PIŠE: **Nastja Strnad**, redaktorica

DR. DENIS ČALETA: »Korporativne varnosti SE MORAMO LOTITI STRATEŠKO«



Dr. Čaleta – profesor na GEA College, priznani strokovnjak za področje korporativne varnosti, predsednik Inštituta za korporativno varnost (ICS), dejaven na veliki mednarodni konferenci v Sloveniji – Counter terrorism challenges in Region of SE Europe. Ob dogodku je s kolegico dr. Corinno A. Robinson iz ZDA izdal novo knjigo z naslovom »Violent Extremism and Radicalization Processes as Driving Factors to Terrorism Threats«.

S katerimi tveganji se soočajo sodobne organizacije – katera tveganja so najbolj razširjena in ali nastajajo nova?

Poslovno okolje, v katerem poslujejo naše organizacije, je vedno bolj kompleksno in prežeto s celim nizom varnostnih tveganj. Neprekinjenost delovanja naših organizacij ter poslovno učinkovito, varno in skladno poslovanje še naprej ostajata ključni cilj vsakega strateškega menedžmenta. Za zagotavljanje teh ciljev pa se je treba zavedati tveganj, ki so jim izpostavljene naše organizacije. Ob klasičnih tveganjih kriminala, tehnoloških nesrečah, kot posledicah neustreznega upravljanja z infrastrukturo, terorizma, odtekanja ključnih poslovnih informacij, nam Informacijska doba vsekakor prinaša povečanje tveganj, ki prihajajo iz kibernetskega okolja. Prav tako so vedno bolj poudarjena tveganja, ki so povezana z zaposlenimi v naših organizacijah, da tveganj, ki jih prinaša spremenjeno geopolitično okolje, kot so migracije in s tem povezani dejavniki, sploh ne poudarjamo.

Lahko postrežete s kakšnim konkretnim primerom, ko je podjetje preprečilo nastanek škode zaradi zavedanja pomena korporativne varnosti ali pa ravno obratno – ko tega ni storilo?

Primeri dobrega upravljanja s korporativno varnostjo se zrcalijo skozi vsa podjetja, ki uspešno poslujejo in zagotavljajo neprekinjenost delovanja svoje osnovne poslovne dejavnosti. Vedno pa v javnosti odmevajo tisti primeri, ki kažejo na odsotnost ustreznega varnostnega zavedanja v posameznih poslovnih sredinah, kar ima za posledico tudi varnostne incidente. Seveda veliko število varnostnih incidentov nikoli ne pride v javnost, saj jih želijo podjetja zaradi ohranitve dobrega imena, prikriti. Naj omenimo samo nekatere, ki so v preteklosti odmevali v Sloveniji, in sicer primer Kemisa, pranje denarja v bančnem sektorju, informacijski vdori v cel niz slovenskih podjetij, ki so prinesli pomembne finančne izgube ali omejevanje neprekinjenosti delovanja organizacij, zlorabe položajev in notranje prevare. V tujini je bilo kar nekaj primerov odtujevanja ključnih informacij in podatkov tako iz državnih institucij kakor tudi iz poslovnega okolja. Procesov radikalizacije med zaposlenimi in možnih strelskih situacij AMOK sploh ne omenjam, ker so v zahodnih družbah, predvsem v ZDA, postali stalnica. Vsi ti primeri imajo isto izhodiščno točko, in sicer nedelovanje sistema korporativne varnosti in nadzornih mehanizmov v organizaciji.

Je poklic menedžerja korporativne varnosti poklic prihodnosti ali je že uveljavljen v podjetjih? Kakšen delež slovenskih podjetij že ima tovrstne strokovnjake?

Vsa resna večja podjetja že imajo ali pospešeno vzpostavljajo funkcije korporativne varnosti ter tako poskušajo povezati vse procese, ki se nanašajo na področje obvladovanja in upravljanja z varnostnimi tveganji v organizaciji. Celovito področje korporativne varnosti za ustrezno obvladovanje varnostnih tveganj v korporaciji nujno vključuje področje varnosti, procesa neprekinjenega poslovanja, informacijske varnosti, varovanja ključnih informacij podjetja, varnosti zaposlenih in varnosti pri delu. Procesi zagotavljanja korporativne varnosti so nedeljiva celota krovnega modela upravljanja korporacij, ki se izraža skozi korporativno upravljanje in korporativno družbeno odgovornost. Posebej so tukaj izpostavljena podjetja, ki upravljajo določeno kritično infrastrukturo, ki je pomembna ne samo za delovanje samega podjetja, temveč tudi širšega družbenega okolja. Seveda tudi druga srednja in velika podjetja pospešeno vzpostavljajo te funkcije. Večja težava je pri mikro in malih podjetjih, ki si tako funkcijo težko privoščijo znotraj podjetja – storitev sicer dobijo na trgu, ki pa je pri nas na žalost še slabo razvit. Vse to predstavlja velik potencial za zaposlovanje korporativno varnostnih strokovnjakov.

V okviru GEA College predavate na študijskem programu Upravljanje s tveganji in korporativna varnost, ki je edini na tem področju v Sloveniji. Kdo

so udeleženci programa, za prenos katerih znanj in veščin skrbite?

Kompleksnost procesa korporativne varnosti od kadrov zahteva multifunkcionalna znanja. Korporativni varnostni menedžer mora imeti poleg varnostnih znanj tudi znanja s področja prava, podjetništva, informatike, financ, psihologije in organizacije, kar posledično pomeni, da takega kadra v Sloveniji in tudi v mednarodnem okolju močno primanjkuje. V Republiki Sloveniji smo na tem področju dokaj hitro stopili korak v pravo smer. Na Fakulteti za podjetništvo/GEA College se je oblikoval magistrski program z nazivom »Upravljanje tveganj in korporativna varnost«, kjer diplomanti dobijo vsa potrebna multidimenzionalna znanja za oblikovanje ustreznih kompetenc, ki jih od strokovnjaka na področju korporativne varnosti zahteva globalno poslovno okolje. Pri razvoju strokovnjakov z omenjenega področja pa imata pomembno vlogo tudi Institut za korporativne varnostne študije in Slovensko združenje za korporativno varnost, ki v svojem obsegu združuje praktično vsa najpomembnejša podjetja v Sloveniji.

V okviru Instituta za korporativne varnostne študije podeljujete nagrade za dobre prakse na tem področju. Kdo so aktualni prejemniki Slovenske velike nagrade varnosti?

Slovenci smo narod, ki se neradi hvalimo s svojimi dosežki, kar je po moji oceni napačno, saj imamo nekaj odličnih organizacijskih sredin, ki so tudi na področju obvladovanja tveganj lahko za vzor drugim. Institut za korporativne varnostne študije in Slovensko združenje za korporativno varnost vsako leto, v šestih kategorijah, podeljujeta prestižno nagrado »Slovenian Grand Security Award«, ki jo med drugimi prejmejo tudi najbolj varna podjetja in najboljši korporativno varnostni menedžerji leta. Med temi velja zagotovo iskati odgovor na vprašanje, kje imamo najboljše prakse. Na žalost imamo tudi celo vrsto negativnih primerov, o katerih poročajo mediji, predvsem, ko govorimo o nekaterih deviantnih okoliščinah. Na vseh nas je, da to stopnjo zavedanja dvignemo v celotni družbi.

Koliko so slovenska podjetja lahko tarča takim tveganjem, koliko se teh tveganj moramo »bati«?

Enostavno rečeno, si določen del strateškega menedžmenta v podjetjih zatiska oči pred raznovrstnimi varnostnimi tveganji, ki so jim vedno bolj izpostavljena tudi slovenska podjetja. Še posebej so temu izpostavljena tista podjetja, ki poslujejo v globalnem okolju. Neupoštevanje realnih tveganj za poslovanje podjetja se lahko za tako podjetje konča zelo negativno, in sicer z zmanjšanjem dohodka, izgubo konkurenčne prednosti, lahko pa tudi tragično z izgubo življenj zaposlenih ali celo s propadom podjetja. Na srečo se število takih neodgovornih menedžerjev zmanjšuje. Informatizacija postaja dejavnik spremembe poslovnega okolja in procesov. Poleg mnogovrstnih pozitivnih stvari pa je na področju varnosti ta proces prinesel veliko tveganj. Iz analize preteklih izkušenj lahko vidimo, da so tudi slovenska podjetja vedno bolj podvržena varnostnim tveganjem, ki izhajajo iz tega okolja. Vdori v informacijske sisteme, spletne banke in plačilne sisteme podjetij, odtujitev podatkov, širjenje zlonamernih kod in virusov ter druga informacijska tveganja so v današnjem kibernetskem okolju postala stalnica. Poleg sistemskih pristopov na področju zagotavljanja informacijske varnosti lahko tukaj storimo največ na ozaveščanju in usposabljanju svojih zaposlenih. Popolne varnosti pa na žalost tudi na tem področju ni mogoče zagotoviti. Zato je pomembno, da ta tveganja zmanjšamo na še sprejemljivo raven, ki nima bistvenega vpliva na učinkovitost našega poslovanja.

> »Neupoštevanje realnih tveganj za poslovanje podjetja se lahko za tako podjetje konča zelo negativno, in sicer z zmanjšanjem dohodka, izgubo konkurenčne prednosti, lahko pa tudi tragično z izgubo življenj zaposlenih ali celo s propadom podjetja.«

Morda kakšen nasvet, kako naj se podjetja lotijo urejanja tega področja?

Vsekakor se je treba zadeve lotiti sistemsko, strateško vodstvo pa mora tudi s svojim zgledom v vsakem trenutku nuditi ustrezno podporo za uveljavitev ključnih ukrepov v organizacijah. Seveda so finance potreben dejavnik učinkovitosti obvladovanja tveganj, niso pa edini. Samo z veliko količino finančnih vložkov se čez noč ne da reševati določenih tveganj, ki jim je izpostavljeno podjetje. S takimi nesistemskimi pristopi največkrat doživimo razočaranje glede vloženih sredstev in dobljenih rezultatov. Področje zagotavljanja korporativne varnosti je dolgotrajen proces, ki se ga je treba lotevati načrtno in premišljeno. Največkrat se pri strateškem menedžmentu in lastnikih postavlja vprašanje o merljivih učinkih korporativne varnosti. V Institutu za korporativne varnostne študije smo razvili ustrezne metode za izračun teh učinkov na poslovanje podjetja in ga tudi finančno ovrednotili. Treba pa se je zavedati, da so nekateri učinki dolgoročne narave in jih je težje matematično izmeriti. Vsekakor smo vedno pripravljeni priskočiti na pomoč pri izgrajevanju sistemov korporativne varnosti.

