Korporativna varnost

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

Letnik 2019, junij • št. 20



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

Moderno varnostno okolje postavlja pomembne izzive za varovanje zasebnosti

ga. Mojca Prelesnik, Informacijska pooblaščenka Republike Slovenije



30 PREDANI ODLIČNOSTI | NIL

nil.com



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
junij 2019

Izvod revije je brezplačen

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

ISSN 2232-6170

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

Letos smo priča pomembnima jubilejoma, ki ju prinaša deseta obletnica delovanja Instituta za korporativne varnostne študije, ICS-Ljubljana in Slovenskega združenja za korporativno varnost, kateri je prerasel v najpomembnejšo strokovno-civilno asociacijo s področja varnosti v Republiki Sloveniji. Tokrat pa imamo pred seboj še prav poseben jubilej in sicer 20. številko strokovne revije Korporativna varnost. V uredniškem odboru, s ponosom in veseljem, gledamo na prehojeno pot, ki se je odrazila v dvajsetih številkah omenjene revije Korporativna varnost. Kar pa je najpomembneje, da revija skozi celotno področje svojega izhajanja strokovno raste in svoj obseg strokovnih tem širi na različna področja, ki so posredno in neposredno povezana s celovitim obvladovanjem varnostnih tveganj. Pri izdelavi vsake številke revije se porajajo osnovna vprašanja »ali smo bili vsebinsko dovolj aktualni in provokativni, da bomo zadovoljili zahtevna pričakovanja naših bralcev?«. Dosedanji odzivi so bili vedno zelo pozitivni, še več, pojavlja se vedno več avtorjev, ki bi želeli svoja strokovna spoznanja in dobre prakse skozi revijo deliti s širšo strokovno javnostjo. Kar pa nam je v uredniškem odboru izredno pomembno in si štejemo za poseben uspeh, pa predstavlja dejstvo, da revijo prebira vedno več predstavnikov strateškega managementa. To dejstvo je pomembno iz večih vidikov, prvi je vsekakor, da smo uspeli tudi s pomočjo revije Korporativna varnost dvigovati varnostno zavedanje vseh tistih, ki v organizacijah javnega in gospodarskega okolja odločajo o strateških odločitvah in so odgovorni za učinkovito delovanje organizacij. Drugi zelo pomemben vidik pa je, da strateški management v vedno večih organizacijah prepozna proces korporativne varnosti in strokovnjake, ki ga izvajajo, kot pomembno orodje in pomoč pri zagotavljanju obvladovanja tveganj, katerim so podvržene organizacije pri svojem delovanju v kompleksnem in zahtevnem poslovnem okolju. In zadnje, vendar ne nepomembno, strateški management, se skozi vsebine, ki jih prinaša revija, tudi izobražuje in širi svoja znanja na področja, ki so zelo pomembna za učinkovitejše sprejemanje odločitev v zahtevnih razmerah konkurenčnega mednarodnega trga, kjer poslujejo slovenske organizacije. Vse to dokazuje, da je kljub začetnim izjavam iz določenih krogov, »da ta petelin v družbi, ki ni pripravljena razumeti pomena teh znanj s področja korporativne varnosti, prezgodaj kikirika«, lahko danes z gotovostjo rečemo, da so vsebina in strokovna znanja, ki jih širimo, tudi s pomočjo visoko strokovne revije, še kako slišana in tudi upoštevana.

V tokratni jubilejni številki ponovno odpiramo pomembne teme, ki pa so tokrat zelo tesno povezane z različnimi procesi zaščite kritične infrastrukture in zagotavljanja kibernetske varnosti. Revija pa, kot je že v navadi, prinaša zanimive intervjuje z odločevalci strateškega okolja. Nova znanja in rešitve, ki jih prinašamo na področje metodologije ocenjevanja tveganj v kritični infrastrukturi in modelom vzpostavljanja javno-zasebnega sodelovanja v organizacijah, katere upravljajo kritično infrastrukturo, pa so tista ključna vsebina tokratne številke.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



KOLUMNA

BO DRŽAVA ZNALA IZKORISTITI TO POMEMBNO PRILOŽNOST?

9



METODOLOGIJA ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

Ocenjevanje, upravljanje in obvladovanje tveganj za delovanje kritične infrastrukture (v nadaljevanju: KI) je kompleksno in interdisciplinarno zahtevno delo. Pristop k ocenjevanju tveganj je metodično zasnovan na principih sistemskega inženiringa, vsebinsko na preprečevanju možnih škod in izgub, operativno pa na sodobnih rešitvah upravljanja in obvladovanja tveganj.

14



IZZIVI UPRAVLJANJA TVEGANJ V KRITIČNI INFRASTRUKTURI

V prispevku bomo kratko pregledali bistvene izzive upravljanja tveganj v kritični infrastrukturi, s katerimi se bodo soočali vsi deležniki, ki v sistemu zagotavljajo zaščito in neprekinjeno delovanje kritične infrastrukture. Sprejeti zakonodajni okvir je postavil minimalne standarde na področju zagotavljanja varnosti in obvladovanja tveganj v kritični infrastrukturi.

19



GDPR IN (NE)DOLOČENOST ZAVAROVANJA OSEBNIH PODATKOV

V zadnjih letih se je, tudi zaradi javnega izpostavljanja nekaterih primerov neustreznega zavarovanja osebnih podatkov v slovenskih institucijah, večkrat odprlo vprašanje ali smo kot družba ustrezno pripravljeni na izzive zagotavljanja informacijske varnosti, še posebej, ko gre za varovanje osebnih podatkov.

28



IZZIVI UVAJANJA IOT V OPERATIVNE POSLOVNE PROCESE

Internet stvari (ang. IoT - Internet of Things) ali internet vsega (ang. IoE – Internet of Everything) se nanaša na omrežja naprav z dodeljenim IP naslovom. Te naprave imajo sposobnost zaznavanja, zbiranja in pošiljanja podatkov z uporabo vgrajenih senzorjev, komunikacijske opreme in procesorja. IoT je tehnologija, ki je zmožna sprožiti pravo revolucijo na način življenja, kot ga živimo danes.

33

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
ga. Mojca Prelesnik
Informacijska pooblaščenka Republike Slovenije

MODERNO VARNOSTNO OKOLJE POSTAVLJA POMEMBNE IZZIVE ZA VAROVANJE ZASEBNOSTI

Moderno in dinamično varnostno okolje pred nas prinaša vedno nova tveganja in izzive, na drugi strani pa tehnologija napreduje z nesluteno hitrostjo. Če v ta okvir dodamo še dvigovanje zavedanja posameznikov o pomembnosti varovanja zasebnosti in osebnih podatkov, lahko z gotovostjo potrdimo, da je to področje trenutno podvrženo velikim izzivom, ki jih je potrebno ustrezno uravnavati. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se ob koncu prvega mandata na mestu Informacijskega pooblaščenca Republike Slovenije, pogovarjali z gospo Mojco Prelesnik.

Pred vami je končanje prvega mandata na izredno pomembni funkciji Informacijskega pooblaščenca. Kaj bi izpostavili kot temeljne pridobitve tega mandata?

Menim, da je treba izpostaviti predvsem učinkovit prehod na novo pravno ureditev varstva osebnih podatkov, ki jo je prinesla Splošna uredba o varstvu podatkov (GDPR), kljub številnim pomislekom in strahovom številnih upravljavcev zbirk osebnih podatkov. Prehod ni bil lahek, saj smo se soočili z velikim porastom števila prijav, telefonskih klicev, zaprosil za mnenja in javne nastope, ob vsem tem, pa smo tudi mi sami morali dodobra spoznavati nove določbe in prilagajati naše notranje procese in postopke. Informacijski pooblaščenec je reorganiziral in okrepil svoje oddelke tako na področju nadzora kot na področju skladnosti in preventive in tako še bolj intenzivno prispeval k varovanju osebnih podatkov. Vesela sem, da nam je uspelo prepoznati in nasloviti tudi ključne težave in vprašanja, s katerimi so se ob prehodu na nov predpis srečevali upravljavci zbirk osebnih podatkov.

> Nemogoče je od malih podjetij, ki predstavljajo več kot 90% vseh slovenskih podjetij, pričakovati poznavanje 250 členov zakonodaje o varstvu osebnih podatkov, s tem pa tudi ne moremo govoriti o zagotavljanju učinkovitega varovanja naših podatkov.

*avtor je član Slovenskega združenja korporativne varnosti



Uveljavitev določil uredbe GDPR je v tej fazi, da vas lahko prosimo za določeno analizo stanja na področju uveljavljanja teh pomembnih mehanizmov?

Splošna uredba se je v enem letu dobro prijela. Zlasti velika podjetja, so po našem mnenju, bila že prej precej dobro pripravljena na njene določbe in velikih težav tu niti nismo pričakovali. Se je pa z njeno uveljavitvijo pokazalo, da predvsem malim podjetjem manjka poznavanje zakonodaje o varstvu osebnih podatkov, ne samo Splošne uredbe, saj smo prejeli kar veliko vprašanj že o osnovnih pojmih, ki bi zavezancem že morali biti jasni. Žal še vedno ni bil sprejet ZVOP-2, zato so naše možnosti sankcioniranja po Splošni uredbi omejene, a tudi brez izrekanja kazni je zavedanja o novi uredbi veliko. Prinaša pa, po naši oceni, Splošna uredba tudi pomemben sklop preventivnih ukrepov za zagotavljanje skladnosti, kot so ocene učinka, evidence dejavnosti obdelave in pooblaščene osebe za varstvo osebnih podatkov, ki bodo na dolgi rok prav gotovo pomembno prispevale k dvigu ravni varovanja osebnih podatkov. Uveljavlja pa se tudi institut samoprijave oziroma prijave kršitev varnosti (tako imenovan data breach notification), kar je za nas novost in terja od upravljavcev, katerim se kršitev zgodi, da to prijavijo Informacijskemu pooblaščencu. V prvem letu Splošne uredbe smo tako prejeli 120 samoprijav.

Kibernetska varnost postaja eden od najpomembnejših izzivov modernega varnostnega okolja. Kako v tem okviru zagotavljati ustrezno raven varovanja osebnih podatkov v informacijskem okolju?

Prav gotovo je ključno opraviti pravočasne ocene učinkov na varstvo podatkov ter analize varnostnih tveganj, na podlagi teh ugotovitev pa sprejeti ustrezne tehnične in organizacijske ukrepe za varnost podatkov. Glede na hiter tehnološki napredek je prav tako pomembno stalno usposabljanje, velja pa opozoriti še na eno težavo, ki še ni bila uspešno rešena, čeprav smo skupaj s Slovenskim združenjem za korporativno varnost opozarjali na nujnost in pomen ureditve tega področja. Gre pa za odgovorno poročanje o varnostnih ranljivostih (angl. responsible disclosure) – tu pa Slovenijo čaka še precej dela.

Kdaj je pred uvedbo postopkov uvedbe nove informacijske tehnologije nujna presoja varstva osebnih podatkov?

Tako imenovane ocene učinka na varstvo osebnih podatkov (angl. Data Protection Impact Assesment) so glede na določbe Splošne uredbe potrebne, kadar gre za sistematično in obsežno vrednotenje osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo. Med te primere sodijo npr. informacijske rešitve za obdelavo osebnih podatkov pri bankah, zavarovalnicah, operaterjih elektronskih komunikacij, kot so npr. CRM in »billing« sistemi ali klubi zvestobe. Prav tako izvedbo ocene učinka terjajo obsežne obdelave posebnih vrst podatkov iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10 – sem bi sodili zdravstveni informacijski sistemi, rešitve in aplikacije ter npr. informacijske rešitve za vodenje prekrškovnih in kazenskih evidenc. Podrobnejši seznam vrst obdelave, ki terjajo izvedbo ocene učinka, je

sprejel Informacijski pooblaščenec in je na voljo v naših smernicah na to temo na naši spletni strani.

Kako sta se v praksi uveljavili pravici do pozabe oz. izbrisa in pravica do prenosljivosti podatkov?

Po naših ugotovitvah posamezniki še vedno relativno slabo poznajo svoje pravice glede osebnih podatkov. Nekoliko bolj posegajo po pravici do dostopa do osebnih podatkov. Tako je Informacijski pooblaščenec v letu 2018 vodil nekaj čez 100 postopkov, kjer je odločal, ali mora upravljavec posamezniku omogočiti dostop do njegovih podatkov. Uveljavljanja pravice do izbrisa je le nekaj primerov, s primerom prenosljivosti pa se še sploh nismo srečali - posamezniki torej na nas še niso naslovili pritožbe zaradi zavrnitve te pravice, so se pa z majhnim številom zahtev po prenosljivosti srečali nekateri zavezanci. Menimo, da gre za pomembni pravici in zlasti pravica do prenosljivosti podatkov, kot nadgradnje pravice do seznanitve z lastnimi osebnimi podatki, bo mogoče na dolgi rok prispevala k večji konkurenci med ponudniki tudi na področju varstva osebnih podatkov, ter pripomogla k boljšemu razumevanju, koliko so v resnici vredni naši osebni podatki.

Katera so tista glavna pričakovanja od novo nastajajočega ZVOP-2?

Predvsem si želimo, da bi bil sprejet kratek in jasen zakon, ki ne bo podvajal določb Splošne uredbe, saj bi s tem kljub dobrim željam predlagatelja zakona, povzročili težave v naših postopkih, manjšo pravno predvidljivost in varnost, s tem pa tudi nižje varstvo pravic posameznika in višje stroške za zavezance. Nemogoče je od malih podjetij, ki predstavljajo več kot 90% vseh slovenskih podjetij, pričakovati poznavanje 250 členov zakonodaje o varstvu osebnih podatkov, s tem pa tudi ne moremo govoriti o zagotavljanju učinkovitega varovanja naših podatkov. Pričakujemo tudi jasno in učinkovito ureditev pogojev za izrekanje upravnih glob oziroma prekrškov ter relacij do drugih področij in pravic, kot je recimo pravica dostopa do informacij javnega značaja. Še vedno menimo, da bi bilo ustrezneje Splošno uredbo in t.i. »policijsko direktivo« v naš pravni prostor umestiti z dvema ločenima zakonoma in upamo, da bo tudi Ministrstvo za pravosodje to prepoznalo.

Kakšna je vaša ocena glede imenovanj pooblaščenih oseb za varstvo osebnih podatkov v organizacijah in ali ta rešitev prinaša določene rezultate pri dvigovanju ravni varovanja osebnih podatkov v organizacijskih okoljih?

Temeljne človekove pravice do varstva osebnih podatkov ni mogoče zagotoviti brez ustrezno usposobljenih strokovnjakov, zavedanja vodstva, ustrezne podpore s strani vodstva in dojemanja varnosti kot procesa.

Gre za enega od institutov za zagotavljanje skladnosti z zakonodajo o varstvu osebnih podatkov in ocenjujemo, da že prinaša določene rezultate. Njihova vloga je namreč vloga notranjih revizorjev na področju varstva osebnih podatkov z dodatnimi nalogami glede ozaveščanja in svetovanja. Že samo imenovanje takšnih oseb pa pomeni poznavanje vsaj tistih določb, ki urejajo njihovo imenovanje, položaj in naloge, s tem pa tudi razmislek o njihovi vlogi, položaju in nalogah v organizaciji. Prejeli smo že več kot 2100 obvestil o imenovanju pooblaščenih oseb in izdali posebna priporočila glede njihovih nalog, kakor tudi glede izogibanja konfliktu interesov. S časom se bo okrepilo tudi njihovo znanje in vloga – organizacije, ki se bodo zavedale pomena njihovega delovanja, bodo razumele, da jih varujejo pred nezakonitimi ravnanji in s tem pred inšpekcijskimi postopki, sankcijami, negativno publiciteto in izgubo zaupanja svojih strank.

Kakšen pomen v uradu namenjate procesom izobraževanja in usposabljanja. Je to z vaše perspektive učinkovit vzvod za dvigovanje splošnega zavedanja?

Vsekakor ocenjujemo, da je treba veliko truda nameniti izobraževalnim aktivnostim, saj gre vendarle za relativno novo zakonodajo, ki je obenem precej





S kombinacijo umetne inteligence in masovnih podatkov se lahko zgodi, da se bo o nas in našem življenju odločalo na podlagi drugih podatkov (trendov, povprečij in drugih statistik) in ne več na podlagi naših lastnih osebnih podatkov. Nadzorni organ zato predvsem v okviru mednarodnega sodelovanja sprejema smernice in priporočila, na kaj moramo paziti ob uvajanju tehnologij, ki temeljijo na umetni inteligenci in masovnih podatkih.

kompleksna in zlasti za mala podjetja in organizacije predstavlja velik zalogaj. V letih 2017 in 2018 smo tako izvedli več kot 200 brezplačnih predavanj za različna združenja in zbornice ter nastopili na številnih konferencah. Uspešno smo kandidirali na razpisu Evropske unije in pričeli izvajati projekt RAPID.SI, v sklopu katerega vodimo več aktivnosti za ozaveščanje posameznikov in malih podjetij. Med drugim smo vzpostavili dve posebni spletišči, tiodlocas.si za posameznike in upravljavec.si za mala podjetja. Vzpostavili smo tudi linijo za brezplačno telefonsko pomoč, kjer lahko podjetja na telefonski številki 080 2900 vsak delovnik med 8:30 in 12:30 dobijo telefonsko svetovanje glede osebnih podatkov. Prav tako pa bomo v okviru projekta v sodelovanju z Gospodarsko, Obrtno in Trgovinsko zbornico izvedli 20 brezplačnih seminarjev po vsej Sloveniji in tako dosegli kar največ podjetij. Podjetja se lahko prijavijo tudi na elektronske novice ter sledijo našim objavam na Facebooku in LinkedInu.

Predstavniki Urada IP so izredno aktivni pri delovanju v okviru Slovenskega združenja korporativne varnosti. Kakšne so vaše izkušnje z delovanjem v omenjenem združenju?

ICS izvaja številne aktivnosti na področju informacijske varnosti, ki predstavlja enega od temeljev ustreznega varstva osebnih podatkov. Temeljne človekove pravice do varstva osebnih podatkov ni mogoče zagotoviti brez ustrezno usposobljenih strokovnjakov, zavedanja vodstva, ustrezne podpore s strani vodstva in dojemanja varnosti kot procesa. Na vseh teh področjih ICS pomembno prispeva z različnimi aktivnostmi.

ICS že vrsto let združuje priznane varnostne strokovnjake na področju informacijske in korporativne varnosti in skrbi za njihova redna srečanja, dodatna izobraževanja, izmenjavo izkušenj in znanj. Redno organizira delavnice, posvete in konference s področja informacijske in korporativne varnosti ter izdaja strokovno revijo Korporativna varnost, s čimer pripomore k dvigu ozaveščenosti o posameznih aktualnih temah na področju varnosti.

Poleg navedenih rednih aktivnosti je ICS, v sodelovanju z Informacijskim pooblaščencem, v letu 2017 pripravil dva odmevna in dobro udeležena javna posveta in sicer Posvet o stanju kibernetske varnosti v državi v luči vedno pogostejših hekerskih vdorov ter Posvet o odgovornem razkrivanju varnostnih ranljivosti.

Menimo, da je s tem pomembno pripomogel k povezovanju deležnikov, proaktivnemu pristopu k varovanju podatkov in javni ozaveščenosti o pomenu informacijske in korporativne varnosti za zaščito naših osebnih podatkov, zato smo mu tudi podelili nagrado Ambasador zasebnosti za leto 2017.

Za konec bi vas prosili, da kratko ocenite izzive, ki nas, ko govorimo o razvoju umetne inteligence in avtomatskega obdelovanja velike količine podatkov na področju varovanja osebnih podatkov še čakajo?

Umetna inteligenca prav gotovo predstavlja velike izzive, ne samo za varstvo osebnih podatkov, temveč za praktično vsa področja našega življenja. Čas, ko bodo stroji zmogli bolje od človeka odločati o temu, ali dobimo stanovanjski kredit ali ne, kakšna je naša diagnoza in kakšno najbolj ustrezno zdravljenje, ali se naj določenega pripornika izpusti in odgovarjali na druga vprašanja, ki jih sedaj rešuje človek, je vedno bližje. S tem pa tudi vse nevarnosti, ki jih to prinaša, predvsem s sprejemanjem odločitev, ki imajo za posameznika lahko bolj ali manj kritične posledice (od zavrnitve kredita ali štipendije do napačnega zdravljenja), pogojena pa so lahko s slabimi, pomanjkljivimi in pristranskimi vhodnimi podatki, nepravilno delujočimi algoritmi oziroma celo z algoritmi, čigar delovanja in sprejemanja odločitev sploh ne razumemo več. Predvsem pa njihovo odločanje ne vključuje človeških, etičnih in moralnih vidikov, ki bi včasih morali pretehtati nad golimi podatki. S kombinacijo umetne inteligence in masovnih podatkov se lahko zgodi, da se bo o nas in našem življenju odločalo na podlagi drugih podatkov (trendov, povprečij in drugih statistik) in ne več na podlagi naših lastnih osebnih podatkov. Nadzorni organ zato predvsem v okviru mednarodnega sodelovanja sprejema smernice in priporočila, na kaj moramo paziti ob uvajanju tehnologij, ki temeljijo na umetni inteligenci in masovnih podatkih. Izpostavila bi predvsem mnenja Mednarodne delovne skupine za varstvo podatkov v telekomunikacijah, katere član je že vrsto let tudi Informacijski pooblaščenec. ■

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



KOLUMNA

BO DRŽAVA ZNALA IZKORISTITI TO POMEMBNO PRILOŽNOST?

V okviru Slovenskega združenja za korporativno varnost je bil v mesecu maju ustanovljen poseben posvetovalni odbor za kritično infrastrukturo, ki vključuje direktorje in vodje področja korporativne varnosti iz ključnih infrastrukturnih upravljalcev kritične infrastrukture, kateri so vključeni v združenje. S tem posvetovalnim odborom Republika Slovenija stopa korak naprej v smeri celovitejšega in usklajenega pristopa obvladovanja tveganj za nemoteno delovanje kritične infrastrukture.

Dinamično varnostno okolje postaja vedno bolj zahtevno in pred družbo postavlja vedno nove dileme, kako učinkovito obvladati tiste ključne segmente, ki so potrebni, da le ta nemoteno in neprekinjeno deluje. V tem okviru je še posebej izpostavljena kritična infrastruktura, kot tisti sistemski, procesni in infrastrukturni segment, ki mora delovati neprekinjeno, če želimo, da lahko določeni nujno potrebni deli družbe neprekinjeno delujejo. Seveda se je potrebno zavedati, da gre za kompleksni sistem, kjer si težko privoščimo, da posamezni segmenti tega sistema ne funkcionirajo. Ta zahteva pa je postavljena tudi pred vse deležnike, ki so vpleteni v ta sistem in s svojimi pristojnostmi, znanji, dobrimi praksami in ustrezno zakonsko regulativo, zagotavljajo njegovo nemoteno delovanje. V okviru deležnikov moramo jasno prepoznati državo, ki s svojimi institucijami skrbi za postavljanje ustreznega zakonskega okvira za vzpostavitev sistema zaščite kritične infrastrukture in skozi nacionalne ter sektorske koordinatorje zagotavlja neposredno usklajevanje sektorskih in medsektorskih posebnosti posamezne kritične infrastrukture. V drugem kotu tega pomembnega trikotnika se pojavljajo upravljalci kritične infrastrukture, ki so neposredno zadolženi za njeno upravljanje in izvajanje operativnih zaščitnih ukrepov, da kritična infrastruktura deluje neprekinjeno. Seveda smo tudi v Sloveniji podvrženi trendu, da pomemben del upravljalcev kritične infrastrukture počasi prehaja v zasebno lastništvo, imamo pa tudi primere popolnega javnega lastništva in mešanih lastniških razmerij v posameznih organizacijah. To posebej izpostavljamo zato, ker je zavedanje lastnikov oz. upravljavcev kritične infrastrukture ravno tako zelo pomembno za učinkovito sistemsko delovanje pri zagotavljanju njene neprekinjenosti delovanja. In tretji ključni dejavnik predstavlja javno okolje, ki predvsem skozi civilne strokovne asociacije in znanstveno raziskovalne institucije zagotavlja izmenjavo izkušenj in dobrih praks, predvsem pa zagotavlja nove rešitve in pristope, ki pomagajo dvigovati učinkovitost zaščite kritične infrastrukture.

Slovensko združenje za korporativno varnost omogoča odlično platformo za združevanje vseh treh nosilnih stebrov celovitega sistema zaščite kritične infrastrukture. Ta civilno-strokovna asociacija v svojih vrstah združuje večino najpomembnejših organizacij, ki upravljajo s kritično infrastruktu-

Slovensko združenje za korporativno varnost omogoča odlično platformo za združevanje vseh treh nosilnih stebrov celovitega sistema zaščite kritične infrastrukture.

*avtor je član Slovenskega združenja korporativne varnosti

Seveda se nam v tem okviru postavlja logično vprašanje ali bo država znala v celoti izkoristiti potencial, ki ga prinaša tako sodelovanje. Potrebno se je namreč zavedati, da ima Republika Slovenija zaradi svoje velikosti omejene vire, zato je potrebno racionalno pristopati k izvajanju procesov in izkoriščati vse potenciale, ki so na voljo, ne glede na to ali prihajajo iz državnih, civilnih, raziskovalnih ali gospodarskih okvirov.

ro, združuje akademsko in strokovno okolje ter ob logistični in raziskovalni podpori Instituta za korporativne varnostne študije zagotavlja stalen pritok novih spoznanj in izmenjavo dobrih praks iz različnih nacionalnih in mednarodnih korporativnih okolij ter kot tretji pomemben segment zagotavlja tudi participacijo določenih državnih in javnih institucij, ki imajo zelo pomembno vlogo pri obvladovanju širšega spektra varnostnih tveganj. To vsekakor predstavlja neko posebnost, ki je v Republiki Sloveniji redek, če ne celo edini primer takega sodelovanja. Če v tem okviru dodamo, da je bil znotraj združenja ustanovljen Posvetovalni odbor za kritično infrastrukturo, kateri omogoča, da se v opredeljenem krogu udeležencev izmenjujejo tudi tiste ključne informacije, ki niso v celoti za javno razpravo, potem lahko ocenimo, da imamo na mizi vse potrebne mehanizme. Le ti nam zagotavljajo, da je sodelovanje in izmenjava ključnih informacij in dobrih praks v polnem obsegu dobro delujoč mehanizem, ki bo zagotovil višjo kvaliteto, boljšo operativno dinamičnost odzivanja na nove izzive in seveda zagotavljal višjo raven učinkovitosti zaščite kritične infrastrukture.

Seveda se nam v tem okviru postavlja logično vprašanje ali bo država znala v celoti izkoristiti potencial, ki ga prinaša tako sodelovanje. Potrebno se je namreč zavedati, da ima Republika Slovenija zaradi svoje velikosti omejene vire, zato je potrebno racionalno pristopati k izvajanju procesov in izkoriščati vse potenciale, ki so na voljo, ne glede na to ali prihajajo iz državnih, civilnih, raziskovalnih ali gospodarskih okvirov. V tujini je ta oblika sodelovanja že uveljavljena praksa, še posebej v tistih državah, ki so bile najbolj izpostavljene določenim grožnjam, nesrečam in napadom na kritično infrastrukturo. To sodelovanje je pravzaprav tisti glavni temelj javno-zasebnega partnerstva, ki smo ga v Sloveniji, zaradi določenih zlorab, razumeli in ga v določenih okoljih še razumemo popolnoma napačno. Določena skrb, ki nas lahko navdaja z nelagodjem, je tudi nerazumevanje takih oblik sodelovanja, s strani ključnih odločevalcev, kakor tudi srednjega managementa v pomembnih državnih institucijah. Tukaj ni ključno vprašanje, kdo je tisti, ki je na mizo prvi prinesel to iniciativo, ali je prišla od zgoraj, s strani države, ali od spodaj, s strani upravljalcev ali strokovne javnosti, pomembno je, da jo imamo pred seboj, vzpostavljeno in delujočo. Kako bo učinkovita, pa je odvisno od vseh nas deležnikov, ki smo neposredno in posredno odgovorni, da bo celovit proces zaščite kritične infrastrukture in obvladovanja tveganj, deloval čim bolj učinkovito in racionalno.

Zaupanje za izmenjavo ključnih informacij je sicer proces, ki ga je težko začeti in traja daljše časovno obdobje, da se vzpostavi ustrezna raven zaupanja. Vendar moramo nekje začeti in nikakor ne smemo čakati, da nas določene situacije presenetijo in imajo negativne vplive na neprekinjenost delovanja kritične infrastrukture. Če hipotetično pogledamo situacije povezane z radikalizacijo posameznikov, katera lahko vodi v terorizem. Če so take osebe zaposlene v organizaciji, ki upravlja kritično infrastrukturo, je za učinkovito odkrivanje, spremljanje in ukrepanje ter preprečitev dejanj, ki bi imele lahko katastrofalne posledice za organizacijo, družbo in državo, samo ena pot. To je pot nujnega sodelovanja med organi nacionalne varnosti (policija, obveščevalno-varnostni se-





gment) in korporativno varnostjo, ki zagotavlja vse aktivnosti v procesu korporativne varnosti v sami organizaciji, katera upravlja kritično infrastrukturo. Za učinkovito sodelovanje, pa je seveda treba predhodno vzpostavljati kanale izmenjevanja operativnih podatkov o določenih situacijah, poznavanja strokovnjakov v javnem in zasebnem okolju, poenotenju razumevanja zakonskih omejitev in pristojnosti, ter nenazadnje razumevanja izzivov in tveganj, ki stojijo pred našo družbo in organizacijami. Tisti zagovorniki strogih birokratskih in formalnih pristopov pri izmenjevanju ključnih informacij se morajo počasi začeti zavedati, da je varnostno okolje postalo preveč dinamično, da bi vse ukrepe lahko temeljili samo na golem birokratskem in vnaprej predpisanem formalnem kanalu komunikacije. Izkušnje in prakse vseh najbolj tragičnih primerov v zadnjem obdobju kažejo in nas napotujejo k intenziviranju dopolnilnih komunikacijskih in koordinativnih kanalov, ki v največjih primerih rešujejo situacije. To je po naši oceni tudi najmočnejša dodana vrednost, ki jo lahko prinese učinkovito javno-zasebno sodelovanje na področju zagotavljanja varnosti kritične infrastrukture.

Moramo biti optimisti in usmerjati vse sile in energijo v nadaljevanje izgradnje dobrih praks in mehanizmov, ki nam bodo jutri omogočali, da bomo bolj pripravljeni na sprejemanje novih izzivov, katere pred nas postavlja varnostno okolje. Poleg človeškega faktorja, ki se izraža skozi radikalizacijo, nas še posebej lahko skrbijo procesi kibernetskih groženj, ki jih prinaša družba, katera temelji na popolni odvisnosti od informacijskih tehnologij.

Prvi odzivi določenih ključnih strateških voditeljev institucij, ki zagotavljajo nacionalno varnost, so pozitivni in z razumevanjem sprejemajo te ideje in ponujene mehanizme, pa čeprav prihajajo s strani upravljalcev in strokovne javnosti.

> Tukaj ni ključno vprašanje, kdo je tisti, ki je na mizo prvi prinesel to iniciativo, ali je prišla od zgoraj, s strani države, ali od spodaj, s strani upravljalcev ali strokovne javnosti, pomembno je, da jo imamo pred seboj, vzpostavljeno in delujočo. Kako bo učinkovita, pa je odvisno od vseh nas deležnikov, ki smo neposredno in posredno odgovorni, da bo celovit proces zaščite kritične infrastrukture in obvladovanja tveganj, deloval čim bolj učinkovito in racionalno.

Seveda pa je sedaj potrebno stopiti korak naprej, ki bo pokazal ali je to deklerativno podporo in razumevanje zahtev varnostnega okolja, mogoče spraviti v neposredno in učinkovito delujoči sistem sodelovanja. Odgovor na, v naslovu zastavljeno vprašanje te kolumne, bo pred nami prej, kot bi si ga sami upali in želeli dobiti. K temu nas bo namreč prisilila realna varnostna situacija in grožnje, na katere nismo imuni niti v Republiki Sloveniji. ■

Slovensko združenje korporativne varnosti

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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

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

www.ics-institut.si

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

Članstvo v **SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI**

vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

Pošta Slovenije
Mestna občina Ljubljana
Občina Slovenska Bistrica
SmartIS Pametni informacijski sistemi
Informacijske storitve in inženiring, d.o.o. INFORMATIKA
triglav
PETROL Energija za življenje
Telekom Slovenije
AKRAPOVIČ
interblock Luxury Gaming Products
spica
Ford SUMMIT AVTO
Elektro Ljubljana
Elita i.b. d.o.o.
SIEMENS
DARS
CINKARNA
UNISTAR PRO
Nova KBM Pripravljeni na jutri
LON
ZARJA ELEKTRONIKA
Slovenske železnice
energetika ljubljana

www.ics-institut.si

Avtor: doc. dr. Brane Bertoncelj / Institut za korporativne varnostne študije*



METODOLOGIJA ZA OCENJEVANJE TVEGANJ ZA DELOVANJE KRITIČNE INFRASTRUKTURE

Ocenjevanje, upravljanje in obvladovanje tveganj za delovanje kritične infrastrukture (v nadaljevanju: KI) je kompleksno in interdisciplinarno zahtevno delo. Pristop k ocenjevanju tveganj je metodično zasnovan na principih sistemskega inženiringa, vsebinsko na preprečevanju možnih škod in izgub, operativno pa na sodobnih rešitvah upravljanja in obvladovanja tveganj. Pomembno omejitev pri tem predstavlja dejstvo, da je za temeljito razumevanje metodologij ocenjevanja tveganj potrebno določeno strokovno predznanje.

Uvod

Študijo »Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture« je naročilo Ministrstvo za obrambo Republike Slovenije, financirana pa je bila s podporo Evropske unije iz Sklada za notranjo varnost. Študijo je izdelala projektna skupina, ki je bila sestavljena iz predstavnikov Instituta za korporativne varnostne študije in Slovenskega združenja korporativne varnosti.

Različni pristopi družboslovnega raziskovanja in vrste možnih metod ter metodologij za ocenjevanje tveganj so izpostavili problem, kateri njihovi deli bi bili lahko uporabni kot primer dobre prakse za ocenjevanje tveganj za delovanje KI v Republiki Sloveniji. Organizacije KI se soočajo z notranjimi in/ali zunanjimi dejavniki ogrožanja poslovanja, kar vpliva na negotovost in nepredvidljivost doseganja ciljev poslanstva.

Pregled metod in metodologij za ocenjevanje tveganj za delovanje KI je bil opravljen na podlagi poglobljene analize literature. Ugotovljenih je bilo več kot tisoč ustreznih referenc. Njihovo primernost smo analizirali in vrednotili na podlagi naslednjih izbranih kriterijev: ustreznost koncepta metodologije, načrtovanje (formalen pristop k načrtovanju metodologij za ocenjevanje tveganj naj bi zmanjšal število napak in težo njihovih posledic), procesa in postopka ocenjevanja ter upravljanje sprememb.

Izbrana metodologija

Na podlagi zgoraj navedenih izbranih kriterijev smo izbrali kombinacijo metodologije **MOSAR** (Method organised systematic analysis of risk, metoda za sistematično analizo tveganja) in metodologije **FMEA** (Failure mode and effect analysis, analiza načina in učinka okvar) kot najprimernejši za ocenjevanje tveganj za delovanje KI.

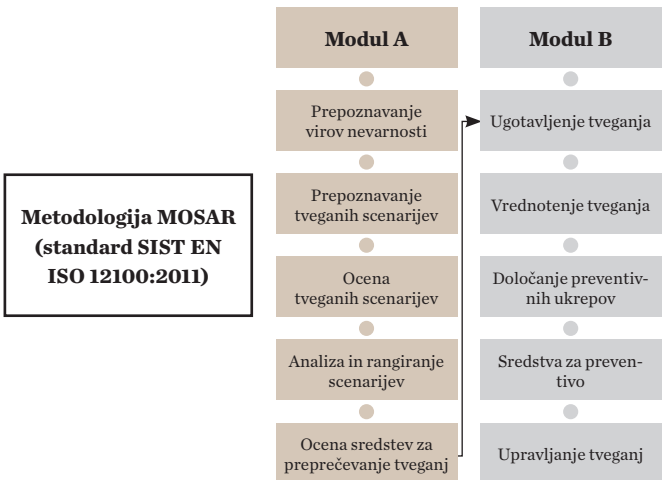
MOSAR[1] je sistemska analiza tveganj, poznana tudi kot »Analiza drevesa napak«, pa tudi kot diagram vzrokov in posledic (»Ishikawa diagram«). Metodologija sistematično analizira tveganja v okolju in predstavlja pristop k ocenjevanju ter vrednotenju tveganja, določevanju prioritet, obravnavanju tveganj in upravljanju z njimi.

FMEA[2] se uporablja kot metoda za podporo proizvodnih procesov, storitev in vzdrževanja. Je učinkovita, preventivna, timsko orientirana in sistematična analiza napak sistema. Obsega interdisciplinarne postopke, sistematično in funkcijsko obravnavanje, preprečevanje napak, kreativno razmišljanje in kritično ocenjevanje.

V nadaljevanju bosta obe metodologiji predstavljeni v obliki desetih korakov za ocenjevanja tveganj.

*avtor je član Slovenskega združenja korporativne varnosti

Cilj metodologije MOSAR je odkrivanje neustreznega delovanja in upravljanje s tveganji kompleksnega sistema. Je pripomoček za lažje odločanje, iskanje glavnih scenarijev odpovedi sistema, določanje potrebnih ukrepov in postopkov za nevtraliziranje ali zmanjševanje posledic izrednega dogodka. Prikazana je na sliki 1.

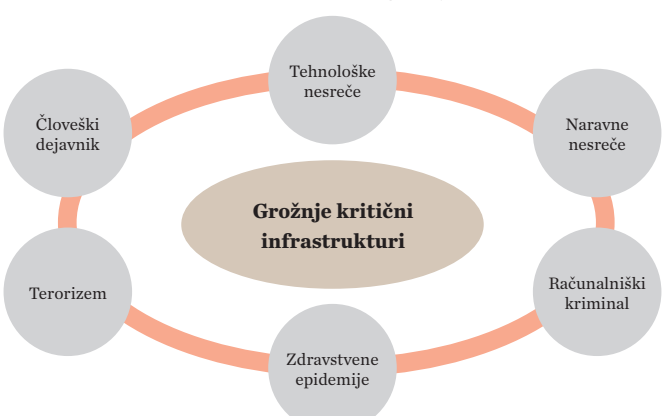


Slika 1: Metodologija MOSAR (prirejeno po standardu SIST EN ISO 12100:2011)

Modul A MOSAR v petih korakih:

Prepoznava vira nevarnosti (1. KORAK)

Nevarnost nastopi v trenutku, ko ogrožajoči dejavniki, ki po svojem številu, intenzivnosti in pogostosti delovanja prekoračijo določeno vrednost, s tem pa je sistem moten v svojem delovanju, tako da ne more več opravljati svoje funkcije v prejšnjem obsegu. Na sliki 2 so prikazani globalni viri nevarnosti. Nanašajo se na tehnološke nesreče, naravne in druge nesreče, računalniški kriminal, zdravstvene epidemije, terorizem in nevarnosti zaradi človeškega dejavnika.



Slika 2: Globalni viri nevarnosti (interni vir ICS)

Prepoznavanje tveganih scenarijev (2. KORAK)

Proces odgovarjanja na vprašanje: »Kaj se zgodi, če...« se imenuje prepoznavanje scenarijev. Njihova bistvena značilnost je vnaprejšnje prepoznavanje tveganih scenarijev organizacije. Proces prepoznavanja scenarijev se nanaša na izdelavo scenarijev (kako določiti in prepoznati vire možnih zunanjih ali notranjih izrednih dogodkov), oceno scenarijev (opisna ocena tveganih scenarijev), kvaliteto podatkov in informacij (kako zanesljivi so ti ob negotovi prihodnosti), določitev vrednosti parametrov tveganih scenarijev (kvalitativna ali kvantitativna) in rezultati modela (ocena posledic realiziranega izrednega dogodka).

Ocena tveganih scenarijev (3. KORAK)

Ocena tveganih scenarijev je izdelana na podlagi kriterijev možne škode v primeru izrednega dogodka in resnosti ter verjetnosti izrednega dogodka. Resnost ogrožanja se nanaša na razdejalni, katastrofalen, pomemben, resen ali zmeren učinek. Verjetnost se nanaša na ekstremno neverjetno (en primer na sto tisoč primerov), zelo neverjetno (en primer na sto tisoč primerov do en primer na deset tisoč primerov), neverjetno (en primer na deset tisoč primerov do en primer na tisoč primerov), verjetno (en primer na tisoč primerov do en primer na sto primerov) in zelo verjetno (en primer pod sto primerov).

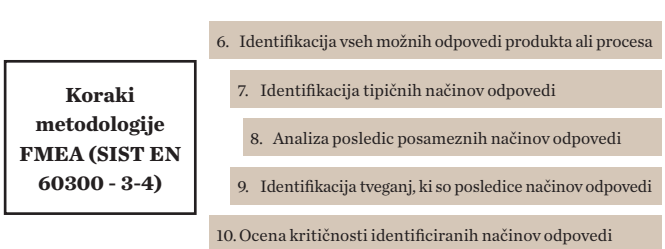
Analiza in rangiranje tveganih scenarijev (4. KORAK)

Uporabijo se najbolj tvegani scenariji in se jih analizira s pomočjo naslednjih kazalnikov: opis najslabšega možnega scenarija, vpliv na poslovni cilj, vpliv na zaupanje uporabnikov, vpliv na finančna sredstva, verjetnost izrednega dogodka in obrazložitev scenarija.

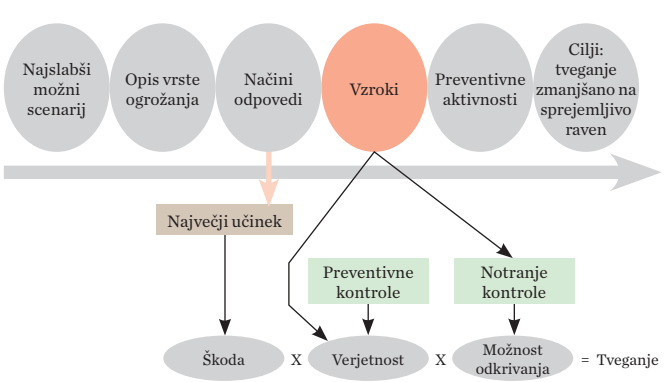
Ocena sredstev za preprečevanje tveganj (5. KORAK)

Na zaključku uporabe MOSAR se je treba odločiti o načinih obvladovanja tveganj**.** Na tej stopnji je treba razmisliti o naslednjem: ali je mogoče tveganja odpraviti, če to ni mogoče, kako je mogoče tveganja obvladovati, da ne bodo ogrožala neprekinjeno poslovanje sistema, zagotoviti ustrezna finančna sredstva in kadre. Najbolj tvegane scenarije je potrebno v najkrajšem možnem času obravnavati pri vodstvu upravljavca KI in sprejeti aktivnosti, ukrepe ter postopke za zmanjševanje tveganja (kaj, kdo in kdaj).

Koraki **FMEA** metodologije so shematsko prikazani na sliki 3, na sliki 4 pa logične povezave med posameznimi FMEA elementi.



Slika 3: Koraki metodologije FMEA



Slika 4: Logične povezave med FMEA elementi (SIST EN 60300 - 3-4)

Logične povezave iz slike 4 se nanašajo na identifikacijo najslabših možnih scenarijev (identificirani po MOSAR metodologiji), opis vrste ogrožanja, način in vzroke odpovedi, oceno tveganja, preventivne aktivnosti (ukrepi in postopki, odgovornosti, roki izvedbe aktivnosti), ponovno oceno izvedenih aktivnosti in oceno tveganj. Vse navedeno je treba opisati in analizirati na delovnem listu FMEA (prikazan na sliki 5).

Proces / produkt: _____ Številka FMEA: _____

Projektna skupina: _____ Datum izdelave: _____

Vodja skupine: _____ Datum revizije: _____

FMEA ref	Element (proces, produkt)	Možni način odpovedi	Možni vzrok odpovedi	Učinek odpovedi	Ocena resnosti (S)	Ocena verjetnosti (0)	Ocena odkrivanja (D)	Tveganja na ravni RPN=Sx0xD	Predlagani ukrepi	Odgovoren	Izredne aktivnosti	Ponovnon ocena S, O, D, RPN

Slika 5: Primer delovnega lista FMEA (prirejeno po standardu)



V delovnem listu FMEA je pomembna postavka razdelava strukture produkta / storitve. Struktura se nanaša na številne poslovne procese, vsak poslovni proces pa je razčlenjen na zaposlene, strojno opremo, uporabljen material in delovno okolje.

Opis korakov za izvedbo metodologije

6. KORAK: Identifikacija vseh možnih odpovedi produkta ali procesa

- Prepoznavanje funkcij sistema (temeljit pregled produkta/ procesa v ločenih podsistemih, elementih, delih, sklopih, in opredelitev njihove funkcije.

7. KORAK: Identifikacija tipičnih načinov odpovedi

- Osnova je identifikacija načinov odpovedi (po MOSAR metodologiji),
- za vsako funkcijo se identificira način odpovedi poslovanja,
- sledi identifikacija posledic načinov odpovedi sistema, z njim povezanih podsistemov, procesov, povezanih procesov, izdelkov, storitev, uporabnikov. To so potencialni učinki odpovedi. Vprašanje je »Kaj se zgodi, ko se pojavi ta napaka?« Za vsak način odpovedi se določi možni vzrok,
- določi se lokalni učinek odpovedi, naslednja višja raven učinka in končni učinek.

8. KORAK: Analiza posledic posameznih načinov odpovedi

- Oceni se resnost posledic Si (ang. Severity of effects), pogostost pojava Oi (ang. Occurence of failures) in možnost pravočasnega zaznavanja (odkrivanja) odpovedi Di (ang. Detection of failures),
- ugotovi se, kako resen je vsak učinek, z določevanjem Si, Oi, Di, za vsak način odpovedi,
- vsak način in kriterij ocenimo z ocenami od 0 do 10, kjer je 1 nepomemben in 10 je katastrofalni učinek,
- izračuna se faktor tveganja RPNi (angl. Risk Priority Number) = Si x Oi x Di (zmnožek treh ocen: RPN = resnost x pogostost x odkrivanje),
- če je ocena faktorjev S,O ali D med 1 in 2, to pomeni manjši vpliv, med 9 in 10 pa večji vpliv na sistem, pri čemer je RPN max = 10 × 10 × 10 = 1000, RPN min = 1 × 1 × 1 = 1,
- **prag za KI je RPN 10, prag za nekritične sisteme pa je RPN 100.**

9. KORAK: Identifikacija tveganj, ki so posledice načinov odpovedi

- Prepoznavanje priporočenih aktivnosti iz navodil in dobre prakse. Ti ukrepi in postopki se nanašajo na zmanjšanje ali odpravo vzrokov odpovedi. So lahko načrt ali proces sprememb, dodatni sistemi in kontrolni sistemi za izboljšanje detekcije odpovedi. Upošteva se tudi, kdo je odgovoren za te aktivnosti in ciljni datumi zaključka,
- po prvi oceni RPN se za kritične poslovne procese izvedejo preventivni in korektivni ukrepi. Po njihovi implementaciji se postopek FMEA v razumnem roku ponovi z izdelavo novega delovnega lista FMEA,
- izdela se matrika tveganj. V njo se vnesejo rezultati faktorjev tveganja RPNi. Končni produkt Metodologije FMEA je izdelava registra (kataloga) tveganj.

10. KORAK: Ocena kritičnosti identificiranih načinov odpovedi

Ocena kritičnosti identificiranih načinov odpovedi se nanaša na tri večje sisteme: tehnični sistem (v obliki opreme, strojev, naprav ipd.), pravni in organizacijski sistem (v obliki internih splošnih aktov, ki določajo postopke in način delovanja), izvajanje posameznih poslovnih procesov v smislu razmerja posameznik - posameznik in posameznik - oprema.

Zaključek

Ob temeljiti analizi različnih metodoloških pristopov in uporabljenih metodologij za ocenjevanje tveganj smo se odločili za smiselno uporabo metodologije MOSAR, ki je temeljito razdelana in v določenih izvedbenih korakih dopolnjena z metodologijo FMEA.[1] Navedeno je rezultat celovitega postopka identifikacije, analize in vrednotenja različnih metodologij tveganj. Splošna ugotovitev kaže, da je večina podsektorjev KI povezana z določenim tehnično-tehnološkim procesom, kjer je uporaba predlagane metodologije ustrezna.

Kombinacija različnih pristopov, modelov, metodologij, konceptov in analiz različnih primerov, podaja ustrezno podlago za ocenjevanje tveganj za delovanje KI Republike Slovenije. Izbrani metodologiji MOSAR in FMEA sta znanstveno in strokovno utemeljeni in pomenita enega od možnih pristopov. Priporočamo tudi določeno uporabo programske računalniške opreme na področju ocenjevanja tveganj, ki bo upoštevala predlagano metodologijo.

Za implementacijo sistemskega pristopa na navedenem področju je potrebno več vlagati v stalno izobraževanje in dograjevanje znanj ter veščin. Področje ocenjevanja tveganj bo v prihodnosti eno od tistih področij, ki bo podvrženo potrebi po neprekinjenem usposabljanju ustreznih strokovnjakov, ki bodo v organizacijah KI izvajali te procese.

[1] MOSAR smo uporabili po standardu SIST EN ISO 12100:2011, Varnost strojev - Splošna načela načrtovanja - Ocena tveganja in zmanjšanje tveganja (ISO 12100:2010, slovenski prevod).

[2] FMEA smo uporabili po standardu SIST EN 60300 - 3-4, Upravljanje zanesljivosti – 3.-4. del: Vodilo za uporabo - Vodilo za specifikacijo zahtev zanesljivosti (IEC 60300-3-152 4:2007) - Dependability management - Part 3-4: Application guide - Guide to the specification of dependability requirements (IEC 60300-3-4:2007).

[3] Celoten tekst študije »Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture (SPOTKI) je objavljena na spletnih straneh Ministrstva za obrambo Republike Slovenije in Instituta za korporativne varnostne študije http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/javne_objave/2019/Studija_SPOTKI.pdf. ■



Vodilno globalno podjetje na področju varovanja

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

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

CE FC RoHS ISO 9001:2000

www.dahuasecurity.com

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

Avtor: mag. Miran Vršec / Institut za korporativne varnostne študije*



IZZIVI UPRAVLJANJA TVEGANJ V KRITIČNI INFRASTRUKTURI

V prispevku bomo kratko pregledali bistvene izzive upravljanja tveganj v kritični infrastrukturi, s katerimi se bodo soočali vsi deležniki, ki v sistemu zagotavljajo zaščito in neprekinjeno delovanje kritične infrastrukture. Sprejeti zakonodajni okvir je postavil minimalne standarde na področju zagotavljanja varnosti in obvladovanja tveganj v kritični infrastrukturi. Sedaj je potrebno predpisano implementirati v neposredno okolje in zagotoviti, da bodo rešitve sistemsko umeščene in kot take zagotavljale ustrezno raven zaščite kritične infrastrukture.

Uvod

V zadnjih dveh letih se je s sprejemom zakonodaje, ki ureja področje kritične infrastrukture, področje informacijske varnosti in področje varovanja poslovnih skrivnosti, začrtal zakonski (minimalni) okvir delovanja upravljavcev kritične infrastrukture. Po uvedbi Splošne uredbe o varstvu osebnih podatkov (GDPR) v kratkem pričakujemo še sprejem novega Zakona o varstvu osebnih podatkov, s čimer bo ta zakonodajni okvir bolj ali manj sklenjen. Vsekakor bo v prihodnjem obdobju potrebno sprejeti ali novelirati še kakšen zakon ali podzakonski akt, ki posredno posega v področje upravljanja kritične infrastrukture, a bistvenih posegov v procese upravljanja kritične infrastrukture, zaradi tovrstnih sprememb, vsaj na kratek rok, ni pričakovati. Na upravljavcih kritične infrastrukture je torej sedaj odgovornost, da zakonodajne novosti in spremembe, ki določajo njihovo delovanje, implementirajo v njihove procese in s tem zagotovijo zakonito in neprekinjeno upravljanje s kritično infrastrukturo. V fazi vzpostavljanja skladnosti poslovanja z zakonodajo, vzpostavljanja sistemov upravljanja tveganj in neprekinjenega delovanja upravljavce kritične infrastrukture čaka kar nekaj izzivov, ki jih bom na kratko predstavil v nadaljevanju.

Da bi se dosegla tudi neodvisnost delovanja in suverenost sprejemanja odločitev, mora biti korporativni varnostni menedžer, kot poslovodja (direktor) omenjene enote, odgovoren neposredno poslovodnemu organu (upravi) ali poslovodji (direktorju) upravljavca kritične infrastrukture.

Ključni izzivi upravljanja tveganj v kritični infrastrukturi

Strokovni izzivi

Med strokovnimi izzivi izpostavljam predvsem izzive povezane z vzpostavljanjem ustreznih pogojev in podlag za delovanje sistema upravljanja tveganj v kritični infrastrukturi (v nadaljnjem besedilu: SUT KI), izzive povezane z vzpostavljanjem celovitega sistema upravljanja operativnih informacij, kibernetskih incidentov, izrednih dogodkov in kriznih situacij v SOC (Security Operation Center), INC (Internem nadzornem centru) in/ali VNC (varnostno nadzornem centru) pogodbenega izvajalca zasebnega varovanja ter izzive na področju uvajanja varnostnih in drugih standardov v SUT KI.

Med omenjenimi izzivi predstavlja največji strokovno-organizacijsko-tehnološki izziv vzpostavitev celovitega sistema upravljanja operativnih informacij, kibernetskih incidentov, izrednih dogodkov in kriznih situacij. Upravljavci kritične infrastrukture, ki so po Zakonu o informacijski varnosti prepoznani kot izvajalci bistvenih storitev, morajo temu segmentu posvečati še toliko več pozornosti. Glede na to, da so v dosedanji praksi upravljavci kritične infrastrukture različno

*avtor je član Slovenskega združenja korporativne varnosti

Upravljavec kritične infrastrukture si ne sme dovoliti, da bi bil neustrezen plačni sistem in sistem nagrajevanja tisti odločujoči (prevladujoči) faktor, ki bi bil vzrok za povečevanje odhodov zaposlenih. Prekomerna fluktuacija je namreč eden pomembnih faktorjev tveganja v organizaciji, kar je za upravljavca kritične infrastrukture povsem neprimerno in nedopustno.

organizacijsko strukturo upravljavca kritične infrastrukture. Nadalje zagotovitev neodvisnosti delovanja in suverenost sprejemanja odločitev korporativnega varnostnega menedžerja, ki je pri upravljavcu kritične infrastrukture odgovoren za vodenje SUT KI.

Nujni pogoj za zagotavljanje učinkovitega delovanja SUT KI je vzpostavitev samostojne organizacijske enote (sektorja), v okviru katere se izvajajo vsi upravljavski in operativni procesi povezani s SUT KI, tako na področju informacijske, kot tudi fizično-tehnične varnosti. Da bi se dosegla tudi neodvisnost delovanja in suverenost sprejemanja odločitev, mora biti korporativni varnostni menedžer, kot poslovodja (direktor) omenjene enote, odgovoren neposredno poslovodnemu organu (upravi) ali poslovodji (direktorju) upravljavca kritične infrastrukture.



pristopali k reševanju omenjenega izziva, se moja ideja razvija v smeri povezovanja vseh omenjenih varnostnih centrov v enovit Varnostno operativni komunikacijski center (SOCC – Security Operation Communication Center) v katere bi se vsebinsko in operativno združevali vsi dosedanji centri. Na ta način bi se lahko zagotovilo centralno in celovito upravljanje z operativnimi informacijami, kibernetskimi incidenti, izrednimi dogodki in kriznimi razmerami, tako na področju informacijske, kot tudi fizično-tehnične varnosti.

Organizacijski izzivi

Na organizacijskem področju izpostavljam predvsem izzive povezane z vzpostavljanjem ustrezne umestitve SUT KI v

Kadrovski izzivi

Vse večja problematika povezana z zagotavljanjem ustreznih kadrovskih resursov narekuje posebne izzive tudi na tem področju. Predvsem tu želim izpostaviti izzive povezane z zagotavljanjem kompetentnih kadrovskih resursov, izzive na področju zagotavljanja stalne zasedenosti posameznih delovnih mest (v to se štejejo tudi ustrezne rezerve za razna nadomeščanja), ki so vzpostavljena v SUT KI in izzive na področju dolgoročnega zagotavljanja ustreznega nivoja znanj zaposlenih na vseh delovnih mestih. V tem kontekstu bo potrebno vzpostaviti tudi ustrezen plačni sistem in sistem nagrajevanja zaposlenih, ki bo dovolj motivacijski in bo kot tak zagotavljal potrebno socialno varnost in zadovoljstvo zaposlenih.

Upravljavec kritične infrastrukture si ne sme dovoliti, da bi bil neustrezen plačni sistem in sistem nagrajevanja tisti odločujoči (prevladujoči) faktor, ki bi bil vzrok za povečevanje odhodov zaposlenih. Prekomerna fluktuacija je namreč eden pomembnih faktorjev tveganja v organizaciji, kar je za upravljavca kritične infrastrukture povsem neprimerno in nedopustno.

Ekonomski izzivi

Za stabilnost, neodvisnost in neprekinjenost delovanja SUT KI so potrebna finančna sredstva. Zato je iz ekonomskega vidika izjemno pomemben izziv zagotovitve ustreznega proračuna, ki bo zagotavljal zadostna sredstva za delovanje SUT KI. Proračun mora biti neodvisen in se mora voditi kot samostojno stroškovno mesto z jasno definiranimi stroškovnimi nosilci. Proračun mora biti sestavljen tako, da zagotavlja zadostna finančna sredstva za tekoče poslovanje in ustrezna obratna sredstva za financiranje nadgradenj, posodobitev in nujnih sprememb SUT KI. Korporativno varnostni menedžer mora proračun pripraviti na način, ki bo poslovodnemu organu omogočal preglednost financiranja ter pravočasnost potrjevanja in zagotavljanja (rezerviranja) planiranih sredstev.

Pri pripravi proračuna so izjemnega pomena pojasnila posameznih postavk, s katerimi se, z uporabo različnih metod (npr. Cost Benefit) argumentira potrebna (planirana) sredstva in njihova dodana vrednost. Ob tem je potrebno pripraviti tudi ustrezne kazalnike uspešnosti in učinkovitosti delovanja SUT KI, s katerimi se vzpostavi matrika doseganja zastavljenih ekonomskih in operativnih učinkov vzpostavljenega SUT KI.

Tehnološko-tehnični izzivi

Na področju tehnično-tehnoloških izzivov bi izpostavil predvsem izzive, ki jih prinaša stalen razvoj obstoječih tehnologij, novo razvijajoče se tehnologije, novi tehnološki procesi in novi poslovni modeli. Pri tem imam v mislih avtomatizacijo procedur, digitalizacijo procesov, integrirano nadzorovanje prenosnih poti, centralizacijo upravljanja varnostnih sistemov, testiranje varnostnih sistemov pred zunanjimi in notranjimi vdori in uvajanje umetne inteligence v SUT KI.

Velike spremembe se dogajajo tudi na področju tehničnih rešitev, kjer se veliki napredki v razvoju tehnike pojavljajo na področju video nadzorih sistemov, sistemov termovizije, sistemov kontrole pristopa in nadzora območij z droni. Hitre spremembe na teh področjih predstavljajo še poseben izziv, saj bodo morali upravljavci kritične infrastrukture na tem področju stalno spremljati razvojne trende in jih smiselno uvajati v svoje procese.

V kontekstu tehnološko-tehničnih izzivov bi izpostavil še strokovni vidik treh izzivov. Pri tem mislim predvsem na ustreznost projektiranja tehnološko-tehničnih rešitev, zagotavljanje združljivosti in povezljivosti obstoječih varnostnih rešitev z novimi, izpolnjevanje varnostnih standardov pri dobavi sistemov tehničnega varovanja, strokovno in zakonito montažo, servisiranje in vzdrževanje sistemov tehničnega varovanja ter njihovim nadgradnjam in posodobitvam, neprekinjenost delovanja, celovitost upravljanja operativnih informacij, kibernetskih incidentov, izrednih in kriznih dogodkov, izpolnjevanje zakonskih zahtev in kompetentnost pogodbenih izvajalcev in ne nazadnje spoštovanje zahtev s



področja varstva osebnih podatkov, kar predstavlja še posebej velik izziv.

Izzivi upravljanja outsourcinga

Problematiki outsourcinga oziroma pogodbene izvedbe sem v prejšnjih edicijah revije namenil že kar nekaj besed. Naj ob tem izpostavim predvsem naslednje izzive: izpolnjevanje zahtev javnega naročanja, ki trenutno upravljavcem kritične infrastrukture prinašajo več težav kot koristi, s tem povezane izzive ustreznega izbora strateških partnerjev, zagotavljanje kadrovske ustreznosti pogodbenih izvajalcev, neprekinjenost dobav pogodbenih izvajalcev ter njihovo neprekinjenost delovanja. Zavedati se je namreč potrebno, da neustreznost izbora pogodbenih izvajalcev in posledično odkloni od dogovorjenih okvirov sodelovanja, upravljavcem kritične infrastrukture prinašajo dodatna tveganja, ki lahko v določenem preseku časa in prepletu dogodkov usodno vplivajo na zanesljivost delovanja upravljavcev kritične infrastrukture.

Revizije delovanja SUT KI

Nadzor delovanja SUT KI je ključnega pomena za zagotavljanje njegove zanesljivosti in neprekinjenosti delovanja. V tem kontekstu je potrebno vzpostaviti sistemski nadzor in revizije delovanja SUT KI, s katerimi se ugotavlja v kakšni »kondiciji« je SUT KI in kako SUT KI upravlja s kibernetskimi incidenti, izrednimi dogodki in kriznimi razmerami. Nadzor in revizije delovanja SUT KI se lahko izvajajo z več vidikov, kot na primer: z vidika organizacije, z vidika odzivnosti na kibernetske incidente, izredne dogodke in krizne razmere ter ustreznosti njihovega upravljanja, z vidika skladnosti delovanja idr. Revizije in nadzore lahko izvajamo z lastnimi, zunanjimi ali kombinacijo lastnih in zunanjih nadzornih resursov. Z ugotavljanjem neželenih odklonov od načrtovanega stanja in njihovim odpravljanjem, zagotavljamo stalnost, učinkovitost in kakovost delovanja SUT KI ter uvajanje stalnih izboljšav v SUT KI. To pa je tisti nujni pogoj, ki zagotavlja dolgoročno zanesljivo in neprekinjeno delovanje SUT KI.

Krizno upravljanje in komuniciranje

V kolikor se želimo učinkovito spopasti s kibernetskim incidentom, izrednim dogodkom ali kriznimi razmerami moramo medsebojno uskladiti večje število akterjev in resursov in jih tudi ustrezno voditi. Večji kot je vpliv določenega dogodka na delovanje upravljavca kritične infrastrukture, višje nivoje je potrebno angažirati v procese upravljanja s temi dogodki. V upravljanje dogodkov, ki najbolj kritično vplivajo na delovanje upravljavca kritične infrastrukture, je potrebno vplesti tudi poslovodne organe ali neposredno poslovodjo upravljavca kritične infrastrukture. Sistem kriznega upravljanja mora temeljiti na načrtu kriznega upravljanja, katerega neločljivi del je tudi načrt kriznega komuniciranja, ki mora zagotavljati učinkovito in ustrezno komunikacijo med upravljavcem kritične infrastrukture, pristojnimi državnimi organi in, javnostjo, tako pred, med in po dogodku. Vzpostavitev učinkovitega kriznega upravljanja in komuniciranja, temelječega na ustreznih načrtih in navodilih, predstavlja izziv za upravljavce kritične infrastrukture.

Sklepna misel

Zakonodaja upravljavcem kritične infrastrukture določa minimalni okvir pogojev za njihovo delovanje. Da bi lahko upravljavci kritične infrastrukture zagotavljali zanesljivost in neprekinjenost delovanja, morajo, poleg vzpostavitve skladnosti delovanja z zakonodajo, najti ustrezne odgovore na vse zgoraj izpostavljene izzive in še polno drugih, ki se bodo pojavljali v procesu vzpostavljanja SUT KI. Ključno podlago za vzpostavljanje SUK KI predstavlja ocena tveganj (v širšem pomenu ocena ranljivosti, ogroženosti in tveganj), ki temelji na izboru ustrezne metodologije in metod ocenjevanja tveganj. Pri tem si lahko upravljavci kritične infrastrukture pomagajo z izdelano študijo »Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture«, ki jo je po naročilu Ministrstva za obrambo izdelal Inštitut za korporativne varnostne študije in je dostopna na spletnih straneh omenjenega ministrstva. ■



Nadzor in varnost, združena v inovativen elektronski sistem pristopa





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

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

Varnostni prehodi za nadzorovan dostop oseb na občutljiva območja



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



IDealni partner za identifikacijo in varnost

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

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*



REPORTAŽA:
Mednarodna konferenca »Dnevi korporativne varnosti 2019«

PODELITEV NAGRAD »SLOVENIAN GRAND SECURITY AWARDS 2019«

Deseta mednarodna konferenca „Dnevi korporativne varnosti 2019“ je ponovno potrdila ugled najpomembnejšega tovrstnega dogodka v regiji. Letos smo priča pomembni obletnici, katero predstavlja 10. obletnica organiziranja mednarodne konference »Dnevi korporativne varnosti«, kakor tudi enaka obletnica delovanja Instituta za korporativne varnostne študije, ICS-Ljubljana.

Inštitut za korporativne varnostne študije (ICS-Ljubljana) je marca organiziral 10. mednarodno konferenco „Dnevi korporativne varnosti“. So-organizatorja dogodka sta bila Slovensko združenje korporativne varnosti in regijsko združenje SE Corporate Security Association (SECSA). Letos je bila prireditev še posebej slovesna, saj ICS-Ljubljana praznuje 10. obletnico delovanja. Konferenca je sicer potekala v čudovitem ambientu Kongresnega centra Brdo pri Kranju. Udeležba več kot 200 udeležencev in uglednih gostov iz širšega regijskega prostora, vrsta odličnih predavanj, 4 okrogle mize in predstavitev cele vrste sodobnih tehnoloških rešitev, ki so jih na konferenci predstavili različni razstavljavci, je še enkrat potrdila, da je to srečanje nedvomno postalo največji tovrstni dogodek v tem delu Evrope.

Omenjena konferenca je že davno prerasla nacionalne okvire in tudi v širšem regijskem prostoru predstavlja enega izmed najbolj izpostavljenih dogodkov s področja korporativne varnosti. To vsekakor dokazuje tudi udeležba najpomembnejših gostov iz poslovnega, političnega in strokovnega okolja. Ši-







*avtor je član Slovenskega združenja korporativne varnosti





ritev konference in vedno večje število udeležencev kaže na to, da se zavedanje o pomenu varnosti počasi a vendar vztrajno dviguje. Najbolj prepoznavna rast udeležencev je zaznana ravno iz gospodarskega okolja, k čemur verjetno pripomore dejstvo, da je varnostno okolje, v katerem delujejo poslovne organizacije, vedno bolj zahtevno. Učinkovitega poslovanja si enostavno ni mogoče zamisliti brez dejstva, da je pomembno težišče namenjeno obvladovanju dinamičnih tveganj, s katerimi se soočamo na globalnih trgih. Dodatno prepoznavnost dogodku daje tudi podelitev prestižne nagrade Slovenian Grand Security Award, ki se vsako leto izvede v okviru otvoritvene slovesnosti omenjene konference.

Otvoritveno slovesnost so s svojimi nagovori popestrili dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti, g. Alojz Kovšca, predsednik Državnega sveta Republike Slovenije, dr. Klemen Grošelj, državni sekretar na Ministrstvu za obrambo, ga. Tatjana Bobnar, generalna direktorica Policije in predstavnik generalnega sponzorja, g. Aleksander Mervar, direktor ELES d.o.o..

V uvodnem delu mednarodne konference so bile podeljene nagrade »**Slovenian Grand Security Awards**« za izjemne dosežke v letu 2018. Ta nagrada je najvišje priznanje na področju varnosti v Republiki Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativen prispevek k razvoju in izvajanju varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti. Predsednik organizacijskega odbora konference, dr. Denis Čaleta, je v nagovoru poudaril, da so letošnji zmagovalci svetilniki odličnosti, ki jim je vredno slediti.

Nagrada je bila podeljena v sedmih kategorijah, podelitev pa so opravili g. Kovšca, predsednik Državnega sveta Republike Slovenije, ga. Bobnar, generalna direktorica Policije, ga. Prelesnik, Informacijska pooblaščenka, g. Grošelj, Ministrstvo za obrambo, g. Mervar, direktor ELES-a, g. Slapar, predsednik uprave Zavarovalnice Triglav, mag. Vršec in dr. Čaleta, predstavnika ICS Ljubljana. Letošnji nagrajenci so tako postali: Akrapovič d.d. (najvarnejše podjetje), g. Matjaž Peklaj, Kontrola zračnega prometa Slovenije (korporativni varnostni menedžer leta), podjetje HSI d.o.o. (najbolj inovativna varnostna rešitev), Mestna občina Ljubljana (najvarnejše mesto) in Občina Tržič (najvarnejša občina), revija Korporativna varnost (najboljši varnostni prispevek) in v kategoriji inovativna medijska promocija varnosti TV oddaja 24UR ZVEČER.

Skozi razprave med strokovnjaki, smo lahko razbrali, kako pomemben je proces upravljanja s tveganji in sodelovanje predstavnikov strateškega managementa v celotnem programu konference. V ta namen je bila organizirana okrogla miza na temo „Pričakovanja strateškega managementa od risk managementa“, ki jo je moderirala mag. Katja Kraškovic, dekanja Fakultete za podjetništvo - GEA College. Na okrogli mizi so sodelovali g. Aleksander Mervar - direktor ELES-a, g. Boštjan Gorjup – direktor BSH hišni aparati in hkrati predsednik Gospodar-











ske zbornice Slovenije, ga. Mojca Šimnic Šolinc - direktorica Tosame, g. Enzo Smrekar - predsednik uprave Droga Kolinska in direktor strateškega poslovnega področja Atlantic Grupe, Lovro Peterlin - direktor A1 Slovenije. Poudarili so, da se soočajo z zelo široko paleto tveganj, od kibernetskih napadov do tržnih tveganj in da posebno pozornost, veliko časa ter sredstev namenjajo obvladovanju tveganj v svojih podjetjih.

V nadaljevanju je konferenca ponudila vrsto odličnih predavanj priznanih gostov iz Slovenije in tujine. Izpostavimo lahko zelo zanimiv voden pogovor o izzivih korporativne varnosti v kompleksnem mednarodnem poslovnem okolju, ki ga je imel g. Andrej Podvršič (Chief Security Officer, Global Security CHEMOURS) s svojim gostom, g. Klausom H. Tipsmarkom (Chief Security Officer, Richemont International SA).

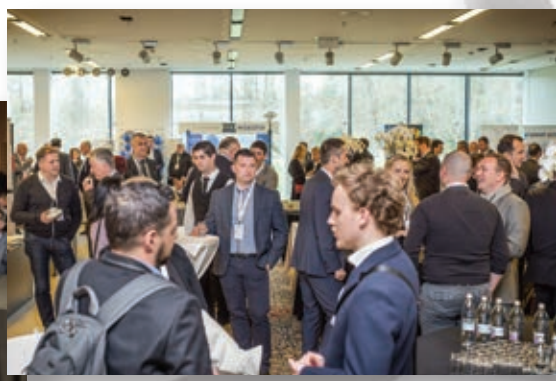
Naj omenimo še nekatere bolj izpostavljene predavatelje - g. Faiz Djellouli, izvršni direktor, Holiseum SAS iz Francije, Graeme Ballard, direktor Devolution Media (Anglija & Wales), Božidar Dajčman, direktor sektorja za upravljanje fizične in informacijske varnosti v Novi KBM (Slovenija), dr. Vittorio Rosato, vodja laboratorija ENEA za analizo in zaščito kritične infrastrukture (Italija) ...

Letošnja rdeča nit je bila zagotovo povezana s kibernetsko varnostjo, obvladovanjem tveganj, nadzorom ključnega osebja, zaščito ključne infrastrukture, izvajanjem GDPR in številnimi aktualnimi vprašanji. Glavna tema in izziv konference je bil povezan z „Upravljanjem s tveganji v kibernetskem okolju - integracija fizičnih in informacijskih procesov, nujnost kibernetskega okolja“. S pomočjo odličnih razprav in okroglih miz je bilo to povsem upravičeno. Obstajajo močni strokovni temelji, ki jih bodo strokovnjaki na tem področju lahko uporabljali v neposrednem poslovnem okolju.

Naj omenimo, da smo lahko na konferenci videli tudi veliko razstavljavcev oziroma sponzorjev dogodka. Predstavljali so različne novosti in možne rešitve na področju fizično-tehnične in IT varnosti ter možne sinergije obeh področij znotraj korporativne varnosti.

Skozi celoten program konference je cela vrsta dogodkov omogočala tkanje novih strokovnih stikov, izmenjavo novih izkušenj in seveda strokovno afirmacijo določenih strokovnjakov in ponudnikov varnostnih rešitev.

Po dveh dneh predavanj se je konferenca zaključila v prijetnem vzdušju z izmenjavo mnenj, izkušenj in dobrih praks, pri čemer je bila dana obljuba, da se bodo takšna strokovna srečanja nadaljevala tudi v prihodnje. Za konec se je dr. Čaleta zahvalil vsem udeležencem konference in jih povabil na »Dneve korporativne varnosti 2020 - največjo konferenco na področju korporativne varnosti v regiji jugovzhodne Evrope«. ■







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

PRAVA TEHNIČNA VARNOST SE ZAČNE Z DOBRIM NAČRTOVANJEM LICENCIRANEGA PROJEKTNEGA BIROJA

PET OBMOČIJ VAROVANJA

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

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

VARNOSTNI RAZREDI

Centrala mora nadzirati prenosne poti:

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

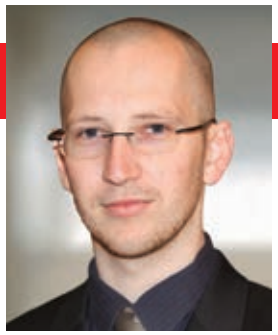
UPRAVLJANJE PROTIVLOMNEGA SISTEMA JE PREGLEDNO, PREPROSTO IN UPORABNIKOM PRIJAZNO

NAPREDNE TEHNOLOGIJE VAROVANJA

Vgrajujemo profesionalni sistem najvišjega kakovostnega razreda - Tecnoalarm

ZARJA ELEKTRONIKA

Avtor: mag. Matjaž Drev / Urad Informacijskega pooblaščenca*



GDPR IN (NE)DOLOČENOST ZAVAROVANJA OSEBNIH PODATKOV

V zadnjih letih se je, tudi zaradi javnega izpostavljanja nekaterih primerov neustreznega zavarovanja osebnih podatkov v slovenskih institucijah, večkrat odprlo vprašanje ali smo kot družba ustrezno pripravljeni na izzive zagotavljanja informacijske varnosti, še posebej, ko gre za varovanje osebnih podatkov.

Nekaj sistemskih prizadevanj je bilo opaznih, na primer kadrovsko okrepljen SI-CERT in vztrajni poizkusi vzpostavitve nove krovne (državne) institucije za zagotavljanje informacijske varnosti, t.i. SIGOV-CERT. Prav tako se je 25. maja 2018 v EU začela neposredno uporabljati Splošna uredba o varstvu podatkov (GDPR), ki je postavila nov okvir v zvezi z zagotavljanjem varnosti osebnih podatkov. Glavni izziv v zvezi s tem je – in to je tudi rdeča nit prispevka – kaj GDPR glede varnosti osebnih podatkov dejansko zahteva, kaj zgolj priporoča, kaj od tega je razumljivo (in razumno), kaj pa ostaja nedoločeno. Praksa inšpekcijskega nadzora namreč kaže, da odgovori na zastavljena vprašanja pogosto niso jasni ali enoznačni, da obstajajo različna tolmačenja glede »prave mere« varnosti osebnih podatkov in, da so upravljavci nemalokrat v nezavidljivem položaju, ko želijo zagotoviti ustrezno zavarovanje osebnih podatkov, a se ustavijo pri vprašanju kaj »ustrezno zavarovanje« sploh pomeni.

Kako ureja zavarovanje osebnih podatkov ZVOP-1?

Od začetka leta 2005 do 25. maja 2018, ko se je začela v EU neposredno uporabljati Splošna uredba o varstvu podatkov (GDPR), je področje zavarovanja osebnih podatkov v Sloveniji urejal Zakon o varstvu osebnih podatkov (ZVOP-1). Ta je v 14. členu določal, da morajo biti občutljivi osebni podatki, ki se prenašajo po telekomunikacijskem omrežju, šifrirani in elektronsko podpisani. Kar je nedvomno dobra varnostna usmeritev, a se je v praksi izkazalo, da je konkretno zahtevo (zaenkrat) nemogoče implementirati v vseh okoliščinah, ki vključujejo prenos občutljivih osebnih podatkov po telekomunikacijskih omrežjih. Zakaj? Najprej zato, ker ni povsem jasno kakšen način šifriranja podatkov naj bi se uporabljalo. Šifriranje med končnima uporabnikoma ali šifriranje med poštnima strežnikoma? Šifriranje celotne vsebine ali samo dela, ki vključuje občutljive osebne podatke? Kako je s šifriranjem ostalih telekomunikacijskih kanalov (prenosni telefoni, navadni telefoni, spletne aplikacije, glasovna in tekstovna sporočila)? GDPR te zahteve ne postavlja, kar je modro, saj gre za specifičen ukrep, ki ga je kljub dobrim namenom težko v celoti implementirati. Res pa je, da bo nov ZVOP-2 verjetno nadaljeval isto zgodbo in bo zahteva po šifriranju komunikacije še vedno prisotna.

Praksa inšpekcijskega nadzora namreč kaže, da odgovori na zastavljena vprašanja pogosto niso jasni ali enoznačni, da obstajajo različna tolmačenja glede »prave mere« varnosti osebnih podatkov in, da so upravljavci nemalokrat v nezavidljivem položaju, ko želijo zagotoviti ustrezno zavarovanje osebnih podatkov, a se ustavijo pri vprašanju kaj »ustrezno zavarovanje« sploh pomeni.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Je pa zato ZVOP-1 splošne varnostne zahteve opredelil v 24. členu, ki določa, da *»zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov, tako da se varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami, da se varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki, da se preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih, da se zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov, ter da se omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vnešeni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.«*

Zapisane zahteve, ki izhajajo iz temeljnih načel zavarovanja podatkov (zaupnosti, celovitosti, dostopnosti) so splošne, kar je po eni strani nujno, saj je namen (dobrega) zakona, da v svojih dikcijah zaobseže čim širši nabor situacij in je pri zahtevah dovolj univerzalen, da ga je mogoče aplicirati na kar najbolj raznoliko število primerov. V tem pogledu (če izvzamemo specifične zahteve prej opisanega 14. člena) je ZVOP-1 dober zakon.

Vendar se prav zaradi kvalitete splošnosti v praksi zastavljajo konkretna vprašanja, ki jih ni mogoče zadovoljivo pojasniti s pitijskim odgovorom »od primera do primera«.

Kaj denimo pomeni »varovanje prostorov«? Zaklepanje strežnika v posebno sobo? Uporaba lesenih ali kovinskih vrat? Uporaba določenih tipov ključavnic? Kako je z alarmi? Kako je s preprečevanjem »nepooblaščenega dostopa do osebnih podatkov«? Zadošča omejitev dostopa z ustreznim naborom uporabniških pravic in gesel (v zvezi z dolžino, kompleksnostjo in pogostostjo menjave gesel niti varnostna teorija ni več enotna). Je dopustno uporabljati napredne požarne zidove, ki analizirajo vsebino prometnih podatkov (DPI)? In kako je z revizijsko sledjo? Se mora beležiti prav vsaka obdelava osebnih podatkov? Zadošča beleženje vpogledov ali tudi sprememb? Kako dolgo hraniti revizijske sledi (pet oziroma šest let je v številnih primerih popolnoma nepraktično)? Kako zagotoviti sledljivost namenov obdelave (vpis namena v okence ob vsakem vpogledu, beleženje v beležko, zaupanje spominu uporabnika)? Celo, če najdemo sprejemljiv kompromis zagotavljanja sledljivosti pri obdelavi osebnih podatkov, ta velja, ko gre za sledljivost digitaliziranih podatkov. Kaj pa, ko brskamo po fizičnih mapah in fasciklih, ko dokumente fotokopiramo ali jih prepošiljamo iz enega konca organizacije na drugega?

Zastavlja se vprašanje ali je ob upoštevanju vseh bistvenih in pogosto zelo raznolikih okoliščinah (velikosti upravljavca, narave in obsega osebnih podatkov, varnostnih tveganj) sploh mogoče natančno opredeliti pogoje, ki bi jih bilo treba izpolnjevati.

In kako je z varnostjo osebnih podatkov v GDPR?

GDPR v členu 32 (podobno kot prej predstavljeni ZVOP-1 v 24. členu) opredeljuje splošni okvir varnosti osebnih podatkov. Določa, da *»ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljavec in obdelovalec z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotovita ustrezno raven varnosti glede na tveganje, vključno med drugim z psevdonimizacijo in šifriranjem osebnih podatkov, zmožnostjo zagotoviti stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo, zmožnostjo pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta, ter postopkom rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave osebnih podatkov.«*

Vsebinsko gre za splošen in celovit pristop k varnosti osebnih podatkov, ob tem pa se, kot v primeru ZVOP-1, zastavijo podobne dileme. Prav tako ni docela jasno ali so ukrepi kot denimo »psevdonimizacija in šifriranje osebnih podatkov« priporočilo ali zahteva. Po dosedanjih izkušnjah iz prakse in ob upoštevanju omejenih virov, ki jih imajo organizacije na voljo, gre predvsem za priporočilo oz. usmeritev k dobri varnostni praksi, ki pa se utegne v perspektivi nekaj let in ob vse večji prisotnosti kibernetskih groženj preoblikovati v zahtevo.

Poleg (na kratko orisanega) splošnega okvirja za zagotavljanje varnosti osebnih podatkov, GDPR prinaša nekatere novosti, ki se že bolj ali manj uspešno uveljavljajo v praksi in ki se zaenkrat kažejo kot koristen prispevek k vzpostavitvi bolj robustnega varnostnega okvirja.

Tako člen 25 določa, da bi si morali upravljavci in obdelovalci prizadevati za »vgrajeno in privzeto varstvo podatkov«, kar pomeni, da naj bi se že v fazi snovanja različnih oblik in rešitev obdelave osebnih podatkov sistematično razmišljalo o tem kako ustrezno zavarovati osebne podatke in kar najbolj zmanjšati morebitno škodo, ki bi zaradi zlorab lahko nastala.

Člen 33. in 34. urejata mehanizem poročanja o kršitvah varstva osebnih podatkov nadzornim organom in prizadetim posameznikom. Gre za mehanizem, ki sili upravljavce in obdelovalce k večji odgovornosti in previdnosti pri obdelavi osebnih podatkov, saj nalaga dolžnost, da se v primeru nekaterih kršitev (spet ostaja odprto vprašanje kdaj



je samoprijava nujna in kdaj ne) varstva osebnih podatkov samoprijavijo oz. o incidentu obvestijo prizadete posameznike. Ukrep še zdaleč ni nedolžen, saj izpostavlja upravljavce in obdelovalce ne le povečanemu nadzoru s strani nadzornih organov, ampak potencialno tudi pritiskom prizadete javnosti in medijev.

Člen 35 določa, da je v nekaterih primerih, zlasti ko gre za obsežno obdelavo osebnih podatkov s pomočjo novih tehnologij, potrebno predhodno izdelati oceno učinka v zvezi z varstvom osebnih podatkov. Podobno, kot v primeru »vgrajene zasebnosti«, gre tudi tukaj za težnjo, da se upravljavce prisili k sistematičnemu in projektnemu pristopu k obdelavi osebnih podatkov, kar se utegne izkazati kot eden koristnejših ukrepov, saj je žal celo pri izvedbi največjih nacionalnih projektov obdelave osebnih podatkov, pogosto manjkal temeljit razmislek o tem, kako zastaviti in izvesti obdelavo osebnih podatkov na način, da bodo podatki kar najbolje zavarovani, poseg v zasebnost posameznikov, pa ob upoštevanju namena obdelave osebnih podatkov, čim manjši. Ker se temu v preteklosti ni namenjalo dovolj premisleka, je bila posledica ta, da je prihajalo do nesorazmerno obsežnih obdelav osebnih podatkov, ki nemalokrat niso bili ustrezno zavarovani, odprave takšnih pomanjkljivosti pa so bile pogosto zelo drage.

Še ena opazna novost, ki jo ureja člen 37, 38 in 39, je imenovanje pooblaščene osebe za varstvo podatkov. GDPR določa kdo in kdaj mora takšno osebo imenovati, določa tudi nabor dolžnosti, ki jih mora pooblaščena oseba za varstvo podatkov izvajati. Zahteve in naloge so dovolj splošne, da jih bo mogoče v praksi izvajati, se pa zastavlja vprašanje, ali bo novi ZVOP-2 te pogoje tako zaostril, da (vsaj v začetnem obdobju) preprosto ne bo dovolj ljudi, ki bi lahko izvajali delo pooblaščenih oseb za varstvo podatkov. Upajmo, da si s prenovo domače zakonodaje ne bomo po nepotrebnem otežili uresničevanja ideje, ki se zdi tako v teoriji kot v praksi precej obetavna.

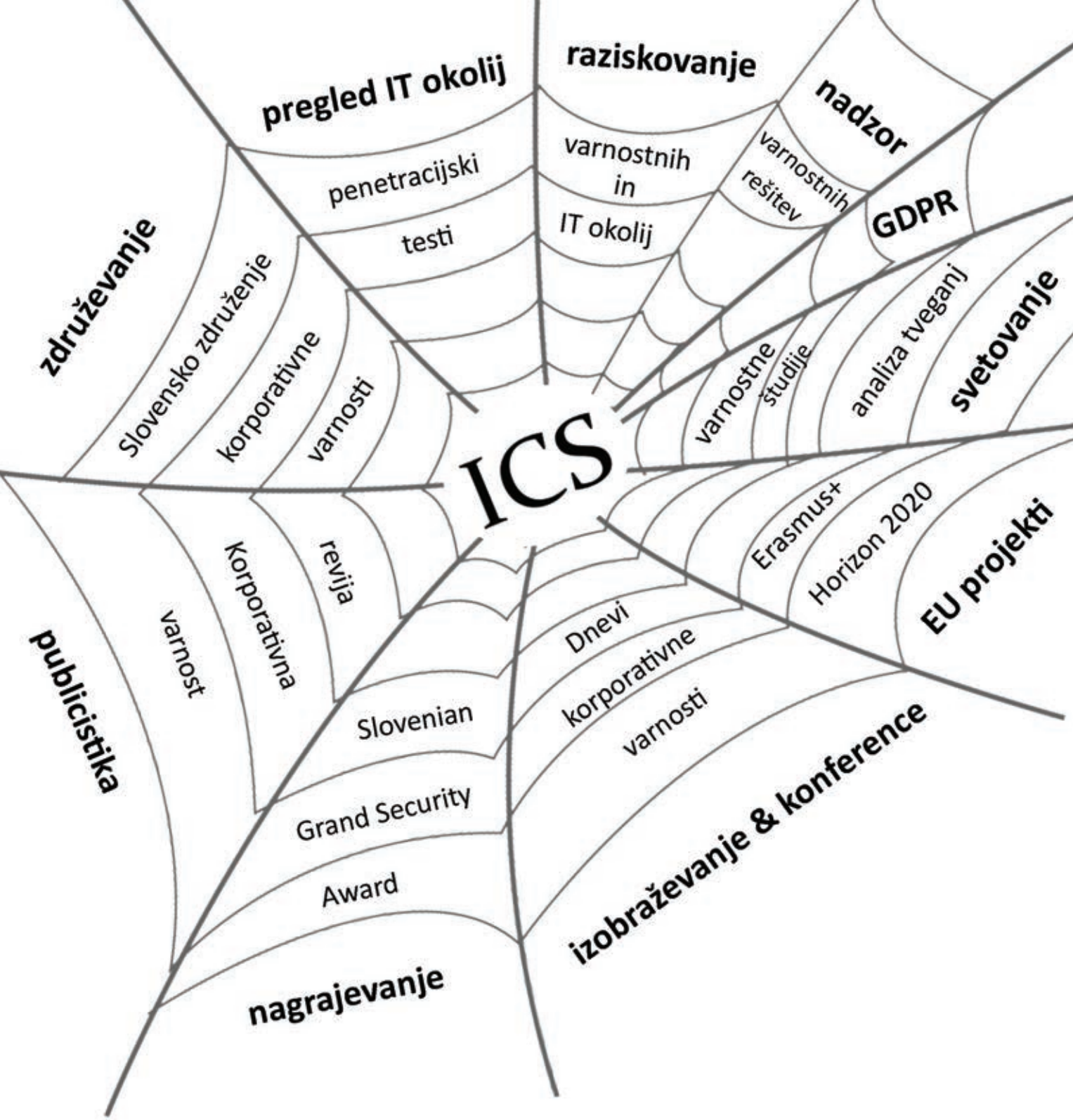
Kako ravnati?

Preprostega odgovora na vprašanje kako zagotoviti ustrezno raven varnosti osebnih podatkov glede na zahteve določb ZVOP-1 in GDPR ni. In sicer zato, ker (ne)ustrezna raven varnosti osebnih podatkov nikoli ni bila natančno opredeljena. Zastavlja se vprašanje ali je ob upoštevanju vseh bistvenih in pogosto zelo raznolikih okoliščinah (velikosti upravljavca, narave in obsega osebnih podatkov, varnostnih tveganj) sploh mogoče natančno opredeliti pogoje, ki bi jih bilo treba izpolnjevati. Prizadevanja na področju informacijske varnosti so sicer šla v to smer, če omenimo samo varnostni standard ISO/IEC 27001 in 27001, usmeritve NIST, okvir COBIT, priporočila organizacije ENISA in SANS, v primeru spletnih strani še priporočila projekta OWASP, pri plačevanju s kreditnimi karticami pa zahteve standarda PCI DSS. Vendar niti ZVOP-1 niti GDPR izrecno nikjer ne določata, da bi upravljavci, ki obdelujejo osebne podatke, morali slediti naštetim standardom in usmeritvam. To je nenazadnje razumljivo, saj je večina organizacij premajhnih in razpolaga s premalo viri, da bi lahko usmerjeno in sistematično sledile prej naštetim usmeritvam. Zato zaenkrat ostaja ustrezen pragmatičen pristop, ki od upravljavcev in obdelovalcev terja poznavanje zahtev ZVOP-1 in GDPR, v primeru nejasnosti pa tudi usmeritve ustreznih smernic Informacijskega pooblaščenca (zlasti smernice o zavarovanju osebnih podatkov in smernice o pripravi ocen učinkov na varstvo osebnih podatkov) in Delovne skupine iz člena 29.



Viri

- Smernice o zavarovanju osebnih podatkov. Informacijski pooblaščenec, Ljubljana, 2015.
- Smernice o ocenah učinka na varstvo osebnih podatkov. Informacijski pooblaščenec, Ljubljana, 2018.
- Smernice o pooblaščenih osebah za varstvo podatkov. Evropska komisija, Delovna skupina iz člena 29, Bruselj, 2017).
- Smernice o oceni učinka na varstvo podatkov. Evropska komisija, Delovna skupina iz člena 29, Bruselj, 2017).
- Smernice o uradnem obvestilu nadzornemu organu o kršitvi varstva osebnih podatkov. Evropska komisija, Delovna skupina iz člena 29, Bruselj, 2018.
- Predlog Zakona o varstvu osebnih podatkov (z dne 6.3.2019).
- Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov oz. GDPR) .
- Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07-UPB1; ZVOP-1). ■



ICS

INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE
CESTA ANDREJA BITENCA 68, LJUBLJANA
WWW.ICS-INSTITUT.SI

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



IZZIVI UVAJANJA IOT V OPERATIVNE POSLOVNE PROCESE

Internet stvari (ang. IoT - Internet of Things) ali internet vsega (ang. IoE – Internet of Everything) se nanaša na omrežja naprav z dodeljenim IP naslovom. Te naprave imajo sposobnost zaznavanja, zbiranja in pošiljanja podatkov z uporabo vgrajenih senzorjev, komunikacijske opreme in procesorja. IoT je tehnologija, ki je zmožna sprožiti pravo revolucijo na način življenja, kot ga živimo danes. Seveda pa na drugi strani omenjene naprave predstavljajo pomemben varnostni izziv, ki se ga moramo zavedati in ustrezno obvladovati.

V bistvu vsaka naprava, ki ima IP naslov in inteligenco, izpolnjuje pogoje, da se kvalificira kot IoT naprava. Če samo pomislimo na vse individualne naprave za pametne hiše, termostate, spletne kamere, krmilnike, zvonce na vhodnih vratih,.. Vse te naprave so v bistvu majhni računalniki, kar pomeni, da so lahko zlorabljeni kot vzvod napadalcem, da izvedejo različne napade, kot na primer DoS (ang. Denial of Service) napad, okužijo naprave s škodljivo programsko opremo, prestrežejo podatke na omrežju in tako dalje.

V internetu stvari, se beseda »stvar« nanaša na napravo, ki je lahko nameščena na naravnih, človeško narejenih ali na strojno izdelanih objektih in ima funkcionalnost komuniciranja po omrežju. Naprava kot taka, je lahko kontrolirana s strani oddaljenega napadalca. 21. oktobra leta 2016, je prišlo do ogromnega, pravzaprav največjega DDoS (ang. Distributed Denial of Service) napada v zgodovini, ki je baziral in bil izveden s pomočjo IoT naprav povezanih v svetovno omrežje. Napadeno je bilo ameriško podjetje Dyn, ki deluje na področju sistema domenskih imen (ang. DNS). Obstajajo poročila, ki pravijo, da je napad dosegel največjo magnitudo okoli 1.2 TB/s.

IoT naprave lahko komunicirajo s spletom na več načinov. Lahko imajo vzpostavljeno direktno komunikacijo s spletom ali pa uporabijo IoT prehod (ang. Gateway).

Naprave za komunikacijo uporabljajo različne tehnologije in protokole. Uporabljajo protokol brezžične komunikacije kratkega, srednjega in dolgega dosega ter seveda žični komunikacijski kanal.

Izzivov, ki jih s seboj prinaša svet IoT naprav je veliko. Najpomembnejši je pomanjkanje varnosti in zasebnosti. Lahko imajo ranljive spletne vmesnike, odprte ne šifrirane protokole in ne potrebna vrata. Prav tako je te naprave težko posodabljati ročno in največkrat njihovi operacijski sistemi niso deležni varnostno še kako pomembnih posodobitev, kar jih na neki točki lahko naredi ranljive. Vse to jih izpostavlja in pravzaprav postavi ob bok klasičnim računalnikom. Prav tako so te naprave napadene bolj ali manj na iste načine. Z varnostnega vidika o teh napravah ljudje premalo razmišljajo in jih brezglavo priklapljajo v omrežja ter jim s tem odpirajo vrata v svetovni splet.

Kot v pomoč pri zmanjševanju tveganj povezanih z IoT napravami, imamo lahko sledečo tabelo, ki vodi naše razmišljanje skozi 10 kategorij, ki nam jih je nastavila neprofitna organizacija OWASP (Open Web Application Security Project).

Niso samo proizvajalci teh naprav tisti, ki morajo upoštevati varnostne posledice uporabe interneta stvari. Na drugi strani smo vedno uporabniki teh naprav, ki se moramo zavedati varnostnih lukenj, ki jih neko ugodje ob pridobitvi te naprave, potegne s seboj.

*avtor je član Slovenskega združenja korporativne varnosti

OWASP Top 10 IoT ranljivosti

- Nezavarovan web dostop;
  a. Uporabniki pustijo nastavljene privzete nastavitve,
  b. Odsotnost mehanizma, ki zaklene račun v primeru večkratne neuspešne prijave,
  c. CSRF, SQLi, XSS ranljivosti.
- Nezadostna avtentikacija/avtorizacija;
  a. Nezanesljiv mehanizem obnovitve gesel,
  b. Šibka gesla,
  c. Odsotnost dvojnega faktorja avtentikacije.
- Nezavarovane mrežne nastavitve;
  a. Ranljivost na napad, ki onemogoča storitve (DoS),
  b. Izpostavljeni porti preko UPnP (ang. Universal Plug and Play),
  c. Odprti ne željeni porti, za katere največkrat niti ne vemo, da so odprti.
- Pomanjkanje šifriranja med transportom in verifikacije integritete;
  a. Občutljive in zaupne informacije so poslane nešifrirano skozi omrežje,
  b. Odsotnost SSL/TLS ali nepravilna konfiguracija,
  c. Uporaba primernih šifrirnih protokolov.
- Zasebnostni pomisleki;
  a. Zbranih je veliko osebnih informacij,
  b. Zbrane informacije niso pravilno manegirane in zavarovane,
  c. Končni uporabnik nima na voljo možnosti izbire pri zbiranju določenih podatkov.
- Nezavarovan vmesnik v oblaku (ang. Cloud interface);
  a. Vmesniki niso redno pregledani za varnostne ranljivosti,
  b. Prisotnost šibkih gesel,
  c. Pomanjkanje dvojnega faktorja avtentikacije.
- Nezavarovan mobilni vmesnik;
  a. Prisotnost šibkih gesel
  b. Odsotnost mehanizma, ki zaklene račun v primeru večkratne neuspešne prijave,
  c. Pomanjkanje dvojnega faktorja avtentikacije.
- Nezadostna varnostna nastavljivost;
  a. Pomanjkanje varnostnih možnosti,
  b. Pomanjkanje šifrirne možnosti,
  c. Pomanjkanje možnosti za omogočanje varnostnih beležk.
- Nevaren software/firmware;
  a. Nezadostno zavarovani strežniki za varnostne posodobitve,
  b. Nezavarovan, ne šifriran prenos posodobitev do naprave,
  c. Nepodpisane posodobitve za naprave.
- Slaba fizična varnost;
  a. Odprti nezaželeni zunanji vhodi kot npr. USB porti,
  b. Oddaljeni dostopi do operacijskega sistema,
  c. Brez možnost omejevanja upravnih zmogljivosti.

Vir: https://www.owasp.org

Cilj napadalcev je komprimirati pametne naprave, kot na primer: CCTV nadzorne kamere, avtomobile, tiskalnike, ključavnice, pralne stroje, itd. Z namenom pridobitve neavtoriziranega dostopa do omrežnih virov in IoT naprav, s katerim lahko ustvarijo svoje omrežje teh naprav ti. Botnet, ki čakajo na nadaljnje ukaze, največkrat izvršitev DDoS napada. Seveda gre dostikrat tudi za prodajo prestreženih podatkov na črnem trgu.

Nekaj nasvetov za obrambo pred IoT hekerskimi napadi;
- Onemogočite »guest« in »demo« uporabniške račune v primeru, da so aktivni,





- Uporaba funkcije »lock out«, ki zaklene račune s prevečkrat neuspelo prijavo,
- Implementirajte:
  a. močne avtentikacijske mehanizme,
  b. IPS (ang. Intrusion Prevention System) in IDS (ang. Intrusion Detection System),
  c. Šifriranje celotnega prometa z uporabo PKI (ang. Public Key Infrastructure),
- Uporabite VPN (ang. Virtual Private Network) arhitekturo za varno komunikacijo,
- Dovolite samo zaupanja vrednim IP naslovom dostop do naprave iz interneta,
- Onemogočite:
  a. telnet protokol (vrata 23),
  b. UPnP vrata na ruterjih.
- Zaščitite naprave pred fizičnim spreminjanjem,
- Nameščajte varnostne popravke in posodobitve na rednem intervalu,
- Spremljajte promet na vratih 48101, ker največkrat okužene naprave poskušajo razširiti okuženo datoteko ravno preko porta 48101.

In še nekaj nasvetov za proizvajalce IoT naprav;
- Vedno uporabljajte SSL/TLS za komunikacijske namene,
- Vzpostavite vzajemno preverjanje SSL certifikatov in seznam preklicanih potrdil,
- Spodbujajte uporabnike k uporabi močnih gesel,
- Proces posodabljanja naj bo preprost in varen z verigo zaupanja (ang. Chain of trust),
- Implementirajte mehanizem zaklepanja računa po nekaj neuspelih poskusih prijave in s tem preprečite napade s surovo silo (ang. Brute force),
- Zaklepajte naprave kadarkoli in kjerkoli je to mogoče, da jih zavarujete pred napadi,
- Periodično preverite naprave, če ima nameščena neuporabljena orodja in dovolite le zaupanja vrednim orodjem ali aplikacijam, da se izvajajo,
- Uporabite varno verigo za zagon (ang. Secure boot chain), da preverite vso programsko opremo, ki se izvaja na napravi.

Niso samo proizvajalci teh naprav tisti, ki morajo upoštevati varnostne posledice uporabe interneta stvari. Na drugi strani smo vedno uporabniki teh naprav, ki se moramo zavedati varnostnih lukenj, ki jih neko ugodje ob pridobitvi te naprave, potegne s seboj. Vsi se zavedamo, da je potrebno braniti računalnike in telefone pred virusi, vendar se malokdo zaveda, da so naše pozornosti še kako potrebne tudi naprave z zmožnostjo komuniciranja in procesiranja, ki so povezane v splet. Ker trend interneta stvari strmo narašča, z njim vzporedno naraščajo varnostne luknje. Po raziskavah »Juniper Networks« pričakujejo, da naj bi število pametnih naprav (IoT) do leta 2022 preseglo 50 milijard.

To ne pomeni, da se moramo bati ali izogibati IoT naprav. Ozaveščanje je ključnega pomena in predstavlja prvo linijo obrambe. Pa vendar tudi paranoja včasih reši kašno življenje. Kljub vsemu je potrebno redno preverjati naše v svet povezane naprave, jih redno testirati in iskati ranljivosti, ki jih posedujejo. ■

11. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 11.—12. MAREC 2020



PODELIJO SE IZBRANIM INSTITUCIJAM IN POSAMEZNIKOM ZA NJIHOV INOVATIVNI PRISPEVEK NA PODROČJU RAZVOJA IN UVELJAVLJANJA VARNOSTI. NAGRADO PODELJUJE ICS-LJUBLJANA V SODELOVANJU S SLOVENSKIM ZDRUŽENJEM KORPORATIVNE VARNOSTI. NEODVISNA KOMISIJA OCENJUJE IN IZBIRA KVALITETO TER IZVIRNOST PRIJAVLJENIH UDELEŽENCEV V NASLEDNJIH KATEGORIJAH:

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

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

Avtorica: Nataša Klenovšek Arh, univ. dipl, ing. rač. in inf., mag. dr. inf. / SI-CERT*



NAJPOGOSTEJŠE GROŽNJE, KI CILJAJO NA PODJETJA

Uporaba tehnologije ima vsekakor veliko prednosti, ki nam olajša delo, smo pa zagotovo uporabniki tisti, ki se premalo zavedamo, da je pri uporabi lete potrebno upoštevati vsaj osnovna načela informacijske varnosti. Zelo hitro lahko namreč en klik uporabnika pomeni popolno blokado delovanja celotnega podjetja, ter podjetju povzroči grozljive finančne posledice.

Kaj so osnovna načela informacijske varnosti? Zelo verjetno ste že nekolikokrat slišali za močna gesla, nameščanje popravkov, izdelavo varnostih kopij, zavedanje o problematiki objavljanja osebnih podatkov na družabnih omrežjih in previdnost pri odpiranju priponk v elektronskih sporočilih. Pa se teh načel tudi držimo? Glede na statistiko obravnavanih incidentov, ki jih prejmemo na SI-CERT, v letu 2018 jih je bilo nekaj manj kot 2500, bi na to vprašanje težko odgovorili pritrdilno.

Res je, da nepridipravi poskušajo na različne načine pretentati uporabnike in za to izkoriščajo različne tehnike "goljufanja", tako da vsekakor tega ni enostavno prepoznati, ko se ti lotijo nas.

Ali lahko danes plačamo?

Socialni inženiring je v zadnjem času izredno priljubljena tehnika, ki se je poslužujejo nepridipravi za izvedbo goljufij. Ena izmed teh goljufij pa je tudi t.i. direktorska prevara ali v angleščini CEO fraud. V Sloveniji se je pojavila nekje v letu 2016 in je še danes zelo aktualna.


From Marko Novak <mobile3453416@aol.com>
Subject računa
To racunovodstvo@podjetje.si

Dobro jutro,

Kakšno je razpoložljivo stanje bančnega računa? Ali lahko danes plačamo 32.700,00 evrov?

Lep pozdrav
Marko Novak

pošlji iz aplikacije za mobilne naprave

Primer elektronskega sporočila direktorske prevare

Direktorska prevara cilja na računovodje v podjetjih. Nepridipravi poiščejo vse potrebne informacije na spletni strani podjetja, nato pa preprosto ponaredijo naslov pošiljatelja in se lažno predstavijo kot direktor podjetja. Pošiljatelja v elektronskem sporočilu je namreč zelo enostavno ponarediti. To je približno tako težko, kot če nekomu pošljete navadno pismo, na v zgornjem levem kotu kuverte pa kot pošiljatelja napišete nekoga povsem tretjega.

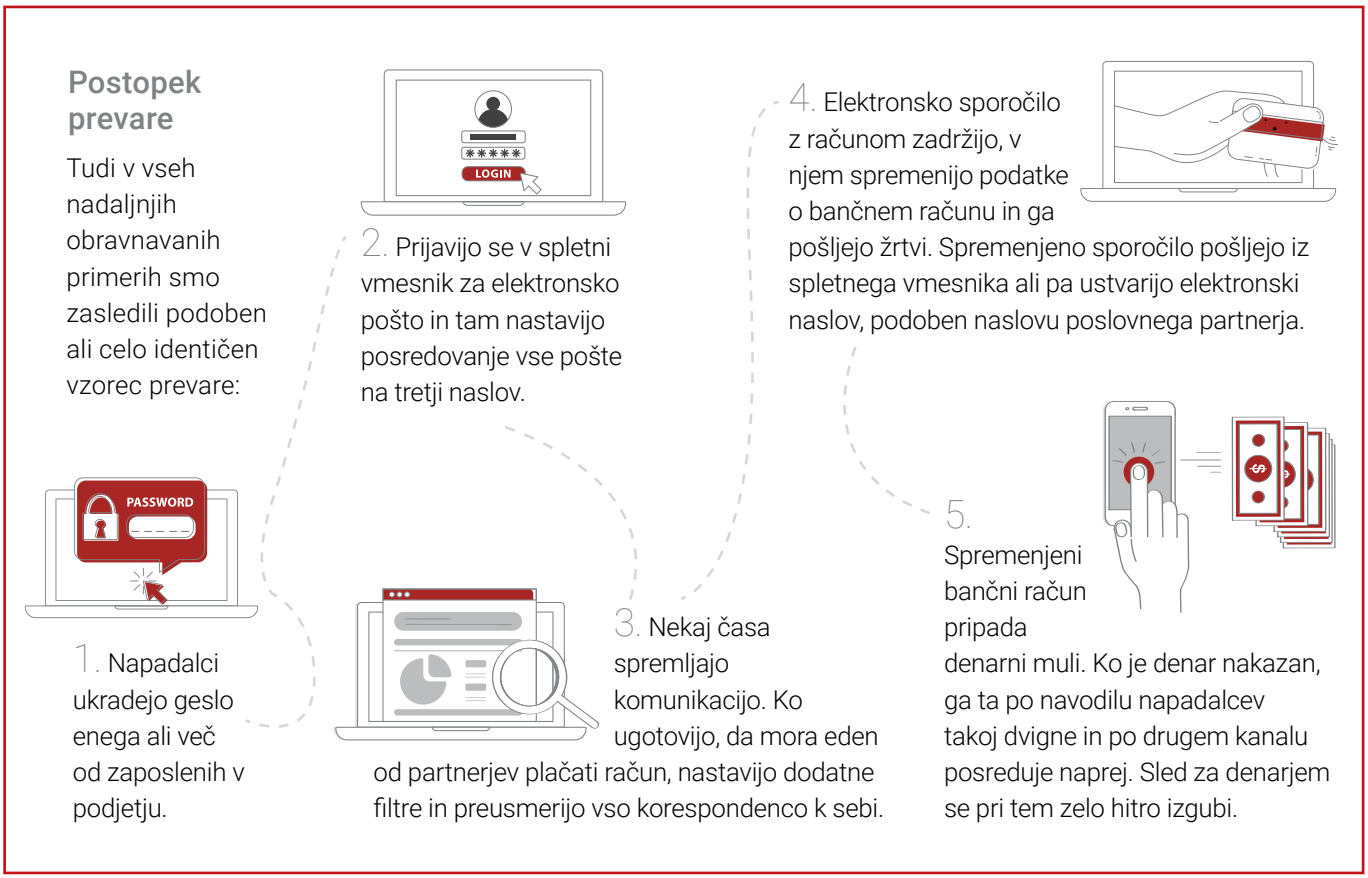
V elektronskem sporočilu nepridipravi nato v imenu direktorja prosijo za nakazilo večje vsote denarja v tujino. Tako lahko manjša nepazljivost podjetje stane precej denarja. Zato je v tovrstnih primerih vsekakor na mestu, da se vsakršno nenapovedano zahtevo za plačilo preveri na kakšen drug način, recimo preko telefona. Pa četudi je komunikacija z direktorjem še tako zelo neprijetno opravilo.

Nov bančni račun poslovnega partnerja

Napadi usmerjeni na posameznika (t.i. phishing) so eni med najpogostejšimi oblikami napada z namenom kraje podatkov, ki storilcu omogočajo dostop do različnih storitev v našem imenu. Z phishingom pa se začne tudi goljufija, ki jo imenujemo vdor v poslovno komunikacijo oziroma Man-In-The-E-mail.

Goljufija poteka tako, da nepridipravi, običajno preko povsem enostavnega phishing napada, najprej nekomu od zaposlenih ukradejo geslo za službeno elektronsko pošto. Nato pa se, ne da bi zaposleni karkoli sumil, prijavijo v njegov spletni vmesnik za elektronsko pošto, v njem nastavijo svoj elektronski naslov, kamor se pošilja kopija vse prejete pošte in nekaj časa samo spremljajo vsebino komunikacije. Na ta način pridobijo podatke tako o poslovnih partnerjih kot o načinu komunika-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti (v času pisanja članka še zaposlena na SI-CERT)



Postopek prevare vdora v poslovno komunikacijo

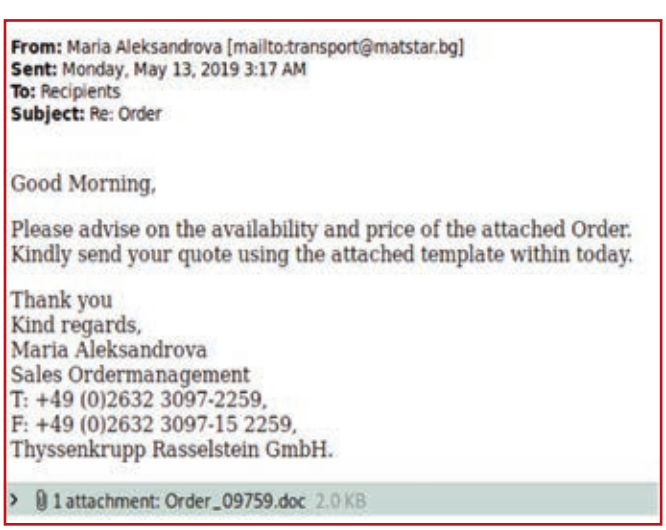
cije. V ključnem trenutku, ko si podjetje s svojim poslovnim partnerjem v tujini začne izmenjevati račune, pa aktivno posežejo v komunikacijo. Z uporabo filtrov in preusmeritev v spletnem vmesniku za elektronsko pošto, k sebi preusmerijo vso komunikacijo med poslovnima partnerjema, v elektronskem sporočilu zamenjajo številko bančnega računa za plačilo storitve ali blaga, in tako spremenjeno sporočilo pošljejo žrtvi. Spremenjeno sporočilo ne vsebuje praktično nobenih sumljivih znakov, da bi prejemnik lahko zaznal prevaro, zato so ti napadi praviloma uspešni.

Da je nekaj narobe, se običajno posumi šele takrat, ko plačana roba ni dostavljena, ali pa vas pozovejo, da že končno plačajte račun. Sled za denarjem je takrat že povsem izgubljena, podjetje pa čaka dolgotrajna in zapletena analiza vdora, ter odprto vprašanje krivde oziroma katero podjetje bo odgovorno za nastalo škodo – tisto, ki so mu vdrli v elektronsko pošto, ali tisto, ki pred nakazilom ni dovolj preverilo pravilnost bančnega računa.

Neplačan račun

Napadalci izbirajo raznovrstne poti s katerimi bi uporabnike prepričali v odpiranje datotek, ki so pripete elektronskim sporočilom in bi privedli do okužbe računalnika, ter s tem pridobili dostop do sistema in podatkov.

Zelo pogosto poskuša vsebina elektronskega sporočila pod pretvezo neplačanega računa uporabnika prepričati, da bi pripeto datoteko, najpogosteje je to vrste MS Office Word (.doc), odprl. Po odprtju .doc datoteke, le-ta običajno od uporabnika zahteva vklop makrov. Makro je programska koda, ki v tovrstnih primerih izvede povezavo na oddaljen naslov, iz katerega se prenese in samodejno zažene zlonamerna izvršljiva .exe datoteka, ki okuži računalnik z eno izmed različic trojanskega konja. Trojanski konj je zlonamerna programska oprema, ki poskuša pridobiti podatke na okuženem sistemu (gesla, bančne poverilnice...), ter jih nato pošilja na oddaljeni spletni naslov.


From: Maria Aleksandrova [mailto:transport@matstar.bg]
Sent: Monday, May 13, 2019 3:17 AM
To: Recipients
Subject: Re: Order

Good Morning,

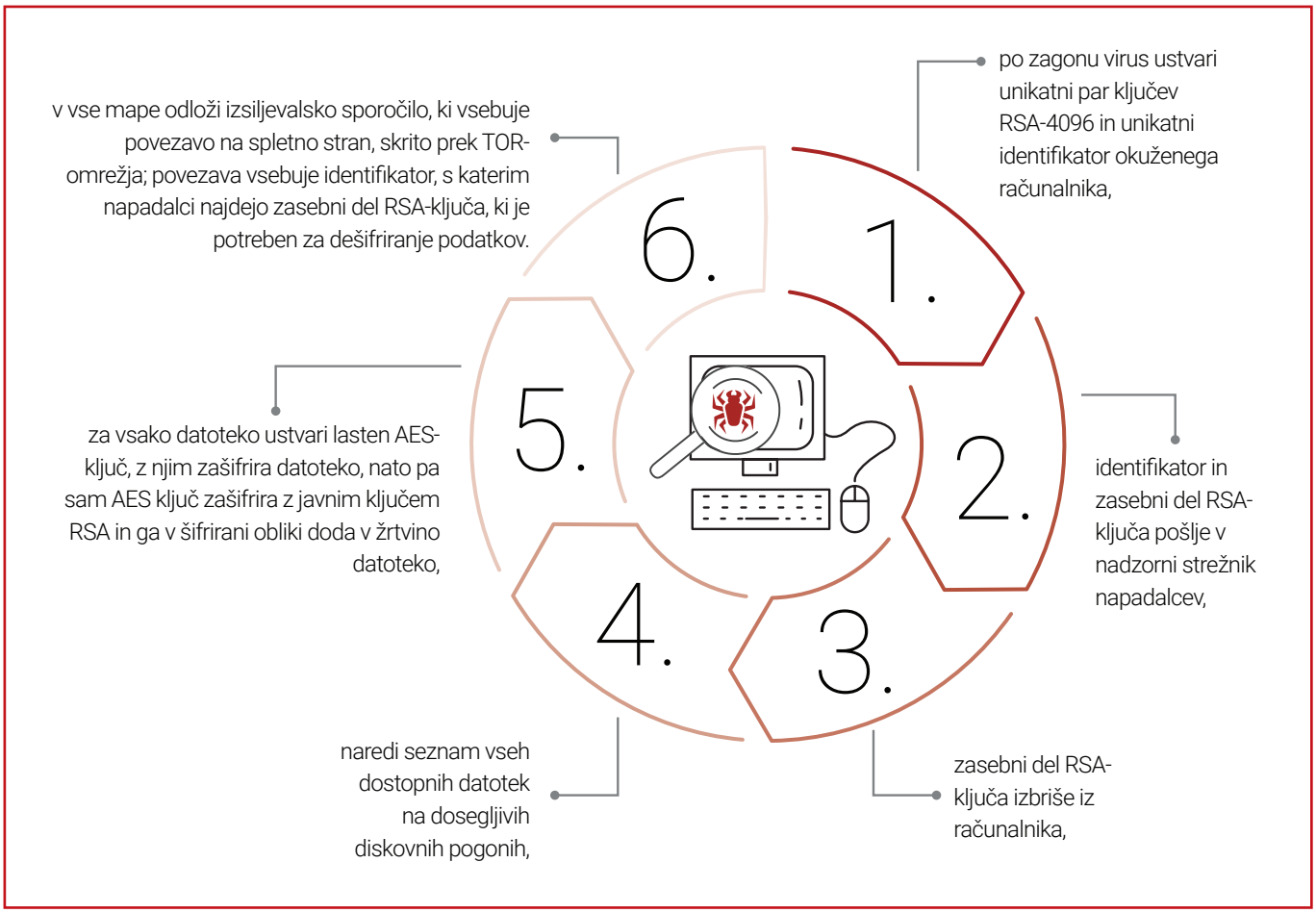
Please advise on the availability and price of the attached Order.
Kindly send your quote using the attached template within today.

Thank you
Kind regards,
Maria Aleksandrova
Sales Ordermanagement
T: +49 (0)2632 3097-2259,
F: +49 (0)2632 3097-15 2259,
Thyssenkrupp Rasselstein GmbH.

1 attachment: Order_09759.doc 2.0 KB

Zlonamerna elektronska pošta s .doc priponko

Da bi tovrstna zlonamerna sporočila delovala legitimno in tako prejemnika prepričala v odpiranje priponke, pa v ta namen nepridipravi zelo pogosto zlorabijo tudi ime kakega podjetja. Zato je dodatna previdnost pri tovrstnih sporočilih še toliko bolj pomembna.



Danes delam od doma

Delo od doma oziroma delo iz oddaljene lokacije je vsekakor dobrodošla možnost, ki omogoča fleksibilnost dela. Za vse prednosti, ki jih omogoča, pa ima delo od doma tudi slabosti.

Odprta storitev za oddaljen nadzor in upravljanje s sistemom, npr. Remote Desktop (Oddaljeno namizje) je namreč izredno pogosto tarča napadov in zlorab. Veliko vdorov v informacijske sisteme podjetij se namreč zgodi preko storitve za oddaljen dostop. Z vdorom pa podjetje tvega izgubo podatkov, ki se zgodijo s krajo ali pa z namestitvijo enega izmed izsiljevalskih virusov, kateri zašifrira vse datoteke.

Razvoj izsiljevalskih virusov skozi nekaj let je pripeljal do postopka, ki ga uporabljajo skoraj vse sodobne različice

Najbolj izpostavljena tarča so strežniki do katerih administratorji preko storitve oddaljenega namizja dostopajo od doma. Storilci najpogosteje s poskušanjem različnih kombinacij uporabniških imen in gesel, t.i. napad s surovo silo, pridobijo geslo za dostop. Kot za vsako storitev zaščiteno z geslom, se zato tudi tukaj priporoča uporaba kompleksnih gesel, lahko pa dostop s požarnim zidom omejite zgolj na določene IP naslove ali pa zaščitite preko tuneliranih šifriranih povezav z ustrezno avtentikacijo. Še najbolje pa je, če storitev oddaljenega dostopa v času, ko le-tega ne potrebujete, izklopite.

Veliko vdorov v informacijske sisteme podjetij se namreč zgodi preko storitve za oddaljen dostop. Z vdorom pa podjetje tvega izgubo podatkov, ki se zgodijo s krajo ali pa z namestitvijo enega izmed izsiljevalskih virusov, kateri zašifrira vse datoteke.

Inovativnost nepridipravov, ki želijo izkoristiti hiter poslovni tempo in komunikacijske vrzeli ne pozna meja, zato je potrebno biti pozoren na vsa odstopanja in preveriti le-ta pri ključnih odločevalcih po več komunikacijskih poteh. Pri povezovanju z oddaljenih lokacij pa uporabljati šifrirane tunelirane povezave in tako zaščititi komunikacijsko pot. ■

GREMZVLAKOM

ZAGREB / 9 €

OPATIJA, REKA / 9 €

PULJ / 19 €

BEOGRAD / 29 €

BUDIMPEŠTA / od 15 €

DUNAJ / od 29 €

MÜNCHEN / od 29 €

ZÜRICH / od 29 €

FRANKFURT / od 49 €

PRAGA / od 39 €



Slovenske železnice

www. slo-zeleznice.si

Avtor: Borut Lončarevič / visoki gasilski častnik, predsednik komisije za industrijsko gasilstvo pri Gasilski zvezi Slovenije*



VLOGA INDUSTRIJSKEGA GASILSTVA PRI ZAGOTAVLJANJU KORPORATIVNE VARNOSTI

Prihaja čas, ko moramo gasilca predstaviti kot enakopravnega gradnika korporativne in globalne varnosti. Z razvojem tehnologij in hitrim odzivom industrije na trg se povečujejo tudi tveganja in škode, ki nastanejo ob različnih nesrečah v industriji. Škode nastajajo zaradi poškodb ljudi, opreme, objektov, izdelkov ter izpada proizvodnje. Ko nad potekom nesreče izgubimo nadzor, imamo velike posledice v ožjem in širšem okolju.

Gasilci že dolgo nismo zgolj krotilci ognjenega petelina, saj se ukvarjamo s širokim spektrom nevarnosti in reševanj. V industriji se gasilci pojavljamo na različnih področjih in različnih organizacijskih strukturah. Naše naloge zajemajo preventivne dejavnosti, aktivne dejavnosti za zmanjševanje tveganj in krizne dejavnosti s ciljem neprekinjenega delovanja industrije oziroma čim hitrejšega vzpostavljanja v normalno stanje.

S spremembo družbene ureditve in prehoda na novo tržno naravnano industrijo ter nekontroliranim lastninjenjem, so ugašale tudi gasilske enote. Na ostankih velikih in dobro organiziranih tovarnah so nastale številne manjše poslovne enote, katere niso imele potreb, sredstev ali želje za organiziranje gasilske enote.

Industrijsko gasilstvo v Sloveniji

Gasilska Zveza Slovenija (GZS) se kot krovna gasilska organizacija zaveda pomena delovanja Prostovoljnih industrijskih gasilskih društev, za zagotavljanje učinkovite požarne in druge varnosti. Stanje industrijskih gasilskih društev po letu 1991 se je drastično poslabšalo. Od zabeleženih 200 industrijskih gasilskih društev po osamosvojitvi Slovenije se na današnji dan pogovarjamo o 44 delujočih društvih. Še bolj zaskrbljujoč podatek je, da se je na anketo Komisije za industrijsko gasilstvo odzvalo samo 23 industrijskih enot, kar najverjetneje sovpada tudi z dejansko aktivnostjo industrijskih gasilskih enot. Statistični podatki kažejo na nadaljnje upadanje industrijskega gasilstva. V zadnjem kongresnem obdobju se je trend zmanjševanja števila industrijskih društev nekoliko umiril; zabeležili smo celo ustanovitev dveh novih enot.

Za lažje razumevanje nastale situacije je potrebno omeniti nekaj vzrokov, ki so pripeljali do nastale situacije. S spremembo družbene ureditve in prehoda na novo tržno naravnano industrijo ter nekontroliranim lastninjenjem, so ugašale tudi gasilske enote. Na ostankih velikih in dobro organiziranih tovarnah so nastale številne manjše poslovne enote, katere niso imele potreb, sredstev ali želje za organiziranje gasilske enote. Procesu lastninjenja je sledila sprememba lokalne samouprave, ko smo iz 62 občin leta 1991, ustanovili 212 občin. Vsem nastalim spremembam je bolj ali manj posrečeno sledila tudi zakonodaja. Kapital počasi spoznava dejstvo, da se vsega žal, ali pa morda tudi na srečo, ne da kupiti. Gasilstvo je način življenja, razmišljanja in predanega dela. Zato bodo leta zanemarjanja tega področja v

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Industrija žal šele skozi številne nesreče spoznava dodano vrednost organiziranega gasilstva znotraj svojih industrijskih obratov. Vse premalo se zavedamo uničujočih posledic velikih nesreč v industriji, katere se kažejo na uničenem okolju, ljudeh in živalih.



industriji vsekakor pustila dolgoročne posledice.

Kljub vsemu pa nesreče ne počivajo in nastalo situacijo rešujejo teritorialna gasilska društva in poklicne gasilske enote. Industrija žal šele skozi številne nesreče spoznava dodano vrednost organiziranega gasilstva znotraj svojih industrijskih obratov. Vse premalo se zavedamo uničujočih posledic velikih nesreč v industriji, katere se kažejo na uničenem okolju, ljudeh in živalih.

Organiziranost gasilstva

Gasilci se v industriji lahko pojavljamo na različne načine. Nekaj najpogostejših možnosti: kot zaposleni v podjetju, člani Prostovoljnega industrijskega gasilskega društva (PIGD) ali člani industrijske gasilne enote (IGE), kot člani lokalnih Prostovoljnih gasilskih društev (PGD) ali del javne poklicne gasilske službe. Lahko pa tudi kot poklicni gasilci zaposleni v podjetju.

Podrobneje lahko gasilstvo ločimo glede na območje delovanja:
- teritorialno;
- industrijsko gasilstvo.

Organiziranost teritorialnega gasilstva

Trajno in nemoteno opravljanje javne gasilske službe zagotavljajo lokalne skupnosti in država. Lokalna skupnost skladno s svojimi pristojnostmi zagotavlja organiziranost, opremljanje in delovanje gasilstva.

Organizacija gasilstva v lokalni skupnosti se skladno z merili za organiziranje in opremljanje gasilskih enot določi z načrtom varstva pred požarom lokalne skupnosti. Obseg in način opravljanja javne gasilske službe se določi skladno z merili za organiziranje in opremljanje gasilskih enot, časi določenimi za prihod gasilskih enot na kraj nesreče, merili za požarno pokrivanje posameznih vrst objektov, načrtom varstva pred požarom ter načrti zaščite in reševanja ob naravnih in drugih nesrečah posamezne občine.

Teritorialne gasilske enote (TGE)

Teritorialne prostovoljne in poklicne gasilske enote opravljajo javno gasilsko službo in so razvrščene v sedem kategorij, katerim je prilagojena kadrovska sestava enot in njihova tehnična opremljenost. Gasilske enote (GE) I., II. in III. kategorije se organizirajo kot prostovoljne gasilske enote, GE IV. in V. kategorije kot prostovoljne gasilske enote ali kot prostovoljne enote s poklicnim jedrom, GE VI. in VII. kategorije pa kot poklicne enote.

Razvrstitev gasilskih enot na podlagi meril za organiziranje in opremljanje opravi župan na predlog gasilskega poveljstva občine in občinske strokovne službe. Dodatna oprema teritorialnih gasilskih enot za gašenje požarov v naravnem okolju se določi na podlagi meril za gozdove.

Večina tveganj ob nastanku interventnega dogodka pade na teritorialne prostovoljne in poklicne gasilske enote. Zaradi načina organiziranosti, standardov izvoza na kraj nesreče, časovnega zamika pri javljanju na dogodek se povečuje tudi obseg dogodka in nastala škoda. Zato je še kako pomembna primerna gasilska organiziranost znotraj posameznih podjetij.

Industrijske gasilske enote (IGE)

Industrijske gasilske enote morajo ustanoviti gospodarske družbe, zavodi in druge organizacije, če imajo povečano nevarnost nastanka požara, eksplozije ali druge posebne nevarnosti. Vrsta in obseg industrijskih gasilskih enot se določita skladno z merili za organiziranje in opremljanje gasilskih enot. Gasilsko zaščitno in reševalno opremo za delovanje gasilske enote mora zagotoviti ustanovitelj. Industrijske gasilske enote so razvrščene v štiri kategorije; te so določene na podlagi meril za razvrščanje industrijskih gasilskih enot. Točkovanje za določanje potrebe in nivo enote je sestavljeno iz petih področij:
- vrsta dejavnosti in nevarnosti (kovinska, lesna, gumarska, tekstilna, ind.);
- število zaposlenih;

- površina za opravljanje dejavnosti;
- oddaljenost od poklicne gasilske enote;
- vgrajen sistem aktivne požarne zaščite in povezava s poklicno gasilsko enoto.

Na podlagi točkovnika se oblikuje minimalna zahteva Industrijske gasilske enote.

Uredba o organiziranju in opremljanju gasilskih enot predstavlja temelj za zasnovo industrijskih gasilskih enot. Glede na to, da se je industrija preoblikovala po svojih zakonitostih, bodo v prihodnje verjetno potrebne nekatere korekcije uredbe. Gasilci so v času, skozi številna izobraževanja in različne intervencije,

Tabela 1: Prisotnost gasilcev in opreme v IGE

Obvezna prisotnost gasilcev

Kategorija GE	Na delovno izmeno		Izven delovnega čas		Pripadajoča gasilska
	poklicnih	nepoklicnih	poklicnih	nepoklicnih	vozila in oprema
GE I. kategorije	-	3	-	-	
GE II. kategorije	-	5	5	1	GV-1 ali GV-V1
GE III. kategorije	2	1	1	1	GVC-16/25
GE IV. kategorije	4	5	4	5	GVC-16/15, GVC-24/50 ali GVS-V

Vir: Uradni list RS, št. 42/07 (pojasnilo kratic GV-1: gasilsko vozilo 1, GV-V1: gasilsko vozilo z vodo, GVC-16/25: gasilsko vozilo s cisterno)



postali splošna reševalna služba. Kot splošna reševalna služba pa industrijski gasilci lahko pripomorejo k povečani korporativni varnosti na različnih področjih.

Potenciali gasilcev v industriji

- Izgubljeni kapital: gasilci se skozi gasilski izobraževalni sistem izobražujejo na številnih področjih. Ker gre za specifična znanja, tovrstno izobraževanje in trening ostaja za delodajalce neznanka. Gasilci se tako izobražujejo iz gradbeništva, elektrike, kemije, prve pomoči, strojništva, tehničnih nesreč, preventive, informatike, radijskih in ostalih zvez, taktike, kriznega vodenja, osebnosti in motivacije in številnih drugih vsebin. Gasilec skozi temeljna izobraževanja opravi več kot 600 ur izobraževanj, ki jih dopolnjuje še s številnimi specialnimi znanji (tehnično, kemično reševanje, vrvne tehnike itd.). V zgoraj navedenem seštevku ur izobraževanj ni všteto stažiranje in operativne aktivnosti. Brez zadržka lahko govorimo, da delodajalec ob zaposlitvi gasilca dobi dodatno usposobljenega sodelavca s širokim profilom znanja.

- Ocena tveganj: zaposleni gasilski častniki lahko sodelujejo pri ocenah tveganj za nastanek požara, izliva vode, izpada električne energije, nevarnost strojeloma, obnašanje objekta ob različnih nesrečah (poplave, neurja,



potres) ter pripravljenost podjetja na omenjene nevarnosti.

- Preventivne aktivnosti: gasilci lahko odigrajo aktivno vlogo pri postavljanju aktivne požarne varnosti, preventivnih pregledih na opremi in objektu, sodelujejo pri projektiranju, vršijo nadzor pri vgrajevanju opreme in naprav, požarni straži.
- Krizni management: gasilski častniki se v sklopu izobraževanj usposobijo za delovanje v kriznih situacijah. Obvladajo sistem vodenja gasilskih intervencij IPS- intervencijski poveljniški sistem. Pripravljeni so na hitro načrtovanje, delegiranje nalog, sprejemanje odločitev in izvajanje. Tako pridobljeno gasilsko znanje je lahko v veliko pomoč pri normalnem delovanju podjetja ali v kriznih situacijah.

Podrobneje bodo področja opisana v naslednjih prispevkih.

Izzivi za prihodnost

Z obravnavo tematike se odpirajo številne težave, hkrati pa je to možnost za predloge izboljšav in dopolnitev sistema delovanja industrijskega gasilstva. Krepiti moramo zavedanje, da je gasilstvo oz. (v tem primeru) industrijsko gasilstvo pomembno za zagotavljanje korporativne varnosti organizacij. Komisija za industrijsko gasilstvo si bo prizadevala za odpiranje različnih tem omenjenega področja ter pomoč pri realizaciji:

- Revizije operativnih načrtov in načrtov alarmiranja v organizacijah;
- Dopolnitev uredbe o organiziranju IGE;
- Povezovanje z izobraževalnimi ustanovami in inštituti;
- Prepoznavanje gasilskega potenciala s strani delodajalcev;
- Olajšave s strani države za podjetja, ki imajo organizirano IGE ali PIGD;
- Zniževanje stroškov zavarovanj zaradi tveganja nastanka nesreč in zmanjševanja škod;
- Izobraževanje gasilcev in nosilcev odgovornosti v podjetjih.

Sodelovanje med GZS in Inštitutom za korporativne varnostne študije se mora v prihodnosti odraziti na področjih varnostnega zavedanja o pomenu vzpostavitve učinkovitih organizacijskih procesov za delovanje industrijskega gasilstva, kot tudi v razvijanju novih organizacijskih pristopov, standardov in predvsem pri izmenjavi dobrih praks, ki bodo v prihodnosti dvigovale kvaliteto zagotavljanja korporativne varnosti.

Slovensko združenje za korporativno varnost predstavlja pomembno strokovno okolje, kjer GZS neposredno sodeluje v strokovni interakciji s predstavniki vseh najpomembnejših gospodarskih in javnih organizacij. V prihodnosti bo potrebno tej strokovni izmenjavi novih znanj in izkušenj dati poseben poudarek.

Literatura:

- GZS (2018). XVII. Kongres Gasilske zveze Slovenije, 55, 303
- Vir: URSZR http://www.sos112.si
- Uradni list RS, št. 42/07: 4547. Uredba o organiziranju, opremljanju in usposabljanju sil za zaščito, reševanje in pomoč, stran 12323
- Gradivo Komisije za industrijsko gasilstvo. ■

Gasilnik

2 L / 6 L

Bonpet systems

Zanesljivi gasilni sistemi

Enostavni in varni gasilniki za vse, ki prisegate na klasiko.



Gasilnike uporabljamo za gašenje začetnih požarov, predvsem gorečih maščob in olj v gostinskih lokalih, v kuhinjah, kantinah, strojnicah, pekarnah, pisarnah, na hodnikih, v delavnicah, na kmetijah, v skladiščih ipd.

Za gašenje požarov tipa A, B in F.

Prednosti:

- Ročno delovanje.
- **Specialist za olje in maščobe (F razred).**
- Vsebuje ljudem in okolju prijazno gasilno sredstvo Bonpet.
- 2-letna garancija in 20-letna življenjska doba ob rednem vzdrževanju.
- Slovenski izdelek.

Tehnične karakteristike 2 L

Dimenzije: 375 x 110 mm
Skupna teža: 4,0 kg
Gasilna sposobnost: 8A, 55B, 25F
Prostornina: 2 L gasilne tekočine Bonpet

Tehnične karakteristike 6 L

Dimenzije: 580 x 150 mm
Skupna teža: 10,2 kg
Gasilna sposobnost: 27A, 144B, 75F
Prostornina: 6 L gasilne tekočine Bonpet

Certificirano na MPA Dresden,
po standardu EN 3-7:2004 + A1: 2007

MPA Dresden

Pot Vitka Pavliča 9, 1430 Hrastnik
info@bonpet.si

www.bonpet.si

Avtor: Aleš Ribič / direktor HSI d.o.o.



KDO ODLOČA O PRIORITETAH OB IZREDNIH DOGODKIH V KRITIČNI INFRASTRUKTURI?

Glavna prioriteta upravljalca kritične infrastrukture je, da zagotavlja nemoteno delovanje storitev. Ta skrb v največji meri pripada direktorju upravljalca, le ta pa skozi sistemizacijo pooblasti ustrezne službe oziroma osebe, ki so zadolžene, da se storitve na vseh nivojih zagotavljajo z največjo možno razpoložljivostjo.

Da bi to dosegli, se v večjih podjetjih organizira služba za korporativno varnost, ki na vseh nivojih skrbi za obvladovanje rizikov in implementacijo ustreznih rešitev, da se le te zmanjšajo na minimum. Podjetja, ki nimajo službe za korporativno varnost, te naloge razdelijo med več drugih služb, kot na primer službo za informacijske tehnologije, službo za varnost in varovanje, kadrovsko službo, splošni sektor in druge.

Da bi lahko službe, ki so za to pooblaščene s strani direktorja družbe, izvajale svoja dela na področju zagotavljanja kontinuitete storitev, je potrebno izvesti precej aktivnosti. V tem članku se bom osredotočil na sodobne sisteme tehničnega varovanja, ki prinesejo dragocen čas v katerem lahko bistveno zmanjšamo učinke incidentov in s tem povečamo razpoložljivost storitev upravljalca kritične infrastrukture.





Ko govorimo o prioritetah za zagotavljanje storitev, govorimo o vsaj treh področjih, ki jih je potrebno razjasniti:
- določanje rizikov in katere rešitve moramo vpeljati, da bodo riziki čim manjši oziroma jih ne bo
- prioritete pri implementaciji rešitev
- ukrepanje v primeru incidenta in izkoriščanje dodatnega časa, ki ga lahko pridobimo.

Določanje rizikov na fizičnem in kibernetskem prostoru

Tako fizični dostopi kot kibernetski vdori zahtevajo sisteme za odkrivanje le teh. Različni objekti kritične infrastrukture zahtevajo različen pristop s tem pa tudi različne sisteme za zaznavanje vdorov.

Na fizičnem nivoju je potrebno zagotoviti ustrezno mehansko zaščito (ograje, rešetke, zapornice, protivlomne folije...), ki zagotavljajo otežen dostop do objektov. Bolj je dostop otežen, več časa si s tem »kupimo«. Sistemi tehničnega varovanja (sistemi za zgodnje odkrivanje požara, video nadzori z analitiko, termalne kamere, proti-vlomni sistemi..), pa nam zagotavljajo, da se bo potencialni rizik takoj zaznal. Čas, ki smo ga pridobili, je odvisen od vrste in kvalitete mehanske zaščite in pa od sistema zaznave vloma. Zaznavanje vloma se lahko vrši na perimetru s termalnimi kamerami, ki pokrivajo veliko področje in dolge razdalje, kot tudi z varovanjem območja z radarskimi sistemi ali zakopanimi optičnimi kabli. Proti-požarni sistem zaznava rizike potencialnih požarov, kjer pa je prav tako pomembno ravno zgodnje pred-alarmno stanje. Dogodki iz nastalih sistemov se morajo prioritetno obdelovati, kar pa nam prinese dragocen čas, katerega izkoristimo za zmanjšanje ali celo preprečitev incidenta.

Na kibernetskem nivoju je nekoliko težje, kajti če se nekdo prikrade v naše omrežje, tega ni moč videti s klasičnimi tehničnimi sistemi varovanja. Za ta namen so razvita posebna programska orodja, ki lahko v realnem času zaznajo odstopanja v mrežnem prometu in na namenskem monitorju sporočijo operaterju to odstopanje. Za razumevanje delovanja teh orodij, je v večini primerov potrebno strokovno znanje s področja omrežij in IT infrastrukture. Takega strokovnjaka bi potrebovalo vsako podjetje, ki se zaveda rizikov na tem področju. Strokovnjaki trdijo, da je polovica podjetij že bila kibernetsko napadena, druga polovica pa še ne ve, da je bila. Ta ocena je sicer pretirana, pa vendar pove veliko o potencialu, ki ga imajo spletni kriminalci. Napadi se vršijo na dnevnem nivoju. Obstaja nekaj spletnih strani, ki kažejo napade v realnem času. Seveda so to zaznani napadi. Tistih, ki jih programska orodja ne zaznajo, jih ne vidi nihče. Ena izmed takih spletnih strani je: https://threatmap.fortiguard.com/ Incidenti v kibernetskih napadih so samo posledica dolgotrajnega raziskovanja omrežja s strani napadalcev. V primeru ukrajinskega napada na elektro omrežje, se je napad izvajal več kot pol leta prej. Pri teh napadih se napadalci zavedajo, da bodo v omrežju težko odkriti. Tudi, če se jim zapre pot, preko katere so vstopili v omrežje oziroma »vdrli v sistem«, bo njihova identiteta zelo težko izsledljiva. Kibernetski napadalci torej fizično niso prisotni na samemu objektu, kar jim daje svojevrstno prednost pri svojem delu.

Opisane tehnične rešitve nam doprinesejo dragocen čas, in če ga pravilno razporedimo, lahko preprečimo ali omilimo marsikateri napad na kritično infrastrukturo. Ko govorimo o doprinosu časa, govorimo od nekaj sekund, ko gre za vlomne ali požarne incidente, do nekaj dni, ko gre za kibernetske napade.

Izbira pravih rešitev in pravega poslovnega partnerja, na področju tehničnega in kibernetskega varovanja, je ključnega

pomena. Na podlagi teh odločitev, bo na dolgi rok temeljila celotna varnost vaše kritične infrastrukture.

Prioritete pri implementaciji rešitev

Prva naloga upravljalca kritične infrastrukture je, da skozi implementacijo rešitev zagotovi enotnost sistemov za vse svoje objekte. Druga prioriteta, pa govori o določanju vrste varnostne rešitve glede na rizike določene v varnostnem načrtu. Za nekatere je prioriteta kibernetska varnost, za druge pa mehanska zaščita. Pri tem pa se moramo zavedati, da so upravljalci kritične infrastrukture zavezani različnim zakonom, ki jim morajo slediti. S tem predvsem mislim na zakon o javnih naročilih, zaradi katerega se lahko hitro zgodi, da imamo v objektih vrsto rešitev, ki pa medsebojno niso združljive. To nas na koncu privede do veliko slabših reakcijskih časov in odzivov na incidente, posledično pa so škode in izpadi kontinuitete delovanja storitev kritične infrastrukture veliko večji. Zagotavljanje enotnosti opreme, znotraj upravljalca kritične infrastrukture, je ključnega pomena za hitro in učinkovito ukrepanje. Z vidika kibernetske varnosti moramo iskati rešitve različnih proizvajalcev in sicer: vsi objekti naj imajo protivlomno varovanje od enega proizvajalca, medtem, ko naj imajo vsi objekti video nadzor drugega proizvajalca. Vsi tehnični sistemi varovanja pa naj bodo od različnih proizvajalcev. Na ta način smo otežili delo kiber-napadalcu, kajti različni programerji, ki so zaposleni pri proizvajalcih opreme, nehote za seboj puščajo različne hrošče. Napadalci morajo te hrošče odkriti, če želijo napad uspešno izvesti. Ker različni proizvajalci uporabljajo različne tehnologije pri razvoju produktov, morajo tudi napadalci, da zaobidejo nek sistem, raziskovati dlje časa. To pa nam daje čas, da to zaznamo in pravočasno ukrepamo.

Ukrepanje v primeru incidenta in izkoriščanje dodatnega časa

Služba za korporativno varnost oziroma za to zadolžena služba, mora izdelati natančna navodila za ukrepanje ob zgodnjem zaznavanju incidentov. Zgodnje zaznavanje je čas od prvega dogodka, ko se obvesti operaterja o odstopanjih, pa do začetka incidenta, ko nastane prva škoda v smislu prekinitve storitev. Če se v tem času hitro in učinkovito ukrepa, seveda pa z ustreznimi prioritetami obvešča, smo ves pridobljeni čas izkoristili in preprečili incident. Le tako se povrne ROI v celotno opremo. Da pa se na te incidente hitro in učinkovito odreagira, pa mora upravljalec razmisliti o interni nadzorni sobi, v kateri se zbirajo informacije iz vseh objektov in vseh sistemov tehničnega varovanja. Tak sistem se imenuje centralno nadzorni sistem (CNS) oziroma v angleškem jeziku physical security information management (PSIM). Tak sistem zagotavlja hiter pregled stanja nad vsemi objekti, tako v smislu video nadzora, pristopne kontrole, protivlomnih sistemov, sistemov za zgodnje odkrivanje požara, domofonskih sistemov, nadzora klimatov in drugih. Nadzornik, ki ima pregled nad sistemom PSIM, ima pregled tudi nad zemljevidi in tlorisi objektov, kjer se vizualno prikažejo spremembe stanja. Pri tem pa moramo vedeti, da nadzorna soba NI varnostno nadzorni center (VNC), kjer pa veljajo drugačna pravila. VNC ima v večini primerov nadzor nad protivlomnimi sistemi in sistemi za zgodnje odkrivanje požara, medtem, ko dostopa do drugih sistemov, tudi z vidika uredbe GDPR, nima. Nadzornik se na podlagi vseh sistemov, do katerih ima dostop, in na podlagi jasnih navodil o prioritetnih ukrepih, odloča in obvešča o situaciji in jo spremlja v realnem času.

Navodila za ukrepanje morajo vsebovati različne scenarije. Vsak scenarij je določen glede na vrsto incidenta. Posamezni scenarij mora vsebovati vsaj naslednje elemente:

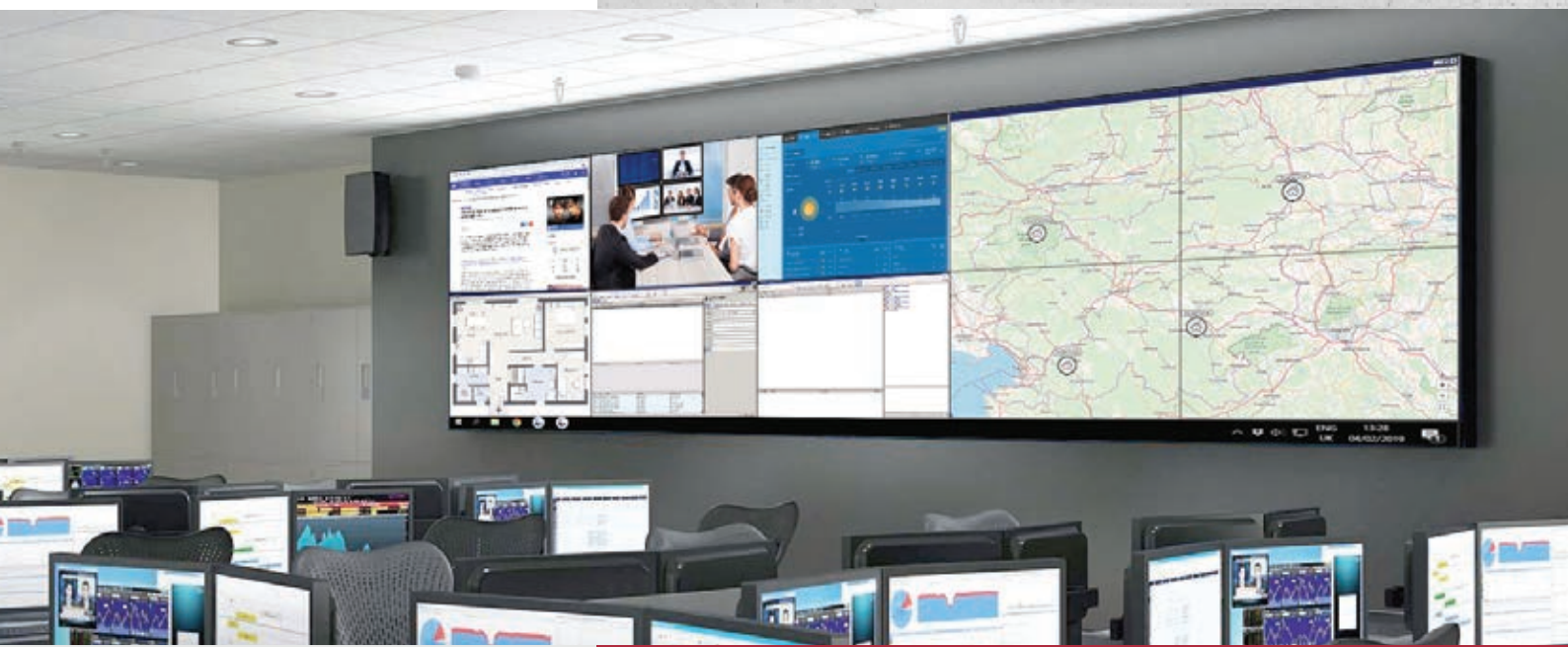
- kdo in v kakšnem primeru obvešča:
  - odgovorne osebe za posamezne objekte ter vodstvo družbe
  - policijo, gasilce ali reševalce
  - center za obveščanje
  - varnostno službo
  - medije in jim podaja informacije o incidentu
- protokol vstopa v objekt:
  - kje so ključi, kartice in kdo ima dostop do njih v izrednih primerih
  - kdo lahko vstopi v objekt in pod kakšnimi pogoji
  - izobraževanje zunanjih izvajalcev za varen vstop v objekt
  - določena pot po kateri se lahko gibajo osebe, ko vstopijo v objekt
  - kje so prepovedni prostori, kamor se ne sme vstopati oziroma se vstopa po posebnem protokolu
- spremljanje incidenta in eskaliranje:
  - dodatno obveščanje ob zaznavi incidenta
  - sprotno obveščanje o spremembah, ki so zaznane tokom poteka incidenta
  - komunikacija z ožjim vodstvom o poteku incidenta
  - sklic kriznega sestanka, kjer se odloča o nadaljnjih ukrepih, ki presegajo navodila o ukrepih
  - sprotno natančno beleženje poteka dogodkov ter komunikacije in zbiranje informacij s terena
- zaključek incidenta
  - zbiranje vseh informacij o samem incidentu
  - pisanje poročila o poteku incidenta
  - predstavitev poročila vodstvu družbe

Povzetek

O prioritetah se začne govoriti, ko se vodstvo s službo za korporativno varnost odloči, da zagotovi ustrezne rešitve, ki omogočajo zbiranje informacij na enem mestu, in sicer v nadzorni sobi naročnika. Te informacije vsebujejo veliko količino osebnih podatkov, ki se morajo hraniti znotraj organizacije kritične infrastrukture in naj se NE dajejo na vpogled ali celo posest zunanjim službam. S tem zagotovimo, da so osebni podatki na varnem mestu in da jih ne more zlorabiti tretja oseba, ki bi želela ohromiti ali onemogočiti zagotavljanje storitev kritične infrastrukture. S premišljeno izbiro tehničnih sistemov si pridobimo dragocen čas, v katerem lahko preprečimo marsikateri incident. Seveda pa ne moremo mimo dejstva, da je v celotni organizaciji potreben ustrezen, preverjen in usposobljen kader, ki se zaveda odgovornosti, ki jo nosi kot posameznik v celotni verigi zagotavljanja storitev. Vse osebe, ki so kakorkoli vpletene v proces reševanja incidentov, morajo biti seznanjene z navodili, ki jih ima tudi nadzornik v nadzorni sobi. Za različne scenarije pa je potrebno občasno narediti »suho vajo«, ki pokaže pripravljenost in morebiti tudi kakšno možnost izpopolnjevanja samih navodil. Tako varnostni načrt, kot navodila za ravnanje v primeru posameznega incidenta, so živi dokumenti, za katere je določena odgovorna oseba, ki skrbi, da so ti dokumenti vedno skladni z drugimi akti v podjetju ter, da so vsi zaposleni, ki so povezani v verigi reševanja incidentov, ustrezno usposobljeni za take situacije. ■

HSI
HARDWARE SOFTWARE INOVATIONS

www.hsi.si
info@hsi.si



Alarm-PSIM

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

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

Avtomatiziran Hiter Zanesljiv
Uporabniku prijazen

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

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

VPRAŠAJTE NAS

Avtorji: Alenka Glas, višja svetovalka, Tina Jereb, svetovalka, Tevž Delak, svetovalec / Pro.Astec d.o.o.

ANALIZA POSLOVANJA PODJETJA

Poslovanje podjetja poteka v dinamičnem, spreminjajočem se svetu, kjer je potrebno veliko prilagajanj na okolje tako pri doseganju ekonomskih kot drugih ciljev podjetja. Ob tem se podjetja posvečajo kakovosti, učinkovitosti, varnosti in zakonski skladnosti poslovanja. Za zagotavljanje vseh teh ciljev predstavljamo nekaj osnovnih analiz poslovanja, ki podjetju ponudijo primeren nabor podatkov za odločanje o investicijah, zaposlitvah, spremembah organiziranosti in upravljanju skladnosti poslovanja.

Poslovanje podjetja poteka v dinamičnem, spreminjajočem se svetu, kjer je potrebno veliko prilagajanj na okolje tako pri doseganju ekonomskih kot drugih ciljev podjetja. Poslovni procesi predstavljajo učinkovito organiziranost poslovanja podjetja, pri čemer je njihovo oblikovanje in delovanje osnova uspešnega poslovanja. Taka organiziranost se oddaljuje od splošno sprejete tradicionalne organiziranosti.

Poslovni procesi podjetju zagotavljajo izvedbo storitve ali izdelavo izdelka, oba sta namenjena končnemu odjemalcu. Ker so pogoji izvedbe poslovnega procesa spremenljivka, se mora podjetje temu ustrezno prilagajati in pogosto tudi v naprej načrtovati odzive na spremembe.
Analiza poslovanja s poudarkom na analizi vplivov na poslovanje temelji na poslovnih procesih. Analiza poslovanja, in znotraj tega analiza vplivov na poslovanje, naj podjetju zagotovi predvsem primerne informacije za:
- postavitev vizije in strategije,
- uspešno in kakovostno poslovanje,
- stroškovno učinkovito izvedbo,
- realizacijo zastavljenih ciljev,
- neprestan razvoj podjetja.

Fleksibilnost podjetja pri izvajanju gornjih aktivnosti je ključna, zagotavljanje učinkovitega izvajanja poslovnih procesov pa samo posledica fleksibilnosti.

Poslovni procesi predstavljajo učinkovito organiziranost poslovanja podjetja, pri čemer je njihovo oblikovanje in delovanje osnova uspešnega poslovanja.

Ocenitev poslovnih tveganj in vpliva potencialnih nevarnosti z analizo tveganj in analizo vplivov na poslovanje

Osnovni analizi poslovanja sta analiza vplivov na poslovanje (BIA) in analiza tveganj (RA).

Analiza tveganj in analiza vplivov na poslovanje morata postavljati izhodišča za strategijo družbe predvsem v povezavi z upravljanjem tveganj in iz tega izhajajočih upravljanj storitev, neprekinjenega poslovanja, varovanja informacij in podobno.

Analiza vplivov na poslovanje
Analiza vplivov na poslovanje (BIA – Business Impact Analysis) pokaže vplive delovanja / nedelovanja / napačnega delovanja posameznega procesa na poslovanje podjetja. Poleg tega analiza vplivov na poslovanje opredeljuje medsebojno odvisnost procesov, potrebe po sredstvih (ljudje, tehnična sredstva, komunikacije ipd.) za izvajanje procesa na minimalnem nivoju, možnosti izvajanja procesa z alternativnimi metodami (ročno izvajanje, delo od doma ipd.) ter vrsto dodatnih parametrov, pomembnih za določitev strategije in izdelavo načrtov neprekinjenega poslovanja.

Analiza vplivov na poslovanje je primerna osnova za izvajanje upravljanja (predvsem) IT storitev, kar vključuje katalog IT storitev, upravljanje zahtevkov in dogodkov, upravljanje sprememb in problemov in podobno.

Na podlagi analize zbranih podatkov mora poročilo o izvedeni analizi vplivov na poslovanje oziroma strategija načrtovanja neprekinjenega poslovanja upoštevati:

- kvantitativne finančne vplive
- kvantitativne vplive na podjetje
- kvalitativne vplive na kakovost
- kvalitativne vplive na odnose
- seznam poslovnih funkcij, urejen po nujnosti časa obnove
- potrebe za minimalno delovanje
- možnosti za alternativno okrevanje.

Analiza tveganj (RA)

Z analizo tveganj (RA – Risk Analysis) se identificirajo kritična tveganja, na podlagi katerih se skozi upravljanje tveganj vzpostavijo nadzorstva (ukrepi, kontrole). Z nadzorstvi se v čim večji možni meri preprečuje tako razvoj prekinitev in katastrofalnih dogodkov kot tudi škodljive posledice takih dogodkov, kadar jih ne moremo preprečiti (na primer potresa).

Analiza tveganj in analiza vplivov na poslovanje morata postavljati izhodišča za strategijo družbe predvsem v povezavi z upravljanjem tveganj in iz tega izhajajočih upravljanj storitev, neprekinjenega poslovanja, varovanja informacij in podobno.

Opredeljevanje potrebnih izhodišč delovanja

Iz podatkov, ki so bili zajeti v obeh analizah, se pridobijo naslednji podatki:

Podatek	Način pridobitve podatka	Analiza
Ciljni čas okrevanja (RTO) in najdaljši sprejemljivi čas izpada (MTPD)	Opredeljen na podlagi BIA analize, kjer se opredeljujejo kvantitativni in kvalitativni vplivi na poslovanje v različnih časovnih terminih. RTO je določen tako, da se poslovni proces poskuša izogniti vsem katastrofalnim vplivom, MTPD pa tako, da se proces poskuša izogniti vsem velikim vplivom na poslovanje.	BIA
Okrevanje podatkovnih virov in ciljne točke okrevanja (RPO)	RPO se opredeli na nivoju podjetja za vsak podatkovni vir posebej. Temelji na BIA posameznih poslovnih procesih, kjer poslovni procesi opredelijo vpliv izgube podatkov v različnih časovnih obdobjih.	BIA
Točka ene napake	Točka ene napake se opredeli na nivoju podjetja za posamezne vire. Temelji na BIA posameznih poslovnih procesih, kjer poslovni procesi opredelijo take vire.	BIA
Podatki v edini kopiji	Podatki v edini kopiji se opredelijo na nivoju podjetja za posamezne podatkovne vire. Temelji na BIA posameznih poslovnih procesoih, kjer poslovni procesi opredelijo take vire.	BIA
Informacijska infrastruktura	V BIA vsak posamezen poslovni proces opredeli najnujnejšo informacijsko infrastrukturo (programsko opremo) za nadaljevanje poslovanja v krizni situaciji. Iz zbranih podatkov je razvidna oprema rezervne lokacije.	BIA
Strojna oprema	V BIA vsak posamezen poslovni proces opredeli najnujnejšo strojno opremo za nadaljevanje poslovanja v krizni situaciji. Iz zbranih podatkov je razvidna oprema rezervne lokacije.	BIA
Komunikacije	V BIA vsak posamezen poslovni proces opredeli najnujnejše komunikacije za nadaljevanje poslovanja v krizni situaciji. Iz zbranih podatkov je razvidna oprema rezervne lokacije.	BIA
Prostori rezervne lokacije	V BIA vsak poslovni proces opredeli potrebno minimalno število delovnih mest za nadaljevanje poslovanja v krizni situaciji. Iz zbranih podatkov je razvidna oprema in velikost rezervne lokacije.	BIA
Potrebe po kadrih	V BIA vsak poslovni proces opredeli potrebno minimalno število ljudi in njihovo sestavo glede na delovna mesta, ki jih potrebuje za nadaljevanje poslovanja v krizni situaciji.	BIA
Ostali viri	V BIA vsak posamezen poslovni proces opredeli najnujnejše ostale vire za nadaljevanje poslovanja v krizni situaciji. Iz zbranih podatkov je razvidna oprema rezervne lokacije.	BIA
Model delovanja neprekinjenega poslovanja	Na podlagi zbranih podatkov iz BIA in RA se opredeli model delovanja neprekinjenega poslovanja predvsem v smislu priprave rezervne lokacije in kopiranja podatkov. Model delovanja je odvisen predvsem od RTO, MTPD, RPO in pripravljenosti podjetja glede na sprejemanje tveganj, ki ob tem nastopajo.	BIA RA



Ocenitev vplivov na zasebnost in skladnost

Ocena učinkov v zvezi z varstvom osebnih podatkov – DPIA

Namen in vzroki za izvedbo ocene učinka na zasebnost

Uredba (EU) 2016/679 (Splošna uredba o varstvu podatkov) predpisuje izvedbo ocene učinka na zasebnost v primerih, kadar bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave »povzročila veliko tveganje za pravice in svoboščine posameznikov«. Izvedba ocene učinka na zasebnost se zahteva zlasti v primerih:

- sistematičnega in obsežnega vrednotenja osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;
- obsežne obdelave posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški, ali
- obsežnega sistematičnega spremljanja javno dostopnega območja.

Ob tem je treba upoštevati Smernice[1] Delovne skupine za varstvo podatkov iz člena 29[2], ki natančneje podajajo naslednjih devet meril, da se zagotovi konkretnejši niz dejanj obdelave, za katere se zahteva ocena učinka v zvezi z varstvom podatkov zaradi velikega tveganja, ki je z njimi neločljivo povezano.

Izvedba DPIA

Osnovna izhodišča, ki jih zajema DPIA, so sledeča:

- opis predvidenih dejanj obdelave in namenov obdelave, načini pridobivanja podatkov, in sredstva za obdelavo podatkov, zakoniti interesi in drugo;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj glede na zasebnost posameznikov, na katere se nanašajo osebni podatki;
- ukrepe za obravnavanje tveganj, kar vključuje organizacijske in tehnično tehnološke ukrepe;
- izdelava poročila, v katerem je opisan projekt, ocenjena tveganja in opredeljeni ukrepi

V okviru izvedbe procesa Ocene učinkov v zvezi z varstvom podatkov, se opravijo sledeče aktivnosti:

- Prepoznava osebnih podatkov s ključnimi parametri obdelave osebnih podatkov;
- Opredelitev in prepoznava ključnih tveganj; proces upravljanja tveganj povezanih z varstvom osebnih podatkov;
- Opredelitev in opis predlaganih ukrepov za zmanjševanje tveganj, povezanih z varstvom osebnih podatkov,
- Evidenca sprejetih ukrepov, s katerimi se znižuje tveganja (evidenca odobrenih ukrepov),

Ocena učinka na varstvo osebnih podatkov služi kot orodje za identifikacijo in zmanjševanje tveganj na področju varstva osebnih podatkov. DPIA predstavlja orodje znotraj širšega procesa, ki ga je za potrebe projekta prenove informacijske podpore potrebno definirati za zagotavljanje rednega izvajanja ocene učinka.

DPIA je analiza, ki se izvaja v štirih fazah:

- Pregled področne interne in zunanje regulative
- Zbiranje informacij
- Analiza zbranih informacij.
- Poročilo o analizi.

Zbiranje informacij poteka v obliki razgovorov med izvajalcem DPIA in ključnimi izvajalci poslovnih procesov. Rezultati analize so ugotovitve o stanju in opredelitve tveganj v povezavi z osebnimi podatki. Rezultati so predstavljeni v zaključnem poročilu, vsebujejo interpretacije in priporočila za zmanjševanje tveganj. Poleg vseh zbranih informacij, ugotovitev in priporočil vsebuje zaključno poročilo tudi povzetek za poslovodstvo in povzetke.

Zakoniti interes – LIA

Zakoniti interes je ena izmed šestih pravnih podlag za obdelavo osebnih podatkov. Izmed vseh pravnih podlag je najbolj prilagodljiva, vendar ni vedno najbolj ustrezna. Najbolj primerno je, če se uporabi podatke o posameznikih na načine, ki bi jih le-ti razumno pričakovali in ki imajo minimalen vpliv na zasebnost, ali kjer obstaja prepričljiva utemeljitev za obdelavo.

Če se podjetje odloči, da se bo zanašalo na zakoniti interes, prevzema dodatno odgovornost za upoštevanje in zaščito pravic in svoboščin posameznikov. To pomeni, da mora podjetje izvesti oceno upravičenosti zakonitega interesa (Legitimate interes assessment - LIA) kot pravno podlago za obdelavo osebnih podatkov.

V sklopu izvedbe LIA mora podjetje opredeliti tri ključne elemente, ki jih mora upoštevati:

- Opredelitev interesa, kjer se definira ali gre za interes podjetja ali tretjih oseb. To lahko vključuje poslovni interes, individualni interes ali širšo družbeno korist.
- Potrebnost obdelave za doseganje interesa (namena), kjer podjetje dokaže da ne more enakega rezultata doseči na drug, manj vsiljiv način.
- Podjetje mora svoje interese uravnotežiti z interesi (pravicami in svoboščinami) posameznika.

V kolikor želite pri svojem poslovanju obdelovati osebne podatke, za katere nimate pravne podlage v zakonu, pogodbi ali privolitvi posameznika, izvedete oceno upravičenosti zakonitega interesa – LIA.

Rezultat izvedene LIA-e vam poda seznam ukrepov, ki jih je potrebno uvesti za ustrezno in zakonito obdelavo osebnih podatkov in s tem ustrezno obvladovanje tveganj na področju zagotavljanja pravic in svoboščin posameznika. Dokumentiranost ocene upravičenosti zakonitega interesa (LIA), pa vam bo pomagala dokazati skladnost.

[1] Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679.

[2] Ta delovna skupina je bila ustanovljena na podlagi člena 29 Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Njene naloge so opisane v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES. ■



Avtor: Dalibor Vukovič / Institut za korporativne varnostne študije*



POSLOVNA OBVEŠČEVALNA DEJAVNOST

Vsi, ki se kakorkoli ukvarjamo z varnostjo vemo, da je ta za uspešno delovanje korporacij zelo pomembna. Kvalitetna varnostna politika in razvijanje varnostne kulture sta temelj delovanja vseh resorjev. Poleg fizičnega in tehničnega varovanja, ki sta že dolgo nazaj postala osnovni standard, dajemo velik pomen varovanju intelektualne lastnine, osebnih podatkov, poslovnih skrivnosti, informacijskega sistema, varovanju ugleda družbe in še bi lahko naštevali. Hkrati pa si seveda želimo pridobiti čim več informacij o delovanju konkurence.

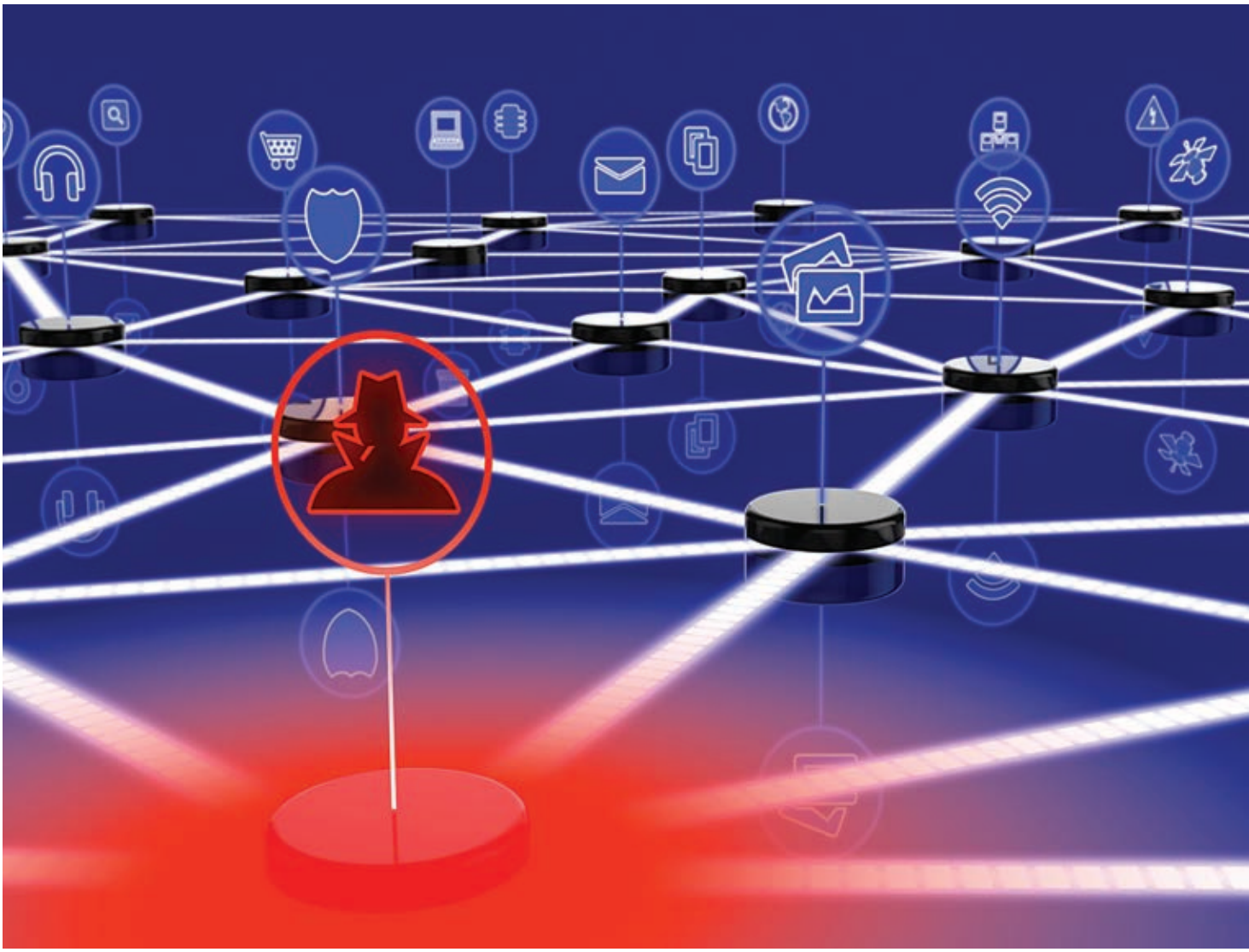
Zakaj uporabljati poslovno obveščevalno dejavnost?

Če v članek, ki ga trenutno berete, vključim misel Francisa Bacona: »*Vedeti več pomeni imeti moč*«, bi s tem povedal, da je uspešno delovanje korporacij zelo odvisno od pravočasnih in točnih informacij. V času globalizacije, ko je svetovno gospodarstvo v procesu nenehnih sprememb, tekmovalnost pa ima na vseh področjih veliko vlogo, je še posebej izrazit boj med korporacijami in multinacionalkami, saj te za svoj obstoj potrebujejo konkurenčno intelektualno lastnino, artikel ali storitev. Najuspešnejša podjetja morajo biti hitrejša v realizaciji idej, v investiranju, v vstopu na nova tržišča, osredotočena morajo biti na inovacije in na najvišji tehnološki nivo. Zato v strahu pred zaostankom za konkurenco uporabljajo najrazličnejše metode, ki bi jim pripomogle na poti k vrhu. Od vrha jih loči le prava informacija v pravem trenutku. Pri pridobivanju informacij, pa je vse bolj pogosta tudi obveščevalna dejavnost, ki je sicer širok pojem, vendar pa v vsakem primeru definira načrtovanje, zbiranje, obdelavo in analizo podatkov, z namenom pridobivanja želenih informacij, ki bi pomenile prednost pred ostalimi korporacijami. Podatki, ki jih v poslovni obveščevalni dejavnosti pridobivamo, prihajajo iz odprtih virov in so javno dostopni (OSINT), ni pa do njih vedno enostavno priti.



Podatki, ki jih v poslovni obveščevalni dejavnosti pridobivamo, prihajajo iz odprtih virov in so javno dostopni (OSINT), ni pa do njih vedno enostavno priti.

*avtor je član Slovenskega združenja korporativne varnosti



Temeljna razlika med tradicionalno in poslovno obveščevalno dejavnostjo

Čeprav zna izraz »obveščevalna dejavnost« včasih imeti negativno konotacijo in ga širša javnost povezuje s tradicionalno obveščevalno dejavnostjo v državnih in vojaških institucijah, pa se poslovna od tradicionalne v nekaterih segmentih vseeno razlikuje.

Obveščevalni ciklus, ki je glavni proces obveščevalne dejavnosti, je enak ali zelo podoben kot pri tradicionalni obveščevalni dejavnosti (poznamo sicer več modelov) in vsebuje vsaj osnovne štiri faze:

- Načrtovanje - v tej fazi izdelamo osnovni načrt obveščevalnega ciklusa.
- Zbiranje - v tej fazi pridobimo čim več potrebnih podatkov.
- Analiza – je najpomembnejša faza, s katero podatke spremenimo v smiselno informacijo.
- Posredovanje – ali zaključna faza, ko analizirano in sestavljeno poročilo predamo v uporabo.



Osnovne faze obveščevalnega ciklusa

Najpomembnejša razlika pa se veže na pooblastila, ki so v poslovni obveščevalni dejavnosti nižja, saj v postopkih ne smemo uporabljati nobenih prikritih metod poizvedovanja oz. pridobivanja podatkov. Vse podatke pridobivamo iz javno dostopnih virov, člankov, javnih avdio in video zapisov ter s pogovori z osebami, ki z nami želijo deliti svoje mnenje.

Na srečo je več kot 90 % informacij javno dostopnih in jih je možno dobiti z uporabo številnih enostavnih metod (internet, časopisi, revije, TV, radijski sprejemniki, kliping storitve, geo lokacija,...), okoli 5 % podatkov je sicer javnih, a je do njih težko priti in ravno ti imajo največjo vrednost, zato za njihovo pridobitev uporabljamo napredne oz. namenske računalniške programe. Strateški oz. najpomembnejši podatki pa se po navadi skrivajo v 1 % in nam niso dostopni oziroma bi s pridobivanjem teh kršili zakonodajo.

V poslovni obveščevalni dejavnosti dostopamo do podatkov v ti. zeleni in rumeni coni, kamor spadajo odprte informacije. Izjemoma uporabljamo tudi rdečo cono, kjer so taktične informacije, ki so zelo težko dostopne, a niso izrecno prepovedane. Poznamo še črno cono, kjer gre za zaupne informacije in pridobivanje predstavlja kršenje kazenske in gospodarske zakonodaje. To pridobivanje je izključno v domeni vladnih služb s soglasjem sodišča oz. tožilstva.

Kibernetski prostor - največji vir obveščevalnih podatkov

Glede na razvoj informacijske tehnologije in interneta v večini procesov uporabljamo napredne informacijske metode, opremo in programska orodja. Dejansko lahko večino podatkov pridobimo iz pisarne. Če bi postopek opisali tako kot so to storili v *Economic intelligence leta 2002,* bi to bilo videti tako:

- Dobimo ali definiramo cilj trenutne dejavnosti
- Opredelimo vire informacij
- Zbiramo informacije
- Analiziramo pridobljene informacije
- Predstavimo obdelane informacije
- Poročamo

V celotnem procesu je najpomembnejše, da s pomočjo kvalitetnih analitičnih metod na koncu ponudimo razumevanje situacije in ne zgolj novice o situaciji. Na tak način lahko uporabnik na podlagi prejetega poročila sprejema odločitve.

Do tega pa pridemo le, če imamo urejene podatkovne baze, kvalitetne programe za podatkovno rudarjenje in indeksirane dostope do preteklih informacij.

V zadnjih letih je obveščevalna skupnost zelo napredovala in ima na razpolago cel kup uporabnih spletnih in programskih orodij. Ne glede na vse, pa sta najbolj pomembna znanje in izkušnje uporabnikov le teh.





V celotnem procesu je najpomembnejše, da s pomočjo kvalitetnih analitičnih metod na koncu ponudimo razumevanje situacije in ne zgolj novice o situaciji. Na tak način lahko uporabnik na podlagi prejetega poročila sprejema odločitve.

Najbolj uporabljana orodja za pridobivanje OSINT podatkov

Za uporabo informacijskih orodij je seveda treba imeti specifično računalniško znanje in povprečnemu uporabniku spleta ne bodo koristila, nikakor pa ni odveč, če jih nekaj predstavimo:

Uporabni spletni iskalniki: Yandex, Duck Duck Go, Baidu, Ask, Exalead, Google, Bing.
Digitalni arhiv svetovnega spleta: Wayback machine.
OSINT orodja: Check Usernames, Tineye, Searchcode, Shodan, Maltego, Metagoofil, The Harvester,...
Orodje za hrambo podatkov in izvajanje analiz: MicroStrategy.

Zaključek

Z globalizacijo in razvojem informacijske tehnologije javni viri prevladujejo pri pripravi obveščevalnih informacij. Zagotovo pa je strokovno znanje tisto, ki je ključno pri sestavi končnega produkta obveščevalnega procesa.

Uspešne korporacije intenzivno koristijo tehnična orodja za pridobivanje, analizo in uporabo konkurenčnih informacij, saj te strateškemu managementu omogočajo opazovanje notranjega in zunanjega organizacijskega okolja, oblikovanje strategij, uspešen vstop na nove trge ter jih pozicionirajo pred neposredne in tudi potencialne konkurente.

Rekli bi, da razumejo uvodno misel »*Vedeti več pomeni imeti moč*«. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Upravljanje s tveganji in korporativna varnost

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

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

Zakaj Upravljanje s tveganji in korporativna varnost?

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

Komu je študij namenjen?

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



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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



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

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

Predmetnik

I. LETNIK

Skupni obvezni predmeti

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

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

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

Smer Korporativni varnostni manager – podjetnik

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

Izbirni predmeti (študent izbere dva):

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

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

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

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

CENTER VIŠJIH ŠOL

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

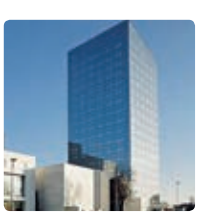
FAKULTETA ZA PODJETNIŠTVO

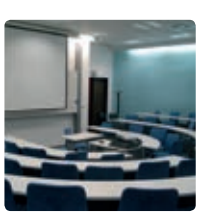
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

POSLOVNO-IZOBRAŽEVALNI CENTER

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





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

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo


Prenašamo
energijo,
ohranjamo
ravnovesje.
WWW.ELES.SI
ELES