-T-Lock UK - Watchlock
- Access Control Product of the Year (including biometrics): Codegate - ePod
- Communication Product of the Year: Tesor Plus Corporation - SM-500
- Integrated Security Product of the Year: AD Network Video – FireVu Solution
- Security Project or Security Installation of the Year: Siemens - PPG Chemicals automated wide surveillance
- Guarding Service Delivery to the Customer: Interr Security - Nido Student Living
- Best Policing Partnership of the Year: Glasgow Community & Safety Services - Glasgow Community & Safety Services project ■

Slovenian Grand Security Award 2012



Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti.

Neodvisna komisija ocenjuje in izbira kvaliteto in izvirnost prijavljenih udeležence v naslednjih kategorijah:

Najbolj varno mesto
Najbolj varno podjetje
Zasebno-varnostna služba leta
Korporativno varnostni manager leta
Najboljša knjiga s področja varnosti
Inovativna medijska promocija varnosti.

www.ics-institut.si

4. mednarodna konferenca

Dnevi korporativne varnosti

Ljubljana, 21.—22. marec 2013



ICS

Institut za korporativne varnostne študije

“Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!”

www.ics-institut.si