Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2019, marec • št. 19



Institut za korporativne varnostne študije, ICS-Ljubljana praznuje 10. obletnico delovanja

Podelitev prestižne nagrade »Slovenian Grand Security Award«

Kongresni center Brdo pri Kranju, 13. marec 2019

Tel: +386 1 8317 488
Service tel.: + 386 1 8317 452
Web: www.zarja.com
E-mail: info@zarja.com

PRAVA TEHNIČNA VARNOST SE ZAČNE Z DOBRIM NAČRTOVANJEM LICENCIRANEGA PROJEKTNEGA BIROJA

PET OBMOČIJ VAROVANJA

Standard EN 50131-1 uvaja koncept treh (od petih) koncentričnih con varovanja (zaznavnih območij/senzorskih linij), ki sestavljajo protivlomni sistem:

- prva cona – varovanje notranjih prostorov (hodnik, spalnica, dnevna soba ...),
- druga cona – varovanje zunanjosti objekta (balkoni, terase, vrata in okna),
- tretja cona – varovanje okolice oz. perimetra (dvorišče in ograja/zid).

VARNOSTNI RAZREDI

Centrala mora nadzirati prenosne poti:

- protivlomnih detektorjev;
- vdornih zaščitnih naprav;
- zunanjih vklopnih/izklopnih naprav;
- alarmno-signalnih naprav;
- med decentraliziranimi deli centrale;
- med oddajnikom in sprejemnikom – opreme za prenos alarma, če le-ta ni integralni del centrale.

UPRAVLJANJE PROTIVLOMNEGA SISTEMA JE PREGLEDNO, PREPROSTO IN UPORABNIKOM PRIJAZNO

NAPREDNE TEHNOLOGIJE VAROVANJA

Vgrajujemo profesionalni sistem najvišjega kakovostnega razreda - Tecnoalarm

ZARJA ELEKTRONIKA



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
izr. prof. dr. Denis Čaleta

Trženje:
ICS-Ljubljana
info@ics-institut.si

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
marec 2019

Izvod revije je brezplačen

Naslovnica in slike:
ID 68533754 © Sinemaslow | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

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

Letos smo priča pomembni obletnici, katero predstavlja deseta obletnica organiziranja mednarodne konference Dnevi korporativne varnosti, kakor tudi enaka obletnica delovanja Instituta za korporativne varnostne študije, ICS-Ljubljana. Omenjena konferenca je že davno prerasla nacionalne okvire in tudi v širšem regijskem prostoru predstavlja enega izmed najbolj izpostavljenih dogodkov, s področja korporativne varnosti. To vsekakor dokazuje tudi udeležba najpomembnejših gostov iz poslovnega, političnega in strokovnega okolja. Razmah konference in vedno večje število udeležencev kaže na to, da se zavedanje o pomenu varnosti počasi a vendar vztrajno dviguje. Najbolj prepoznavna rast udeležencev je zaznana ravno iz gospodarskega okolja, k čemur verjetno pripomore dejstvo, da je varnostno okolje, v katerem delujejo poslovne organizacije, vedno bolj zahtevno. Učinkovitega poslovanja si enostavno ni mogoče zamisliti brez dejstva, da je pomembno težišče namenjeno obvladovanju dinamičnih tveganj, s katerimi se soočamo na globalnih trgih. Dodatno prepoznavnost dogodku daje tudi podelitev prestižne nagrade Slovenian Grand Security Award, ki se vsako leto že tradicionalno podeljuje v okviru otvoritvene slovesnosti omenjene konference.

Korporativna varnost je postala eden od najpomembnejših procesov pri delovanju organizacij. Potreba po celovitem pristopu k obvladovanju tveganj danes predstavlja nujo, ki se ji ne more izogniti nobena uspešna organizacija, pa naj si gre za javno ali zasebno organizacijo. V realnem okolju se dogajajo tudi pomembne spremembe, ki pred nas postavljajo nove zahteve po prilagajanju naših aktivnosti in procesov za učinkovitejše izvajanje le teh. V okvir korporativne varnosti se vedno bolj prenaša tudi procese za zagotavljanje informacijske varnosti, saj je fizične, tehnične in informacijske ukrepe nemogoče izvajati ločeno, da bi lahko zagotavljali ustrezno varnost naših organizacij, ki so vedno bolj odvisne od obvladljivega kibernetskega in posledično informacijskega okolja. Človeški potencial še vedno ostaja najpomembnejši del vsakega učinkovitega sistema, saj v primeru neustrezne varnostne osveščenosti predstavlja tudi največji vir tveganja. Zavedanje, da je potrebno ukrepe, s katerimi gradimo učinkovite varnostne sisteme, razvijati tako s tehnološkega vidika, kakor tudi z vidika usposabljanja zaposlenih, je nujna determinanta sodobnih varnostnih sistemov.

V tokratni številki, ki je sicer posvečena mednarodni konferenci Dnevi korporativne varnosti, smo odprli cel niz aktualnih tem. Posebno pozornost namenjamo 10. obletnici delovanja ICS-Ljubljana. K pogovoru smo povabili več zanimivih in izpostavljenih sogovornikov, ki so vsak iz svojega strokovnega stališča pomembno obogatili tokratno številko revije. Posebne teme pa so posvečene kibernetski varnosti, varnosti zaposlenih na potovanjih ter izrednim situacijam v katerih se lahko znajdejo naše organizacije. Izbiri ustreznih metodologij na področju ocenjevanja tveganj, pa posvečamo težiščno pozornost, saj je ta proces, v okviru zagotavljanja zaščite kritične infrastrukture, izrednega pomena.

V uredništvu revije upamo, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji. Za vas se bomo skupaj trudili tudi nadaljnjih deset let.

izr. prof. dr. Denis Čaleta
Glavni urednik



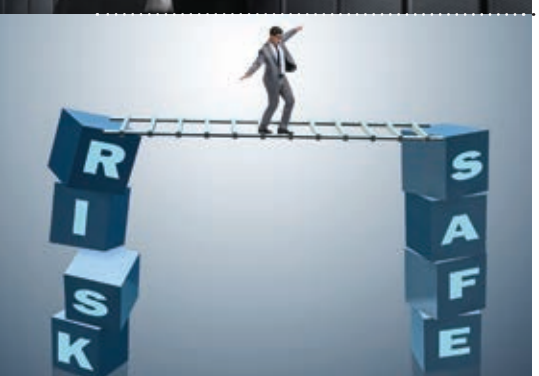
KOLUMNA

PROCES OCENJEVANJA TVEGANJ IN KRITIČNA INFRASTRUKTURA 9



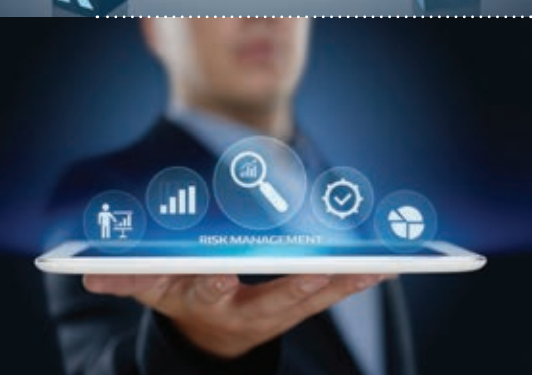
INTERVJU
dr. Uroš Rosa, izvršni direktor, Akrapovič d.d.

UČINKOVITO OBVLADOVANJE KLJUČNIH INFORMACIJ POGOJ ZA USPEŠNO POSLOVANJE PODJETJA 14



ZAZNAVA TVEGANJA: KAKO JO LAHKO IZBOLJŠAMO?

Tveganje je naša osebna, strokovna in družbena preokupacija. Skupni imenovalec čedalje bolj težke odločitve, ko je treba ugotoviti: »Koliko varno je dovolj varno?«, se nanaša na določitev sprejemljivega tveganja v negotovih razmerah. Gre za razprave med znanostjo in družbeno skupnostjo, ki so postavile pod vprašaj obstoj objektivnega zaznavanja tveganja (npr. perspektive raziskovalcev Douglasa, Giddensa in Becka). 24



PROCES UPRAVLJANJA TVEGANJ V KRITIČNI INFRASTRUKTURI NA BAZI STANDARDOV

Tokratno pisanje o kritični infrastrukturi (v nadaljevanju KI) se nanaša na razlago procesa upravljanja tveganj na bazi uveljavljenih standardov. Izhajava iz (izvirne) študije, ki jo je projektna ekipa Inštituta za korporativne varnostne študije lanskega leta izdelala za potrebe Ministrstva za obrambo. 29



SOCIALNI INŽENIRING KOT UMETNOST PSIHOLOŠKE MANIPULACIJE

Socialni inženirji so umetniki manipulacije, ki izkoristijo obnašanje in navade ljudi z namenom pridobitve občutljivih ali zaupnih podatkov, do katerih niso avtorizirani. Napadalci se primarno odločajo za te vrste napadov, ker je v praksi velikokrat lažje izkoristiti človeško naravno nagnjenost k zaupanju, kot zlorabiti programsko opremo žrtve in na ta način priti do občutljivih podatkov. 48

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

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

KORPORATIVNO VARNOST TRDNO ZASIDRALI MED PROCESE VSAKE RESNE POSLOVNE ORGANIZACIJE

»Letos praznujemo 10. obletnico ustanovitve Instituta za korporativne varnostne študije, ICS-Ljubljana. Pot do uspeha je tlakovana s trdim in sistematičnim delom. Rezultatov, ki smo jih dosegli v teh desetih letih, tako v nacionalnem kot tudi mednarodnem okolju, si nismo upali predstavljati tudi v najbolj optimističnih sanjah. Danes praktično ni več organizacije v Republiki Sloveniji, ki se ne bi zavedala potrebe po učinkovitem obvladovanju tveganj.« trdita Vršec in Čaleta.

Letos praznujete 10. obletnico ustanovitve Instituta za korporativne varnostne študije ICS-Ljubljana. Institut postaja na področju korporativne varnosti, vedno bolj referenčna institucija tako v Sloveniji, kot tudi v regiji. Ste zadovoljni s prehojeno potjo?

Čaleta: Ne morem verjeti, da je za nami že deset let. 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 razi-

Slovensko združenje korporativne varnosti predstavlja izredno pomemben del našega delovanja in mu prav zaradi tega namenjamo posebno pozornost. Naša želja, da združenje postane najmočnejša strokovno-referenčna asociacija, je danes postala realnost.

skano 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. Posebej pa me veseli, da korporativna varnost, kot proces v podjetjih, dobiva ustrezno vlogo. Počasi se je začelo sistematično uokvirjati različne razpršene procese v celovit proces korporativne varnosti. Še posebej to velja za fizično in tehnično

*avtor je član Slovenskega združenja korporativne varnosti



varnost, informacijsko varnost, varnost ključnih podatkov, analizo in ocenjevanje tveganj, varnost in zdravje pri delu, neprekinjenost poslovanja in seveda vse kar je povezano z zaščito kritične infrastrukture.

Vršec: Ko se obrnem nazaj in pomislim, kako je bilo na začetku, ko je bil ICS-Ljubljana še v idejnem oblačku, se spominjam, da sem imel po predstavitvi ideje o ustanovitvi inštituta, ki bi razvijal znanja in rešitve na področju korporativne varnosti in upravljanja z varnostnimi tveganji na strateškem nivoju upravljanja večkrat občutek, da petelin spet prezgodaj kikirika. Večina sogovornikov je bila tega mnenja, le peščica njih pa je verjela v to idejo in nas tudi moralno podpirala. Ja, bilo je težko. A že kot ničkolikokrat do sedaj, sem tudi takrat verjel v to idejo in v ljudi, ki so bili takrat okoli mene. Predvsem tu mislim na Denisa, s katerim sva skupaj orala to ledino in utirala razvojno pot inštitutu, na očeta, ki je bil že takrat guru varnostnega menedžmenta in še nekatere druge prijatelje in partnerje, ki so verjeli v naju z Denisom in naju pri tem tudi podpirali. Sedaj lahko rečem, da nama je uspelo, uspelo predvsem v tem, da je podjetniško, gospodarsko in družbeno okolje prepoznalo pomen korporativne varnosti, jo začelo pravilno umeščati v svoje organizacijske strukture in v korporativni varnosti prepoznalo priložnost za učinkovitejše obvladovanje tveganj in zagotavljanje zanesljivejšega delovanja na dolgi rok.

Kateri so tisti dejavniki, ki bi jih posebej izpostavili?

Vršec: Kot rečeno, je bilo najprej potrebno v stroko na pravi način in pravo mesto umestiti pojem korporativne varnosti. Ko nam je to uspelo, smo morali odločevalce v različnih poslovnih okoljih prepričati, da varnost in celovito upravljanje s tveganji ni strošek, ampak investicija, ki organizaciji na dolgi rok prinaša dodano vrednost. Dodano vrednost, ki se izkazuje skozi zmanjševanje škod in izgub, neprekinjenosti poslovanja, povečevanju dobička, krepitvi dobrega imena podjetja in nenazadnje družbeni odgovornosti organizacije. V zadnjem času pa nam je uspel še en preboj. Preboj na področju, kjer smo pričakovali, da bo potrebno vložiti precej več napora, a smo bili očitno tudi na podlagi naših dosedanjih dosežkov zelo prepričljivi in hitro razumljeni. Gre za nujnost povezave dveh, do sedaj povsem razdvojenih in po mnenju večine strokovnjakov nezdružljivih področij, to je področja fizične varnosti (v to vštevam vse kar je povezano s fizičnim in tehničnim varovanjem) in področja informacijske varnosti. Ja res je, uspelo nam je prepričati strokovnjake z obeh področij, da novi varnostni izzivi zahtevajo združitev omenjenih dveh področij, saj je to nujni pogoj, ki bo organizacijam omogočal učinkovito obvladovanje in upravljanje z novimi varnostnimi tveganji in izzivi.

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. Naša želja, da združenje postane najmočnejša strokovno-referenčna asociacija, je danes postala realnost. 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 gospodarske organizacije, ki upravljajo s pomembnimi infrastrukturnimi področji od energetike, prometa pa vse do informacijsko komunikacijskega področja. Posebej pa me veseli, da so svoj interes pri sodelovanju našle tudi pomembne javne institucije, katere še posebej predstavljajo Urad Informacijske pooblaščenke, SI-CERT in Gasilska zveza Slovenije. Seveda pa odlično sodelujemo tudi z ostalimi javnimi institucijami, ki imajo pomembno mesto na področju zakonodajnega urejanja varnosti. 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.

Dnevi korporativne varnosti so postali najbolj odmeven dogodek v celotni regiji s področja obvladovanja varnostnih tveganj. Kakšno je glavno sporočilo in vpliv dogodka?

Čaleta: Temu dogodku v ICS-Ljubljana posvečamo veliko pozornost, saj smo mišljenja, da ta v slovensko okolje prinaša neka nova znanja in pristope, ki so nujni, da se bo dolgoročno zavedanje strateškega managementa in drugih upravljavskih 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. Posebej nas veseli, da na dogodek poleg stroke prihaja vedno več predstavnikov strateškega managementa, kar pomeni, da se to zavedanje počasi, vendar vztrajno krepi tudi pri vodstvenih strukturah v poslovnih organizacijah. Otvoritev dogodka je povezana s podelitvijo prestižnih nagrad »**Slovenian Grand Security Award**«, kjer se izpostavijo najboljši v preteklem letu. 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. 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 pa predstavlja vpliv tega dogodka v širšem regijskem prostoru saj je prepoznan kot ena izmed najbolj kvalitetnih konferenc, kar se kaže tudi v vsakoletnem porastu udeležencev iz tujine.

> Vključevanje v mednarodne znanstvene, raziskovalne, strokovne in poslovne mreže je danes pogoj za razvoj znanj in veščin, ki so predpogoj za učinkovito delovanje na področju upravljanja z novimi varnostnimi izzivi in paradigmami. ICS-Ljubljana v zadnjih letih postaja vse pomembnejši partner na tem področju tudi v mednarodnem okolju.

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 si 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, prinesla določeno konkurenčno prednost pred tekmeci in s tem tudi uspešnejše in učinkovitejše poslovanje. Trenutno smo prisotni v dveh največjih projektih, ki potekajo v okviru raziskovalnega programa HORIZONT 2020. Projekt DEFENDER je povezan z Zaščito energetske kritične infrastrukture EU, projekt INFRASTRESS pa obravnava zaščito kritičnih industrijskih postrojenj EU, ki sodijo v okvir kritične infrastrukture. Prisotni pa smo tudi v celem nizu ostalih projektov EU in NATO. 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.



Na področju svetovanja različnim gospodarskim subjektom, upravljavcem kritične infrastrukture, izvajalcem bistvenih storitev, državnim organom in javnim inštitucijam imamo bogate izkušnje in vrhunske reference.

Revija korporativna varnost z vami ravno tako praznuje ta pomemben jubilej. Kakšno moč ima ta tiskani medij v Republiki Sloveniji na dvigovanje varnostnega zavedanja in širjenje strokovnih znanj?

Čaleta: Reviji Korporativna varnost namenjamo veliko energije in jo predvsem vidimo kot ključen moment pri dvigovanju varnostnega zavedanja v širši družbeni skupnosti, predvsem poslovni. Revija je namreč brezplačna in jo posredujemo na naslove vsega strateškega managementa v slovensko gospodarstvo in javno upravo. Seveda pa je dostopna tudi v elektronski obliki na spletni strani ICS-Ljubljana. Revija res zagotavlja aktualne in visoko strokovne vsebine, zato je dobrodošlo branje za vse strokovnjake s področja korporativne varnosti, obvladovanja varnostnih tveganj, zagotavljanja neprekinjenega delovanja, kibernetske varnosti in varnosti povezane s ključnim kadrovskim potencialom.

Vršec: Izjemno sem ponosen tudi na našo revijo Korporativna varnost, ki je postala vodilni (če ne celo edini) strokovni tiskani medij na širšem območju Adriatic regije, ki obravnava aktualno problematiko s področja korporativne varnosti, informacijske varnosti, Risk menedžmenta, neprekinjenega poslovanja in še mnogih drugih z varnostjo povezanih področij. Ob tej priliki bi se rad iskreno zahvalil uredniškemu odboru revije, vsem dosedanjim avtorjem in ostalim deležnikom brez katerih revija Korporativna varnost ne bi postala to kar je. Eden od posebnih izzivov za prihodnost je, da bi revija Korporativna varnost postala globalni tiskani medij za obravnavo aktualnih vprašanj in izzivov na prej omenjenih strokovnih področjih in bi dosegla tak faktor vpliva, da bi bila zanimiva za objave najbolj odmevnih znanstveno raziskovalnih člankov.

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

Vršec: Vključevanje v mednarodne znanstvene, raziskovalne, strokovne in poslovne mreže je danes pogoj za razvoj znanj in veščin, ki so predpogoj za učinkovito delovanje na področju upravljanja z novimi varnostnimi izzivi in paradigmami. ICS-Ljubljana v zadnjih letih postaja vse pomembnejši partner na tem področju tudi v mednarodnem okolju. To izkazujemo z vključenostjo v dva največja mednarodna projekta na področju energetike in logistike in še v nekatere druge evropske projekte. Trenutno smo aktivni in pomembni partnerji v skupini več kot 50 eminentnih evropskih podjetij in znanstveno raziskovalnih inštitucijah, ki delujejo na celotnem območju EU in celo zunaj njenih meja. Naš pogled pa sega še naprej. Smo v procesu vzpostavljanja evropske projektne skupine, ki bo iskala povsem nove rešitve na področju upravljanja z varnostnimi tveganji in bo v te procese vključevala tudi najsodobnejše rešitve s področja umetne inteligence. Prepričani smo namreč, da bi z uporabo umetne inteligence v procesih upravljanja z varnostnimi tveganji lahko bistveno izboljšali učinkovitost upravljana s tveganji, ter hitrost in kakovost sprejemanja odločitev tudi v najbolj kritičnih in stresnih situacijah.



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 nov pristop. Nam lahko navedete nekaj primerov tega sodelovanja?

Vršec: Res je. Na področju svetovanja različnim gospodarskim subjektom, upravljavcem kritične infrastrukture, izvajalcem bistvenih storitev, državnim organom in javnim inštitucijam imamo bogate izkušnje in vrhunske reference. V procesu sodelovanja s končnimi uporabniki smo razvijali nova znanja in rešitve in jih skozi čas nadgrajevali in prilagajali konkretnim uporabniškim zahtevam in specifikam varnostnega okolja. V zadnjem času veliko energije usmerjamo v razvoj novih rešitev in iskanju novih sinergijskih učinkov kot posledice povezovanja ali celo združevanja področij fizične in informacijske varnosti, centralizaciji upravljanja z varnostnimi sistemi, optimizaciji stroškov varovanja in povečevanju učinkovitosti sistemov upravljanja s tveganji. Tu imamo izvedenih že kar nekaj uspešnih projektov, ki že izkazujejo svoj namen v praksi. Vse bolj pa postajamo aktivni tudi na področju odkrivanja ranljivosti v delovanju informacijskih sistemov, ranljivosti pri uporabi sodobnih informacijskih tehnologij, ranljivosti pri uporabi raznih socialnih omrežij, ranljivosti na področju varnosti osebnih, tajnih in poslovnih podatkov in na splošno ranljivosti na področju upravljanja z informacijami. Na tem področju naš čaka neizmerno veliko novih izzivov, saj digitalizacija procesov in poslovanja ter digitalna transformacija družbe kot take, prinaša nove, do sedaj še neznane varnostne pojave in izzive. ■

100-ODSTOTNO PRIPRAVLJENI

Hiter odziv je najboljša obramba pred poslovno škodo.

NIL-OV VARNOSTNO OPERATIVNI CENTER



NIL

nil.com

Avtor: izr. prof. dr. Denis Čaleta / Institut za korporativne varnostne študije*



KOLUMNA

PROCES OCENJEVANJA TVEGANJ IN KRITIČNA INFRASTRUKTURA

Zadnje obdobje v strokovnem krogu poteka pomembna razprava o vlogi procesa ocenjevanja tveganj za ustrezno zaščito kritične infrastrukture. Splošna ugotovitev je, da učinkovit in sistematičen proces ocenjevanja tveganj predstavlja bazo za praktično vse ukrepe, ki jih izvajamo v nadaljevanju, s ciljem celovitosti vzpostavljanja zaščite kritične infrastrukture in zagotavljanja njenega neprekinjenega delovanja.

Podrobna analiza stanja na področju metodoloških pristopov k ocenjevanju tveganj, pa nas postavi v dokaj neprijetno situacijo. Pred nami se namreč odpre cel niz metodoloških pristopov in različnih pogledov na proces ocenjevanja tveganj. Deloma je to razumljivo, saj je globalno varnostno okolje zelo kompleksno, kakor tudi tveganja, katerim so izpostavljene naše organizacije. Če ob tem upoštevamo še različne sektorje kritične infrastrukture, ki imajo svoje posebnosti in določene zakonitosti, se hitro zavemo, da je sprejem ene same celovite metodologije praktično nemogoč. Kljub tej ugotovitvi, pa je potrebno zelo jasno poudariti, da za sistematični pristop, h kateremu mora težiti država pri urejanju teh pomembnih področij za nemoteno delovanje širše družbene skupnosti, potrebujemo celovite pristope in vsaj minimalne skupne standarde. Osnova minimalnih standardov v procesu ocenjevanja tveganj, mora biti tista skupna izhodiščna točka, ki zagotavlja, da so izmerjene vrednosti med posameznimi sektorji kritične infrastrukture primerljive in v skladu s tem tudi osnova za graditev nacionalnih ukrepov za učinkovito zaščito kritične infrastrukture. Pri tem je potrebno upoštevati še ključno komponento, ki se zrcali skozi nadaljnji proces ocenjevanja in načrtovanja potrebnih virov za izvajanje ustreznih ukrepov zaščite kritične infrastrukture. Če so izhodiščne osnove tako različne, kot smo jim v praksi zaščite kritične infrastrukture v Republiki Sloveniji danes priča, je nemogoče zagotavljati neke realne in celovite ocene.

Osnova minimalnih standardov v procesu ocenjevanja tveganj, mora biti tista skupna izhodiščna točka, ki zagotavlja, da so izmerjene vrednosti med posameznimi sektorji kritične infrastrukture primerljive in v skladu s tem tudi osnova za graditev nacionalnih ukrepov za učinkovito zaščito kritične infrastrukture.

V nadaljevanju se vrnimo v, po naši oceni, izhodiščno stopnjo, iz katere v nadaljevanju izhaja večina problemov nesistemskega in neučinkovitega uvajanja procesov ocenjevanja tveganj v organizacijah, ki v Republiki Sloveniji upravljajo kritično infrastrukturo. Država s svojim nekonsistentnim pristopom sprejemanja zakonodajnih aktov, na področju med katere sodi tudi zaščita kritične infrastrukture, prinaša parcialne pristope posameznih ministrstev. Vlada Republike Slovenije in kasneje tudi Državni zbor nista bila sposobna izvesti konsolidacijo in predvsem poenostavitev zakonskih aktov, ki bi bili bolj pregledni, učinkoviti in sistematično naravnani. Nasprotno, v državi še naprej ubiramo pot nadaljnjega spreje-

*avtor je član Slovenskega združenja korporativne varnosti

manja zakonskih in podzakonskih predpisov, ki namesto jasne ureditve, še dodatno kompliciraju in predvsem birokratsko urejajo posamezna pomembna področja. Če se osredotočimo samo na upravljalce kritične infrastrukture, potem zelo hitro lahko ugotovimo, da je večina subjektov, ki upravlja s kritično infrastrukturo, poleg Zakona o kritični infrastrukturi, podvržena še celemu nizu drugih zakonskih in podzakonskih predpisov, ki vsi prinašajo dokaj različne metodološke pristope, ne samo pri procesu ocenjevanja tveganj, temveč pri celem nizu drugih sistemskih pristopov za zagotavljanje neprekinjenosti delovanja teh ključnih infrastrukturnih zmogljivosti. Ti subjekti so, kot ponudniki bistvenih storitev, praktično vsi podvrženi Zakonu o informacijski varnosti, Uredbi o obveznem organiziranju varovanja, predpisom s področja obrambe, kjer se znajdejo kot subjekti posebnega pomena za obrambo, na del njih pa vpliva tudi Zakon o elektronskih komunikacijah (ZEKom) in še bi lahko naštevali. Da je ta konfuznost še kompleksnejša, tudi ureditev znotraj EU ne prinaša korakov pri zagotavljanju sinergij, saj se posamezni deli birokratskega aparata EU ukvarjajo s predpisovanjem posameznih temeljnih področij. Tudi različne agencije, ki v nadaljevanju skrbijo za uveljavljanje in koordinacijo aktivnosti na posameznih področjih, v določenih primerih med seboj niso ustrezno usklajene. Ta neusklajenost ima še poseben vpliv ravno na področju izbire ustreznih metodologij za ocenjevanje tveganj, ki bi v nadaljevanju lahko nudile ustrezno osnovo za izvedbo vseh nadaljnjih ukrepov, predvsem v smeri večje sistematičnosti, učinkovitosti in preprečevanja celega niza varnostnih praznin, ki nastajajo zaradi tako različnih pristopov.



Na podlagi Zakona o kritični infrastrukturi je bilo predvideno, da bi moralo ministrstvo za obrambo sprejeti ustrezno Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture. Glede na dejstvo, da je podobne procese potrebno izvesti tudi na podlagi Zakona o informacijski varnosti, je bila to odlična priložnost za poenotenje pristopov in končno usklajeno delovanje države na teh, za nacionalno varnost in neprekinjenost delovanja družbe, ključnih procesov. Na žalost je bil pristop priprave vsebine Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije, ki ga je sprejelo Ministrstvo za obrambo, ponovno tehnokratski. Sprejem tako oblikovanega akta s tako splošno vsebino, ki z ničemer ne izboljšuje ali usmerja procesov na področju ocenjevanja tveganj za delovanje kritične infrastrukture, je zagotovil samo birokratsko realizacijo zakonskega navodila, v ničemer pa ni pripomogel k vsebinski vrednosti ureditve tega kompleksnega področja. V strokovni javnosti in med samimi upravljalci kritične infrastrukture so bila izražena jasna pričakovanja, da bodo postavljeni jasni minimalni metodološki okviri, ki bodo omogočali podobno izhodiščno osnovo procesa ocenjevanja tveganj, ne glede na to v katerem sektorju upravljalec deluje. Postavljeni normativi so zastavljeni tako široko in nedefinirano, da bi tako oblikovani kvečjemu sodili v samo zakonsko materijo, nikakor pa ne v navodilo, od katerega se pričakuje zelo podrobne usmeritve in metodološka napotila. Trenutno postavljen okvir dopušča tako različne subjektivno izvedene ocene na področju ocenjevanja tveganj, da bo že znotraj posameznih sektorjev nemogoče izvajati določene analize in pripravo učinkovitih ukrepov za zaščito kritične infrastrukture.

V tem trenutku imamo dve možnosti rešitve nastale situacije. Da ministrstvo za obrambo dopolne omenjeni akt s konkretnejšimi metodološkimi minimalnimi standardi, oz. da se konkretneje določijo metodološki pristopi na posameznih sektorjih kritične infrastrukture. V tem drugem pristopu se lahko pojavijo določene težave, saj so določeni upravljalci zaradi specifike svojih procesov vezani na več podsektorjev kritične infrastrukture. V vsakem primeru je potrebno v čim krajšem roku sektorskim koordinatorjem posredovati študijo z nazivom »Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture«, ki jo je za ministrstvo za obrambo izdelala projektna skupina iz ICS-Ljubljana.

Ključen moment v kratkoročnem obdobju razvoja teh zahtevnih procesov, bo ustrezno usposobiti sektorske koordinatorje in sprejeti posamezno metodološko nadgradnjo, ki jo v nadaljevanju splošnega metodološkega pristopa, zahteva specifika posameznih podsektorjev. Dolgoročno pa bo nujno potrebno v Republiki Sloveniji angažirati vse resurse, da se bo izvedel temeljit pregled in novo oblikovanje zakonskih podlag za delovanje teh ključnih področij, ki bodo izvedene v smeri racionalizacije procesov in predvsem večje optimizacije. Tukaj moramo doseči večjo učinkovitost in preglednost procesov z jasnim ciljem racionaliziranja in povečevanja učinkovitosti omejenih virov, ki jih družba na vseh nivojih namenja za obvladovanje ključnih tveganj za delovanje kritične infrastrukture. ■

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.

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

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

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

www.ics-institut.si

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih mesečnih strokovnih srečanjih,
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS-Ljubljana,
- popusti pri nakupu izdanih publikacij ICS-Ljubljana,
- brezplačna naročnina na revijo Korporativna varnost.

Dodatne ugodnosti za korporacijske člane združenja:

- postavitev logotipa na spletno stran ICS-Ljubljana in v reviji Korporativna varnost na straneh namenjenih združenju,
- popusti pri oglaševanju v reviji Korporativna varnost in na konferencah v organizaciji ICS-Ljubljana,
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS-Ljubljana za vse zaposlene v podjetju,
- popusti pri članarinah za strokovne člane, ki prihajajo iz vrst organizacij katere so korporacijski člani združenja,
- korporacijskega člana v združenju zastopata dve osebi,
- druge bonitete objavljene na spletnih straneh združenja.

Članstvo v **SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI**

vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

Občina Slovenska Bistrica

Pošta Slovenije

Informacijske storitve in inženiring, d.d. INFORMATIKA

triglav

PETROL Energija za življenje

Telekom Slovenije

AKRAPOVIČ

interblock Luxury Gaming Products

spica

Ford SUMMIT AVTO

ELEKTRO LJUBLJANA

Elita i.b. d.o.o.

SIEMENS

DARS

CINKARNA

UNISTAR PRO

Nova KBM Pripravljeni na jutri

LON

ZARJA ELEKTRONIKA

Slovenske železnice

energetika ljubljana

www.ics-institut.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
dr. Uroš Rosa, izvršni direktor, Akrapovič d.d.*

UČINKOVITO OBVLADOVANJE KLJUČNIH INFORMACIJ POGOJ ZA USPEŠNO POSLOVANJE PODJETJA

Podjetje AKRAPOVIČ je dobitnik prestižne nagrade Slovenian Grand Security Award v kategoriji najbolj varno podjetje za leto 2018. Prizadevanja za učinkovito obvladovanje varnostnih tveganj se kažejo v dobrih rezultatih poslovanja, smeri novih izzivov in poslovnih priložnosti. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z dr. Urošem Roso.

Podjetje AKRAPOVIČ d.d. predstavlja enega od vodilnih podjetij na področju izpušnih sistemov. Nam lahko, prosim, podrobneje pojasnite, kaj vaše podjetje dela boljše od konkurence.

Podjetje Akrapovič d.d. največ pozornosti namenja kakovosti produkta. Trudimo se, da bi bil vsak izdelek boljši od obstoječih, serijskih in tudi konkurenčnih produktov, zato morajo biti visokokakovostni in dosegati najboljše možne rezultate pri vseh opravljenih meritvah. Pri izboljšavah produkta veliko pozornosti namenjamo zniževanju teže ter povečevanju zmogljivosti in se osredotočamo predvsem na podrobnosti. Z investicijami v razvoj tehnologije in spodbujanjem inovativnosti, ustvarjamo svoje tehnološke rešitve, s katerimi dosegamo želene rezultate. Že od začetka delovanja podjetja, poleg razvoja produkta, razvijamo tudi blagovno znamko, ki ta izdelek podpira in ki je postala prepoznavna po vsem svetu.



S svojim poslovanjem ste močno prisotni v mednarodnem okolju, kjer so varnostna tveganja še posebej specifična. Ali svoje odločitve o širitvi poslovanja na določene trge temeljite na strateških anali-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



zah varnostnega okolja ali bolj upoštevate poslovne možnosti?

Oboje. Pri širitvi poslovanja upoštevamo poslovne priložnosti, ki se nam ponujajo. Poleg tega pred širitvijo vedno izvedemo analizo tveganja in analizo varnosti poslovnega okolja. V današnjem svetu je to skoraj neizogibno, saj nekaterih poslovnih priložnosti ne moreš izkoristiti, ne da bi izgubil druge priložnosti. Poslovanje v nekaterih državah prinaša večje varnostno in tudi poslovno tveganje, saj lahko s takim sodelovanjem pridobiš prepoved poslovanja v katerih izmed drugih držav. Poleg takih političnih tveganj so varnostna tveganja povezana tudi s segmenti, na katere vstopaš – z vstopom na nove segmente se tveganje povečuje.

Ste podjetje, ki veliko sredstev vlagate v lasten razvoj novih tehnoloških rešitev. Nam lahko zaupate svojo vizijo na tem področju za prihodnje obdobje?

Veliko vlagamo v razvoj in raziskave novih materialov, tehnoloških rešitev in novih inovacij, da bi naredili čim lažje in čim bolj tehnično dovršene izpušne sisteme, ki bodo lahko izpolnjevali vse najzahtevnejše regulative. V preteklih letih smo veliko investirali tudi v večjo kompetentnost razvojnih ekip in v dodatne storitve, ki jih ponujamo kupcem. V razvoj novih rešitev investiramo tudi na področju livarne in proizvodnje. Na tem področju smo v zadnjih letih veliko vlagali v infrastrukturo, lani pa smo začeli projekt digitalizacije proizvodnje. Ta projekt bo dvignil tehnološko raven podjetja in nam omogočil hitrejše prilagajanje zahtevam trga.

Kako so po vašem mnenju pomembne ključne informacije podjetja v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču. Ali varovanju teh informacij v podjetju Akrapovič namenjate veliko pozornost?

To je zelo pomembno področje, saj so ključna znanja, ki jih ima vsako podjetje, njegova glavna konkurenčna prednost. Vsako podjetje mora najprej prepoznati ta ključna strateška znanja, tehnologije in druge pomembne informacije. Na podlagi tega se mora odločiti, kako jih bo uporabilo, da bo konkurenčno prednost v prihodnosti tudi ohranilo ali jo povečalo. Pri varovanju informacij je veliko dela na področju intelektualne lastnine, ki jo lahko zaščitimo s patenti, modeli in izumi. Za podjetje so pomembne tudi tiste informacije, ki jih ima v znanju (know-how) in ki jih tako ne more ustrezno zavarovati. Iz tega razloga je zato zelo pomembno, da ostanejo znotraj podjetja.



Glede na to, da ste visoko tehnološko podjetje, ste vi in posredno tudi vaše stranke, v svoji dejavnosti zelo izpostavljene kibernetskim tveganjem. Kakšne ukrepe v podjetju izvajate na področju zagotavljanja informacijske varnosti?

Ukrepi, ki jih uporablja naše podjetje, sledijo standardom industrije. Interno in prek zunanjih strokovnjakov redno osvežujemo strojno opremo in tudi mrežne opreme. Poleg tega skrbimo za ozaveščanje zaposlenih o komunikaciji po elektronski pošti in o varni uporabi mobilnih telefonov. Predvsem komunikacija zaupne narave na mobilnem telefonu je za podjetje veliko tveganje, zlasti če telefon pride v napačne roke (se izgubi, je ukraden). Enako je s prenosnimi računalniki. Poleg tega uporabljamo tudi storitve zunanjih strokovnjakov za analize tveganja in varnosti našega omrežja.

Kako uspete v podjetju zagotavljati uravnoteženost med na eni strani zelo restriktivnimi varnostnimi zahtevami varovanja ključnih informacij organizacije in na drugi strani raziskovalno iniciativnostjo, ki je včasih zelo občutljiva na prevelike omejitve delovnega okolja?

Glavne raziskovalne dejavnosti in inovacije izvajamo v podjetju. Storitev zunanjih izvajalcev uporabljamo samo za nekatere zelo specifične segmente, ki ne razkrivajo dela na preostali celoti. V primeru sodelovanja z zunanjimi izvajalci investiramo v njihovo storitev in ne dopustimo uporabe pridobljenih podatkov za strokovne članke. Zaposleni v podjetju so seznanjeni s temi varnostnimi zahtevami in se zavedajo pomembnosti informacij, ki jih uporabljajo. Poleg tega vse zaposlene vežejo tudi pogodbe o varovanju tajnosti podatkov.

Ste letošnji prejemniki prestižne nagrade Slovenian Grand Security Award v kategoriji »Najbolj varno podjetje«. Nam lahko zaupate, kaj vam pomeni prejem take nagrade?

Za podjetje Akrapovič d.d. je ta prestižna nagrada priznanje za dolgoletni trud na področju varovanja informacij, znanja in ustrezne strukturiranosti podjetja.

Vaše podjetje je tudi eden od korporativnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s področja korporativne varnosti potrebne in lahko prinesejo v naš prostor dodatno kvaliteto?

Seveda. Taka združenja so zelo pomembna, saj pripomorejo k izboljšanju kakovosti varnostnih ukrepov na področju korporativne varnosti. Omogočajo nam koristno izmenjavo mnenj in izkušenj ter s tem pripomorejo k večanju znanja na tem področju. ■

10. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

13. – 14. MAREC 2019



PODELIJO SE 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 TER IZVIRNOST PRIJAVLJENIH UDELEŽENCEV V NASLEDNJIH KATEGORIJAH:

- NAJBOLJ VARNO PODJETJE
- NAJBOLJŠA KNJIGA S PODROČJA VARNOSTI
- NAJBOLJ VARNO MESTO/OBČINA
- KORPORATIVNO VARNOSTNI MANAGER LETA
- NAJBOLJ INOVATIVNA VARNOSTNA REŠITEV
- INOVATIVNA MEDIJSKA PROMOCIJA VARNOSTI

VEČ O NAGRADI IN NAGRAJENCIH NA SPLETNI STRANI INSTITUTA WWW.ICS-INSTITUT.SI!

Nadzor in varnost, združena v inovativen elektronski sistem pristopa





Neomejena fleksibilnost pri zagotavljanju kontrole dostopa, ki ne zahteva večjih posegov.

- Kombinacija ključev in elektronskih medijev.
- Brez predelave vrat in ožičevanja.
- On-line sistem delovanja.
- Nizka investicija, veliko prednosti.
- Preprosto in samostojno spreminjanje pravic uporabnikom.
- Pregled nad preteklimi vstopi.
- Blokiranje izgubljenih medijev in ustvarjanje novih avtorizacij.
- Na voljo različne komponente: elektronski ščit, digitalni cilinder, pametna kljuka, digitalna obešanka, čitalec ...

Varnostni prehodi za nadzorovan dostop oseb na občutljiva območja





- Visoka in nizka vrtljiva vrata, hitri prehodi, plačljivi prehodi ...
- Možnost neposrednega preverjanja kartic, čipov ali kart.
- Integracija z obstoječimi sistemi.
- Nižji stroški fizičnega varovanja.
- Zvočni ali svetlobni alarmi.
- Primerno za velik pretok uporabnikov.

IDealni partner za identifikacijo in varnost

ID Shop, d. o. o. Litostrojska 44d, 1000 Ljubljana
T: +386 (0)1 500 40 50
E: info@idshop.si **W:** www.idshop.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Matjaž Peklaj, Vodja varovanja, Kabinet direktorja,
Kontrola zračnega prometa Slovenije*

KORPORATIVNA VARNOST KLJUČEN DEJAVNIK ZA OBVLADOVANJE TVEGANJ V ORGANIZACIJAH KRITIČNE INFRASTRUKTURE

V današnjem kompleksnem svetu je zagotavljanje neprekinjenosti delovanja organizacij, ki upravljajo s kritično infrastrukturo, nujna komponenta za uspešno funkcioniranje širše družbene skupnosti. Korporativna varnost ima v tem okviru posebej izraženo vlogo in odgovornost.

Obvladovanje varnostnih tveganj je zelo pomembna nit vaše strokovne kariere. Nam lahko poveste katera so ključna področja pristojnosti, ki ste jih v svoji bogati karieri konkretno izvajali?

Obvladovanje varnostnih tveganj je področje, ki je neločljivo povezano s področjem zagotavljana varnosti v najširšem pomenu, kar je tudi moja naloga v podjetju. Vpet sem v zagotavljanje fizične in tehnične varnosti, informacijske varnosti, obrambnega načrtovanja, požarne varnosti, že prej omenjeno ocenjevanje tveganj, vse to pa izvajam skupaj z mojimi izvrstnimi sodelavci.

g. Matjaž Peklaj je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2018«

V zadnjem obdobju ste zelo močno vpeti v zagotavljanje določenih procesov korporativne varnosti v Kontroli zračnega prometa Slovenije, d.o.o. Menite, da je ustrezno razumevanje sprememb kompleksnega varnostnega okolja lahko konkurenčna prednost podjetij?

Vsekakor. Ciljno spremljanje, razumevanje, prilagajanje oziroma odzivanje na spremembe v varnostnem okolju, je po mojem mnenju eden od pomembnejših elementov zagotavljanja konkurenčnosti podjetij. Razumevanje sprememb v kompleksnem varnostnem okolju je pomembno z vidika kreiranja in odzivanja sistema varnosti v podjetju, saj le-ta zagotavlja adekvatno okolje za razvoj in delovanje poslovnih procesov.

Primeren varnosti sistem, v najširšem pomenu besede, zagotavlja tudi odpornost podjetja na posamezne varnostne dogodke oziroma pojave, da le-to lahko nadaljuje z izvajanjem svojega poslanstva oziroma

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



se lahko dvigne na višjo tehnološko raven in omogoča nadaljnjo varno, stabilno in široko poslovanje oziroma izpolnjevanje zahtev do svojih odjemalcev.

Kontrola zračnega prometa Slovenije, d.o.o. predstavlja podjetje, ki se ukvarja z zelo specifično dejavnostjo in je v določenih procesih vsekakor pomemben del nacionalne kritične infrastrukture. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Obvladovanje tveganj v našem podjetju je kompleksen proces. Gre za obsežno nalogo, ki se dnevno izvaja na več ravneh, z glavnim ciljem; stalnim zagotavljanjem varnosti v zračnem prometu. Kot element kritične infrastrukture moramo pri ocenjevanju tveganj upoštevati tudi različne akterje v mednarodnem varnostnem okolju, kar v določenih primerih še oteži samo vrednotenje tveganj.

Procesi, ki se izvajajo za ocenjevanje tveganj, so med seboj soodvisni, sprememba, ki se zgodi v enem procesu vpliva oziroma lahko vpliva na vse in naj bo še tako majhna, je nikakor ne smemo zanemariti. Ob tem pa se nam ob izvajanju ocenjevanja tveganj konstantno pojavlja vprašanje, do katerega nivoja je smiselno krepiti samo odpornost sistema oziroma procesov.

Kibernetska varnost je v vaši dejavnosti izrednega pomena. Kako v vašem podjetju ocenjujete izvajanje potrebnih ukrepov na tem kompleksnem področju?

Zagotavljanje kibernetske varnosti je v naši družbi, kot ste omenili, izrednega pomena. Podjetje je vpeto v mednarodno okolje in je element civilnega letalstva, pri tem pa za svoje delovanje uporablja širok nabor informacijsko komunikacijskih tehnologij. Vsekakor se je v vsakem trenutku potrebno prilagajati spremembam, trendom in dogodkom, ki se dogajajo v kibernetskem prostoru. V naši dejavnosti je potrebno pred uvedbo posameznega novega ukrepa ali tehnologije pripraviti ustrezno oceno tveganj, kar posledično lahko podaljša oziroma podaljšuje odzivni čas na nepredvidene dogodke.

V zadnjem obdobju je v Sloveniji prišlo do posameznih premikov na področju zagotavljanja kibernetske varnosti, vendar je potrebno to področje razvijati še naprej in slediti posameznim drugim evropskim državam, ki temu področju namenjajo veliko več pozornosti.

V zadnjem obdobju je v Sloveniji prišlo do posameznih premikov na področju zagotavljanja kibernetske varnosti, vendar je potrebno to področje razvijati še naprej in slediti posameznim drugim evropskim državam, ki temu področju namenjajo veliko več pozornosti.

Se v Republiki Sloveniji po vaše dovolj zavedamo pomembnosti področja kibernetske varnosti? So ukrepi, ki jih izvaja država na tem področju ustrezni ali pogrešate konkretnejše ukrepe?

Zavedanje o pomenu kibernetske varnosti počasi napreduje. Veliko imamo še za postoriti, tako na ravni države, kot na ravni podjetja. Dejstvo je, da se kibernetski prostor konstantno spreminja, posledično je potrebno, da se področje kibernetske varnosti konstantno prilagaja okolju. Na ravni države so bili sprejeti posamezni normativno pravni akti, ki pa morda v celoti še niso povsem vpeljani.

V Sloveniji se v zadnjem obdobju pojavlja večje število podjetij, ki tržijo različne storitve povezane z zagotavljanjem kibernetske varnosti, dejstvo pa je, da je le malo teh kvalitetnih oziroma povsem kompetentnih. Npr. izvajanje penetracijskih testov še ni zagotavljanje kibernetske varnosti, je le eden od elementov. Ob tem moram tudi poudariti, da moramo naročniki testov natančno vedeti katere segmente omrežij želimo, da se pregledajo in na kakšen način, hrkati imeti dovolj znanja, da lahko usmerjamo izvajalce takih testiranj, rezultate razumemo in jih znamo postaviti v kontekst.

Nam lahko zaupate kako pomemben je v takih primerih učinkovit sistem varovanja ključnih poslovnih informacij.

Učinkovit sistem varovanja poslovnih informacij se, po mojem mnenju, začne že z samo identifikacijo le-teh. Za podjetje ali organizacijo je najpomembnejše, da je sposobna identificirati ključne poslovne informacije, saj jih le-tako lahko ustrezno ščiti, hkrati pa ne ustvarja viška ukrepov (»overhead-a«) tam, kjer to ni potrebno.

Zavedanje o pomenu kibernetske varnosti počasi napreduje. Veliko imamo še za postoriti, tako na ravni države, kot na ravni podjetja. Dejstvo je, da se kibernetski prostor konstantno spreminja, posledično je potrebno, da se področje kibernetske varnosti konstantno prilagaja okolju.

Sam sistem varovanja informacij je močan toliko, kot njegov najšibkejši člen. Dostikrat se veliko sredstev vlaga v sisteme (zaščite) varovanja informacij, ob tem pa se pozablja na druge deležnike, kot na primer zaposlene in ustrezne postopke, ki so dostikrat ključ za uspešno delovanje sistema, hkrati pa je potrebno sinhronizirano delovanje vsem elementov sistema, saj bo sistem varovanja informacij le tako deloval uspešno oziroma dosegal cilje, ki jih organizacija in okolje v katerem deluje postavlja pred njih.

Kako pristopate k prepričevanju strateškega managementa, da za delovanje procesov korporativne varnosti nameni ustrezne organizacijske in finančne vire?

V prvi vrsti smo zadovoljni, da imamo v našem podjetju strateški management, ki razume potrebe po ustreznih virih, tako organizacijskih, kadrovskih in finančnih, hkrati pa se tudi dobro zaveda obstoja tako varnostnih, kot tudi drugih tveganj, ki jih je potrebno ustrezno naslavljati. Podjetje deluje v visoko regulirani dejavnosti, kjer so posamezni standardi in zahteve natančno določeni, hkrati pa vodje področij, pripravljamo predloge za izboljšave, podprte z analizo, ter stalnim spremljanjem uspešnosti in učinkovitosti naših procesov.

Verjetno 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?

Občutek imam, da se je zavedanje strateškega managementa v Sloveniji o pomembnosti varnosti v podjetjih, predvsem informacijske varnosti, izboljšalo, malo manj pa zavedanje o pomembnosti fizične varnosti oziroma prepletenosti posameznih področij varnosti. Posamezno področje ne more uspešno delovati brez sodelovanja ali odsotnosti drugega. Morda področja varnosti še ne jemljejo kot možnosti za konkurenčno prednost, se pa vsekakor zavedajo, da je varnost podjetja osnova za dobro in predvsem stabilno poslovanje družbe.

Je vlaganje v izobraževanje kadrovskih potencialov organizacij lahko tista potrebna kvaliteta, ki tudi na področju varnostnega zavedanja loči uspešna podjetja od povprečnih?

Ustrezno in ciljno naravnano izobraževanje zaposlenih je ključna in nujna prvina za zagotavljanje ustreznega varnostnega sistema v podjetju. Zaposleni morajo imeti visoko varnostno kulturo, ki jo ustvarimo z ozaveščanjem in izobraževanjem zaposlenih. Še posebej pomembno, je po mojem mnenju, izobraževanje ključnih kadrov, tudi o varnosti in varnostnih tveganjih, saj so le-ti pogostokrat ciljna tarča napadov, vdorov in drugih kriminalnih dejanj. Varnostna tveganja se danes spreminjajo hitreje kot kdaj koli, zato je izobraževanje in samozavedanje tisto, ki nas naredi odpornejše na zunanje varnostne vplive.

Vaše podjetje je tudi eden od pomembnih korporativnih 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?

Združevanje strokovnjakov s področja varnosti je koristno in izmenjava izkušenj med kolegi je vedno dobrodošla. Združenja lahko pripomorejo k širitvi dobrih praks med člani, hkrati pa z osveščanjem strokovne javnosti, v določenih primerih pa tudi širše javnosti, širijo zavedanje o pomenu varnosti.

Kaj vam pomeni prejeta nagrada Slovenian Grand Security Award v kategoriji »korporativno varnostni manager leta«?

Nagrado jemljem predvsem kot pohvalo in priznanje za prizadevanja vseh mojih sodelavcev in kolegov, s katerimi se trudimo za doseganje ciljev in upam, da bomo še naprej izvajali dobre projekte. ■





Vodilno globalno podjetje na področju varovanja

Dahua Technology se uvršča med vodilna podjetja na področju rešitev z videonadzorne sisteme.

Zaposluje več kod 16,000 ljudi na globalnem področju. Njene rešitve so v uporabi v več kod 180 državah.

CE FC UL RoHS ISO 9001:2000

www.dahuasecurity.com

DAHUA TECHNOLOGY
Cesta na Okroglo 7, 4202 Naklo, Slovenija
www.dahuasecurity.com

Avtor: doc. dr. Brane Bertoncelj / Slovensko združenje korporativne varnosti*



ZAZNAVA TVEGANJA: KAKO JO LAHKO IZBOLJŠAMO?

Tveganje je naša osebna, strokovna in družbena preokupacija. Skupni imenovalec čedalje bolj težke odločitve, ko je treba ugotoviti: »Koliko varno je dovolj varno?«, se nanaša na določitev sprejemljivega tveganja v negotovih razmerah. Gre za razprave med znanostjo in družbeno skupnostjo, ki so postavile pod vprašaj obstoj objektivnega zaznavanja tveganja (npr. perspektive raziskovalcev Douglasa, Giddensa in Becka).

Zaznavanje tveganja je subjektivna presoja in socialni konstrukt, ki jo posamezniki podajo o značilnostih in resnosti tveganja. Obstaja več teorij, ki pojasnjujejo, zakaj različni posamezniki različno zaznavajo tveganja. Razvite so tri glavne teorije: (i) psihološki pristopi (hevristika in kognitivni pristop), (ii) pristopi antropologije / sociologije (kulturna teorija) in (iii) interdisciplinarni pristopi (družbeno ojačanje okvira tveganj). Kako se zazna tveganje? Preden se lahko pojavi tveganje, je treba tveganje najprej oceniti, obdelati in preoblikovati v vedenjski vzorec ukrepanja. Proces zaznave tveganja ima v ozadju nekaj umskih in fizičnih omejitev, saj je mogoče obdelati samo zaznane dražljaje ali spoznanja. Zaznavanje tveganja je zato zelo oseben proces odločanja, ki temelji na posameznikovem referenčnem okviru, ki ga je razvil v življenju.

Obstaja vse večje nezadovoljstvo o tem, kako je dosedaj urejeno upravljanje tveganj, zlasti na področju kritične infrastrukture, saj raziskovalci, vladne institucije in vodilni zahtevajo nove pristope in sveže ideje. Del navedenega se nanaša tudi na zaznavanje tveganja, saj gre za večplastno razumevanje posameznika kot ocenjevalca tveganj, kako misli, čuti in ukrepa glede nevarnosti, ogrožanja in z njimi povezanih tveganj.

Preden se lahko pojavi tveganje, je treba tveganje najprej oceniti, obdelati in preoblikovati v vedenjski vzorec ukrepanja. Proces zaznave tveganja ima v ozadju nekaj umskih in fizičnih omejitev, saj je mogoče obdelati samo zaznane dražljaje ali spoznanja. Zaznavanje tveganja je zato zelo oseben proces odločanja, ki temelji na posameznikovem referenčnem okviru, ki ga je razvil v življenju.

Posebna pozornost je namenjena povezavam med zaznavanjem tveganja in različico tako imenovanih »petih« osebnostnih faktorjev, ki jih je predlagal Zuckerman (2005). Ti so iskanje impulzivnih občutkov, nevrotizem — anksioznost, agresivnost, družbenost — ekstraverzija in dejavnost. Razlike v kognitivnem slogu so bile preučene tudi glede na zaznavanje tveganja, zlasti ravni samoučinkovitosti.

Realistično zaznavanje tveganja je pomembno na različnih področjih dejavnosti, a raziskave (Kahneman, Tversky – 1974, najbolj vplivna psihološka teorija v zadnjem obdobju) razkrivajo, da je naša samozaznava v resnici polna pomanjkljivosti. Na posameznikovo zaznavanje tveganja vplivajo številni dejavniki, zlasti kot so smrtne posledice tveganja, vplivi na prihodnje generacije, prostovoljnost izpostavljenosti, katastrofalni potencial, poznavanje nevarnosti in vzbujanje grozote.

Dejavniki, ki vplivajo na zaznavanje tveganja

Rezultati raziskav psiholoških eksperimentov kažejo, da posamezniki niso

*avtor je član Slovenskega združenja korporativne varnosti

ravno najboljši ocenjevalci verjetnosti in da sistematično kršijo načela razumnega odločanja pri soočanju z negotovostjo. Njihove izbire ne ustrezajo osnovnim zahtevam doslednosti in skladnosti. Na zaznavanje tveganja najbolj vplivajo izkušnje in predvidevanja, mišljenje, čutenje in hotenje.

Rezultati raziskav psiholoških eksperimentov kažejo, da posamezniki niso ravno najboljši ocenjevalci verjetnosti in da sistematično kršijo načela razumnega odločanja pri soočanju z negotovostjo. Njihove izbire ne ustrezajo osnovnim zahtevam doslednosti in skladnosti. Na zaznavanje tveganja najbolj vplivajo izkušnje in predvidevanja, mišljenje, čutenje in hotenje.

Zaznavanje tveganja je redko povsem racionalno. Namesto tega posamezniki zaznavajo tveganje z uporabo mešanice kognitivnih veščin (npr. tehtanje dokazov, uporaba argumentov in logike za dosego zaključkov) in čustvene ocene (intuicija ali domišljija). Specifični dejavniki, ki vplivajo na zaznavanje tveganja, zlasti na področju kritične infrastrukture, so naslednji: ***zaupanje*** (kadar uporabniki storitev kritične infrastrukture zaupajo strokovnjakom, ki zagotavljajo informacije o določenem tveganju, so manj prestrašeni, kot če ne bi zaupali); ***nadzor*** (pomemben je zaznani nadzor nad rezultati); ***narava nevarnosti*** (nevarnosti v naravi se dojemajo kot relativno neoporečne, medtem ko so človeške nevarnosti bolj grozljive); ***področje uporabe*** (kataklizmični dogodki, ki lahko hkrati ubijejo veliko posameznikov, so bolj strašljivi kot kronična stanja, ki lahko ubijejo prav toliko posameznikov, v daljšem obdobju); ***zavedanje*** (zasičenost medijskega poročanja o velikih nesrečah povečuje ozaveščenost o posebnih tveganjih, bolj kot drugi. Prav tako izredni dogodek, ki je blizu doma, poveča zaznavanje tveganja); ***razpoložljivost preteklih dogodkov*** (tipični miselni vzorec je tisti, po katerem za nek dogodek menimo, da je verjeten in pogost, če si z lahkoto zamislimo njegove primere. Verjetnost nedavnih, živih intenzivnih dogodkov je običajno precenjena); ***sidranje*** (je verjetno najpomembnejši vir pristranskosti. Tu se prvi podatek o pojavu izrednem dogodku napačno jemlje kot izhodiščni, iz katerega se posledično napačno gradi končna ocena tveganja); ***kultura delovnega okolja***, iz katere prihaja ocenjevalec; ***nepripravljenost*** postavljati ekstremne vrednosti ocen tveganja; želja po ponujanju odgovorov, za katere ocenjevalec smatra, da bi jih uporabnik pričakoval (ali želel); ***domišljija*** (ko so grožnje nevidne ali težko razumljive, se posamezniki zmedejo glede narave tveganja, dogodek pa postane bolj strašljiv); ***strah*** (dogodki, ki povzročajo strah, prestrašijo posameznike bolj kot tisti, ki jih ne), ***prizadeta starost*** (tveganja so bolj zastrašujoča, zlasti če vplivajo na otroke); ***negotovost*** (dogodki vzbujajo več strahu, ko strokovnjaki ne sporočajo, kaj je znano, ali ko so tveganja preprosto neznana); ***poznavanje*** (nova tveganja se zdijo nevarnejša kot bolj znane grožnje); ***specifičnost*** (žrtve, ki so javno identificirane, sprožajo večji čustveni odziv kot tisti, ki ostajajo neimenovani ali brezosebni); ***osebni vpliv*** (tveganja, ki prizadenejo posameznika, so bolj zastrašujoča kot tista, ki vplivajo na neznance).

Zaznavanje tveganja dodatno otežuje pretirana prepričanost o pravilnosti lastne sodbe. Posamezniki prevečkrat pretirano zaupajo lastnim, napačnim sodbam. Psihološka osnova za to je verjetno njihova neobčutljivost za pomanjkljivost domnev, na katerih slonijo njihove sodbe. Najbrž noben dejavnik presojanja ni bolj odločujoč kot pretirana samozavest. Narava problema in sodbe določa tudi raven samozavesti. Splošno znanje povzroča razmeroma visoko stopnjo pretirane samozavesti, velja pa tudi obratna trditev.

V zvezi z zaznavanjem pa je prisotno na eni strani podcenjevanje in na drugi strani precenjevanje tveganja. Običajno posamezniki podcenjujejo tveganja za znana ogrožanja in za tista, ki jih lahko





kontrolirajo, precenjujejo pa tveganja za neznana ogrožanja in za tista, ki so zunaj zmožnosti človeške kontrole. Prispevek vsake izbire k vrednosti tvegane odločitve je obtežen s svojo verjetnostjo. Raziskave so pokazale, da lahko razlikujemo med objektivno verjetnostjo in subjektivno verjetnostjo (Klein, 2009). Nizko verjetnost običajno precenjujemo, srednje in visoke verjetnosti pa podcenjujemo.

Hevristika

Hevristika je psihološki vidik reševanja problemov, kako najti najenostavnejšo rešitev. Če ima posameznik pridobljene izkušnje, je reševanje problemov razmeroma enostavno, saj uporablja bližnjice v sklepanju. Kolikor je izkušenj manj, se mora zanesti na že znana spoznanja, statistiko in dobro prakso, ki lahko prispevajo k rešitvi nekega problema.

Te hevristike so ponavadi koristne bližnjice za razmišljanje, vendar lahko v nekaterih primerih vodijo do netočnih sodb, v tem primeru govorimo o kognitivni pristranskosti. Problemi v zaznavi tveganja so: ***reprezentativnost*** (ponavadi se uporablja, ko se od posameznikov zahteva, da presodijo verjetnost, da izredni dogodek pripada nizu predhodne verjetnosti, problem predstavlja tudi neobčutljivost na velikost vzorca, napačno razumevanje naključja, neobčutljivost na predvidljivost, iluzijo veljavnosti, napačno razumevanje regresije); ***hevristična razpoložljivost*** (dogodki, ki jih je mogoče lažje predstaviti ali zamisliti, so ocenjeni kot bolj verjetni kot dogodki, ki si jih ni mogoče zlahka predstavljati: problem pristranskosti zaradi prikrivanja primerov, pristranskosti zaradi učinkovitosti niza raziskav, predsodki); ***asimetrija med dobičkom in izgubami*** (posamezniki so v nasprotju z dobičkom nenaklonjeni tveganju, raje se prepričajo v to, da gre za igro z višjo pričakovano koristnostjo, vendar predstavlja tudi možnost, da ne dobijo ničesar.

Zavajajoče izkušnje lahko ocenjevalce vodijo v prepričanje, da so imuni na mnoga ogrožanja, da se »to njim ne more pripetiti«. Iz povedanega izhaja zaključek, da na tisto, česar ne vidimo (ali se še ni zgodilo), tudi ne pomislimo. Dejansko je zaznava tveganja zapleten psihološki proces, zasnovan bolj na teoretičnih analizah.

Zaključek

Zaznavanje tveganja zahteva presojo verjetnosti in zmožnost inteligentnega ter deduktivnega razmišljanja o malo verjetnih, toda pomembnih izrednih dogodkih. Zaznavi tveganja praviloma pripisujemo verjetnostno naravo, ocenjujemo jo kot bolj ali manj verjetno in v skladu s to oceno sprejemamo posamezne odločitve.

Pomisleki in težave pri zaznavi tveganja na podlagi strokovnega mnenja izhajajo iz psiholoških značilnosti odločanja posameznika v razmerah negotovosti. Zato se lahko postavlja vprašanje ali njihove ocene ustrezajo osnovnim zahtevam doslednosti in skladnosti ocenjevanja tveganja. Pri tem moramo upoštevati, da so ocenjevalci oblikovane osebnosti (glede na znanje, delovne in vodstvene izkušnje) in da težko sprejemajo drugačne poglede (mnenja, pripombe, stališča) od sedanjih.

Dejansko in zaznano tveganje sta pogosto zelo različna. Uporabljamo vse vrste bližnjic, da bi napovedali realno tveganje. Za izboljšanje zaznave tvega-

nja predlagam naslednje razmišljanja in aktivnosti:

- poskušajte predvideti, kaj se bo zgodilo, vendar ne preveč pesimistično (ta pristop vpliva na občutke strahu, zaradi tega pretiravanja tveganje ocenjujemo kot višje, kot je),
- nadzor (imamo potrebo po občutku nadzora in pogosto dojemamo, da imamo več nadzora, ki kot ga dejansko imamo.Ta »kontrolna iluzija« nas vodi do tega, da tveganja zaznavamo manjše, kot je v resnici),
- narava proti posamezniku (včasih se zdijo naravne nesreče manj tvegane kot zaradi dejavnosti posameznika, morda zato, ker imamo večji nadzor nad človeškimi dogodki),
- izbira (če imamo izbiro med dvema enako tveganima dogodkoma, potem lahko zaznavamo, da je tveganje nižje, kot je v resnici, verjetno iz občutka nadzora, ki nam daje možnost izbire),
- novost (tveganja, ki jih še nismo doživeli, povzročajo, da več časa razmišljamo o njih in se nam zato zdijo bolj tvegana),
- medijsko oglaševanje (če tveganje vzbuja veliko pozornost javnosti, je zaradi hevristične razpoložljivosti tveganje ocenjeno kot pomembnejše, kot je v resnici),
- osebna izpostavljenost (če smo izpostavljeni tveganju, to ocenimo kot višje),
- izravnava tveganja in koristi (če obstajajo priložnosti in tveganja, ki se mešajo skupaj in bi izbira lahko privedla do koristi, lahko to pomeni, da se dejansko tveganje obravnava kot manjše, kot je dejansko),
- zaupanje (kadar tveganje vključuje dejanja drugih, bo način, kako ocenjujemo tveganje, bistveno vplival na obseg zaupanja vpletenih strani),
- vzemite si čas (posameznikov sistem zaznavanja tveganj podzavestno in hitro vzpostavi svoj um, še preden pridobi vsa dejstva. Ta »utripajoči« instinkt je lahko koristen za izogibanje preprostim in takojšnjim nevarnostim, vendar to ni najbolj premišljen način, da bi ugotovili, kaj storiti glede kompleksnih prihodnjih groženj),
- pazite na optimizem predsodkov (posameznik je preveč optimističen, ko so podrobnosti nejasne. Poskušajte si predstavljati stvari, kot da so neizbežne),
- razmislite o kompromisih!

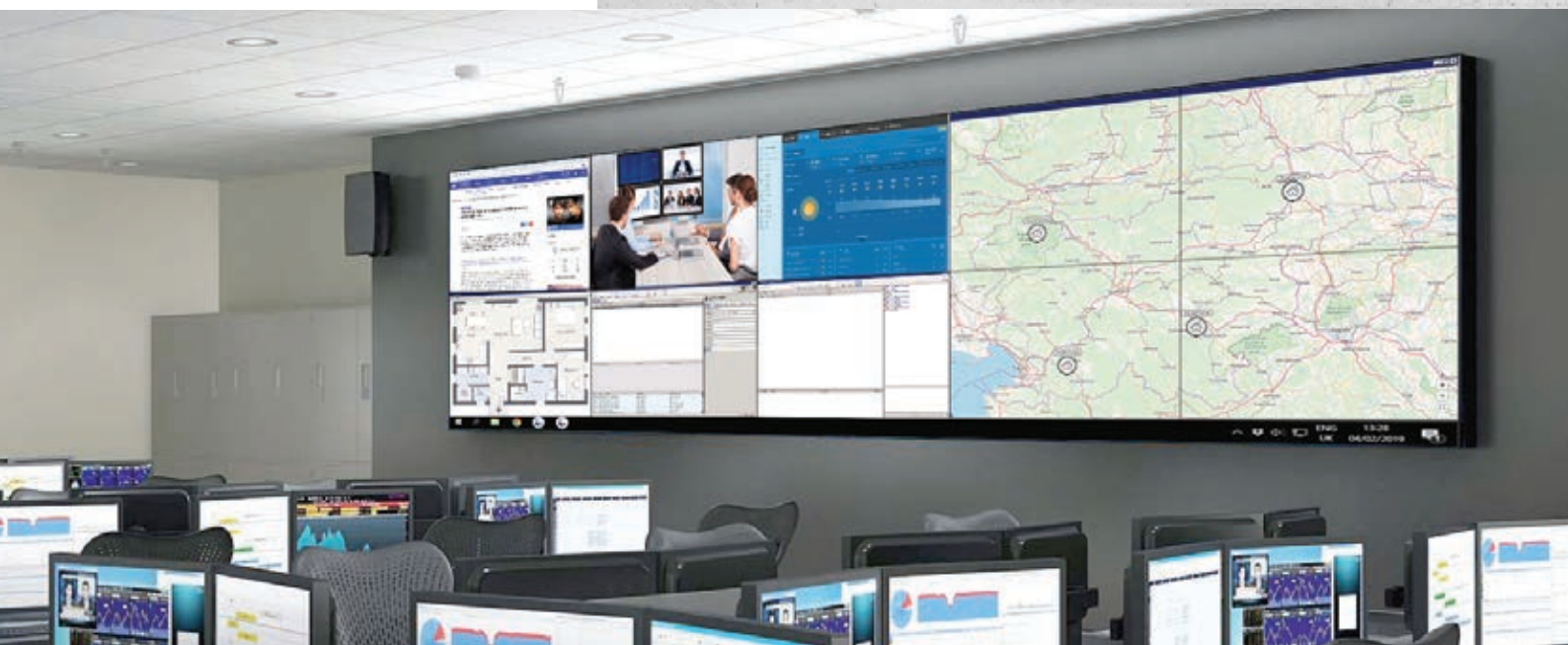
Literatura

- Breakwell, G. M. (2014): The Psychology of Risk. Cambridge University Press.
- Klein, G. (2009). Streetlights and Shadows: Searching for the Keys to Adaptive Decision Making. Cambridge, MA: MIT Press.
- Tversky, A., Kahneman, D. (1974): Presoja v negotovosti: hevristika in pristranskost. Science 185 (4157): 1124-1131.
- Slovic, P. (1987): Percepcija tveganja. Science 236 (4799): 280-285.
- Slovic, P., Finucane, M. L., Peters, E. and MacGregor, D. (2004): Risk as analysis and risk as feelings: some thoughts about affect, reason, risk and rationality. Risk Analysis, 24, 311-322.
- Zuckerman, M. (2005): Psychobiology of Personality. New York: Cambridge University Press, second edition. ■



HSI
HARDWARE SOFTWARE INOVATIONS

www.hsi.si
info@hsi.si



Alarm-PSIM

Centralno nadzorni sistem Alarm-PSIM povezuje varnostne sisteme v eno skupno središče.

- Protipožarni sistemi
- Protivlomni sistemi
- Video nadzorni sistemi
- Nadzor pristopa
- Domofonski sistemi
- Video-wall

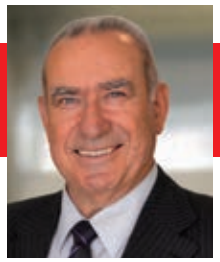
Avtomatiziran Hiter Zanesljiv
Uporabniku prijazen

Alarm-PSIM omogoča avtomatiziran in hiter odziv v izrednih primerih, v katerih so ogrožena življenja in so pomembne sekunde.

+(386) 7 600 19 60 info@hsi.si www.hsi.si

VPRAŠAJTE NAS

Avtorja: doc. dr. Milan Vršec, mag. Miran Vršec /
Institut za korporativne varnostne študije*





PROCES UPRAVLJANJA TVEGANJ V KRITIČNI INFRASTRUKTURI NA BAZI STANDARDOV

Tokratno pisanje o kritični infrastrukturi (v nadaljevanju KI) se nanaša na razlago procesa upravljanja tveganj na bazi uveljavljenih standardov. Izhajava iz (izvirne) študije, ki jo je projektna ekipa Inštituta za korporativne varnostne študije lanskega leta izdelala za potrebe Ministrstva za obrambo.

Študija je izdelana v skladu z Zakonom o kritični infrastrukturi (v nadaljevanju ZKI) in v skladu z drugo pravno podlago ter v skladu s standardi ter bo v pomoč upravljavcem KI pri ocenjevanju tveganj ter posledično načrtovanju zaščite KI, ki jo upravljajo. Pripomogla bo tudi k dolgoročni vzpostavitvi enotnega in celovitega okvira upravljanja tveganj, ki bo uporaben v vseh sektorjih KI. Posredni končni uporabniki študije so tudi nosilci sektorjev KI (ministrstva), ki usmerjajo upravljavce KI in jim nudijo strokovno pomoč pri upravljanju tveganj kot tudi pri načrtovanju zaščite KI. Upravljavcem KI je študija neposredna podlaga za izdelavo lastne ocene tveganj« (Čaleta, Vršec, Bertoncelj, Vršec: 2018). Izhajava tudi iz najinega prispevka, ki je bil pod naslovom Upravljanje tveganj v KI objavljen v prejšnji številki (18) te revije. Tam je bilo v shemi (na strani 25) nakazano, da celovito ocenjevanje tveganj poteka tudi na podlagi standardov kakovosti, varnostnih standardov in standardov upravljanja tveganj. Kajti postopek ocenjevanja tveganj je ena od poglavitnih aktivnosti v procesu upravljanja tveganj, kar je razvidno tudi iz slike v tem prispevku. Uvodoma je treba tudi povedati, da proces upravljanja tveganj obravnavamo z več vidikov: z ekonomskega, finančnega, poslovnega, proizvodnega, tehnološkega, logističnega in okoljskega vidika, predvsem pa z varnostnega vidika in vidika človeških virov. Kajti vedno bolj prihajajo v ospredje varnostna tveganja, ki jih povzročajo človeški viri v katerih igra pomembno vlogo posameznik (več o tem: Bertoncelj 2017 in Čaleta 2018). Torej govorimo o ekonomskih, poslovnih, projektnih, finančnih, tržnih, logističnih, kibernetskih, okoljskih, varnostnih in drugih (specifičnih) tveganjih, ki so predmet obravnave v procesih upravljanja tveganj v KI. V tem kontekstu - že v praksi uveljavljena - poslovna modrost pravi, »da je dodana vrednost (dobiček, ugled, konkurenčnost) poslovnega sistema rezultat uspešnega obvladovanja tveganj, zmanjševanja škod in izgub, zadovoljstva zaposlenih in zadovoljstva porabnikov« (smiselno povzeto po SIST EN ISO 9001: 2015, SIST ISO 31000: 2018 in World Economic Forum WEF 2018). Ta modrost bi morala biti vtkana tudi v procese korporativnega upravljanja KI tako pri nosilcih kot tudi pri upravljavcih KI.

Vse pogostejšim spremembam ter vse bolj kompleksnim tveganjem podvrženo korporativno upravljanje KI terja, da morajo upravljavci KI nameniti več pozornosti vprašanjem varnosti in v okviru tega vprašanjem, ki se nanašajo na integrirano obvladovanje tveganj. Kajti KI je vsestransko ranljiva in je lahka tarča za kriminalne in teroristične napade (Bennet 2018, Baggett/Simpkins 2018), poleg tega pa še ranljiva in ogrožena z vidika naravnih in okoljskih nesreč. Da bi prišli do baze podatkov o ranljivosti in ogroženosti posameznih sektorjev KI morajo vodstva gospodarskih in drugih družb v teh sektorjih poskrbeti za oceno ranljivosti, oceno ogroženosti, SWOT (Strengths – Weaknesses – Oportunities – Threats) analizo in po potrebi za druge analize in študije notranjih in zunanjih (okoljskih) vplivov na poslovanje. Ti dokumenti so

> Pri vzpostavljanju in neprekinjenem delovanju procesa upravljanja tveganj v KI se je treba osredotočiti na uporabo standardov kakovosti, varnostnih standardov in standardov upravljanja tveganj.

*avtorja sta člana Slovenskega združenja korporativne varnosti

Glede na to, da je po ZKI ocena tveganj eden od dokumentov načrtovanja zaščite kritične infrastrukture in neposredna podlaga za izdelavo načrta ukrepov za zaščito KI, je jasno, da je proces upravljanja s tveganji eden od osrednjih procesov, ki je vpet v vse poslovne procese gospodarske družbe, zavoda in državnega organa, ki upravlja s kritično infrastrukturo.

namreč ključna vsebinska podlaga za identificiranje vseh vrst tveganj (Vršec/Vršec 2012, 2016, 2018).

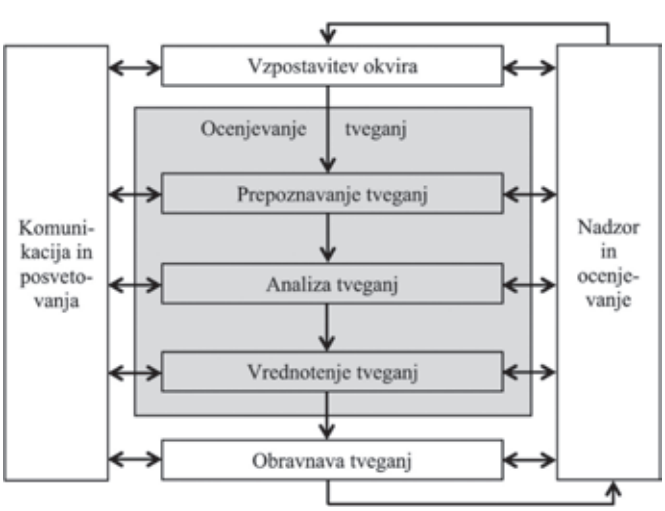
Pri vzpostavljanju in neprekinjenem delovanju procesa upravljanja tveganj v KI se je treba osredotočiti na uporabo standardov kakovosti, varnostnih standardov in standardov upravljanja tveganj. Vsi nakazani standardi predpisujejo **procesni pristop**, ki je trdno zasidran že v standardu kakovosti **SIST EN ISO 9001:2015** in podprt z Demingovim, modelom PDCA (plan - do - check - act). Tiste gospodarske družbe v sektorjih KI, ki imajo v poslovne procese uvedene standarde kakovosti so že v sklopu tega standarda zavezane k vzpostavitvi procesa upravljanja s tveganji. Nekatere gospodarske družbe v sektorjih kritične infrastrukture imajo uvedene tudi standarde SIST EN ISO 14001 (okoljska tveganja), standard OHSAS 18001 in ISO 45001:2018 (tveganja varnosti in zdravja pri delu), HACCP in ISO 22000 (tveganja varnosti in sledljivosti živil) in druge standarde, kar še dodatno upravljavcem KI nalaga obveznosti po obvladovanju specifičnih tveganj v določenih gospodarskih družbah, ki upravljajo s povsem določeno KI (npr. upravljanje prenosnega električnega omrežja v sektorju energetike, upravljanje kliničnih tveganj v sektorju zdravstva, idr.).

Če so standardi kakovosti, s spremljajočimi varnostnimi standardi, **prvi okvir** za proces upravljanja tveganj v KI, lahko rečemo, da je **drugi okvir** za oblikovanje procesa upravljanja tveganj posodobljeno poslovno orodje **COSO ERM 2017** (The Committee OF Sponsoring Organizations of the Treadway Commission-Enterprise Risk Management, Lam 2014, Moeller 2018). To poslovno orodje smo izbrali zato, ker prinaša sodobne in učinkovite metodološke usmeritve za vzpostavljanje sistemov upravljanja s tveganji tudi v KI. Je torej splošno uporabna metodologija, ki ob primerni implementaciji zagotavlja uspešno obvladovanje tveganj. Poleg tega je COSO ERM podlaga tudi za standard obvladovanja tveganj **ISO 31000:2018**, ki je po naši presoji eno od ključnih izhodišč za proces upravljanja in obvladovanja tveganj. Ta standard je treba uporabljati v sklopu standardov kakovosti (Hutchins 2018), kot tudi za obvladovanje projektnih tveganj (Cooper 2014, Blokdyk 2018).

Po COSO ERM 2017 je proces upravljanja tveganj **neprekinjen proces**, ki ga vzpostavi najvišje vodstvo v upravljavcih kritične infrastrukture (uprava, upravni odbor, generalni direktor) in to tako, da je proces upravljanja tveganj vraščen v poslovno politiko, razvojno strategijo, notranje akte, poslovne procese, poslovne načrte in varnostne načrte. To je skladno z zakonsko zahtevo po **neprekinjenem poslovanju kritične infrastrukture** (ZKI, členi 3/15., 10/3., 19., 24.), kakor tudi z metodiko **standarda neprekinjenega poslovanja ISO EN 22301:2014**. Kajti ta standard navaja zahtevo po obvladovanju tveganj in obvladovanju kriznega vodenja (Engemann 2011). »Pri vzpostavljanju procesa upravljanja tveganj je treba upoštevati z ocenami ugotovljene ranljive točke, realno in potencialno ogroženost, preteče nevarnosti in verjetne izredne dogodke, ki bi lahko negativno vplivali na poslovne procese« (Vršec/Vršec, 2018). V tem kontekstu COSO ERM 2017 navaja naslednje usmeritve:

- vzpostaviti korelacijo tveganj s strategijo, poslovno uspešnostjo, varnostno kulturo, poslovno etiko in blagovnimi znamkami,
- obvladovanje notranjih in zunanjih sprememb zagotavlja poslovno odpornost,
- pri upravljanju in obvladovanju tveganj ne gre samo za to, da se preprečujejo škode in izgube ampak gre tudi za utrjevanje dobičkonosnosti in konkurenčnosti,
- ni dovolj, da z obvladovanjem tveganj računamo samo na preživetje temveč je treba računati na stabilen razvoj poslovnih procesov,
- proaktiven pristop k tveganjem vpliva na zmanjšanje stroškov obvladovanja izrednih dogodkov,
- hitro in strokovno odzivanje na izredne dogodke je ena od prioritet obvladovanja tveganj,
- nujna je izdelava načrtov neprekinjenega poslovanja in kriznega vodenja,
- v sistemu obvladovanja tveganj mora biti zagotovljeno merjenje uspešnosti obvladovanja posameznih vrst tveganj,
- v procesu obvladovanja tveganj se mora povečati uporaba sodobne informacijske in komunikacijske tehnologije.

Navedene usmeritve COSO ERM 2017 so združljive s strukturo in z vsebino standarda upravljanja tveganj ISO 31000:2018, zato vzamemo za **tretji okvir** oblikovanja procesa upravljanja tveganj v KI družino standardov: **ISO 31000:2018 (**Risk Management-Guidelines**), ISO/IEC 31010:2018 (**Risk Management-Risk Assessment Techniques**), ISO Guide 73:2016** (Risk Management Vocabulary), **in ISO/IEC 51:2014** (Safety Aspects-Guidelines their Inclusion in Standards). Prvi standard razumemo kot osnovni standard, naslednji trije pa v bistvu dopolnjujejo osnovnega in so opredeljeni kot podporni standardi. Strukturo in vsebino teh standardov predstavlja naslednja slika:



Upravljanje tveganj po standardu ISO 31000



Iz slike je razvidno, da v osrednji del procesa ocenjevanja tveganj sodijo naslednje aktivnosti:
- prepoznavanje tveganj (Risk identification),
- analiza tveganj in (Risk analysis),
- vrednotenje tveganj (Risk evaluation).

Pri **vzpostavitvi okvira** (zgornji del slike) je treba poskrbeti za izdelavo politike upravljanja tveganj in za skladnost z zakonodajo, pri **obravnavi tveganj** (spodnji del slike) pa je treba poskrbeti za izdelavo kataloga tveganj kot dinamičnega dokumenta upravljanja s tveganji. **Komunikacije, posvetovanja, nadzori in ocenjevanja** (levi in desni del slike) uspešnosti upravljanja s tveganji, pa so aktivnosti med deležniki (vodstva, odbori, forumi, odgovorne osebe), ki upravljajo s tveganji.

Glede na to, da standard ISO 31000 (eksplicitno) ne izhaja iz ocen ranljivosti in ogroženosti, iz SWOT analize in potrebami po prenosu (visokih) tveganj (npr. požarnih tveganj) na zavarovalnice, vzamemo za dodatno orodje upravljanja s tveganji **splošni model upravljanja tveganj** (podrobneje sva ga predstavila že v prejšnjih številkah revije), ki vsebuje glavne segmente standarda ISO 31000, poleg tega pa še kontrolo tveganj ter izravnavo tveganj z zavarovanjem premoženja in človeških virov pri zavarovalnicah.

Široka uporabnost splošnega modela upravljanja s tveganji je v tem, da izhaja iz ocene ogroženosti, ki pove kje so nevarnosti in kateri verjetni izredni dogodki se lahko pripetijo v sektorjih kritične infrastrukture oziroma na kompleksih gospodarskih družbah, zavodov, državnih organov in bank, ki upravljajo s povsem določeno KI. Vedeti je treba, kateri so prvi koraki v upravljanju tveganj, da bi se lahko lotili naslednjih korakov. »Prvi korak v analizi tveganj je zaznava in prepoznava groženj in ranljivosti« (Fisher/Halibozek, 2012). V našem modelu je to **prvi sklop** upravljanja tveganj, to je analiza tveganj, ki - kot je že rečeno - temelji na oceni ogroženosti, poleg tega pa še na oceni ranljivosti in na SWOT analizi poslovanja. S prvim korakom v analizi, ki ga imenujemo zaznava tipov tveganj gre za zavedanje o obstoju tveganj, ki izhajajo iz ranljivih točk in iz varnostno vitalnih točk v določeni KI. Temeljito poznavanje in zavedanje ranljivih točk v poslovnih procesih in vrzelih v sistemih varovanja bi morali lastnikom, upravljavcem in nadzornikom povzročati nelagoden občutek in potrebo po ustreznem odzivanju na prepoznana tveganja. Pri drugem koraku analize tveganj, ki je označen kot razpoznavanje (prepoznavanje) tveganj, pomeni ugotoviti od kje tveganja izhajajo: ali iz človekovega, ali tehnično-tehnološkega ali naravnega okolja. Uporaba analitičnega postopka kot tretjega koraka v analizi tveganj je namenjena razvrstitvi tveganj na tveganja, ki pomenijo hazardiranje (vse dobiš ali vse izgubiš), na ekstremna in zelo visoka tveganja, ki so predmet zavarovanja pri zavarovalnicah, ter srednja in nizka tveganja, ki jih lahko obvladujemo s tekočimi ukrepi opredeljenimi v katalogu tveganj. **Drugi sklop** upravljanja s tveganji je kontrola tveganj, s katero poskušamo tveganja skrčiti, nekatera izločiti, nekaterim tveganjem pa se preprosto izogniti. Če je analiza tveganj dobro pripravljena, potem je dokaj preprosto izločiti tista tveganja, ki predstavljajo hazardiranje, ostala tveganja pa obvladujemo z ustreznimi notranjimi ukrepi in z zavarovanjem. Pri **tretjem sklopu** upravljanja s tveganji gre torej za izravnavo tveganj, kar pomeni neposredno sodelovaje z zavarovalnicami, ki za primerno zavarovalno premijo prevzamejo upravljanje tveganj.

Iz opisanega pristopa k vzpostavljanju procesov upravljanja tveganj v kritični infrastrukturi lahko govorimo o »celovitem pristopu k obvladovanju tveganj« (Čaleta 2017), ali drugače povedano, govorimo o »integriranem pristopu k obvladovanju tveganj« (Vršec/Vršec 2018). Le s takim pristopom bo



v prihodnje možno obvladovati nove poslovne, varnostne, tehnološke, kibernetske, človeške, in okoljske izzive**.** Integriran pristop k upravljanju tveganj potemtakem pomeni, da izhajamo iz ocene ranljivosti, ocene ogroženosti in iz SWOT (Strengths – Weaknesses – Oportunities - Threats) analize. Iz teh ocen analiz in študij ugotovimo vse vrste tveganj, ki jih nato na podlagi standardov upravljanja tveganj, varnostnih standardov in ustreznih modelov uporabimo za izdelavo kataloga (registra) tveganj. Ta katalog, ki se – glede na spremenjene razmere – stalno dograjuje, je glavno dinamično orodje v procesu upravljanja tveganj. Pri tem se je očitno treba sprijazniti z dejstvom, da proces upravljanja tveganj stalno spremljajo negotovost, izpostavljenost, spremembe ter poslovni in varnostni izzivi. Pri tem bi bilo smiselno izpostaviti tudi predlog, da se, poleg kataloga (registra) tveganj, izdela tudi katalog (register) škodnih dogodkov in izgub povezanih z njimi, ki služi upravljavcu KI kot vodilo pri pripravi izboljšav v procese upravljanja tveganj v KI.

Glede na to, da je po ZKI ocena tveganj eden od dokumentov načrtovanja zaščite kritične infrastrukture in neposredna podlaga za izdelavo načrta ukrepov za zaščito KI, je jasno, da je proces upravljanja s tveganji eden od osrednjih procesov, ki je vpet v vse poslovne procese gospodarske družbe, zavoda in državnega organa, ki upravlja s kritično infrastrukturo. Kajti z oceno tveganj dobijo nosilci in upravljavci kritične infrastrukture tiste informacije, ki v procesih njihovega odločanja omogočajo realno načrtovanje neprekinjenega poslovanja, izdelavo potrebnih načrtov varovanja, učinkovito odzivanje na nastale izredne dogodke in obvladovanje kriznih razmer.

Viri

- Baggett, Ryan, Simkins, Brian K. (2018). Homeland Security and Critical Infrastructure Protection, 2nd Edition. Praeger Security International. Praeger Santa Barbara, US.
- Bennet, Brian T. (2018). Understanding Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personel. Wiley&Sons Inc. Hoboken, USA.
- Bertoncelj, Brane (2015). Kako zmanjšati tveganja v podjetju in preprečiti najhujše. Gea College, Fakulteta za podjetništvo. Ljubljana.
- Bertoncelj, Brane (2017). Zanesljivost posameznika pri delovanju kritične infrastrukture sodobne države. Sodobni vojaški izzivi, letn. 19, št. 4, str. 111-131.
- Blokdyk, Gerardus (2018). ISO 31000 Risk Management. Practical Tools-Self Assessment. SSTARC Cooks.
- Cooper, Dale, Bosnich, Pauline (2014). Project Risk Management Guidelines: Managing Risk with ISO 31000 and IEC 62198. Wiley&Sons Ltd.
- Čaleta, Denis (2017). Nujno sprejetje paradigme o celovitosti pristopov obvladovanja tveganj. Korporativna varnost, št. 14/2017. ICS Ljubljana.
- Čaleta, Denis (2018). Tveganja radikalizacije zaposlenih v organizacijah kritične infrastrukture. Korporativna varnost, št. 17/2018. ICS Ljubljana.
- Čaleta, Denis, Vršec, Milan, Bertoncelj, Brane, Vršec Miran (2018). Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture. Izvirna študija o upravljanju tveganj v kritični infrastrukturi. ICS Ljubljana in Ministrstvo za obrambo.
- Engemann, Kurt J., Henderson, Douglas M. (2011). Business Continuity and Risk Management: Essentials of Organizational Resilience. Rothstein Associates Inc.. Brookfield Connecticut, USA.
- Fischer, Robert, Halibozek, Edward (2012). Introduction to Security. Butterworth-Heinemann. Boston, London.
- Hutchins, Greg (2018). ISO 31000:2018). Enterprise Risk Management (CERM Academy Series on Enterprise Risk Management, Certified Enterprise Risk Manager Academy. Portland. USA.
- Moeller, Robert R. (2011).COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes. Wiley&Sons, Inc. Hoboken, New Jersey.
- Vršec, Milan (1993). Varnost podjetja – tokrat drugače. Viharnik, Ljubljana
- VRŠEC, Milan (2008). Redefiniranje ranljivosti in ogroženosti podjetij z izvirnim metodološkim pristopom = Redefining the vulnerability and threat to companies with an authentic methodological approach. Zbornik 27. mednarodne znanstvene conference, Portorož, 19.-21. marec 2008. Kranj: Moderna organizacija. 2008, str. 3061-3074.
- Vršec, Milan, Vršec Miran (2012). Upravljanje poslovnih, varnostnih in drugih tveganj v multinacionalnih gospodarskih družbah. Mednarodna znanstvena konferenca Dnevi korporativne varnosti 2012. ICS Ljubljana.
- Vršec, Milan in Vršec, Miran (2016). Ranljivost, varnostne grožnje in varnostna tveganja si podajajo roke. Korporativna varnost, 12/2016. ICS Ljubljana.
- Vršec, Milan, Vršec, Miran (2017). Načrti neprekinjenega poslovanja in krizni načrti v funkciji obvladovanja tveganj. Korporativna varnost, št. 17/2018. ICS Ljubljana.
- Vršec, Milan, Vršec, Miran (2018). Upravljanje tveganj v kritični infrastrukturi. Korporativna varnost, št. 18/2018. ICS Ljubljana.
- Zakon o kritični infrastrukturi, Ur. l. RS, št. 75. ■

SISTEMSKE REŠITVE PRED POŽARI, – Z ENO BESEDO BONPET!

Samodejna gasilna ampula BONPET je najučinkovitejše gasilno sredstvo za gašenje začetnih požarov ter požarno zaščito manjših zaprtih prostorov brez stalne prisotnosti ljudi. Je tudi gasilni aparat estetskega izgleda. Nepogrešljiva je na vseh mestih, kjer predvidevate, da bo ob izbruhu požara temperatura najhitreje narasla (npr. na stropu ali zidu, najbližje mestu potencialnemu izbruhu požara).
Življenjska doba ampule je deset let brez vzdrževanja.



Pooblaščeni inštituti so potrdili učinkovitost in neškodljivost za človeka in okolje. Sodobna oblika in barva ampule zagotavljata tudi skladnost z ambientom.

NOVO
v ponudbi: BONPET SAMODEJNI GASILNIK 2, 4, 6 ali 12L.

SAMODEJNE GASILNE AMPULE BONPET

priporočajo tudi **slovenske zavarovalnice** s popusti zaradi zmanjšanja rizika tveganja.



Bonpet gasilnik, specialist za olja in maščobe (F razred)

Bonpet® systems

Zanesljivi gasilni sistemi

Pot Vitka Pavliča
1430 Hrastnik
Tel.: 080-26-63
e-pošta: info@bonpet.si
www.bonpet.si

Avtorji: mag. Janez Anžič, mag. Matevž Mutec, Rok Peršak, Aleš Skubic / Telekom Slovenije*

IZKUŠNJE TELEKOMA SLOVENIJE NA PODROČJU ZAGOTAVLJANJA STORITEV KIBERNETSKE VARNOSTI

Zagotavljanje kibernetske varnosti v poslovnem okolju, ki temelji na neprekinjenem poslovanju, hkrati pa sledi najvišjim standardom na področju informacijske varnosti in skladnosti poslovanja, je rezultat sistematičnega in strateško načrtovanega izvajanja aktivnosti. V procesu zagotavljanja kibernetske varnosti so potrebne natančno opredeljene aktivnosti za preprečevanje, odkrivanje in odzivanje na varnostne grožnje, pa tudi ponovno vzpostavitev poslovanja.

Uvod

Tako kot se povečuje uporaba informacijskih tehnologij v celotnem poslovnem in zasebnem okolju, s še večjo hitrostjo prihaja tudi do različnih zlorab na področju varnosti informacijskih tehnologij. Zlorabe informacijsko-komunikacijskih tehnologij so vedno bolj napredne, tehnološko dovršene, prikrite in inovativne, do njih pa prihaja tako na gospodarskem in političnem kot na zasebnem področju. Motivi za to so različni: od premoženjske koristi, zlonamernosti, dokazovanja, kraje identitete, kraje podatkov ali pridobivanja konkurenčne prednosti do onemogočanja delovanja kritične infrastrukture ali pridobivanja geopolitičnih prednosti. Osnovni namen zlonamernežev je, da uporabnikom s svojim dejanjem izbrišejo oz. uničijo podatke, jih zaklenejo, jim onemogočijo poslovanje ali pridobijo protipravno korist. Pri tem uporabljajo različne metode oz. tehnike napadov, kot so socialni inženiring, ribarjenje, zlonamerne kode, virusi, DDoS (Distributed Denial-of-Service) itd. V zadnjem obdobju se aktivnosti vedno bolj selijo na končne naprave in so vedno bolj usmerjene na uporabnika samega. V tem prispevku se bomo omejili na področje kibernetske varnosti, ki predstavlja aktivno zaščito na več področjih (sistemih, virih), pred različnimi tehnikami napadov, z uporabo digitalnih tehnologij. V Telekomu Slovenije kibernetska varnost sodi med strateške prioritete. Zato smo vzpostavili Operativni center kibernetske varnosti, ki predstavlja jedro operativnih zmogljivosti tako za Telekom Slovenije kot druge organizacije, javne ustanove in podjetja, ter osnovali odzivno skupino za varnostne incidente. Zagotavljanje kibernetske varnosti pri tem temelji na aktivnem sodelovanju strokovnjakov, tehnologije in izdelanih procesov. Aktivnosti lahko razdelimo na pet korakov: priprava, preprečevanje, odkrivanje, odzivanje, obnovitev.

Večina organizacij ugotavlja, da kršitve varstva osebnih in drugih podatkov ter ostali incidenti, povezani z varnostjo na področju informacijsko-komunikacijskih tehnologij, predstavljajo poslovno kritično operativno tveganje

Osnova zagotavljanja kibernetske varnosti je dobra priprava

Večina organizacij ugotavlja, da kršitve varstva osebnih in drugih podatkov ter ostali incidenti, povezani z varnostjo na področju informacijsko-komunikacijskih tehnologij, predstavljajo poslovno kritično operativno tveganje. Razširjenost in resnost takšnih kršitev ugotavljajo različne raziskovalne, varnostne in druge organizacije oz. organi. Stroški posame-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



znega varnostnega incidenta lahko narastejo tudi na nekaj milijonov evrov, prav tako so lahko visoke pravne obveznosti, pa tudi regulatorna izpostavljenost in škoda, ki nastane zaradi izgube zaupanja oz. ugleda. Ustrezne priprave omejijo verjetnost nastanka tovrstnega incidenta in omejijo škodo, ki lahko ob tem nastane. Obvladovanje tveganj je sistematičen in stalen proces. Njegov namen je maksimiranje verjetnosti želenih (priložnosti) in minimiziranje verjetnosti neželenih dogodkov (nevarnosti).

Tveganja na področju kibernetske varnosti so v zadnjih letih ocenjena z najvišjo stopnjo. Zato je na področju upravljanja tveganj za zagotavljanje kibernetske varnosti potrebno sprejemati različne ukrepe za zmanjševanje stopnje tveganja. V prvem koraku je tako potrebno pripraviti popis virov (fizične in virtualne naprave) in aplikacij ter opredeliti kritične vire na podlagi varnostne politike in politike upravljanja s tveganji ter jih nato tudi nenehno posodabljati. Način uvedbe ukrepov za zmanjševanje tveganj, s katerimi zadostimo standardom skladnosti poslovanja in varnostne politike, opredelimo v postopku preventive ali preprečevanja.

Preventivne aktivnosti za preprečevanje varnostnih incidentov

Podjetja in organizacije pri svojem poslovanju uporabljajo različna sredstva, pri čemer se izraz »sredstvo« v skladu z ISO-standardi, s področja varovanja informacij, uporablja zelo široko, saj je sredstvo pravzaprav vse, kar za podjetje predstavlja določeno vrednost (ISO 27000), pa naj gre za fizične, logistične ali človeške vire.

Glavni cilj preventivnih aktivnosti je upravljanje z zaupnostjo, celovitostjo, razpoložljivostjo, avtentičnostjo in neovrgljivostjo posameznih sredstev. Prav vsako sredstvo pa je vir potencialnih tveganj oz. groženj, ki jih moramo v skladu z metodologijo, omenjeno v prejšnjem poglavju, upravljati. Tveganja najpogosteje zmanjšujemo z investicijami v varnostne ukrepe in rešitve. Med varnostne ukrepe sodijo aktivnosti, postopki ali mehanizmi, ki zmanjšujejo verjetnost ali posledico varnostnih incidentov, na tveganje pa vplivajo različno: lahko odkrivajo in preprečujejo incidente, odvračajo grožnje, omejujejo tveganja, popravljajo nastalo škodo zaradi incidenta, pomagajo pri okrevanju po incidentu, izvajajo nadzor ali ozaveščajo. Glede na učinke lahko varnostne ukrepe razvrstimo v tri glavne skupine: preventivne, korektivne in detekcijske ukrepe. Preventivni ukrepi zmanjšujejo število uspešnih incidentov in s tem verjetnost za nastanek incidenta, korektivni ukrepi zmanjšujejo izgubo v primeru incidenta, detek-

Najpogostejši viri groženj so uporabniki, pri čemer je pogosto težko na prvi pogled oceniti, ali je šlo za načrtno zlorabo ali le za trenutno nepazljivost in neznanje uporabnika. Predpogoj za pravočasen in predvsem pravi odziv so izkušeni strokovnjaki, ki pri svojem delu uporabljajo ustrezne programske rešitve, saj lahko napačna interpretacija varnostnega dogodka vodi v iskanje izvora groženj, ki to niso.

cijski ukrepi pa skrajšajo čas, v katerem se incident zazna, in omogočajo zbiranje podatkov za nadaljnje analize. Med preventivne ukrepe uvrščamo varnostno politiko, kriptografijo, varno arhitekturo omrežja in aplikacij, ažurno posodabljanje programske opreme, požarne zidove, sisteme za preprečevanje vdorov v omrežja, DDoS-zaščito, mehanizme overjanja in avtorizacije uporabnikov, protivirusno programsko opremo in še kaj. Med preventivne ukrepe sodijo tudi različna testiranja ranljivosti sistemov in vdorni testi, pa izobraževanja in testiranja zaposlenih glede odzivanja na različne tehnike napadov.

Nemalokrat se ob vseh aktivnostih pozablja na dobro zaščito končnih naprav. V tovrstnih primerih za zaščito ni dovolj zgolj protivirusni program, temveč je potrebno uporabiti naprednejšo zaščito, ki spremlja delovanje vsakega procesa na posameznem računalniku. Na ta način poleg zaščite pred znanimi grožnjami končne točke ščitimo tudi pred neznanimi, izoliramo končne točke in lahko dokaj hitro ugotovimo vzrok za neželeno obnašanje nekega procesa. Ob tem je poleg zaščite na končnih točkah potrebno zagotoviti tudi ustrezno zaščito povezav (fizično in logično) ter ustrezno požarno pregrado (IDS+IPS).

Odkrivanje temelji na ustreznih pripravah in informacijah, v zadnjem obdobju pa tudi na avtomatizaciji s pomočjo umetne inteligence

Orodje ali sistem orodij za odkrivanje zbira dnevniške zapise (event logov, logov, syslogov itd.) iz sistemov. Zapise obdela, jih normalizira, ustrezno agregira in na koncu prikaže v obliki varnostnih dogodkov. Na trgu je veliko izbire - od osnovnih pregledovalnikov dnevniških zapisov do kompleksnih sistemov, katerih dodana vrednost je uporaba umetne inteligence za odkrivanje potencialnih ranljivosti in groženj, pa tudi samodejno posodabljanje pravil za kreiranje varnostnih dogodkov. Učinkovitost orodja za odkrivanje je odvisna od več dejavnikov, kot so kakovost dnevniških zapisov, kakovost odstranjevanja šuma (lažni pozitivni dogodki), ustrezno povezovanje potencialnih varnostnih dogodkov z aktualnim dogajanjem v svetu (odkrite nove ranljivosti, grožnje kibernetskih napadov ...). Nenazadnje je seveda lahko pri odkrivanju ranljivosti učinkovit tudi ustrezno usposobljen strokovnjak. Klasične protivirusne programske rešitve in rešitve pred škodljivo programsko opremo se pri odkrivanju groženj opirajo na baze podatkov, primerjajo vsebine datotek s podatki iz baze ter zelo dobro skrbijo za sprotno čiščenje in zaščito. Navedeno seveda velja za primere, da je bila grožnja v preteklosti že odkrita ter je analizirana in vnesena v bazo. Ob tem pa so vsi ti mehanizmi v primeru novih ali variacij nekaterih že poznanih groženj popolnoma neuporabni. Zato je pomembno skrbno spremljanje vsakega procesa posebej.

Če se priprava, preventiva in odkrivanje opravijo z odliko, je odziv na varnostni dogodek enostavnejši in hitrejši

Najpogostejši viri groženj so uporabniki, pri čemer je pogosto težko na prvi pogled oceniti, ali je šlo za načrtno zlorabo ali le za trenutno nepazljivost in neznanje uporabnika. Predpogoj za pravočasen in predvsem pravi odziv so izkušeni strokovnjaki, ki pri svojem delu uporabljajo ustrezne programske rešitve, saj lahko napačna interpretacija varnostnega dogodka



vodi v iskanje izvora groženj, ki to niso. Posledica je predvsem izguba časa in virov, nenazadnje tudi neupravičeno motenje delovnih procesov, upad učinkovitosti, izguba zaupanja in kompetentnosti. Zato je pomembno, da strokovnjaki najprej ugotovijo resnost grožnje in njen obseg, skladno s klasifikacijo pa nato izvedejo prve ukrepe. Pri tem je potrebno, pri grožnjah z visoko stopnjo resnosti, z ustrezno izolacijo sistema, najprej poskrbeti za njihovo zajezitev, ter izvesti obveščanje in ostale aktivnosti, ki so, glede na vire ogrožanja, potrebne za nemoteno izvedbo preiskav. Samo z ustrezno preiskavo lahko namreč podobne grožnje preprečimo tudi v prihodnje. Pri tem je pomembno, da vsak postopek in vsako tudi najmanjšo informacijo ob reševanju varnostnega incidenta sproti beležimo v ustrezen informacijski sistem za upravljanje z napakami, prek katerega izmerimo učinkovitost delovanja.

Obnovitev poslovanja

Uspešen kibernetski napad lahko traja več ur, dni, tednov ali pa še dlje, posredna škoda pa lahko nastaja tudi še nekaj mesecev po napadu. Po podatkih Gartnerja ima samo tretjina podjetij pripravljen načrt odziva na kibernetski napad, pri tem pa gre večinoma za načrte v primeru enostavnih napadov ali napadov enega samega tipa. Osnovo za pripravo na obnovitev poslovanja nam lahko predstavlja veriga odziva na napad (Cyber Kill Chain), ki vključuje zbiranje informacij o tarči, analizo zbranih informacij ter izbor tehnike napada oz. dostave v končne naprave prek ribarjenja, instalacijo po več virih ali sredstvih ter skrivanje, nadzor, prevzem in izvršitev napada. Notranji krog predstavlja korake napadalca, zunanji pa zaščito pred napadom. Za vsako točko, kjer morebitni napadalec vidi svojo priložnost, morajo podjetja opredeliti vpliv na poslovanje. Za vsako sredstvo/vir pa je potrebno pripraviti načrt okrevanja virov, načrt okrevanja storitev in načrt kriznega komuniciranja. Prvi del predstavlja pripravljalna oziroma načrtovalska faza, drugi del, ko se napad že zgodi, pa odziv in obnovitev poslovanja. V pripravljalni fazi se pripravljamo na področjih organiziranosti, analiz in planov, zagotavljanju odpornosti posameznih sredstev (zaščita podatkov) ter kriznega komunikacijskega upravljanja. V fazi priprave organiziranosti vzpostavimo ustrezno sodelovanje med odzivno skupino za varnostne incidente (CSIRT), Operativnim centrom kibernetske varnosti (OCKV) in skupino za okrevanje poslovanja. V tem okviru ustanovimo enotni tim za krizno vodenje, pregledujemo sposobnost ekip in virov, ki so potrebni za obnovo poslovanja, ter preverjamo sodelovanje med načrtovalci in operativo. Hkrati proučujemo različne scenarije varnostnih in kibernetskih napadov ter njihov vpliv na poslovanje, spremljamo odziv in obnovitvene postopke, pogosto izvajamo vaje na različnih področjih posameznih sredstev/virov, ki sestavljajo poslovanje podjetja, izvajamo teste ranljivosti, vdorne teste, teste socialnega inženiringa (na primer e-sporočilo za ribarjenje), izvajamo scenarije različnih napadov in preverjamo pripravljenost. Navedene aktivnosti izvajamo na podlagi standardov ISO 22301, ISO 27001, NIST ter drugih standardov in priporočil. Na področju kriznega komunikacijskega upravljanja pripravimo komunikacijski načrt v odvisnosti od velikosti in vpliva kibernetskega napada. V obnovitveni fazi, v kateri napad poteka, pa je pomembno tesno sodelovanje med upravljanjem neprekinjenega poslovanja (strokovnjaki za vire), skupino za okrevanje poslovanja in odzivno skupino za varnostne incidente v podjetju ali pa celo na nacionalnem nivoju. V okviru priprav določimo vodjo za koordiniranje obnovitve, ki je navadno član skupine za okrevanje poslovanja. Glede na vpliv napada sprožimo ustrezne obnovitvene postopke, izvedemo prve forenzične preiskave, obnovimo poslovanje in zaščitimo dokaze. Naloga ekip je, da se čim prej vzpostavi normalno poslovanje organizacije ali podjetja, ob zaključku napada pa je potrebno ustrezne podatke predati pristojnim organom. Prav tako je potrebno pripraviti natančno analizo aktivnosti, opredeliti dobre in slabe strani reakcije na kibernetski napad ter na tej osnovi sprejeti ustrezne ukrepe za izboljšanje priprave, preprečevanja, odkrivanja, odzivanja in obnovitve poslovanja.

Vgradnja varnostnih kontrol v aplikacijski varnosti

V Telekomu Slovenije načrtovanje varnostnih kontrol vključujemo že v začetne faze načrtovanja aplikacij. Tako opravimo oceno tveganj, izvedemo identifikacijo in implementacijo varnostnih kontrol ter ugotavljamo morebitne ranljivosti. V fazi testiranja posamezne aplikacije z varnostnega vidika opravimo verifikacijo implementiranih varnostnih kontrol in ranljivosti, interno varnostno preverimo kakovost kode (to je naloga ključnih razvijalcev) ter po potrebi izvedemo vdorna testiranja. Na podlagi pridobljenih rezultatov ponovno opravimo načrtovanje za odpravo pomanjkljivosti, implementacijo in ponovni test.

Nov vidik aplikacijske varnosti v zadnjem obdobju predstavlja vse množičnejša uporaba naprav interneta stvari (IoT; Internet-Of-Things). Pri tem nepridipravi množično izkoriščajo slabo oziroma nezadostno varnostno zaščito posameznih IoT-naprav in jih vključujejo v množične napade (DDoS). Veliko grožnjo predstavljajo tudi IoT-naprave, ki krmilijo naš vsakdan (od dobave tekoče vode do distribucije plina), tako da veliko pozornosti namenjamo zagotavljanju varne transportne poti in varnega komunikacijskega okolja s segmentiranim dostopom, izvajamo striktno preverjanje uporabljenih varnostnih komunikacijskih protokolov, avtentikacije ter sistemsko utrjevanje aplikacijskih strežnikov in operacijskih sistemov.

Zaključek

V Telekomu Slovenije smo tako za lastne potrebe kot za druge organizacije, javne ustanove in podjetja uvedli različne storitve zagotavljanja kibernetske varnosti. Jedro te storitve predstavlja Operativni center kibernetske varnosti, v katerem združujemo procese, tehnologijo in vrhunske strokovnjake. Kot izkušen ponudnik storitev zagotavljanja kibernetske varnosti storitve uvajamo na dveh nivojih. Prvega predstavlja specializacija vsebine in ustreznost ključnih poslovnih procesov, glede na panogo ali okolje, drugi pa postopno uvedbo procesa zagotavljanja kibernetske varnosti, v katerem nenehno izboljšujemo zrelost IKT-sistema naročnika (preprečevanje, odkrivanje) in operativo (odkrivanje, odzivanje, obnovitev). Predvsem pa skrbimo za usklajeno delovanje vseh usposobljenih ekip za zagotavljanje najvišje ravni kibernetske varnosti. ■

TelekomSlovenije

STE ZAŠČITENI PRED **KIBERNETSKIMI NAPADI?**

Vsak dan po omrežju potuje ogromna količina različnih podatkov, ti pa imajo danes veliko tržno vrednost. Zato so podjetja **izpostavljena vdorom ter krajam in zlorabam podatkov**. Poskrbite za ustrezno zaščito in **nadzorujte vsa tveganja kibernetskih napadov** s pomočjo Operativnega centra kibernetske varnosti Telekoma Slovenije.

OPERATIVNI CENTER KIBERNETSKE VARNOSTI TELEKOMA SLOVENIJE ZAGOTAVLJA:

ZNIŽEVANJE OPERATIVNIH TVEGANJ POVEZANIH S KIBERNETSKO VARNOSTJO + DOSEGANJE IN OHRANJANJE SKLADNOSTI S STANDARDI IN REGULATIVO + ZAZNAVANJE VARNOSTNIH DOGODKOV, ODZIVANJE, OMEJITEV IN POVRNITEV PODATKOV IN STORITEV



OPERATIVNI CENTER KIBERNETSKE VARNOSTI TELEKOMA SLOVENIJE OMOGOČA VIŠJO RAVEN VARNOSTI OB NIŽJIH STROŠKIH.

www.telekom.si/poslovni

Avtorja: dr. Andrej Bregar, dr. Ciril Kafol / Informatika d.d.*





VAROVANJE KIBERNETSKEGA OKOLJA V ELEKTROENERGETIKI Z VZPOSTAVITVIJO SEKTORSKEGA VARNOSTNEGA OPERATIVNEGA CENTRA

Kompleksni informacijski, poslovni in tehnični sistemi so vse bolj izpostavljeni kibernetskim grožnjam in tveganjem, na kar nakazuje tudi statistika podjetja WatchGuard, po kateri je bilo samo v tretjem četrtletju leta 2018 zaznanih skoraj milijon omrežnih kibernetskih napadov.

Uvod

Kibernetska varnost je še posebej resen izziv v organizacijskih okoljih z izrazito prisotnostjo infrastrukturnih virov. Mednje spada elektroenergetski sektor, ki se srečuje z več kritičnimi koncepti, kot so pametna omrežja, integracija IT in OT, prehod na izpostavljene spletne tehnologije, avtomatizacija in digitalna transformacija poslovanja ter uvedba zakonodajnih sprememb. V okviru slednjih opredeljuje 24. člen Zakona o informacijski varnosti sektorski varnostni operativni center kot osrednje telo, v katerega pristojnosti je odzivanje na incidente. Predpisan je za izvajalce storitev v posameznih reguliranih sektorjih, tudi v energetiki, ki je med elementi ključne infrastrukture druga najbolj izpostavljena panoga z vidika kibernetske varnosti. Posledica tega je, da se v energetiki srečujemo s številnimi izzivi, med katerimi je eden pomembnejših dejavnikov uvedba mehanizmov kibernetske varnosti, ki ščitijo sisteme, zlasti njihove ključne in kritične dele, pred kibernetskimi ranljivostmi (Orlić & Kafol, 2017).

Dejavniki kibernetske varnosti v elektroenergetskem sektorju

Primarnega pomena je zaščita pred napadi na kritično infrastrukturo (Jeznik, 2015), saj ima izguba elektrike lahko katastrofalne posledice za energetski sektor, države, regije, posameznike in celotno družbo. Ker je energetski sektor reguliran ter strateško in politično pomemben, je ena glavnih tarč sofisticiranih groženj. Dokumentiranih je bilo več napadov, na primer na ukrajinsko energetsko omrežje in na sisteme SCADA, ki jih je prizadel črv Stuxnet (Yong idr., 2012). Tako je nujno zagotoviti maksimizacijo razpoložljivosti in minimizacijo tveganj ter se soočiti z izzivoma omejevanja zunanjih in notranjih groženj ter okrevanja po napadih. Osnova za to so pristopi k aplikacijski, omrežni in informacijski varnosti, nadzor dostopa, upravljanje s spremembami, ocenjevanje ranljivosti, poročanje o incidentih in usposabljanje.

Kibernetskim napadom so v energetskem sektorju zelo izpostavljena pametna omrežja, zato mora biti kibernetska

> Učinkovit varnostni operativni center mora vključevati tri temeljne elemente – ljudi, procese in tehnologijo. Le-ti morajo biti neposredno vpeti v elektroenergetski sektor ter medsebojno tesno povezani in sočasno podprti, da omogočijo izvajanje nalog kibernetske varnosti.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

varnost eden njihovih ključnih vidikov (Wang & Lu, 2013). Poglavitna težava je velika množica naprav in senzorjev, na eni strani integriranih s sodobnimi oblačnimi storitvami, na drugi strani pa s starejšo infrastrukturo in programsko opremo, ki ni skladna z aktualnimi varnostnimi standardi. To izpostavlja varnostne luknje in ranljivosti. Poleg tega lahko digitalizacija, povezljivost in koncepti IoT zmanjšajo stroške, povečajo učinkovitost ter izboljšajo storitve, vendar pa postanejo sistemi zaradi povezanih tehnologij bolj kompleksni, varnostno ranljivi in zanimivi za napadalce.

Kot posledica intenzivne povezljivosti, integriranosti in odvisnosti od informacijskih sistemov so pametna omrežja izpostavljena ranljivostim v komunikacijah in omrežnih sistemih. Tako sta tveganjem podvrženi fizična in kibernetska infrastruktura. Ker lahko nastopijo negativne posledice za distributerje in odjemalce, je ključno ščititi parametre razpoložljivosti, integritete podatkov in zaupnosti informacij. Sredstva, ki jih v ta namen uporabljamo, vključujejo varne omrežne arhitekture in varne podatkovne protokole, predvsem pa je možno doseči celovito in sistematično zmanjšanje kibernetskih tveganj z uvedbo varnostnega operativnega centra.

Vloga varnostnega operativnega centra

Odgovornost za zaznavanje kibernetskih napadov in implementacijo rešitev lahko prevzame varnostni operativni center, kot osrednja avtoriteta za udejanjanje varnostnih politik in strategij. Njegov cilj je sistematično zmanjšati tveganja z obravnavo vseh ključnih vidikov varnosti, od organizacijskih, poslovnih in sistemskih do tehničnih, informacijskih in podatkovnih. Takšen center zagotovi infrastrukturo in strokovni analitični kader ter poskrbi za implementacijo več komplementarnih mehanizmov, ki zajemajo zbiranje podatkov o incidentih, poročanje, razvoj in raziskave, inteligenco za obravnavo groženj, bazo znanja, upravljanje varnostnih informacij in dogodkov (SIEM) ter agregacijo in koreliranje podatkov.

Učinkovit varnostni operativni center mora vključevati tri temeljne elemente – ljudi, procese in tehnologijo. Le-ti morajo biti neposredno vpeti v elektroenergetski sektor ter medsebojno tesno povezani in sočasno podprti, da omogočijo izvajanje nalog kibernetske varnosti. Ključni dejavnik je kultura kibernetske varnosti, ki jo je potrebno vzpostaviti in komunikacija med ljudmi, zlasti z analitičnim varnostnim kadrom, pa tudi vsemi ostalimi v sistemu. Pomanjkanje zavedanja kibernetske varnosti namreč povečuje operativna tveganja, ker je 93 % kibernetskih napadov in podatkovnih vdorov posledica človeških napak. Iz tega razloga je kibernetska varnost predvsem poslovni ter vodstveni problem in ne le problem tehnologije. Posledično je potrebno zagotoviti zadostno raznolikost ekspertnih znanj, kajti tehnična znanja v splošnem ne zadoščajo. Dopolnjevati jih je potrebno z ustreznimi varnostnimi in socialnimi znanji.

Naloge varnostnega operativnega centra se velikokrat ponavljajo, zaradi česar sta bistvenega pomena standardizacija in avtomatizacija obrambnih aktivnosti. Dosežemo ju z ustrezno metodologijo in zasnovo tehnologij za podporo varnostnim operacijam. Takšno metodologijo smo definirali v sklopu pripravljalnih aktivnosti za vzpostavitev varnostnega





operativnega centra (Kafol & Bregar, 2017). Pri tem smo obravnavali vse temeljne vidike, ki povezujejo ljudi, procese in tehnologijo, ter jih sistematizirali v referenčni model kibernetske varnosti. Učinkovit pristop naj bi upošteval tudi dognanja antropoloških študij, ki so razkrile, da je komunikacija med varnostnimi analitiki in uporabniki redkokdaj uspešna, zato je tehnologija kvečjemu tako dobra kot ljudje, ki jo uporabljajo (Squires & Shade, 2015).

Procesni vidik mora združevati elemente preprečevanja, zaznavanja in ukrepanja, ki varujejo tri edinstvene atribute informacije, in sicer zaupnost, integriteto ter dostopnost/razpoložljivost. Med procesnimi dejavniki so bistveni standardi, strategija in nivo zrelosti. Ker so posamične matrike nezadostne, je nujno uvesti formalen sistem merjenja zrelosti kibernetske varnosti. Obstaja nekaj standardov in zrelostno-zmožnostnih modelov, kot so COBIT, ISO 27001 in ES-C2M2. Izbira najprimernejšega pa ni vselej preprosta (Rea-Guaman idr., 2017). Prav tako velja, da je upravljanje kibernetskih tveganj sestavni del celovitega upravljanja tveganj v organizacijskem sistemu. Preprečevanje zunanjih in notranjih vdorov je torej le eden od vidikov strategije kibernetske varnosti. Enako pomembno je ukrepanje in okrevanje po vdorih.

Vpeljava sektorskega varnostnega operativnega centra

Naš cilj je, da v skupnem prizadevanju za kibernetsko varnost pristopimo k vzpostavitvi varnostnega operativnega centra v sodelovanju z družbami za distribucijo električne energije in drugimi ključnimi vlogami v energetskem sektorju. Izhajamo iz predpostavke, da je družba Informatika naravno okolje za realizacijo in delovanje sektorskega varnostnega operativnega centra, saj zagotavlja aplikativno, informacijsko in infrastrukturno podporo distributerjem električne energije ter premore ustrezna znanja, izkušnje in sistemske ter človeške vire.

Pri oblikovanju varnostne strategije in vzpostavitvi varnostnega operativnega centra je potrebno upoštevati celoten nabor dejavnikov, ki se nanašajo na ljudi, procese, tehnologijo in značilnosti energetskega sektorja. Potrebno je opraviti večji sklop aktivnosti, ki smo jih delno realizirali že v okviru vpeljave demonstracijskega varnostnega operativnega centra. Le-te so:

- pregled in analiza zrelosti kibernetske varnosti v energetskem sektorju;
- oblikovanje celovite strategije z identifikacijo nalog, ciljev in storitev;
- določitev kritičnih storitev in procesov ter identifikacija ključnih tveganj;
- specifikacija zahtevanih nivojev varovanja podatkov in infrastrukture;
- analiza razkoraka med obstoječim in želenim stanjem kibernetske varnosti v sektorju ter oblikovanje smernic za premostitev razlik;
- usklajevanje in povezovanje vidikov kibernetske in fizične varnosti.

Trenutno izhodišče je demonstracijski sektorski varnostni operativni center. Pri izvedbi smo sodelovali z zunanjimi partnerji, za integracije notranjih sistemov, pa smo uporabili lastno znanje in vire. Sistem temelji na IBM-ovi platformi – IBM QRadar za sistem SIEM, IBM Resilient za upravljanje z incidenti in IBM Guardium za nadziranje aktivnosti podatkovnih baz. Dodatni viri zajemajo relacijske podatkovne baze, strežniško infrastrukturo in omrežno opremo s stikali, krmilniki, usmerjevalniki in požarnimi pregradami. SIEM upravlja s podatki iz več virov, in sicer s podatki elektrodistribucijskih in zunanjih družb ter notranjimi podatki. Nadzor vršimo v vizualizacijski sobi. V uporabi je več nadzornih zaslonov za podrobne in splošne varnostne informacije, zahtevke podpornega centra, notranji nadzor in opozorila.

Sektorski varnostni operativni center skrbi za doseganje ustrezne stopnje kibernetske varnosti na organizacijskem, operativnem in sistemskem nivoju. Ta center je pomemben, ker se podobno kot v vseh kompleksnejših poslovnih in reguliranih okoljih tudi v energetski domeni izvajajo številni temeljni procesi, ki so standardizirani in vezani na kritično infrastrukturo.

Postopek odzivanja na incidente sestoji iz štirih faz, ki se po potrebi iterativno ponavljajo. Prva faza priprave zajema izvajane simulacij in eskalacijo dogodkov iz obstoječih virov. V fazi ocenitve vrednotimo podatke in dogodke glede na dobre prakse, zahteve po skladnosti in inteligenco nevarnosti. Faza upravljanja obravnava incidente, varnostna opravila in poročanje o napredku. V zadnji fazi minimiziramo tveganja na osnovi odzivov na incidente, korektivnih ukrepov in izboljšav. Postopek je zasnovan tako, da pokrije različne scenarije, kot sta nadzor kritičnega dostopa do podatkov in nadzor virtualnih povezav zunanjih uporabnikov.

Nabor kompetenc centra zajema zaznavanje in obravnavo incidentov, poročanje, vzpostavitev sistemov vab, modeliranje groženj, testiranje vdorov, preverjanje pristnosti, analizo izvorne in škodljive kode, odkrivanje ranljivosti, načrtovanje varnosti, ozaveščanje in usposabljanje.

Sklep

Sektorski varnostni operativni center skrbi za doseganje ustrezne stopnje kibernetske varnosti na organizacijskem, operativnem in sistemskem nivoju. Ta center je pomemben, ker se podobno kot v vseh kompleksnejših poslovnih in reguliranih okoljih tudi v energetski domeni izvajajo številni temeljni procesi, ki so standardizirani in vezani na kritično infrastrukturo. Zato morajo biti vzpostavljeni mehanizmi celovite in trajnostne kibernetske zaščite. Le-ti se morajo vzporedno in sistematično navezovati tudi na komplementarni vidik fizične varnosti.

Ključna težava pri vzpostavitvi varnostnega operativnega centra je pomanjkanje virov. Iz tega razloga je smiselna vpeljava hibridnega modela, pri katerem uporabimo notranje in zunanje kadrovske in tehnološke vire. Ker je ljudi na tržišču malo, je nujna skupna aktivnost, ki temelji na sodelovanju z vsemi deležniki in ponudniki v Sloveniji. Tako lahko govorimo o skupnem energetskem varnostnem operativnem centru, ki omogoča porazdelitev investicij in stroškov med deležnike, kar pomeni nižje stroške na posameznega deležnika. Hkrati se združitev prilagodi vsaki individualni organizaciji, zaradi česar ni potrebno odpovedovanje suverenosti na področju kibernetske zaščite.

Nadgradnja tega principa je operativno in poslovno povezovanje varnostnih operativnih centrov iz različnih področij. Tako lahko nastane VOC Slovenija, ki bo uspešen, če povežemo ljudi in organizacije, ki poznajo raznolike stroke na področju kibernetske varnosti. Na ta način učinkovito uporabimo obstoječe vire v Sloveniji ter poskrbimo za razvoj manjkajočih virov in povezovanje z mednarodnimi deležniki in bazami. Energetski varnostno operativni center bo s tem postal aktiven deležnik zagotavljanja kibernetske varnosti na nivoju Slovenije in širše.



Literatura

- Jeznik, N. (2015). Informacijska varnost v energetiki. Korporativna varnost, 9, 51–54.
- Kafol, C., & Bregar, A. (2017). Cyber security – building a sustainable protection. DAAAM International Scientific Book, vol. 16, str. 81–90. Dunaj: DAAAM International Vienna.
- Orlić, D., & Kafol, C. (2017). Kibernetska varnost energetskega sektorja v Sloveniji. 13. konferenca slovenskih elektroenergetikov CIGRE-CIRED.
- Rea-Guaman, A. M., Feliu, T. S., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative study of cybersecurity capability maturity models. International Conference on Software Process Improvement and Capability Determination, str. 100–113.
- Squires, S., & Shade, M. (2015). People, the weak link in cyber-security: Can ethnography bridge the gap? Ethnographic Praxis in Industry Conference, str. 47–57.
- Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57 (5), 1344–1371.
- Yong, W., Dawu, G., Daogang, P., Shuai, C., & Heng, Y. (2012). Stuxnet Vulnerabilities Analysis of SCADA Systems. Communications in Computer and Information Science, vol. 345. Berlin: Springer. ■

www.posta.si

Za vsako zgodbo, **samo en naslov je pravi!**



KRAFTWERK

ZANESLJIVO Z VAMI!

Ko za posel v oblaku ste pravi in vas na poti k uspehu nič ne ustavi. Ko potrebujete rezervni del ali partnerja, ki bo za vas vsak dan poskrbel. Če ste prepozni za banko ali želite v zbirko dodati novo znamko. Ko želite razveseliti z voščilom ali presenetiti z lepim darilom. **Za vsako zgodbo, samo en naslov je pravi!**

Pošta Slovenije
Zanesljivo z vami!



Poskrbite za varnost na spletu pri vašem poslovanju.

Zavarovanje kibernetske zaščite za podjetja

Vse bo v redu.

triglav

www.triglav.si

Avtorja: Marko Zavadlav / PRO.astec
Mihael Nagelj / Gospodarska zbornica Slovenije





VPLIV PROJEKTA CYBER INTERREG EU NA ZAGOTAVLJANJE VARNOSTI V MALIH IN SREDNJIH PODJETJIH TER RAZVOJ NOVIH STORITEV KIBERNETSKE VARNOSTI

Mala in srednja podjetja so v modernem digitalnem svetu enako izpostavljena kibernetskim tveganjem kot velika, le da za učinkovito zagotavljanje varnosti nimajo na voljo ustrezne opreme in kadrov za izvajanje potrebnih nalog varovanja informacij. Kako pomagati malim in srednjim podjetjem, s področja kibernetske varnosti, pri zagotavljanju ustreznih rešitev, je namen projekta Cyber Interreg Europe.

Današnje poslovno okolje zahteva hitre odzive, učinkovitost in natančnost. Z nenehnim in hitrim razvojem so se informacijske tehnologije vključile v vsakodnevno poslovanje. Praktično ni več poslovnega okolja, pa naj bo še tako majhno, ki ne bi bilo podprto z informacijsko tehnologijo. Nihče ne vodi računovodstva in saldakontov ročno, vsi uporabljamo elektronsko pošto za komunikacijo, uporabljamo pisarniške programe, imamo spletne strani in drugo. To pa je šele začetek. Vedno več malih in srednjih podjetij, delujočih v tradicionalnih branžah z nizko stopnjo uporabe informacijske tehnologije, vse intenzivneje digitalizira svoje ključne procese z vedno novimi tehnologijami in novimi koncepti njihove uporabe.

Vsi smo povezani v internet, preko njega so dosegljive naše ključne informacije, za marsikatero sploh nimamo več analogne kopije. Večkrat ste že slišali, če ne doživeli, kako se lahko pripeti, da se z izgubo ali okvaro navadnega mobilnega telefona izgubijo vsi poslovni kontakti (seveda tudi zasebni). Kako je nekdo imel celotno poslovanje na osebnem računalniku, pa je prejel izsiljevalski virus. Nove tehnologije pa poleg koristi prinašajo tudi nove ranljivosti, ki se, s povečevanjem intenzivnosti komuniciranja vse večjega števila naprav na internetu, še povečujejo. V digitalnem okolju številnih koristi in priložnosti so svoje priložnosti našli tudi zlonamerneži in organiziran kriminal. V medijih beležimo velik porast novic o spletnih napadih, o zlorabah, spletnih prevarah in izsiljevanjih, ki se ne dogajajo samo drugje. To je tudi naša realnost.

Splošni cilj projekta CYBER Interreg EU je povečati konkurenčnost malih in srednjih podjetij na področju kibernetske varnosti, in sicer izboljšanjem javnih politik in odpravo skupnih ovir, kot so razdrobljenost trga ali pomanjkanje strokovnega kadra ter izboljšanja eco sistema v celoti.

Ker preprosto ne moremo živeti odrezani od digitalnega sveta, se moramo ustrezno zaščititi tudi sami. Razvoj digitalizacije daje priložnosti tudi malim in srednjim podjetjem s podorčja kibernetske varnosti, da razvijejo nove storitve in izdelke za čas, ki je pred nami. Splošni

cilj projekta CYBER Interreg EU je povečati konkurenčnost malih in srednjih podjetij na področju kibernetske varnosti, in sicer izboljšanjem javnih politik in odpravo skupnih ovir, kot so razdrobljenost trga ali pomanjkanje strokovnega kadra ter izboljšanja eco sistema v celoti. Rešitve vidimo predvsem v povezovanju nosilcev raziskav in razvoja s podjetji na trgu na eni strani in ponudnikov ter uporabnikov storitev na drugi s ciljem razvoja inovativnih in učinkovitih rešitev tudi s sodelovanjem na globalnem trgu. V nadaljevanju govorimo o dveh primerih takšnih rešitev.

Tveganja v informacijskem svetu lahko v grobem delimo na tista, ki so odvisna od zlonamernežev oziroma kriminalcev, tista, ki so posledica napačnega delovanja opreme, ki jo uporabljamo pri svojem delu in pa na tista, ki so posledica dejanj nas in naših zaposlenih zaradi malomarnosti ali nevednosti. Največ se govori o tveganjih, povezanih s kibernetskimi napadi in zlorabami, zato si jih natančneje oglejmo in jih analizirajmo, saj si ne moremo več zatiskati oči, da se ta tveganja ne morejo uresničiti pri nas. Če poskusimo primerjati analogni in digitalni svet opazimo, da se v analognem svetu lahko gibljemo »pod radarjem«. Malo verjetno je, da nam bo nekdo poskusil ukrasti avto, ki ni vreden več kot 20.000 €, da nam bo kdo vlomil v stanovanje, če bo na daleč jasno, da v njem nimamo primernih dragocenosti. Vlomilci namreč najprej ocenijo, ali se jim splača tvegati. V digitalnem svetu, če seveda ne govorimo o vrhunskih kriminalcih, ki natančno vedo, koga napadajo, ne moremo biti varni. Običajni napadalci namreč vržejo vabo, ki doseže ogromno število ljudi, torej lahko dosežejo dobiček s svojim »poslovnim modelom« že pri majhnih izplenih na posameznika. Digitalizacija namreč omogoča, da ja napadalec lahko kjerkoli, torej lahko doseže ogromno število potencialnih žrtev v izjemno kratkem času. Dodatna težava je tudi v tem, da za izvedbo takega napada ni potrebno veliko znanja ali premetenosti. Danes se na črnem tržišču že za relativno majhen denar lahko nabavi storitve ali programsko opremo za take napade. Če pogledamo primere z izsiljevalskimi virusi, so napadalci od vsake zaklenjene delovne postaje zahtevali recimo 1 bitcoin. Danes to pomeni vrednost okoli 3.000 €. Seveda so lahko zahtevali tudi manj. Za izvedbo celotne kampanje so porabili recimo 10.000 € (nabava strojne in programske opreme, zakrivanje sledi in ostalo), virus so razposlali naokoli, in če se je ujelo 500 posameznikov, je računica izjemna. Celotna kampanja je trajala maksimalno dva meseca. Torej, koliko so zlonamerneži lahko zaslužili v dveh mesecih?

Drugi primer je izguba podatkov zaradi napake v delovanju opreme. Premalokrat se zavedamo, da imamo na računalniški opremi izjemno pomembne podatke, brez katerih težko ali pa sploh ne moremo poslovati. Vedno pa se pojavi problem visokih stroškov opreme.

Tretji primer pa govori o nas samih. Včasih se nam preveč mudi, ne vemo natančno, kaj moramo narediti, nismo dovolj izobraženi ali usposobljeni za izvajanje določenih operacij. Vsi načelno vemo, kaj je potrebno za zagotavljanje ustreznega nivoja varnosti. Gre za varnostne naprave, za vrhunsko opremo ter za usposabljanje in izobraževanje.

Velike organizacije si lažje privoščijo požarne pregrade naslednje generacije, sisteme za zaznavo in preprečevanje vdorov, spremljanje in alarmiranje v primeru zaznanih poskusov zlorabe. Lahko si privoščijo vrhunsko informacijsko opremo, redundantne strežnike, varnostne kopije na več lokacijah ali rezervne lokacije. Za izvajanje varnostnih funkcij lahko izobrazijo lastne strokovnjake, lahko nenehno ozaveščajo in izobražujejo zaposlene.

Kaj pa majhna in srednja podjetja? Običajno imajo mnogo bolj omejene vire. Ne morejo si privoščiti zelo dragih na-





prav, ne morejo zaposliti vrhunskih strokovnjakov, ne morejo imeti opreme »na zalogo«. Torej so, ne glede na to, da z vidika kriminala niso tako zanimivi, mnogo bolj ranljivi in izpostavljeni.

Ravno zato se morajo poslužiti drugih načinov zagotavljanja zaščite. Veliko funkcij se da izdvojiti in jih predati v upravljanje zunanjemu izvajalcu storitev. Danes so zelo zanimivi produkti, ki jih lahko poimenujemo Varnost kot storitev (Security as a Service). Obstajajo različni načini in nivoji, a skupno jim je to, da lahko za razumno ceno, ki je bistveno nižja od stroškov lastne postavitve varnostnih naprav, njihovega upravljanja in posodabljanja. S tako storitvijo majhne in srednje velike organizacije lahko dosežejo zadovoljiv nivo varnosti. Naslednja storitev, ki jo organizacija lahko izdvoji, je varnostno kopiranje in hranjenje. V naslednjem koraku se organizacija lahko odloči tudi za ostale oblačne storitve (strežnike, programsko opremo, storitve). Danes so vsi ti načini za manjše organizacije dokazano cenejši kot upravljanje lastnega informacijskega okolja.

V letu 2018 pa je na slovensko tržišče prišla še ena zanimiva možnost zmanjševanja tveganja in sicer s tako imenovanim načinom prenosa tveganja na druge. Gre za zavarovanje kibernetskega tveganja. Zavarovalnice so začele ponujati zavarovalne pakete, v katerih lahko zavarujemo svoje podatke, zavarovalnica pa nam krije stroške, ki nastanejo ob kibernetskem napadu. Govorimo o stroških strokovnjakov, ki so na voljo za zajezitev in odpravo varnostnega incidenta, za vzpostavitev prvotnega stanja, za kritje stroškov, ki bi nastali ob kršitvah zakonodaje, tipično zaradi kršitve varstva osebnih podatkov ter stroške, ki bi nastali tretjim osebam, če bi utrpeli škodo zaradi varnostnega incidenta, ki bi izviral iz našega omrežja.

Zgornja dva primera storitev kibernetske varnosti za mala in srednja podjetja sta samo dva med številnimi možnostmi. Nikakor ne smemo pozabiti na področje izobraževanja in ozaveščanja, katera bodo prispevala k dvigovanju varnostne kulture. Posebno pozornost zahteva izobraževanje vrhunskih specialistov zagotavljanja varnosti, ustrezno konkurenčno okolje in ne nazadnje tudi okolje, ki bo spodbujalo v razvoj novih kompetenc in produktov varnosti. Na projektu Cyber Interreg EU, ki poteka v okviru GZS, je bil med drugimi podan tudi predlog vzpostavitve kompetenčnega centra, ki bi malim in srednjim podjetjem lahko nudil razne oblike ozaveščanja in izobraževanja ter s svojim delovanjem pomagal pri spreminjanju varnostne kulture malih in srednjih podjetij ter prispeval k povečanju varnosti tudi v takšnih organizacijah.

Majhna in srednja podjetja so močno izpostavljena informacijskim varnostnim tveganjem o čemer pričajo številni primeri. Stroški za obvladovanje tveganj znotraj organizacije z lastnimi kadri so nesorazmerni v primerjavi s številnimi drugimi možnostmi na trgu. Organizacije morajo le oceniti, kakšno vrednost jim pomenijo informacije v njihovih informacijskih sistemih ter se odločiti za optimalen način varovanja. Mala in srednja podjetja na področju kibernetske varnosti pa potrebujejo izboljšano okolje za svoje delovanje in razvoj ter uspešno prilagajanje spremembem v konceptih kibernetske varnosti. ■

Na projektu Cyber Interreg EU, ki poteka v okviru GZS, je bil med drugimi podan tudi predlog vzpostavitve kompetenčnega centra, ki bi malim in srednjim podjetjem lahko nudil razne oblike ozaveščanja in izobraževanja ter s svojim delovanjem pomagal pri spreminjanju varnostne kulture malih in srednjih podjetij ter prispeval k povečanju varnosti tudi v takšnih organizacijah.

astec®

Poslovno svetovanje
Upravljanje in vodenje projektov
Kibernetska varnost
Izobraževanje in certificiranje
Revizije IS
Upravljanje IT
Informacijska varnost in skladnost
Neprekinjenost poslovanja
GDPR
Informacijsko svetovanje
Upravljanje storitev
Priprava organizacije za certificiranje

PRO.astec d.o.o.
Dunajska cesta 158
1000 Ljubljana

T +386 1320 71 33
E info@astec.si

www.astec.si

take a challenge
UNISTAR PRO
Challenge, Passion, Trust.

Stay Untouched.
And Secure Your Security.
www.cactusconcept.com

Beyond Human Vision
MOBOTIX

tend
/ IT rešitve / IT solutions /

ORG. TEND d.o.o.
Kraljevica Marka ulica 19
SI-2000 Maribor
E: mobotix@tend.si
W: www.tend.si

Avtor: Žiga Podgoršek, Certificirani Etični heker / Institut za korporativne varnostne študije*



SOCIALNI INŽENIRING KOT UMETNOST PSIHOLOŠKE MANIPULACIJE

Socialni inženirji so umetniki manipulacije, ki izkoristijo obnašanje in navade ljudi z namenom pridobitve občutljivih ali zaupnih podatkov, do katerih niso avtorizirani. Napadalci se primarno odločajo za te vrste napadov, ker je v praksi velikokrat lažje izkoristiti človeško naravno nagnjenost k zaupanju, kot zlorabiti programsko opremo žrtve in na ta način priti do občutljivih podatkov.

Najšibkejši člen varnostne verige je človek. Ni pomembno koliko ključavnic imamo na vratih in kako se potrudimo za fizično in tehnično varnost na splošno, če zaupamo osebi, ki pri vstopu v našo organizacijo trdi, da je na primer na novo zaposleni vzdrževalec in ga spustimo v naše prostore, ne da se trdno prepričamo, da je ta oseba res tisto za kar se izdaja. Potrebno se je prepričati ter osebo ustrezno preveriti in ji ne slepo zaupati.

Varnost velikokrat pomeni zavedanje komu in kaj zaupati. Potrebno je znati preceniti, kdaj zaupati nekomu in oceniti, ali je ta oseba res tisto za kar se izdaja. Enako je pri obiskovanju spletnih strani in pri prejetih elektronskih sporočilih. Potrebno je znati oceniti ali je stran oz. sporočilo legitimno ter ali je varno vnesti svoje informacije oziroma tisto kar od nas zahteva.

Danes je ta vrsta napada postala prava epidemija, ki obstaja v mnogih oblikah. Poznamo več vrst napadov, ki spadajo v skupino socialnega inženiringa kot na primer: ribarjenje (ang. phishing), spear phishing, vishing (voice phishing), pretexting (lažno predstavljanje), whaling (phishing oseb na višjem položaju), SMiShing (SMS phishing), watering hole, tailgating, brskanje po smeteh,.. Kot najpogosteje izkoriščeni metodi izmed naštetih se pojavljata phishing in spear phishing.

Če pomislimo na tipičen pretok elektronskih sporočil na dnevni ravni, ko prejemamo legitimna sporočila, marketinške ponudbe, vsiljeno pošto in »goli phishing«. Največkrat »phishing« sporočila končajo v mapi z vsiljeno pošto, vendar napadalec po metodi zbiranja podatkov iz javnih virov (ang. OSINT – Open-source intelligence), lahko ustvari tekst in ga

Ker gre pri socialnem inženiringu za vrsto napada, kjer je ključen faktor človek, se pred njim težko ubranimo, če ne izobrazimo svojih zaposlenih.



*avtor je član Slovenskega združenja korporativne varnosti



prilagodi tarči, kateri bo vsaj na prvi pogled izgledal dokaj legitimno.

Podatki iz javnih virov predstavljajo vse informacije in podatke, ki so na voljo javno in so, na svetovnem omrežju, prosto dostopni vsakomur.

Ko je tarča izbrana, se jo tako v službi, kot v privatnem okolju, na prvem mestu celovito profilira. Kot del profiliranja se največkrat, kot zelo koristna izkažejo socialna omrežja, kjer je prava poplava uporabnih informacij, katere smo v večini objavili sami. Velikokrat se med slikami pojavijo posnetki delovnega mesta, slike iz katerih je možno razbrati ali se v nekem delovnem okolju na primer uporabljajo delovne obleke in kako izgledajo, katere vrste pristopne kontrole so v uporabi, morda je mogoče iz katere slike razbrati napisana gesla in podobno.

Ena izmed osnovnih oblik socialnega inženiringa je tako imenovani »baiting«, kjer napadalec naloži »payload« (zlonamerna koda), ki je tipično zlonamerna programska oprema ali »revere shell«, na žrtvin sistem preko okuženega USB ključa, SD kartice, QR kode,.. Velikokrat so prenašalci te kode označeni z mikavnim napisom kot na primer, »last uprave« ali »plače zaposlenih« s čimer želijo napadalci izkoristiti človeško naravno željo po vsevednosti in nas zavesti, da si želimo ogledati vsebino.

Ko govorimo o »vishingu«, govorimo o eni zapletenejših oblik socialnega inženiringa. Pri tem napadalec opravi telefonski razgovor z žrtvijo pod pretvezo, da opravlja določeno anketo, kot izgovor za vprašana osebna vprašanja, kar zahteva veliko improvizacije in raziskovalne predpriprave, da je situacijo možno profesionalno in uspešno izpeljati. Raziskave kažejo, da kar 90% vprašanih ljudi pove svoje osebne podatke kot so ime, priimek in naslov elektronske pošte in 67% ljudi pove poleg še svoje rojstne podatke, ne da bi poznali identifikacijo sogovornika.

Najbolj razširjena oblika pa je »phishing« preko elektronskih sporočil. Napadalec preprosto pošlje e-pošto žrtvi ali več žrtvam sočasno v upanju, da bodo v prepričljivo formo vnesli svoje podatke, odprli povezavo v sporočilu ali prenesli okuženo datoteko. Napadalci velikokrat uporabijo domeno, ki je izjemno podobna neki preverjeni in zaupanja vredni domeni, saj s tem poskušajo zavesti žrtev. Ta tehnika se imenuje »domain squatting«.

»SMiShing« je, kot že samo ime pove, napad povezan s prejetim SMS sporočilom, ki žrtve poskuša zavesti, da kliknejo na povezavo, ki jo vsebuje ali odpre priponko (npr. slika) in si s tem naložijo zlonamerno kodo. Ne dolgo nazaj je v svet prišla novica, da so določene android naprave ranljive in se lahko okužijo že samo z ogledom PNG slike. Ne glede na to, kaj sporočilo od nas zahteva, se na takšna sporočila ne odzovemo.

O »tailgating« napadu govorimo, kadar želi napadalec vstopiti v območje omejenega dostopa, kjer se pristop kontrolira z elektronsko pristopno kontrolo. Napadalec lahko izkoristi take dostope, s sledenjem zaposlenega, ki pred njim odpre vrata v območja omejenega dostopa.



Prav tako v skupino OSINT spadajo sledeče storitve: čistilni servisi, vzdrževalni servisi, oskrba s hrano (v primeru okrepčevalnice na lokaciji), IT dobavitelji in IT tehnologije v uporabi (VPN, WiFi, operacijski sistemi, anti virusni programi), delovni čas, cikli usposabljanj, iztrebljevalci,..

Poznati nekatere od teh storitev, lahko potencialno omogočijo ali olajšajo napadalcu iskanje ranljivosti, ki so v uporabi v ciljnem okolju. Napadalec lahko, na podlagi teh informacij razvije zgodbo, katero dobro preuči in poskuša z njo zavesti žrtev. Napadalci velikokrat pristopijo do žrtve in poskušajo z njo speljati pogovor, kjer na podlagi prej prirejene zgodbe poskušajo priti do občutljivih in pomembnih podatkov, kateri lahko doprinesejo še več njemu pomembnih informacij ali kako drugače vplivajo na žrtev, kar mu omogoči nadaljnje manevre. Na spletni strani podjetja, kjer so objavljeni razpisi za nova delovna mesta ali storitve, je odlično mesto za začetek iskanja. Na podlagi tam objavljenih informacij, lahko napadalec pridobi ogromno podatkov o tem, kaj podjetje potrebuje, na katerih platformah deluje in katere sisteme uporablja.

Ker gre pri socialnem inženiringu za vrsto napada, kjer je ključen faktor človek, se pred njim težko ubranimo, če ne izobrazimo svojih zaposlenih. Priporočamo izobraževanja na četrtletni ravni, kar pripomore k dobri splošni ozaveščenosti in vzpostavi splošno mentaliteto zavedanja o tovrstnih napadih. Izjemno pomembno je ozavestiti prav vse zaposlene od top managementa do delavca.

Poleg izobraževanja na teoretični ravni, je izjemno pomembno tudi praktično izobraževanje. Pri tem govorimo o simulacijah »phishing« tehnik in s tem tudi testiranja zaposlenih. S tem zagotovimo pravilno reakcijo zaposlenih in primerno ter vestno poročanje o incidentih. Vse kaže, da socialni inženiring, ki izvira že iz daljne zgodovine, ne bo kaj kmalu usahnil ali prišel do svojega konca. Zaradi tega ponovno izpostavljam nujnost širjenja ozaveščenosti v vsaki organizaciji in izobraževanja prav vseh zaposlenih v periodičnem ciklu, kar pripomore k zavedanju trojanskih konjev, ki prežijo na vse. ■

Spreminjamo pravila poslovne varnosti!

Z A1 naprednimi varnostnimi rešitvami za vse vrste podjetij.

A1 Protekt
Varnostna rešitev v omrežju A1

F-Secure
Celovita zaščita pred virusi, vdori in nezaželeno pošto

Stormshield
Požarni zid naslednje generacije

iStor
Varnostno kopiranje podatkov v realnem času

Vectra
Zaznavanje kibernetskih napadov s pomočjo umetne inteligence

Wallix
Platforma za upravljanje privilegiranih dostopov

A1.si

Več o storitvah in vse Posebne pogoje uporabe storitev ter cene najdete na A1.si, 040 40 40 40 in na A1 prodajnih mestih. A1 Slovenija, d. d., Šmartinska 134b, 1000 Ljubljana.

GREY A1 Slovenija, d.d., Šmartinska cesta 134b, 1000 Ljubljana

Avtor: Rok Novak / Reisswolf d.o.o.*



5 KORAKOV ZA VARNO UPRAVLJANJE Z DOKUMENTACIJO

Varnost podatkov je za različne deležnike različno pomembna. Ko govorimo o varnosti osebnih podatkov, gre za varnostni interes posameznika, na katerega se osebni podatek nanaša, ko govorimo o varnosti poslovnih podatkov, gre za varnostni interes organizacije in ko govorimo o varnosti tajnih podatkov, gre za varnostni interes države. V dinamičnem poslovnem okolju se največkrat srečujejo vsi trije omenjeni deležniki, torej posameznik, organizacija in država in tako prihaja do prepletanja teh treh interesov na različnih nivojih, v različnih procesih in v različnih okoljih. In v takem dinamičnem okolju ima varnost podatkov še toliko večji pomen.

Se še spomnite, ko smo kot otroci v vrtcu ali prvih razredih osnovne šole risali in pisali na tako imenovani »šmirpapir«, že uporabljen, potiskan, popisan papir, za drugotno rabo. Veliko je bilo primerov, ko smo domov staršem vsi ponosni in vzhičeni prinesli na eni strani svoje risarske izdelke, na drugi strani pa izpis plače iz nekega podjetja. Verjamem, da je to v tem času, ob povprečni stopnji varnostne ozaveščenosti, skorajda nemogoče ponovljiv scenarij, se pa sedaj pojavljajo povsem nova tveganja, povezana z upravljanjem in obdelavo raznih vrst podatkov, predvsem tistih, ki se obdelujejo v e-obliki. S pojavom digitalizacije, digitalne transformacije poslovnih procesov podjetij in družbe kot celote, ta tveganja postajajo še bolj kompleksna in globalno izpostavljena. Naj omenim le nekaj odmevnih primerov iz zadnjega časa: vdor v Facebook račune v mesecu novembru 2018 (kompromitiranih 50 mio uporabniških računov), vdor v bazo podatkov hotelske verige Marriot (kraja podatkov 500 mio gostov potekala več let), Kršitev varstva osebnih podatkov v portugalski bolnišnici (dostop do podatkov o bolnikih – 400.000 EUR globe), kršitev varstva osebnih podatkov na letališču Heathrow Airport (zaradi slabega varstva osebnih podatkov globa 120.000 GBF), vdor v baze osebnih podatkov zdravstvene zavarovalnice Anthem (vdor v bazo podatkov in dostop do podatkov 80 mio ljudi). Omenjene slabe prakse nakazujejo na občutljivost predvsem elektronskih baz podatkov in kompleksnost zagotavljanja dostopnosti in varnosti le-teh.

Vsa ta nova tveganja, ki se pojavljajo v digitalnem svetu, v povezavi s tveganji upravljanja z dokumentacijo v fizični obliki, nakazujejo na nujnost poznavanja in razumevanja življenjskega cikla določenega podatka in pomembnost prepoznavanja ranljivosti, ogroženosti in tveganj, ki se pojavljajo v posamezni fazi življenjskega cikla konkretnega podatka.

Vsa ta nova tveganja, ki se pojavljajo v digitalnem svetu, v povezavi s tveganji upravljanja z dokumentacijo v fizični obliki, nakazujejo na nujnost poznavanja in razumevanja življenjskega cikla določenega podatka in pomembnost prepoznavanja ranljivosti, ogroženosti in tveganj, ki se pojavljajo v posamezni fazi življenjskega cikla konkretnega podatka. Izkušnje in slabe prakse v zadnjem času nakazujejo predvsem na pomanjkanje zavedanja o pomenu varnosti podatkov, ki se nahajajo na različnih podatkovnih nosilcih (dokumentacija v fizični obliki, diski, CD-ji, spominski ključki ipd.) predvsem v zadnjih fazah njihovega življenjskega cikla, to je v času shranjevanja v arhivih, ko govorimo o fizični dokumentaciji in strežnikih ali prenosnih medijih, ko govorimo o dokumentaciji v e.obliki. Podjetja veliko pozornosti posvečajo upravljanju in obdelavi podatkov

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

v času, ko so le ti aktivni, torej v fazi od njihovega nastanka ali prejema, pa vse do konca njegove uporabe. In v tej fazi se v večini primerov aktivna obdelava podatka – dokumenta zaključi. Dokument se izloči iz uporabe in na tak ali drugačen način odloži v hrambo. Obdelovalec podatka pa s tem ne zaključi s svojo odgovornostjo, saj je podatek na dokumentu še vedno aktiven in se mora hraniti glede na zakonske ali kako drugače določene minimalne roke hrambe. V tej fazi se morata torej upravljavec in obdelovalec podatkov zavedati, da je potrebno tudi v fazi arhiviranja (hrambe) in uničenja dokumentacije ali ostalih podatkovnih nosilcev zagotoviti varnost in sledljivost v fazi dostopnosti do arhivirane dokumentacije, v fazi same hrambe dokumentacije in na koncu tudi v fazi uničenja dokumentacije ali kakršnegakoli drugega podatkovnega nosilca.

V podjetju Reisswolf smo razvili celovito rešitev, ki upravljavcem in obdelovalcem podatkov omogoča varno in sledljivo upravljanje in obdelavo v celotnem življenjskem ciklu podatka, torej od njegovega nastanka oziroma prejema do njegovega uničenja. Z našo rešitvijo in našimi znanji vam lahko v samo 5 korakih vzpostavimo varen in sledljiv proces upravljanja in obdelave podatkov in s tem zagotovimo skladnost upravljanja in obdelave podatkov z veljavno zakonodajo, standardi in dobrimi praksami s tega področja, ne glede na vrsto podatka s katerim se upravlja in katerega se obdeluje.

1. Korak: Posnetek stanja in izdelava klasifikacijskega načrta

Nujni pogoj za vzpostavitev dolgoročne celovitosti, sledljivosti in varnosti upravljanja in obdelave podatkov je izdelava posnetka stanja in t.i. Blueprinta s katerim se ugotovi dejansko stanje na področju upravljanja in obdelave podatkov, vrzeli v obstoječem sistemu ter oceni tveganja na tem področju. Posnetek stanja služi kot podlaga za pripravo predlogov izboljšav obstoječega sistema ter definira morebitne nove uporabniške zahteve. Končni rezultat posnetka stanja je izhodni dokument, imenovan klasifikacijski načrt, ki točno definira proces upravljanja in obdelave podatkov, vrste podatkov, razvrščaje podatkov po stopnjah zaupnosti (osebni podatki, posebni osebni podatki, poslovne skrivnosti, tajni podatki ipd.), baze podatkov, način označevanja podatkov, dokumentacije in baz podatkov, nosilce in njihove odgovornosti, načine dostopov do posameznih baz podatkov in same dokumentacije, roke hrambe in ostale posebnosti povezane z upravljanjem in obdelavo podatkov.

2. Korak: Določitev procesa obdelave podatkov

V tej fazi se določi organizacija upravljana in obdelave podatkov (t.i. Wofkflow), torej kje posamezni podatki vstopajo v procese, kdo je skrbnik podatkov/baz podatkov, kako poteka proces obdelave podatkov/baz podatkov, kje so vmesne kontrolne točke in kje podatki izstopajo iz procesa. V tem koraku se definirajo tudi načini hrambe podatkov po izhodu iz procesov, torej po zaključku njihove aktivne obdelave. Drugače povedano, določi se proces arhiviranja podatkov in postopke v primeru potrebe po dostopu do arhiviranih podatkov v njihovem času hrambe. Prav tako se v tem koraku določi tudi način trajnega uničenja podatkov, ki se hranijo v fizični obliki (beri dokumentacije) in trajnega izbrisa podatkov, ki se hranijo v e.obliki.



3. Korak: Varna in sledljiva obdelava podatkov

Vzpostavitev organizacije upravljanja in obdelave podatkov je nujni pogoj za zagotavljanje hitre dostopnosti in optimalne uporabne vrednosti podatka. Tako z zakonskega kot tudi poslovnega vidika, pa je v fazi obdelave podatka pomembno zagotoviti njegovo varnost in sledljivost. Pri tem je pomembno, da do podatka dostopajo le tisti, ki so za to pooblaščeni in podatek potrebujejo pri izvajanju svojega procesa, da z obdelavo podatka obdelovalci prenehajo takoj, ko prenehajo razlogi za njegovo obdelavo ter, da je ves proces obdelave tudi v vsakem trenutku sledljiv in kot tak omogoča rekonstrukcijo obdelave v primeru pojava zlorabe ali izgube določenega podatka.

4. Korak: Vzpostavitev varnega in sledljivega arhiviranja

V tem koraku določimo pravila arhiviranja podatkov. Tu gre za dve različni področji arhiviranja, odvisno od oblike podatkovnega nosilca. V kolikor gre za dokumentacijo v fizični obliki je potrebno zagotoviti arhivske prostore, ki so skladni z zahtevami zakonodaje in standardov in kot taki zagotavljajo predvsem varno hrambo dokumentacije in sledljivost upravljanja z dokumentacijo (sledljivost poizvedb za arhivirano dokumentaciji, vnosov in iznosov dokumentacije in rokov hrambe dokumentacije). Gre predvsem za zagotavljanje ustreznih prostorov in opreme, ustreznih klimatskih pogojev (predvsem ustreznega in konstantnega nivoja vlage ter temperature), zavarovanje pred vlomom, požarom, izlivom ali vdorom vode, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi. V kolikor gre za dokumentacijo v e.obliki pa je potrebno poleg varne hrambe in sledljivosti dostopov do dokumentacije upoštevati še varnostna tveganja povezana z dostopnostjo do baz podatkov, kar v zadnjem času, glede na prakse vdorov v informacijske sisteme, predstavlja še posebej velik izziv. Ko govorimo o e.hrambi dokumentacije se mora ves čas hrambe omogočati reprodukcijo vsebine izvirne dokumentacije, dostopnost (varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom), uporabnost (zmožnost reprodukcije in primernost reprodukcije), avtentičnost (dokazljivost povezanosti reproducirane vsebine z vsebino izvirne dokumentacije) in celovitost (nespremenljivost in neokrnjenost ter urejenost reprodukcije).

5. Korak: Vzpostavitve varnega in sledljivega uničenja

Po zaključenem življenjskem ciklu podatka (izteku roka hrambe) je potrebno poskrbeti za varno in sledljivo uničenje dokumentacije in drugih podatkovnih nosilcev. Ko omenjam druge podatkovne nosilce mislim predvsem razne zdravstvene RTG slike, diske, CD-je, ključke in ostale elektronske prenosne medije, na katerih hranimo dokumente v e-obliki, pa tudi službena oblačila z logotipi podjetij in navedenimi osebnimi podatki. Pomembno se je zavedati, da je življenjski cikel podatka zaključen šele v fazi, ko je ta trajno uničen ali izbrisan in njegova reprodukcija oziroma ponovna rekonstrukcija ni več možna. V tej fazi se zaključi tudi odgovornost upravljavca in obdelovalca po zagotavljanju varne in sledljive obdelave podatkov.



Težko je v nekaj odstavkih opisati kompleksen pristop k vzpostavljanju varnega in sledljivega upravljanja in obdelave podatkov, saj gre za izjemno kompleksno področje, tako z vidika zakonodaje in standardov, kot tudi specifičnosti uporabniških potreb posamezne organizacije. Vsekakor je pomembno, da se v prvi vrsti zagotovi skladnost upravljanja in obdelave z zakonodajo in standardi, nato pa se z izborom ustrezne organizacije ter tehničnih in varnostnih ukrepov vzpostavi celovit sistem, ki nam v vsakem trenutku zagotavlja sledljivo obdelavo in varno hrambo ne glede na to v katerem življenjskem ciklu se določen podatek obdeluje.

V Reisswolfu smo zato razvili enostaven, ekonomsko in uporabniško učinkovit, varen in sledljiv sistem upravljanja z dokumentacijo tako v fizični kot tudi e.obliki, ki uporabnikom zagotavlja skladnost upravljanja in obdelave dokumentacije z zakonodajo, standardi in dobrimi praksami. ■

Avtor: mag. Marko Potokar / Vodja varovanja, Upravljanje nepremičnin in storitve,
Novartis Business Services Lek d.d.*



SLUŽBENA POTOVANJA ZAPOSLENIH POMEMBEN VIR TVEGANJA ZA ORGANIZACIJE

Vsako zrelo in odgovorno podjetje se zaveda svoje odgovornosti za zaščito in zmanjševanje tveganj vseh svojih zaposlenih in sredstev, med katere sodijo tudi tveganja na službenih potovanjih zaposlenih. V zadnjem obdobju je zaznati pomembno povečanje izrednih varnostnih dogodkov v katerih so udeleženi zaposleni organizacij, ko se nahajajo na službenih potovanjih v globalnem varnostnem okolju.

Uvod

V dobi informacijske družbe je temu primerno in zahtevnejše postalo tudi upravljanje z varnostnimi tveganji. Svet je še vedno nevaren, v nekaterih primerih bolj kot kdajkoli prej. Začetek delovanja organizacij v globalnem poslovnem okolju z elementi virtualne delovne sile lahko povzroči težave, ki jih v preteklosti ni bilo. Kako zaščititi informacije o podjetju, ko so njegovi zaposleni na terenu ali na mednarodni poti? Kako zaščititi zaposlene, ki ne delajo v prostorih podjetja in so pogosto na tisoče kilometrov od pisarne? Kako varovati vodstvene in vodilne delavce podjetja? Kako zagotoviti kontinuiteto poslovanja? Kako zaščititi zaposlene, objekte in drugo premoženje podjetja v državi, katere vlada morda podpira krajo vitalnih informacij podjetja, da bi pomagala korporacijam svojega naroda?

To so le nekatera od številnih vprašanj in izzivov, s katerimi se srečujejo strokovnjaki za korporativno varnost v svojih prizadevanjih za zaščito premoženja podjetja, katerega najpomembnejši del so njegovi zaposleni.

Osebna varnost

Potovanje z letalom velja za enega od najvarnejših načinov prevoza. Kljub temu ga mnogo ljudi doživlja s tesnobnimi občutki. Pogosto govorimo o strahu pred letenjem, redko pa o strahu pred vožnjo z avtomobilom, vlakom ali ladjo. Zakaj? Eden izmed razlogov je ta, da je verjetnost preživetja potnikov v primeru, da na desetih kilometrih odpove motor, pride do tehnične okvare, terorističnega napada ali pa zmanjka goriva, zanemarljiva. Tako vsaj misli večina.

Kako torej zagotoviti ustrezno stopnjo varnosti na poti, če verjamemo, da nanjo ne moremo vplivati? Dejstvo je, da se naše potovanje in priprava nanj, prične veliko pred vstopom na prevozno sredstvo, pa naj bo to letalo, avtomobil ali hidrogliser.

Priprava na pot

Za varno potovanje je pomembno dobro načrtovanje. Začnimo z zbiranjem informacij o cilju, ki jih lahko dobimo na javno dostopnih spletnih straneh zunanjih ministrstev ali pa od strokovnih služb v podjetju, v katerem delamo, če te obstajajo. Preverimo, ali so razmere v državi, v katero potujemo, stabilne, ali so pogosti neredi in demonstracije, kakšna je stopnja kriminala in ali se je potrebno

Podjetja, katerih zaposleni morajo pogosto potovati v tujino, so dolžna poskrbeti za varnost svojih zaposlenih. Poslanstvo korporativne varnosti je, poleg zagotavljanja varovanja premoženja podjetja, tudi poskrbeti za varnost zaposlenih na službeni poti.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

pred potjo cepiti. Če res moramo oditi na območje, kjer je stopnja nevarnosti visoka, se prej posvetujmo s pristojnimi službami, na primer z varnostno službo podjetja ali zunanjim ministrstvom. Izbirajmo preverjene hotele in prevoznike ter potovalne agencije, na cilj pa poskušajmo priti podnevi. Rezervirajmo hotelske sobe med drugim in sedmim nadstropjem – nižja so bolj vabljiva za vlome, saj želijo vlomilci čim hitreje vstopiti in izstopiti, v višja pa gasilske lestve ne sežejo. Ne bo odveč, če se naučimo nekaj osnovnih besed in stavkov v jeziku domačinov. Če jemljemo zdravila, jih vzemimo na zalogo. In ne pozabimo na zdravstveno zavarovanje ter potni list.

Na poti

Bodimo 'težka tarča', hodimo samozavestno in odločno, a ne agresivno in ne dajmo zločincem priložnosti za kaznivo dejanje. Tudi če smo se izgubili, tega ne pokažimo navzven in dobro presodimo, koga bomo vprašali za pot. Ime in priimek ter delovno mesto naj ne bodo razvidni na prtljagi, vozilu, ali drugih mestih in oznakah. Raje uporabljajmo ime podjetja, svoje ime pa navajajmo le na uradnih računih, na primer pri uporabi bančne kartice.

Če potujemo z najetim službenim avtomobilom, svoje vozilo dobro spoznajmo in opremimo. Rezervoar z gorivom naj bo vedno poln vsaj do polovice, s seboj imejmo vodo in hrano, da se nam ne bo treba ustavljati na sumljivih krajih. Med vožnjo imejmo vrata zaklenjena, okna pa zaprta. Pomembnih ali dragih stvari ne puščajmo na vidnem mestu. Za parkiranje izbirajmo dobro osvetljena, neizpostavljena in varovana parkirišča. Ne ustavljajmo se ob vozilih, v katera se ne vidi (na primer dostavni kombiji). Če se ob našem parkiranem vozilu zadržujejo sumljive osebe ali nam izvoz s parkirišča preprečuje ovira, na primer zaparkirano vozilo, se ne približujmo.

Na cilju

Če za prevoz do mesta bivanja potrebujemo taksi, se odločajmo za taksije z licenco. Če ga naročamo po telefonu, vnaprej povprašajmo po registrski številki. Pri nastanitvi si oglejmo poslopje, v katerem bivamo. Ali so na hodnikih nameščeni gasilni aparati, kje so požarni izhodi, kam vodijo, je možen neoviran prehod in izstop? Ali so prostori in vhodi video nadzorovani, je nameščen protivlomni sistem?

V času bivanja se izogibajmo nevarnih krajev, če je možno hodimo v skupini. Ne obnašajmo se kot turist in na ulici ne nosimo vpadljivega nakita. Hodimo v nasprotni smeri gibanja vozil, saj imamo tako boljši pregled in manj možnosti za ugrabitev. Pri sebi imejmo samo tisto, kar nujno potrebujemo. Denar in druge pomembne stvari imejmo tik ob telesu, če je le mogoče pod oblačili. Nekaj gotovine hranimo na lahko dostopnem mestu, ločeno od drugih vrednih stvari. Tako bomo manjše zneske lahko plačevali, ne da bi razkrili, kje nosimo preostali denar, osebne dokumente ipd.

Upoštevajmo lokalne običaje in se obnašajmo vljudno. Tudi če že imamo izkušnje z neko državo, to še ni zagotovilo, da bomo varni.



Informacijska varnost

Kraja intelektualne lastnine in občutljivih informacij ni nova, vendar pa za storilce ni bila nikoli lažja. Na voljo je vseprisoten in visoko razpoložljiv internet, vedno več je uporabe pametnih telefonov s strani potencialnih žrtev, ki s seboj prenašajo velike količine informacij o podjetju. Vdor v mobilni telefon ne pomeni samo tveganja razkritja osebnih in poslovnih podatkov, ampak je lahko tudi vstopna točka nepooblaščenega vstopa v informacijski sistem podjetja. Pogosto tak vdor ostane neopažen in brez sledi. Kraja informacij pa ni edina grožnja - nepooblaščene spremembe informacij lahko povzročijo še večje težave. Ves čas se moramo zavedati, da so elektronski podatki, vključno z govorno komunikacijo, ogroženi kjerkoli in kadarkoli. Čeprav morda ni mogoče v celoti odstraniti vseh tveganj, jih je mogoče vsaj zmanjšati na sprejemljivo raven, glede na naravo informacij.

Če je možno, se tudi na službeni poti srečujmo v prostorih našega podjetja. Bodimo previdni pri uporabi najetih konferenčnih zmogljivosti, kar zajema tako prostore kot informacijsko infrastrukturo in podporo. Imejmo v mislih, da se v hotelski sobi ni varno pogovarjati o poslovnih skrivnostih, pogodbah in drugih občutljivih temah - soba ima lahko skrite naprave za poslušanje. Zagrnimo zavese ali žaluzije, da preprečimo uporabo usmerjenih in laserskih mikrofonov, ki lahko poslušajo skozi zaprta okna. Preverimo, ali se pogovor sliši tudi zunaj sobe.

Kadar uporabljamo računalniške naprave na javnih mestih, bodimo pozorni. 'Shoulder surfing' je način, pri katerem se storilec seznani z informacijami tako, da enostavno pogleduje čez našo ramo, medtem ko delamo na računalniku. Kako ironično je, da so proizvajalci računalnikov leta in leta porabljali ogromne vsote denarja, da bi bil zaslon naše naprave viden iz čim širšega zornega kota, zdaj pa se trudimo dosežke razvijalcev obrniti v nasprotno smer: t.i. filtri za zasebnost so relativno poceni, široko dostopni in preprosto namestljivi na večino računalniških naprav, vključno s tablicami in pametnimi telefoni. Razmislimo o njihovi uporabi pred naslednjim potovanjem.

Pri uporabi interneta imejmo v mislih, da uporabljamo infrastrukturo, ki jo zagotavlja pogosto neznan ponudnik. Ne glede na vrsto povezovanja, žično ali brezžično,

obstaja tveganje nepooblaščenega prestrezanja informacij, zato pri komunikaciji uporabljajmo šifrirne metode. In ne odpirajmo in ne prenašajmo vsebin iz neznanih ali sumljivih virov.

Pri uporabi mobilnega telefona bodimo previdni. Vklopljena funkcija storitev, ki temeljijo na lokaciji (angl.: *location-based services*), uporablja GPS, Bluetooth in Wi-Fi za določanje naše lokacije, ki jo posreduje aplikacijam in spletnim stranem, te pa nam v zahvalo pošiljajo informacije o svojih lokacijah in storitvah. Pri vklopu funkcije za uporabo brezžičnega omrežja (Wi-Fi) nam naš telefon omogoča zaznavo bližnjih brezžičnih omrežij, hkrati pa hrani podatke o omrežjih, v katera se je v preteklosti že povezal. Naša brezžična naprava gre skozi postopek odkrivanja, v katerem se poskuša povezati z razpoložljivimi brezžičnimi omrežji. Pri tem lahko pasivno samo posluša omrežja, ki sama oddajajo ali pa aktivno pošilja pakete zahtevkov za iskanje v omrežju, s katerim se ta povezujejo.

Večina naprav uporablja tako pasivno kot aktivno odkrivanje pri poskusu povezave z znanimi ali prednostnimi omrežji. Zato je zelo verjetno, da naš pametni telefon oddaja imena naših najljubših omrežij, ki jih lahko vsakdo vidi. To pa je že lahko dovolj, da nekdo zbere informacije o naši lokaciji in o nas. Še več, napadalec lahko vzpostavi brezžično omrežje z istim imenom, kot ga ima tisto, s katerim se skušamo povezati, s ciljem, da se naš telefon z njim poveže in prenese podatke prek njega. Izklopimo torej obe funkciji, če ju ne uporabljamo ali se nahajamo na tveganem območju.

Sicer pa tudi to ni dovolj, če smo tarča motiviranega storilca. Osnovni princip delovanja mobilnega telefona je namreč tak, da signal potuje od mobilnega aparata do bazne postaje in naprej do centrale, ki signal sprejme in ga posreduje drugi bazni postaji, v območju katere se trenutno nahaja iskani mobilnik, ali drugemu omrežju, v katerega kliče uporabnik. Povezava med mobilnikom in bazno postajo je brezžična. V trenutku, ko vklopimo svoj mobitel, ta poišče bazno postajo, v območju katere smo. Bazna postaja to naprej sporoči centrali. Od tu naprej obstajata dve možnosti: v primeru, da nas nekdo pokliče, centrala poskrbi za to, da bazni postaji, v območju katere smo, posreduje klic, ki nam je namenjen. Druga opcija je, da kličemo mi. Ko pritisnemo tipko za klicanje, terminal sporoči bazni postaji, kdo smo, bazna postaja pa to informacijo prenese centrali. Centrala nato poskrbi za vzpostavitev zveze s tistim, ki ga kličemo. Če se med pogovorom premikamo in prehajamo iz območja ene bazne postaje v območje druge, si te med seboj podajajo naš signal in nam tako omogočajo nemoten pogovor, morebitnemu prisluškovalcu pa ustrezne informacije o naši lokaciji in gibanju.



In ne pozabimo na že tolikokrat omenjeni prenosni računalnik. Vedno ga imejmo na očeh, ne glede na to, ali se nahajamo na letališču, v restavraciji ali na konferenci. Ne puščajmo ga brez nadzora v hotelski sobi ali v avtomobilu niti v njegovem prtljažnem prostoru. Kraja ni najhujše, kar se mu lahko zgodi. Obstajajo tudi napadi z nameščanjem vohunske kode. V primeru suma, po vrnitvi v domače podjetje, pred priklopom v omrežje, predajmo prenosnik v pregled računalniškim strokovnjakom.

Zaključek

Podjetja, katerih zaposleni morajo pogosto potovati v tujino, so dolžna poskrbeti za varnost svojih zaposlenih. Poslanstvo korporativne varnosti je, poleg zagotavljanja varovanja premoženja podjetja, tudi poskrbeti za varnost zaposlenih na službeni poti. Poleg zagotavljanja osebne varnosti zaposlenih, je pomembno tudi upravljanje z informacijskimi tveganji oziroma zagotavljanje ustreznega nivoja varnosti informacij tako na lokaciji, kjer se zaposleni na službeni poti nahajajo, kot pri komunikaciji in prenosu podatkov do sedeža podjetja. Varnostna tveganja lahko zmanjšamo s svetovanjem, ozaveščanjem in izobraževanjem, pravili ravnanja in logističnimi pripravami.

Zmanjšanje osebnega tveganja in zagotovitev varnega potovanja lahko podjetje doseže z ustreznim varnostnim programom, ki uporabnikom zagotavlja informacije in analizo varnostnega stanja na ciljnih lokacijah, strokovno varnostno svetovanje, zaščito posameznikov, ki potujejo na območja z visokim tveganjem, pomoč v primeru izrednih razmer, kaznivih dejanj, terorističnih dogodkov, nestabilnosti, konfliktov in naravnih nesreč ter evakuacijsko podporo osebju v času povečane grožnje, vključno z obravnavanjem nujnih zdravstvenih primerov.

Informacijsko varnost in varovanje poslovnih skrivnosti ter osebnih podatkov na službenem potovanju, podjetje zagotavlja z uporabo varnih komunikacijskih kanalov ter z ustrezno zaščito lastnih informacijsko-komunikacijskih naprav, kot je na primer šifriranje podatkov na prenosnih napravah in z ustrezno ozaveščenimi in izobraženimi uporabniki teh naprav.

Zavedati pa se moramo, da smo za lastno varnost v prvi vrsti odgovorni sami.

Viri

- Europol (2012). *Strategije za preventivo in preživetje*.
- Group IT Securtiy, Novartis (2018). *I.T. Security When Travelling*.
- ISRM Policy Framework, Novartis (2018). *Information Security & Risk Management*.
- Woodford, C. (2018). *How cellphones work*. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Upravljanje s tveganji in korporativna varnost

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

Omogočiti obvladovanje poslovno varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Zakaj Upravljanje s tveganji in korporativna varnost?

- **Študij za poklic prihodnosti.** Študij daje multidisciplinarna teoretična in praktična znanja s področja managementa in obvladovanja najrazličnejših tveganj v podjetju.
- **Nadgradnja širokega poslovnega znanja.** Študij omogoča spoznavanje vsebin, ki so značilne za korporativno varnost: geostrateški in politični vidiki varnostnih tveganj, varnostni standardi v poslovnih procesih, upravljanje varnostnih tveganj, načrtovanje in razvoj korporativne varnosti na vseh nivojih, procesi nadzora, gospodarsko poizvedovanje in mehanizmi za obvladovanje najrazličnejših tveganj.
- **Spoznavanje globalnega poslovnega okolja.** Tekom študija se obravnava številne primere iz domačih in mednarodnih podjetij, ki jih predstavljajo vrhunski strokovnjaki na področju varnosti v regiji.
- **Mreženje in osebni pristop.** Študij poteka v manjših skupinah, ki omogočajo neposredno sodelovanje predavateljev in študentov.

Komu je študij namenjen?

- Managerjem in strokovnjakom s področja korporativne varnosti, ki si želijo razširiti svoje poslovno znanje in pridobiti širšo perspektivo za dobro razumevanje globalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja.
- Tistim, ki si želijo pridobiti znanje za vodenje oddelkov na področju korporativne varnosti v javnem in gospodarskem okolju ter mednarodnih korporacijah.
- Podjetnikom in zaposlenim v sistemih, ki delujejo na področju energetike, telekomunikacij, informatike, transporta, financ in vsem, ki se srečujejo z vprašanjem varnosti ter tveganj v organizacijah.



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

- **RAZPISANE SMERI:**
  - **Korporativni varnostni manager**
  - **Korporativni varnostni manager - podjetnik**
- **POGOJI ZA VPIS:** diploma 1. stopnje ali starega visokošolskega strokovnega študijskega programa. Možen je tudi vpis neposredno v 2. letnik. Podrobnosti o vpisnih pogojih so na voljo na spletni strani: www.gea-college.si.
- **TRAJANJE ŠTUDIJA:** študij traja 2 leti in obsega 120 kreditnih točk po ECTS.
- **PRIDOBLJENI NAZIV:** magister/magistrica korporativne varnosti.
- **IZREDNI ŠTUDIJ:** izvaja se po razporedu, ki je prilagojen zaposlenim (študentom). Predavanja potekajo med tednom v popoldanskem času in ob sobotah dopoldne.
- **PRIZNAVANJE ZNANJ IN SPRETNOSTI:** na podlagi znanj, ki jih je posameznik pridobil s formalnim ali neformalnim izobraževanjem na tečaju, delavnici ali seminarju, se lahko prizna del študijskih obveznosti.
- **DODATNE AKTIVNOSTI IN PREDNOSTI:** mednarodna izmenjava (študij ali praksa) na več kot 30 partnerskih institucijah, podpora Kariernega centra, mednarodna konferenca, Alumni klub, ekskurzije in druge študentske aktivnosti. Študij je podprt tudi s sodobnim e-portalom, ki nudi študijske vsebine 24 ur na dan.



"Velika dinamika poslovnega okolja in stanje kriznih razmer sta danes postali stalnici. Tisti, ki tega ne razumejo, ostajajo v preteklosti. Ujemite prihodnost in dovolite, da vas s pomočjo interdisciplinarnih znanj, ki temeljijo na prenosu dobrih praks iz neposrednega poslovnega okolja, opremimo, da boste sposobni obvladovati tveganja in ustvarjati nove poslovne priložnosti."

izr. prof. Denis Čaleta, predavatelj, predsednik Slovenskega združenja korporativne varnosti

Predmetnik

I. LETNIK

Skupni obvezni predmeti

- *Management korporativne varnosti*
- *Geostrateški in politični vidiki varnostnih tveganj v mednarodnem poslovnem okolju*
- *Pravni vidiki korporativne varnosti*
- *Ekonomika obvladovanja tveganj v poslovnem okolju*

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

- *Varnostni standardi v poslovnih procesih*
- *Upravljanje varnostnih tveganj*
- *Načrtovanje in razvoj korporativne varnosti*

Smer Korporativni varnostni manager – podjetnik

- *Trženje/Marketing*
- *Finance*
- *Procesi nadzorstva v korporativnem varnostnem okolju*

Izbirni predmeti (študent izbere dva):

- *Management človeških virov*
- *Okoljski vidiki korporativne varnosti*
- *Metode raziskovanja varnostnih pojavov*
- *Zavarovalništvo v procesih zagotavljanja gospodarske varnosti*
- *Gospodarsko poizvedovanje in varovanje poslovnih informacij*
- *Informacijska varnost*

- *Študijski praktikum opravlja študent v 1. in 2. letniku*
- *Magistrsko delo*

GEA College je sodoben izobraževalni center in vodnik na poti k poslovni odličnosti.

GEA College nudi uporabna znanja s poudarkom na podjetništvu in managementu. Preko vpetosti v poslovno okolje spodbuja razvijanje inovativnih idej ter širjenje znanja in zavesti o tem, da je podjetništvo gonilna sila razvoja gospodarstva.

CENTER VIŠJIH ŠOL

Višješolski programi
(2 letni študij):
- Ekonomist
- Poslovni sekretar
- Informatika
- Organizator socialne mreže
- Gostinstvo in turizem

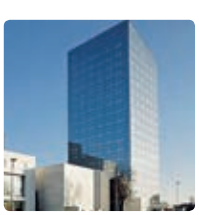
FAKULTETA ZA PODJETNIŠTVO

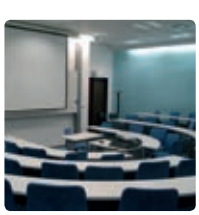
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

Magistrski programi
(2 letni študij):
- Podjetniški management
- Management korporativne varnosti

POSLOVNO-IZOBRAŽEVALNI CENTER

- Poslovni seminarji in delavnice
- Usmerjena poslovna izobraževanja
- Izobraževanja v podjetjih





GEA College - Fakulteta za podjetništvo
Dunajska cesta 156
1000 Ljubljana
T: (01) 588 13 00
F: (01) 568 82 13
E: podiplomski@gea-college.si
www.gea-college.si

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo

Avtor: Ingo Falk Pasch Wallersberg / Slovensko združenje korporativne varnosti*



IZZIVI ZASEBNEGA VAROVANJA

Riziki, s katerimi se v razvitem svetu srečuje sodobni človek, že čedalje bolj presegajo varnostne zmožnosti držav, da pred kriminalnimi posegi zaščitijo ljudi in pravne osebe na svojem območju. Ti riziki enako presegajo tudi veliko večino nedržavnih varnostnih struktur, vsekakor vse, ki storitve varovanja ponujajo na tržišču in tudi delujejo v okviru splošnih standardov in veljavne zakonodaje o opravljanju zasebnih varnostnih storitev in so tudi neposredno podrejene policijskemu nadzoru.

Distinkcijo, ki jo je v zgornjih dveh trditvah mogoče zaznati, tj., da je lahko del nedržavnih varnostnih organizacij strokovno in tehnično, za obvladovanje navedenih rizikov, bolje usposobljen in opremljen od policijskih sil, še vedno zelo težko sprejmemo. Vendar nam že sam pomislek na nujnost izjemno visoke stopnje zagotavljanja varnosti pri izvajanju posameznih kritičnih dejavnosti, še posebej na področjih izumov, tehničnih izboljšav, razvojnih projektov ali pri uporabi, transportu, hrambi ipd. pomembnega ali občutljivega gradiva ali opravljanju izjemno pomembnih ali zaupnih storitev ipd. ponazarja potrebo, da se v takšnih (izjemnih) primerih uporabijo posebna sredstva in postopki varovanja. V takšnih primerih nikakor vedno ne zadoščajo, še posebej ne visoko kvalitetno kadrovsko in tehnično opremljene ustrezne državne, tj. zlasti policijske službe, če so – razen za neposredne potrebe države - sploh na voljo. Praviloma bo potrebno upoštevati subjektivno stališče naročnika – lastnika varovanih dobrin, še posebej glede primerne usposobljenosti in opremljenosti ustreznih državnih subjektov zaradi zaupnosti in morebitnih posebnih tehničnih ali strokovnih lastnosti in zahtev varovanja.

Profesionalni razvoj varovanja za zadovoljitev visoko strokovnih in specifičnih potreb naročnika se mora na določeni stopnji tudi profesionalno uskladiti s specifičnimi zahtevami naročnikovih potreb. Največkrat pomeni to tudi zahtevo po omejitvi lastne dejavnosti, da ne pride v konkurenco z naročnikom – prav nasprotno zadostiti mora zahtevi za varovanje tajnosti naročnikovih prednosti pri opravljanju njegovih dejavnosti. Zahteva po takšni samoomejitvi lastne dejavnosti, tj. da lahko družbe za zasebno varovanje opravljajo le to dejavnost (ob njej pa izjemoma le ozek spekter drugih stranskih dejavnosti), v zakonodaji ni predvidena. Takšna omejitev pa bi bila tudi sicer v nasprotju z večkrat izraženim stališčem Evropskega sodišča. Po tem stališču ni dopustno predpisati, da družbe, ki opravljajo dejavnost varovanja, ne smejo izvajati drugih dejavnosti. Pri tem niti sodno niti v praksi ni znan primer kakršne koli obvezne omejitve dejavnosti, ki jih ob varovanju lahko opravljajo družbe za zasebno varovanje oziroma njihovi lastniki ali zastopniki* (zaradi česar lahko delujejo celo družbe, ki jim je dejavnost zasebnega varovanja tudi samo ena od stranskih dejavnosti ali pa hkrati opravljajo inkompatibilne dejavnosti).

Ne bom se spuščal v raziskovanje vzrokov tega temeljnega stališča Evropskega sodišča, očitno pa je, da gre pri njem za dosledno vztrajanje pri sicer splošno uveljavljenem kriteriju, po katerem varnostno osebje in družbe za zasebno varovanje lahko izvajajo dejavnost varovanja izključno samo v okviru pooblastil »vsakogar«. To načelno staro pravilo lebdi nepremično že več desetletij nad dejavnostjo zasebnega varovanja ne glede na to, kaj se v praksi dejansko dogaja. Nesporno je, da se zasebno varovanje, ki že več desetletij drsa po tem tankem ledu generalne omejitve svojih pooblastil, marsikje in marsikdaj že dolgo potaplja globoko pod to gladino. Tema je stara, že mnogokrat obravnavana, a nikoli razčiščena.

Ni potrebno, da na široko opisujem vlogo podjetij za zasebno varovanje na vojaškem področju, zlasti ameriških,

Glede na temeljni pomen varnosti za celotno družbo in državo bi dejavnost varovanja že zdavnaj morala imeti popolnoma drug status. Temeljni problem je v tem, da je zagotavljanje varnosti ena izmed prioritetnih nalog države.

*avtor je član Slovenskega združenja korporativne varnosti



angleških ali južnoafriških. Njihova funkcija je načeloma (teoretično) največkrat ločena od neposrednega sodelovanja v oboroženih spopadih in omejena na storitve svetovanja, vojaškega usposabljanja, upravljanja taborišč vojnih ujetnikov ali nudenja tehnične in logistične podpore v okviru določenega vojaškega delovanja. Pri tem velja opozoriti, da izvršilno osebje družbe za zasebno varovanje v takšnih primerih ni vezano na povelja vojaških predstojnikov njihovega naročnika, pač pa so njegove obveznosti in odgovornost vezane na sklenjeno pogodbo njihove družbe z naročnikom. Seveda je družbam skladno z ženevskimi konvencijami in ustreznimi protokoli prepovedano, da bi neposredno sodelovale v vojaških spopadih. Ampak, kot smo to lahko videli v času ameriške invazije na Irak, so v praksi meje tu precej zabrisane. V vojaške spopade se varnostne sile praviloma sicer lahko vključujejo le, če so vključene v redne vojaške enote in delujejo pod poveljstvom rednih vojaških sil. V kruti praksi pa jih srečujemo v vojaških spopadih - pa tudi drugih izrednih dogodkih množičnih invazij, »preseljevanja narodov«, kakršne smo na evropskih tleh doživljali zlasti v letu 2015 - tudi z neposrednim vključevanjem kadrov in kapacitet zasebnega varovanja v obrambo države, to je v sestav vseh razpoložljivih enot obrambnih sil. Takšno izjemno, ad hoc ukrepanje prinese v praksi nemalo težav in pomanjkljivosti, ki se odražajo na eni strani pri uspešnosti vodenja in delovanja teh statusno različnih in organizacijsko ad hoc zbranih enot. Kar pa je posebej zaskrbljujoče, je, da se celo resno zastavlja vprašanje o zakonitosti njihovega ukrepanja, da ne govorimo o možnostih njihovega ustreznega oskrbovanja. Slabosti slednjega so pri nas v največji meri izkusili zlasti kadri iz zasebnega varovanja.

Že dolgo je znano, da je »teorija eno, praksa pa drugo«. To močno velja tudi za področje zasebnega varovanja. Tako so tudi zgodbe o popolnoma prenizki usposobljenosti in porazno nizkem nagrajevanju kadrov v tej panogi, ki naj bi svojim naročnikom zagotavljala najvišjo vrednoto – varnost - , že dolgo znane. Premika na tem področju, ki je absolutno nujen - če se res zavedamo pomena varnosti - ne bo, dokler bo pravno, še posebej v sodni praksi, ostajala v veljavi možnost, da se s sklenitvijo pogodbe o varovanju preprosto prevali odgovornost za morebitno škodo iz varovanih rizikov, tj. zlasti kaznivih dejanj, od naročnika na izvajalca varovanja. Za nastale škodljive posledice je nujno potrebno – kljub pogodbeno zagotovljenemu varovanju - obremeniti tudi naročnika varovanja, če ni dovolj skrbno preveril resničnih možnosti varovanja izvajalca, in sicer poleg njegovih tehničnih možnosti še posebej tudi njegovo potrebno kadrovsko strukturo, njeno za izvajanje potrebnih nalog ustrezno številčnost, usposobljenost in izkušenost ter tudi njeno ustrezno nagrajevanje. Kriterij najnižje cene varovanja, ki pretežno obvladuje naše tržišče že več desetletij, je popolnoma nesprejemljiv in za razvoj dejavnosti varovanja poguben.

Glede na temeljni pomen varnosti za celotno družbo in državo bi dejavnost varovanja že zdavnaj morala imeti popolnoma drug status. Temeljni problem je v tem, da je zagotavljanje varnosti ena izmed prioritetnih nalog države. Dejstvo pa je, da država lahko zagotavlja varnost le v določenem omejenem obsegu. Zagotavljanje varnosti izven tega obsega mora biti zato, da se ohranja državni monopol nad vzpostavljanjem nadzora nad ljudmi in možnostmi zakonite uporabe sile, v neposredni ingerenci države, njegov pomen pa obenem posplošen in razpršen na eno izmed gospodarskih dejavnosti. Razvoj zasebnega varovanja je tako omejen z državne strani, ki izvrševanje te dejavnosti posebej pogojuje in

Le z vzpostavitvijo specializirane in resnično kakovostne strukture nosilcev te dejavnosti se bo lahko vzpostavilo kvalitetno varno okolje, ki ga iščejo resnični investitorji.



nadzira, po drugi strani pa jo pomensko relativizira. Ob izpolnitvi določenih pogojev jo lahko ob vseh drugih dejavnostih izvršuje neomejeno število izvajalcev. Sorazmerno nizka raven zagotavljanja varnosti s strani zasebnih gospodarskih družb je neposredna konsekvenca.

V tej protislovni situaciji, ko se z zakonodajo popolnoma relativizira pomen dejavnosti varovanja, vidim izhod le v lastni iniciativi zainteresiranih organizacij. To pomeni v njihovi prostovoljni specializaciji na opravljanje storitev varovanja, pomembnem dvigu strokovne usposobitve njihovega poklicnega kadra in lastne organiziranosti v okviru posebne asociacije (v okviru obstoječih ali samostojne). Le z vzpostavitvijo specializirane in resnično kakovostne strukture nosilcev te dejavnosti se bo lahko vzpostavilo kvalitetno varno okolje, ki ga iščejo resnični investitorji.

Še posebej bolj kompleksno in evropsko neusklajeno zgodbo pa srečujemo na področju t.i. tehničnega varovanja. V nekaterih državah EU, celo najpomembnejših (npr. v Nemčiji) ta oblika varovanja zakonsko sploh ni posebej urejena, sicer pa so ureditve zelo različne. Video nadzorni sistem, kontrola pristopa ter protivlomni in protiropni sistemi nedvomno zagotavljajo višjo stopnjo varnosti, vprašanje pa je, v kakšnem obsegu mora biti njihovo projektiranje in vgradnja oziroma namestitev licencirana dejavnost – za razliko od vključitve teh sistemov v funkcijo in nato zagotavljanja njihovega delovanja ter izvajanja event. potrebnih intervencij. Sedanja zakonska ureditev je vse preveč pavšalna, tj. dejansko in pravno nezadovoljivo definirana, kar že od nekdaj povzroča težave in nejasnosti v praksi. Poleg tega se zaradi naraščajočih rizikov, povezanih s hitrim tehnološkim, še prav posebej informacijskim razvojem, rizična področja, ki zahtevajo popolnoma nove oblike varovanja, čedalje bolj širijo. Nedvomno je potrebno, na tem zelo širokem in razvejanem področju omogočiti, skladno z dejanskimi potrebami, širši spekter možnosti in pogojev dajanja ponudb ter prav tako aktivirati odgovornost samega naročnika. Na ravni ustreznih državnih ustanov ter objektov in sistemov, posebnega pomena, pa država sama ureja pogoje zagotavljanja njihovega varovanja in s tem tudi krog možnih ponudnikov.

Kot je znano, je lansko leto (11.5.2018) stopil v veljavo zakon o informacijski varnosti (ZInfV), po katerem sta z začetkom tega leta začela z delovanjem oba centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (CSIRT) – (1) nacionalni in (2) državnih organov. O tem, kako bistvenega pomena je zagotavljanje informacijske in kibernetske varnosti ter kako daljnosežne ter izjemno velike so lahko škodljive posledice vdora v elektronska omrežja in s tem v informacijske sisteme, ni potrebno izgubljati besed. Omeniti pa velja, da se je – tako kot se to sicer žal redno dogaja – zavest o nujnosti sistematičnega in učinkovitega ukrepanja zoper te sodobne nevarnosti, največkrat pa hude kriminalne aktivnosti, katerih škodljive posledice so lahko katastrofalne, v resnici prebudila zelo pozno**. Razumljivo je, da so vdori v elektronska omrežja, njihovo okuženje in blokada na ravni komunikacijskih povezav med najpomembnejšimi nosilci storitev za delovanje države (tako pri ključnih državnih organih ter povezavah med njimi kot pri možnosti zagotavljanja ključnih storitev in produktov, potrebnih za prebivalstvo) problematika, ki se obvezno rešuje s takojšnjo vključitvijo pristojnega CSIRT-a in po njegovih navodilih. V tej zvezi pa je treba opozoriti, da med temi organizacijami, ki obvezno rešujejo ugotovljene incidente v območju njihovih elektronskih povezav z vključitvijo pristojnega nacionalnega CSIRT-a ni podjetij za zasebno varovanje (kot seveda tudi ne številnih drugih organizacij, ki niso izvajalci bistvenih storitev iz 13. čl. ZInfV). Ta podjetja lahko sicer prostovoljno rešujejo nastale blokade v njihovih elektronskih povezavah z neposredno vključitvijo nacionalnega CSIRT-a, vprašanje je samo, ali so sama strokovno dovolj močna, da v tem neposrednem razmerju učinkovito razrešujejo nastali zaplet (oziroma da vnaprej razčistijo domnevni zaplet in brez potrebe ne obremenjujejo CSIRT). Tako se v dejavnosti zasebnega varovanja, tudi na ravni elektronskih povezav, zastavlja, kot dodaten izziv, možnost reševanja nastalih težav in morebitnih incidentov z ustanovitvijo posebnega skupnega centra, specializiranega za učinkovito razreševanje teh komunikacijskih zapletov na področju te panoge.

* Izjema je npr. Belgija, kjer so podane omejitve za direktorja varnostne službe.

** Na nujnost zakonske ureditve zagotavljanja informacijske varnosti sem opozoril že pred desetletjem in pol v okviru javne razprave o takratnih spremembah ZZasV. ■

GREMZVLAKOM

ZAGREB / 9 €

OPATIJA, REKA / 9 €

PULJ / 19 €

BEOGRAD / 29 €

BUDIMPEŠTA / od 15 €

DUNAJ / od 29 €

MÜNCHEN / od 29 €

ZÜRICH / od 29 €

FRANKFURT / od 49 €

PRAGA / od 39 €



Slovenske železnice

www. slo-zeleznice.si



ELES

PRENAŠAMO ENERGIJO. OHRANJAMO RAVNOVESJE.

Energija teče skupaj z nami. Kot sistemski operater slovenskega elektroenergetskega prenosnega omrežja skrbimo za njen varen, zanesljiv in neprekinjen prenos 24 ur na dan. Smo strokovnjaki z znanjem in izkušnjami, ki soustvarjamo energetsko prihodnost Slovenije na skrbno zastavljenih temeljih: odgovornosti, zavzetosti, znanju, zanesljivosti, sodelovanju in vztrajnosti. Strateško in trajnostno načrtujemo, gradimo in vzdržujemo prenosno omrežje Republike Slovenije. Za električno energijo na dosegu vaše roke.

Več kot 2550 km
prenosnega omrežja

Več kot 550
zaposlenih

V središče delovanja smo postavili strateške inovacije, ki prinašajo nove rešitve za zagotavljanje zanesljivosti delovanja elektroenergetskega sistema.

www.eles.si