Korporativna varnost

ICS
Institut za korporativne varnostne študije

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha! | Letnik 2012, december • št. 2



Danes si brez učinkovitega varovanja informacij težko zamislimo uspešno organizacijo

ga. Nataša Pirc Musar, Informacijska pooblaščenka Republike Slovenije

4. mednarodna konferenca

Dnevi korporativne varnosti

Ljubljana, 21.-22. marec 2013

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

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

IZVIRNA MISEL

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

PRAVA IZBIRA

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

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

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

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

Integralni varnostni sistemi (celovito varovanje)

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

Varovanje oseb in premoženja

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

Kakovost in varnost

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

Krizno vodenje (krizni menedžment)

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

IZOBRAŽEVANJE

Varnostni menedžment

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





Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
dr. Denis Čaleta

Namestnik odgovornega urednika:
Andrej Kovačič

Trženje:
ICS-Ljubljana
info@ics-institut.si
Aljoša Kandžič
aljosa.kan@ics-institut.si

Oblikovanje in DTP:
Robert Mostar

Tisk:
Schwarz print d.o.o.

Datum izida
december 2012

Izvod revije je brezplačen

Naslovnica:
123RF Limited

ISSN 2232-6170

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

Prva številka revije »Korporativna varnost« je povzročila pravi mali vihar pozitivnih odzivov ciljne publike, ki je presenetil celo same snovalce ideje o potrebi nastanka tovrstne revije. Bralci so v svojih prvih komentarjih posebej izpostavljali vsebinsko aktualnost, odzivi pa so bili ugodni tudi glede oblikovne urejenosti revije. Vse to kaže na dejstvo, da je potreba po sistematičnem obdelovanju in posredovanju novih znanj s področja korporativne varnosti nujen proces, ki bo, poleg vsega, posredno pripomogel k dvigovanju varnostne kulture in zavedanja o pomenu celovitih pristopov do obvladovanja tveganj v naših organizacijskih okoljih. V tem kontekstu bi veljalo posebej izpostaviti lastnike, kot kategorijo, ki je bistvena za zagotavljanje učinkovitega delovanja njihovih organizacij, s tem pa posredno tudi celotnega uspešnega gospodarstva z visoko dodano vrednostjo in novimi delovnimi mesti. Lastniki so kategorija, ki ni mišljena samo na področju zasebnega kapitala, temveč v ta okvir sodi tudi država oz. lokalne skupnosti, kot pomembni lastniki javnih organizacij in velikega dela kritične infrastrukture, ki je nujno potrebna za normalno delovanje družbe. V okviru lastniških struktur je vse premalo zavedanja, da so lastniki tisti prvi, ki so odgovorni za učinkovito delovanje njihovih organizacij. Neustrezen nadzor nad izbranimi managersko-upravljalskimi strukturami je ob prihodu finančne in gospodarske krize v celoti razgalil to neučinkovitost nadzora lastnikov na eni strani in na drugi strani pokazal popolno nerazumevanje potrebe dojemanja nujnosti obvladovanja tveganj, ki so dnevno prisotna v dinamičnem gospodarskem okolju. To nerazumevanje vloge lastniškega nadzora nad upravljanjem njihovega premoženja lahko deloma razumemo skozi procese tranzicijskega obdobja prenosa in konsolidacije lastništva. Lastnina zaradi procesov prehitrega in v določenih primerih tudi sumljivo pridobljenega lastništva ni postala tista težko ustvarjena vrednota, za katero je potrebno usmerjati vse napore za njeno ohranjanje oziroma ustrezno rast vrednosti. Nadzorni sveti še zdaleč niso zadosten in edini mehanizem, ki bi lastnikom omogočil ustrezen nadzor nad upravljanjem njihovega premoženja v gospodarskih družbah. Skozi ponujene vsebine bodo tudi lastniki dobivali tista potrebna znanja in informacije, ki bodo skozi daljše obdobje prispevala k dvigu zavedanja o varnosti kot vrednoti potrebni za varnost njihovega premoženja. S temi vrednotami pa bodo jasno sporočali tudi upravljalcem njihovega premoženja, da je varnost delovanja organizacij, ki so jim bile zaupane v upravljanje, tisti nujen in osnoven proces, ki v končni posledici pomembno odloča tudi o uspešnosti in rasti podjetij. Korporativno-varnostni managerji in procesi korporativne varnosti so lahko učinkoviti mehanizmi, ki dopolnjujejo potreben mozaik nadzornih vzvodov za lažje in učinkovitejše obvladovanje tveganj.

Naslednje pomembno dejstvo kateremu v tokratni številki posvečamo določen del pozornosti je vsekakor namenjeno pomenu informacij, ki kot take lahko v določenem trenutku predstavljajo bistveno konkurenčno prednost. Dileme in izzivi obvladovanja tveganj povezanih s prenosom, varovanjem in uporabo ključnih informacij v dobi razmaka informacijskih in komunikacijskih sistemov je tisti segment, ki mu skozi del intervjujev in prispevkov namenjamo pomemben del medijskega prostora revije.

Glede na dejstvo, da je pričujoča številka zadnja v iztekajočem letu, izkoriščam to priložnost in vam v imenu celotne ekipe, ki v okviru Instituta za korporativne varnostne študije skrbi za izhajanje revije »Korporativna varnost«, zaželim vse dobro v prihajajočem letu 2013. Za nas tudi v letu 2013 velja geslo »**Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!**«.

Doc. dr. Denis Čaleta
Glavni urednik



INTERVJU
ga. Nataša Pirc Musar
Informacijska pooblaščenka Republike Slovenije
DANES SI BREZ UČINKOVITEGA VAROVANJA INFORMACIJ TEŽKO ZAMISLIMO USPEŠNO ORGANIZACIJO 5



INTERVJU
mag. Boris Novak, Generalni direktor Pošte Slovenije in
g. Mitja Štampfer, Direktor področja korporativne varnosti in nadzora
OBVLADOVANJE TVEGANJ SKOZI PERSPEKTIVO POŠTE SLOVENIJE 13



INTERVJU
Izredni profesor dr. Jaka Vadnjal
Dekan GEA College/Fakultete za podjetništvo
PRED VRATI JE NOV PROGRAM PODIPLOMSKEGA IZOBRAŽEVANJA S PODROČJA MANAGEMENTA KORPORATIVNE VARNOSTI 21



OBVLADOVANJE FINANČNIH TVEGANJ

Vodstvo podjetja je odgovorno za zagotovitev spremljanja tveganj, katerim je podjetje izpostavljeno pri poslovanju. Tako se danes gospodarske družbe vsakodnevno srečujejo s tveganji in jih morajo z ustreznimi ukrepi, predvsem notranjimi kontrolami, tudi čim bolj obvladovati. 37



VARNOST NA INTERNETU - KOGA BRIGA DATUM VAŠEGA ROJSTNEGA DNE

Internet je res krasno orodje za raziskovanje sveta in učenje in vsakdanje orodje za delo, vendar se brez nekaterih varnostnih ukrepov lahko hitro spremeni v grozeče okolje. Ob vsem tem pa ne smemo pozabiti, da je internet neoprijemljiv in presega državne meje v svetu, kjer so v globalnem prostoru vrednote relativne. In prav v tem je njegova lepota in tudi njegova nevarnost. 45

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

INTERVJU
ga. Nataša Pirc Musar
Informacijska pooblaščenka Republike Slovenije

DANES SI BREZ UČINKOVITEGA VAROVANJA INFORMACIJ TEŽKO ZAMISLIMO USPEŠNO ORGANIZACIJO

Živimo v kompleksnem in dinamičnem svetu, kjer je na informacijah temelječa družba prežeta z razvojem novih tehnologij.

1. Kako uspe institut informacijskega pooblaščenca spremljati tako nagle spremembe v tej dinamični informacijski družbi?

Bom lagala, če bom rekla, da lahko. Težko. Sploh zaradi tega, ker je primarni fokus našega dela vendarle inšpekcijski postopek, torej tisti nadzor, ki naj bi tudi z vidika neke preventive pomagal urediti stanje na področju varstva osebnih podatkov. Imamo tri fante, ki se vsak dan bolj poglobljeno ukvarjajo z informatiko, z razvojem modernih informacijskih tehnologij. Pri nas je seveda v ospredju vidik, kako moderne informacijske tehnologije vplivajo na zasebnost, in te vsak dan bolj vplivajo na zasebnost. Jaz se velikokrat pohecam, ko mi nekdo iz kakšnega podjetja reče, to je pa informatik rekel, da se ne da. V informatiki ni več misije nemogoče, vse se da, če se hoče. In seveda se da tudi v tisto negativno smer. Torej da se narediti tak sistem, ki očem nevidno posega v zasebnost posameznikov.

Pri informacijskem pooblaščencu se največ ukvarjamo s težavami, ki nastajajo v odnosu delavec – delodajalec, slednji z veliko žlico zajema tehnologije, velikokrat tudi takšne, ki omogočajo nadzor nad zaposlenimi. Od tega, da jim prebira elektronsko pošto, da s preprostimi programi lahko ugotavlja, po katerih internetni straneh je nekdo srfal. Da imamo danes kamere tako majhne, tudi zaradi razvoja nano tehnologij, da jih s prostim očesom ne vidiš več, skriješ jih v požarni senzor, v senzor gibanja, alarmni, to so kamere s premerom 2 mm, ki seveda danes poleg tega, da omogočajo video nadzor, lahko omogočajo tudi avdio nadzor. Ta recimo mene še posebej boli, ker je komunikacijska zasebnost po mojem mnenju tista svoboščina, tista temeljna človekova pravica, na kateri gradiš svobodo človeka in posameznika. Težko, če še enkrat ponovim odgovor od začetka, ampak in jaz in moji sodelavci smo vedno taki, da (pa naj ne zveni pavšalno) ne vržemo puške v koruzo. To pa lahko naredimo žal samo tako, da ko najdemo nekoga, ki je kršitev naredil, z vidika preventive povemo: »Takrat, ko te najdemo, bo bolelo«. In seveda

»Vem, da pravo vedno zaostaja za modernimi informacijskimi tehnologijami, tudi to je rak rana organov nadzora. Ampak ne glede na to, je potrebno narediti vse, da do hujših kršitev, pa tudi do tistih manjših, ne bo prihajalo.«

*avtor je član Slovenskega združenja korporativne varnosti

truditi se, da kljub temu, da je treba pisati tehnološko nevtralno zakonodajo, da vendarle v pravo poskušamo zajeti tudi ta rapiden in hiter razvoj modernih tehnologij. Kar pa ni lahek posel.

2. Nam lahko v kratkem opredelite, katera so tista ključna področja, ki jih obvladujete v okviru Urada Informacijskega pooblaščenca.

Mi imamo pod svojo streho dve temeljni pravici. Ta druga, ki jo morda pri vas, ker ste bolj v tehnične vode in varovanje usmerjeni, ne poznate, je dostop do informacij javnega značaja. To je del širše človekove pravice do svobode izražanja in seveda varstvo osebnih podatkov, ki je del širše pravice do zasebnosti. Znotraj teh dveh je seveda še ogromno enih podskupinic, ki jih javnost ne opazi tako na prvi pogled. Recimo na dostopu do javnih informacij je danes zelo pomembna ponovna uporaba informacij iz javnega sektorja. Tudi tukaj poskuša EU z direktivo regulirati to področje. Evropa sama se zelo zaveda ogromnega potenciala informacij, ki jih proizvaja javni sektor, in te informacije morajo biti na razpolago zasebnemu sektorju, da jih ponovno obdela, doda neko dodano vrednost in seveda obdelane informacije proda na trgu. Pri nas se velikokrat srečujemo z državnimi organi, ki vidijo samo en tak svoj mikro kotiček, makro nivoja sploh ne opazijo in jaz se največkrat zjezim v sebi, ko vidim nekoga, ki reče: »Tega pa ne bom dal ven, mi smo garali, da smo tole naredili. Kaj zdaj bomo pa kar zastonj dal tole zasebnemu sektorju?« Ja, zastonj, ampak pogledati je treba makro nivo in makro učinke. Zasebni sektor bo zaposloval, ti ljudje bodo plačevali davke v državno blagajno in žal je birokratom težko sprejeti tako logiko. Na področju zasebnosti pa seveda, kot sva že rekla, je v fokusu razvoj modernih informacijskih tehnologij. Danes imamo na trgu biometrijo, pametni video nadzor, tele medicino, da ne govorimo o državni upravi, kjer imamo e-socialo, e-zdravje, e-upravo, vse je danes E-. Potem se ukvarjamo z morda premalokrat uporabljeno pravico do vpogleda v lastne osebne podatke. Kar nekaj pritožb prihaja k Pooblaščencu, ko upravljavci nočejo pokazati posameznikom, kaj vse o njem hranijo. Ta pravica je izjemno pomembna. Moram poudariti še eno našo pomembno aktivnost - veliko dela pri nas posvečamo sodelovanju v zakonodajnih postopkih. Danes zakonodajalec tako hitro sprejema zakonodajo, da mene moja pravniška duša zelo boli. In če še razumem, da na področju financ potrebujemo neko hitrost zaradi recesije, hitrosti ne odobravam pri zakonih, ki posegajo v temeljne človekove pravice. Tu hitrost ni pametna, je nespametna, če drugače obrnem. Zadnje 3 mesece dobivam žulje na rokah od vrtenja telefona, jezik me boli od pogovorov z ustreznimi deležniki, govorim namreč o sprejemanju nove policijske zakonodaje. Včasih se res vprašam, ali Slovenija želi postati policijska država, da se policiji tak »carte blanche« daje v roke. Če se spet dotaknem tehnologije, v zadnjem zakonu o policijskem nadzoru je nek člen, ki, posplošeno pravi, da policija lahko uporabi katera koli tehnična sredstva, zato da doseže svoje, sicer zakonite, cilje. Oprostite, časi, ko smo vedeli, da ima policija zgolj kamero, fotoaparat in radar so mimo. Danes ima policija mnogo več kot samo te tri napravice in mislim, da je stvar zakonodajalca, da policijo omejuje tudi v uporabi tehnologij. Ne vem, če nas slišijo na drugi strani. Ampak veste IP je tukaj zato, da ropota, da kriči, jaz sem za to plačana in jaz bom to svojo vlogo odigrala do konca.



3. S povečevanjem individualnega zavedanja o pomenu varovanja osebnih podatkov in na drugi strani pravice do dostopa do informacij javnega značaja se verjetno pripad prijav na vaš urad močno povečuje? Nam lahko postrežete s podatki o trendih na tem področju.

Vsako leto je večji in vsako leto dobivamo nove pristojnosti. Naj omenim samo zadnjo, ki nas čaka. To je t.i. »anticookies« direktiva, direktiva o piškotkih, ki jih spletne strani, ki so fokusirane v oglaševanje, v prodajo produktov, implementirajo v naše računalnike. Slovenija tukaj zamuja z zakonodajo in je že tik pred kaznovanjem, če tega ne bo dala v zakon in ravno pred nekaj dnevi je v zakonodajni postopek prišel zakon o elektronskih komunikacijah. Ta zakon nam daje nove inšpekcijske pristojnosti na področju teh piškotkov. Danes bodo vse spletne strani, ki so fokusirane v oglaševanje, morale delati na principu »opt-in«, torej posameznik se bo moral strinjati in privoliti v to, da ti piškotek nastavijo v tvoj računalnik. Tukaj je britanski IP v pol leta po tem, ko je bila zakonodaja sprejeta, dobil 400 prijav, samo na tem majhnem področju piškotkov. Mi smo pred 3 leti dobili nove pristojnosti na področju zakona o pacientovih pravicah. Največ, okrog ena četrtine, če ne že dve tretjini prijav, dobivamo s področja odnosa delavec - delodajalec. Poseg delodajalca v pravice delavca, tega je vsak dan več. Letno izdelamo okoli 2200 pravnih mnenj, z 32 zaposlenimi naj poudarim. Trije bodo sedaj morali iti zaradi recesije, jim ne bom mogla podaljšati pogodbe za določen čas. Če vlada ne bo povedala kako in kaj, bom morala še tri, ki so zaposleni za nedoločen čas odpustiti, hkrati pa nam takoj z zakonom, ki prihaja v parlament, nalagajo nove pristojnosti. Ampak, dobro nisem tu zato, da bom tarnala, do sedaj smo delali 100%, sedaj bomo 120%, če bo treba. 600 inšpekcij naredimo na leto. Mislim, da je lanska številka 665 z 10 inšpektorji. To so številke, ki tudi nekaj povedo. 2200 pravnih mnenj, oprostite vsem na drugi strani vedno pravim - nobeno vprašanje ne bo ostalo neodgovorjeno, če boste pooblaščenca vprašali, boste odgovor dobili. Da ne govorim seveda potem tudi o inšpekcijskih postopkih po uradni dolžnosti. Vsak nadzornik mora naredit najmanj 10 »exoffo« inšpekcijskih nadzorov letno, in seveda sodelovanje v zakonodajnih postopkih. To je letno 60 do 70 zakonov in to niso lahke stvari. Medresorsko usklajevanje, prepričevanje ministrstev vzame veliko časa. Ni mi ga žal, nikoli.

4. S pravnimi normami je nemogoče v popolnosti opredeliti vse situacije v realnem življenju. Predvidevam, da je ravno pravna praksa skozi vaša mnenja tisto pomembno orodje, ki ga uporabljate pri opredelitvi nenavadnih situacij?

Moram povedati, da sem pristaš korenčka in ne palice, čeprav ima IP korenček in palico. Vedno pravim, vprašajte pooblaščenca, pridite prej, preden začnete kakšno stvar izvajati v podjetjih. Tudi če bomo videli, da je vse narobe, ne bom 10 inšpektorjev poslala v podjetje, ampak bom rekla, pridite sem, se bomo usedli, to naredite tako, tako in tako. Morda bomo prišli čez pol leta ali eno leto pogledat, če ste res naredili vse tisto, za kar smo se dogovorili. In mislim, da je tako prav. Na področju temeljnih človekovih pravic kaznovanje ne sme biti tista alfa in omega. Namreč zakaj? Zato ker se mi zdi, da je veliko bolj pomembno to, da tudi tisti na drugi strani, torej upravljavci zbirk osebnih podatkov, dojamejo, kako zelo pomembno je varovati to dobrino, ki se ji reče varstvo osebnih podatkov. In če skozi sodelovanje pooblaščenec in deležniki na drugi strani, dosežemo to, da bomo vsi dojeli, da delamo nekaj dobrega, pozitivnega, potem smo naredili ogromno. Meni se je to že pokazalo za izrazito dobro v zdravstvenem sektorju. Dolga leta smo gradili na tem, da smo vzpostavili nek odnos z zdravstvom, ki obdeluje najbolj občutljive osebne podatke o posamezniku. In ko so videli, da Pirčeva ni samo slon, ki pridrvi v trgovino s porcelanom in razbija vse vprek, ampak da je IP mesto, kjer se lahko pogovorimo o problemih. In po dveh, treh letih trdega dela, imamo mi danes z zdravstvenim sektorjem izrazito dober odnos. Veliko delamo tudi z operaterji mobilnih telekomunikacij. Tam je »Data Retention« direktiva tista, ki jo morajo mobilni operaterji oz. vsi operaterji telekomunikacij spoštovati. Tudi na tem področju je IP nadzorni organ. Zelo pomembno je tudi, da se vse več pogovarjamo z informatiki. Informatiki so tisti, ki gradijo informacijske sisteme. Če ti ne bodo razumeli, kako je treba implementirati razmerja informatike do zasebnosti, potem bodo taki produkti, ki so zasebnosti neprijazni še vedno prihajali na trg in takrat mi bitke zgubljamo.

5. V Uradu informacijskega pooblaščenca imate tudi inšpekcijske in prekrškovne pristojnosti. Nam lahko prosim osvetlite glavne pomanjkljivosti in deviantnosti, ki jih skozi te nadzore zaznavate v praksi. Lahko ocenite, koliko kazni oziroma glob letno izrečete?

Ja, vem številko, v letu 2012 sedaj, ko smo pri koncu, bo številka okrog 330.000 evrov. Ni veliko, primerljivo s kolegi v tujini je malo, mnogi usekajo za veliko večje denarje in večkrat. Velika glavnina, 70% naših postopkov se konča z opomini. Zato ker se mi zdi, da je prvič vedno treba dat možnost tistemu na drugi strani, da je opozorjen, opomnjen. Ampak naslednjič potem ni več milosti, ker zakon tudi pravi, da enkrat lahko malo pogledaš skozi prste, drugič to ne gre več. Pooblaščencu ni primarni fokus polnjenje proračuna, res ne. Usekamo pa takrat, ko res vidimo, da gre za hudo kršitev, kadar nekdo na drugi strani ne posluša. Recimo zdajle dobesedno »cepam« globe proti gospodarski družbi, ki se ukvarja z urejanjem odškodnin pri zavarovalnicah, ker osebne podatke dobiva nezakonito. Te odškodninske družbe 3 dni po tem, čudežno, ko je bil nekdo na urgenci, pošljejo poziv poškodovanemu - pridite k nam, pa bomo uredili zavarovanje. Da ne govorim, kaj se s temi zavarovanci še potem kasneje dogaja. Pred kratkim sem jim izrekla globo za 40.000 evrov, očitno se jim še vedno splača, ampak jaz jih čakam, jaz imam čas.

> Ne bomo nikoli izgubili vojne, vedno se bomo borili naprej, ampak te male bitke so tako zelo pomembne, da meni ni žal in škoda časa za vsakega izmed teh, ki pride pooblaščencu na pogovor.

6. Mednarodno sodelovanje je danes zelo izrazito na vseh področjih. Skozi katere vzvode v vašem uradu izmenjujete dobre prakse in izkušnje s sorodnimi ustanovami v tujini.

Na področju varstva osebnih podatkov je to sodelovanje res zgledno in ga je ogromno. Ne nazadnje vpetost v zakonodajo in principi delovanja EU terjajo takšno sodelovanje. Na področju varstva osebnih podatkov obstaja posebna *skupina, ki se ji reče »Delovna skupina 29«. To je neke vrste svetovalno telo v Evropski komisiji na področju posegov v varstvo osebnih podatkov. Delovna skupina daje mnenja na recimo afero »Swift«, na PNR* sporazum, to je »passanger name record«, v okviru katerega si Evropa in Amerika izmenjujeta podatke o letalskih potnikih zaradi pregona terorizma. Ukvarjamo se z računalništvom v oblaku, pred kratkim smo izdali smernice na to temo. Koordinirana akcija je potekala v primeru Facebooka preko irskega IP. Vsi pooblaščenci v Evropi smo obveščeni o tem, kaj se na Irskem dogaja. Vsak DPA (data protection authority), ki vodi nek postopek proti nekemu globalnemu »playerju« na trgu, vse skozi obvešča ostale kolege po Evropi, da mi vemo tudi v lastnih državah povedati, kaj se je na sedežu upravljavca, v tem primeru Facebook Dublin, zgodilo in kako to vpliva na slovenski trg. Potem na področju policijskega sodelovanja, sama sem podpredsednica nadzornega odbora Europola, kjer skupaj s še 26 kolegi, torej 27 članov ima ta skupina, nadziramo, kako Europol uporablja baze podatkov nacionalnih policijskih baz. Schengenski informacijski sistem je skupno nadziran, carinski informacijski sistem je skupno nadziran v kompletu 27-terice, Eurodac, to je vizni sistem, ki ga uporabljajo ambasade po celem svetu EU, je pod centralnim nadzorom vseh 27 držav članic. Skratka tukaj je tega sodelovanja ogromno, pa tudi na neformalni ravni. Mi imamo bazo, izmenjavo prek forumov, kadarkoli se zgodi kakšen dogodek, ki ga nek nacionalni IP ne zna razrešit, ali pa se mu zgodi prvič, se samo pošlje vsem 27 – hej, a ti imaš kakšen tak primer, povej kaj si naredil. Zelo hitro dobimo odgovore nazaj. In to je super in prav, več glav več ve, to je dejstvo in na ta način se stvari lahko bolj koncizno, pravno in hitreje rešijo.

7. Kakšno mesto ima v tem okviru EU in ali se nam v kratkem obetajo kakšne pomembne spremembe na področju evropskih direktiv na področju, ki ga v uradu obvladujete?

Ja, nastaja nova uredba, torej direktiva bo prerasla v uredbo in naj bralcem razložim to pomembno razliko med direktivo in uredbo. Direktiva je akt, ki je posredno uporabljiv v državah članicah. Torej določila direktive je treba implementirati v nacionalno zakonodajo. Uredba pa je neposredno uporabljiv pravni akt, ki velja enotno za vse države članice. In na področju varstva osebnih podatkov se je Evropa odločila, da je čas, da iz direktive preidemo na uredbo, ko bo potrebno določene segmente varstva osebnih podatkov centralno regulirat za vseh 27 držav članic oz. 28. Takrat, ko bo uredba nastala, bo Hrvaška že članica EU. Kar precej sprememb v tej uredbi čaka upravljavce zbirk osebnih podatkov. Kar se tiče data security-ja, torej zavarovanje zbirk osebnih podatkov, prihaja ena zelo pomembna novost, to je t.i. »Data bridge Notification«. Kadarkoli se bo zgodil vdor v baze osebnih podatkov, bo o tem potrebno obvestiti vse posameznike, katerih podatki so bili v teh bazah, in seveda IP. To je že en element, ki bo upravljavce prisilil, da bodo na te vdore v informacijske sisteme, na pomanjkljivosti v zavarovanju, bistveno bolj pozorni. To je kar en tak močan argument za to, da bo treba zavarovanje ojačat. Kar je dobro.

Kadarkoli se bo zgodil vdor v baze osebnih podatkov, bo o tem potrebno obvestiti vse posameznike, katerih podatki so bili v teh bazah, in seveda IP.

8. Urad Informacijske pooblaščenke je med drugim tudi korporativni član Slovenskega združenja korporativne varnosti. Verjamem, da so te oblike sodelovanja za vas pomembne saj v različnih družbenih okoljih verjetno bistveno pripomorejo k dvigovanju zavedanja na področju varovanja osebnih podatkov in dostopu do informacij javnega značaja. Bi lahko tako sodelovanje opredelila kot primer dobre prakse, ki bo v bodoče postal standard tudi za druge državne organe pri prenosu idej v različna družbena okolja?

Absolutno in brez zadržkov rečem da. Moje mnenje je, da mora državna uprava, širši javni sektor, sodelovati z zasebnim, biti tudi njegov servis v pravem pomenu besede. Ne nazadnje javna uprava diktira tempo zasebnemu sektorju na mnogih področjih in tu brez tega sodelovanja lahko delamo tudi neumnosti in mi jih prevečkrat delamo v javnem sektorju, kar ni dobro. Politika si zamisli nek zakon, ne vpraša tistih, ki jih bo zakon prizadel na drugi strani, popolnoma nič. Prihaja do konfliktov, do tenzij, naknadno se nato ugotovi se da zakonodaja ni dobra. Na mojem področju sem jaz absolutno za sodelovanje z zasebnim sektorjem. Kot sem že omenila, če ne bomo igrali z roko v roki, kaj meni pomaga, če vsake toliko časa udarim s palico tistega, ki ga najdem, vseh itak ne najdem. Ampak, če bomo vsi skupaj dojeli, da je to dobro in pametno, kaj si želim lepšega, to je ideal. Morda na tem mestu lahko omenim, kje na našem področju vidim eno ogromno polje možnosti za sodelovanja. To je »privacy by design«, t.i. vgrajena zasebnost. Tu IP brez sodelovanja tistih na drugi strani ne more nič kaj dosti. Zato vedno pravim, ko začnete graditi informacijski sistem, pridite prej k nam, vprašajte, kako naj bo zgrajen sistem, da bo zasebnosti prijazen, na kaj vse moraš paziti, da bo zavarovanje zbirk podatkov ustrezno, da pooblaščenec kasneje ne bo pridivjal in pokazal palico in ne korenčka. Samo en primer, kartica Urbana. Super zadeva, saj tehnologije gredo tudi na področju transporta zelo naprej. Podjetje izdela kompletni sistem za LPP in glej ga zlomka, kmalu po implementaciji sistema dobimo prvo prijavo, ker je nekdo izvedel, da v sistemu pri imenskih karticah ostajajo podatki o tistem, ki je potoval, kje je potoval. Torej poseg v lokacijsko zasebnost, ki je danes poleg informacijske in komunikacijske, tista tretja veja zasebnosti, ki je vse bolj na udaru. In res, gremo mi v inšpekcijo na LPP in ugotovimo, da gre vsakič, ko se je nekdo z imensko kartico registriral na avtobus, ta podatek v zbirni center in točno piše - Nataša Pirc je bila ob 8ih zjutraj na avtobusu št. 14 in se je peljala tja in tja. In ko vprašam LPP, zakaj pa vi potrebujete ta podatek? LPP reče, ja gospa IP, saj mi moramo planirat avtobuse glede na gostoto

prometa. Mi moramo vedeti, na katero linijo moramo dati več avtobusov, kdaj je problem, da pošljemo novega itn. Potem jih gledam in vprašam: vi zato rabite imena in priimke, ali vam je dovolj statistični podatek. Uf, saj bi bilo res dovolj, da samo vidimo, koliko ljudi se je peljalo na tej in tej progi in bomo znali svojo logistiko planirati. Vidite, super. Spremenite sistem tako, da v center ne bo šel podatek Nataša Pirc, ampak xy se je peljal takrat in takrat. 150.000 evrov jih je stalo, da so sistem popravili, ker niso prišli prej k nam. »Privacy by design« lahko takšne, ne prav poceni napake, prepreči.

9. Kako gledate na napore Slovenskega združenja za korporativno varnost, da v slovenskem okolju dvigne splošno zavedanje o potrebi celovitih pristopov do obvladovanja tveganj. Lahko v tem okviru najdete tudi povezavo z učinkovitejšim zavedanjem o varovanju osebnih podatkov?

Seveda. Treba se je zavedati, da je varstvo osebnih podatkov en tak širok pojem. Zato je tudi potrebno vedeti in poznati razliko med »data protection« in »data security«, torej varstvo osebnih podatkov in zavarovanje zbirk osebnih podatkov. Ravno ta segment, s katerim se vi ukvarjate, je izjemno pomemben za celotno varstvo osebnih podatkov. Če mi zbirk dobro ne zavarujemo, ne dodeljujemo dostopnih pravic redkim, bo pravica do varstva osebnih podatkov prevel na udaru. Se zgodi, da v nekaterih podjetjih kar vsi dobijo dostopne pravice do baz podatkov. Ja, zakaj za božjo voljo? Odloči se vendar, kdo je tisti, ki rabi dostop in do katerih osebnih podatkov rabi dostopati. Nivojska dostopnost, revizijska sled, to so vse stvari, ki se jih danes v informatiki preprosto da izdelati, če seveda ti že v naprej na to misliš. In Inštitut za korporativne varnostne študije, ki ga vi zastopate, lahko samo pohvalim. Ravno vi poskušate gojiti to kulturo zavedanja in tukaj ste nam v veliko pomoč pri širjenju zavedanja o pomeni te človekove pravice. Sama neizmerno uživam, ko pridem predavat v vaše sredine. Zakaj? Zato, ker se od strokovnjakov na drugi strani ogromno naučim. Ne dajem samo jaz nekomu svoje znanje, jaz ga od vas dobim ogromno tudi nazaj. In to je tisto, kar je dodana vrednost, WIN-WIN pozicija za obe strani. Več tega bi rabili, če sem čisto iskrena.



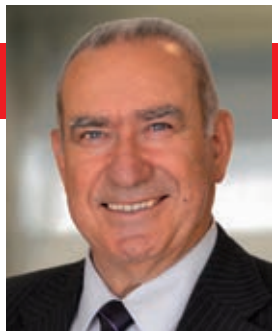
10. Kot informacijska pooblaščenka ste zelo javno izpostavljeni. Na tem področju s pridom izkoriščate svoje bogate izkušnje dela z mediji. Se vam zdi, da so znanja učinkovita komuniciranja z javnostjo standard, ki bi ga moral obvladati vsak manager, tudi v okolju javnega sektorja?

Da. Res pa je, da ni vsak za vse. Zato mora tisti manager, ki se zaveda, da teh komunikacijskih sposobnosti nima, imeti ob sebi ljudi, ki to znajo in zmorejo, vsaj enega. Morda še en nasvet, nikoli tudi ni dobro, da se šef vedno oglaša. Včasih imam že kar težavo, ker vem, da me je ogromno po medijih, ampak k sreči imam še tri, ki mi pri tem pomagajo, to so vsi moji namestniki. Treba pa se je zavedati, da brez komunikacije ne boš znal zastopati svojega podjetja. Saj ne gre samo za komunikacijo navzven, gre tudi za komunikacijo navznoter, na katero managerji dostikrat pozabljajo. Interno komuniciranje je prvo v vrsti, še pomembnejše in če ti nimaš komunikacijskih sposobnosti, če si introvertiran, če se ti ljudi bojiš, tak manager ne bo dober manager. Je lahko vrhunski strokovnjak, je lahko zelo dober inženir, ampak na managerskih pozicijah je treba delati za ljudi, v imenu ljudi in z ljudmi. In tukaj brez komunikacije preprosto ne gre.

11. Kako se vam ob tako napornem urniku funkcije, ki jo opravljate in seveda družine uspe sprostiti in nabrati novih energij. Je res, da ste članica državne reprezentance v bowlingu?

Drži, sem še vedno. Bowling je en tak šport, s katerim se lahko ukvarjamo tudi tisti malce starejši. Je tak šport, ki ga lahko gojiš od ranih let do pozne starosti. Marsikatera tekmovalka je še starejša od mene in me »nabriše kot smrkljo«. Kar je fajn, je treba trenirat. Bowling je en tak filter zame. Če si ti popolnoma posvečen svojemu poslu, in jaz sem popolnoma predana tema dvema človekovima pravicama in poslu, ki ga opravljam, je treba imeti v življenju tudi nekaj, kar krepi še kaj drugega, kot samo znanje. Popolna predanost ne pomeni, da jaz 24 ur na dan počnem samo to. Da bom 8, 10 ali 12 ali kdaj tudi 14 ur v službi to delala dobro in z vso energijo, v svojem prostem času rabim nekaj, kar napolni moje akumulatorje. V službi se mi praznijo, na bowlingu jih polnim. Pa doma seveda. Če doma ne bi bilo posluha za to, bi težko zdržala ves ta tempo. Moja fanta to razumeta in me podpirata, me spremljata kdaj tudi na službenih poteh. ■

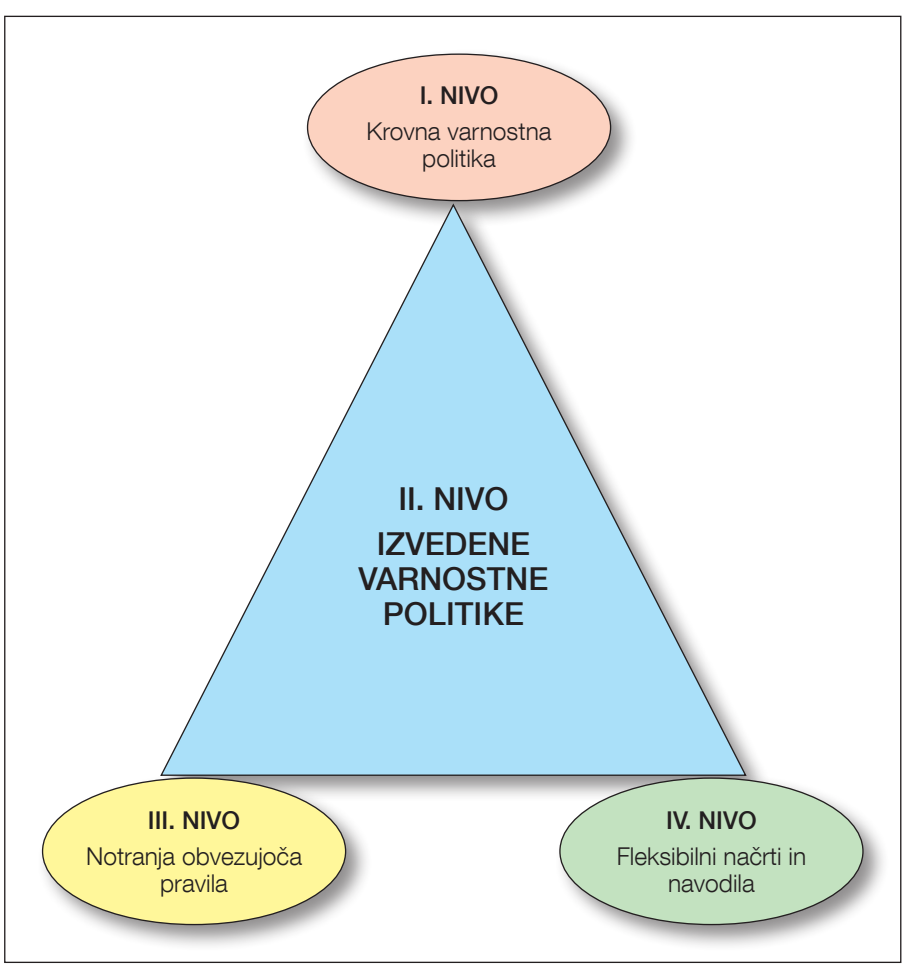
Avtor: doc. dr. Milan Vršec / Inštitut za korporativne varnostne študije*



VARNOSTNA POLITIKA KOT KROVNI DOKUMENT UPRAVLJANJA KORPORATIVNE VARNOSTI

Pri vsaki zadevi je treba nekje začeti. Pri upravljanju korporativne varnosti je to krovna varnostna politika, ki je prikazana v tem sestavku in je logično nadaljevanje mojega članka v prvi številki te revije, v kateri sem opredelil vlogo korporativne varnosti v sistemu in procesih korporativnega upravljanja.

Iz naših projektov vzpostavljanja integralnih varnostnih sistemov v industriji in gospodarstvu ter v nekaterih državnih institucijah je razvidno, da še nismo zasledili, da bi kdo – v pravem pomenu besede - imel izdelano krovno varnostno politiko. Ima pa kar nekaj družb izdelane krovne informacijske varnostne politike, politike varnosti in zdravja pri delu, okoljevarstvene politike in še kakšne, ki izhajajo iz zahtev standardov. Vendar to niso krovne temveč izvedene varnostne politike, ki morajo imeti (poleg standardov) podlago tudi v nekem obvezujočem krovnem dokumentu. Zato je osnovni namen tega sestavka, da poslovodstvom, varnostnemu managementu, varnostnim strokovnjakom in svetovalcem ter splošni javnosti nakažem idejo o metodiki in vsebini izdelave, sprejemanja ter implementiranja tako pomembnega krovnega dokumenta kot je varnostna politika. Koncept krovne varnostne politike kot sredstvo upravljanja korporativne varnosti na strateškem, srednjem in operativnem nivoju je prikazan na naslednji sliki.



*avtor je član Slovenskega združenja korporativne varnosti

Metodika izdelave krovne varnostne politike

Izhajajoč iz dobre prakse izvirnega izdelovanja varnostnih politik v proučevanih gospodarskih in drugih družbah smo oblikovali naslednjo metodiko izdelave krovne varnostne politike:
Preambula *(pravne podlage za izdajo dokumenta KROVNA VARNOSTNA POLITIKA)*

1. Izhodišča za pripravo krovne varnostne politike
   - Nacionalna varnostna politika
   - Veljavna zakonodaja
   - Analiza ranljivosti
   - Analiza ogroženosti
   - Analiza tveganj
   - Poslovna uspešnost
   - Razvojna strategija
   - Družbena odgovornost (vpetost v lokalno in širše okolje)
   - Organizacijska in varnostna kultura zaposlenih ter poslovna etika managementa
2. Poslanstvo in vizija korporativne varnosti
3. Varnostna strategija in strateški varnostni cilji
4. Koncept varovanja - kaj, koliko in kako varujemo sami in koliko, kako in kaj bomo ponudili zunanjim izbranim izvajalcem varovanja
5. Varnostna arhitektura - vzpostavitev integralnega varnostnega sistema
6. Varnostni management
7. Veriga odgovornosti za varnost
8. Upravljanje posameznih področij varnosti na podlagi izvedenih politik
9. Upravljanje varnostnih tveganj
10. Vpetost varovanja in zaščite v sistem vodenja kakovosti po ISO 9001:2008
11. Uvajanje varnostnih standardov
12. Zagotavljanje neprekinjenega delovanja varnostnega sistema
13. Zagotavljanje varovanja v kriznih razmerah
14. Varnostno usposabljanje zaposlenih
15. Varnostna kultura zaposlenih
16. Nadzor nad upravljanjem varnosti
17. Financiranje varnostnega sistema
18. Sinergija med varnostnim sistemom in zavarovalnim portfeljem.

Prvi (strateški) nivo upravljanja korporativne varnosti je izdelava, razprava, sprejem (izdaja) in skrb za implementacijo krovne varnostne politike v poslovne procese, notranjo integriteto, projekte, logistiko, outsourcing odnose s poslovnimi partnerji in družbeno odgovornost. Gre torej za implementacijo krovne varnostne politike na drugi, tretji in četrti nivo upravljanja. To je strateška naloga lastnikov, poslovodstva in nadzornikov.



Vsa notranja pravna podlaga, ki nima stopnje zaupnosti mora biti objavljena v uradnem glasilu gospodarske družbe ali katerekoli druge organizacije, da se z njo seznanijo zaposleni.

Potrebna bi bila kratka razlaga vseh zgoraj navedenih elementov, vendar to na tem mestu (zaradi omejitve prostora) ni možno. Bo pa to možno v naslednjih številkah te revije, kjer bom podrobneje predstavil posamezne izvedene varnostne politike ter še nekatere druge sestavine krovne varnostne politike.

Implementacija krovne varnostne politike

Krovno varnostno politiko pripravi varnostni management, sprejme in izda pa poslovodstvo. Z njo je treba seznaniti tudi lastnike in nadzornike. **Prvi (strateški) nivo** upravljanja korporativne varnosti je torej izdelava, razprava, sprejem (izdaja) in skrb za implementacijo krovne varnostne politike v poslovne procese, notranjo integriteto, projekte, logistiko, outsourcing odnose s poslovnimi partnerji in družbeno odgovornost. Gre torej za implementacijo krovne varnostne politike na drugi, tretji in četrti nivo upravljanja. To je strateška naloga lastnikov, poslovodstva in nadzornikov.

Vendar je poslovodstvo tisti subjekt, ki je prvi odgovoren za korporativno upravljanje, torej tudi za upravljanje korporativne varnosti.

Na drugem (srednjem) nivoju je treba poskrbeti, da bodo na podlagi krovne varnostne politike izdelane vsaj ključne izvedene varnostne politike, ki so:

- politika varovanja informacij in elektronskih komunikacij,
- politika fizičnega in tehničnega varovanja,
- politika varnosti in zdravja pri delu,
- politika varstva pred požari,
- okoljevarstvena politika,
- politika varstva osebnih podatkov,
- politika varovanja tajnih podatkov,
- politika varovanja poslovnih skrivnosti,
- politika varovanja arhivskega gradiva in arhivov,
- politika varovanja konkurenčnih prednosti, blagovnih znamk in ugleda,
- politika varstva pred naravnimi in drugimi nesrečami ter organizacije civilne zaščite.



Izvedene varnostne politike izdelajo vodje posameznih področij varnosti. Pri izdelavi tistih izvedenih varnostnih politik, ki vključujejo tudi varnostne in druge standarde se upoštevajo zahteve teh standardov (ISO 14001, EMAS, OHSAS 18001, ISO/IEC 27000, SIST BS 5979, BS 25999, SA 8000 in drugi). Izvedene varnostne politike so sestavni del krovne varnostne politike zato imajo status prilog h krovni politiki.

Na tretjem in četrtem nivoju gre za **operativni del** upravljanja korporativne varnosti, kjer je najprej treba izdelati notranjo pravno podlago – pravilnike, poslovnike, organizacijske predpise, navodila idr., kot obvezujoče dokumente za vse zaposlene. Vsa notranja pravna podlaga, ki nima stopnje zaupnosti mora biti objavljena v uradnem glasilu gospodarske družbe ali katerekoli druge organizacije, da se z njo seznanijo zaposleni. Šele z notranjo pravno podlago in drugimi dokumenti (analizami, ocenami, študijami, raziskavami, inšpekcijskimi ugotovitvami in odločbami) je možno izdelati kakovostne in uporabne posamezne načrte, navodila in druge operativne dokumente upravljanja korporativne varnosti na operativni ravni. Dokumenti na operativni ravni so fleksibilne narave, (se tekoče dograjujejo), ker se morajo prilagajati oceni ranljivosti, ogroženosti in varnostnim tveganjem ter spreminjajoči se zakonodaji.

Za razmišljanje

Poslovno in finančno zdravje katerekoli organizacije izhaja tudi iz tega, da v poslovnih procesih ne prihaja do škod in izgub. Tu nastopa krovna varnostna politika na vseh nivojih implementiranja. Preprečevanje škod in izgub (Loss Prevention) je potemtakem glavni moto krovne varnostne politike, ki bi moral prodreti v filozofijo korporativnega upravljanja. ■

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

INTERVJU
mag. Boris Novak, Generalni direktor Pošte Slovenije in
g. Mitja Štampfer, Direktor področja korporativne varnosti in nadzora

OBVLADOVANJE TVEGANJ SKOZI PERSPEKTIVO POŠTE SLOVENIJE

Učinkovito vodenje tako kompleksne organizacije je možno samo s stalnim uravnavanjem razmerja med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov.

1. Mag. Boris Novak vodite izredno kompleksno in razvejano organizacijo, ki je že zaradi svojih osnovnih procesov zelo izpostavljena celemu nizu tveganj. Kako se s stališča strateškega managerja spopadate z uravnoteženjem razmerja med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov Pošte Slovenije.

Novak: Proces upravljanja tveganj je ena izmed pomembnih sestavin korporativnega upravljanja, ki ji na Pošti Slovenije (PS) namenjamo veliko pozornosti. Razmerje med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov tako v PS zagotavljamo s sistematičnim pristopom, z jasno definiranim procesom, odgovornostmi in predpisano metodologijo upravljanja tveganj. Zato smo že v letu 2009 prenovili obstoječ sistem upravljanja s tveganji in za stalno spremljanje in obvladovanje tveganj poslovnega okolja vzpostavili celovit sistem korporativnega upravljanja s tveganji, ki ga nenehno preverjamo in dopolnjujemo. Le ta temelji na sprejetem strateškem razvojnem programu.

> Ta pa mora biti ustrezno usklajen oz. integriran v celoten proces korporativnega upravljanja tveganj

Proces upravljanja tveganj pa je vzpostavljen strukturirano, usklajeno in teče neprekinjeno po celi organizaciji. Pomemben je sistematični pristop na nivoju procesov s ciljem pravočasnega prepoznavanja, ovrednotenja in ustreznega obvladovanja tveganj, z namenom odpraviti ali zmanjšati negativne učinke tveganj na poslovanje družbe, oziroma optimalno izkoristiti prepoznane priložnosti.

2. Večina vaših kolegov, ki vodijo podobno velike sisteme prihaja največkrat iz poslovnih okolij. Vi pa imate za razliko od njih v vaši bogati karieri tudi izkušnje pri izvajanju in vodenju procesov zagotavljanja korporativne varnosti. S tega stališča vam je verjetno lažje razumeti pomembnost procesov in vloge korporativne varnosti kot vašega orodja za zagotavljanje sistemskega pristopa do obvladovanja varnostnih in drugih tveganj?

Novak: Seveda je za uspešno in učinkovito vodenje tako kompleksne organizacije izredno pomembno poznavanje celovitih in sistematičnih pristopov obvladovanja tveganj, ter iz tega izhajajočih ukrepov za obvladovanje. V ta okvir sodijo varnostna in seveda tudi druga tveganja. Procesi za zagotavljanje korporativne varnosti tako predstavljajo le enega izmed obrambnih stebrov oz. načinov obvladovanja tveganj v podjetju. Ta pa mora biti ustrezno usklajen oz. integriran v celoten proces korporativnega upravljanja tveganj in s tem vključen v odvijanje procesov na Pošti Slovenije. Tudi pri zagotavljanju korporativne varnosti je zelo pomembna celovita obravnava varnostno relevantnih pojavov, ki se izvajajo z namenom učinkovitega zmanjševanja varnostnih tveganj, katera se pojavljajo v celotnem spektru vseh tveganj PS.

*avtor je član Slovenskega združenja korporativne varnosti



3. Kakšno mesto in vlogo ima v hierarhiji strateških dokumentov v Pošti Slovenije varnostna politika organizacije. Ali tak dokument predstavlja strateški pogled in usmeritve za postavitev in delovanje sistema korporativne varnosti v Pošti Slovenije?

Novak: Varnostna politika PS predstavlja temeljni dokument predvsem za sodelavce, ki v PS skrbijo za korporativno varnost in nadzor. V največji možni meri poskušamo varnostno politiko integrirati tudi na druge nivoje poslovanja. Če gledam primerjalno, bi lahko rekel, da predstavlja varnostna politika za področje, ki se v PS ukvarja s korporativno varnostjo in nadzorom približno enako kot predstavlja poslovni načrt ali Strategija razvoja na ravni družbe. Ker sem do nedavnega sam vodil Področje korporativne varnosti in nadzora lahko povem, da smo na področju varnostne politike naredili izredno veliko predvsem v zadnjih nekaj letih, ko se nam je zaradi razmer v okolju bistveno povečalo tudi varnostno tveganje. Žal pa ugotavljamo, da so nas nekateri dogodki kljub temu vseeno prehiteli oz. jih ni bilo mogoče preprečiti.

4. V Slovenskem okolju ste ena redkih organizacij, ki ima že v svoji organizacijski strukturi opredeljeno Področje za korporativno varnost in nadzor ter postavljenega direktorja korporativne varnosti in nadzora. Kako to, da ste za razliko od ostalih organizacij v Sloveniji spoznali, da vodenje korporativne varnosti in upravljanje tveganj ni možno iz 5 ali 6 organizacijskega nivoja?

Novak: Odkrito lahko povem, da je bilo do leta 2006 tudi v PS to področje relativno odmaknjeno od ključnih procesov odločanja v podjetju. Bilo je kadrovsko podhranjeno, prav tako so se za ta namen namenjala relativno majhna finančna sredstva. Delno obstaja za to tudi opravičilo, saj je bila v letih pred tem varnostna situacija bistveno bolj ugodna kot je danes. Od leta 2007 pa beležimo na PS izredno poslabšanje varnostne situacije, ki je ni bilo možno predvideti. Najprej se je odrazila na področju varnosti prevozov vrednostnih poštnih pošiljk, nato pa še na varnosti poštnih poslovalnic. Takrat smo ocenili, da ustrezne varnosti, v prvi vrsti za zaposlene in šele nato premoženja, ni možno dvigniti na primeren nivo, brez temeljite reorganizacije tega področja. Za dosego tega je bilo potrebno na trgu dela poiskati dodaten strokovni kader ter prepričati takratno vodstvo, da predstavljajo sredstva namenjena za varnost investicijo in ne strošek. To konkretno pomeni, da predstavljajo sredstva namenjena varnosti, investicijo v ljudi za ljudi, za ugled podjetja in nenazadnje za uspešnost celotnega poslovnega procesa. Takšen pogled na varnost imam tudi sedaj, ko sem sam v vlogi generalnega direktorja.

6. Trenutno opravljate vlogo direktorja Področja korporativne varnosti in nadzora. Nam lahko bolj podrobno opredelite kakšne so strateške naloge vašega področja?

Štampfer: Področje korporativne varnosti in nadzora pripravlja in nadzoruje izvajanje varnostne politike, katere del je tudi informacijska varnost, ter ostalih internih predpisov v najširšem pomenu (inšpektorji notranje kontrole). Kot tako celovito obravnava vse relevantne varnostne pojave in poslovanje Pošte Slovenije kot gospodarskega subjekta.

Področje korporativne varnosti in nadzora sestavljajo:

- **Oddelek korporativne varnosti,** ki na podlagi celovite obravnave vseh relevantnih varnostnih pojavov načrtuje, vodi in usmerja storitve zasebnega varovanja ter v posameznih primerih tudi poslovne procese PS v smeri zagotavljanja najvišje stopnje varnosti za zaposlene in za premoženje PS glede na dane možnosti in razmere. Poleg navedenega preventivnega delovanja, ki predstavlja osrednji del funkcij, se zaposleni v tej službi zaradi izkušenj pri odkrivanju storilcev kaznivih dejanj vključujejo tudi v postopke odkrivanja storilcev (tako med zaposlenimi kot drugimi), pri čemer tesno sodelujejo z organi odkrivanja.
- **Oddelek notranje kontrole,** ki s stalno kontrolo in ukrepi, odrejenimi za odpravo nepravilnosti in pomanjkljivosti, sodeluje pri zagotavljanju nemotenega, pravilnega in kakovostnega delovanja poštnega prometa v vseh fazah tehnološkega procesa v notranjem in mednarodnem prometu.
- **Oddelek informacijske varnosti**, ki skrbi za varovanje podatkov, informacij in informacijskih virov. Izvaja ocene IT-tveganj, sodeluje pri izdelavi načrtov neprekinjenega poslovanja in skrbi za njihovo ažurno dopolnjevanje ter nadzoruje njiho-



vo izvajanje, nadzira dodeljevanje dostopov do posameznih informacijskih virov. Razvija in vzdržuje politike, navodila, postopke, priročnike s področja varovanja informacij ter skrbi za program izobraževanja in vzpostavitev ustreznega nivoja varnostne kulture vseh zaposlenih. V sodelovanju s Področjem za informatiko vpeljuje varnostne mehanizme, ki zagotavljajo varno delovanje informacijskega sistema.

- **Pooblaščenec za preprečevanje pranja denarja,** ki skrbi za delovanje in razvoj sistema odkrivanja in preprečevanja pranja denarja in financiranja terorizma; skrbi za pravilno in pravočasno sporočanje podatkov Uradu za preprečevanje pranja denarja; sodeluje pri pripravi programov strokovnega usposabljanja in izobraževanja zaposlenih na področju preprečevanja in odkrivanja pranja denarja in financiranja terorizma itd.

7. Pošta je bila v preteklosti večkrat tarča neposrednih roparskih napadov na njene poslovalnice in zaposlene. Kako ste se lotili ocenjevanja danih grožen in predvsem kakšne ukrepe ste izvedli za zaščito zaposlenih in vaših strank?

Štampfer: Pošta ima izdelan varnostni načrt katerega integralni del je tudi Ocena stopnje tveganja. V tej oceni so opredeljene različne vrste ogroženosti, med katerimi je zelo pomembna ogroženost od kriminalnih ravnanj in dejavniki tveganja za nastanek kriminalnih ravnanj. Najbolj tipično kaznivo dejanje, ki ga storilci kaznivih dejanj izvajajo na škodo Pošte so ropi in roparske tatvine. Glede na objekt napada rope delimo na rope poštnih poslovalnic, rope poštnih vozil in rope pismonoš. Za vsako navedeno kategorijo ropov imamo izdelano oceno stopnje tveganja, kateri prilagajamo način varovanja in ključne ukrepe za obvladovanje tveganj. Pri varovanju poštnih poslovalnic so ključni ukrepi, ki smo jih izvedli v zadnjem obdobju. Ti ukrepi so nadgradnja obstoječega mehanskega varovanja, ki vključuje tudi varnostno zasteklitev odporno na strel, posodabljanje sistemov tehničnega inprotiropnega varovanja, uvajanje sistema dimnih denarnih pasti, sistema video nadzora in postavitev lastnega nadzornega centra. Pri varovanju prevozov so ključni ukrepi uvedba varnostnih kovčkov, uvedba sledenja poštnih vozil z možnostjo posredovanja alarma oz klica v sili, reorganizacija in optimizacija poslovanja z gotovino in drugi.

8. Varnostna kultura in visoko varnostno zavedanje zaposlenih ločuje uspešne organizacije od manj uspešnih. Kako se v tem hitrem dinamičnem okolju, kjer je mobilnost kadrovskega potenciala zelo visoka zagotavljate osnovne varnostne vrednote in standarde varnostne kulture?

Štampfer: Varnostna zavest zaposlenih je poleg tehničnih rešitev nujni pogoj za zagotavljanje čim boljše varnosti in gospodarske odličnosti podjetja. Sistemski pristop k oblikovanju varnostne kulture in dvig varnostne zavesti temelji na integriranem varnostnem sistemu podjetja, ki poleg ukrepov s področja zasebnega varovanja vključuje tudi organizacijske in kadrovske ukrepe za zagotavljanje varnosti. Z namenom izgrajevanja celovitega varnostnega sistema smo v Pošti med ukrepe za zagotavljanje varnosti ljudi in premoženja vključili tudi izvajanje testov integritete in varnostno preverjanje z uporabo poligrafske metode. Veliko skrb pa namenjamo tudi usposabljanju zaposlenih.

9. Standardizacija sredstev na področju tehničnega varovanja in varnostnih procesov na splošno je v tako razvejanem sistemu verjetno nujno potrebna. Kakšne so na tem področju vaše izkušnje in kakšne pristope uporabljate v Pošti Slovenije?

Štampfer: Standardizacijo na področju tehničnega varovanja dojemam kot realnost in hkrati nujnost, saj le standardizirani sistemi tehničnega varovanja zagotavljajo pričakovano kakovost. Hkrati pa se zavedam, da je v »tehnično-tehnološki eksploziji« potrebno nenehno spremljati razvoj tehničnih sredstev doma in v tujini. Od ponudnikov sistemov tehničnega varovanja v PS pričakujemo, da nam ne ponujajo le proizvodov, pač pa da nam ponudijo tehnične rešitve, ki ustrezajo našim potrebam in pričakovanjem.

10. Kakšne so vaše izkušnje pri zagotavljanju določenih segmentov varnosti z uporabo outsourcinga varnostnih storitev?

Štampfer: Dejstvo je, da si zagotavljanja varnosti v družbi kot je PS praktično ne znamo predstavljati brez pomoči za varnost specializiranih družb za zasebno varovanja. Dejstvo pa je tudi, da bi le te lahko naredile bistveno več kot je bilo to videno do sedaj. Ne morem pozabit primera, ko mi je predstavnik ene družbe za zasebno varovanje v pogajanjih rekel, da jih ne moremo plačati tako malo kot lahko oni malo delajo. Ključna ugotovitev mojega sodelovanja z družbami na področju varnostnih storitev je, da ne znajo oz. želijo ponuditi tega kar naročnik dejansko potrebuje ampak ponujajo to, kar imajo sami že v svojem standardnem portfelju storitev/produktov in to, kjer pravilo ma dosegajo najvišji RVC (hvala bogu obstajajo tudi tukaj svetle izjeme). Prav tako ugotavljam, da (nas) je velika večina naročnikov premalo izobražena o naboru varnostnih rešitev, ki obstajajo na trgu, kar omogoča še lažjo »manipulacijo« naročnikov. Ko se ozrem v pretekla leta ugotavljam, da smo večino (predvsem tehničnih) rešitev, ki smo jih v pošti uvedli oz. jih uvajamo, in za katera smo in še namenjamo znatna finančna sredstva, poiskali v tujini, saj so bile rešitve, ki smo jih bili deležni s strani ponudnikov v Sloveniji večinoma neprimerne. Pa naj to ne zveni kot kritika ponudnikom varnostnih storitev ampak kot pobuda za drugačen pristop k naročniku.

11. Pošta Slovenije je eden izmed korporativnih članov Slovenskega združenja korporativne varnosti. Kakšen pomen pripisujete stanovskemu združevanju na področju korporativne varnosti? Je to dolgoročno lahko pomemben korak k dvigovanju varnostnega zavedanja in predvsem pomena korporativne varnosti?

Štampfer: Z odobravanjem smo pospremili idejo o ustanovitvi Slovenskega združenja korporativne varnosti in z zanimanjem spremljali aktivnosti po ustanovitvi. Ko smo ugotovili, da je eden od ključnih ciljev združenja predvsem v povezovanju naročnikov in ponudnikov varnostnih storitev, ki temelji na izobraževanju, deljenju izkušenj in dobrih praks tako v Sloveniji kot v tujini, smo se v to združenje tudi sami včlanili in v okviru katerega aktivno delujemo. Velik izziv oz. potencial združenja predstavlja ravno problematika, ki sem jo nakazal v odgovoru na prejšnje vprašanje. ■



Life gre z mano!

Vodite vaše podjetje vi ali podjetje vodi vas?
S Poslovnim centrom Pošte Slovenije boste svoj biznis obrnili na glavo in ponovno postali gospodar svojega življenja. Vrhunski pisarniški programi, prava strojna oprema in uporabnikom prijazne poslovne storitve – vse na enem mestu, skrbno povezano in izredno preprosto, predvsem pa brez skrbi in preglavic.

Za brezhibno delovanje, varnost in zanesljivost nepogrešljivih poslovnih orodij bodo poskrbeli usposobljeni strokovnjaki Pošte Slovenije, vam pa bo ostalo več časa za biznis... in življenje.

ŽE ZA
21€
/ MESEC*



* Najem prenosnega poslovnega računalnika HP ProBook 6570b za 2 leti.
Cena je v EUR brez DDV in velja ob naročilu na storitve Digitalne pisarne Pošte Slovenije.
Pošta Slovenije d.o.o., Slomškov trg 10, Maribor.

080 14 46
www.poslovnicenter.si

poslovni center
Zanesljivo vsepovsod
POŠTA SLOVENIJE

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



KOLUMNA
denis caleta@ics-institut.si

ALI DRŽAVA ZAMUJA PRILOŽNOST ZA RACIONALIZACIJO STROŠKOV VAROVANJA OBJEKTOV V NJENI LASTI?

Nahajamo se v največji gospodarski krizi od osamosvojitve Slovenije naprej. Država je pred resno dilemo, kako z upadanjem prilivov v državni proračun zagotoviti nemoteno delovanje ključnih državnih mehanizmov. Tako strokovna, kakor tudi širša javnost se jasno zaveda dejstva, da je obseg državnega aparata, glede na učinkovitost preobsežen in da bodo na posameznih področjih potrebne racionalne rešitve, ki bodo zagotovile višjo dodano vrednost delovanja države. Vse te procese pa je potrebno pogledati tudi skozi prizmo varnosti, ki v sodobni družbi tveganj in ogrožanj predstavlja dobrino katera potrebuje vse več pozornosti in sistemskega pristopa. Ustrezen sistemski pristop pri zagotavljanju varnosti v podjetjih in drugih organizacijah javnega in zasebnega okolja prinaša koristi, ki se odražajo na področju konkurenčnosti, sposobnosti preživetja in razvoja v zelo zahtevnih finančnih okoliščinah ter zagotavlja ustrezno delovanje organizacije v stalno spreminjajočem se varnostnem okolju, obremenjenim z najrazličnejšimi oblikami varnostnih tveganj in groženj.

V tem okviru je še posebej izpostavljena potreba po varovanju ključnih objektov na državnem nivoju med katere vsekakor sodijo tudi objekti vezani na obrambno področje, notranje zadeve in nenazadnje subjekti, ki predstavljajo kritično infrastrukturo v Republiki Sloveniji. Projekcije zmanjševanja finančnih, kadrovskih in drugih virov nas silijo v izvajanje vedno novih analiz, kako z drugačnimi organizacijskimi pristopi doseči bistveno zmanjšanje porabe virov ob osnovnem predpogoju, da se stopnja varnosti teh objektov ne zmanjšuje temveč povečuje. Z doseganjem ustrezne sistemske ureditve področja varovanja ključnih nacionalnih objektov in subjektov kritične infrastrukture pa lahko rešujemo tudi druge pereče dejavnike, kot so na primer zmanjšanje neposrednih finančnih stroškov, ki se za to dejavnost namenjajo neposredno iz državnega proračuna, odhodi pripadnikov Slovenske vojske in Slovenske policije iz aktivne službe, reševanje problemov pripadnikov Slovenske vojske in Policije, ki so se med opravljanjem službenih dolžnosti poškodovali in jim je s tega naslova priznana manjša omejitev opravljanja aktivne službe v svojih organizacijah.

Stanje na področju varovanja ključnih objektov države, kar kriči po ustrezni ureditvi in novih pristopih, ki bodo v svojem cilju zagotavljali racionalnejšo porabo državnega denarja s predpostavko, da se raven varnosti ne bo zmanjševala. Problem pa je, da na žalost država s svojim strokovnim potencialom ni sposobna izvesti ustrezne strateške analize, ki bi zagotovila celovit projektni pristop do priprave študije, katera bi služila strateški politiki za sprejem končne odločitve. Glavni cilj predvidenega projekta mora biti, da Vlada Republike Slovenije na podlagi temeljite analize stanja in možnih variant - sprejme ustrezno odločitev o novem organizacijskem pristopu varovanja ključnih nacionalnih objektov in subjektov kritične infrastrukture, kar vodi v zmanjšanje obremenitev državnega proračuna.

*avtor je član Slovenskega združenja korporativne varnosti



Kako do cilja?

Vlada Republike Slovenije se lahko odloči v okviru naslednjih možnosti in analize možnosti novih organizacijskih pristopov k varovanju objektov skozi naslednje variante:

(1) da stanje na področju varovanja ključnih objektov v njeni lasti ostane nespremenjeno in se v okviru obstoječega sistema loteva ukrepov racionalizacije sistema varovanja;
(2) vzpostavitev javne agencije z javnim pooblastilom za izvajanje varovanja nacionalnih objektov in subjektov kritične infrastrukture na katero bi država prenesla varovanje vseh objektov;
(3) vzpostavitev podjetja v javno zasebni lasti (javno-zasebno partnerstvo) s katerim bi država sklenila poseben sporazum za varovanje nacionalnih objektov, del svoje dejavnosti pa bi to podjetje opravljalo normalno na trgu varnostnih storitev;
(4) celoten prenos varovanja na subjekte zasebnega varovanja;
(5) kombinirana varianta.

Osnova za vsako resno analizo predstavlja ocena tveganja in ogrožanja, ki vpliva na stanje varnosti ključnih objektov in subjektov kritične infrastrukture v Republiki Sloveniji. Tukaj se v osnovi pojavi že prva resna težava, saj so bile vse ocene ogroženosti na nacionalni ravni izdelane brez ustrezne enotne metodologije. Vsekakor bo odločitev, ki bo sledila, morala temeljiti na ustreznih zakonskih podlagah z upoštevanjem dinamike trga predvsem s stališča konkurence oz. omejevanje konkurence na obravnavanem področju. Še posebej je to pomembno z vidika odločitve, da bi država ustanovila podjetje, ki bi ponujalo usluge varovanja tudi izven okvira varovanja objektov v lasti države. S tega stališča bo potrebno izvesti tudi realno in temeljito oceno stanja na področju zasebnega varovanja. Trg varnostnih storitev se v Republiki Sloveniji še vedno srečuje z ogromnimi težavami slabe kakovosti ponudbe storitev in nerazumno nizke cene storitev, ki nikakor ne more zagotoviti ustrezne kvalitete. Nekritičen prenos varovanja na subjekte zasebnega varovanja bi v trenutnem stanju pomenil katastrofo in bistveno zmanjšanje stopnje varnosti strateških objektov.

Osnovni cilj, ki ga mora država zasledovati je, poleg racionalizacije, tudi skrb za svoje zaposlene, ki zaradi zakonskih ali zdravstvenih omejitev niso več sposobni za aktivno službo. V tem okviru govorimo predvsem o pripadnikih Slovenske vojske in Policije. Opredelitev kadrovskega mo-



dela s katerim bi država rešila status določenega dela vojakov Slovenske vojske po 45 letih starosti, ko na podlagi Zakona o obrambi končajo aktivno službo v Slovenski vojski je izredno pomemben signal v procesu skrbi za svoje zaposlene. Le ta ima tudi širše posledice, ki se odražajo v poklicni aktivnosti ljudi, kateri so ustrezno usposobljeni za delo z orožjem in imajo druga potrebna znanja, katera jim omogočajo učinkovito nadaljevanje poklicne kariere. Na drugi strani pa bi se bistveno zmanjšala sredstva, ki so se do sedaj namenjala za odpravnine in prešolanja pripadnikov za civilni poklic. Določene rešitve se lahko vodijo tudi v smeri analize možnosti socialnega podjetništva oz. reševanja statusa pripadnikov Slovenske vojske in Policije, ki imajo zaradi posledic opravljanja svojega dela priznane določene zdravstvene omejitve, ki jih omejujejo, da bi nadaljevali aktivno izvajanje svoje službe v Slovenski vojski ali Policiji.

V vsakem primeru, za kakršenkoli model se bo država odločila, je potrebno zagotoviti, da bodo jasno vidni dejavniki vpliva na področju finančnih in kadrovskih virov in možni prihranki za državni proračun. Zagotovljen mora biti ustrezen nadzor z zasledovanjem cilja, da se raven varnosti ključnih nacionalnih objektov in subjektov kritične infrastrukture postopoma zvišuje. V razmislek pa je potrebno vzeti tudi možnost širših vidikov, kot so ureditev stanja na področju trga zasebno-varnostnih storitev v Republiki Sloveniji, za katerega je država preko zakonskih določil tudi prva odgovorna. Vedno pa ostajajo zanimive tudi ideje o podjetniških projekcijah in možnostih za pridobitev dodatnih finančnih virov. V primeru javno-zasebnega partnerstva bi namreč s ponujanjem uslug na tržišču zasebno-varnostnih storitev v Republiki Sloveniji posredno zmanjševala javna sredstva porabljena v namene varovanja na drugi strani pa določen procent dobička od dela takega podjetja namenjala nazaj v integralni proračun Republike Slovenije (Cost/benefit projekta). ■

> Gospodarska kriza je lahko tudi priložnost za korake, ki jih zaradi ustaljenih vzorcev in vrtičkarstva posameznih državnih organov, nismo bili sposobni narediti v preteklosti.

Novi magistrski program 2. stopnje

MANAGEMENT KORPORATIVNE VARNOSTI

geacollege
Fakulteta za podjetništvo

ICS
Institut za korporativne varnostne študije

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

Predavanja bodo skrbno izvajali največji strokovnjaki na področju korporativne varnosti.

*

Veliko število gostujočih predavateljev, ter s tem zagotavljanje implementacije praktičnih spoznanj v izobraževalni proces.

*

Sodelovanja v aktivnostih Slovenskega združenja korporativne varnosti (konference, posveti in neposredni obiski različnih organizacijskih okolij).

*

Visoko zaposljivost naših študentov v nacionalnem in mednarodnem okolju.

*

Neposredna podpora pri zagotavljanju službe najboljšim študentom.

*

Za najbolj uspešne študente zagotovitev izvajanja neposredne prakse v okolju mednarodnih korporacij.

*

Širok nabor znanja tudi za delo na različnih nivojih korporativnega upravljanja.

PRIHODNOST PRIPADA PODJETNIM!

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

INTERVJU
Izredni profesor dr. Jaka Vadnjal
Dekan GEA College/Fakultete za podjetništvo

PRED VRATI JE NOV PROGRAM PODIPLOMSKEGA IZOBRAŽEVANJA S PODROČJA MANAGEMENTA KORPORATIVNE VARNOSTI

Če želimo, da bodo organizacije javnega in zasebnega okolja delovale uspešno, potem jim moramo v roke položiti orodja za učinkovito obvladovanje tveganj, katerim so izpostavljene v tem dinamičnem okolju.

1. GEA College ima v samostojni državi zavidljivo tradicijo izvajanja študija podjetništva. Nam lahko na kratko opišete razvoj te zasebne visokošolske institucije.

GEA College je kot podjetje za izvajanje kratkih seminarjev na temo podjetništva začelo delovati leta 1990 kot odgovor na ekonomske procese, ki so se takrat začeli intenzivno dogajati: prestrukturiranje gospodarstva, razgradnja velikih sistemov, izgube tradicionalnih trgov in posledično velika brezposelnost in na drugi strani ogromno priložnosti so bili dejavniki okolja, ki so takrat sprožali val podjetništva. Po drugi strani je bila v ljudeh nekaj deset let zatrta želja po zasebnem, samostojnem podjetništvu. Čas je bil pravi in logična rast podjetja je vodila v zagon Visoke šole za podjetništvo s prvo generacijo študentov jeseni leta 1996. Bili smo prva zasebna visoka šola v državi, do danes je pri nas diplomiralo več kot 1200 študentov in magistriralo dobrih 120. Leta 2010 smo postali fakulteta, ki izvaja program podjetništva na prvi in drugi bolonjski stopnji. Smo »utrjena« inštitucija s potrebnim znanjem in izkušnjami za nove izzive.

GEA College je kot podjetje za izvajanje kratkih seminarjev na temo podjetništva začelo delovati leta 1990 kot odgovor na ekonomske procese, ki so se takrat začeli intenzivno dogajati.

2. V zadnjem letu skupaj z Institutom za korporativne varnostne študije zelo aktivno razvijate podiplomski magistrski program II. bolonjske stopnje z nazivom »management korporativne varnosti«. Kako se je pojavila ideja o potrebi take vrste študija?

Nastanek ideje je bil pravzaprav podjetniški proces. Z Institutom za korporativne varnostne študije (v nadaljevanju ICS-Ljubljana) oziroma njegovimi ključnimi akterji smo se poznali že prej. Hitro smo se strinjali, da imamo veliko komplementarnega znanja, da delimo vrednote raziskovanja in preizkušanja novega in da imamo namen ideje tudi realizirati in ne o njih samo razpravljati, kako bi bilo to in to fino narediti. Do razdelane ideje o študiju »management korporativne varnosti« je bilo potrebnih samo še nekaj brainstormingov in

*avtor je član Slovenskega združenja korporativne varnosti



osnutek je bil na papirju. Potrebno pa je poudariti, da tak program ne more nastati brez intenzivnega timskega dela, ki mora biti dobro orkestrirano v program smo pritegnili vrsto strokovnjakov, katerih znanje je vendarle treba povezati v zaokroženo celoto.

3. Nam lahko poveste kaj več o ciljih programa in predvsem kompetencah, ki jih bodo dobili diplomanti tega študije?

Integralna varnost v različnih organizacijah je vse bolj aktualna. Ne samo fizična, kot jo laično pojmujemo, da se moramo zavarovati, da ne bo kdo vlomil v podjetje in nam odnesel za nekaj tisoč evrov zaloge. Gre za kompetenco celostnega obravnavanja varnostnih pojavov in tveganj. Med najbolj intenzivnim delom na programu se je zgodila Fokušima. Lep primer, ko so strokovnjaki potem ugotavljali, da je bila možnost take nesreče minimalna, ampak se je vendarle zgodila in to z neslutenimi posledicami. Usposabljali bomo profil managerja, ki bo v organizacije uvajal novo kulturo, v kateri varnost ne bo več strošek, ampak investicija. Seveda se bo ta človek moral znati umestiti v kontekst delovanja organizacije, ki mora preživeti na trgu, ustvarjati dobiček in odgovarjati različnim interesom. Gre torej za ljudi nove dobe, ki bodo temeljito spremenili vrednote in kulturo posameznih organizacij.

4. Predvidevamo, da je bila narejena podrobna analiza potreb po tem profilu kadra v Republiki Sloveniji? Do kakšnih rezultatov ste prišli skozi to analizo?

Analizo je opravil ICS-Ljubljana in dejansko so potrebe velike že zdaj. Ob upoštevanju dejstva, da bo problematika vse bolj pereča pa lahko trdimo, da bodo potrebe po naših diplomantih še večje. Trdimo, da jih bodo potrebovale prav vse inštitucije. Če si jih ne bodo mogle privoščiti kot zaposlene, jih bodo najemale tudi kot zunanje izvajalce – strokovnjake zato verjamemo, da bodo na tem področju tudi mnoge podjetniške priložnosti in tudi za njihovo realizacijo bomo usposabljali naše študente.

5. Katerim težiščem ste skozi predviden predmetnik študija namenili največ pozornosti?

Predmetnik predvideva približno 60% vsebin različnim strokovnim področjem varnosti od kritične infrastrukture do mikrolokacij, od fizičnega in tehničnega, prek informacijskega do okoljskega varovanja. Preostali del so poslovne discipline, nekakšen železni repertoar s priokusom varnosti: poslovne finance s poudarkom tudi na »odtekanju« denarja iz podjetja, marketing z vidikom varovanja poslovnih (tržnih) skrivnosti, ekonomika z izračunov stroškov in koristi vpeljave integralnega varnostnega sistema itd.

6. Študijskim programom v Sloveniji očitajo premalo povezav študijskih vsebin z neposredno dobro prakso v gospodarstvu. Načrtujete v izvedbi vašega programa drugačne pristope?

Vsekakor. Naš študij je popolnoma v skladu z bolonjskimi principi, torej zelo aplikativno naravnan. Posredno to dosegamo tako, da naši predavate-

lji sicer dosegajo pričakovane akademske standarde, vendar imajo vsi tudi precej praktične »kilometrine« bodisi kot aktivni managerji v podjetjih, svetovalci, razvojniki itd. Neposreden način pa je prek tesnega sodelovanja z ICS-Ljubljana, kjer stalno potekajo številni raziskovalni in razvojni projekti ter nekaterimi velikimi, tudi mednarodnimi korporacijami, ki bodo odprte za sodelovanje v smislu reševanja konkretnih problemov ali celo z možnostjo stažiranja naših slušateljev v njihovih oddelkih.

7. Kakšne so mednarodne perspektive prihajajočega študija?

Med rednimi srečanji in izmenjavo izkušen s kolegi si navadno pripovedujemo tudi o razvojnih načrtih, zato da drug pri drugem dodatno testiramo ideje. Ta študij je, še preden se je začel izvajati, vzbudil zelo veliko zanimanja, predvsem v državah bivše Jugoslavije. Vsekakor razmišljamo tudi o izvedbah tudi v teh okoljih, vendar moramo program najprej dobro pognati doma.

8. Kompleksnost varnostnega okolja kaže na dejstvo, da morajo korporativno varnostni strokovnjaki obvladati cel niz raznovrstnih znanj, ki niso vezana samo na ozko varnostno področje. Ali interdisciplinarno zasnovan študij lahko odgovori na izzive modernega poslovnega in dinamičnega okolja?

V to trdno verjamemo, sicer ne bi zasnovali takega študija. Omejili smo se na dve, po našem mnenju ključni področji in sicer na širše področje varnostnih ved in področje poslovnih ved. Interdisciplinarnost razumemo ne samo kot mešanje vsebin dveh raznovrstnih disciplin, ampak predvsem kot to, da se stroki povezujeta na predmetni ravni: varnostni predmeti bodo vsebovali vidik poslovanja in podjetništva, poslovni predmeti pa varnostni vidik. Seveda je to velik izziv pri zasnovi programi in tudi izvedbi, saj bomo od predavateljev zahtevali vrhunsko upoštevanje tega načela. Dodatno interdisciplinarnost programu oziroma končnim kompetencam diplomantov bodo dali diplomanti sami, saj pričakujemo, da se bodo vpisali slušatelji, ki so na prvi (dodiplomski) stopnji diplomirali na zelo različnih področjih: varnostne vede, tehnika, poslovne vede, družboslovje in drugo.



9. Velika večina mladih ima občutek, da jih inštitucije, kjer se izobražujejo po končanem študiju nekako »pozabijo«. V vašem primeru imate drugačen pristop do svojih diplomantov. Kako nameravate te vezi po končanem študiju še okrepiti?

Na GEA College – Fakulteti za podjetništvo imamo zelo dinamičen Alumni klub, v katerega je včlanjenih nekaj sto naših diplomantov in magistrantov. Alumni klub organizira poslovna srečanja, obiske uglednih gostov, različne družabne aktivnosti in tudi zabavnih trenutkov ne manjka. Je pač tako, da so vezi, ki jih je človek stkal v šolskih klopeh zelo močne. Včasih se skrijejo, vendar je potrebno zelo malo, da se spet utrdijo. Model je pri nas že dobro preizkušen in verjamemo, da bo deloval tudi na prihajajočih diplomantih magistrskega programa management korporativne varnosti. Nikakor pa ne smemo pozabiti tudi Slovenskega združenja korporativne varnosti, ki deluje v okviru ICS-Ljubljana in v Sloveniji združuje korporativno varnostne strokovnjake. Korporativni člani tega združenja so tudi vsa pomembna podjetja in organizacije, ki obvladujejo kritično infrastrukturo v naši državi. Študente in predvsem diplomante bomo aktivno vključevali v delovanje tega združenja. Skozi te povezave pa bo prišla tudi možnost zaposlovanja določenega dela teh diplomantov.

10. Najboljši študentje bodo deležni tudi dodatnih pristopov za njihovo uveljavljanje na trgu dela. Najboljšim nameravate omogočati prakso v mednarodnem korporativnem okolju.

Imamo velik privilegij, da je eden od simpatizerjev programa naš rojak, ki je v enem največjih globalnih koncernov na svetu zadolžen za globalno korporativno varnost na nivoju celotne korporacije. V tej korporaciji, ki je zaenkrat ne bi razkrivali so možnosti za praktično usposabljanje naših študentov izjemne. Verjamemo, da jih bomo znali tudi učinkovito izkoristiti. Obstajajo pa tudi vzvodi o katerih sem govoril v prejšnjem odgovoru in se jih bomo zelo aktivno posluževali. ■

Na GEA College – Fakulteti za podjetništvo imamo zelo dinamičen Alumni klub, v katerega je včlanjenih nekaj sto naših diplomantov in magistrantov.

Avtor: Štefan Gostič, univ. dipl. pravnik / Direktor kadrovske službe in vodja varnostne politike v podjetju TNT Express d.o.o*



ZAGOTAVLJANJE KORPORATIVNE VARNOSTI S POMOČJO STANDARDA ISO 28000:2007 – SISTEMA UPRAVLJANJA Z VARNOSTJO

Korporativno oziroma poslovno varnost lahko opredelimo kot varnostni sistem podjetja ali sistem za zagotavljanje notranje varnosti v podjetju. Je celota pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ukrepov za ohranitev reda, spoštovanje zakonov in internih predpisov ter varnosti ljudi in premoženja v podjetju.

Obstoj sistema upravljanja z varnostjo (Security management System – SMS) je izrednega pomena, saj se sleherno podjetje nahaja v bolj ali manj (ne)stabilnem okolju. Nanj vplivajo različni dejavniki ogrožanja, kot na primer najrazličnejša kazniva dejanja v družbi (kriminal), različne nesreče, državni predpisi in ostala oblastna ravnanja, konkurenca, ipd. Notranja varnost podjetja je za njegov poslovni uspeh vitalnega pomena, saj podjetje, ki nima izgrajenega ustreznega in učinkovitega varnostnega sistema stagnira v ekonomskem pomenu, nenazadnje pa takšno podjetje tudi nima ustreznega ugleda v poslovnem in širšem okolju. Korporativno varnost v podjetju lahko učinkovito zagotovimo z vzpostavitvijo sistema upravljanja z varnostjo, skladno z mednarodno priznanim standardom ISO 28000:2007.

Teoretična izhodišča za izgradnjo varnostnega sistema

Poslovna varnost pomeni zagotavljanje pravnih, organizacijskih, funkcionalnih ter tehničnih ukrepov oziroma aktivnosti za zagotavljanje varnega in nemotenega poslovanja podjetja. Ključne aktivnosti v procesu zagotavljanja poslovne varnosti so:

- načrtovanje in izvajanje varnostnih procesov v podjetju;
- izvajanje preventivnih ukrepov za preprečevanje škodnih dogodkov in finančnih izgub v podjetju (preprečevanje poslovnih tveganj);
- izgradnja integralnega varnostnega sistema v podjetju;
- dvigovanje varnostne kulture v podjetju;[1]
- implementacija standardov s področja varovanja;
- odkrivanje in raziskovanje incidentov in kaznivih dejanj v podjetju;
- izdelava ocen ranljivosti, ogroženosti in varnostnih tveganj (ocena ROT).

Varnostni sistem podjetja je sistem za zagotavljanje notranje in poslovne varnosti. Je celota organizacijskih in funkcionalnih ukrepov, s pomočjo katerih se zagotavlja ohranitev reda, spoštovanje zakonov in internih predpisov, varnost zaposlenih ter zaščito

Vzpostavitev ustreznega varnostnega sistema je izrednega pomena, saj vsaka organizacija po naravi stvari teži k entropiji oziroma razpadu.

*avtor je član Slovenskega združenja korporativne varnosti

imetja in infrastrukture podjetja. Je celota organizacijskih in funkcionalnih ukrepov, s pomočjo katerih skrbimo za ohranitev reda, spoštovanje zakonov in internih predpisov, osebno varnost ter zaščito imetja in infrastrukture. **Vzpostavitev ustreznega varnostnega sistema je izrednega pomena, saj vsaka organizacija po naravi stvari teži k entropiji oziroma razpadu.** Nanjo vplivajo različni dejavniki oziroma škodni pojavi, kot na primer najrazličnejša kazniva dejanja v družbi (kriminal), različne nesreče, državni predpisi in ostala oblastna ravnanja, konkurenca, ipd.

Vsako podjetje bi moralo zaradi varnega poslovanja vzpostaviti varnostni sistem oziroma t.i. varnostno arhitekturo, ki jo predstavljajo[2] organizacijski in funkcionalni ukrepi za vzpostavitev oz. zagotavljanje poslovne in notranje varnosti:

- varnostni podsistemi (CCTV, fizično, tehnično varovanje...);
- sodoben informacijski sistem;
- varnostna kultura zaposlenih in
- konkretni varnostni ukrepi.

Škodni dejavniki (varnostna tveganja)

Zagotavljanje poslovne varnosti v podjetju je za njegovo dobro in konkurenčno poslovanje izrednega pomena, saj podjetje kot organizacija, ki nima izgrajenega ustreznega in učinkovitega varnostnega sistema *stagnira v ekonomskem pomenu*, nenazadnje pa takšno podjetje tudi nima *ustreznega ugleda v poslovnem in širšem okolju*. Izgradnja notranje varnosti podjetja je pomembna predvsem zaradi obstoja in delovanja različnih škodnih pojavov oziroma škodnih dejavnikov (varnostna tveganja), ki posredno ali direktno vplivajo na podjetje. Te dejavnike lahko, glede na njihov izvor, delimo na notranje in zunanje.

Vzpostavitev oziroma izgradnja integralnega varnostnega sistema v podjetju – sistema upravljanja z varnostjo po standardu ISO 28000:2007

Integralni varnostni sistem je z internimi akti predpisano usklajeno delovanje zaposlenih v podjetju (predvsem varnostna kultura zaposlenih) in tehničnih sredstev za varovanje premoženja podjetja. Gre za usklajeno delovanje varnostnih podsistemov za: varovanje ljudi in premoženja, požarno varnost, varnost in zdravje pri delu, ekologijo, civilno zaščito, informacijski sistem, podatkovni zapisi, družbeno odgovornost, itd. Integralni varnostni sistem v podjetju je torej sistem za zagotavljanje poslovne varnosti v podjetju, s pomočjo katerega uresničujemo dogovorjeno ali zahtevano (državni predpisi in zahteve strank oz. dobaviteljev) stopnjo varnosti v podjetju. Za učinkovito zagotavljanje poslovne varnosti je potrebno torej organizirati varnostni sistem, s pomočjo katerega se bo zagotavljal nemoten poslovni proces, ki mu bodo zaposleni in stranke zaupale.

Integralni varnostni sistem v podjetju, zavodu, državnem organu ali pri drugih osebah javnega in zasebnega prava lahko učinkovito vzpostavimo s pomočjo standarda **ISO 28000:2007 – sistema upravljanja z varnostjo – Security management System** (v nadaljevanju SMS).

> Namen implementacije standarda ISO 28000:2007 je identificiranje, analiziranje in saniranje obstoječih organizacijskih, kadrovskih, varnostnih in drugih vrzeli v obstoječem sistemu varovanja.

ISO 28000:2007 vsebuje vse potrebne zahteve za upravljanje z varnostjo v podjetju, tako da:

- omogoča nadzor nad varnostjo v podjetju in nad blagom, ki ga podjetje prevaža po kopnem, morju ali zraku;
- onemogoča zlorabe;
- zmanjšuje možnost piratskih in terorističnih napadov.

SMS je sistem, ki je ustvarjen z namenom, da omogoči različnim podjetjem (predvsem gospodarske družbe na področju logistične dejavnosti), da v okviru svoje organizacije upravljajo z varnostjo, in sicer: načrtujejo in izvajajo varnostne politike, procedure in standarde, programe za ocenjevanje varnostnih tveganj – dejavnikov ogrožanja, programe za fizično, tehnično in informacijsko varnost ter nadzor nad izvajanjem SMS. *SMS temelji na:*

- *nenehnem ocenjevanju varnostnih tveganj oziroma dejavnikov ogrožanja (Risk Assessment);*
- *objektivnih ciljih, programih in merljivih KPI – key performance indikator – kazalnikih uspešnosti;*
- *dokumentiranih varnostnih procedurah;*
- *omogoča nenehne izboljšave.*

SMS torej omogoča različnim podjetjem in organizacijam, da upravljajo z varnostjo in sicer preko sistema upravljanja z varnostnimi tveganji. Riskanalysis ali ocena varnostnih tveganj je univerzalen ključ oziroma pristop za sprejem vsem pomembnih (varnostih) odločitev v podjetju. Načrtovanje varnosti poteka skladno z Demingovo teorijo PDCA (Deming Circle: Plan – Do – Check – Act). Standard ISO 28000:2007 nam torej omogoča, da na celovit način vzpostavimo integralni varnostni sistem podjetja. Gre za celoto oziroma nabor vseh postopkov in ravnanj poslovodnega organa (uprave družbe).

Cilj standarda ISO 28000:2007 je v podjetju ali drugi ustanovi ustvariti sistem upravljanja z varnostjo, torej z varnostnimi in drugimi izboljšavami optimizirati sistem varovanja podjetja, da bo varnostno učinkovit oziroma optimalen. S pomočjo implementacije varnostnega standarda ISO 28000:2007 v podjetjih in ustanovah zagotovimo sistem upravljanja z varnostjo, tako da vzpostavimo in vzdržujemo:

A. Organizacijski in funkcionalni vidik varnosti:

1. vzpostavitev varnostnih politik, procedur in standardov v podjetju;
2. vzpostavitev varnostnih standardov v podjetju in standardov, ki so pomembni za varnost podjetij (standard upravljanje z varnostjo ISO 28000:2007, standard kakovosti ISO 9000-9001, ISO 9004:2000, vodenje kakovosti – zadovoljstvo strank, navodila za reševanje pritožb – ISO 10002:2004, standard varnosti in zdravja pri delu OHSAS 18001,...);
3. vzpostavitev zbirke vseh zunanjih in internih predpisov, ki se nanašajo na zagotavljanje varnosti v podjetju;

4. izdelava varnostnega elaborata in razvojnega varnostnega programa;
5. spremljanje in evidentiranje varnostnih dogodkov v podjetju;
6. obravnava pritožb;
7. merjenje izgub in škod;
8. vnaprejšnje varnostno preverjanje kandidatov za zaposlitev;
9. vzpostavljanje in širjenje varnostne kulture v podjetju (usposabljanje in izpopolnjevanje zaposlenih, stalno informiranje zaposlenih o varnostni problematiki);
10. ostalo.

B. Tehnični vidik varnosti:

1. tehnično varovanje;
2. video nadzorni sistem (CCTV);
3. osvetlitev objekta;
4. alarmni sistemi (požarni, protiropni, protivlomni, itn);
5. pristopna kontrola;
6. mehansko varovanje;
7. ...



Koristi in prednosti vzpostavitve varnostnega standarda ISO 28000:2007

S pomočjo vzpostavljenega sistema upravljanja z varnostjo – ISO 28000:2007 v podjetju ali drugi ustanovi zagotovimo:

Zmanjšanje obsega (števila) varnostnih tveganj: vzpostavitev SMS vodi k zmanjšanju pojava t.i. varnostnih incidentov (ropi, tatvine, zlorabe, goljufije, pretepi, alkoholiziranost, druga kazniva dejanja), k zmanjšanju izgub v podjetju, zmanjšanju internih preiskav, zmanjšanju števila pritožb kupcev oz. poslovnih partnerjev, zmanjšanje nezadovoljstva strank in k zmanjšanju regresnih zahtevkov s strani zavarovalnic.

Povečanje odpornosti – prožnosti podjetja: vzpostavitev vseh varnostnih standardov, politik in procedur v podjetju omogoči podjetju, da v primeru varnostnega incidenta (npr. rop, požar, kraja informacij) neprekinjeno in normalno posluje oziroma nemudoma vzpostavi normalno stanje.

Odgovornost za varnost: SMS omogoča podjetju uresničevati odgovornost za varno počutje delavcev, pogodbenih partnerjev ter obiskovalcev.

Doslednost: SMS omogoča dosledno izvajanje sprejetih varnostnih politik, standardov in procedur v podjetju, kar zagotavlja nemoten poslovni proces v podjetju.

Onemogočanje preobsežnih programov: implementacija SMS avtomatično onemogoči kopičenje preobsežnih in neustreznih oziroma neučinkovitih varnostnih programov v podjetju, kar pomeni takojšnje zmanjšanje stroškov in ohranjanje zmanjšanega obsega stroškov v prihodnosti.

Obstoj celovitega varnostnega sistema: ISO 28000:2007 je edini mednarodni varnostni standard, ki na celovit način ureja zagotavljanje varnosti v podjetjih in drugih ustanovah.

Združljivost z ostalimi varnostmi programi: ostali varnostni programi se lahko na enostaven način združujejo z SMS, kar poenostavi nadaljnje rokovanje in upravljanje s temi varnostnimi programi (C TPAT, AEO, STP, TAPA, Aviation Security & Customer Security Requirements).

Povečanje ugleda podjetja: poslovni partnerji in stranke podjetja pričakujejo, da bo njihovo poslovanje potekalo na varen način, še posebej na področju logistike, torej prevoza blaga in dobrin, kjer pričakujejo, da bo njihovo blago prispelo na cilj pravočasno in v brezhibnem stanju. Razpolaganje s standardom ISO 28000:2007 je jasen signal strankam, da se njegovi imetniki zavedajo svoje odgovornosti do strank ter da so v podjetju vpeljani vsi varnostni mehanizmi, ki omogočajo zagotavljanje varnosti premoženja, oseb in blaga.

Konkurenčna prednost: posest varnostnega standarda ISO 28000:2007 pomeni tudi konkurenčno prednost podjetja na konkurenčnem trgu, kjer opravlja svoje storitve

Učinkovito izrabljanje virov: s pomočjo varnostnega standarda ISO 28000:2007 lahko natančno prepoznamo oz. ugotovimo, kateri viri v podjetju (finančni, kadrovski, materialni) se morajo varovati in spremljati, kar posledično pomeni onemogočanje razsipavanja z viri in varčevanje denarja.

Področja trženja standarda ISO 28000:2007

Varnostni standard ISO 28000:2007 je predvsem namenjen za varovanje ljudi in premoženja na področju logistike (skladiščenje, transport, ostale logistične storitve) oziroma na področju celotnega logističnega procesa: vse faze pretoka blaga med proizvajalcem in kupcem (suply chain), v cestnem, morskem in zračnem transportu. Seveda pa je standard uporaben tudi na vseh drugih področjih, torej pri pravnih osebah javnega in zasebnega prava (državni organi, zavodi, občine, razne



gospodarske družbe). V Republiki Sloveniji torej obstaja realna tržna niša:

- v vseh logističnih podjetjih – domača in mednarodna špedicija,
- zračna pristanišča – letališča,
- morska pristanišča,
- državni organi, kot na primer ministrstva, parlament,
- občine,
- šole,
- banka Slovenije,
- poslovne banke,
- zavarovalnice,
- trgovske hiše (npr: Mercator, Lidl, Spar, Tuš, ...),
- naftni distributerji (Petrol, Istrabenz),
- podjetja, ki neposredno proizvajajo blago – dobrine (predvsem hi-tech blago: Sony, Nokia, itn);
- železnice;
- finančna podjetja;
- druga gospodarska podjetja in veliki sistemi.

Zaključek

Security management in *Risk management* oziroma upravljanje z varnostjo ter z varnostnimi ali operativnimi tveganji kot vitalni sestavini korporativne varnosti, postaja tudi v naši državi vse bolj pomemben element poslovanja (predvsem velikih) gospodarskih družb. Kot je bilo navedeno, lahko na podjetje delujejo različni škodni dejavniki, tako zunanji kot notranji. Vsi ti varnostni dogodki lahko podjetju povzročijo neposredno ali posredno izgubo, bodisi izgubo ugleda v poslovnem okolju, finančno, materialno ali kadrovsko izgubo, izgubo konkurenčne prednosti na trgu, itn. Zato je pomembno znanje in (samo)zavedanje o nujnosti vzpostavitve oziroma organizacije korporativne varnosti v podjetju. Slednje pa je še vedno premalo prisotno med slovenski menedžerji oziroma lastniki gospodarskih družb. Za učinkovito organizacijo varnostnega sistema v podjetju je potreben sistemski pristop in temeljito poznavanje področja varnosti ter (kar je seveda tudi ključno) poslovnega procesa v konkretnem podjetju. Za obvladovanje varnostnih tveganj je pomembno, da podjetje sistematično načrtuje, ugotavlja in določa ukrepe in postopke za obrambo pred tveganji. Samo z ustreznim načrtovanjem in izvedbo pravnih, organizacijskih, kadrovskih in tehničnih ukrepov, lahko zagotovimo ustrezen nivo korporativne ali poslovne varnosti. Vse to pa seveda zagotavlja in omogoča varnostni standard ISO 28000:2007. ■

[1] Termin »varnostna kultura« je prvič omenjen v javno-pravnem predpisu: Pravilnik o določitvi varnostnih standardov poslovanja sodišč (Uradni list št. 41/2007).

[2] Seveda je organiziranost varnostnega sistema odvisna od večih dejavnikov, predvsem od velikosti podjetja, njegove dejavnosti ter varnostne problematike. Glede na kriterije za mikro, majhne, srednje in velike družbe po Zakonu o gospodarskih družbah, je organizacijski model za vzpostavitev varnosti v konkretni družbi različen. Ne glede na to pa mora vsako podjetje poskrbeti vsaj za osnoven model varnosti.

Avtorji: Primož Velikonja, Borut Lončarevič, Andraž Ogorevc*

iHELP - MOBILNA APLIKACIJA, KO RABIMO POMOČ

Čas teče. Vedno z enako hitrostjo in ne oziraje se na situacijo. Tudi takrat, ko gre za življenje. Z uporabo mobilne aplikacije iHEPL lahko z enim samim klikom na mobilnem telefonu pomagamo življenje sebi, družinskemu članu, prijatelju ali neznancu.

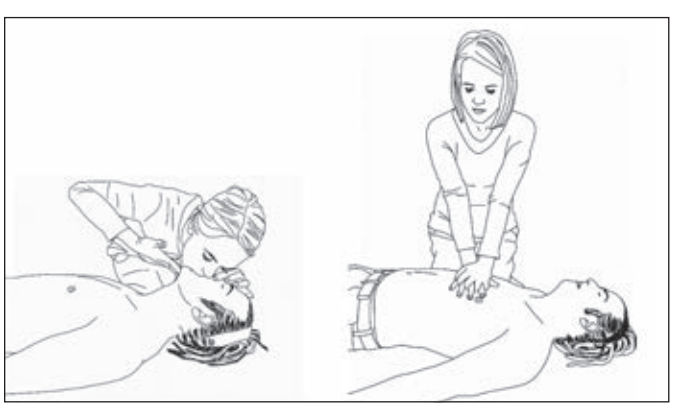
Bolezni srca in ožilja - problem sodobne družbe

Nenaden srčni zastoj je vodilni vzrok smrti v svetu. Kar 74% srčnih zastojev se zgodi v pričo laičnih očividcev (Rajapakse, 2008). V Evropi so srčno žilne bolezni vzrok za 40% smrti pri ljudeh mlajših od 75 let. Pri tem služba nujne medicinske pomoči (NMP) obravnava letno 38 primerov srčnega zastoja na 100.000 prebivalcev zunaj bolnišnice (Nolan et al., 2010). Po ocenah strokovnjakov je v Sloveniji 5 do 6 srčnih zastojev dnevno; v povprečju torej okoli 2.000 na leto (Ploj in Gradišek, 2006).

Tako imenovana veriga preživetja je sestavljena iz štirih členov, ki morajo biti med seboj neprekinjeno povezani. Prvi člen je namenjen zgodnji prepoznavi in hitremu klicu na številko 112. Pri drugem členu, s kakovostno izvedenimi TPO, kupujemo čas. Tretji člen je namenjen zgodnji defibrilaciji, kjer nastala motnja srčnega ritma zahteva električni sunek. Zadnji člen verige je namenjen ohranjevanju delovanja srca in možganov. Izvajajo jo za to usposobljene ekipe NMP (Nolan et al., 2010).

Pri nenadnem srčnem zastoju (nenadno prenehanja delovanja srca, zaradi česar oseba meji med življenjem in smrtjo (Bardy et al., 2008) je hitro ukrepanje ključnega pomena, saj po 4 do 5 minutah brez izvajanja temeljnih postopkov oživljanja (TPO) pride do nepopravljivih okvar v možganih.

Oživljanje oz. izvajanje TPO s strani laikov in zgodnja defibrilacija rešujeta življenje. Pri izvajanju TPO sledimo predpisanemu algoritmu, ki določa vrsto in zaporedje ukrepov (Koster et al., 2010).



Potek obveščanja ob nesreči

Predpostavimo, da je prišlo do nenadnega srčnega zastoja; človek se zgrudi. Najmanj kar lahko storimo je, da pokličemo: »Na pomoč!« ter o dogodku sporočimo na telefonsko številko 112, ki je namenjena klicu v sili. Operater regijskega centra za obveščanje (ReCO) bo od kličočega pridobil osnovne podatke ter lokacijo trenutnega nahajanja. Operater na ReCO preko direktne telefonske linije CB preusmeri klic v dispečerski center NMP. Operater NMP se nato na podlagi zbranih podatkov, in po potrebi s posvetom zdravnika, odloči o sestavi ekipe, ki jo bo poslal na kraj dogodka.

* Člani projektne skupine iHELP * (Primož Velikonja, inštruktor sveta za reanimacijo, Borut Lončarevič vgč., inštruktor radijskih zvez, Andraž Ogorevc, vodja projekta iHELP (MiDS d.o.o.)

Oprema v dispečerskih centrih NMP je zelo različna, prav tako so različne naloge dispečerjev. V našem primeru, ko o življenju odločajo minute, je sila pomembno koliko časa porabimo ravno v prvi fazi alarmiranja.

2 minuti	1 minuta	6 minut	2 minuti
Klicanje reševalne službe	Aktivacija in izvoz reševalcev	Vožnja na mesto intervencije	Prihod defibrilacija

Zahtevani (veljavni) standardi ukrepanja reševalnih enot

Na podlagi predpisa (URL, 2007) mora enota NMP od časa prejema klica (usmerjena vprašanja, navodila za prvo pomoč) do časa, ko vozilo odpelje na kraj dogodka (zapusti izhodiščno lokacijo) trajati dve minuti ali manj. Preizkus je uspešno opravljen, če je v vozilu tričlanska ekipa z zdravnikom, defibrilator z monitorjem in reanimacijski komplet ter kisik.

Po izvozu interventne enote na kraj dogodka, je potreben še čas za vožnjo ter pripravo ekipe za pomoč poškodovancu. Ko seštejemo vse časovne operacije, kaj kmalu ugotovimo, da je posredovanje v manj kot 10 minutah, velik uspeh. Pri tej ugotovitvi se vprašamo ali obstaja način, kako izboljšati odzivni čas pri izvajanju temeljnih postopkov oživljanja v primeru nenadnega srčnega zastoja.

Ideja iHELP

Ideja o projektu iHELP je nastala leta 2011. Pretresljiva statistika bolezni srca in ožilja je pričela porajati vprašanja in razmišljanja na kakšen način širši množici ponuditi oz. omogočiti dostopnejšo, predvsem pa hitrejšo pomoč, ki je ključna pri zagotovitvi preživetja. Za realizacijo projekta je bila izbrana skupina strokovnjakov iz različnih področij delovanja.

Cilj projekta iHELP je znižati trenutno visoko stopnjo umrljivosti v primeru nenadnega zastoja srca, povečati informiranost o možnih načinih pomoči žrtvam srčnega zastoja, izboljšanje mreže defibrilatorjev v Sloveniji kot tudi načina družbeno odgovornega komuniciranja.

iHELP aplikacija pa je ravno tako primerna tudi za hitro obveščanje v primeru prometne nesreče, možganske kapi, epileptičnega napada, diabetičnega napada, padca itd.



Opis iHELP aplikacije

Mobilna aplikacija je enostavna za uporabo. Z enim samim klikom na mobilnem telefonu lahko družinskemu članu, prijatelju, neznancu ali sebi rešimo življenje. iHELP mobilna aplikacija nudi **izobraževanje** o prvi pomoči in **pošilja SOS sporočila** poklicnim reševalcem, družini, prijateljem in vsem iHELP uporabnikom aplikacije v radiju 300 metrov ali več od ponesrečenca.

Vsebina mobilne aplikacije:

- **Podatki uporabnika** (osnovni podatki in koristne informacije pri reševanju),
- **SOS kontakti** (družina, prijatelji, sosedje, osebni zdravnik, ...),
- **Navodila o temeljnih postopkih oživljanja (TPO)** (v besedni, slikovni in avdio obliki),
- **Splošno izobraževalne vsebine** (nasveti oz. vodenje skozi ukrepe pri nenadnem zastoju srca, prometni nesreči, zlomu ali zvinu, krvavitvi, itd.),
- **Geo-lokacija ponesrečenca** (vzporedno s pošiljanjem SOS sporočila se oddajajo tudi GPS koordinate),
- **Dežurstvo** (vsak iHELP reševalec lahko glede na svoj razpoložljivi čas potrdi svoje sodelovanje oz. razpoložljivost),
- **Lokacije (najbližje) avtomatskega električnega defibrilatorja (AED),**

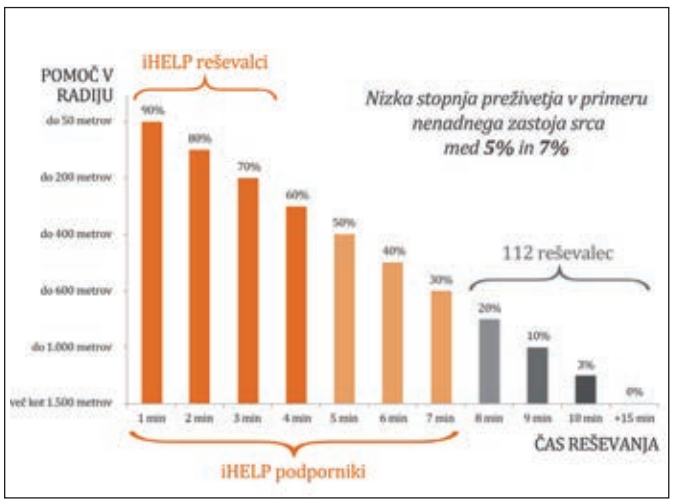
Zgoraj navedeno ter številne **povezovalne aktivnosti**, ki krepijo in vlagajo v skupnost (popis defibrilatorjev, izobraževanja, lestvica najbolj aktivnih "iHELP reševalcev", povabi prijatelje in podjetja, pomagaj graditi skupnost in postani junak...) aplikaciji iHELP še povečujejo njeno dodano vrednost.

Razvili smo tudi **iHELP zapestnico**, ki deluje samo preko iHELP aplikacije.

V primerih, ko uporabnik nima telefona ob sebi, lahko ponesrečenec z pritiskom na gumb na zapestnici aktivira Bluetooth in pošlje signal na mobilni telefon in ta pošlje SOS sporočilo (Geo-Lokacijo in ostale podatke) družinskim članom in prijateljem v primeru nujne pomoči.



va, alergije...). Ko reševalec prispe do ponesrečenca mu iHELP aplikacija nudi navodila za oživljanje (TPO) v besedi, sliki oz. v zvočnem formatu. S tovrstnim načinom reševanja lahko verjetnost preživetja v primeru nenadnega zastoja srca povečamo za kar 70%.



V naslednjih mesecih je načrtovan tudi razvoj dodatkov in nadgradnje iHELP aplikacije:

- **Hitri nasveti** (v primeru glavobola, krvavitve iz nosu, slabosti, pri zdravljenju »mačka«, prehlada, viroze, dehidracije, podhladitve...),
- **SOS opomnik** (če v določenem času le ta ni izključen, pošlje SOS sporočilo članom družine in prijateljem. Dodatek uporaben in primeren predvsem za gornike, potapljače, jamarje, spremljanje svojih starejših članov družine itd.),
- **Senzor za padec telefona** (v primeru padca in 60 sekundne neodzivnosti se odda SOS sporočilo družinskim članom),
- **Video konferenca** med zdravnikom in ponesrečencem in/ali reševalcem,
- **iHELP aplikacija za ljudi s posebnimi potrebami** (gluhi in slepi).

iHELP aplikacija je povezovalni člen znotraj verige preživetja. Gradi jo paleta izvrstnih rešitev, poenostavitev ter odgovorov na mnoga vprašanja. Pa vendar potrebuje ljudi, reševalce kot tudi uporabnike, ki aplikaciji dajejo življenje. Ti so s svojim znanjem ter pripravljenostjo ali potrebo po pomoči osnovni gradniki mreže, ki s pomočjo iHELP aplikacije lahko pomagajo družini ali sočloveku oz. rešujejo življenja.

Skupina iHELP je pripravila t.i. beta verzijo aplikacije, ki jo bo moč preskusiti od maja do oktobra. Vaši nasveti, predlogi kot tudi vaša pomoč pri iHELP projektu so nadvse dobrodošli.

Pišite nam na naslov info@ihelp.si.
Več o projektu na spletni strani: www.ihelp.si

Skupaj rešujemo življenja!

Delovanje mobilne aplikacije

Dotik gumba na aplikaciji »testiraj aplikacijo« omogoča uporabniku, da le ta naredi test delovanja aplikacije, ki na ta način spozna delovanje aplikacije v primeru nujne pomoči.

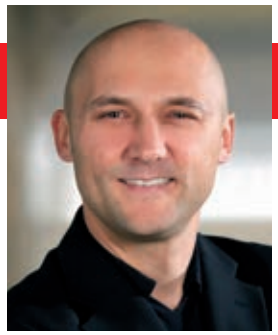
V situaciji, ko potrebujemo pomoč s pritiskom na gumb »NA POMOČ« aktiviramo iHELP mobilno aplikacijo (korak 1). Aplikacija nas vpraša: »Kdo potrebuje pomoč - **JAZ** ali NEKDO DRUG?«. Uporabnik izbere odgovor in pritisne na gumb »KLIČI 112« (korak 2). Poleg vzpostavitve povezave s številko 112, aplikacija avtomatsko pošlje tudi SOS sporočilo, družini, prijateljem, reševalcem in vsem iHELP uporabnikom aplikacije v radiju 300 metrov.

Ko iHELP uporabnik prejme SOS sporočilo in se nanj odzove, se mu na mobilnem telefonu prikaže zemljevid z vrisano lokacijo najbližjega defibrilatorja, lekarne, NMP, lokacijo ponesrečenca ter osnovni podatki o ponesrečencu (starost, spol in morebitne bolezni, vrsto zdravil, ki jih uži-

Viri

- Bardy GH, Lee KL, Mark DP et al. (2008). Home use of automated defibrillators for sudden cardiac arrest. N Eng J Med 17 (4): 1793-804.
- Koster WR, Baubin AM, Bossaert LL et al. (2010). Adult basic life support and use of automated external defibrillators. Resuscitation 81 (10): 1277-92.
- Nolan J, Soar J, Zideman AD et al. (2010). Executive summary. Resuscitation 81 (10): 1219-76.
- Ploj T, Gradišek P (2006). Uporaba avtomatičnega defibrilatorja. V: Ahčan U. Prva pomoč.1.izd. Ljubljana: Rdeči križ Slovenije, 76-80.
- Rajapakse R (2008). Seznanjenost prebivalcev Slovenije z znaki srčnega zastoja in temeljnimi postopki oživljanja. Magistersko delo. Ljubljana: Medicinska fakulteta.
- Uredba o organizaciji in delovanju sistema, opazovanja, obveščanja in alarmiranja. Uradni list RS št.: 45/97.
- Podberšič, M., Prenova sistema osebnega klica, UJMA št. 25, st. 166.
- Ocenjevalni list – točkovnik (Uradni list RS, 2007) ■

Avtor: Andrej Kovačič, dipl. varstvoslovec / Institut za korporativne varnostne študije*



VARNOST V SOSESKAH IN PREPREČEVANJE KRIMINALITETE

V mestih se pojavlja največ kaznivih dejanj in drugih varnostnih problemov. Ena od temeljnih pravic je, da živimo in delamo v varnem okolju. Žal pa varnost in svobodo ljudi v družbi ogroža kriminaliteta kot vsakodnevna stalnica in spremljevalka družbenih interakcij na vseh področjih človekovega bivanja.

Dejavniki, ki vplivajo na višjo stopnjo kriminalitete v urbanih okoljih so: zmanjšanje moči družbenega nadzorstva, socialna prikrajšanost in izključevanje, neprimerna gradnja, družinski problemi, kriza identitete in izguba povezanosti ljudi v soseskah. Kriminaliteto lahko opredelimo, kot družbeni fenomen in neposredno delovanje oziroma nedelovanje posameznikov ali naključnih oziroma organiziranih skupin in pojav, ki je prisoten v vseh družbenih skupnostih. Še posebej pa je za vse državljane zaskrbljujoče dejstvo, da kriminaliteta posega v same temelje demokratične družbe (ReNPPZK 2012–16). Zavedanje (ne)varnosti se v večini primerov začne takrat, ko smo že bili žrtve kaznivega dejanja, tako da je občutenje nevarnosti veliko večje, kot varnosti same. Pri tem gre za kazniva dejanja z elementi nasilja ter hujše oblike premoženjskih kaznivih dejanj, med katerimi najbolj izstopajo tatvine, vlomi in ropi. "Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016 spodbuja številne državne, zasebne in vse druge oblike institucionalnega delovanja družbe ter vsakega posameznika k povezovanju, sodelovanju, razmišljanju in uresničevanju zagotavljanja varnosti na vseh ravneh z ukrepi, ki v največji mogoči meri izhajajo iz realno zaznanih in ovrednotenih virov ogrožanja" (ReNPPZK 2012–16). V prispevku bom govoril o varnosti v soseskah in o vlogi, ki jo varnostni subjekti in mediji imajo oziroma bi jo dejansko morali imeti pri zagotavljanju varnosti in preprečevanju kriminalitete.

> Glede na statistične podatke o subjektivnem doživljanju varnosti prebivalcev dveh največjih mestnih občin v Sloveniji je kar zaskrbljujoče dejstvo, ki izvira iz podatkov slovenske policije, da se v deležu vseh izvršenih kaznivih dejanj, ki jih letno obravnava, povečuje delež tistih kaznivih dejanj, ki najbolj vplivajo na posameznikovo individualno doživljanje in zaznavo varnosti, tako glede osebne integritete, kot njegovega premoženja.

Vloga policije

V zadnjih letih, ko policija izvaja v skupnost usmerjeno policijsko delo je vse več priložnosti, da s sodelovanjem organiziranih skupin in posameznih državljanov pripomorejo k boljšim varnostnim razmeram. Pri tem gre za policijsko delo, ki temelji na dobrih stikih s predstavniki skupnosti in prebivalci v soseskah. Ena izmed nalog policije je tudi povezovalne narave in sicer med skupnostjo in ostalimi organizacijami. Vloga policije pri v sku-

*avtor je član Slovenskega združenja korporativne varnosti

pnost usmerjenem delu je strokovno svetovanje za uporabo različnih aktivnosti v smeri izboljšanja varnostnih razmer, prisluhniti željam in pobudam državljanov za izboljšanje varnosti, razreševanju konkretnih problemov ter seznanjati z varnostnimi razmerami in oblikami deviantnih pojavov (www.mnz.gov.si). Tovrstna sodelovanja prinašajo veliko pozitivnih učinkov na obeh straneh, čeprav ima policija zaradi svoje represivne vloge težjo nalogo, kot bi jo imela sicer.[1] ''Policisti lahko pomagajo pri identifikaciji problemov na določenih območjih, ugotovijo, kdo so posamezniki in skupine, ki povzročajo probleme in kdo so tisti, ki so pripravljeni pomagati policiji in pomagajo pri reševanju varnostne problematike'' (Meško, 2001). Pri zmanjševanju kriminalitete v urbanih okoljih imajo temeljno nalogo državni organi, ki izvajajo svoje naloge na lokalni ravni. Za preprečevanje kriminalitete in zagotavljanja varnosti v urbanih okoljih je potrebno zagotoviti dolgoročno partnersko sodelovanje na nivoju vseh občin v Sloveniji (Jevšek, 2007).

Vloga zasebnega varovanja

»Zasebno varovanje je varovanje ljudi in premoženja na varovanem območju, določenem objektu ali prostoru pred nezakonitimi dejanji, poškodovanjem ali uničenjem z varnostnim osebjem ter sistemi tehničnega varovanja« (www.mnz.gov.si). Za zagotavljanje boljše varnosti v soseskah imajo njeni prebivalci možnost, da najamejo varnostno službo, ki lahko izvaja varovanje s fizično prisotnostjo varnostnika, z obhodnim varovanjem ali varovanje s pomočjo video nadzora, s protivlomnimi sistemi, ipd. Varnostna služba s svojo prisotnostjo zmanjšuje možnosti kaznivih dejanj nad osebami in nad premoženjem. Varnostniki z izvajanjem obhodov skrbijo za red in varnost v soseskah ter s svojo prisotnostjo preprečujejo ogrožanje varnosti ljudi in lastnine. S tehničnim in fizičnim varovanjem se izvaja nadzor nad dostopom vozil v podzemne garaže in preprečuje morebitne tatvine avtomobilov, kot nastanek škode na in v vozilih. Neprekinjen način varovanja in prisotnost varnostnika zmanjšuje tveganje za kazniva dejanja in ostale kršitve v soseskah. Pri obhodnem varovanju gre za način izvajanja varovanja, kjer varnostna služba predvsem v kritičnih urah prihaja v sosesko, izvaja obhode in nadzira dogajanje ter pri ugotovljenih kršitvah ukrepa v skladu z navodili naročnika oziroma pooblastili, ki jih ima po Zakonu o zasebnem varovanju.

Vloga državljanskega samovarovanja

Policija, kot državni organ ne zmore sama zagotoviti takšne stopnje varnosti, ki bi bila sprejemljiva za večji del prebivalstva. Rešitev za to problematiko je tako mogoče iskati v samoorganiziranju prebivalcev sosesk, katerim ni vseeno za lastno varnost in varnost njihovega premoženja (Pečar, 1998). Na področju primarnega preprečevanja kriminalitete dajemo posebno pozornost dvema področjema. Pri prvem gre za preprečevanje kriminalitete z načrtovanjem in oblikovanjem okolja medtem, ko gre pri drugem za organizirano sosedsko opazovanje. Pri načrtovanju in oblikovanju okolja so pomembne tehnike za ustvarjanje tretjih pogojev storitve kaznivega dejanja, možnost za boljši nadzor med zgradbami in vhodi v zgradbe, zbujanje občutkov varnosti, gradnjo, kjer je boljša preglednost, kjer se uporabljajo dobre ključavnice in je ustrezna osvetljenost okolja (Meško, 2002). Pri drugem področju primarnega preprečevanja kriminalitete gre za prostovoljno udeležbo in prizadevanja državljanov za varnejšo skupnost. Takšen način organiziranja in preprečevanja kriminalitete s strani državljanov temelji na lastnih in sponzorskih sredstvih ter sposobnostih, kot na kadrovskih zmogljivostih pri uresničevanju programov. V teh prizadevanjih gre zato, da sosedje pomagajo drug drugemu in da izvajajo državljanski nadzor na območjih, kjer je moč pričakovati več kriminala. Z različnimi programi je na ta način mogoče povezati ljudi v soseskah ter tako razvijati odgovornost za lastno varnost, varnost sosedov in svojih bližnjih, kot za varnost nasploh. V svetu poznamo različne načine organiziranja državljanov, kot so Neighbourhood (crime) watch, crimestoppers in podobne, ki se ukvarjajo s preprečevanjem kriminalitete. Njihov namen je vzdrževati budnost prebivalcev v bivalnem okolju z nenehnim posredovanjem ustreznih informacij z namenom preprečevanja kriminalitete.

Vloga medijev

Pri preprečevanju kriminalitete imajo pomembno vlogo tudi mediji. V rednih TV in radijskih oddajah z varnostno tematiko, kjer bi strokovnjaki z varnostnega področja obravnavali izbrano problematiko, je mogoče osveščati državljane o varnosti, o samozaščiti in tako krepiti varnostno kulturo.

Problematiko, ki je povezana s kriminaliteto in z drugimi oblikami škodnih ravnanj najbolje poznajo in občutijo prebivalci sosesk, zato je le te potrebno spodbuditi k večjem sodelovanju.

V Slovenskem združenju za korporativno varnost in Inštitutu za korporativne varnostne študije se zavedamo, kako pomembno je ne samo varno poslovno okolje, temveč tudi okolje v katerem živimo. V ta namen pripravljamo raziskavo, s katero želimo med drugim ugotoviti, kaj občinske uprave dejansko naredijo za zagotavljanje varnosti svojih občanov, kakšnim inovativnim in varnostnim standardom sledijo, ali imajo zaposlenega strokovnjaka za varnost in ali imajo vzpostavljene varnostne sosvete na nivoju lokalnih skupnosti.

V medijih je mogoče poročati o vlogah varnostnih subjektov, o varnostnih sosvetih in prostovoljnih prizadevanjih državljanov za preprečevanje kriminalitete ter na ta način spodbuditi državljane k čim širšem sodelovanju in zavedanju pomena varnosti. Seminarje in ostala predavanja s področja varnosti je mogoče objaviti na internetu in na ta način omogočiti večini državljanov dostop do tovrstnega znanja in varnostnega osveščanja.

Zaključek

Način življenja v mestih se je v zadnjih letih zelo spremenil, gradijo se visoke ograje, slabo poznamo svoje sosede, ni občutka pripadnosti skupnosti in splošnega sodelovanja. Da bi dosegli čim višjo stopnjo varnosti v soseskah in v mestih nasploh, je naloga države in mestnih oblasti, da k preprečevanju kriminalitete privabijo čim večje število državljanov, da sprejmejo ustrezno zakonodajo[2] in da ustvarijo ostale osnovne pogoje[3] za bivanje. Ker je policija na eni strani represivni organ, na drugi strani pa se ji pripisuje povezovalne naloge, bi bilo v teh pogledih bolje, če bi te naloge na nivoju občin prevzele druge strokovne službe. Glavno vlogo v povezovanju vseh varnostnih subjektov, medijev in državljanov, ki želijo sodelovati za varnejšo skupnost bi morali prevzeti strokovnjaki za varnost v občinskih upravah. Temeljni cilj povezovanja in sodelovanja je preprečevanje kriminalitete ter zagotavljanje čim višje stopnje varnosti v soseskah in v mestih nasploh. Prihodnost tako kliče po uresničevanju in čim širšem partnerskem sodelovanju vseh omenjenih v varnostnih sosvetih. Še posebej pa bi k sodelovanju morali povabiti predstavnike mladih, da bi na ta način širili zavedanje o pomenu varnosti že v osnovnih in srednjih šolah ter fakultetah. Na ta način bi lahko dosegli uresničevanje ciljev in okoliščin, ki bi omogočile visoko raven individualnega in družbenega življenja ter zagotavljale življenje v varnem okolju za vse generacije. Iz povedanega velja, da bi moralo preprečevanje kriminalitete temeljiti na dejavnosti države in mestnih oblasti, na državljanskih in medijskih pobudah ter na njihovi krepitvi partnerskega sodelovanja.



Viri

- http://www.pro-vigil.com/2008/08/taking-neighborhood-security-to-the-next-level-10-strategies-for-community-security-organizers/ Pridobljeno 5.10.2012
- http://www.mnz.gov.si/si/mnz_za_vas/zasebno_varovanje_detektivi/zasebno_varovanje/ Pridobljeno 3.10.2012
- http//www.crimereduction.homeoffice.gov.uk. Pridobljeno 12.9.2012
- Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016. MNZ RS.
- Jevšek, A. (2007). Nacionalni program kriminalitetne politike. Revija Podjetje in delo; let. 33, št. 6/7, 2007, GV Založba, Ljubljana, 2007, str. 1613–1625.
- MEŠKO, G. (2002). Osnove preprečevanja kriminalitete. MNZ RS, Visoka policijsko-varnostna šola, Ljubljana, 2002.
- Meško, G.(2001). V skupnost usmerjeno policijsko delo – izzivi za slovensko policijo, Teorija in praksa, let. 38, 2/2001, str. 272-289.
- Pečar, J. (1998). Zasebno varovanje in samovarovanje v lokalni skupnosti. Urednik: Anžič, A. Zasebno varovanje in detektivska dejavnost. Visoka policijsko-varnostna šola. ■

1 Osebno mnenje avtorja članka.

2 Zaradi primerov, kjer se na glavni obravnavi v kazenskem postopku pričo "razgali" z vsemi osebnimi podatki, je iluzorno pričakovati, da bodo državljani množično želeli sodelovati pri preprečevanju kriminalitete. V izogib težavam zaradi pričanja se tako raje obrnejo stran ali pa v obravnavanih postopkih "izgubijo spomin".

3 Gre predvsem zato, da je gradnja novih sosesk pogosto z varnostnega vidika neustrezna, kot zaradi nedoseganja socialnega kapitala med ljudmi, ki ga je težko razviti, če ni prostorskih pogojev za skupna druženja prebivalcev v soseskah.

4. mednarodna konferenca

Dnevi korporativne varnosti

Upravljanje korporativne varnosti — novi pristopi in izzivi prihodnosti

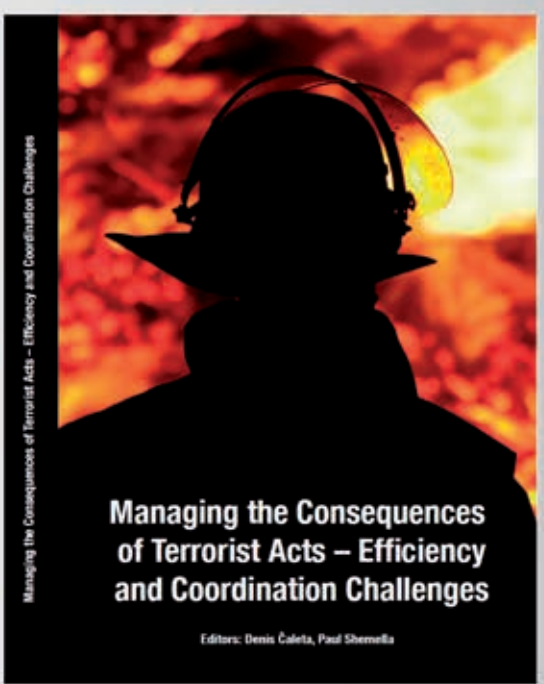
Ljubljana, 21.—22. marec 2013

ICS

Institute for Corporative Security Studies

Izšla je nova knjiga

Managing the Consequences of Terrorist Acts



www.ics-institut.si

Avtor: Peter Kotar / Univerzitetni diplomirani varstvoslovec*



PRILOŽNOSTI ZA POVEZOVANJE JAVNE IN KORPORATIVNE VARNOSTI

V današnjem času globalizacije in hitri rasti podjetij na širnih trgih po vsem svetu, je treba poleg poslovne uspešnosti nameniti tudi dobršen del truda za zagotavljanje varnosti.

Uvod

Varnost običajno pojmujemo kot stanje, kjer lahko posameznik uveljavlja svoje pravice in tudi dolžnosti, poenostavljeno pa lahko rečemo, da varnost predstavlja red. V zadnjem času varnost zagotavljajo različni subjekti tako javni kot korporativni. Ravno sodelovanje med slednjimi bo v prihodnosti zagotovo bistvenega pomena.

Javni sektor in javna varnost

Pojmujemo kot izraz, s katerim zajemamo vse javnopravne organizacije (ali osebe javnega prava). Javni sektor je torej celota vseh oseb javnega prava države in vseh drugih oseb javnega prava, ki jim država zagotavlja pravno subjektiviteto in določena pooblastila. V javnem sektorju se opravljajo javne funkcije, uresničujejo javni interesi in zadovoljujejo javne potrebe. Gre za tiste potrebe, interese in funkcije, glede katerih se sprejme odločitev, da jih bomo urejali kot javne zadeve na ravni državne ali lokalnih skupnosti. V demokratični državi je določitev kroga teh zadev rezultat demokratičnega procesa. Obseg javnih zadev in s tem razmejitev javne in zasebne sfere ni objektivno dana, ampak je stvar odločanja državne skupnosti. Obseg kroga javnih zadev se od države do države, v posameznih državah pa tudi od obdobja do obdobja razlikuje.

Javni sektor tako lahko definiramo kot skupek organizacij, ki opravljajo javne funkcije, izvajajo oblastni del javnega sektorja predvsem pa zagotavljajo javne službe oziroma javne storitve. Vse te organizacije delujejo v javnem interesu in zadovoljujejo javne potrebe.
Del tega javnega sektorja je tudi javna varnost, za katero lahko rečemo, da je del državne uprave, ki skrbi zlasti za osebno, premoženjsko, prometno varnost itd.

Korporativna varnost

Za korporativno varnost lahko rečemo, da ta v najobsežnejšem pomenu besede pomeni takšno dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Ravno zaradi tega je korporativna varnost ena izmed osnovnih funkcij za nemoteno delovanje podjetja, kot takšna pa se izvaja v stalnem tesnem sodelovanju z vsemi drugimi ključnimi funkcijami v podjetju. Celostno področje korporativne varnosti za ustrezno obvladovanje varnostnih tveganj nujno vključuje področje varnosti, procesa neprekinjenega poslovanja in varnosti pri delu (Čaleta, 2011).

Iz skupnega lahko ocenimo, da je korporativna varnost pogoj za uspešnost podjetja, zanjo pa ne skrbijo zasebne varnostne službe, kot si mnogi podjetniki zmotno predstavljajo. Danes je namreč vsako delovanje podjetja v zahtevnem globalnem okolju neposredno povezano z učinkovitim izvajanjem korporacijske varnosti. Z njo organizacija ali podjetje obvladuje in upravlja z varnostnimi in drugimi tveganji. Organizacije se pri svojem delovanju soočajo s celim nizom tveganj, ki jih lahko ločimo na zunanja tveganja, tveganja zaradi notranjih dejavnikov ter kombinacijo obeh. Kot večje nevarnosti lahko opredelimo odtekanje pomembnih informacij, nizko varnostno kulturo v organizaciji, nepotrebno malomarnost in podobno.

Sodelovanje obeh institucij bi v prihodnosti zagotovo pripomoglo k izboljšanju tako javne kot korporacijske varnosti, predvsem z izmenjavo podatkov o tveganjih in grožnjah s katerimi se dnevno srečuje posamezna stran.

*avtor je član Slovenskega združenja korporativne varnosti



Povezovanje javne in korporativne varnosti

Tako ena kot druga zagotavljajo določeno stopnjo varnosti na posameznih področjih – bodisi v javni upravi in javnem življenju, bodisi v organizacijah ali korporacijskih družbah. Za obe lahko z gotovostjo trdimo, da svoje poslanstvo opravljajo na podlagi predvidenih varnostnih tveganj za katerih obvladovanje uporabljajo dokaj podobne metode dela. Obvladovanje varnostnih tveganj je eden od bistvenih predpogojev za doseganje odličnosti in konkurenčnosti, kot dejavnikov, ki sta še posebno izpostavljena v poslovno-ekonomskem okolju.

Medsebojno sodelovanje bi moralo dejansko stremeti k dvigovanju zavedanja o potrebnosti obvladovanja varnostnih tveganj in tako prispevati k pospeševanju vlaganj v slovenski javni upravi na področju zagotavljanja varnosti, kar ima posredni in neposredni vpliv na povečanje učinkovitosti organov javne uprave, kvalitetnega zagotavljanja nalog usmerjenih k zadovoljevanju potreb države, lokalne skupnosti in vsakega posameznega uporabnika.

Ob mednarodni pravni primerjalni analizi je opaziti temeljno značilnost, ki se nanaša na prisotnost ali odsotnost vpliva lokalnih skupnosti na zagotavljanje varnosti. Določen vpliv v obliki sodelovanja v različnih posvetovalnih telesih policije obstaja v zelo veliko državah, pristojnost organiziranja institucionaliziranih lokalnih instrumentov zagotavljanja varnosti pa imajo pretežno lokalne skupnosti v decentraliziranih državah (npr. Franciji, Italiji), medtem ko v federalnih državah (Nemčija, Avstrija) lokalna skupnost praviloma ne organizira lastnih varnostnih služb. Tradicionalno pomembno vlogo pa imajo lokalne varnostne službe v državah tako imenovanih anglosaksonskih državah, zlasti Združenem kraljestvu Velike Britanije in Združenih državah Amerike. V državah, kjer lokalne varnostne službe sicer niso del varnostne tradicije, se zaradi vedno novih varnostnih izzivov ukvarjajo s temi vprašanji.
V Sloveniji so posamezne občine sprejele Občinske programe varnosti, kateri so razvojno zasnovani in imajo hkrati dovolj konkretno naravo priporočil in programskih smernic. Eden od glavnih namenov Občinskih programov varnosti je dvig varnostne kulture vseh tistih, ki se tako ali drugače srečujejo z varnostnimi problemi in vprašanji in so v okviru svojih pristojnosti odgovorni za varnost, cilj pa je tudi spodbuditi vse druge, ki jim je posamezna občina dom ali poslovni oziroma drugi center, k samozaščitnemu varnostnemu ravnanju.

Zaključek

Kot sem že omenil, je danes varnost dobrina, ki si jo želi imeti vsak posameznik. Koliko vsak naredi sam zase, za doseganje določene stopnje varnosti je drugo vprašanje. Po lastnih izkušnjah, dostikrat storimo premalo ali celo nič. V kolikor takšno (ne) aktivnost prenesemo v organizacijo, kjer smo zaposleni in se ne čutimo poenoteni z njeno vizijo in delom v prihodnje, to lahko pomeni določeno varnostno tveganje, katero lahko pripelje do najhujših posledic.

V zadnjem času je zavedanje o določenih varnostnih problemih na višjem nivoju. Razlog takšnemu zavedanju je gotovo tudi ustanavljanje različnih strokovnih institucij, ki se s svojim delom trudijo pri spodbujanju razvoja celovitih varnostnih procesov na področju korporativne varnosti, ki neposredno vplivajo na obvladovanje tveganj v poslovnih, razvojnih, gospodarskih, javnih in drugih okoljih.

Strokovno povezovanje različnih varnostnih subjektov zagotovo pripomore k večji stopnji zagotavljanja varnosti kljub predvidenim tveganjem, ki se v posameznih okoljih pojavljajo. Izmenjava izkušenj, usposabljanja, izobraževanja predvsem pa sodelovanja so tista, ki so v današnji družbi ključnega pomena, da se lahko v celoti brez skrbi »ponoči sprehodimo tako po osvetljenih kot tudi neosvetljenih ulicah.« ■

Avtor: doc. dr. Boštjan Aver / GEA College*



OBVLADOVANJE FINANČNIH TVEGANJ

Vodstvo podjetja je odgovorno za zagotovitev spremljanja tveganj, katerim je podjetje izpostavljeno pri poslovanju. Tako se danes gospodarske družbe vsakodnevno srečujejo s tveganji in jih morajo z ustreznimi ukrepi, predvsem notranjimi kontrolami, tudi čim bolj obvladovati.

Podjetja morajo neprestano nadgrajevati sistem upravljanja s tveganji. Vedno bolj se poudarja natančna opredelitev odgovornosti organizacijskih enot (OE) podjetja in posameznih zaposlenih. Zato mora sprejeti ustrezne ukrepe za obvladovanje tveganj. Vodstvo mora zagotoviti tudi organizacijo sistema notranjih kontrol na vseh področjih poslovanja podjetja. Namen tega prispevka je prikazati osnove obvladovanja finančnih tveganj podjetja.

Finančna tveganja

Med finančna tveganja uvrščamo predvsem tržna tveganja, med katera uvrščamo likvidnostno, trgovalno, valutno in obrestno tveganje.

Tržno tveganje je tveganje, ki izvira iz negotovosti zaradi sprememb v vrednosti ali likvidnosti finančnih naložb in se odrazi kot strukturna neusklajenost bilance stanja podjetja. Tako je priporočljivo, da podjetje dnevno, tedensko ali mesečno ugotavlja njegovo izpostavljenost likvidnostnemu, trgovalnemu, valutnemu in obrestnemu tveganju.

Likvidnostno tveganje je tveganje, da podjetje ob zapadlosti obveznosti ne bo sposobno poravnati teh obveznosti. Zato je potrebno vzpostaviti model likvidnosti, kjer npr. vsa sredstva in vse vire sredstev razporedimo v razrede glede na zapadlost (do 1. meseca, od 1. do 3. mesecev, od 3. do 6. mesecev itd.).

> Tudi na področju obvladovanja finančnih tveganj podjetja mora vodstvo vzpostaviti najpomembnejše notranje kontrole.

Pri tem lahko uporabimo kot mero likvidnosti npr. količnik likvidnosti, ki meri razmerje sredstva / viri sredstev po razredih zapadlosti. Vodstvo podjetja nato postavi limit (ali več limitov), kot npr. minimalna vrednost količnika likvidnosti posameznega razreda zapadlosti.

Trgovalno tveganje je tveganje, da se spremeni vrednost podjetja zaradi njegovih naložb v lastniške vrednostne papirje, in sicer zaradi volatilnosti oz. spremenljivosti cen vrednostnih papirjev, tako lastniških kot tudi dolžniških ali izvedenih. Zato je dobro postaviti model tržnega VaR-a (»Value at Risk«) oz. model tvegane vrednosti, ki na podlagi volatilnosti cen vrednostnih papirjev, korelacije teh volatilnosti ter določenih vrednosti parametrov modela (stopnja zaupanja, dnevi likvidacije papirjev, dolžina časovne vrste), izračuna največjo pričakovano izgubo zaradi sprememb cen vrednostnih papirjev. Nato vodstvo podjetja lahko postavi skupen VaR limit.

Valutno tveganje je tveganje, da se spremeni vrednost podjetja zaradi odprtosti v tujih valutah in volatilnosti tečajev teh valut. Dobro je postaviti model valutnega VaR-a (»Value at Risk«) oz. tvegane vrednosti, tj. statistični model, ki na podlagi volatilnosti deviznih tečajev, korelacije teh volatilnosti ter določenih vrednosti parametrov modela (stopnja zaupanja, dnevi zaprtja pozicije, dolžina časovne vrste), izračuna največjo pričakovano izgubo zaradi sprememb deviznih tečajev.Postavi se lahko skupen VaR limit (za vse valute skupaj) ali posamezen VaR limitza posamezno valuto.

Obrestno tveganje je tveganje nastanka finančne izgube zaradi neenakega prilagajanja sredstev in virov sredstev podjetja tržnim obrestnim meram (razmerje med ročnostjo in fiksno/spremenljivo obrestno mero). Podjetje ali finančna institucija ima možnost razviti npr. model zapadlosti, model trajanja ali model repricing, kot ga uporabljajo tudi številne poslovne banke.

Tudi na področju obvladovanja finančnih tveganj podjetja mora vodstvo vzpostaviti najpomembnejše **notranje kontrole**, kot so jasna opredelitev odgovornosti posameznih organizacijskih enot in posameznih delavcev, razmejitev nezdružljivih nalog (na primer razmejitev odobravanja naložb od evidentiranja naložb,...), vzpostavitev po-

*avtor je član Slovenskega združenja korporativne varnosti



ročanja po hierarhiji, potrjevanje transakcij, dokumentiranje transakcij in dogodkov, arhiviranje...

Področna politika obvladovanja finančnih tveganj

Finančna tveganja so nedvomno tista tveganja, s katerimi so povezane največje potencialne izgube.Vodstvo podjetja je odgovorno, da je pregled posamezne vrste finančnih tveganj strukturiran tako, da so najprej podani opis in posledice posameznega tveganja, nato sledi poglavje o prioriteti in zadolženosti v zvezi s posameznim tveganjem. Pomembni so seveda **ukrepi**, ki so oz. bi jih bilo potrebno uvesti, da bi se posamezno finančno tveganje učinkovito obvladovalo.

Tveganje zunanjega okolja

Opis in posledice: S tveganjem zunanjega okolja v prvi vrsti mislimo na spremembe cen vrednostnih papirjev zaradi spremenljivih gospodarskih razmer, poslovanja podjetij, inflacije, obrestnih mer, deviznega tečaja in zakonodaje. Večja kot je spremenljivost cen vrednostnih papirjev, večje je tveganje povezano z naložbo. Sama spremenljivost cen je sicer pomembna, vendar je z vidika, kako tvegana je posamezna naložba, nikoli ne smemo gledati v izolaciji od ostalih naložb v portfelju podjetja. Tveganje portfelja podjetja ni odvisno samo od tveganja posameznih naložb podjetja, temveč nanj vpliva korelacija, ki vlada med posameznimi naložbami v portfelju. Tveganje sprememb cen naložb se meri z mero VaR (»Value at Risk«), ki meri največjo možno izgubo vrednosti portfelja podjetja na podlagi pretekle volatilnosti cen z določeno stopnjo značilnosti v določenem časovnem intervalu.

Prioriteta in zadolženost: Skrbništvo nad tem tveganjem naj bi imela OE odgovorna za finance in naložbe podjetja. Nanj močno vpliva tudi likvidnostna situacija podjetja. V primeru, da je likvidnost dobro načrtovana, da so denarni tokovi znani, lahko poiščemo boljše naložbe, poleg tega pa tudi ne prihaja do situacije, da smo prisiljeni v prodajo naložb, ki jih ne želimo prodati.

Ukrepi za obvladovanje tveganja:

- priprava **naložbene politike podjetja** (cilji: ciljna donosnost, tveganje, likvidnost, čas nalaganja, davčni okvir, zakonske omejitve, izredne okoliščine);
- dnevno **spremljanje makroekonomskega okolja** in temu primerno **prilagajanje predvsem taktike** pri nalaganju sredstev podjetja;
- spremljanje **gibanja obrestnih mer**;
- spremljanje **gibanja deviznih tečajev**;
- **izdelava modelov VaR** za ugotavljanje največje možne izgube, ki jo ob predpostavki pretekle volatilnosti lahko utrpi podjetje v različnih časovnih obdobjih (dnevno, mesečno, letno).

Tveganje neusklajenosti virov in sredstev podjetja (valutno, vrednostno)

Opis in posledice: (Ne)usklajenost naložb podjetja z viri (vrednostno) je potrebno spremljati vsaj mesečno. Druga usklajenost je valutna usklajenost, kar pomeni, da mora podjetje imeti čim večji % vseh naložb v enaki valuti, kot so njegove obveznosti. Valutno tveganje je tveganje, da se vrednost naložb zmanjša zaradi depreciacije valute, v kateri je denominirana določena naložba.

Prioriteta in zadolženost: Posebno pozornost je sicer potrebno posvečati višini virov in naložb še posebej pri bolj izvozno usmerjenih slovenskih podjetij. Zadolženost za upravljanje teh vrst tveganja je na strani OE odgovorne za finance in naložbe podjetja.

Ukrepi za obvladovanje tveganja: Ukrepi za obvladovanje teh tveganj so povezani zgolj **s spremljanjem in poročanjem v zvezi s tem valutnim tveganjem.**

Tveganje neusklajenosti virov in sredstev podjetja (likvidnostno in obrestno tveganje)

Opis in posledice: **Likvidnostno tveganje** je opredeljeno kot tveganje, da podjetje ne more poravnati zapadlih obveznosti takrat, ko le-te zapadejo. Posledično se zmanjša kredibilnost podjetja, družba mora plačati zamudne obresti. Z namenom reševanja tekoče likvidnosti je podjetje lahko prisiljeno tudi v prodajo naložb v trenutku, ko to ni optimalno oz. pod slabšimi pogoji. Likvidnostnemu tveganju se lahko s pravilnim nalaganjem v naložbe z ustrezno ročnostjo v določeni meri izognemo.

Prioriteta in zadolženost: Likvidnostno tveganje je eno izmed najbolj pomembnih tveganj, s katerimi se soočajo danes podjetja. Prioriteta je v večini primerov najvišja. Skrbnik nad tveganjem naj bi bilaOE za finance in naložbe podjetja, vendar pa odgovornost nosijo tudi drugi sektorji, službe.



Upravljanje z likvidnostjo bi morala postati aktivnost, ki bi vključevala več udeležencev iz najrazličnejših OE, če bi želeli povečati učinkovitost upravljanja s sredstvi. V preteklosti je bilo predvsem pomembno, da je bila ročnost naložb usklajena. Ugotavljanje trajanja obveznosti in naložb je zadnja leta postalo zelo pomembno.

Ukrepi za obvladovanje tveganja: Prvi ukrep za obvladovanje likvidnostnega tveganja je **dobro planiranje likvidnosti** podjetja (letno, mesečno, tedensko in dnevno). Upravljanje z likvidnostjo sodi med najbolj pomembne naloge podjetja. Pri planiranju likvidnosti podjetja si je treba pomagati s primerjavo trenutnega kumulativnega stanja odlivov v določenem mesecu s stanjem odlivov v predhodnih mesecih ter na tej podlagi in na podlagi izkušenj oceniti dejanske odlive podjetja v tekočem mesecu.

Dobro je izdelovati **plan odlivov** podjetja(tedensko, mesečno, trimesečno). Pravilnost plana bi se preverjala z izdelavo analiz, ki bi pripomogle (ko bi razpolagali z zgodovinskimi podatki) k boljšemu napovedovanju odlivov podjetja. Večino odlivov za obratovanje podjetja je težko napovedovati. Najboljši način bi bil, da se bi takoj ob prejemu računa v podjetje valuta računa in vrednost vnesla v sistem, iz katerega bi OE za finance in naložbe črpal podatke za likvidnost. Prilivi podjetja pa so običajno odvisni od števila kupcev, datumov plačil terjatev in discipline plačevanja kupcev. Zato bi podjetje moralo izdelovati svoj **letni** in **mesečni plan prilivov**.

Podjetje torej mora izdelati **mehanizem za napovedovanje** prilivov in odlivov posameznih organizacijskih enot. Vse z namenom lažjega upravljanja z likvidnostjo in zmanjšanja sredstev (varnostnih rezerv za potrebe likvidnosti), ki so obrestovana po nižjih obrestnih merah. Na tej osnovi je treba pripraviti dnevne, tedenske, mesečne in letne **plane likvidnosti**.

Poleg zgoraj navedenega je koristno tudi:

- sprejeti **strategijo za upravljanje z likvidnostnim tveganjem**;
- sprejeti **politiko** za upravljanje z likvidnostnim tveganjem;
- **delovanje likvidnostne komisije**, ki se dnevno sestaja (nadzor);
- **vzpostavitev informacijske podpore**, ki omogoča ažurnost, točnost in popolnost podatkov.

Do **obrestnega tveganja** lahko pride, če so naložbe in viri z vidika ročnosti neusklajeni. Podjetje lahko meri razmike za posamezne segmente (vrste) obrestnih mer, ki kažejo, kateri razredi ročnosti so neizravnani. Izračun kratkoročnega (v obdobju enega leta) vpliva spremembe obrestnih mer na neto obrestne prihodke podjetja kaže, da zvišanje/znižanje obrestnih mer v vseh opredeljenih segmentih zvišuje/znižuje neto obrestne prihodke. Podjetje lahko ugotavlja tudi, v katerem segmentu obrestnih mer je najvišja obrestna občutljivost in ocenjuje učinke spremembe obrestnih mer (za npr. 1 odstotno točko) na neto obrestne prihodke podjetja.

Podjetje ali finančna institucija lahko mesečno ugotavlja tudi obrestni razmik za posamezne vrste obrestnih mer na zadnji dan v mesecu, tj. tveganje refinanciranja.Tveganje refinanciranja prikazuje izpostavljenost družbe učinkom spremembe obrestnih mer na neto obrestne prihodke glede na obdobje uskladitve obrestnih mer naložb in virov novemu nivoju obrestnih mer.

Občutljivost tržne vrednosti naložb in obveznosti na spremembo obrestnih mer na zadnji dan v mesecu se lahko računa na podlagi modela trajanja (»duration model«).Na podlagi ocene občutljivosti tržne vrednosti naložb in virov na spremembo obrestnih mer ugotavljamo spremembo tržne vrednosti sredstev (aktive) in virov sredstev (pasive) zaradi spremembe obrestne mere. ■

Slovensko združenje korporativne varnosti

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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

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

Ugodnosti za člane združenja:

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

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

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

SKUPAJ SMO MOČNEJŠI!

Avtor: dr. Boštjan Delak / samostojni svetovalec v podjetju ITAD, revizija in svetovanje, d.o.o,[1]



(NE)VARNOSTI RAČUNALNIŠTVA V OBLAKU

Računalništvu v oblaku je nova nastajajoča oblika storitve za zagotavljanje informacijskih sistemov (IS), infrastrukture in virov v okviru informacijske komunikacijske tehnologije (IKT). Namesto da se s programsko opremo izvaja in upravlja podatke na namiznih računalnikih ali strežnikih, uporabniki lahko za izvedbo aplikacij in dostopov do svojih podatkov na zahtevo uporabljajo storitve iz oblaka kjerkoli na svetu.

Uvod

Preko interneta lahko uporabniki izkoristijo skoraj neomejeno paleto računalniških virov in različnih ravni storitev računalništva v oblaku (v nadaljevanju - oblak). To so nekatere prednosti, ki jih nudi ta storitev. V prispevku bodo predstavljene še druge, vendar ima vsaka stran dve plati. Nova storitev ima tudi slabosti, ki so prav tako navedene v tem prispevku.

V prvem delu prispevek predstavlja nove zmogljivosti informacijskih sistemov in nekatere svetovne perspektive o prihodnosti teh smernic. V drugem delu prispevek opisuje zunanje izvajanje IKT, odgovornost poslovodstva in skladnost s korporativno varnostjo. V tretjem delu prispevek predstavi pomembnosti pri odločitvah o uporabi storitve oblaka, nato sledi opis varnostnih kontrol in možnih revizij. V zaključku pa prispevek predstavi nasvete potencialnim uporabnikom ob prehodu na take storitve, ki omogočajo upravljanje, obdelavo in hrambo podatkov v oblaku.

Kaj je to računalništvo v oblaku?

Oblak je novo nastajajoča platforma za zagotavljanje infrastrukture IS in sredstev IS ter IKT storitev. Lahko ga opišemo kot trend v praksi IKT in tudi v znanstvenih računalniških krogih, ki ima potencial, da korenito spremeni način izdelave aplikacij IKT in storitev IKT v smislu sestave, upravljanja in dobavljanja. Izraz »oblak« je nastal v letu 2006 in od takrat je bilo veliko različnih definicij. Ena od razlag terminologije oblaka je (NIST, 2011):
»Računalništvo v oblaku je slog računalništva, pri katerem so dinamično razširljiva in pogosto virtualizirana računalniška sredstva na voljo kot storitev preko interneta«.

Model oblaka je sestavljen iz petih značilnosti:
Širok mrežni dostop - računalniške zmogljivosti so dostopne skozi mehanizme, ki podpirajo različne odjemalce, kot so delovne postaje, prenosniki, mobilni telefoni in tablice.

Oblak je novo nastajajoča platforma za zagotavljanje infrastrukture IS in sredstev IS ter IKT storitev.

Samopostrežba na zahtevo - uporabnik se lahko samostojno odloči za zakup informacijskih zmogljivosti, glede na trenutne potrebe brez dodatne komunikacije s posameznimi ponudniki storitev.

Združevanje sredstev – poleg klasične virtualizacije oblak uporablja tudi zmožnosti avtomatizacije in sobivanja na istih informacijskih virih.
Visoka elastičnost – uporabnik lahko za svoje trenutne potrebe hitro poveča ali zmanjša obseg zakupljenih informacijskih virov.

Plačilo na osnovi uporabe – oblak avtomatično nadzira in optimizira vire in opravi obračun glede na uporabo.
V oblaku poznamo tri osnovne storitvene modele in sicer:

- *Infrastruktura kot storitev* (IaaS – »Infrastructure as a Service«),
- *Platforma kot storitev* (PaaS – »Platform as a Service«) in
- *Programska oprema kot storitev* (SaaS – »Software as a Service«).

Poleg treh osnovnih storitvenih modelov so se v zadnjem času razvile tudi njihove različice (Riedl, Letmeister, Böhm and Yetton, 2010).

Izvedbeni modeli oblaka so naslednji:
Javni oblak (»Public Cloud«) je dosto-



pen javnosti in ni omejitev glede tega, kdo storitve lahko uporablja. Preko interneta lahko do storitev ponudnika dostopa kdorkoli.
Zasebni oblak (»Private Cloud«) je dostopen samo v zasebnem omrežju. Storitve kot tudi infrastruktura so pod nadzorom ponudnika.
Oblak skupnosti (»Community Cloud«) je dostopen omejenemu številu uporabnikov, vezanih na skupnost.
Hibridni oblak (»Hybrid cloud«) so storitve v oblaku, ki so sestavljene iz storitev javnega in zasebnega oblaka. Kot vsaka novost tudi oblak sproža veliko konceptualnih, tehničnih in upravljavskih vprašanj, ki jih morajo obravnavati tako akademiki kot praktiki. Oblak nudi številne prednosti, med katerim je morda najbolj zanimiva prednost v prihranku v naložbe lastne infrastrukture IKT. Obstajajo pa tudi slabosti, s katerimi pa so najpogosteje povezana tudi določena tveganja. Z večino tveganj se srečamo pri vsakem zunanjem izvajanju računalniških storitev.

Kaj je to zunanje izvajanje IKT?

Slovenski terminološki slovar informatike (iSlovar, 2012) opredeljuje zunanje izvajanje (»outsourcing«) kot »*pogodbeno izvajanje opravil pri zunanjih, praviloma stroškovno ugodnejših izvajalcih*«. Dodeljevanje storitev zunanjega izvajanja tudi v Sloveniji dosega vedno večji razmah. Organizacije se vse pogosteje odločajo za zunanje izvajanje dela storitev ali celo vseh storitev IS tudi zaradi racionalizacije stroškov. S prenosom dela ali celotne podpore IS se organizacije srečujejo z novimi težavami in pastmi, predvsem pa s tveganji. Obstaja več definicij tveganj, med drugimi tudi: »*Verjetnost ali nevarnost za nastanek škode. Poškodbe, izgube, kršenja obveznosti ali kakšen drug negativen dogodek, ki ima zunanje ali notranje vzroke in ga je mogoče nevtralizirati z zaščitnimi akcijami*«.

Pred tveganji, povezanimi z zunanjim izvajanjem, se mora vsaka organizacija primerno zaščititi, za kar se uporablja več mehanizmov: primerne pogodbene obveze, izvedbe analiz tveganj in redna preverjanja nivoja varnosti zunanjega izvajalca s pomočjo pridobivanja zagotovil o ustreznem delovanju varnostnih kontrol.

Še posebej moramo biti pozorni, če zunanjemu izvajalcu posredujemo v obdelovanje osebne podatke, med katere podatke štejemo vse podatke, ki se nanašajo na posameznika, ne glede na obliko, v kateri so predloženi (npr.: rojstni datum, naslov, številka vozniškega dovoljenja, številka socialnega zavarovanja, davčna številka, EMŠO[2], IP naslov, itd).

Pri zunanjem izvajanju IKT mora obdelovalec osebnih podatkov spoštovati določbe varstva osebnih podatkov, ki veljajo za glavnega pogodbenega obdelovalca in za vse njegove podizvajalce. Odgovornosti upravljavca varstva osebnih podatkov ni mogoče prenesti na pogodbenega obdelovalca, mora pa biti vključeno določilo o nadzoru upravljavca nad izvajanjem določil zavarovanja osebnih podatkov pri pogodbenem obdelovalcu in vseh njegovih podizvajalcih. Prenos izvajanja IKT na zunanjega izvajalca – pogodbenega obdelovalca, ima zelo pomembne in usodne posledice na poslovanje celotne organizacije in mora biti v skladu s korporativno varnostjo.

Varovanje informacij – izziv za storitve v oblaku

Varovanje informacij postaja eno od najbolj pomembnih pravnih vprašanj, s katerimi se danes soočajo podjetja. Zaskrbljenost glede varstva zasebnosti posameznika, občutljivih osebnih podatkov, varnosti poslovnih podatkov, verodostojnosti in celovitosti poslovnih podatkov zahteva uveljavitev novih zakonov in predpisov, ki bodo zagotovili, da bodo podjetja ustrezno obravnavala varnost lastnih podatkov in podatkov, ki so jim zaupani v upravljanje. Obstaja več virov obveznosti za izpolnitev varnostnih zahtev: zakoni in podzakonski akti, skupne pravne obveznosti, pravila o dokazovanju, industrijski standardi, pogodbene obveznosti ter dobre prakse. Ti viri zajemajo osebne podatke, večino drugih poslovnih podatkov in vse digitalne zapise. Za ustrezno obvladovanje varovanja informacij skrbi korporativna varnost.

Ne glede na različne metodologije upravljanja s tveganji se vedno vključujejo: ocena ključnih poslovnih sredstev, potencialne grožnje, šibke točke oziroma ranljivosti IKT in ukrepi, ki lahko zmanjšajo tveganja na sprejemljivo raven. Med ključnimi varnostnimi vprašanji v zvezi z oblakom so:

zaupnost in segregacija, zasebnost, zaupanje, identiteta, skladnost, prenosljivost in interoperabilnost, zanesljivost in prožnost, preglednost in možnost upravljanja. Kot opisuje CSA[3] (2009), se varnostni nadzor v oblaku ne razlikuje od varnostnega nadzora v vseh okoljih IKT, oziroma se ne razlikuje od nadzora, ki ga imamo ob zunanjem izvajanju IKT.

Vsi se moramo zavedati tveganj, povezanih z oblakom. Vedeti moramo, da odgovornosti nad podatki in s tem povezanih varnostnih kontrol ni mogoče preseliti z »zemlje« na »oblak« oziroma na zunanje izvajalce.



Kontrola – revizija IKT storitev v oblaku

Kdorkoli se je že v praksi srečal z revizijo IS, ve, da je to zahtevna in odgovorna naloga. S tem ko organizacija del storitev IS ali celoto preda v pogodbeno obdelovanje zunanjemu izvajalcu, postane revizija IS še kompleksnejša. ISACA[4] je pripravila ustrezne standarde in smernice za izvedbo aktivnosti revizije IS, ki jih preizkušeni revizorji IS uporabljamo pri svojih aktivnostih. Za revizijo IS storitev v oblaku so pripravili tudi poseben program (ISACA, 2010).

Urad informacijske pooblaščenke v Sloveniji je skupaj z izkušenimi strokovnjaki za IS in varovanje informacij, iz Cloud Security Alliance Slovenija Chapter, Slovenskega inštituta za revizijo – slovenskega odseka ISACA, Zavoda e-Oblak in Euroclud Slovenia (2012), pripravil zelo koristen dokument Varstvo osebnih podatkov & računalništvo v oblaku, ki vsebuje tudi kontrolni seznam za preverjanje skladnosti z obstoječimi zahtevami zakona o varstvu osebnih podatkov.

Na medmrežju najdemo vrsto svetovalnih organizacij za to področje, pogosti so webinarji na to temo, različna podjetja pa nudijo razne študije in opise, ki jih dnevno preko elektronskih kanalov posredujejo uporabnikom in naročnikom. V medijih se pojavljajo reklame in ponudbe različnih slovenskih in drugih globalnih podjetij, ki nudijo različne storitve v oblakih. Kdorkoli razmišlja o prehodu na te storitve, mora imeti v mislih, da je odgovornost za podatke njegova in da te odgovornosti ni moč prenesti na zunanjega izvajalca.

Priporočila

Kadar načrtujemo selitev ali zunanje izvajanje aktivnosti naših IS v oblak, moramo imeti v mislih vprašanja skladnosti. Predlagam, da organizacija upošteva naslednje avtorjeve predloge:

- zaščitite podatke s šifriranjem;
- opredelite lokacijo za shranjevanje in obdelavo vaših podatkov v pogodbi s ponudnikom storitve oblaka z zavezo, da vas obvešča o svojih načrtih za prihodnost (na primer: potencialne združitve, prevzemi itd);
- ponudnik mora vzpostaviti, izvajati in ustrezno nadgrajevati načrt neprekinjenega poslovanja v državi EU;
- preverite pri ponudniku možnost pridobitve dnevniških zapisov o dostopu do podatkov in njihovi obdelavi (bodisi brez dajatev ali s posebno pristojbino) v zahtevanem časovnem okviru in v skladu z zakonskimi zahtevami;
- zahtevajte od ponudnika, da vam posreduje informacije o obdelavi osebnih podatkov;
- poskrbite, da boste dobili vsa redna in izredna poročila revizij IS pri ponudniku;
- izogibajte se posredovanju, hranjenju in obdelavi osebnih podatkov v javnih in hibridnih oblakih.

Zaključek

Vloga zunanjega izvajanja IS se drastično spreminja in se bo še bolj v prihodnje, ko se bodo podjetja še v večjem številu odločala za oblake in bodo imela vedno več poslovnih procesov podprte s takimi storitvami. ISACA (2009) navaja, da je oblak vsekakor pripravljen zagotoviti številne koristi. Prinesel bo novo obdobje uporabe IS v podjetjih, kar bo privedlo do pomembnih in velikih sprememb v poslovanju podjetij ter IKT. Strokovnjaki, tako poslovni kot tudi IKT, bodo morali odgovoriti na zgornje dileme, ko bodo načrtovali strategijo in taktične načrte shranjevanja, obdelovanja in upravljanja poslovnih in osebnih podatkov v oblaku. Dejavnosti upravljanja s tveganji je potrebno izvajati v celotnem življenjskem ciklu informacije. Tveganja pa je potrebno redno ocenjevati, še posebej ob vsakih spremembah.

Podjetjem, ki razmišljajo, da bi prenesle podatke (lastne poslovne in tudi osebne podatke zaposlenih in njihovih strank) v oblak, svetujem, da si pomagajo z navedenim kontrolnim seznamom za preverjanje skladnosti, vključijo svetovalce s pravnega področja za pregled osnutka pogodbe in dogovora o izvajanju ravni storitve (SLA – Service Level agreement), prav tako naj vključijo tudi izkušenega revizorja IS,

Strokovnjaki za varovanje informacij morajo opraviti analize vpliva na poslovanje in oceno tveganja ter seznaniti z ugotovitvami vodilne v podjetjih oziroma tiste, ki se odločajo o novih usmeritvah.



da jim svetuje pri odločitvah. Še prej pa naj pridobijo od ponudnika storitve oblaka izjavo, kje se bodo nahajali njihovi osebni podatki, ter preverijo lokacije s seznamom, ki jih potrjuje državni nadzorni organ. Prav tako naj zahtevajo, da jih bo ponudnik storitve oblaka ustrezno ter vnaprej obveščal o spremembah lokacije hranjenja njihovih podatkov. V pristopnih pogajanjih naj si tudi zagotovijo redno seznanjanje in vpogled v revizijska poročila IKT, ki jih izvajajo tretje osebe na ponudnikovem oblaku.

Viri

- CSA. 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, Cloud Security Alliance;
- Informacijski pooblaščenec & Cloud Security Alliance Slovenia Chapter, Slovenski inštitute za revizijo – Slovenski odsek ISACA, Zavod e-Oblak, Eurocloud Slovenia. 2012 Varstvo osebnih podatkov & računalništvo v oblaku, https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf (dne 23.10.2012)
- ISACA, 2009. *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspective.* ISACA, An ISACA Emerging Technology White Paper
- ISACA, 2010. *Cloud Computing Management Audit /Assurance Program,* ISBN 978-1-60420-162-8
- iSlovar – Slovenski terminološki slovar informatike (www.islovar.org) (dne 17.10.2012)
- NIST, 2011. Definition of Cloud Computing,
- Riedl, C., Letmeister, S., Böhm, M and Yetton, P. 2010, *Competing in the Clouds: A Strategic Challenge for ITSP Ltd.*, Communications of the Association for Information Systems, Vol. 27, No. 1, Article 40, http://aisel.aisnet.org/cais/vol27/iss1/40 (dne 17.10.2012) ■

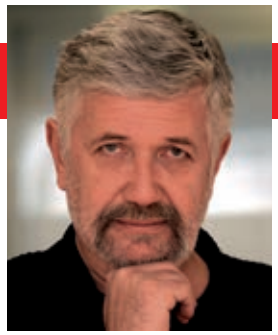
[1] Ustanovna članica Sekcije upravljanja varovanja informacij pri Območni Zvezi Ljubljana, Gospodarske zbornice Slovenije.

[2] EMŠO – Enotna matična številka občana

[3] CSA – »Cloud Security Aliance«

[4] ISACA – Information System Audit and Control Association

Avtor: Brane Šalamon



VARNOST NA INTERNETU - KOGA BRIGA DATUM VAŠEGA ROJSTNEGA DNE

Internet je res krasno orodje za raziskovanje sveta in učenje in vsakdanje orodje za delo, vendar se brez nekaterih varnostnih ukrepov lahko hitro spremeni v grozeče okolje. Ob vsem tem pa ne smemo pozabiti, da je internet neoprijemljiv in presega državne meje v svetu, kjer so v globalnem prostoru vrednote relativne. In prav v tem je njegova lepota in tudi njegova nevarnost.

Internet in brskanje po spletu sta postala del našega vsakdana in ju uporabljamo za vse mogoče. Internet uporabljamo kot delovni pripomoček v službi, uporabljajo ga v šolah in univerzah in uporabljamo ga še za vsemogoče. Od vsakdanjega brskanja za zabavo, do izmenjave sporočil, plačevanja, nakupovanje in še česa. Uporabo oz. način uporabe interneta, kako brskati po spletu in kako uporabiti številne njegove možnosti je večina razumela zelo hitro, nikoli pa se nismo dovolj naučili o tem, kako vse to početi varno.

V običajnem življenju vemo, kako zavarovati svoje stanovanje pred vlomilci, kako obraniti svoj avto. Vemo, kako se vesti do neznancev in vsaj v večini primerov tudi, kdo je vreden našega zaupanja in kdo ne. Daleč so časi, ko smo lahko pustili odklenjena vrata stanovanja ali avtomobila, dandanes pa za vse to uporabljamo ključavnice, alarme in storitve varnostnih služb.
In v svetu elektronskih komunikacij oz. v svetovnem spletu smo bili v trenutku nebogljeni. Je res tako nevaren, ker je vanj vključenega skoraj milijarda drugih, ki nimajo vsi lepih namenov? In ker veliko slišimo o računalniških kriminalcih, hekerjih, ki vdirajo v računalnike, podobno kot večina vlomilcev, ki kradejo podatke, šifre in še kaj?

Vse te nevarnosti v resnici niso tako hude, kot se zdijo na prvi pogled, čeprav je res, da se moramo tudi v svetovnem spletu obnašati podobno, kot v običajnem življenju. In če že zaklepamo vrata stanovanja ali pisarne, potem moramo elektronsko zaklepati tudi naša vrata v svet komunikacij in tudi tu biti previdni do neznancev.

Temeljna zaščita je geslo oz. šifra

Temelj vse zaščite in varovanja pri delu z računalniki in internetom je izbira pravega gesla oz. šifre. To je še posebno pomembno, ko drugim posredujemo svoje podatke, kupujemo ali opravljamo kakršnekoli druge denarne transakcije. V mnogih kritičnih primerih sta pravo geslo in šifra preprečila marsikatero nevarnost. Geslo oziroma šifra sta najpreprostejši in velikokrat najučinkovitejši zaščiti vašega računalnika in predvsem podatkov. Po možnosti izberite geslo oziroma šifro, ki je naključna kombinacija črk in številk, vsekakor pa naj bo takšno, da si ga boste zapomnili.

Če pri delu uporabljate preveč gesel in šifer, vam svetujemo, da izberete takšno, ki je podobno še kakšnemu, ki ga uporabljate kje drugje. PIN-številka za mobilni telefon je verjetno eno izmed vaših najbolj varovanih gesel.

Če želite povsem ohraniti vaše geslo oziroma šifro, ga zamenjajte najmanj enkrat letno in zamenjajte ga tudi ta-

Izbira pravega gesla oziroma šifre je najboljša zaščita, zato nikoli ne uporabljajte lahko razumljivih ali prepoznavnih kombinacij in pri izbiri ne uporabljajte slovarjev ali enciklopedij.

Če torej kdaj počnete kaj zares zaupnega, kot je na primer delo na poslovnih skrivnostih vašega delodajalca, ko si želite popolno varnost, je edini prav način odklop iz omrežja ali interneta, da kdaj pa kdaj res fizično osamite računalnik, po domače potegnete kabel iz omrežja ter potem delajte z računalnikom.

krat, ko se vam zdi, da bi ga lahko kdo odkril, oziroma ko ga poskuša odkriti. Gesla oz. šifre uporabljamo za dostop do vsebin različnih spletnih strani in tudi za dostope do samega računalnika, ki bo zahteval vstopno geslo, še preden se bodo naložil celotni sistem in geslo oz. šifro za dostop do zaslona, ko bo po vključenem ohranjevalniku zaslona možen dostop do vašega računalnika le z vpisom gesla za zaslon.

Vaš osebni požarni zid

Vaš računalnik, povezan v internet, je zelo ranljiv, saj je dostopen tako rekoč vsem uporabnikom, ki so v internet povezani tisti trenutek. Nujno je, da se pred vsiljivci z interneta zavarujete tako, da si omislite požarni zid.

To je pravzaprav varnostni sistem, posebna programska, včasih pa tudi strojna oprema, ki deluje kot nekakšen vratar med vašim službenim omrežjem ali domačim računalnikom in internetom. Požarni zid filtrira vse prenose podatkov z interneta in blokira vhode v službeno omrežje ali domači računalnik ter je najzanesljivejša zaščita pred računalniškimi vsiljivci. Požarni zid prepreči drugim, da bi vdrli v vaš računalnik in nepooblaščeno spreminjali ali brisali programe in podatke na vašem disku.

Požarni zidovi za službena omrežja so navadno nameščeni na posebnih strežnikih, za domačo uporabo pa lahko požarni zid najdemo na internetu in ga namestimo sami.

Kaj vedo o vas

Vaš spletni brskalnik ob obisku katerekoli spletne strani pusti za seboj številne sledi in upravljavci spletnih strani vedo za vaše ime, za vaš e-naslov, vrsto računalnika in operacijski sistem, ki ga uporabljate, vedo, od kod vstopate v internet in še marsikaj drugega. V svetu in pri nas vse več govorimo o zaščiti osebnosti in osebnih podatkov, z uporabo brskalnikov pa dobesedno puščamo številne podatke na sleherni spletni strani, ki jo obiščemo. Rešitve so enostavne.



Pobrišite zgodovino (History), saj spletni brskalniki hranijo seznam vseh strani, ki ste jih v določenem obdobju obiskali. Seznam nam je lahko v pomoč, ko pozabimo naslov kakšne spletne strani, vendar je pri popolni varnosti na internetu včasih bolje, da ga ni.

Pobrišite začasne (Cache), ker se ob vsakem vstopu na spletne strani v računalniku hranijo začasne datoteke. Kasnejši obisk in iskanje nekoč že obiskanih spletnih strani sta lahko hitrejša in delo z internetom je veliko lažje, vendar te začasne datoteke predstavljajo vstop v zasebnost vašega računalnika. Izbrišite jih.

Pobrišite sledi, saj je v spletu veliko podatkovnih baz, kjer so hranjeni vaši podatki in tako so nastali številni imeniki in seznami, kjer so na kakršenkoli način vključili tudi vaše ime in vaš e-naslov in večina teh seznamov omogoča, da se lahko tisti, ki so v njih, izbrišejo. Obiskati boste morali vsako stran posebej in zahtevati izbris ali pa to storite sami in potrdite izbris.

Bodite anonimni, ker je največji problem varnosti oz. zaščite na internetu e-pošta, saj vaš e-naslov odpira številne možnosti zlorabe, vsekakor pa vam lahko povzroči številne nevšečnosti. Če se pri pošiljanju e-pošte ne želite razkriti uporabite anonimne pošiljatelje e-pošte.

Bodite previdni pri spletnih obrazcih, ko na mnogih spletnih straneh občasno izpolniti tudi obrazce z različnimi podatki o uporabniku in pri njihovem izpolnjevanju bodite pozorni in ne izpolnjujte vsega. Na obrazcih je velikokrat posebej označeno, z zvezdico ali drugačno barvo, tisto, kar je treba nujno izpolniti, in tisto, kar izpolnjujete po lastni želji. Tistega, česar ni treba izpolniti, ne izpolnite. Če od vas kljub temu zahtevajo dodatne osebne informacije, premislite, koliko jih boste napisali v resnici. Iz dosedanje prakse se je pokazalo, da lahko napišete tudi kakšne izmišljene in neresnične podatke. O sebi na spletnih straneh odkrivajte čim manj podatkov.

Zares zaupno le »off-line«

Nič v življenju ni popolno in tudi najbolj zapletena gesla in šifre, požarni zidovi tudi najbolj skrbni ponudniki internetnih storitev vas ne morejo povsem obvarovati pred vdorom ali krajo, čeprav boste varni vsaj pred 99% vseh vsiljivcev.

Ko delo končate iz računalnika počistite vse zaupne datoteke in pri tem ne pozabite na različne začasne datoteke, ki so jih ustvarili programi, s katerimi ste delali in se seveda spet vključite v internet.

In preden se vključite vedno pomislite na nekaj osnovnih varnostnih korakov pri delu z internetom:

Varnostni razmislek ob e-pošti. Ko pošiljate elektronsko pošto, pomislite, kako varna je ta pošta oziroma koliko zasebnosti ste si lahko zagotovili v teh sporočilih? Največjo varnost boste dosegli, le če v običajni elektronski pošti ne boste pošiljali zasebnih podatkov, fotografij ali podobnih informacij o vas in vaši družini. Ko sprejemate elektronsko pošto, se zavedajte, da vam v svetovnem omrežju lahko takšno elektronsko sporočilo pošlje kdorkoli od koderkoli. Če dobite sporočilo od neznanega pošiljatelja, bodite še posebno previdni in se ne zanašajte na njegovo vsebino.

Varnostni razmislek ob deskanju. Splet je lahko divji kot nekdanji divji zahod, zato bodite previdni, kam greste in komu zaupate. Tudi pri iskanju podatkov bodite previdni, saj vseh spletnih strani ne pripravijo zaupanja vredne institucije ali ljudje. Preden se odpravite v splet tudi preverite nastavitve svojega brskalnika, da ne boste nevede spustili pri deskanju na svoj računalnik cele kupe piškotkov in da ne boste povsod puščali sledi vašega deskanja.

Varnostni razmislek ob spletnih nakupih. Preden začnete nakupovati v spletni trgovini, preverite, ali je spletna povezava varna, kar je razvidno, če je namesto običajnega naslova http naveden naslov https – to pomeni, da gre za varno povezavo. To lahko preverite tudi tako, da se vam v spodnjem delu ekrana ob zahtevi za vpis vstopne šifre in gesla prikaže ključavnica živo rumene barve. Samo po takšni povezavi bodo vaše finančne transakcije in podatki varni.

Varnostni razmislek ob posredovanju podatkov. Temeljni pogoj varnega dela z računalnikom in na spletnih straneh sta varna šifra in geslo, ki naj bi zagotavljala vašo zasebnost. Ob tem vedno preverite ali imajo ponudniki storitev in uslug na svojih spletnih straneh zapisane pogoje varnega dela, npr. Izjavo o zasebnosti, kjer zagotavljajo, da vaših podatkov ne bodo posredovali drugim oz. nepoklicanim. Vedno temeljito premislite na katera vprašanja boste na spletnih straneh odgovarjali in ali tisto, ki vas sprašuje za vse mogoče podatke ima kakšen vzrok, da zahteva vaše osebne podatke?

Če posredujete občutljive podatke (npr. številko kreditne kartice), vedno izberite šifrirano povezavo in preverite varnost povezave, kar je razvidno, če je namesto običajnega naslova http naveden naslov https – to pomeni, da gre za varno povezavo. To lahko preverite tudi tako, da se vam v spodnjem delu ekrana ob zahtevi za vpis vstopne šifre in gesla prikaže ključavnica živo rumene barve. Samo po takšni povezavi bodo vaši podatki varni.

Varovanje zasebnosti

Zasebnost mora biti temelj za komuniciranje s katerokoli spletno stranjo, kjer zahtevajo vaše podatke, pa naj bodo osnovni ali zaupni. Kadarkoli se odločite, da boste na kateri od spletnih strani opravili kakršnokoli dejavnost in izkoristili njihovo uslugo ali storitev oziroma boste opravili kakšne nakupe, morate biti prepričani, da ta stran varuje vašo zasebnost. To velja še posebno za primere, ko upravljavcem spletnih strani posredujete osebne ali celo zaupne podatke, kakršen je številka kreditne kartice. Zaupanja vredne spletne strani imajo vse pogosteje posebej poudarjeno varovanje zasebnosti (Privacy Policy). Obveze, določila in garancije o varovanju vaše zasebnosti bi morale biti na vseh spletnih straneh, kjer zahtevajo kakršenkoli vaš podatek, ki je namenjen, kot na splošno napišejo, »interni uporabi«. O varovanju vaše zasebnosti mora biti napisanega veliko več v posebnem oknu, kjer natančno opišejo, kaj počnejo in kaj bodo počeli z vašimi podatki. Imejte več zaupanja v tiste spletne strani, ki imajo varovanje zasebnosti posebej omenjeno. To pomeni, da bi zagotovilo o varovanju zasebnosti morale imeti skorajda vse strani.

Ko vstopate v svetovni splet ne pozabite, da svet ni Slovenija in vse države ne zagotavljajo enakega varstva zasebnosti in predvsem osebnih podatkov. V naši državi je namreč varstvo zasebnosti zapisano v ustavo, imamo izjemno strog Zakon o varstvu osebnih podatkov in natančnega inšpektorja na Ministrstvu za pravosodje. Enako je v državah članicah Evropske unije, podobno pa tudi v drugih evropskih državah. Povsem drugače pa je na ostalih kontinentih, zato bodite pozorni. ■





SITI BESED

SEPTEMBER 2013



Pridružimo se pobudi, da v slovenskih šolah od septembra 2013 ne bo več lačnih otrok.

www.sitibesed.si
Fb: Siti besed

Sredstva za prehrano šolskih otrok lahko nakažete na: **Zveza prijateljev mladine Slovenije, Miklošičeva 16, 1000 Ljubljana, št. računa: SI56 6100 0000 3512 232, BIC: HDELSI22, sklic: 00 07-2401, koda namena: CHAR (namen SITI BESED, dodajte oznako AN, če želite ostati anonimni).**

iHELP





MiDS d.o.o.
Vino 17a
SI-1291 Škofljica
info@ihelp.si
www.ihelp.si

Avtor: Elvis Guštin / EM-Soft sistemi d.o.o.



VAROVANJE PRENOSNIKOV V TRANSPORTU IN V HOTELIH

Verjetno ste lastnik prenosnega računalnika, ki ga nosite s seboj na službena potovanja ter počitnice. Ste kdaj pomislili, kakšne podatke hranite v njem? Občutljive službene kalkulacije in dokumente, elektronske certifikate, privatne podatke in še marsikaj. Kaj se lahko zgodi takrat, ko prenosnik pozabite v taksiju, vam ga ukradejo iz avtomobila, odtujijo v hotelu ali kaj podobnega? Kakšna škoda nastane za vas in vaše podjetje?

Ne razmišljajte tako, kot večina lastnikov: »Saj imam varnostno kopijo podatkov doma, nič hudega ne bo«, ker je to le metanje peska v oči. Res je, da je varnostna kopija zelo pomemben člen v verigi varovanja podatkov, vendar ni edini. Že nekaj časa se zavedamo, da je največje bogastvo informacija. S tem, ko vam je tretja oseba računalnik odtujila, si je prislužila tudi dostop do vaših podatkov. Torej lahko zelo hitro ugotovimo, da varnostna kopija še zdaleč ni dovolj, če ostanete brez vašega prenosnega računalnika.

Prišel je čas, da dodamo tej naši prvi, nepopolni zaščiti, druge komponente, ki bodo ščitile vsebino našega računalnika pred posegi tretjih oseb. Najprej se moramo zavedati, da nepooblaščena oseba, ki dobi naš prenosni računalnik v roke, lahko neomejeno dostopa do naše opreme in se poskuša dokopati do naših podatkov. Torej, pričnimo razmišljati o zaščiti prenosnega računalnika kot celote, sestavljene iz strojne opreme in podatkov.

Eno izmed najosnovnejših pravil je, da moramo biti najprej mi, kot uporabniki, previdni, kako vsebino uporabljamo in komu jo sporočamo. Nedolgo nazaj, ste mogoče iz vaše banke prejeli sporočilo, da nikomur ne sporočajte vaših vstopnih podatkov za dostop do spletne banke. Zakaj pošiljajo taka opozorila? Ko vam nekdo pošlje v imenu banke prošnjo, da mu nazaj pošljete svoje osebne podatke, na najbolj enostaven način dobi od vas informacije, saj predpostavlja, da mu boste zaupali. Hacker pošlje par tisoč takih sporočil, na katere bo dobil mogoče sto odgovorov. Na tak način ima dejansko brez stroškov dostop do sto računov (seveda tu ne mislim samo bančnih podatkov, ampak tudi tistih za dostop do elektronske pošte, do podjetja,...). Od tu naprej je vsa dodatna varnost brezpredmetna, saj je že prišlo do zlorabe.

Najprej se moramo zavedati, da nepooblaščena oseba, ki dobi naš prenosni računalnik v roke, lahko neomejeno dostopa do naše opreme in se poskuša dokopati do naših podatkov.

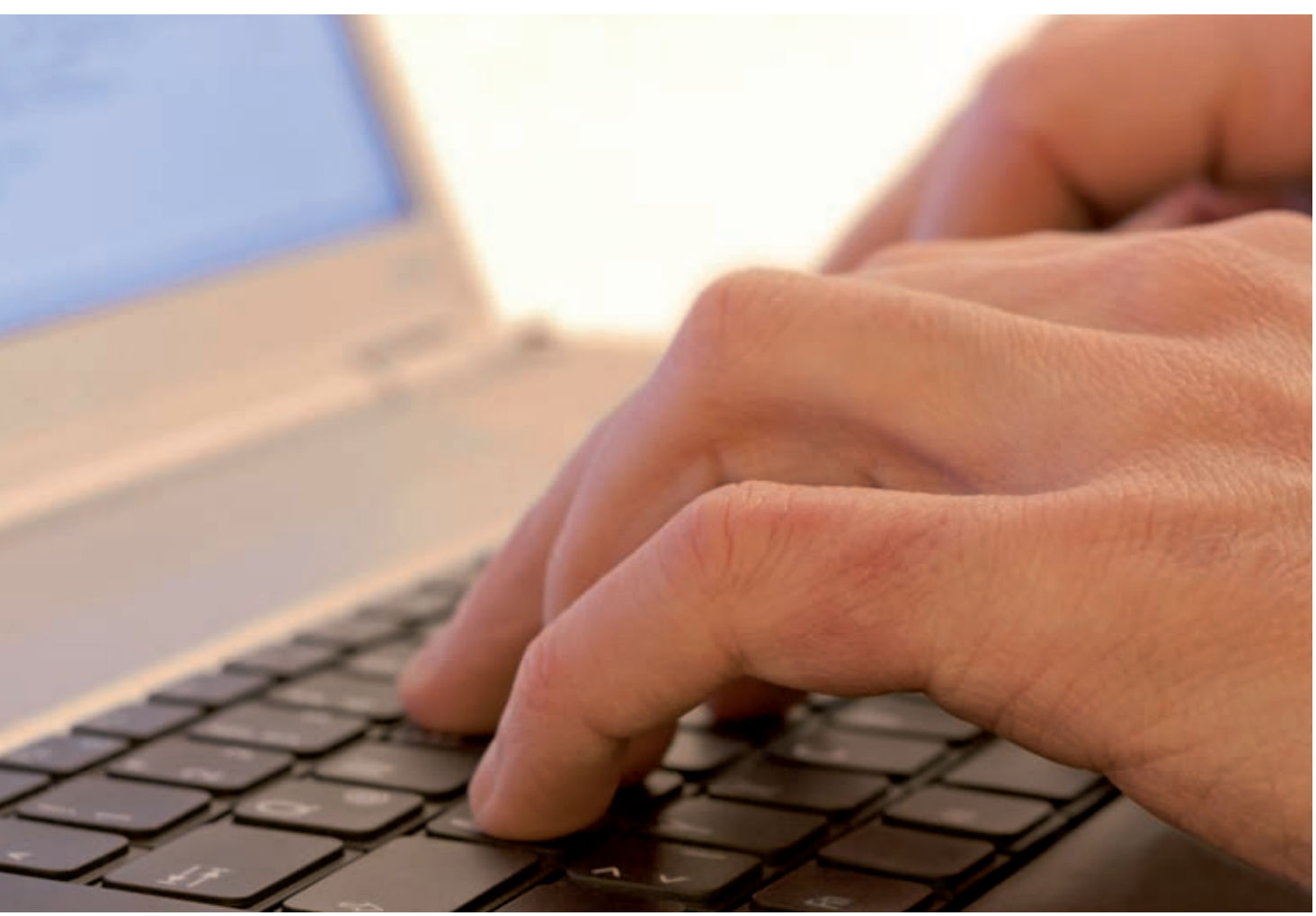
Zaščitite dostop do operacijskega sistema z geslom. Prva stvar, ki bo novi lastnik naredil z računalnikom je ta, da ga bo prižgal. Lepo je, da mu začetno delo otežite že kar takoj, z geslom. Seveda imajo gesla tudi svojo logiko. Administratorji, ki delamo na področju varnosti vemo, da je večino gesel možno ugotoviti tako, da vpišemo znamko računalnika, imena družinskih članov, ljubljenčkov, konjičke, avtomobilske znamke in še kaj bi lahko našteval. Prva rešitev tega problema so tako imenovana kompleksna gesla. Marsikateri administrator bo od vas zahteval zelo dolgo, kompleksno in varno geslo, ki se pa na koncu (zaradi svoje kompleksnosti) znajde napisano pod tipkovnico, nalepljeno na prenosni računalnik,... Rešitev so varna in za nas enostavna gesla. Geslo, ki se ga bomo zlahka zapomnili je na primer »Barvajo cesto!«. Kako sem prišel do njega? Pogledal sem skozi okno in videl nekaj, kar bo naše enostavno geslo. Glede na to, da je prva črka napisana z veliko in da imam na koncu klicaj, je tudi kompleksno. Če želite lahko določene črke zamenjate tudi s številkami, »o« postane nič, »i« postane 1, ... uporabite malo domišljije. Naše geslo ima še eno zelo dobro karakteristiko: po par vpisih si ga bom zapomnil in opisuje slučajen dogodek. Morebitni nepridiprav, ki bo prišel v mojo pisarno in poizkušal uga-

Stvari, ki jih boste pustili, da se bodo odvijale same, bodo zavile v slabo smer.

niti geslo, ne bo vedel, da sem jaz gledal delavca, ki je barval cesto. Ni ga več. Pa še nasvet: uporabljajte gesla z najmanj devetimi znaki, čeprav sam priporočam gesla daljša od petnajstih (z uporabo stavkov ni težko).

Pri prenosnem računalniku pomislite na celotno, kompleksno zaščito. Večina, če ne že vsi novejši prenosni računalniki imajo že vgrajen TPM element (Trusted Platform Module). Ta nam omogoča, v kombinaciji z operacijskim sistemom, zaščititi podatke na nivoju celotnega računalnika. Možnosti uporabe je več, vendar je najpogostejša raba v kombinaciji z Microsoftovo BitLocker tehnologijo. Uporaba te tehnologije je zelo priporočljiva, saj zahteva in vzpostavi varnost na visokem nivoju. Najprej vsili geslo za dostop do BIOS-a in s tem onemogoči osnovni dostop do nastavitev računalnika. Nato šifrira celoten disk tako, da zagon sistema ali dostop do podatkov na njem ni možen v primeru, da pride do sprememb na sistemu ali na strojni opremi. Za spremembe v sistemu imam v mislih viruse, za spremembe na strojni opremi pa poizkus zagona iz drugega računalnika, poizkus vdora ipd. Tehnologija je na razpolago v Microsoftovih produktih Windows Vista Ultimate in Enterprise, Windows 7 Ultimate in Enterprise ter v Windows 8. Tak način varovanja podatkov nujno zahteva varnostno kopijo podatkov. Vsaka okvara na računalniku, kot na primer okvara osnovne plošče, lahko namreč pomeni izgubo podatkov. Dobra novica za tiste, ki varnostne kopije niste naredili je ta, da do podatkov, šifriranih z BitLocker tehnologijo, sicer lahko pogojno dostopamo tudi z drugih računalnikov. Z uporabo 48 mestne številčne kode, ki se generira ob začetku šifriranja diska in je za vsako izvedbo postopka različna, lahko svoje podatke ponovno spravite k življenju. To kodo torej shranite na varno mesto, ker jo boste mogoče še potrebovali. Kljub možnosti izbire izdelave USB medija slednjo potezo odsvetujem, kajti tudi tak medij se lahko pokvari.

V okviru tega vedno priporočam uvedbo zaščite podatkov z BitLocker-jem na nivoju podjetja. To storimo z nastavitvami varnostne politike tako, da prenosnemu računalniku, brezpogojno vsilimo šifriranje vseh pogonov. V takem primeru, se tudi vsi ključi za dešifriranje pogonov hranijo v podjetju, na centralni lokaciji (Aktivni imenik) in je tako celoten postopek varen in avtomatiziran. Z verzijo operacijskega sistema Windows 7 je na tem področju prišla na dan še ena bistvena novost. To je šifriranje USB ključkov. Vemo, da na take medije dajemo vedno več in vedno bolj občutljive podatke. Vedno pogosteje jih pozabimo ali izgubimo, zato moramo tudi te medije vedno bolj paziti. Tako imenovan »BitLocker To Go« je namenjen prav tem napravam. Z razliko od navadnega BitLocker-ja je dostop do podatkov mogoč na vsakem računalniku, po vnosu PIN kode. Ome-



jitev je tu samo pri sistemih Windows XP, kjer lahko podatke le beremo, ne moremo pa na ključek ničesar napisati.

Kaj pa ko pridete v hotel? Se enostavno priključite na njihovo omrežje? No, večina ljudi to stori, vendar prav bi bilo, da bi se tudi tu zavedali nevarnosti in načinov, kako jih odpravimo. Nemogoče je sicer odpraviti vse pomanjkljivosti, katerim smo na javnih mestih izpostavljeni, vendar se mnogim lahko izognemo. Na javnih mestih bi se bilo vedno priporočljivo povezati preko lastnih omrežij (npr. GSM kartice), vendar to večinoma ni možno in zato uporabimo tisto, kar imamo na razpolago. Ker se zavedamo, da smo na javnem omrežju in pomislimo na najslabšo situacijo - da je naš konkurent v sosednji sobi ter da hotel nima urejene varnosti - moramo čim več stvari urediti mi. Nekatere stvari lahko uredite sami, s pomočjo vašega razmišljanja in brez velikih vlaganj. Najprej se prepričajte, da imajo vsi uporabniški računi na vašem računalniku geslo. Tako bo dostop do vašega računalnika že otežen. Ne dajajte map v skupno rabo, saj je to najenostavnejši način dostopa do podatkov. Zavedati pa se morate, da ni mogoče ukiniti tako imenovane »Administratorske skupne rabe« do katere imajo dostop uporabniki z administratorskimi pravicami. Torej, to nakazuje na dve rešitvi: izogibajte se administratorskih pravic in tistim računom, ki te pravice morajo imeti, dajte zelo močno geslo. Zadnji enostaven ukrep, ki ga lahko sami uredite in v kolikor imate operacijski sistem Windows Vista ali novejši pa je, da izklopite odkrivanje računalnika v omrežju. Ta funkcija zapre dostope do računalnika na požarnem zidu in vam lahko precej pomaga pri anonimnosti. Vsi nadaljnji ukrepi so bolj zapleteni za vzpostavitev, zahtevajo precej bolj kompleksno načrtovanje s pristopom na ravni celotne organizacije in mora zanje poskrbeti vaš IT vzdrževalec.

Torej, če za konec povzamem vse napisano:

1. Izdelujte si varnostno kopijo vaših podatkov. Okvare in kraje so del vsakdanjika.
2. Skrbno varujte vaše uporabniške podatke in gesla. To so VAŠI podatki, zato jih NE POSREDUJTE DRUGIM V NOBENEM PRIMERU.
3. Uporabljajte dobra in dovolj dolga gesla za dostope do vseh elektronskih virov.

V okviru tega vedno priporočam uvedbo zaščite podatkov z BitLocker-jem na nivoju podjetja. To storimo z nastavitvami varnostne politike tako, da prenosnemu računalniku, brezpogojno vsilimo šifriranje vseh pogonov.

4. Ščitite celoten prenosni računalnik. Vstopno geslo za operacijski sistem ni dovolj. Uporabljajte moderne tehnologije, kot so TPM modul, BitLocker ali podobne programske rešitve.
5. Premislite, kaj lahko naredite, da boste bolj varni, ko boste priklopljeni v javna omrežja.

Kot vidimo, sem vam predstavil kar nekaj bolj ali manj enostavnih ukrepov, ki jih lahko uporabite za lastno varnost in varnost podjetja. Dejstvo je, da je povračilo zavarovalnice (preverite pogoje, ker je zavarovanje v večini primerov neveljavno na javnih mestih) le minimalno in izguba podatkov nima cene.

K nam so že nekajkrat prišli ljudje, ki so doživeli krajo podatkov. Zato vas svarim, da naša ljuba dežela na sončni strani Alp, ni najbolj varen kotiček tega sveta in da se vam nevšečnosti lahko zgodijo kadarkoli in kjerkoli. Iz lastnih izkušenj vam povem, da so se naši pristopi pokazali kot pravilni in dobrodošli, še posebej takrat, ko so prenosnik ukradli direktorju podjetja. ■



Avtor: Andrej Maslo, uni. dipl. politolog - smer obramboslovje, dipl. varstvoslovec*



VAROVANJE V IGRALNICI

Varovanje v igralnici mora biti prepoznano kot dodana vrednost in sestavni del celotne ponudbe posamezne igralnice. V tem pogledu ne gre samo za zagotavljanje zakonitosti dejavnosti prirejanja posebnih iger na srečo, ampak tudi širše za zagotavljanje varnosti gostov, zaposlenih, zunanjih izvajalcev del kot tudi vseh procesov, ki se neposredno prepletajo z igralniško dejavnostjo in imajo neposreden vpliv na obvladovanje tveganj igralniških in neigralniških procesov.

Uvodna beseda

V prvi številki revije Korporativna varnost je avtor članka Videonadzor v igralništvu, Andrej Kovačič, predstavil pravni, organizacijski, funkcionalni ter operativni okvir službe za videonadzor v igralništvu. Videonadzor v igralništvu predstavlja t.i. ožji okvir dejavnosti varovanja v igralnici, ki je specializiran za nadzor procesov prirejanja posebnih iger na srečo (igralniških procesov). Širši okvir varovanja v igralnici pa predstavljajo vsi tisti procesi, ki so potrebni za zagotavljanje okvira nemotenega delovanja tako igralniških kot neigralniških procesov v sklopu celotne igralniške ponudbe. Pravno, organizacijsko in funkcionalno je varovanje utemeljeno v obstoju in delovanju varnostne službe koncesionarja posebnih iger na srečo[1].

Varnostna služba v igralnici

Varnostna služba je pomemben segment v zagotavljanju varnosti v igralnici, saj lahko z uporabo pravno-formalnih, varnostno-tehničnih, materialnih, organizacijskih in drugih ukrepov, neposredno posega v obvladovanje različnih tveganj ter varnostnih dogodkov na varovanem območju. Vsekakor pa pri tem vloga varnostne službe ni in ne sme biti osamljena, ampak se odvisno od primera do primera vanjo vključujejo tudi druge službe koncesionarja[2].

Zakon o zasebnem varovanju iz leta 2011 je v 70. členu uzakonil obveznost subjektov, da organizirajo varovanje skladno z določbami zakona, če na posameznem objektu neposredno poslujejo z gotovino in drugimi vrednostmi v protivrednosti najmanj 200.000 €. V tem okviru zakon tudi našteje subjekte, ki jih ta določba zajema ter med njimi tudi omenja igralnice in igralne salone[3]. Pred uveljavitvijo sprememb zakona je bil obseg in oblika organiziranosti varnostnih služb pri posameznih koncesionarjih zelo različen. Tako so obstajali koncesionarji, ki so imeli organizirano lastno službo varovanja (Hit, d.d.; Casino Portorož, d.d.), koncesionarji, ki so imeli najeto pogodbeno službo varovanja ter koncesionarji, ki niso imeli organizirane nobene od omenjenih oblik službe varovanja. Kljub temu, da stari zakon o zasebnem varovanju ni posebej omenjal obveznosti organiziranja službe varovanja v igralnici oz. igralnem salonu, so te varnostne službe delovale na podlagi določil istega zakona. Tudi po uveljavitvi sprememb zakona v letu 2011 še ni prišlo do večjih sprememb na tem področju, saj je zakon uveljavil prehodno petletno obdobje za uveljavitev sprememb.

Zaradi različnih praks na tem področju je zelo težko govoriti o enotnem modelu umeščenosti varnostne službe v organizacijski strukturi podjetja. Ustrezno in pravilno je, da ima varnostna služba v organizacijski strukturi koncesionarja takšen položaj, ki ji omogoča samostojno in strokovno delovanje ter neposreden dostop do virov odločanja.

Varnostna služba v igralnici deluje v okvirih Zakona o zasebnem varovanju, kar pomeni, da ima varnostna služba pridobljene ustrezne licence za izvajanje posameznih oblik varovanja, prav tako pa ima tudi zaposleno varnostno osebje pridobljene službene izkaznice, s katerimi izkazuje upravičenost za neposredno opravljanje nalog varovanja. Organiziranost,

*avtor je član Slovenskega združenja korporativne varnosti

pristojnosti, naloge in odgovornosti pa varnostni službi dodatno določajo notranji akti koncesionarja – pravilniki, organizacijska navodila, delovna navodila, različni načrti varovanja in protokoli postopanja v različnih varnostnih situacijah. Koncesionarji, ki imajo organizirano lastno službo varovanja, imajo to organizirano kot samostojno organizacijsko enoto, na čelu katere je varnostni manager, sestavljajo pa jo še varnostniki nadzorniki in varnostniki.

V teh okvirih varnostna služba v igralnici v pretežnem delu izvaja naloge s področja varovanja ljudi in premoženja, tako da je služba pristojna za varovanje življenja in zdravja ljudi, za vzdrževanje reda ali javnega reda ter za varovanje premoženja na varovanem območju. Posredno pa določene pristojnosti in naloge varnostni službi v igralnici nalaga tudi Zakon o igrah na srečo, s tem ko predpisuje, da koncesionar določa pogoje za obisk igralnice (nadzor nad vstopi v igralnico) ter pri tem daje možnost, da se posameznikom tudi prepove nadaljnja udeležba pri igrah (izdaja prepovedi vstopa v igralnico)[4]. Navedene pristojnosti in naloge lahko varnostna služba v igralnici učinkovito izvaja v okviru ukrepov varnostnega osebja po Zakonu o zasebnem varovanju[5].

V zadnjem času, po uveljavitvi Uredbe o obveznem organiziranju službe varovanja na javnih prireditvah, se vse bolj pojavlja tudi potreba po opravljanju nalog s področja varovanja prireditev v gostinskih lokalih. Vse več igralnic v sklopu svoje ponudbe organizira različne prireditve (koncerti in druge oblike zabavnega programa), kar narekuje potrebo, da se na prireditvenem prostoru organizira varovanje prireditev, skladno z zahtevami navedene uredbe. To pomeni, da mora imeti zavezanec po uredbi organizirano službo varovanja, ki ima pridobljeno licenco za varovanje prireditev v gostinskih lokalih[6].

Poleg navedenih področij varovanja varnostne službe v igralnici, se lahko občasno pojavlja tudi potreba po opravljanju nalog s področja varovanja oseb, gostov igralnice, katerim je potrebno, zaradi njihove izpostavljenosti varnostnim tveganjem, ponuditi določen nadstandard varovanja. Tveganja pri takšnih osebah izhajajo iz njihovega družbenega položaja ter ekonomske moči, ki jo takšne osebe imajo, čemur se prilagaja tudi način izvedbe varovanja.


foto: Arhiv Hit

Varnostna služba koncesionarja razpolaga s sistemom videonadzora, ki je ločen od sistema videonadzora po Zakonu o igrah na srečo, za katerega je pristojna služba videokontrole. Ločitev obeh sistemov videonadzora v praksi pomeni, da se na istem objektu, na določenih varovanih točkah, hkrati izvajata dva ločena sistema videonadzora – videonadzor varnosti ter videonadzor videokontrole. Sistem videonadzora varnosti se izvaja skladno z določili Zakona o varovanju osebnih podatkov in je vzpostavljen na vseh tistih območjih, kjer je to potrebno za varnost ljudi in premoženja, za zagotavljanje nadzora nad vstopnimi točkami v objekt oziroma tam, kjer zaradi narave dela tudi obstoja večja ogroženost zaposlenih. Sistem videonadzora se kombinira tudi z drugimi varnostno-tehničnimi elementi, s katerimi neposredno upravlja varnostna služba: protivlomni sistem, protipožarni sistem, sistem pristopne kontrole, centralno-nadzorni sistem za uspešno upravljanje različnih, vendar med seboj povezljivih sistemov tehničnega varovanja ipd.. Vsi sistemi tehničnega varovanja se upravljajo iz ene, centralizirane točke, ki jo lahko imenujemo varnostno-operativni center varnostne službe in za katerega veljajo najstrožja merila varovanja.
Na podlagi predstavljenega lahko dela in naloge varnostne službe v igralnici razdelim na sedem velikih področij, ki se lahko dodatno delijo še na posamezna podpodročja:
- področje igralnice;
- področje halla[7];
- področje varnostno-operativnega centra;
- področje prireditvenega prostora;
- področje varovanja gostov;
- področje neigralniških prostorov;
- področje zunanjosti objekta.

V kolikor v sklopu igralnice obratuje tudi hotel, lahko navedenim področjem dodamo tudi področje dela in nalog v hotelu (z njegovimi posameznimi podpodročji).

Varnostni dogodki v igralnici

Na stanje varnosti v igralnici vplivajo številni dogodki in okoliščine, zato mora biti delo varnostne službe, poleg obravnave varnostnih dogodkov, v prvi vrsti usmerjeno v informiranje, obveščanje, opozarjanje in osveščanje oseb na mogoča škodljiva ravnanja in njihove posledice. Zaradi narave dela z gosti, ki so lahko tekom obiska igralnice izgubili določeno vsoto denarja, je pomembno, da je komunikacija varnostnega osebja s takšnimi osebami kvalitetna in korektna, s ciljem pomirjanja in nadzora situacije ter s tem preprečevanja morebitnih nezaželenih varnostnih pojavov.



foto: Arhiv Hit

V kolikor pa do varnostnih dogodkov v igralnici pride, se ti v pretežnem delu kažejo kot kršitve reda na varovanem območju (nespoštovanje pravil reda na varovanem območju in določil hišnega reda igralnice). Temu sledijo intervencije varnostne službe pri dogodkih, ki niso posledica kaznivih dejanj oziroma kršitev javnega reda in miru (npr. nudenje prve pomoči gostom in zaposlenim, prometni incidenti na varovanem območju, različne kršitve internih navodil in pravilnikov s strani zaposlenih ipd.), v manjšem delu pa se pojavljajo kot kršitve javnega reda in miru na varovanem območju (neprimerno in nedostojno vedenje na javnem kraju) ter različne oblike kaznivih dejanj (poškodovanje tuje stvari, tatvine, vlomi, ponaredki, zatajitev najdbe ipd.).[8] V tem delu niso zajete kršitve pravil iger na srečo, glede na to, da je za beleženje tovrstnih dogodkov pristojna služba videokontrole.

V tem delu bi se še posebej omejil na službo videokontrole, ki ima zelo pomembno vlogo pri nadzoru varnosti igralniških procesov. Za dobro sodelovanje med službo videokontrole in varnostno službo je ključnega pomena dober in hiter pretok informacij med obema službama, zaradi obvladovanja varnostne situacije na operativni ravni. Služba videokontrole ne nastopa direktno v razmerju do udeležencev igralniških procesov (zaposleni, gostje igralnice, zunanji izvajalci del) ter nima t.i. neposredno izvršljivih pooblastil, zaradi česar je v tem delu zelo pomembna vloga varnostne službe z ukrepi, ki jih ima na razpolago na podlagi določil Zakona o zasebnem varovanju. Tako se varnostna služba tudi pojavlja pri vseh tistih dogodkih, na katere pri svojem delu postane pozorna služba videokontrole in imajo značaj kršitev pravil posebnih iger na srečo (goljufije in druge oblike kršenja pravil igre). Vloga varnostne službe je v takšnih primerih omejena na uporabo ukrepov zoper kršitelje ter obveščanje ustreznih služb. Glede na to, da v takšnih primerih varnostna služba nastopa kot podaljšana roka videokontrole, je ključnega pomena, da se v teh postopkih podajajo relevantne informacije, saj je uporaba ukrepov varnostnikov vezana na izpolnjevanje zakonsko določenih pogojev za njihovo uporabo.

Z vidika obvladovanja tveganj ter obvladovanja, obravnave in analiziranja varnostnih dogodkov je pomembno tudi sodelovanje varnostne službe z drugimi službami tako znotraj podjetja (videokontrola, pravna služba, posamezni igralniški oddelki ipd.) kot tudi navzven (policija, gasilci, reševalci ipd.).

Zaključek

Z zaključkom prejšnjega poglavja sem izpostavil tudi problematiko, da se z varnostjo povezane zadeve v igralnicah obravnavajo v okviru ločenih služb, ki pa imajo skupen cilj zagotavljanje najvišje stopnje varnosti igralnice. Zato bi bilo z vidika optimizacije in racionalizacije varnostnih procesov, potrebno razmišljati o zasnovi in uveljavitvi koncepta integralne varnosti igralnice, kjer bi v okviru enotne službe obvladovali različna varnostna tveganja, ki se pojavljajo v tekočem poslovanju igralnice. ■

[1] Po Zakonu o igrah na srečo je koncesionar pravna oseba, ki je organizirana kot delniška družba in ima svoj sedež na območju Republike Slovenije. Koncesija se lahko podeli za prirejanje posebnih iger na srečo v igralnem salonu (ponudba iger na srečo samo na igralnih avtomatih) ali v igralnici (ponudba iger na srečo s t.i. živo igro ter na igralnih avtomatih).

[2] Ena od teh služb je že omenjena služba videokontrole, poleg nje pa še službe odgovorne za področje preprečevanja pranja denarja, varovanja informacij, varstva pri delu in požarnega varstva, kadrovsko-pravna služba, služba notranje revizije itd..

[3] Poleg igralnic in igralnih salonov zakon našteje še: banke, hranilnice, menjalnice, pošte in druge subjekte, ki se ukvarjajo z drugimi finančnimi storitvami ali neposredno poslujejo z vrednostmi.

[4] 45. člen Zakona o zasebnem varovanju navaja med drugim, da sme varnostnik uporabljati tudi druge ukrepe, če tako določa zakon, ki ureja posamezno področje. Pri tem pa je tudi omenjeno področje varovanja igralnic.

[5] Skladno s 45. členom Zakona o zasebnem varovanju sme varnostnik pri opravljanju nalog varovanja uporabljati naslednje ukrepe: a) opozorilo, b) ustna odredba, c) ugotavljanje istovetnosti, d) površinski pregled, e) preprečitev vstopa oziroma izstopa iz varovanega območja, f) zadržanje osebe, g) uporaba fizične sile, h) uporaba sredstev za vklepanje in vezanje. Prav tako sme varnostnik pri svojem delu uporabljati plinski razpršilec, službenega psa ter nositi in uporabljati orožje.

[6] Navedeno je recimo primer za Hitove igralniško-zabaviščne centre v Novi Gorici, Kranjski Gori in Šentilju v Slovenskih goricah.

[7] Hall je izraz za območje igralniške recepcije, to se pravi celotno območje vhoda v igralnico.

[8] Navedena delitev varnostnih dogodkov sloni na varnostnih dogodkih v obravnavi s strani varnostne službe v igralnici, evidentiranih s strani avtorja na podlagi različnih virov.

Boris Peršak / strokovni sodelavec za poizvedbe in raziskavo prevar, Generali zavarovalnica d. d.

ZAVAROVALNIŠKE GOLJUFIJE

Zavarovalniška industrija je nastala iz potrebe po varnosti, s ciljem porazdeliti tveganje med več posameznikov, ki imajo skupni interes zaščititi se pred morebitnimi tveganji, ki so negotova, a še vedno verjetna in v preteklosti večkrat izkazana.

Za posameznika je samostojna zaščita pred tveganjem predstavljala prevelik finančni zalogaj, iz praktičnih izkušenj pa je bilo znano, da se tveganja na primer znotraj posamezne interesne oziroma poklicne skupine pojavljajo relativno redko glede na število članov, a je vseeno negotovo, kdaj bodo koga izmed njih prizadela. Ta negotovost je najprej vodila do vzpostavljanja mehanizmov vzajemne pomoči znotraj zaprtih, navadno cehovskih skupin, vendar se je to v začetku dogajalo po škodnem dogodku, ko so zbirali pomoč za cehovskega kolega, ki je utrpel škodo.

Zaradi zbiranja pomoči po nastali škodi je prihajalo do dodatne škode, ko cehovski kolega ni mogel opravljati svojega dela, dokler njegovi delovni pogoji ali sposobnost za delo tega niso omogočali, v primeru smrti zaradi škodnega dogodka pa je družina preminulega ostala brez sredstev preživljanja. Tako vzpostavljena solidarnost je imela svoje pozitivne učinke, a praviloma le znotraj zaprte skupine, ni pa veljala tudi za osebe, odvisne od člana skupine. Možnosti goljufanja znotraj tako zaprte skupine z navadno omejenim številom članov je bila minimalna, saj so se med seboj vsi poznali in o nastali škodi vsi vedeli vse.

Nedvoumno so se manjše interesne skupine z različnih medsebojno ločenih področij povezovale med seboj in je v primeru večjega katastrofalnega dogodka, ki je prizadel eno skupino, na primer večji požar, ena skupina ali več teh pomagala prizadeti skupini, vse po principu vzajemnosti: jaz zate, ti zame. Tudi v teh primerih so bile možnosti za nastanek goljufij majhne, zaradi komponente oddaljenosti med obema okoljema pa ne tudi nemogoče.

> Špekulativni posamezniki, ki so za določeno vsoto prevzemali odgovornost za povračilo morebitne škode, so takšne posle sklepali s čim več interesenti, pri tem pa so za izpolnitev začeli postavljati določene pogoje in izključitvene razloge, kar je pripeljalo do prve preproste standardizacije zavarovalnih pogojev.

Z razvojem matematične znanosti, predvsem s prvimi zametki sodobne statistike, ko so s pomočjo računskih tehnik odkrivali trende nastajanja škodnih dogodkov, se prvič v zgodovini pojavijo napovedi verjetnosti nastanka določenega tveganega dogodka. Dejstvo, da obstaja morebitno tveganje za kogarkoli, da bo postal žrtev neke škode, ki ne samo, da lahko uniči njegovo dejavnost, ampak ogrozi od njega odvisne druge posameznike, je sprožilo sklepanje posebnih terminskih dogovorov med tistimi, ki so bili tem tveganjem podvrženi in špekulativnimi posamezniki, ki so se za določeno vplačano vsoto obvezali, da bodo izpolnili dogovor o povračilu nastale škode, če ta nastane znotraj določenega časovnega obdobja.

Dostikrat so takšni dogovori sprejemniku dogovora o povračilu morebitne škode nalagali tudi povrnitev škode povezanim osebam iz gospodinjstva oškodovanca, s tem pa se je znesek vplačane vsote zavarovalnega dogovora temu primerno povečal, število upravičencev do odškodnine ob nastanku možnega bodočega škodnega dogodka pa ni bilo znano vnaprej, kar je že predstavljalo določeno stopnjo tveganja za morebitno lažno prikazovanje števila članov gospodinjstva oškodovanca. Interesenti za zavarovanje pred tveganji so na drugi strani s povpraševanjem in tudi nezainteresiranostjo po tovrstnih storitvah prisiljevali ponudnike zavarovanj k prilagajanju svoje ponudbe dejanskim potrebam in okoliščinam v določenem času in prostoru.

Prvi tovrstni posli, tudi pred njimi obstoječe cehovske solidarne pomoči, so v porazdelitvi bremena škode za posameznike, ki so prispevali za povrnitev škode, še vedno predstavljali precej veliko breme, to pa je lahko nadalje ogrozilo tudi njihov obstoj in



varnost. Tako so si premije za zavarovanje lahko privoščili le redki posamezniki, velik del oseb, ki bi si morda tudi želele zagotoviti vsaj določeno stopnjo zavarovanja pred najbolj grozečimi in verjetnimi tveganji, pa je iz tega ostala izvzeta.

V primerih, ko so člani zaprte interesne skupine vedeli, da določen posameznik umira ali obstajajo kakšni drugi razlogi, ki bodo zagotovo privedli do njegovega oškodovanja, so solidarno zbrali sredstva za sklenitev dogovora o prevzemu povračila nastale škode z določenim špekulantom, kar je zaradi gotovega nastanka škode pomenilo špekulacijo na strani vnaprej gotovega oškodovanca in vnaprejšnji špekulativni nakup varnosti za povezane osebe. Za osebe, ki so poskušale preslepiti špekulativnega zavarovatelja, so se takšne zgodbe večkrat končale tragično, vendar se je isto lahko zgodilo tudi samim špekulativnim zavarovateljem, kadar so ti iz nesprejemljivih razlogov odklonili izpolnitev dogovorjene obveznosti povračila nastale škode.

Pojavljali so se tudi špekulativni zavarovatelji, ki so pobrali premijo od čim več oseb, z namenom, da nikoli ne izpolnijo danih zavez o povračilu škode, nato pa s tem denarjem pobegnili v neznano. Med kupci varnosti so posamezniki po vplačilu premije lažno prikazovali nastalo škodo ali uprizorili svojo smrt, da bi zase in za povezane osebe pridobili korist, ki jim na podlagi dogovora ni pripadala. Nepošteno ravnanje na katerikoli strani že v prvih dneh zavarovalništva kaže na pojav goljufij, zato so bili nujni nekateri sistemski ukrepi za odpravo slabosti.

S porazdelitvijo tveganja na širši krog interesentov za zavarovanje pred tveganji, so se zmanjšale možnosti za sesutje vzpostavljenega sistema varnosti, pri tem pa so se iz povsem praktičnih razlogov začele oblikovati rezerve za morebitne prihodnje škodne dogodke, kar je pomenilo porazdelitev tveganja za nastanek škod ne samo med večje število posameznikov, ampak tudi na daljše časovno obdobje.

Nemalokrat so špekulativni zavarovatelji imeli dobre informacije o verjetnosti nasprotne špekulacije za pridobitev izplačila za vnaprej znano škodo, zato so takšne dogovore odklanjali, po več takšnih dogodkih pa so začeli ocenjevati bodoče tveganje na podlagi sklenitve dogovora in iz tega izračunavali razmerje med verjetno višino bodoče škode in zneskom, ki bi takšna izplačila škod izravnal z zadostno vsoto vplačanih premij, kar je vplivalo na določitev potrebnega števila zavarovancev v odnosu do določitve višine posamezne premije.

Vse zgoraj opisano je narekovalo vzpostavitev takšne ureditve poslov zavarovanja, da so prevzemniki tveganja in kupci zavarovanj poslovali le pod določenimi reguliranimi pogoji, s tem pa je nastala dejavnost, ki je bila predhodnik današnje sodobne zavarovalniške industrije. Akumulacija teh sredstev je pomenila pasiven kapital, ki je sčasoma zaradi inflacijskih okoliščin izgubljal vrednost, to pa je pripeljalo do pojava dejavnosti za bogatitev zbranih sredstev, da bi ohranjala vsaj enako, če že ne višjo vre-

dnost, kot so jih ta sredstva imela ob plačilu premije. Večji obseg zavarovalnega kapitala pa je pomenil tudi večjo ležernost pri sprejemanju bolj rizičnih tveganj v kritje ter posledično več priložnosti za vlaganje lažnih ali delno neresničnih zahtevkov za povračilo domnevne škode.

Vedno večja kompleksnost zavarovalnih procesov in vedno večje število različnih zavarovalnih vrst je ob naraščanju števila zavarovancev pripeljala do položaja, ko posameznih primerov več ni bilo možno obvladovati »s svinčnikom in kosom papirja« ter se s to dejavnostjo več niso mogli ukvarjati posamezniki. Pojavile so se prve zavarovalne družbe z vzpostavitvijo specifičnih zavarovalnih postopkov in posledično razpršitvijo posameznih specializiranih dejavnosti na več različnih služb znotraj družbe in na večje število zaposlenih. Nadzor nad delom služb in posameznikov je predstavljal kritično komponento, ki je ločnica med obvladovanjem tako notranjih kot tudi zunanjih goljufij, pregled nad celoto zavarovalnih postopkov pa je določal odnos do pojavov goljufij. Z večanjem števila zavarovancev je prišlo do nižanja premij in posledično so te postale dosegljive večini prebivalstva, prav tako se je velikostni razred tveganja za posameznega zavarovanca spustil na tako nizko raven, da je to predstavljalo dober temelj za odpravo negotovosti v morebitno nezmožnost izpolnitve prevzetih zavez za poplačilo oziroma odpravo nastalih škod. Z večanjem števila zavarovancev se je večala tudi verjetnost nastanka škod, med katerimi so se pojavljali tudi lažni zahtevki za škode, ki niso nastale oziroma so nastale v bistveno manjšem obsegu, kar pa se je zopet izravnavalo z večanjem števila zavarovancev in z vračunavanjem tveganja za goljufije v premije.

Danes so razmere na področju tveganja za zavarovalniške goljufije podobne tistim iz začetkov te industrije, spreminjajo se samo pristopi in tehnike, cilj goljufov pa ostaja enak: pridobiti neupravičeno korist na škodo vseh ostalih poštenih plačnikov premij. Razlogi za goljufanje se v času sicer menjujoče spreminjajo in so odvisni od trenutnih ekonomskih razmer, vendar ostajajo v okviru dveh stalnic: priložnostno goljufanje z namenom pridobiti neupravičeno korist, ker se je ravno pokazala možnost (napihovanje obsega škode dejanskega škodnega dogodka, prijava splošne okvare predmeta zavarovanja kot posledice vremenskih dejavnikov, dodajanje domnevno izginulih predmetov po nedavnem vlomu idr.) ter profesionalno goljufanje, ko posameznik zavestno od zavarovalnic zahteva povračilo za domnevno škodo, ki mu ni nastala oziroma jo je povzročil namerno z namenom izplačila odškodnine oziroma zavarovalnine.

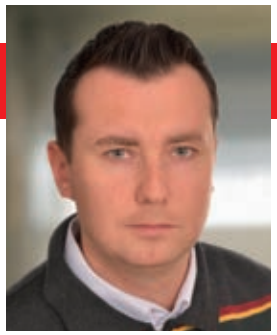


Danes bolj kot kdajkoli prej velja, da se informacije o tehnikah goljufanja zavarovalnic zelo hitro širijo preko elektronskih poti in morajo zavarovalnice tudi same spremljati tovrstne pretoke informacij ter temu primerno prilagajati pogoje zavarovanja. Po drugi strani pa se morajo medsebojno povezovati pri skupnem nastopu zoper goljufe, ki ogrožajo varnost zavarovancev in iz njihovih žepov kradejo denar, ki jim ne pripada. Edina pot je medsebojno povezovanje registrov prijavljenih škod in iskanje povezav med dogodki, osebami in predmeti zavarovanja ter dosledno prijavljanje teh nesprejemljivih ravnanj pristojnim organom pregona.

Največ pa lahko storimo zavarovanci sami, tako da smo pozorni in o zaznanih primerih goljufij obvestimo zavarovalnice ali organe pregona ter ne dovolimo, da nas goljufi potegnejo v svoje igre, iz katerih bomo vedno prišli kot poraženci, saj je cilj goljufov samo in edino neupravičeno polnjenje lastnih žepov na račun vseh nas, ki pošteno plačujemo premije za primer, da se nam kaj zgodi in takrat pričakujemo, da nam bo zavarovalnica stala ob strani. ■

Danes bolj kot kdajkoli prej velja, da se informacije o tehnikah goljufanja zavarovalnic zelo hitro širijo preko elektronskih poti in morajo zavarovalnice tudi same spremljati tovrstne pretoke informacij ter temu primerno prilagajati pogoje zavarovanja.

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



VAROVANJE RAZISKAV V RESNEM KORPORATIVNEM OKOLJU

Za varovanje podatkov v resnem korporativnem okolju so značilne dovršenost, zahtevnost in dinamičnost. To je doseženo z ekspertnim notranjim kadrom, izrazito dobrim poznavanjem resničnih groženj ter rednim spremljanjem ofenzivnih tehnik, taktik in procedur.

Za varovanje raziskovalnih podatkov v resnem korporativnem okolju je pavšalno poznavanje varnostnih tehnologij in njihova sistemska integracija premalo, da bi lahko govorili v vsaj zadostni informacijski varnosti. Za varovanje podatkov v informacijskih sistemih v resnih korporativnih okoljih ne morejo skrbeti IT podjetja, katera pokrivajo bistveno prevelik segment informacijske varnosti, da bi lahko ponujala ekspertno storitev.

Resno korporativno okolje in varovanje raziskav

Pod pojmom resno korporativno okolje[1] smatramo večje organizacije, ki imajo za potrebe zagotavljanja ciljev dobro organizirane formalne organizacijske procese. Še posebej izstopajo dovršene funkcije planiranja, organiziranja, vodenja in kontroliranja, ki so temeljne funkcije upravljalno-ravnalnega procesa. Takšne organizacije delujejo v mednarodnem okolju in jih srečujemo na različnih področjih: biotehnologija in farmacija, napredni materiali, industrijska kemija, informacijsko-komunikacijska tehnologija ipd. Jasno je, da se v sredinah teh organizacij združuje precejšnje raziskovalno, razvojno in analitično znanje.

Varovanje raziskav z različnih področij je pomembno iz številnih razlogov. Na ravni proizvodov in storitev je pogosto razlog ohranjanje oziroma pridobivanje konkurenčne prednosti. Na nekaterih drugih področjih je glavna skrb varstvo osebnih podatkov udeležencev v raziskavah. Poteke in rezultate raziskav je včasih treba varovati pred javnim razkritjem, ker obstaja nevarnost nerazumevanja, napačne interpretacije ali etičnih pomislekov javnosti. Po številu korporacij redka, vendar po obsegu močno prisotna pa je potreba po varovanju raziskav iz geostrateških razlogov.

Poglavitno grožnjo v obravnavanem okolju predstavljajo ofenzivne računalniško-omrežne operacije, ki močno presegajo penetracijske teste, ki jih izvajajo številna IT podjetja.

Pristop k varovanju podatkov v resnih korporativnih okoljih

Zaradi številnih groženj ter posledic, ki jih lahko povzroči izguba raziskovalnih podatkov, je varovanje le-teh na precej boljšem nivoju, kot ga srečujemo v organizacijah v sklopu javne uprave ter malih in srednje velikih podjetjih. Nenazadnje imajo resna korporativna okolja, kot so tehnološke multinacionalke, razvojne oddelke na ravni najuglednejših državnih raziskovalnih inštitutov. Posledično za varovanje podatkov v informacijskih sistemih skrbi visoko kompetenten notranji kader. Poglavitno grožnjo v obravnavanem okolju predstavljajo ofenzivne računalniško-omrežne operacije, ki močno presegajo penetracijske teste, ki jih izvajajo številna IT podjetja. Medtem ko so standardizirane ocene tveganj ter izvajanje varnostnih preizkusov na področju informacijskih sistemov v prvi fazi vzpostavljanja varnosti zaželeni, se je vendarle treba zavedati omejitev. Habib in ostali (2008) izpostavijo preveliko površnost na videz ustreznih varnostnih mehanizmov. Slabe formalne predstavitve pogosto vplivajo na premalo dovršene varnostne smernice.

Že v sami zasnovi sistema je poskrbljeno, da se bo s točno določenimi podatki

*avtor je član Slovenskega združenja korporativne varnosti



seznanil za to pooblaščen kader. Slednje ne zahteva večjih naporov, saj so organizacijski in logično-tehnični ukrepi znani, v pomoč pa so nam še številne smernice in najboljše prakse s področja zavarovanja podatkov v informacijskih sistemih. Večjo nevarnost v korporativnih okoljih predstavljajo »notranji sovražniki«, ki jih predstavljajo pooblaščene, zaupanja vredne osebe z odklonskim ravnanjem. Zato je treba vzpostaviti stanje »who knew«. Pogoj za to pa je uvedba načela »potrebe po vedenju«, ki je pogosto napačno razumljena. Z vidika kontrole dostopa do podatkov načelo preprečuje samovoljno pregledovanje zapisov s strani oseb, ki sicer imajo za to ustrezne dostopne pravice. Bistven je mehanizem, kjer subjekt z nižjim varnostnim dovoljenjem izloči uporabnika z višjim varnostnim dovoljenjem.

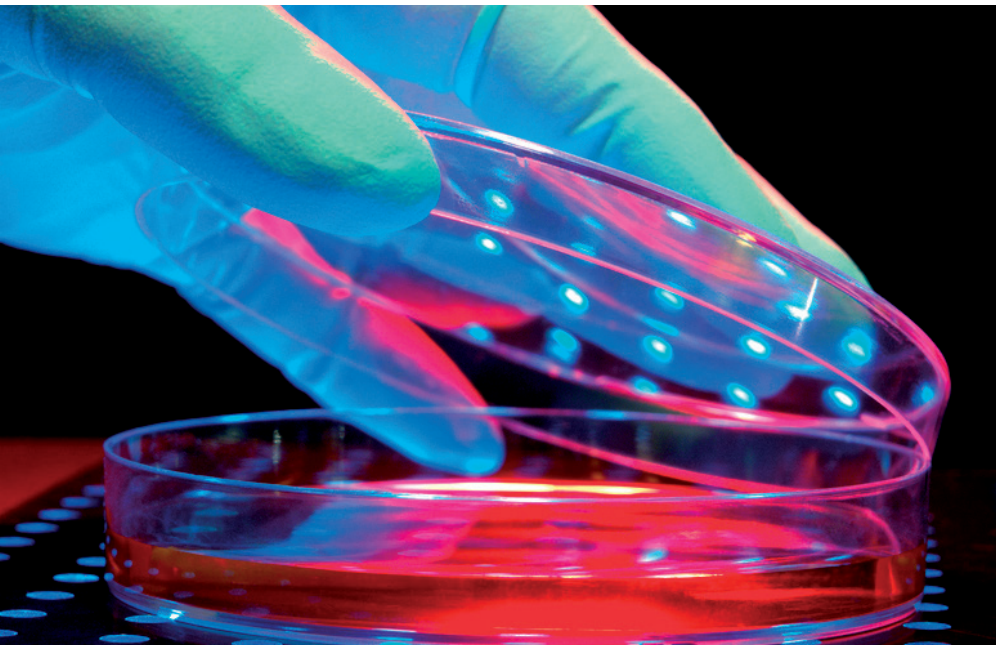
Čeprav bi težko popolnoma izkoreninili število incidentov s strani notranjega sovražnika, jih lahko drastično zmanjšamo. Tako Shaikh in ostali (2011) izpostavijo, da znani modeli kontrole dostopa ne upoštevajo negotovosti in tveganja kot atributov pri dodeljevanju dostopa. Tako je treba poskrbeti za dinamičen mehanizem, ki na podlagi izračuna omenjenih atributov vpliva na dostop subjekta do objekta. V Sloveniji se srečujemo s pomanjkanjem znanja, ki bi omogočal implementacijo ustrezne politike kontrole dostopa. Resna korporativna okolja si to lahko privoščijo, saj za informacijsko varnost skrbi skrbno izbran kader. Tak kader ima izkušnje tako s področja računalniško-omrežnih operacij, poznavanjem resnih varnostnih dogodkov in pogosto prihaja iz tehnološko naprednih okolij.

Pomen visoko kompetentnega kadra znotraj resnih korporacij

Ključni pogoj za zagotavljanje varovanja podatkov je prisotnost najboljšega kadra znotraj posamezne organizacije. Najboljši kader, zaposlen znotraj resnih korporacij, ne samo povečuje varnost, temveč tudi zmanjšuje stroške, potrebne za nabavo in sistemsko integracijo »out-of-box« varnostnih rešitev. Takšen kader ima izkušnje z računalniško-omrežnimi operacijami. Buckshaw in ostali (2005) povedo, da ekipo, ki sodeluje pri varnostnih presojah, med drugim sestavljajo strokovnjaki s področja poznavanja agentov grožnje, razvijalci metod ocenjevanja in izkoriščanja ranljivosti ter sistemski inženirji z znanjem zasnove varnih sistemov. Hkrati ne gre zanemariti sodelovanja z mednarodno akademsko raziskovalno sfero. Ta lahko predlaga številne varnostne rešitve, opozori na nove in nastajajoče grožnje ter najbolj relevantno oceni odzive nanje. Gao in ostali (2012) tako predstavijo kontrolo dostopa na ravni varnega informacijskega sistema za deljenje informacij, ki ustreza večnivojski varnosti. Tak predstavljen informacijski sistem sestoji iz varnega računalniškega okolja, varnega komunikacijskega omrežja, varnostno upravljalnega središča in meje varovanega območja. Wu in ostali (2008) pa predlagajo varen sistem za občutljive podatke, ki omogoča varovanje zaupnosti kljub kompromitaciji sistema ter zaznavanje in preprečevanje prevar.

Pri določitvi in ublažitvi tveganj se uporabljajo različni pristopi. Od osnovnih, ki temeljijo na uporabi

Najboljši kader, zaposlen znotraj resnih korporacij, ne samo povečuje varnost, temveč tudi zmanjšuje stroške, potrebne za nabavo in sistemsko integracijo »out-of-box« varnostnih rešitev.



smernic in najboljših praks, do podrobne analize tveganj, ki predstavlja formalni strukturiran proces. V resnih korporativnih okoljih, kjer je informacijska varnost že v fazi vzpostavitve skladna z zahtevnimi okoljsko specifičnimi standardi, je za kasnejše obravnave najpomembnejši neformalni pristop, ki se izvede z uporabo nabora ekspertov. Pogosto večino teh ekspertov zaradi kompetenc in specifične tehnologije predstavljajo že zaposleni v organizaciji.

Pojav novih in nastajajočih groženj zahteva primeren odziv, ki ga je pametno preučiti skupaj z ljudmi, ki sistematično spremljajo nove ofenzivne tehnike, taktike in procedure. Slednje je eden izmed razlogov, da imajo številne tuje korporacije močnejše kadrovske vire za izvedbo ofenzivnih in defenzivnih računalniško-omrežnih operacij, kot jih posedujejo vladne službe in notranje organizacijske enote obrambnega ministrstva.

Kako naprej v Sloveniji

V Sloveniji nujno potrebujemo visoko vplivne znanstvene konference s področja informacijske varnosti. Pri nas prevladujejo komercialne konference in srečanja. Posledično je možno opaziti, da je znanje vodij informacijske varnosti v organizacijah in oseb, zadolženih za varstvo podatkov, po večini na ravni reklamnih člankov, ki jih pripravijo proizvajalci oziroma uvozniki varnostnih rešitev. Tako ostajajo mehanizmi delovanja »črna škatla« za ključni kader, ki naj bi varoval podatke. To je tudi razlog, ki omogoča ofenzivnim informacijskim operacijam še vedno lahek in popolnoma prikrit dostop do podatkov v navidez odlično zavarovanih okoljih.

V Sloveniji prav tako potrebujemo več osebja, ki pozna in lahko zagotavlja varnost na nižjih, poglobljenih nivojih. Informacijska varnost je preobsežno področje, da bi ga lahko pokrival posameznik. Žal se zaradi nezavedanja te omejitve dogaja, da imamo v Sloveniji poplavo kadra, ki v zelo poprosteni in nerealni obliki sicer pozna varnostne protiukrepe in organizacijske pristope. Žal pa pavšalno poznavanje obravnavanega področja tako kot zaganjanje avtomatiziranih varnostnih ogrodij in že pripravljenih programov ter skript ne ponuja ničesar resnega z vidika varovanja podatkov. Zato tudi pri nas potrebujemo kompetenten kader, zadolžen za varovanje podatkov. V pomoč so lahko naslednje točke:

- Varnostna vprašanja je treba presojati z vidika agentov grožnje, za kar pa je potreben nabor izvornih znanj, seznanjanje z najnovejšimi dognanji in vrhunsko poznavanje nasprotnika.
- Nujna je povezava akademsko-raziskovalne sfere s tujimi ali domačimi korporacijami, ki posedujejo nabor izvornih znanj.
- Pri skrbnikih informacijskih sistemov še vedno ne srečujemo ustreznega kadra. Potrebna je vzpostavitev visoko kompetentnih oddelkov za informacijsko varnost.

Viri

- Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M. in Saydjari, S. O. (2005). Mission Oriented Risk and Design Analysis of Critical Information Systems. *Military Operations Research*, 10 (2), 19–37.
- Gao, C., Xiao, C., Xu, X. in Gao, Y. (2012). Secure Information Systems: Extensions to BLP Model. *Advances in information Sciences and Service Sciences,* 4 (4), 58–65.
- Habib, L., Jaume, M. in Morisset, C. (2008). A formal comparison of the Bell & LaPadula and RBAC models. *Fourth International Conference on Information Assurance and Security.* 3–8. Washington, DC: IEEE Computer Society.
- Shaikh, R. A., Adi, K., Logrippo, L. in Mankovski, S. (2011). Risk-based Decision Method for Access Control Systems. *Ninth Annual International Conference on Privacy, Security and Trust.* 189–192.
- Wu, X., Le, P. D. in Srinivasan, B. (2008). Dynamic Keys Based Sensitive Information System. V Zhang, J. J. (ur.) *9th International Conference for Young Computer Scientists*, 1895–1901. ■

[1] Poleg notranjega sovražnika kot agenta grožnje je v članku predpostavljeno, da je močno razvojno naravnana korporacija, ki deluje v mednarodnem okolju, izpostavljena resnim ofenzivnim informacijskim operacijam. Slednje zahtevajo izvedbeni kader, ki poseduje nabor izvornih znanj in je na ravni »establishmenta« ofenzivnih in defenzivnih informacijskih tehnik, taktik in procedur. Predstavljene grožnje presegajo grožnje, proti katerim je zasnovano varovanje podatkov v informacijskih sistemih v Republiki Sloveniji.

Avtor: Jelenko Vidic / Slovensko združenje korporativne varnosti



RAVNANJE S TVEGANJI

Uporaba varnostnih standardov postaja generator dobička. Zato je naloga varnostnih managerjev, da z uporabo standardov zagotavljajo varne pogoje poslovanja, naloga »strateškega managementa« pa, da jim to omogoči.

Za vzpostavitev in implementacijo procesa ravnanja s tveganji v organizaciji je odgovorno poslovodstvo. Le-to imenuje projektno skupino (Risk management team), ki z uporabo ene ali več metod in tehnik analizira prepoznana tveganja, jih ovrednoti, ter na podlagi ugotovitev razvije zasnovo rešitve za obvladovanje tveganj. Glede na svoje specifike ter prepoznane grožnje, nevarnosti, ranljivosti in tveganja, mora vsaka organizacija izbrati zase najustreznejši pristop. Kot smo opisali že v članku predhodne revije, se v svetovni praksi uporabljajo različni modeli, tehnike, orodja in pristopi. Pri izbiri nam je v veliko pomoč mednarodna standardizacija s področja družbene (societalne) varnosti.

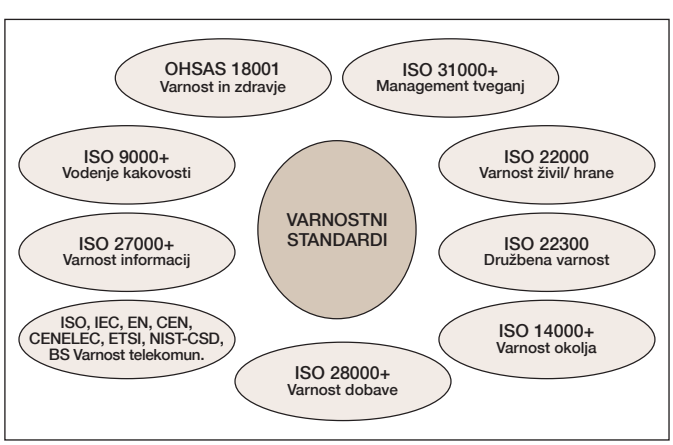
Mednarodna standardizacija s področja družbene (societalne) varnosti

Zaradi porasta kriznih situacij v svetu in pri nas, so napori držav, družbenih entitet, poslovnih skupnosti ter strokovne in akademske javnosti, vse bolj usmerjeni k odkrivanju in vzpostavljanju tehničnih, organizacijskih in upravljalskih pristopov, s ciljem nepretrganega ravnanja v kriznih situacijah. To je bila tudi spodbuda za standardizacijo na tem področju. Za dosego tega je potrebno pospeševati tehnične, človeške, organizacijske in funkcionalne vezi med vsemi zainteresiranimi stranmi s ciljem pripravljenosti na krizne situacije in ustreznega reagiranja ob njihovem pojavu. Z ekonomsko poslovnega vidika lahko rečemo, da uporaba varnostnih standardov postaja generator dobička. Zato je naloga varnostnih managerjev, da z uporabo standardov zagotavljajo varne pogoje poslovanja (Kekić, 2011), naloga »strateškega managementa« pa, da jim to omogoči. Ob enem je standardizacija varnostnih procesov na vseh segmentih korporacijske varnosti tudi pomemben dejavnik zagotavljanja odličnosti (www.ics-institut.si).

Mednarodna standardizacija na področju družbene (societalne) varnosti ima za cilj razvijanje sposobnosti družbe za upravljanje s krizami in zagotavljanje nadaljevanja gospodarskih in poslovnih aktivnosti skupnosti v kriznih pogojih.

Mednarodni standard ISO 31000:2009

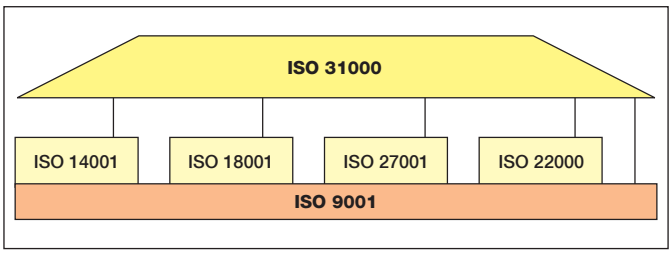
Da bi management tveganj olajšali in poenotili, so v mednarodni organizaciji za standardizacijo ISO ustvarili družino standardov managementa tveganj - ISO 31000 (Risk management). V družino sodijo sprejeti standardi: ISO 31000:2009 Risk Management - Principles and Guidelines on Implementation, ISO/IEC 31010:2009 Risk Management - Risk Assessment Tehniques in ISO Guide 73:2009 Risk Management - Vocabulary. Družina managementa tveganj sodi v skupino varnostnih standardov (slika 1)..



Slika 1: Poenostavljen prikaz mednarodnih varnostnih standardov

Standard ISO 31000 podaja osnovni okvir in smernice za vzpostavitev in implementacijo procesa ravnanja s tveganji v obstoječi sistem vodenja, oziroma podpira oblikovanje,

implementacijo, vzdrževanje in izboljševanje procesov ravnanja s tveganji v integriranih sistemih vodenja (slika 2).



Slika2: Integrirani sistemi vodenja in ravnanje s tveganji

Pomembno je, da je praktična uporaba procesa ocene tveganj določena z metodološkim pristopom. Ocena tveganj mora opredeliti potreben nivo varnosti in zaščite virov organizacije. To je ob enem tudi najbolj zapleten segment ravnanja s tveganji organizacije. Le-ta zahteva, da je integriran v vse organizacijske procese in aktivnosti, da je zagotovljena ustrezna komunikacija ter posvečenost vseh nivojev managementa in zaposlenih vsem korakom ocene tveganja. Tehnike ocenjevanja tveganj so postopki s katerimi se izvaja merjenje, oziroma predvidevajo posledice tveganj, kakor tudi vpliv, ki ga ima pojavljanje tveganja na določen projekt, aktivnost ali dogodek. Ključni dejavniki v proceduri za oceno tveganja, oziroma za izbor modela, pa so razlogi ocene tveganja, vrsta potrebnih rezultatov in dostopnih virov, kompleksnost in velikost ocene, kot tudi vrsta aktivnosti ali sistema ter izbrani incidenti. V odvisnosti od merljivosti rezultata, so tehnike ocenjevanja tveganj lahko:

- kvalitativne – kadar rezultata ni mogoče prikazati številčno-uporabljajo se določene opisne ocene;
- kvantitativne – kadar je rezultat številčno jasen; in
- polkvantitativne – kadar se uporabi kombinacijo predhodnih dveh modelov na posreden način.

Kvalitativna ocena definira verjetnosti in posledice po naprej postavljenih stopnjah (visoka, srednja, nizka itd.). ***Polkvantitativne metode*** uporabljajo številčne skale za določanje verjetnosti in posledice, ter določajo nivo tveganja z njihovo kombinacijo in uporabo matematičnih enačb. ***Kvantitativna analiza*** pa ocenjuje praktične vrednosti posledic in verjetnosti njihovega nastanka in, v tem kontekstu, ocenjuje nivoje tveganj v posebnih enotah. V okviru deskriptivnega modela ocene tveganj so običajno v uporabi naslednje kvalitativne metode (Keković, Nikolić, 2006): 1. preliminarna analiza nevarnosti, analiza nevarnosti in operativnosti, analiza možnih napak in njihovih učinkov; 2. tehnike »drevesne analize« (analiza napak, analiza vzrokov in posledic, analiza tveganj upravljalskih napak; 3. tehnike dinamičnih sistemov (metoda »pojdi na..«, graf/diagraf napak, analiza po Markovu, metodologija analitične logike dinamičnih dogodkov, drevesna analiza dinamičnih dogodkov, ipd.).

Orodja in tehnike za ocenjevanje tveganj po standardu ISO/IEC 31010

Standard ISO/IEC 31010 (Risk Management – Risk Assessment Technique) tehnike ocenjevanja tveganj razvršča v različne skupine, kot so: metode pregleda, podporne metode, analize scenarijev, funkcionalne analize, ocenjevanje kontrol in statistične metode. Poleg tega napotuje na to, kako lahko organizacije naredijo izbor med različnimi tehnikami, da jih lahko uporabijo v posameznem primeru, ter opiše vrsto orodij in tehnik, ki se lahko uporabijo pri ocenjevanju tveganj, oziroma so pomoč v procesu ocenjevanja tveganj. Za vsako fazo procesa ocenjevanja poda tudi primernost uporabnosti posamezne tehnike oziroma metode. V tabelah primeroma podajamo vrste tehnik ocenjevanja (tabela 1), kratek opis tehnike in pomembnost dejavnikov vpliva (tabela 2) ter orodja in tehnike, ki so zelo uporabne za vse faze procesa ocenjevanja tveganj: prepoznavo, analizo in vrednotenje (tabela 3).

Tabela 1: Vrste tehnik ocenjevanja tveganj (vir: IEC/FDIS 31010)

Vrste tehnik ocenjevanja tveganj	
Metode pregleda	**Ocenjevanje kontrol**
Kontrolni listi (CL) Preliminarna analiza nevarnosti (PHA)	Analiza ovir (BA/LOPA) (analiza nivoja zaščite), Analiza vozlišč (napak,vzrokov,posledic) BTA
Podporne metode	**Statistične metode**
Strukturirani intervjuji in viharjenje, Delphi tehnika, Strukturirana vprašanja »kaj če?«, SWIFTAnaliza človeške zanesljivosti (HRA)	Analiza po Markovu, Monte-Carloanaliza, Analiza po Bayesu
Analize scenarijev	**Funkcionalne analize**
Analiza temeljnih vzrokov (RCA) Analiza scenarijev (SA), Ocenjevanje toksikoloških tveganj(TRA), Analiza vplivov na poslovanje (BIA), Drevesna analiza napak (FTA), Drevesna analiza dogodkov (ETA), Analiza vzrokov in posledic (C/CA), Analiza vzrokov in učinkov (C/EA)	Analiza možnih napak-učinkov -FMEA/FMECA Analiza zanesljivosti vzdrževanja (RCM), Analiza prikritih napak (SCA), Analiza nevarnosti in operativnosti (HAZOP), Analiza nevarnosti in kritičnih kontrolnih točk (HACCP)

Tabela 2 : Opis posamezne tehnike in pomembnosti dejavnikov vpliva (vir:IEC/FDIS 31010)

Vrsta tehnike	Opis	Pomembnost dejavnikov vpliva			Kvantitativni rezultat
		Viri in zmožnosti	Narava in stopnja negotovosti	Kompleksnost	
Preliminarna analiza nevarnosti	Prepoznava nevarnosti, nevarnih situacij in dogodkov	**nizka**	**visoka**	**srednja**	**Ne**
Analiza človeške zanesljivosti	Vpliv človeških dejavnikov na delovanje sistema (ocena vpliva človeških napak)	**srednja**	**srednja**	**srednja**	**Da**
Analiza scenarijev	Kvalitativna ali kvantitativna prepoznava možnih scenarijev temelječih na trenutnem ali različnih tveganjih	**srednja**	**visoka**	**srednja**	**Ne**
Drevesna analiza napak	Grafični prikaz možnih pojavov dogodka (logični diagram) in razmišljanje o zmanjšanju/odpravi potencialnih vzrokov	**visoka**	**visoka**	**srednja**	**Da**
Analiza vozlišč	Opis in analiza krivulje tveganj od nevarnosti do posledic ter pregled kontrol	**srednja**	**visoka**	**srednja**	**Da**

Tabela 3: Vrste orodij in tehnik ocenjevanja tveganj (vir: IEC/FDIS 31010)[1]

Orodja in tehnike	Proces ocenjevanja tveganj				
	Prepoznava tveganj	Analiza tveganj			Vrednotenje tveganj
		Posledice	Verjetnost	Stopnja tveganja	
Ocenjevanje okoljskih tveganj	**ZU**	**ZU**	**ZU**	**ZU**	**ZU**
Strukturirana vpr. »kaj če?« (SWIFT)	**ZU**	**ZU**	**ZU**	**ZU**	**ZU**
Analiza možnih napak in učinkov	**ZU**	**ZU**	**ZU**	**ZU**	**ZU**
Analiza človeške zanesljivosti	ZU	**ZU**	**ZU**	**ZU**	U
Analiza zanesljivosti vzdrževanja	**ZU**	**ZU**	**ZU**	**ZU**	**ZU**
Analiza temeljnih vzrokov	NU	**ZU**	**ZU**	**ZU**	**ZU**
Matrika posledic/verjetnosti	**ZU**	**ZU**	**ZU**	**ZU**	U

V standardu so podani tudi nekateri referenčni dokumenti, kjer se lahko podrobneje seznanimo s posameznimi tehnikami, kot npr.:

- IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector,*
- IEC 61508 *Functional safety of electrical/electronic/ programmable electronic safety - related systems* (all parts),
- IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide,*
- ISO 22000, *Food safety management systems – Requirements for any organization in the food chain,*
- ISO/IEC Guide 51, *Safety aspects – Guide lines for their inclusion in standards,*
- IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance,*
- IEC 61649, *Weibull analysis,*
- IEC 61078, *Analys is techniques for dependability – Reliability block diagram and boolean Methods,*
- IEC 61165, *Application of Markov techniques,*
- ISO/IEC 15909 (allparts), *Software and systems engineering – High-level Petri nets,*
- IEC 62551, *Analysis techniques for dependability – Petri net techniques,*
- IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide.*



Sklepno

Iz kratkega prikaza izhaja neizogibna potreba po integraciji različnih sistemov vodenja. To se kaže v porastu števila organizacij, ki imajo dva ali več integriranih sistemov vodenja. Vloga integriranih standardov/sistemov je v tem, da definirajo vse aktivnosti procesov, prepoznajo vse vidike in nevarnosti, ki vplivajo na življenjsko in delovno okolje, splošno varnost, varnost informacij itd., ter določijo ukrepe za zmanjšanje vseh tveganj. Kot temeljno izhodišče za integracijo se uporablja družina standardov ISO 9000. Ostali so nadgradnja in se v nekaterih vidikih popolnoma opirajo na procesni pristop, PDCA, ipd. V zadnji spremembi standarda ISO 9001:2008 je prepoznano dejstvo, da so tveganja eden od ključnih elementov, ki odrejajo celovito vodenje kakovosti. S to verzijo standarda se tudi formalno pristopa k problemom ravnanja s tveganji v okviru sistema vodenja kakovosti, predvsem pri upravljanju poslovnih procesov. Tako morajo organizacije v sistem vodenja kakovosti vključiti tudi ravnanje s tveganji, oziroma dokazati, da obvladujejo poslovna tveganja.

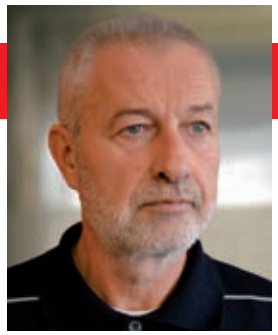
V uvodu članka smo zapisali, da morajo organizacije za vzpostavljanje in implementacijo ravnanja s tveganji najti zase najustreznejši pristop. Pri tem se nam zastavlja vprašanje, kateri pristop pa je to? Za ene je izbor pristopa »zelo preprost«, za druge pa »nočna mora«. Dejansko je nekje vmes, seveda odvisno od tega kakšno znanje imamo, kako na stvari gledamo, jih dojemamo in razumemo. Druga plat medalje pa so varnostni interesi lastnikov in poslovodstva ter njihova pripravljenost za celovito ravnanje s tveganji v svoji organizaciji. Skratka, iz prikazanega izhaja, da je na razpolago veliko metod, tehnik in orodij. Potrebna je samo volja za resen pristop k obvladovanju tveganj.

Viri

- IEC/FDIS31010:2009(E):Risk Management - Risk Assessment Tehniques. Pridobljeno
- 25.10.2012 na http://www.previ.be/pdf/31010_FDIS.pdf.
- Keković, Z. in Nikolić, V.(2006). *Metode analize hazarda i rizika.* V: Keković, Z. in Kešetović, Ž. Krizni menadžment I, Prevencija krize. Univerzitet u Beogradu, Fakultet bezbednosti. 2006.
- Keković, Z., Savić, S., Komazec, N. in drugi (2011). Procena rizika u zaštiti lica, imovine i poslovanja. Centar za analizu rizika i upravljanje krizama. Beograd, 2011.
- Spletna stran Instituta za korporativne varnostne študije - www.ics-institut.si. ■

[1] V standardu je podanih 31 orodij in tehnik. Njihovo uporabnost za posamezno fazo ocenjevanja označi kot: zelo uporabna, uporabna, ni uporabna.

Avtor: Vito Murgel, univ. dipl. ekon. / Svetovalec direktorja, NovaPanorama d.o.o.



MEDNARODNI SEJMI KOT ZNANILCI SMERI RAZVOJA NA PODROČJU VARNOSTI "SECURITY ESSEN 2012"

Letošnji sejem Security Essen je bil že dvajseti po vrsti. Kot eden najpomembnejših sejmov na področju varnosti pred požari in varovanja premoženja združuje proizvajalce iz vsega sveta, ki vsakokrat prikažejo zadnje smernice v razvoju sistemskih rešitev, tehnologije in programske opreme za preventivno delovanje na tem področju.

Eno od pomembnih področij, za katere so razstavljalci prikazali sistemske rešitve, je bilo celovito zagotavljanje varnosti javnih prostorov, prometna varnost, nadzor in varnost objektov in naprav.

Hitro razvijajoči segment je tudi področje varovanja regionalnih mej in alarmiranja prebivalstva ob naravnih in drugih nesrečah. Sejem v Essnu je stičišče, kjer se srečajo proizvajalci/ponudniki s predstavniki državnih in meddržavnih institucij in izmenjujejo poglede ter rešitve tudi na tem področju.

Današnji hiter razvoj na področju mobilne telefonije je omogočil tudi hiter razvoj aplikacij, s katerimi je mogoče preko t.i. pametnih telefonov, ne samo spremljati dogajanje na določeni lokaciji, objektu ali prostoru, pač pa programska oprema za pametne telefone omogoča celovito upravljanje in nadzor vseh funkcij sistemov na področju požarne varnosti in področju varovanju premoženja.

Pametni telefoni so uporabni tudi kot brezkontaktni ključi za odpiranje vrat in kot brezkontaktne kartice pristopne kontrole in registracije delovnega časa.

Razvoj IP kamer je šel v smeri izrednega povečanja kakovosti slike istočasno z razvojem sofisticirane sistemske opreme, ki ob varnostnem incidentu, avtomatično prikaže in pre-





pozna osebe, ki so povzročile incident. Kakovostna slika se zajema v HD resoluciji (1.920x1.080pikslov), programska oprema snemalnih naprav pa omogoča vrsto naprednih nastavitev tako kamer samih kot načina, kako so posnetki shranjeni. Vedno bolj prihajajo v ospredje tudi 360° panoramske kamere, saj lahko zaradi svoje funkcionalnosti ena taka kamera nadomesti 2 do 3 kamere z običajnim vidnim poljem.

Letošnji sejem v Essnu je dal velik poudarek na varnosti pred požari tako v sektorju industrije kot tudi sektorju privatnih hiš ter stanovanjskih enot v blokih. Rešitve na področju požarne varnosti se razvijajo v smeri vedno tesnejšega sistemskega povezovanja s področjem varovanja premoženja, saj je veliko razstavljalcev prikazalo programsko opremo, ki združuje nadzor in upravljanje tako protipožarnih sistemov in sistemov za varovanja premoženja v eni sistemski rešitvi – centralni nadzorno/upravljalni enoti.

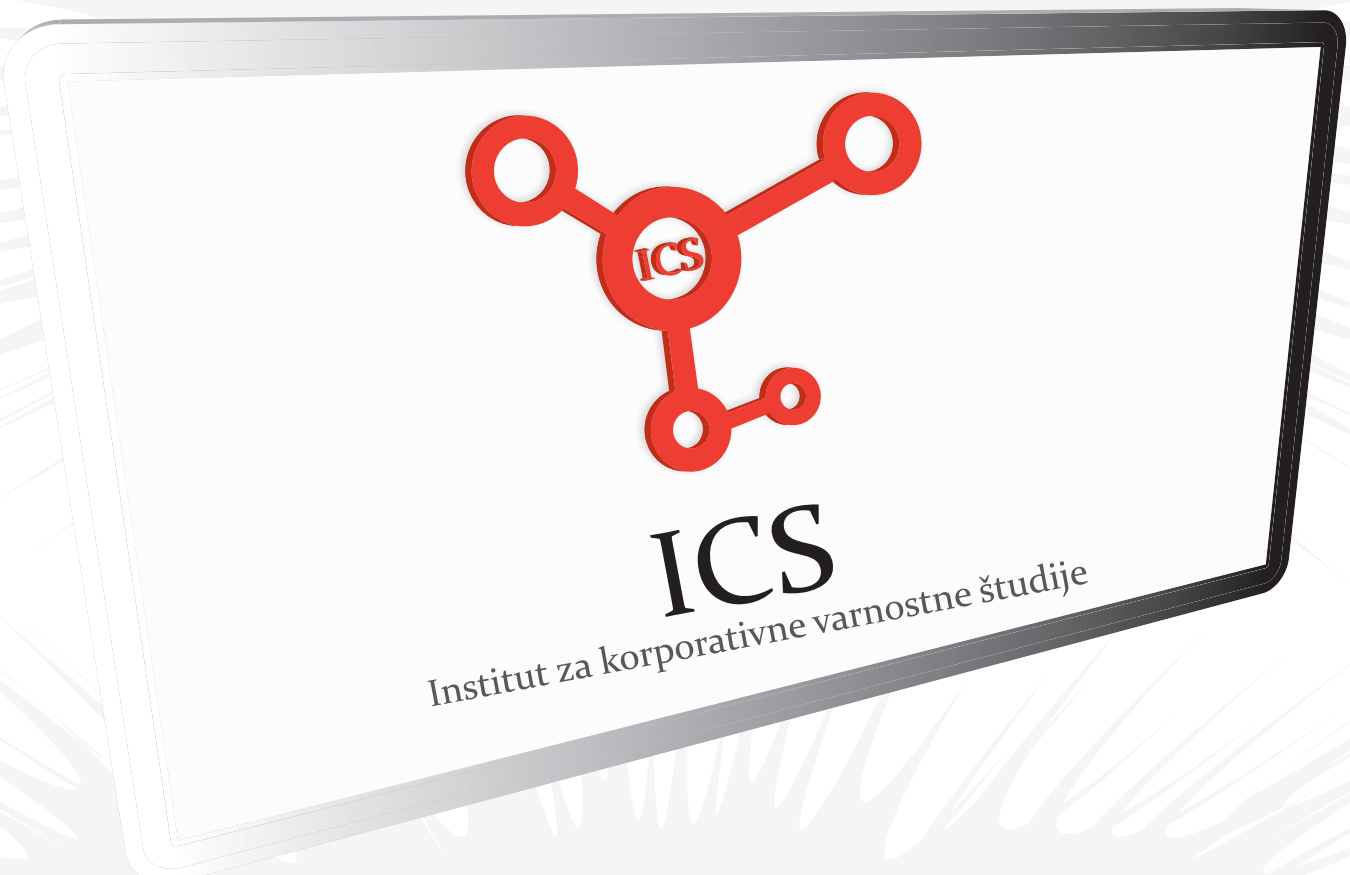
Prikazane so bile tudi rešitve za prenos vseh komunikacij v danes tako popularen oblak, preko katerega prav tako lahko nadzorujemo/upravljamo vse sisteme.

Prikazan je bil tudi nov način za zgodnje odkrivanje požara z optičnim detektorjem brez plina, katerega bistvena prednost je v hitrosti zaznavanja požara.

Za zaključek je pomembno poudariti, da je regionalno področje Slovenije del evropskega področja in standardi na področju varovanja, ki so implementirani v Evropski skupnosti, postajajo del našega vsakdana. Zato je Security Essen odličen prikazovalnik smeri, v katero se mora razvijati tudi naše razmišljanje o varovanju premoženja v celoti. ■

Današnji hiter razvoj na področju mobilne telefonije je omogočil tudi hiter razvoj aplikacij, s katerimi je mogoče preko t.i. pametnih telefonov, ne samo spremljati dogajanje na določeni lokaciji, objektu ali prostoru, pač pa programska oprema za pametne telefone omogoča celovito upravljanje in nadzor vseh funkcij sistemov na področju požarne varnosti in področju varovanju premoženja.

Slovenian Grand Security Award 2012



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

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

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

www.ics-institut.si

TERMOELEKTRARNA TOPLARNA LJUBLJANA



Energetsko srce Ljubljane

Odločno gradimo nizkoogljično prihodnost prestolnice. S toplotno in električno energijo, proizvedeno iz lesne biomase, smo v letu 2009 zmanjšali izpuste CO_2 za 67.000 ton. Z uvedbo zemeljskega plina leta 2015 bo naš ogljični odtis še manjši.

zmanjšujemo CO_2 energija iz obnovljivih virov

www.te-tol.si
m.te-tol.si