Korporativna varnost

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

Letnik 2022, marec • št. 28



Tradicionalna 13. mednarodna konferenca »Dnevi korporativne varnosti 2022«

Brdo pri Kranju, 31. maj - 1. junij 2022

Putinova vojna in evropski mir

Veleposlanik Vojko Volk



VAŠA 360° VARNOST 365 DNI V LETU

MODRO JE IZBRATI OPERATIVNI CENTER KIBERNETSKE VARNOSTI

360° varnost vam zagotavlja **najsodobnejšo kibernetsko zaščito**. Na mobilni, stacionarni, oblačni in lastni infrastrukturi, ki je lahko tarča kibernetskega napada ali zlorabe. Zaradi vedno večje kompleksnosti kibernetskega okolja in varnostnih groženj brez kibernetske varnosti digitalni razvoj ni mogoč. Človekova zmožnost uvida v dogodke in povezovanje informacij pa je kljub vsej tehnologiji nepogrešljiva. Zato naj za vas vse dni in noči skrbijo naši **strokovnjaki Operativnega centra kibernetske varnosti (OCKV)**, ki ves čas spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske napade.

Ob morebitnem kibernetskem napadu vam zagotovijo omejitev napada in zmanjševanje škode, zbiranje in zavarovanje dokazov, zagotavljajo revizijsko sled in vas sproti seznanijo s pomembnimi dogajanji, ki jih zaznajo. OCKV Telekoma Slovenije je certificiran **po mednarodnem standardu za informacijsko varnost ISO 27001**, ob tem pa ima Telekom Slovenije tudi **certifikat za neprekinjeno poslovanje ISO 22301**. Naše storitve s področja 360° varnosti so tako primerne za podjetja vseh velikosti, saj OCKV za vsakogar poišče ustrezne rešitve.

telekom.si/poslovni

TelekomSlovenije

Za več informacij o prodajni ponudbi obiščite www.telekom.si ali pokličite 080 70 70. Telekom Slovenije, d.d., Ljubljana.



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:
tiskano v Sloveniji

Datum izida:
marec 2022

Izvod revije je brezplačen

Naslovnica in slike:
ID 136191118 © Alexandersikov | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

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

Obdobje, v katerem se trenutno nahajamo, je vsekakor močno obremenila kriza v Ukrajini, ki je dokončno razgalila vse geostrateške izzive post globalizacijskega sveta. Verjetno si do nedavnega ni bilo možno resno zamisliti velikega oborožen spopada na območju Evrope z vsemi dodatnimi implikacijami, ki so dvignile napetosti do te mere, da se resno analizira vse nadaljnje korake, ki bi lahko pripeljali celo do neobvladljivega svetovnega spopada. Vojaška agresija Ruske federacije na suvereno državo Ukrajino je, poleg vojaških, odprla tudi druge implikacije, ki imajo zelo pomemben vidik za države EU, vključno s Slovenijo. Tveganja in grožnje so se močno povečale tudi v kibernetskem prostoru, kjer se kaže neposredna ogroženost za neprekinjeno delovanje kritične infrastrukture in drugih bistvenih storitev pomembnih za funkcioniranje moderne družbe. Moderna, na digitalizacijskih procesih temelječa družba, je še posebej ranljiva ravno na tveganja, ki prihajajo iz kibernetskega okolja. Zveza NATO je jasno sporočila, da bodo tudi dejanja, ki bodo imela vzrok v obliki kibernetskih napadov na infrastrukturo in na storitve držav članic, smatrana za neposredno sovražno dejanje in napad na posamezno članico. V racionalnem pristopu, če ga je v trenutni situaciji še kaj ostalo, ni pričakovati neposrednega izzivanja konfliktov med velesilami. Bolj pa nas lahko skrbijo akterji, ki niso pod neposrednim vplivom držav vpetih v ta konflikt.

Ne glede na trenutne ocene in strateška pričakovanja moramo v lastnih organizacijah narediti največ, kar je v dani situaciji mogoče, da zagotovimo varnost in neprekinjenost delovanja. V vsaki krizni situaciji pa je vedno potrebno izluščiti pozitivne vidike, ki se v tem trenutku odražajo še v večji potrebnosti in prepoznavnosti delovanja subjektov, ki skrbijo za korporativno varnost v organizacijah. V teh trenutkih je potrebno dokazati vso strokovnost in sposobnost za zagotavljanje obvladljivosti dejavnikov tveganja, ki bodo zagotovili nemotenost izvajanja poslovnih procesov. Strateško vodstvo danes, bolj kot kadarkoli potrebuje to oporo, da bodo lahko poleg procesov, ki so nujni za nadaljevanje digitalne transformacije, izvedli tudi učinkovite korake za izhod iz poslovne krize, ki jo je prinesla omenjena situacija. V takih trenutkih pa prihaja še bolj do izraza neposredno strokovno združevanje in izvajanje usklajenih skupnih strokovnih korakov, ki jih stroka izvaja v okviru Slovenskega združenja za korporativno varnost.

Ravno zaradi tega, smo v tokratni številki revije želeli vsebinsko osvetliti dovolj širok spekter strokovnih prispevkov, da v tem okviru prenesemo določene nove vidike in izkušnje tudi na področja, ki jih prinaša uvajanje novih pristopov in tehnologij. Posebej bi želel izpostaviti strateško geopolitično oceno, ki jo tudi tokrat prinaša kolumna. Izkoristili smo priložnost in se pogovorili s pomembnimi strateškimi voditelji in strokovnjaki z različnih področij, ki so z nami delili svoje izkušnje in strateške poglede.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
mag. Valentin Hajdinjak, predsednik uprave DARS d.d.
mag. Anton Travner, svetovalec uprave in po pooblastilu vodja službe za korporativno varnost

DARS PREDSTAVLJA POMEMBNO INFRASTRUKTURNO HRBTENICO NA PODROČJU CESTNEGA TRANSPORTNEGA SEKTORJA

14



INTERVJU
dr. Uroš Svete, direktor Urada za informacijsko varnost

POMEMBNA JE VZPOSTAVITEV USTREZNEGA EKOSISTEMA KIBERNETSKE VARNOSTI

20



INTERVJU
mag. Jože Knavs, zastopnik družbe Informatika d.o.o.

DIGITALIZACIJA V ELEKTROENERGETIKI POSTAJA REALNA POTREBA

26



INTERVJU
Gregor Janc, direktor Korporativne varnosti v Telekomu Slovenije

KORPORATIVNA VARNOST NUJEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE

30



INTERVJU
Thomas Tomsich, direktor Zarja Elektronika d.o.o.

PODROČJE TEHNIČNEGA VAROVANJA IMA ŠE VEDNO POMEMBNO MESTO V SISTEMU INTEGRALNE VARNOSTNE ZAŠČITE

34

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

INTERVJU
Blaž Košorok, državni sekretar na Ministrstvu za infrastrukturo*

STRATEŠKI VARNOSTNI IZZIVI ENERGETIKE V PRIHODNJEM OBDOBJU

G. Blaž Košorok, državni sekretar na Ministrstvu za infrastrukturo je v pogovoru z nami analiziral stanje in izzive na področju razvoja energetike v Republiki Sloveniji. V pogovoru je med drugim posebno težišče namenil ukrepom, ki jih bo v prihodnosti potrebno narediti za povečanje razumevanja varnosti delovanja ključnih infrastrukturnih sektorjev v državi. Nismo se mogli izogniti tudi pogovoru o najbolj aktualni temi, ki jo predstavlja vojaška agresija Ruske federacije na suvereno državo Ukrajino.

Obdobje zdravstvene krize je med drugim prineslo tudi večje zavedanje o pomenu neprekinjenega delovanja energetske kritične infrastrukture. So po vašem mnenju procesi zagotavljanja neprekinjenosti delovanja energetske infrastrukture v Sloveniji ustrezno delovali?

Kar se je pokazalo že čisto na začetku, s prvim valom epidemije marca/aprila 2020, ko smo bili soočeni s to krizo, je slovenska energetika kot celota, od proizvodnje, distribucije in seveda tudi prenosa odreagirala zelo ustrezno. To kaže na to, da v energetiki obstaja neka dolgoletna tradicija zavedanja ključnih ljudi, ki v tej piramidi delujejo že vrsto let. Kar se tiče prenosa je Eles med prvimi sprejel zelo drastične ukrepe. Kasneje so sledili tudi vsi ostali distributerji, tako za elektriko, kot za zemeljski plin. To se je v praksi odrazilo tako, da v nadzornih centrih pri ključih ekipah praktično ni bilo prisotnosti virusa. Sploh v tem prvem obdobju so bili ključni kadri, ki so skrbeli za obratovanje sistema popolnoma izolirani od zunanjega sveta in so se menjavali na predvidene časovne intervale. Sistem je deloval, in menim, da kar se tega tiče je bil odziv pravilen. Na ministrstvu smo bili v rednih stikih z njimi, ne samo s kritično infrastrukturo energetike, ampak tudi transporta, in mislim, da smo dovolj dobro odreagirali, kar se je tudi odrazilo v neprekinjenosti delovanja sistema.

> Marsikaj je bilo sprejeto v času slovenskega predsedovanja, tudi potrditev direktive NIS2 ”Network and Information Security”, ki je bila potrjena na Svetu EU, kar beležimo za neke vrste uspeh. S tem trenutna vlada kaže na to, da je področje kibernetske varnosti še kako pomembno.

V zadnjem obdobju smo vedno pogosteje priča opozorilom strokovne javnosti, da bo Slovenija potrebovala ustrezno robusten sistem zagotavljanja električne energije. Kateri so po vaši oceni tisti koraki, ki bi bili ustrezni za zagotovitev dodatnih zmogljivosti za proizvodnjo nujno potrebne električne energije?

Izhajati moramo iz »ustave« slovenske energetike, ki jo predvideva nacionalni energetski in podnebni načrt (NEPN). Tam so zapisani cilji, ki so podobni kot pri drugih državah članicah EU. Zavedati pa se je potrebno, da mi nismo samo člani EU, ampak smo tudi člani Energetske unije. Imamo dolo-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Veljava združenja pa se odraža tudi v dejstvu, da so v to asociacijo vključena vsa največja slovenska podjetja, še posebej tista, ki upravljajo ključno infrastrukturo. Menim, da je ta izmenjava informacij in širjenje dobrih praks zagotovo prava pot tudi vnaprej.

čene pravice in določene obveznosti. Fokus je na robustnem delovanju, če pa želimo zagotavljati to robustno delovanje elektro energetskega sistema, potrebujemo najprej stabilno in robustno proizvodnjo električne energije. V Sloveniji v tem trenutku temeljimo na 1/3 termo proizvodnje, 1/3 hidro proizvodnje oz. obnovljivih virov energije in 1/3 jedrske energije. Soočeni smo z zunanjimi dejavniki in to je potreba, da se fosilni viri umikajo in želimo biti do leta 2050 ogljično nevtralni, ali pa vsaj zmanjšati ogljični vtis praktično na nič. S celim nizom ukrepov, tudi v času našega predsedovanja, je bilo objavljenih kar nekaj zakonodajnih paketov na tem področju. Skoraj 2/3 teh ukrepov je vezanih na naše ministrstvo in je posebej usmerjeno v sektorja energije in transporta. Pred nekaj meseci je bila sprejeta strategija o odstopu od premoga, kot energetskega vira. S tem torej zgubimo 1/3 zanesljivega vira energije. Ključna dilema je kako to nadomestiti. Odgovor je seveda s povečanjem obnovljivih virov energije, kot so sončna, vetrna ali hidro energija. Ne smemo pa pozabiti tudi na geotermijo in pa seveda priložnost za drugi blok nuklearne elektrarne. Slovenija je in bo ostala jedrska država. Dejstvo je, da zadnjih 40 let jedrska elektrarna Krško odlično deluje in predstavlja stabilen in zanesljiv vir energije. Vedno pa se pojavljajo dileme, kako en vir nadomeščati z drugim. V tem okviru nikakor ne smemo pozabiti na priložnosti za distribucijo električne energije, torej na elektro distributerje, na katerih se bo gradila ključna hrbtenica prehoda na nizko ogljično prihodnost. To pomeni, da moramo distribucijski nizko in srednje napetostni sistem okrepiti. V tem kontekstu pa ne smemo pozabiti na Eles, kot sistemskega operaterja, ki pa že kar napredno vlaga in črpa evropska sredstva za razvoj tega področja.

Digitalizacija in uvajanje v zeleno usmerjene vire pridobivanja električne energije tudi v energetskem sektorju prinaša vedno večjo razpršenost omrežja. Kako obvladovati vedno večjo kompleksnost tega omrežja v luči, da elektro energetski sistem nujno temelji na uravnoteženosti?

V luči zadnjih dogodkov je veliko vprašanje kako najti razmerje med tem, da bo cena, ki jo poznamo danes, še vedno takšna kakršne smo bili navajeni. Menim, da bo potrebna popolna paradigma razmisleka, kje smo in kam gremo. Pred našimi očmi se geopolitične strateške povezave spreminjajo, kar se seveda odraža na trgu z energenti. Trenutno si težko predstavljamo kakšne drastične spremembe so bodo zgodile na trgu z elektriko, zemeljskim plinom in na trgu z naftnimi derivati. Težko ocenimo kako se bo ta transformacija trga končala in kakšno bo novo stanje. Če smo še pred tremi meseci napovedovali, da če bo zima kratka in mila se bodo cene energentov umirile ali padle. Sicer so se kazali znaki možnega konflikta, ki ga je napovedovala Rusija, vendar ni nihče predvidel tako drastičnega konflikta, ki se je kasneje sprevrgel v agresijo. Ta ge-

opolitična sprememba, ki jo prinaša ruska vojaška agresija v Ukrajini postavlja zadeve na popolnoma nove temelje, ki so posebej za področje zagotavljanja energetske oskrbe EU, zelo zahtevne.

Ravno ti procesi prinašajo tudi vedno večjo potrebo po ustrezni zagotovitvi informacijske varnosti v organizacijah elektro energetskega sektorja. Kateri strateški koraki so bili narejeni v mandatu trenutne vlade, ki utrjujejo zavedanje o potrebnosti učinkovitih sistemov zagotavljanja informacijske varnosti v energetiki?

Vlada si je za eno od treh točk predsedovanja v Svetu EU zadala tudi kibernetsko varnost. Marsikaj je bilo sprejeto za časa slovenskega predsedovanja, tudi Uredba o informacijski varnosti, kar beležimo za neke vrste uspeh. S tem trenutna vlada kaže na to, da je področje kibernetske varnosti še kako pomembno. Pravilnost izbire teh težišč poudarjanja potrebe po ustreznem sistemu kibernetske varnosti se kaže tudi v trenutnem konfliktu v Ukrajini. Vsakodnevno smo s strani Ruske federacije, pa tudi s Kitajske, priča določenim tveganjem in napadom v kibernetskem okolju. Marsikdo zamahne z roko in temu ne posveča prav velike pozornosti, na našem ministrstvu pa je želja, da skušamo zadeve ustrezno poenotiti in sistemsko urediti. Nenazadnje je tudi želja SDH, ki se pojavlja kot upravljalec premoženja, da skozi različne vzvode zagotovi poenotenje procesov in virov na področju zagotavljanja kibernetske varnosti. Če pogledamo konkretno v energetiko, je potreben skupen napor po usklajenosti in enovitosti sistema zagotavljanja kibernetske varnosti, pa naj si gre za področje elektro distributerjev, prenosa ali proizvodnje. Nujno potrebujemo skupen in dobro delujoč sistem zagotavljanja kibernetske varnosti.

Ta centralizacija upravljanja s kibernetsko varnostjo je verjetno eden od strateških ciljev?

Zagotovo. Nenazadnje tudi vzpostavitev Uprave za informacijsko varnost kaže na to potrebo po centralizaciji upravljanja s temi procesi. Na žalost nas varnostno izpostavljeni dogodki, kot je trenutno ruska vojaška agresija v Ukrajini, še dodatno opominjajo o tej potrebi. Postajamo ranljivi, ne samo na informacijskem področju, ampak tudi na fizičnem. Vedno pogostejša so poročila o višjih stopnjah tveganja, kot smo jih poznali prej.

Katera so tista težišča katerim bo v energetiki namenjeno največ pozornosti, ko govorimo o sredstvih iz sklada za okrevanje?

Eno je sklad za načrt za okrevanje in odpornost, kjer je bilo posebej prepoznano, da moramo krepiti distribucijski sistem. Kot sem že prej omenil je tukaj posebej izpostavljen pomen razvoja srednje in nizko napetostnega omrežja. Na drugi strani pa ne želimo pozabiti na pomen razvoja transporta. Načrtno želimo iti v neko brezogljično oz. nizkoogljično prihodnost in ravno tukaj je transportni sektor za Slovenijo eden od največjih izzivov. Slovenija je kar se tega tiče zelo pretočna država, veliko transporta gre čez našo državo in tukaj se pojavlja priložnost, hkrati pa tudi tveganje, kako bomo dosegli vse zastavljene cilje za zmanjšanje izpustov in na drugi strani povečanje za obnovljive vire energije. Ravno zaradi tega je poseben poudarek namenjen železniškemu transportu. Glavni izziv je kako javni potniški promet narediti bolj atraktiven, in tako skozi načrt za okrevanje in odpornost pridobiti kar velik del sredstev. Če pa pogledamo sektor energetike, pa bo fokus predvsem v razvoj obnovljivih virov energije, in sicer v vseh segmentih od sončne do vetrne energije. Ne smemo pa pozabiti, da smo





pred novo finančno perspektivo, torej za obdobje 2022-2027 in tudi tukaj velik del pozornosti namenjamo proizvodnji obnovljivih virov, učinkoviti rabi energije in zavzemanju, da čim več prometa spravimo s cest na železnice ali pa na javni potniški promet.

V najinem pogovoru se nikakor ne moremo izogniti krizi v Ukrajini. Kakšne vplive pričakujete na področju zagotavljanja energentov v Sloveniji?

Sedaj imamo možnost dnevnega spremljanja posledic, ki jih prinaša vojaška agresija Ruske federacije na suvereno državo Ukrajino. Ukrajinska stran ima že vrsto let prošnjo, da bi se vključila v evropsko elektro energetsko omrežje, zdaj se je ta proces še intenziviral. Seveda so to podprle vse države članice. Vendar se je potrebno zavedati določenih tveganj, ki jih je glede na razvoj dogodkov V Ukrajini v tem trenutku nemogoče predvideti. O teh stvareh je potrebno izvesti tehtni premislek, kako in na kakšen način se bo ta energija, iz ali pa v Ukrajino, transportirala. To vprašanje v strokovnih okoljih intenzivno pregledujemo že zadnjih štirinajst dni. Ukrepi, ki bodo sledili na področju prepovedi uvoza energentov iz Rusije, predstavljajo tudi velik izziv. V tem okviru sta posebej izpostavljena zemeljski plin in nafta, ki prihajata iz Ruske federacije. Energetska odvisnost Slovenije od te dobavne verige je zelo visoka. V tem okviru zelo intenzivno potekajo pogovori, analize in koordinacija kako se ustrezno prilagoditi situaciji, ki bo sledila določenim političnim odločitvam. V Slovenijo zemeljski plin doteka in odteka po treh glavnih dobavnih smereh. Tudi po prenehanju vojnih aktivnosti menim, da se bo svet korenito spremenil. To pomeni, da bo prihodnji strateški cilj Evropske unije, da bistveno zmanjša svojo energetsko odvisnost od Rusije. To bo pomembno energetsko presečišče prihodnjih strateških aktivnosti.

V zadnjem obdobju ste na ministrstvu zelo aktivno podpirali prijave slovenskih partnerjev na EU raziskovalne projekte na področju zaščite kritične infrastrukture. Kakšna so vaša pričakovanja od rezultatov teh projektov, kjer imajo slovenski infrastrukturni in raziskovalni partnerji pomembne vloge?

Po pregledu teh prijav oziroma samih projektov mislim, da je prioriteta takšne stvari podpirati tudi v naprej. Nasploh velja izpostaviti raziskovalne projekte, ki se znajo potem zelo dobro implementirati v praksi. Nekaj teh projektov že uspešno poteka, saj ne nazadnje tudi vaš Institut za korporativne varnostne študije pri tem uspešno sodeluje. Lahko z lahkim srcem rečem, da takšne projekte podpiramo in jih bomo tudi v prihodnje. Želimo ustvariti spodbudno okolje, ki bi omogočilo, da se pojavi še več podobnih projektov in s tem zagotovi tudi učinkovito črpanje evropskih sredstev.

V zadnjem obdobju je bilo vaše ministrstvo zelo aktivno tudi v Slovenskem združenju za korporativno varnost, kamor ste se vključili pred letom dni? Je delovanje v omenjeni asociaciji doseglo vaša pričakovanja?

Zagotovo. To združenje pridobiva na veljavnosti, ne nazadnje sploh zdaj ob zadnjih dogodkih. Tudi iz medijev lahko razberemo, da ste postali neprecenljivi sogovorniki, ko govorimo o zaščiti kritične infrastrukture in kibernetski varnosti. Veljava združenja pa se odraža tudi v dejstvu, da so v to asociacijo vključena vsa največja slovenska podjetja, še posebej tista, ki upravljajo ključno infrastrukturo. Menim, da je ta izmenjava informacij in širjenje dobrih praks zagotovo prava pot tudi vnaprej. Tako, da upam, da se vam bo združenje tudi v prihodnje razvijalo in imelo še pomembnejšo vlogo pri dvigovanju varnostnega zavedanja in sistemskem pristopu pri zagotavljanju obvladovanja varnostnih tveganj. ■

Avtor: Vojko Volk / veleposlanik



KOLUMNA

PUTINOVA VOJNA IN EVROPSKI MIR

„Trditev, da so se ekonomije avtoritarnih družb v času krize Covid-19 obnesle bolje kot ekonomije demokratičnih družb, se je sesula v prah“

/Paul Krugman, Nobelov nagrajenec za ekonomijo/

Ruski predsednik Putin je ves čas prepričeval ves svet, da se bo NATO razširil na Ukrajino pa čeprav ta povsem obubožana država za to ni imela nobenih možnosti, ni izpolnjevala niti temeljnih pogojev in je bil njen vstop v NATO zavrnjen že leta 2008. Da je bil NATO samo izgovor je priznal sam Putin, ko je razglasil, da je cilj njegove invazije „demilitarizacija in denacifikacija Ukrajine“. Nazadnje se je na Ukrajino razširila Rusija. In to brutalno, z vojaško silo in enormno premočjo, ne oziraje se na temeljna načela mednarodnih odnosov in mednarodnega prava, ne oziraje se na dejstvo, da je mesto za reševanje sporov med sosedi v Organizaciji združenih narodov in ne glede na strahotne posledice, ki jih bodo zahodne sankcije imele, na že tako nizek življenjski standard ruskega prebivalstva. V prostranih za karpatskih stepah so ljudje komajda pozabili na zločine in stradanja, ko je od lakote pomrlo na milijone Ukrajincev, že so znova v vojni in znova jim grozijo nasilje, smrt in lakota. Zakaj že? Ker predsednik Putin pravi, da Rusija kot daleč največja država sveta za svojo varnost potrebuje še dodatna ozemlja, pa čeprav niti tistega, ki ga ima, sploh ne obvladuje. Na vzhodu si je obširne dele Rusije že de facto prisvojilo prebivalstvo kitajskih zahodnih in severnih provinc, medtem ko Rusi postajajo manjšina v lastni državi. Putin je s prstom kazal na NATO in zahod, potem pa sam izvedel bliskovit napad na Ukrajino in prevaral ves svet. Opravičevalci Putinovega napada na Ukrajino so s svojimi zgodovinskimi in ideološkimi opravičevanji Putinove blaznosti prestopili vse črte moralnega delovanja in predvsem zdravega razuma. Kadar človek opravičuje razloge Goljata, da zatolče Davida, je meja prestopljena in človek se vrne k živali, kjer vlada zakon močnejšega. Ko je nori srbski vožd Milošević 25. junija 1991 organiziral napad jugoslovanske vojske na Slovenijo, je imel natanko iste načrte, kot zdaj Putin v Ukrajini. V dveh dneh naj bi zastrašujoča sila letal, tankov in raket prestrašila slovensko ljudstvo, aretirali bi slovensko vodstvo in že tretji dan instalirali marionetno, pro-srbsko oblast v Sloveniji. Pa se ni izšlo, kako se je končalo vemo vsi.

Največja krivda, ki jo ima pri vsem skupaj Evropa, je bila naša naivnost in verovanje, da sta stabilnost in mir v Evropi dana sama po sebi in da sta zaščita okolja in globalno segrevanje največji problem sveta. Zdaj je že v prvem tednu vojne v Ukrajini nastala večja ekološka škoda, kot v desetletju pred tem. Čez noč nam je postalo jasno, da obstajajo večji problemi, v prvi vrsti naša varnost, predvsem pa, da problemi Evrope niso tudi problemi Rusije in Putina. V času vladavine ameriškega predsednika Trumpa smo dovolili, da je Trump sistematično podiral vse, kar so ZDA in EU pred tem desetletja gradile za mir in za svet brez jedrskega orožja, od sporazumov z Rusijo do sporazuma z Iranom. Novi predsednik Biden se je znašel na čistini, v kateri je najprej poskrbel za svoj položaj in potem s paničnim pobegom iz Afganistana storil še strateško napako. V EU smo bili šokirani nad ameriškim begom in prepustitvijo ljudi srednjeveškemu režimu talibanov, Putin pa je ta beg pravilno razumel kot šibkost ZDA. EU ni nič dosegla v Siriji niti v Libiji, do kriznih žarišč smo se obnašali neodločno. Putin pa je ocenil, da je zahod

Največja krivda, ki jo ima pri vsem skupaj Evropa, je bila naša naivnost in verovanje, da sta stabilnost in mir v Evropi dana sama po sebi in da sta zaščita okolja in globalno segrevanje največji problem sveta.

Putinov napad na Ukrajino pa je enotnost EU in NATO dobesedno zabetoniral, celo tako močno, da se nam je z drastičnimi sankcijami pridružila še nevtralna Švica, česar ni storila nikoli v preteklosti in niti med drugo svetovno vojno.

šibak in lahko počne kar hoče. A zdaj se bo Putinova vojaška moč soočila z gospodarsko močjo zahoda in cena, ki jo bo plačal ruski narod bo ogromna. Če se bo Putin lotil atomskega orožja pa bo v zrak zletel ves svet.

Medtem, ko smo na zahodu zadnjih dvajset let razmišljali, kako bomo ohranili zdravo okolje, reševali naš planet in izvedli zeleno tehnološko revolucijo, je Putin razmišljal, kako bi Rusiji povrnil ozemlje nekdanjega sovjetskega imperija. Medtem, ko smo si v Evropi prizadevali za človekove pravice, demokracijo in vladavino prava, za enakopravnost žensk in njihov boljši položaj v družbi, za pravice vseh manjšin, se je ruski vladar boril za svojo osebno oblast in interese. Mašili smo si oči in ušesa pred vladarjem, ki nam je sporočal, da nas ne razume in nas vsako leto bolj odkrito prezira, sporočal nam je, da smo dekadentni zahod, ker dovoljujemo gay parade in ženskam splav s čimer, da uničujemo tradicionalne vrednote. A natanko tako je svoj upor proti dekadentni Evropi med obema vojnama utemeljil že Hitler v svojem Mein Kampf. Zaradi ljubega miru smo Putinu pogledali skoz prste, ko je napadel in priključil Krim, ko je moril ruske novinarje in oporečnike, ter po svetu zastrupljal svoje politične nasprotnike. Ceneni ruski plin nam je bil pomembnejši od spoštovanja temeljnih načel mednarodnega prava in zaščite človekovih pravic. Predvsem pa je Putin vedel, da bo za nas pomemben le še toliko časa, dokler bo Evropa odvisna od ruskega plina in nafte. In to je bilo zdaj. Ostale so mu samo še gola vojaška moč, atomske bombe in slab ducat zvestih oprod, ki mu lahko ugovarjajo samo za ceno svojih življenj. Zdaj skupaj z njimi igra z Evropo igro, ki se lahko konča s pogubo sveta.

Putinov napad na svetovno ureditev prihaja v trenutku, ko je po dveh letih pandemije Covid-19 postalo jasno, da bodo iz te krize v najboljši ekonomski formi izšle demokratične države zahoda, ki so se krize lotile tako, da so pomagale najprej ljudem in potem gospodarstvu. Danes so stopnje gospodarske rasti EU najvišje na svetu, medtem ko Kitajska ne zmore iz tunela recesije, Rusija pa nazaduje. Nobelov nagrajenec za ekonomijo Paul Krugman v svoji zadnji knjigi „Covid's Economic Mutations" na tej podlagi zavrača





poenostavljene ocene, ki so jih zadnja leta na zahodu širili populisti od Le Penove do Orbana, češ da so „avtoritarni režimi gospodarsko uspešnejši, ker so disciplinirani in bolje organizirani“. ZDA pa so po Krugmanu pri okrevanju manj uspešne zato, ker so po zadnjih volitvah notranje še vedno globoko razklane, politični razred pa ne zmore sprejeti zdaj že res nujno potrebnih reform. In seveda obratno, EU je uspel veliki razvojni met ravno zato, ker je v najhujši krizi po drugi svetovni vojni uspela doseči soglasje o Načrtu okrevanja za Evropo in investirati v lastno prihodnost. EU je dobesedno čez noč presenetila preostali svet in postala predmet zanimanja ekonomistov. Putinov napad na Ukrajino pa je enotnost EU in NATO dobesedno zabetoniral, celo tako močno, da se nam je z drastičnimi sankcijami pridružila še nevtralna Švica, česar ni storila nikoli v preteklosti in niti med drugo svetovno vojno.

Velika Kitajska, za katero je kazalo, da utegne biti vsaj posredno na strani Putina, pa je očitno presodila, da se ji to ne izplača. Putin je Peking obiskal 4. februarja in bržkone prosil vsaj za razumevanje pri napadu na Ukrajino, v zameno za nove plinske in naftne pogodbe ali pa morda celo ponudbo podpore za kitajski napad na Tajvan. A je pozabil, da Kitajska nima zaveznikov zato, ker jih ne potrebuje. Kitajska zdaj sedi na ograji in gleda, kako se bo iztekla Putinova vojna in kako bo vplivala na zahod. Komur bo bolje kazalo, tistemu se bo Kitajska priklonila. Medtem se posli med Kitajsko in zahodom že zdaj krepijo, saj Kitajska hiti zapolniti vrzel, ki nastaja po tem, ko je Rusija izključena iz svetovnih finančnih trgov in trgovinskih, zlasti surovinskih tokov.

Kitajska zdaj sedi na ograji in gleda, kako se bo iztekla Putinova vojna in kako bo vplivala na zahod.

Pred dvema letoma niti najbolj okoreli optimisti med Evropeisti niso verjeli, da se bo – zdaj že legendarna – kanclerka Merklova odpovedala svojim varčevalnim politikam in sprejela dolgoročno zadolževanje za nov razvojni ciklus Evrope. Škoda je samo, da Merklova ne vodi več Nemčije v trenutku, ko bi jo najbolj potrebovali. Bila je edini zahodni politik, ki je Putinovo kgb-jevsko nrav poznala do obisti in v njem zbujala spoštovanje in strah. Putinovo vojno lahko ustavi samo evropski mir. ■

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.

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

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

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.

www.ics-institut.si

Članstvo v združenju vam lahko olajša obvladovanje tveganj v vaših organizacijskih sredinah. SKUPAJ SMO MOČNEJŠI!

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih mesečnih strokovnih srečanjih,
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS,
- 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,
- 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.

CAA, URSIV, Melamin, tus, 30 SMART COM, Občina Slovenska Bistrica, telemach, SIEMENS, NIJZ Nacionalni inštitut za javno zdravje, Republika Slovenija Ministrstvo za pravosodje, Ministrstvo za infrastrukturo, Javni medobčinski stanovanjski sklad Maribor, GENERALI, SmartIS Pametni informacijski sistemi, Pošta Slovenije, Mestna občina Ljubljana, PETROL Energija za življenje, Telekom Slovenije, AKRAPOVIČ, interblock Luxury Gaming Products, triglav, Informacijske storitve in inženiring, d.o.o. INFORMATIKA, Elektro Ljubljana, SPICA, DARS, Elita i.b. d.o.o., ZARJA ELEKTRONIKA, UNISTAR PRO, NovaKBM, LON, CINKARNA, Slovenske železnice, energetika ljubljana

www.ics-institut.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
mag. Valentin Hajdinjak, predsednik uprave DARS d.d.*
mag. Anton Travner, svetovalec uprave in po pooblastilu vodja službe za korporativno varnost

DARS PREDSTAVLJA POMEMBNO INFRASTRUKTURNO HRBTENICO NA PODROČJU CESTNEGA TRANSPORTNEGA SEKTORJA

DARS je kot ključni upravljalec avtocestne infrastrukture soočen z veliko izzivi, ki sami po sebi zahtevajo sistemski pristop pri zagotavljanju neprekinjenosti delovanja te pomembne transportne infrastrukturne mreže. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Valentinom Hajdinjakom in mag. Antonom Travnerjem.

mag. Valentin Hajdinjak

V svoji karieri ste opravljali strateške funkcije v različnih organizacijskih okoljih. V zadnjem obdobju opravljate zahtevno funkcijo predsednika uprave DARS. Nam zaupate kje vidite glavne izzive, ki jih prinaša trenutna funkcija?

Družba DARS je v svojih skoraj treh desetletjih obstoja prehodila zelo dinamično pot. V zadnjem obdobju poleg gradbenika in vzdrževalca avtocest, krepimo tudi vlogo učinkovitega in aktivnega upravljalca avtocestnega sistema, kar nas postavlja ob bok sodobnim in primerljivim upravljalcem avtocestnega omrežja. Izzivi današnjega časa pa od nas zahtevajo neprestano prilagajanje. Če želimo slediti hitremu razvoju tehnologij in poslovnih procesov ter ustvarjanju novih poslovnih modelov, moramo postati fleksibilnejši, hkrati pa stremeti k poslovni odličnosti. Zato smo oblikovali ambiciozno strategijo za obdobje 2021–2025, ki pomeni orodje za nadaljnji uspešen razvoj družbe DARS.

Strategija temelji na viziji, usmerjeni v prihodnost. Lahko bi jo opisali z besedami: trajnostno, zeleno, digitalno in pametno. V njej smo si zadali tri ključne strateške usmeritve, ki udejanjajo zahteve in pričakovanja relevantnih deležnikov. Prvič, zavedamo se svoje odgovornosti do uporabnikov avtocestnega

V družbi DARS se zavedamo resnosti posledic, ki bi nastale z uresničitvijo različnih vrst tveganj. V vse bolj negotovem poslovnem okolju je obvladovanje tveganj pomemben dejavnik poslovnega uspeha družbe, zato veliko pozornosti namenjamo pravočasnemu zaznavanju tveganj in uspešnosti njihovega upravljanja oziroma preprečevanja.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



omrežja, s katerimi nas povezuje skrb za prometno varnost, pretočnost, zanesljivost in udobje na poti. Drugič, med prioritete postavljamo odgovornost za trajnostni razvoj družbe in celotnega okolja ter dolgoročno poslovno stabilnost. In tretjič, zaposlenim želimo zagotoviti varno, ustvarjalno in stimulativno delovno okolje.

V vašem mandatu ste izvedli nekaj pomembnih infrastrukturnih projektov, kar nekaj pa ste jih zastavili v projektno fazo. Zaupajte nam prosim kateri se vam iz vašega strateškega vidika zdijo ključni za boljšo povezljivost vseh delov Slovenije in njen nadaljnji regijski razvoj.

Najprej se mi zdi pomembno poudariti, da ima DARS pred seboj močan investicijski cikel. Samo v letošnjem letu načrtujemo investicije v višini 271 milijonov evrov, od tega za novogradnje namenjamo 74 milijonov, za obnove pa 75 milijonov evrov. Investiramo v gradnjo novih avtocestnih odsekov ter obnavljanje obstoječih, načrtujemo pa tudi investicije v vzpostavitev inteligentnih transportnih sistemov za nadzor in vodenje prometa. Največja investicijska projekta sta trenutno dva. Prvi je nadaljevanje izkopa druge cevi predora Karavanke, kjer dela dobro potekajo in smo že preko polovice 3.446 metrov dolgega slovenskega dela izkopa ter znotraj zadanih časovnih okvirjev. Drugi pa je dolgo pričakovana avtocestna povezava s Koroško na severu ter Dolenjsko in Belo krajino na jugu. Vesel sem, da nam je jeseni 2020 uspelo zagnati gradnjo tretje razvojne osi. Na njenem severnem delu, na odseku med Velenjem in Slovenj Gradcem, dela trenutno potekajo na dveh sklopih, Gaberke in Jenina, razpisa za izbor izvajalcev pa imamo še za štiri sklope, pridobivamo tudi gradbena dovoljenja. Začeti želimo tudi z gradnjo tretje razvojne osi na jugu, torej od Novega mesta do Bele krajine. Dobili smo že gradbeno dovoljenje za odsek Novo mesto-Osredek, vendar pa zaradi tožbe s strani tamkajšnje civilne iniciative čakamo na odločitev upravnega sodišča in upamo na skorajšnji pozitiven razplet. Ob tem pa aktivno delamo še na projektu vpadnic oziroma tako imenovanega tretjega pasu v Ljubljano, tako s primorske kot štajerske smeri, s čimer bi se znebili nepotrebnih jutranjih in popoldanskih zastojev, pridobivamo pa tudi gradbeno dovoljenja za hitro cesto med Gorišnico in Markovci. Sicer pa bi rad poudaril še en segment, in sicer, da želimo na avtocestnem križu vpeljati red. V ta namen smo aktivno sodelovali pri ustanovitvi avtocestne policije in tudi sofinanciramo njeno opremo, prepovedali smo prehitevanje tovornih vozil čez dan in dosledno sankcioniramo njihovo nedovoljeno parkiranje na uvozih in izvozih s počivališč, kar je doslej predstavljalo veliko nevarnost. Vse to neposredno prispeva k večji varnosti in pretočnosti prometa. Zadovoljni pa smo tudi, da smo uspeli prepoloviti število pretežkih tovornih vozil, ki uničujejo vozišče.

Uspešno smo uvedli še e-vinjeto in tako naredili velik korak naprej k digitalizaciji. V letošnjem letu pa je pred nami še prenova malih počivališč ob avtocestnem križu, ki bodo bolj prijazna in bodo uporabnikom avtocest nudila boljšo uporabniško izkušnjo.



Upravljanje s tveganji, ki niso samo finančne narave, je verjetno za vsakega strateškega managerja postala stalnica. Kako pristopate do tega pomembnega varnostnega procesa v svojem poslovnem okolju, ki ga vodite?

V družbi DARS se zavedamo resnosti posledic, ki bi nastale z uresničitvijo različnih vrst tveganj. V vse bolj negotovem poslovnem okolju je obvladovanje tveganj pomemben dejavnik poslovnega uspeha družbe, zato veliko pozornosti namenjamo pravočasnemu zaznavanju tveganj in uspešnosti njihovega upravljanja oziroma preprečevanja.

Proces upravljanja tveganj je postal del našega strateškega poslovanja, izvajamo pa ga v treh obrambnih linijah. Na prvi obrambni liniji je poslovodstvo, ki je odgovorno za vzpostavitev in uspešno delovanje notranjih kontrol ter izvajanje postopkov obvladovanja na dnevni ravni. Naloga poslovodstva je prepoznavanje in ocenjevanje tveganj, kot tudi opredelitev ustreznega odziva na tveganja – skladno s cilji organizacije. Druga obrambna linija vključuje tiste funkcije, ki izvajajo nadzor nad poslovnimi procesi in tveganji, kot so kakovost, računovodske kontrole, fizično varovanje in podobne kontrole. Zaposleni na omenjenih funkcijah so odgovorni za pravilno vpeljavo sistema obvladovanja tveganj. Spodbujamo opredeljevanje izpostavljenosti posameznim tveganjem in spremljanje uvajanja postopkov za obvladovanje tveganj ter razvijanje sistema poročanja o tveganjih. Tretjo obrambno linijo pa predstavlja notranje revidiranje. Skladno s sprejeto strategijo družbe se spreminjajo oziroma dopolnjujejo operativni cilji, ki podpirajo strateške cilje, na njihovi osnovi pa so prepoznana tudi strateška tveganja. Sistem tekoče preverjamo in dopolnjujemo, da bi bila tveganja, ki jim je DARS izpostavljen, pravočasno prepoznana, ovrednotena in obvladovana.

Učinkovitost sistema upravljanja tveganj se je nenazadnje izkazala kot ustrezna v pogojih poslovanja epidemije covida-19, ko smo dokazali, da je družba DARS organizacijsko in izvedbeno prilagojena na spremenjene razmere poslovanja. K temu je zagotovo pripomogla tudi ustanovitev interne koordinacijske skupine za obvladovanje tveganj ob pojavu koronavirusa. Pred nami pa so žal očitno še bolj negotove in zaskrbljujoče razmere zaradi vojne v Ukrajini. V upravi smo zato že imenovali krizno skupino, ki tekoče spremlja posledice oboroženih spopadov v povezavi z izpostavljenostjo družbe. Prepričan sem, da bomo tudi v tem primeru poslovanje ustrezno obvladovali na vseh kritičnih točkah svojih poslovnih procesov.

V Republiki Sloveniji je bil do sedaj na področju procesov opredeljevanja kritične infrastrukture sektor cestnega prometa kar nekako zanemarjen. Šele v zadnjem obdobju je dozorelo spoznanje, da je avtocestna infrastruktura v nekaterih delih izredno kritična in pomembno vpliva na ostale transportno-logistične segmente v državi. Kako vam je uspelo prepričati odgovorne v državi, da so prisluhnili vašim argumentom?

Že ob nastopu funkcije predsednika uprave družbe DARS, julija 2020, sem bil neprijetno presenečen, da avtoceste

in hitre ceste niso prepoznane kot kritična infrastruktura. Avtocestna infrastruktura ne le, da pomembno vpliva na druge transportno-logistične segmente v državi, ampak v primeru Slovenije predstavlja mednarodne povezave v pomembnih prometnih koridorjih. Na to dejstvo smo ustrezno opozorili pristojno ministrstvo za infrastrukturo. Predlagali smo jim, da znova preučijo pogoje opredelitve cestnih povezav kot kritično infrastrukturo. Sedaj teče postopek ponovnega preverjanja in na podlagi naših utemeljitev tudi pričakujemo, da bo avtocestna infrastruktura uradno prepoznana kot del kritične infrastrukture.

Vam je pri sprejemanju strateških odločitev bilo v pomoč, da ste tudi že v preteklosti zelo tesno sodelovali s Slovenskim združenjem za korporativno varnost in s tem ohranjali seznanjenost z razvojem procesov na tem zahtevnem področju?

Pred prihodom v družbo DARS sem delal tako v gospodarstvu kot v državni upravi, med drugim tudi na ministrstvu za obrambo. Varnostno področje me je namreč vseskozi zanimalo, zato sem bil včlanjen in aktiven tudi v Slovenskem združenju za korporativno varnost. Preden sem prevzel funkcijo predsednika uprave, področju korporativne varnosti nikakor ni bilo posvečene dovolj pozornosti. Še več, DARS, čigar dejavnost je tudi upravljanje s tako pomembno infrastrukturo, namreč sploh ni imel sistemsko pokritega področja korporativne varnosti, kot imajo to na primer druga primerljiva podjetja. Zavedati pa se moramo, da je varnost v današnjem času izjemnega pomena, to velja tudi za DARS, zato je treba temu področju posvečati še posebno pozornost. Zaradi tega sem se odločil, da bomo okrepili področje korporativne varnosti v najširšem smislu, z identifikacijo in izvajanjem vseh potrebnih sistemskih ukrepov za obvladovanje varnostnih tveganj. S spremembo akta o organiziranosti družbe DARS smo ustanovili službo za korporativno varnost, ki jo vodi mag. Anton Travner, varnostni strokovnjak s številnimi domačimi in mednarodnimi izkušnjami.

mag. Anton Travner

Neprekinjenost delovanja ključnih procesov v organizaciji, ki jo vodite je zelo pomembna, še posebej v času epidemiološke krize. Kakšen pomen ima v vaši organizaciji proces neprekinjenega poslovanja in kako pristopate k ocenjevanju, kaj je zares kritično za vašo poslovno organizacijo?

Trenutno res še nismo upravljalec kritične infrastrukture, vendar se v družbi dobro zavedamo, da je naše ključno poslanstvo, da zagotavljamo varen in nemoten promet po omrežju avtocest in hitrih cest. To v praksi pomeni, da moramo zagotavljati neprekinjeno poslovanje. Celoten koncept temelji na treh postulatih: zagotavljanje zadostnega in ustreznega kadra, ustrezna infrastruktura in ukrepi za vodenje in upravljanje prometa. Vse troje je v izjemno močni medsebojni korelaciji, zaradi česar pozornost posvečamo vsem trem elementom sočasno. V času epidemiološke krize smo največ pozornosti polagali prav zagotavljanju ustreznega kadra. Z dnevnim sledenjem vpliva virusa na odsotnost zaposlenih in z več kot 70 različnih ukrepov smo v družbi zagotovili, da smo uporabnikom ves čas omogočali nemoten prevoz. Ukrepe smo natančno načrtovali glede nujnosti izvajanja posameznih poslovnih procesov.

Je razumevanje strateškega vodstva do potreb korporativne varnosti dovolj izraženo, da vam to omogoča uvajanje novih tehnoloških rešitev za dvigovanje nivoja varnosti v podjetju?

Že samo dejstvo, da je z zadnjo reorganizacijo v družbi bila ustanovljena služba za korporativno varnost, in da je služba razmeroma dobro kadrovsko popolnjena, kaže na dejstvo, da se vodstvo družbe dobro zaveda, da je področje korporativne varnosti pomemben segment poslovanja družbe, ki ima pozitivne učinke predvsem na odhodkovni strani bilance. Brez uvajanja novih tehnoloških rešitev, posodobitve poslovnih procesov in digitalizacije, si tudi zagotavljanja učinkovitega sistema varovanja interesov družbe ne znam predstavljati, pri čemer je izražena popolna podpora vodstva družbe.

Zavedati pa se moramo, da je varnost v današnjem času izjemnega pomena, to velja tudi za DARS, zato je treba temu področju posvečati še posebno pozornost. Zaradi tega sem se odločil, da bomo okrepili področje korporativne varnosti v najširšem smislu, z identifikacijo in izvajanjem vseh potrebnih sistemskih ukrepov za obvladovanje varnostnih tveganj.

Procesi v podjetjih se vedno bolj digitalizirajo, kar na drugi strani prinaša določena nova tveganja na področju informacijske varnosti. Kakšen pomen dajete informacijski varnosti v vaši organizaciji?

Smo zelo specifična organizacija, značilna po segmentaciji posameznih poslovnih področij (upravljanje, vzdrževanje, cestninjenje, gradnje ...). Segmentacija je rezultat preteklih potreb, prioritet in poslovodnih odločitev. Ta delitev se močno odraža v vrsti ločenih informacijskih in telekomunikacijskih sistemov, kar že samo po sebi pomeni svojevrstno težavo, še težje pa je v takšnem okolju zagotavljati informacijsko varnost. Živimo v času, ko postaja digitalizacija in s tem informacijska tehnologija vse bolj in bolj pomembna za poslovanje družbe, na drugi strani pa se grožnje in napadi multiplicirajo. Poskušamo biti v koraku s časom, v največji meri zavarovati naše IT sisteme, na drugi strani pa ocenjujemo, kakšne posledice bi ob tem ali onem scenariju napada lahko utrpeli. Morda je s tega zornega kota segmentacija, neodvisnost in paralelnost različnih sistemov celo dobrodošla, saj je možnost popolnega lockdowna sistemov bistveno zmanjšana. V zadnjih dneh je tveganje, da bi bili tarča napadov, bistveno povečano in temu primerno je zagotavljanje informacijske varnosti povsem na vrhu naših prioritet.

Človeški potencial je vedno bolj pomemben za uspešno delovanje podjetij. Določena varnostna tveganja, kot so socialni inženiring, pa človeški faktor postavljajo tudi v položaj, ko nizko varnostno ozaveščen posameznik, za organizacijo lahko predstavlja pomembno tveganje. Kakšne pristope uporabljate za dvigovanje varnostnega zavedanja kolegov, ki v organizaciji delajo na različnih strateških pozicijah in kako pristopate v razmerju do vsakega zaposlenega?



Zaposleni so naše največje bogastvo in temu primerno se v družbi tudi vedemo. Je pa tudi res, da smo ljudje nepredvidljivi, da ima vsak posameznik sebi lastne navade, razvade in tudi slabosti. S primernim pristopom je negativne učinke individualnosti in s tem povezanimi tveganji za gospodarsko družbo moč zmanjšati, v idealnem primeru minimalizirati. Nevednost je naš največji sovražnik, zato s področja korporativne varnosti veliko naporov posvečamo usposabljanjem in ozaveščanju. Eno od prvih kislih jabolk, v katero sem zagrizel, je bilo varovanje poslovnih skrivnosti. Imam občutek, da so nov pravilnik, spremenjen sistem varovanja poslovnih skrivnosti in predvsem usposabljanja zaposlenih (tudi preko e-učenja) že prinesli nekatere pozitivne učinke. Za prvi in drugi nivo managementa smo pripravili varnostna usposabljanja s poudarkom na samozaščitnem ravnanju, preko e-pošte. Na intranetu pa redno opozarjamo in ozaveščamo zaposlene o varni rabi elektronske pošte in pasteh, ki na vse nas prežijo s svetovnega spleta.

Ste se v vaši organizaciji že začeli ukvarjati z razumevanjem hibridnih groženj, med katerimi je širjenje lažnih novic izredno izpostavljen dejavnik. Se s strateškim vodstvom pogovarjate in analizirate tudi tovrstne varnostne dejavnike?

Pojem hibridnih groženj se pojavlja v zadnjem času, vendar v praksi ni to čisto nič novega. Vso svojo kariero se ukvarjam z različnimi varnostnimi vprašanji, izzivi, grožnjami in zelo redko so bila zgolj eno-dimenzionalna. Pravijo, da ko ima hudič mlade, jih ima veliko in na področju zagotavljanja varnosti je to pogosto, če ne kar praviloma. Če je v preteklosti bila neinformiranost ali nepoznavanje eden od elementov varnostnega tveganja, se sedaj srečujemo s poplavo lažnih novic in informacij. Če včasih nekaj nismo vedeli, smo zvedeli. Sedaj smo prepričani, da nekaj vemo, in nismo pripravljeni sprejeti drugačne resnice, kar v bistvu pomeni večje tveganje. Epidemiološka kriza je bila idealni poligon preverjanja verodostojnosti informacij. V družbi smo ponosni, da smo že v lanskem letu dosegli skoraj 73-odstotno precepljenost. Verjamem, da je to odgovor na vaše vprašanje, ali tem dejavnikom posvečamo dovolj pozornosti.

Kje v prihodnosti na varnostnem področju pričakujete največje izzive, ki jim bo potrebno posvetiti posebno pozornost?

Bodoče izzive na varnostnem področju bi razdelil v dve kategoriji. Prva kategorija so bolj klasična področja, kot so kibernetska varnost, varovanje informacij in varovanje premoženja, druga kategorija pa so nepričakovana tveganja, kot je bila pandemija in sedaj vojna v Ukrajini. Največji izziv je zagotoviti fleksibilnost in hitro odzivnost, saj je od tega odvisna tudi učinkovitost spopadanja z izzivi. ■

Foto: Barbara Reya


SMART COM
UDEJANJAMO VAŠE VIZIJE
www.smart-com.si
Zagotovite varno, zanesljivo in odgovorno digitalno prihodnost
Smart Center upravljanih varnostnih in omrežnih storitev
Kibernetska varnost v poslovnem in industrijskem okolju ter okolju kritične infrastrukture
Sodobna omrežja nove generacije za odlično uporabniško izkušnjo
Hiperkonvergenčna infrastruktura v podatkovnih centrih in enostaven prehod v računalniški oblak

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

INTERVJU
dr. Uroš Svete, direktor Urada za informacijsko varnost*

POMEMBNA JE VZPOSTAVITEV USTREZNEGA EKOSISTEMA KIBERNETSKE VARNOSTI

Urad za informacijsko varnost nadaljuje s pomembnimi koraki v smeri zagotavljanja kibernetske varnosti Republike Slovenije. Izkoristili smo priložnost in se pogovorili z dr. Svetetom, da nam podrobneje razjasni vizijo razvoja ekosistema na področju kibernetske varnosti.

Pred kratkim ste bili dokončno potrjeni na funkcijo direktorja Urada za informacijsko varnost s polnim mandatom, za kar vam čestitamo. Sedaj bo lažje nadaljevati sistemsko delo, ki bo usmerjeno v dolgoročno obdobje. Kje bodo vaši glavni poudarki te dolgoročne usmerjenosti?

Hvala za čestitke. Lahko rečem, da potrditev na funkcijo direktorja Urada za informacijsko varnost ni bistveno vplivala ne na moje delo, ne na delo urada oz. mojih sodelavcev in sodelavk. Od prvega dne namreč želim uveljaviti koncept temelječ na sistemskem pristopu, ki bo sodoben v smislu sledenja izzivom kibernetske varnosti, kakor tudi celovitem načinu njenega zagotavljanja. Ključno je, da delamo na dolgi rok, tako pri tehničnem obvladovanju kibernetskih groženj, sodelovanju upravljalcev informacijske infrastruture, kot pri dvigu odpornosti celotne družbe. Kajti digitalizacija je v sodobnem svetu neobhodna, vendar pa tako kot vsaka tehnologija prinaša tudi ranljivosti in tveganja. Čeravno smo v zadnjih letih zelo pospešili prizadevanja za krepitev kibernetske varnosti, pa določenih razvojnih faz žal ne moremo preskočiti. Prav tako se bomo morali, ko gre za informacijsko tehnologijo in kibernetsko varnost, navaditi na novo realnost, spremenjeno vlogo države, sodelovanje javnega in zasebnega sektorja, za vse to pa v prvi vrsti potrebujemo izgradnjo zaupanja. Skratka, končni cilj je sistem, ki bo učinkovito deloval tudi v kriznih razmerah, prav tako pa bo dovolj koheziven, da bo odporen na vse vrste sprememb, vključno s kadrovskimi. V ta namen bomo uporabili vsa možna orodja, od tehničnih, finančnih, razvojnih do zakonskih in organizacijskih.

Z veseljem lahko potrdim, da smo na pravi poti. S preoblikovanjem pristojnega organa za informacijsko varnost v samostojno vladno službo smo naredili preskok na organizacijskem področju in dosegli ustrezno strateško umestitev, ki je primerljiva z vodilnimi evropskimi državami in nam omogoča nadaljnjo rast.

Republika Slovenija je ob zaključku lanskega leta uspešno zaključila predsedovanje EU. Na področju informacijske varnosti so se dogajale pomembne razprave in prebojni koraki. Kaj je tisto kar bi veljalo posebej izpostaviti?

S področja kibernetske odpornosti je bila ključna obravnava predloga Direktive evropskega parlamenta in sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (t.i. "Network and Information Security" - NIS2 direktiva), v zvezi s katero je Svet EU 3. decembra 2021 dosegel splošni pristop, s čimer je bil podeljen mandat za začetek pogajanj z EP (trialogi). Francosko predsedstvo Svetu EU je trenutno v fazi pogajanj z Evropskim parlamentom. Zaključek pogajanj ter končno potrditev besedila direktive pa načrtuje predvidoma v maju 2022. Nova direktiva bo po sprejetju nadomestila sedanjo direktivo NIS in pripomogla k višji stopnji kibernetske odpornosti EU, zmogljivosti

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



odzivanja na incidente in zaščiti kritične infrastrukture. Cilj zakonodajnega predloga je odpraviti pomanjkljivosti prvotne direktive (NIS1), katere sprejetje leta 2016 prestavlja prvi zakonodajni akt EU na področju kibernetske varnosti v EU.

EU si prizadeva tudi za izboljšanje okvira za kibernetsko krizno odzivanje. V ta namen je EK 23. 6. 2021 predstavila priporočilo o vzpostavitvi Skupne kibernetske enote (Joint Cyber unit - JCU). Ta bi delovala kot fizična in virtualna platforma za sodelovanje različnih skupnosti na področju kibernetske varnosti v EU, osredotočena pa bi bila na operativno in tehnično usklajevanje v boju proti večjim čezmejnim kibernetskim krizam. Glede kibernetskega kriznega odzivanja so bili na zasedanju Sveta za splošne zadeve - GAC 19. oktobra 2021 potrjeni Sklepi Sveta o raziskovanju potenciala pobude o vzpostavitvi Skupne kibernetske enote (JCU). Sklepi dajejo politične smernice za nadaljnje delo in izkazujejo zavezo Sveta EU in držav članic h krepitvi kibernetske odpornosti in nadaljnjemu razvoju okvira EU za upravljanje kibernetskih kriz. Izpostavljajo pomen okrepitve že obstoječih struktur, spoštovanja obstoječih mandatov in predvsem potrebo po postopnem procesu, ki bi omogočil ustrezno sodelovanje DČ in institucij, organov in agencij EU. Izpostavljajo tudi potrebo po zagotovitvi vključenosti širšega nabora različnih skupnosti oz. deležnikov. Slovensko predsedstvo Svetu EU je pripravilo dva dokumenta predsedstva – 20. oktobra in 13. decembra s predlogi nadaljnjih korakov. V času francoskega predsedstva Svetu EU se zaenkrat razprava o JCU ne nadaljuje, predvidoma pa bo pogosteje na agendi v drugem trimesečju letošnjega leta.

Urad za informacijsko varnost dobiva vedno nove pristojnosti in odgovornosti. Kako uspete ta razvoj podpirati s prihodom novih kadrov, ki so potrebni za izvajanje vedno širših aktivnosti, ki se pričakujejo od vaše organizacije? Je tukaj dovolj razumevanja s strani Vlade Republike Slovenije, da bo temu področju namenila več virov, kot jih je namenjala do sedaj?

Pridobivanje kadrov na področju informacijske in kibernetske varnosti je izziv, tako za državne organe kot za podjetja, kajti tovrstnih znanj je na trgu dela v Sloveniji preprosto premalo. Kar se Urada RS za informacijsko varnost tiče, imamo vsekakor dovolj razumevanja s strani Vlade RS, seveda pa moramo ostati znotraj pogojev, ki veljajo za zaposlene v javni upravi. A vendarle je mogoče najti rešitve tudi v togem birokratskem sistemu. Ena od zelo pomembnih pristojnosti in odgovornosti urada je tudi inšpekcijski nadzor, katerega izvaja Inšpekcija za informacijsko varnost, ki nadzira skladnost zavezancev (izvajalcev bistvenih storitev in organov državne uprave) z zakonodajo s področja informacijske varnosti. Potrebna znanja in kompetence inšpektorja za informacijsko varnost pa so zelo široke. Zaradi kroničnega pomanjkanja strokovnjakov s področja informacijske varnosti na trgu dela smo pričeli z intenzivnim usposabljanjem inšpektorjev na Upravni akademiji, SIQ Ljubljana in Laboratoriju za telekomunikacije (Fakultete za elektrotehniko, Univerze v Ljubljani). Za potrebna usposabljanja smo tako v 2022 ustrezno povečali finančne vire.

Veliko pozornosti seveda namenjamo tudi razvoju kadrov ter krepitvi zavedanja o pomenu kibernetske varnosti med mladimi IT- strokovnjaki. V ta namen smo zagnali projekt Kibertalent, s katerim želimo popularizirati področje kibernetske varnosti

V RS imamo zlasti na področju izmenjave podatkov o kibernetskih incidentih še ogromno rezerv.

med mladimi, predvsem srednješolci in študenti, da bi se le-ti v večji meri odločali za študij in kariero na tem področju. Ravno v marcu smo pričeli z nizom brezplačnih on-line delavnic kibernetske varnosti, ki so na voljo vsem, predvsem pa že omenjeni ciljni skupini. Prav tako smo v okviru projekta lansko leto pričeli s financiranjem izbora, priprave in udeležbe slovenske ekipe na tekmovanju mladih talentov v kibernetski varnosti European Cybersecurity Challenge. Lansko tekmovanje je potekalo v Pragi, kjer je naša ekipa prejela tudi nagrado za nalogo o možnostih uporabe umetne inteligence v kibernetski varnosti. Letošnje tekmovanje bo septembra na Dunaju.

Ne dolgo tega ste kot nujen korak posebej poudarjali potrebo po vzpostavitvi celovitega sistema vseh deležnikov na področju kibernetske varnosti. Se je v tem obdobju uspel ta ekosistem razvijati v pravo smer?

Z veseljem lahko potrdim, da smo na pravi poti. S preoblikovanjem pristojnega organa za informacijsko varnost v samostojno vladno službo smo naredili preskok na organizacijskem področju in dosegli ustrezno strateško umestitev, ki je primerljiva z vodilnimi evropskimi državami in nam omogoča nadaljnjo rast. Med deležniki smo dvignili zavedanje o pomenu kibernetske varnosti za delovanje države in gospodarstva. Okrepljeno delovanje koordinacije na področju kibernetske varnosti daje ustrezne rezultate. Ja, srečujemo se s težavami, zapuščino preživetih načinov razmišljanja, zanemarjanja področja v preteklosti, preobilico nalog, a kot sem rekel, smo na pravi poti. Na URSIV bomo to leto posvetili graditvi odnosov z zavezanci in krepitvi SIGOV-CERT, ki je s spremembo Zakona o informacijski varnosti sedaj umeščen v naš urad. Ob tem sem dolžan opozoriti, da na Ministrstvu za javno upravo deluje samostojen varnostno operativni center, ki postaja pomemben partner naše skupnosti. Nestrpno pričakujemo spremembe Zakona o elektronskih komunikacijah, ki bodo formalno uredile odnose med našim uradom, AKOS-om, operaterji elektronskih komunikacij in SI-CERT-om. Skupaj z Ministrstvom za obrambo in Službo Vlade RS za digitalno preobrazbo načrtujemo spremembe na področju sektorja kritične infrastrukture informacijsko-komunikacijskih omrežij in sistemov. Nosilec sektorja naj bi postal URSIV.

URSIV s sredstvi nacionalnega programa za okrevanje in odpornost v prihodnje načrtuje izvedbo več projektov, ki bodo pripomogli k dvigu ravni kibernetske varnosti. Na nacionalni ravni želimo vzpostaviti enotno platformo za priglasitev incidentov. Z davkoplačevalskega vidika bi bilo smiselno, da taka platforma ne pokrije le obveznosti po ZinfV, ampak morda tudi po ZKI in ZEKom. V tem primeru bi bilo potrebno sodelovanje več različnih deležnikov, a bi to nedvomno olajšalo življenje zavezancem, ki so zavezani poročati po različnih zakonih. Na strani organov bi taka platforma zagotovila informacije v realnem času, kar je nujno za situacijsko zavedanje.

Poleg tega si URSIV želi vzpostaviti center za deljenje in analizo informacij (ISAC), ki bi analiziral informacije iz različnih virov (od priglasitev incidentov, odprtih in plačljivih virov, informacij pridobljenih od partnerskih organov iz tujine itd.) in jih delil z organi na operativni ravni (CSIRTi in SOCi), pa tudi z regulatorji sektorjev in subjekti v teh sektorjih. Tukaj pridemo do tretjega projekta, vzpostavitve partnerskega omrežja zaupanja za deljenje informacij s področja kibernetske varnosti, kjer bi se prej omenjene informacije izmenjevale s končnimi uporabniki.

Poleg izvedbe omenjenih projektov načrtujemo tudi pripravo vzorčne varnostne dokumentacije in vzorčnih varnostnih ukrepov za organizacije različnih velikosti, vključitev tem s področja kibernetske varnosti v kurikulume na osnovni in srednješolski ravni za ozaveščanje splošne populacije, pa tudi aktivnosti za popularizacijo področja kibernetske varnosti med mladimi, s končnim ciljem povečanja števila strokovnjakov na tem področju (izgradnja zmogljivosti).

Vsi omenjeni projekti in aktivnosti imajo sicer različne ciljne skupine, a vsi skupaj razvijajo in krepijo skupnost na področju kibernetske varnosti.

Urad je prevzel tudi pomembno funkcijo nacionalnega kompetenčnega centra za kibernetsko varnost. EU namerava v naslednjem obdobju pomemben vir, za raziskave in razvoj na področju kibernetske varnosti, usmeriti skozi to mrežo kompetenčnih centrov. Nam lahko pojasnite težišča delovanja na tem področju?

Gre za zelo pomembno pobudo, ki jo ureja evropska uredba o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov. Slovenija je pravočasno izpolnila zavezo iz 6. člena omenjene uredbe in imenovala URSIV kot organ, ki opravlja naloge nacionalnega koordinacijskega centra za kibernetsko varnost v Mreži nacionalnih koordinacijskih centrov. A to je šele prvi korak. Slovenija vidi dodano vrednost v krepitvi evropske koordinacije in v strateški usmerjenosti investicij iz programov Obzorje Evropa in Digitalna Evropa v raziskave, tehnologije in industrijski razvoj na področju kibernetske varnosti. Menimo, da lahko pomembno prispeva h krepitvi varnosti digitalnega enotnega trga, evropske digitalne suverenosti in strateške avtonomije ter h krepitvi evropske globalne konkurenčnosti. Gre za proaktiven, dolgoročnejši in strateški pristop k raziskavam, razvoju in industrijski politiki na področju kibernetske varnosti. Ta pristop bo prispeval ne le k prelomnim rešitvam za kibernetsko varnostne izzive, s katerimi se soočata zasebni in javni sektor, ampak bo tudi podpiral učinkovito uvajanje teh rešitev. S povečanjem tehnološke suverenost z obsežnimi projekti kibernetske varnosti na področjih, kot so obveščevalni podatki o kibernetskih grožnjah, kibernetsko zaščitena strojna oprema in operacijski sistemi ter varnostno certificiranje bomo prispevali k dvigu kibernetske varnosti. Raziskovalnim in industrijskim skupnostim ter javnim organom bo vzpostavitev kompetenčnega centra omogočila dostop do ključnih zmogljivosti, kot so obrati za preizkušanje in poskuse, ki državam članicam zaradi nezadostnih finančnih in človeških virov pogosto niso dostopne. Seveda brez sodelovanja z ustreznimi javnimi organi in zainteresiranimi stranmi, ki lahko prispevajo k spodbujanju in razširjanju izobraževalnih programov za kibernetsko varnost, ne bo šlo. Gre za celovit pristop spodbujanja dviga kompetenc s področja kibernetske varnosti, ki je eden od pomembnih segmentov pospešene digitalizacije družbe.

Mreža nacionalnih koordinacijskih centrov na področju kibernetske varnosti bo torej namenjena tudi krepitvi evropskega ekosistema, strateškemu povezovanju, iskanju poslovnih partnerjev, olajšanemu dostopu do finančnih virov, dostopu do testirane opreme, prenosu dobrih praks in krepitvi kompetenc ter nadgradnji potrebnih znanj. Centri bodo krovno povezani pod skupno streho v okviru Evropskega kompetenčnega centra, kateri bo zadolžen, za komunikacijo med vsemi NCC, prenosu novosti na evropskih projektih/skladih/razpisih, povezovanju med centri,

ter krepitvi evropske kibernetske neodvisnosti. Kompetenčni center je trenutno v fazi vzpostavljanja, prav tako pa njegovi sateliti na nacionalni ravni, torej NCC. Primarno bosta oba črpala sredstva iz programa DIGITAL, ki je namenjen uporabi digitalnih tehnologij, medtem ko za RRI ostaja krovni program OBZORJE.

Glede teh vzpostavitev bo več znanega v nekaj mesecih, ko bodo stekli prvi postopki in razpisi, ter ko se ključne aktivnosti za vzpostavitev kompetenčnega centra realizirajo. V Sloveniji smo trenutno v fazi pripravljanja potrebnih nalog za optimalno vzpostavitev NCC, vsekakor pa bo morala biti to živa tvorba, ki se bo sposobna prilagajati hitrim spremembam na tem področju, ter bo zaobjela različne deležnike, kakor tudi ciljne skupine.

Se je sistem zbiranja ključnih podatkov o kibernetskih incidentih po vaši oceni v zadnjem letu izboljšal? Ali koraki, ki se razvijajo skozi mrežo CERT-ov, naj omenimo uvajanje platforme MeliCERT, prinašajo določene rezultate?

V RS imamo zlasti na področju izmenjave podatkov o kibernetskih incidentih še ogromno rezerv. Sicer smo določene izboljšave dosegli, ko je Vlada RS na naš predlog sprejela nacionalni načrt odzivanja na kibernetske incidente (NOKI), ki se nanaša tudi na prijavo incidentov in izmenjavo podatkov, a smo od operativno delujočega sistema še precej daleč. Imamo sicer različne platforme in tehnične rešitve. Tu lahko omenim MISP in platformo MeliCERT, oziroma njene novejše izpeljanke, ki predstavljajo skupek podpornih orodij za delo CERTov z namenom vzpostavitve poenotenega omrežja, namenjenega sodelovanju in izmenjavi informacij nacionalnih CSIRTov. Vsekakor bomo omenjene tehnične rešitve upoštevali, ko bomo vzpostavili platformo za priglasitev incidentov in bo morala omogočiti povezavo z MeliCERT-i oziroma z njenimi novejšimi izpeljankami (npr. https://www.cerebrate-project.org/). Vendar pa je večji problem prepričati tako zavezance kot varnostno-operativne centre in CSIRT skupine, zakaj je izmenjava podatkov pomembna, kot pa najti tehnično rešitev. Še vedno namreč opažamo previdnost in skepso, vsakršna "prisila" (seveda na zakonski osnovi), pa je zgolj navidezna rešitev. Zato bomo vse moči usmerili v krepitev zaupanja in izgradnjo slovenske kibernetske skupnosti, ki bo na koncu brez težav našla tudi primerno orodje za medsebojno povezljivost.

Urad za informacijsko varnost je vedno bolj aktiven tudi kot pomemben deležnik pri sodelovanju v mednarodnih konzorcijih, ki razvijajo določene kibernetske rešitve in procese. Boste tudi v prihodnje temu področju namenjali ustrezno podporo?

Če sodelovanje v takih konzorcijih lahko pripomore k razvoju rešitev in procesov, prenosu dobrih praks in gradnji zaupanja med vključenimi deležniki, kar vse pozitivno vpliva na dvig ravni kibernetske varnosti, se bo URSIV še naprej prizadeval za tako sodelovanje.

Procesi digitalizacije prodirajo v vse segmente družbenih procesov. Na drugi strani to odpira pomembne izzive na področju zagotavljanja informacijske varnosti. Imate občutek, da ste dovolj vključeni v pripravo procesov digitalizacije s stališča zagotavljanja informacijske varnosti?

Absolutno. Glede na zadnje spremembe in naše pozicioniranje kot samostojne vladne službe, imamo dovolj vpogleda nad procesi digitalizacije in podajanji mnenj. Imamo možnost vpliva tudi na to, da se digitalizacija v RS končno začne izgrajevati po principu "security by design".

Kakšni so načrti na področju razvoja kvantnih komunikacij in predvsem kvantnega šifriranja komunikacij? Bo imel vaš urad v prihodnosti na tem področju pomembno koordinativno vlogo?

URSIV je odgovoren za izvedbo projekta SI-EuroQCI, v katerem bo vzpostavljeno nacionalno omrežje kvantne komunikacijske infrastrukture za distribucijo kvantnih šifrirnih ključev. Projekt je del vseevropskega projekta EuroQCI v katerem se bodo nacionalna omrežja povezala med seboj preko zemeljskih optičnih postaj pa tudi s konstelacijo satelitov za komunikacijo na velike razdalje. Pri nas bodo v omrežje povezani organi, ki delujejo na področju nacionalne varnosti. Izvedba projekta je sicer zelo odvisna od pridobitve sredstev na evropskih razpisih DEP in CEF, medtem, ko se bo nacionalna soudeležba financirala iz sredstev NOO. URSIV bi v prihodnje lahko sodeloval pri upravljanju omrežja.

Vam je uspelo v zadnjem letu narediti kakšne pomembne korake pri zagotavljanju konsistentnosti zakonodaje na področju zagotavljanja informacijske varnosti? Predvsem sta tukaj izpostavljena Zakon o informacijski varnosti in Zakon o kritični infrastrukturi?

V preteklem letu je treba kot bistveno pridobitev najprej izpostaviti sprejem in uveljavitev novele Zakona o informacijski varnosti (t.i. ZInfV-A). Osnovni Zakon o informacijski varnosti iz leta 2018 (ZInfV-18) je namreč določal umestitev pristojnega nacionalnega organa (URSIV) kot organa v sestavi Ministrstva za javno upravo (MJU), kar je bilo sicer skladno s "sistemsko ureditvijo" v Republiki Sloveniji (RS). V praksi npr. pri obravnavi incidentov in koordinaciji aktivnosti, pa so bile zaznane slabosti takšne ureditve. Zato se je z novelo ZInfV-A spremenila umestitev pristojnega nacionalnega organa za informacijsko varnost in se je Uprava Republike Slovenije za informacijsko varnost, organ v sestavi MJU, preoblikovala v samostojno vladno službo in sicer v Urad Vlade Republike Slovenije za informacijsko varnost. Urad z lastno inšpekcijsko službo izvaja nadzor nad izvajanjem ZInfV ter pripravlja tudi predloge predpisov s področja informacijske in kibernetske varnosti za Vlado Republike Slovenije. V novo vladno službo (urad – URSIV) se je umestil tudi CSIRT organov državne uprave, skupina, ki se odziva na incidente na področju informacijske varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov. Z novo umestitvijo URSIV, ki je vladna služba, njen direktor pa je neposredno odgovoren predsedniku vlade, se je posledično dvignil nivo koordinacije kibernetske varnosti, doseglo pa se je tudi primerljivo ureditev z vodilnimi državami.

Dodatne spremembe so z vidika boljše medsebojne usklajenosti in koordinacije že predvidene tudi na področju izvajanja Zakona o kritični infrastrukturi (ZKI) in sicer je s strani Ministrstva za obrambo (MORS) že pripravljen predlog Sklepa o

Mreža nacionalnih koordinacijskih centrov na področju kibernetske varnosti bo torej namenjena tudi krepitvi evropskega ekosistema, strateškemu povezovanju, iskanju poslovnih partnerjev, olajšanemu dostopu do finančnih virov, dostopu do testirane opreme, prenosu dobrih praks in krepitvi kompetenc ter nadgradnji potrebnih znanj.

V URSIV Slovensko združenje za korporativno varnost vidimo kot ekosistem, ki združuje tako rekoč vse subjekte, ki so pomembni za delovanje družbe. Zato bo preko združenja lažje dostopati ne samo do izvajalcev bistvenih storitev (IBS), ponudnikov digitalnih storitev (PDS) in organov državne uprave (ODU), ki so zavezanci po ZinfV, ampak tudi do subjektov kritične infrastrukture in drugih subjektov, ki so tako ali drugače pomembni za nemoteno delovanje slovenskega gospodarstva in družbe.

spremembah Sklepa o določitvi nosilcev sektorjev kritične infrastrukture Republike Slovenije in z njimi sodelujočih državnih organov. Predvidena sprememba navedenega sklepa upošteva, da je bila z uveljavitvijo ZInfV-A pristojnost na področju informacijske varnosti podeljena vladni službi - URSIV, na podlagi Zakona o spremembah Zakona o državni upravi (ZDU-1M) pa je naloge s področja elektronskih komunikacij, ki jih je do tedaj opravljalo MJU, prevzela Služba Vlade Republike Slovenije za digitalno preobrazbo (SDP). Zato se predlagata spremembi v delu, ki se nanaša na nosilca sektorja kritične infrastrukture »informacijsko-komunikacijskih omrežij in sistemov«, ki bo po novem Urad Vlade Republike Slovenije za informacijsko varnost (URSIV), z njim sodelujoči državni organ pri izvajanju njegovih nalog po ZKI pa bo SDP.

Prav tako je URSIV v preteklem obdobju, vključno z namenom konsistentnosti zakonodaje na področju zagotavljanja informacijske varnosti, sodeloval s SDP oziroma predhodno z MJU (glede na vsakokratno pristojnost za področje elektronskih komunikacij) pri pripravi predloga novega sistemskega zakona za področje elektronskih komunikacij (t.i. ZEKom-2) in sicer v delu, ki se nanaša na področje informacijske varnosti. Pri tem je šlo za poglavje predloga ZEKom-2 o varnosti omrežij in storitev ter delovanje v stanjih ogroženosti. Glavnina sprememb (glede na sedaj veljavni zakon - ZEKom-1) je posledica sprememb regulativnega okvira na področju elektronskih komunikacij ter predvidene implementacije ukrepov, predvidenih s Sporočilom EK »Varna uvedba tehnologije 5G v EU – izvajanje nabora orodij EU« (Nabor orodij EU), ki je rezultat skupnih prizadevanj in pristopa držav članic Evropske unije (EU), predstavnikov Agencije Evropske unije za kibernetsko varnost (ENISA) in Evropske komisije (EK), ki ga je podprla tudi RS. Za operaterje elektronskih komunikacij so se s predlogom ZEKom-2 okrepile zahteve in pogoji glede varnosti omrežij in storitev, v luči varnostnih tveganj, ki jih prinaša tehnologija 5G, pa še posebej za operaterje mobilnih komunikacijskih omrežij, ki zagotavljajo ta omrežja določenim subjektom, ki z vidika države in družbe zagotavljajo t. i. kritične storitve, kar ima pomen tudi za nacionalno varnost. Hkrati se je želelo predlagano ureditev približati sistemski ureditvi področja informacijske varnosti (ZInfV) in tudi sistemskemu zakonu s področja kritične infrastrukture (ZKI). Treba je namreč pojasniti, da sedaj veljavna Direktiva NIS, ki jo v slovenski pravni red prenaša ZinfV, izključuje urejanje zahtev informacijske varnosti za operaterje elektronskih komunikacij, ker to trenutno ureja področna ureditev elektronskih komunikacij tako na EU kot na nacionalnem nivoju (z direktivami EU in z nacionalno zakonodajo elektronskih komunikacij). Prizadevali smo si torej, da se ureditev tudi v teh okoliščinah kolikor mogoče približa ureditvi po ZinfV. Vsekakor ocenjujemo, da bi sprejem ZEKom-2 doprinesel k konsistentnosti in medsebojni usklajenosti zakonodaje na področju informacijske varnosti, pa tudi sicer bi v luči (spremenjenih) varnostnih razmer okrepil informacijsko varnost na področju elektronskih komunikacij.

Slovensko združenje za korporativno varnost res postaja tista strokovna mreža, kjer je na enem mestu združena večina poslovnih organizacij in državnih institucij, ki imajo pomembno vlogo na področjih informacijske varnosti, kritične infrastrukture in ostalih s tem povezanih vidikih. Tudi Urad za informacijsko varnost je postal član te asociacije. Kje vidite še dodatne možnosti za krepitev tega ekosistema, ki lahko pomembno prispeva k dvigovanju zavedanja o pomembnosti informacijske varnosti?

Jaz in moji uslužbenci se na dnevni bazi srečujemo z vprašanjem, kaj lahko naredimo bolje za dvig kibernetske varnosti v naši državi. S podobnimi dilemami se srečujejo tudi ostali pristojni nacionalni organi po Evropi. Menim, da je na področju kibernetske varnosti pomembno sodelovanje in zaupanje deležnikov. Na to so me opozorili tudi kolegi iz Evrope. Moja vizija razvoja urada gre v preseganje birokratskih okvirov, ki nam uradnikom omogočajo navidezno izpolnjevanje zakonskih določb in življenja v mehurčku, daleč od realnih problemov skupnosti. Iz omenjenega razloga smo se vključili tudi v vaše združenje. Naše poslanstvo je, v skladu z določbami zakona, tudi koordiniranje delovanja sistema informacijske varnosti. Slednje ne razumemo kot ozko usmerjenost na področje države in nacionalne varnosti. Koordiniranje razumemo kot partnerski odnos med pristojnim nacionalnim organom, odzivnimi in varnostno operativnimi centri, subjekti javne uprave in gospodarstva, raziskovalno-razvojnimi organizacijami, znanstvenimi institucijami, interesnimi združenji in posamezniki. Slovenija zaradi svoje majhnosti, šibkega kadrovskega nabora in specifik delovnega trga ne bo zmožna graditi in ohranjati kapacitet, ki si jih lahko privoščijo vodilne države. Zato pa lahko s sodelovanjem, koordinacijo in jasnim strateškim pogledom dosežemo maksimiranje učinkov naših resursov. V tej vlogi, podpornika prizadevanjem in glasnika prihodnosti, vidim tudi vaše združenje. V URSIV Slovensko združenje za korporativno varnost vidimo kot ekosistem, ki združuje tako rekoč vse subjekte, ki so pomembni za delovanje družbe. Zato bo preko združenja lažje dostopati ne samo do izvajalcev bistvenih storitev (IBS), ponudnikov digitalnih storitev (PDS) in organov državne uprave (ODU), ki so zavezanci po ZinfV, ampak tudi do subjektov kritične infrastrukture in drugih subjektov, ki so tako ali drugače pomembni za nemoteno delovanje slovenskega gospodarstva in družbe. Na ta način bi se lahko izvajali prilagojeni programi ozaveščanja. Po drugi strani bi združenje, ki združuje različne strokovnjake, s predlogi lahko sodelovalo pri pripravi nove strategije kibernetske varnosti in kasneje novega zakona o informacijski varnosti. Kar veliko članov združenja vidimo tudi kot potencialne člane partnerskega omrežja zaupanja za deljenje informacij s področja kibernetske varnosti, katerega vzpostavitev v prihodnosti načrtujemo na URSIV. ■

Foto: arhiv URSIV

WWW.SILVERBULLETRISK.COM

Tveganja povežite s poslovnimi kazalniki uspešnosti

Kulturo upravljanja tveganj pa vpeljite v čisto vse organizacijske procese



SVETOVANJE O UPRAVLJANJU TVEGANJ

CELOVITO **UPRAVLJANJE TVEGANJ**

UPRAVLJANJE **ŠKODNIH DOGODKOV**

Silver Bullet Risk je vodilno podjetje na področju celovitega upravljanja in obvladovanja tveganj v Sloveniji.

Izkoriščamo moč znanja, izkušenj in tehnologije, da lahko podjetjem in organizacijam ponudimo najcelovitejši nabor storitev s področja upravljanja tveganj na enem mestu.

V zadnjih nekaj letih je našo programsko opremo in svetovalne storitve uporabilo več kot 100 največjih podjetij v Sloveniji.

UČINKI IN IZBOLJŠAVE ZA VAŠO ORGANIZACIJO

- 30-50% učinkovitejša izraba časa za upravljanje tveganj
- Nižji stroški realiziranih tveganj
- Spremljanje finančnih in drugih vplivov
- Gradnja lastne baze znanja o tveganjih
- Ustrezno ukrepanje v realnem času
- Zagotovljena skladnost z zahtevami in predpisi

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Jože Knavs, zastopnik družbe Informatika d.o.o.*

DIGITALIZACIJA V ELEKTROENERGETIKI POSTAJA REALNA POTREBA

Informatika s svojim razvojem uspešno drži korak z zahtevami kompleksnega varnostnega okolja in ključnih procesov, ki se v elektroenergetiki dogajajo v zadnjem obdobju. O ključnih izzivih, ki jih prinašajo digitalizacija, zelena transformacija in potrebe po dvigovanju kibernetske varnosti smo se pogovarjali z mag. Jožetom Knavsom.

Informatika predstavlja pomemben del podpornih procesov za celoten elektrodistribucijski sistem Slovenije. Nam lahko na kratko opredelite glavne težiščne naloge podjetja?

Informatika d.o.o. ima več kot pol stoletja izkušenj z izvajanjem informacijske podpore za ključne poslovne procese elektrodistribucijskih podjetij v Sloveniji, med katerimi je glavni obračun omrežnine in električne energije. V okviru te podpore smo razvili in upravljamo enotno vstopno točko za izmenjavo podatkov med B2B deležniki na trgu električne energije, portal Moj elektro in Centralno elektroenergetsko podatkovno središče (CEEPS).

Poleg tega našim uporabnikom ponujamo širok portfelj IKT storitev. Tako jim nudimo odzivno, visoko razpoložljivo strežniško in telekomunikacijsko infrastrukturo, vključno z upravljanjem in podporo. Ponujamo in vzdržujemo standardne ERP rešitve, rešitve za upravljanje s sredstvi ter IKT storitveni center. Ponujamo storitve podatkovnega skladišča, ki ga nadgrajujemo z rešitvami podatkovne analitike.

Dodatno izvajamo projekte razvoja programske opreme na zahtevo. V začetku leta pa smo vzpostavili sektorski varnostni operativni center (VOC), ki ga uporabljajo vsa slovenska elektrodistribucijska podjetja.

Zaposleni in njihova znanja so in bodo za Informatiko zelo pomembni, zato bomo tudi v prihodnje aktivno dodajali manjkajoče kompetence, skrbeli za intenzivno izobraževanje in pridobivanje novih znanj, ki bodo potrebna v prihodnosti.

V zadnjem obdobju ste bili zaradi rednih in izrednih situacij podvrženi relativno hitri menjavi strateškega vodstva organizacije. Kje so tisti strateški koraki, ki ste si jih začrtali za razvoj Informatike v bližnji prihodnosti?

Elektrodistribucijska podjetja in drugi udeleženci trga z električno energijo so priča velikim spremembam, pogojenim s prehodom na čistejšo energijo. Te se kažejo skozi vzpodbujanje rabe obnovljivih virov in prožnosti sistema ter razvoj novih poslovnih modelov, čemur sledijo spremembe v zakonodaji in zahteve po digitalizaciji in optimizaciji poslovnih procesov ter uvedbi dinamičnih modelov obračunavanja energije in usmerjanja porabe. Da bomo uspeli zadovoljiti potrebe našega primarnega trga, bo potrebnega obilo dela na področju razvoja informacijskih rešitev. Hkrati je to za nas priložnost za izboljšanje in širitev portfelja rešitev in storitev.

Med elementi ključne infrastrukture je energetika za kibernetske napade, druga najbolj izpostavljena panoga. Intenziv-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



na digitalizacija poslovanja in integracija operativnih in poslovnih sistemov pa ogroženost še povečujejo. Obstoječim uporabnikom varnostnega operativnega centra želimo priključiti še druge deležnike, predvsem s trga električne energije. Naš načrt je, da VOC v naslednjem obdobju preraste v sektorski operativni center za kibernetsko varnost z lastnim forenzičnim laboratorijem.

Tudi v prihodnje želimo svoje naročnike podpirati pri optimalnem poslovanju. Za shranjevanje in obdelavo velikih količin podatkov nekatere elektro distribucije že uporabljajo naše centralno podatkovno skladišče (cDWH) in rešitve podatkovne analitike. Še naprej bomo nadaljevali s pridobivanjem in posredovanjem sodobnih, naprednih znanj s tega področja. Ukvarjamo se s prediktivno analitiko za področje distribucije električne energije, razvijamo pa tudi kompetence in storitve na področju masovne obdelave podatkov in umetne inteligence (AI) ter strojnega učenja. Zaposleni in njihova znanja so in bodo za Informatiko zelo pomembni, zato bomo tudi v prihodnje aktivno dodajali manjkajoče kompetence, skrbeli za intenzivno izobraževanje in pridobivanje novih znanj, ki bodo potrebna v prihodnosti.

Digitalizacija in v zeleno usmerjen razvoj energetike vedno bolj izpostavlja pomen novih razvojnih momentov. Kateri so tisti razvojni načrti, ki jih želite v Informatiki nasloviti za hitrejše prilagajanje novim tehnološkim izzivom, ki so pred vami?

Harmonizacija lokalne zakonodaje z zahtevno EU zakonodajo na področju upravljanja z energijo se dotika tudi IT področja. Skupaj z elektrodistribucijskimi podjetji in energetskim sektorjem nasploh, se soočamo z vse večjimi potrebami po digitalizaciji celotnega delovanja, zaradi sprememb v dinamiki in naravi odjema in oddaje energije ter fleksibilnosti obračunavanja le-te. Za primer naj omenim izzive na področju elektrifikacije mobilnosti, konceptov samooskrbnih skupnosti in vpeljave novih akterjev na trg električne energije.

Spremembe povezane z načrtom zelenega prehoda in posledično z regulatornimi spremembami v načinu odjema električne energije zahtevajo vse hitrejše uvajanje vse obsežnejših sprememb na obstoječih rešitvah ter razvoj novih. Med projekti razvoja imajo najvišjo prioriteto tisti, s katerimi sistem eIS, to je informacijski sistem za podporo distribuciji in prodaji električne energije, prilagajamo zakonskim spremembam. Hkrati s tem uvajamo nove koncepte in tehnološko prenavljamo našo osrednjo aplikativno rešitev.

S celovitejšo digitalizacijo na prenovljeni digitalni platformi bodo elektro distribucije bolje pripravljene na nove izzive, ki jih prinašajo regulatorne spremembe na področju električne energije. Doprinesla bo k optimizaciji procesov do končnih strank, pri čemer bo skušala optimizirati tudi nekatere interne poslovne procese.

Informatika je že zelo uveljavljena v vlogi integratorja sistemov. Integracijska platforma, ki jo uporabljamo, je rezultat lastnega razvoja in je odlična os-

nova za boljše obvladovanje integracij z zagotavljanjem transparentnosti v komunikaciji med storitvami, varnosti pri posredovanju transakcij, zanesljivosti dostave sporočil, usmerjanja in podobnih storitev in kot takšna predstavlja našo konkurenčno prednost.

Informacijska varnost v zadnjem obdobju dobiva vedno pomembnejšo vlogo. V razvoju pametnih omrežij imajo distribucijska podjetja ključno vlogo. Kje vidite glavne izzive tega procesa?

Pametna omrežja (smart grids) prinašajo dodaten nivo kompleksnosti elektroenergetskemu omrežju. Uvajajo nove povezane naprave in nove tehnologije za prenos podatkov, ki v kombinaciji s podedovanimi sistemi predstavljajo nove možne točke kibernetskih napadov.

Poleg nadgradnje fizične infrastrukture, ki bo omogočala hitrejši prenos povečane količine podatkov, smo v slovenskem elektrodistribucijskem sistemu identificirali tudi potrebo po sodobni in celoviti rešitvi zagotavljanja kibernetske varnosti. Ta transformacija naj bi v prihodnjih letih nadgradila trenutne parcialne pristope, tako na področju zagotavljanja kibernetske varnosti, kot tudi neprekinjenega delovanja.

Poseben poudarek mora biti na zagotavljanju varne in zanesljive uvedbe nove tehnologije 5G, z novimi povezanimi napravami (internet stvari (IoT) in Industrijski internet stvari (IIoT)), ki bo sčasoma nadomestila obstoječo informacijsko podporo osrednjih procesov EDP ter jih nadgradila v kibernetsko varen in povezljiv celovit sistem upravljanja.



Eden od večjih izzivov bo povezovanje vseh procesov na področju zagotavljanja varnosti, vključno s fizičnimi in tehničnimi sistemi varovanja procesov in objektov EDP. Drugega izziva pa se zavedamo na človeški strani, kjer bo potrebno konstantno izobraževanje in osveščanje z namenom dvigovanja varnostnega zavedanja pri vseh deležnikih tega sistema.

Glavni rezultati bodo višja stopnja kibernetske varnosti, hitrejše uvajanje novih tehnologij in neprekinjenost ter obvladljivost delovanja.

V zadnjem obdobju so tudi distribucijska podjetja razumela potrebo po centralizaciji določenih aktivnosti na ravni zagotavljanja informacijske varnosti. Kje na tem področju vidite dodano vrednost, ki jo lahko prinese Informatika?

Naša družba deluje z roko v roki z naročniki pri zagotavljanju informacijske podpore v energetiki že več kot 50 let. Kot takšna dobro pozna delovanje energetskega sektorja v Sloveniji in ima potrebne kompetence in izkušnje za zagotavljanje rešitev za informacijsko varnost zanj.

Že nekaj desetletij se kontinuirano in uspešno ukvarjamo z varovanjem programske in strojne opreme, omrežij in podatkov. Tako skrb za varnost računalniških rešitev za nas ni nekaj novega. Večkrat smo že spreminjali, prilagajali in izboljševali oblike in metode varovanja v skladu z aktualnimi modeli poslovanja, ter standardi IKT in informacijske varnosti, saj si nenehno prizadevamo za ohranitev varnega okolja za naše stranke, partnerje, dobavitelje in zaposlene. Kibernetsko varnost na podlagi lastnih dolgoletnih izkušenj pojmujemo kot pomemben korak v evolucijskem procesu razvoja metodologij varovanja.

Izgradnja VOC za distribucijska podjetja je bil pomemben procesni in kadrovski zalogaj. Kje vidite glavne sinergije, ki jih bo prinesla ta storitev za celotno skupnost distribucijskih podjetij?

Varnostni operativni center zagotavlja skladnost z zakonodajo, zmanjšanje škode v primeru incidenta in podporo

neprekinjenemu poslovanju podjetja. Združevanje okrog sektorskega VOC zagotavlja vzpostavitev domensko specifičnih načinov varovanja, ki so bolj prilagojeni panogi in so zato bolj učinkoviti, tako z vidika rezultata, kot z vidika človeških in finančnih virov, ki so potrebni za zagotavljanje delovanja storitve 24/7.

Skupna infrastruktura pomeni prihranke na področju nabave strojne in programske opreme, na drugi strani pa zaradi majhnosti trga še vedno zagotavlja zadostne kapacitete za izvajanje optimalne zaščite.

S prenosom znanj in koncentracijo izkušenj omogočamo bolj zanesljivo prepoznavanje groženj s strani kibernetskih varnostnih strokovnjakov, saj je pri zagotavljanju najvišjega nivoja zaščite nujen holističen pristop. V praksi vektorji napada niso omejeni zgolj na eno področje. Pristop k kibernetski varnosti v svoji naravi tudi ne more in ne sme biti egoističen, saj temelji na sodelovanju z namenom varovanja vseh deležnikov. Poleg varnosti posameznega podjetja je smiselno zagotoviti varnost tudi vseh ostalih podjetij v verigi.

Katere so tiste glavne storitve, ki jih skozi VOC zagotavljate v tem trenutku in kakšni so vaši načrti za prihodnost?

Kibernetske ranljivosti so sistemski problem, ki zahteva strateški pristop s preventivnim nadzorom in dobro definiranim načrtom odzivov na napade in vdore v sistem. Ključno je, da tveganja obvladujemo centralno, ter da z varovanjem vseh informacijskih in infrastrukturnih virov na nivoju 24/7, zagotovimo visoko odpornost sistema in neprekinjeno delovanje. Takšen sistematičen pristop podpira tri stebre kibernetske varnosti, ki v varnostnem operativnem centru (VOC) združujejo tehnologijo, procese in ljudi.

Skupaj z našimi partnerji trenutno našim naročnikom zagotavljamo ključne storitve VOC, kot so zaznavanje in obravnavanje incidentov kibernetske varnosti, odkrivanje ranljivosti v informacijskih sistemih, izvajanje testov vdorov, definiranje varnostnih izhodišč za informacijske sisteme, poročanje incidentov deležnikom ter ozaveščanje in usposabljanje.

V zadnjih tednih so se zaostrile varnostne razmere na območju Ukrajine, in posledično med Rusko federacijo in državami EU. VOC Informatika pozorno in redno spremlja situacijo na področju kibernetske varnosti in dogajanje v naših omrežjih in omrežjih EDP, ter redno preverja potencialno nevarne dogodke.

Strategijo, procese in storitve kibernetske varnosti v okviru VOC bomo neprenehno in smiselno nadgrajevali in širili v skladu z rastjo potreb poslovnega okolja in sistemov, ki jih varujemo, kakor tudi v skladu z uveljavljenimi standardi ter najaktualnejšimi tehnologijami za proaktivno zagotavljanje kibernetske varnosti. Na ta način bomo v podjetju kontinuirano dvigovali zrelostni nivo kibernetske varnosti in delovanja VOC ter stremeli k izpolnjevanju cilja, da postanemo verodostojen in vodilen člen ter partner pri udejanjanju celostne kibernetske varnosti v nacionalnem sistemu kritične infrastrukture za sektor energetike ter širše.

Menite, da bo v prihodnosti potrebno določene procese v okviru zagotavljanja varnosti energetske kritične infrastrukture še bolj združevati?

Prav gotovo je usklajeno odzivanje na znane grožnje ter prepoznavanje le teh iz zaznanih vzorcev, ne le pri sebi, temveč tudi pri ostalih deležnikih v sistemu, bolj učinkovito, kot parcialno delovanje, v sklopu le enega podjetja. Različna elektrodistribucijska podjetja namreč uporabljajo podobne sisteme in rešitve, vključno s fizično opremo, kot so pametni števci, in telekomunikacijskimi povezavami. Ranljivosti in možne točke napada so podobne. Vemo, da večji kibernetski napadi ciljajo na celotne sisteme in usklajeno odzivanje vseh deležnikov. To je gotovo bolj učinkovito, tako z vidika rezultatov, kot stroškovno.

Združevanje okrog sektorskega varnostnega operativnega centra zagotavlja vzpostavitev domensko specifičnih načinov varovanja, ki so bolj prilagojeni panogi in so zato bolj učinkoviti. Prav zato želimo pridobiti še kakšnega drugega deležnika iz energetskega sektorja in s tem razširiti poznavanje segmenta in zagotavljati širši nivo varnosti. Saj poznavanje celotnega segmenta zagotavlja zanesljivejše in hitrejše prepoznavanje vektorjev napada in s tem zagotavlja boljšo obrambo posameznikov.

V zadnjem obdobju aktivno sodelujete na EU raziskovalnih projektih. Kaj za vašo organizacijo prinašajo te projekti in kakšni so vaši načrti za prihodnost?

Pri razmišljanju o sodelovanju na EU raziskovalnih in razvojnih projektih iščemo predvsem področja, kjer lahko s sodelovanjem pridobimo nova znanja, gradimo mednarodne povezave in sklepamo poslovna partnerstva za zagotavljanje podpore našim obstoječim in potencialnim naročnikom na slovenskem elektroenergetskem trgu v času spreminjajočih se modelov oskrbe z električno energijo.

Tako trenutno sodelujemo v projektu CyberSEAS (Cyber Securing Energy dAta Services) programa Horizon 2020. Skupaj s 25 partnerji iz 10 držav iščemo in razvijamo rešitve za dvig odpornosti verig oskrbe z energijo in njihovo zaščito pred motnjami. Za energetske oskrbne verige so namreč značilni podedovani sistemi, ki se vse bolj povezujejo z različnimi podatkovnimi viri. To dejstvo izkoriščajo napadalci z zapletenimi scenariji napadov tako na energetsko omrežje, kot na vire podatkov in še posebej osebne podatke.

Tudi v prihodnje nameravamo sodelovati na projektih, ki lahko prinesejo dobrobit za naše naročnike in slovenski elektroenergetski prostor na splošno, tako na področju kibernetske varnosti, kot na področjih povezanih z aktivnim odjemom in pametnim upravljanjem z energijo.

Informatika je že vrsto let korporativni član Slovenskega združenja korporativne varnosti. Kaj so tisti pozitivni dejavniki, ki vam jih prinaša omenjeno strokovno združenje?

Članstvo v Slovenskem združenju korporativne varnosti nam prinaša mreženje s potencialnimi poslovnimi partnerji in široke možnosti izmenjave znanja in dobrih praks s podjetji z našega, pa tudi iz drugih gospodarskih sektorjev, kar je pogosto še bolj dragoceno, saj si s tem širimo obzorja in spoznavamo nove načine razmišljanja, ki nam bodo gotovo prišli še kako prav v prihodnosti, ko se bodo različni sistemi med seboj vse bolj povezovali in bo zagotavljanje informacijske in kibernetske varnosti še bolj zahtevno in hkrati pomembno. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Gregor Janc, direktor Korporativne varnosti v Telekomu Slovenije*

KORPORATIVNA VARNOST NUJEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE

V današnjem poslovnem okolju ustrezna organizacijska in poslovna umeščenost korporativne varnosti odraža zavedanje strateškega managementa o pomembnosti upravljanja poslovnih tveganj, zagotavljanja neprekinjenosti delovanja ključnih procesov in infrastrukture, predvsem pa prinaša dodano vrednost poslovanja.

Pred časom ste prevzeli vodenje korporativne varnosti v Telekomu Slovenije. Nam lahko poveste, katera so ključna področja vaših pristojnosti?

Ključni področji, ki sodita v pristojnost organizacijske enote Korporativna varnost v Telekomu Slovenije, sta splošna varnost in informacijska varnost. Pod pojmom splošna varnost razumemo zagotavljanje varovanja ljudi in premoženja družbe, oblikovanje varnostnih standardov v Skupini Telekom Slovenije ter obravnava varnostnih incidentov s tega področja. Področje informacijske varnosti pa vključuje oblikovanje politik, smernic, navodil, dobrih praks in nadzornih postopkov za zagotavljanje informacijske varnosti, vključno z izvajanjem postopkov na področju upravljanja neprekinjenega poslovanja in varovanja informacij družbe.

Zaposleni v Korporativni varnosti smo pristojni tudi za izvajanje zakonskih določb z našega področja.

Lahko naredite kratko primerjavo v oceni dinamike korporativnega okolja glede na pretekle izkušnje okolij, kjer ste prej opravljali svojo profesionalno pot.

Za uspešno delovanje na trgu so pomembni inovativni pristopi, uporaba najmodernejših tehnologij, skrb za varnost ter nenehen razvoj novih storitev

Dinamika je podobna, pri čemer obstaja razlika z vidika objekta varovanja. V Skupini Telekom Slovenije, poleg Slovenije prek odvisnih družb delujemo tudi v nekaterih drugih državah – na Kosovu, na Hrvaškem, v Bosni in Hercegovini, v Srbiji in Severni Makedoniji.

Telekom Slovenije predstavlja del pomembne infrastrukture na področju sektorja telekomunikacij. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Omrežje Telekoma Slovenije je že 30 let vodilno omrežje Slovenije, ki zagotavlja zanesljivo, stabilno in varno povezljivost največjih hitrosti. Telekom Slovenije ima tako največje mobilno omrežje z največ baznimi postajami, kot največje optično omrežje. To terja neprestano ocenjevanje, spremljanje ter odzivanje na tvega-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

nja, saj naše omrežje vsak dan uporablja okoli milijon uporabnikov. Telekom Slovenije je z vidika uporabnikov tudi najbolj zaupanja vreden ponudnik mobilnih in internetnih storitev, kar potrjuje priznanje Trusted Brand.

Zagotavljanje varnosti in razpoložljivosti tako pomembne infrastrukture je kompleksno, zahtevno in odgovorno. Zato zagotavljamo zanesljivo delovanje storitev in procesov, ter hiter in učinkovit odziv ob izrednem dogodku, kar pomeni tudi manjše tveganje za daljši izpad storitev in procesov. Zagotavljanje zanesljivosti delovanja in v primeru izpada storitev hitrega okrevanja dokazujemo z mednarodnim standardom ISO 22301:2012 (sistem upravljanja neprekinjenega poslovanja), ki smo ga kot prvi v Sloveniji prejeli leta 2016 in ga skozi leta ohranjamo.

V okviru Korporativne varnosti smo zadolženi tudi za pripravo ocen tveganja in izvedbo ukrepov za zaščito infrastrukture. V tem delu je zelo pomembno dobro sodelovanje z državnimi organi, ki usmerjajo in zagotavljajo enovit pristop. Seveda pa izvajanje stalnih in dodatnih ukrepov za družbo predstavlja finančno obremenitev, zato nas veseli, da predlog direktive Evropskega parlamenta in Sveta EU o odpornosti kritičnih subjektov omogoča dodatno financiranje za povečanje odpornosti gospodarskih subjektov, ki ga bo zagotovila Evropska komisija.

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

Za uspešno delovanje na trgu so pomembni inovativni pristopi, uporaba najmodernejših tehnologij, skrb za varnost ter nenehen razvoj novih storitev. Pomena varovanja informacij se dobro zavedamo, zato smo vzpostavili in certificirali tudi sistem upravljanja varovanja informacij. Sprejeto imamo politiko varovanja informacij, neprestano izvajamo ukrepe za zagotavljanje varnosti informacij.

Vsak zaposleni je dolžan v okviru opravljanja del in nalog oziroma svojih pristojnosti varovati podatke, ki predstavljajo poslovno skrivnost skladno z internim aktom, ki ureja varovanje poslovne skrivnosti. To pomeni izvajanje ukrepov in postopkov, da se nepooblaščeni osebi prepreči seznanitev s poslovno skrivnostjo.

Menim, da bi morale družbe, ki v državi zagotavljajo ključne procese in storitve, svoje varovanje zagotavljati le s standardiziranim varnostnim nadzornim centrom, saj lahko le na ta način zagotavljamo enotnost in ustrezen nivo varnosti.

V sistemu ustreznega obvladovanja tveganj ima Varnostno nadzorni center v Telekomu Slovenije izredno pomembno vlogo. Nam lahko zaupate, kako pomemben je za delovanje tega centra proces standardizacije.

Varnostno nadzorni center je srce varnostnega sistema. Standardizacija je ključnega pomena za zagotavljanje varnega, učinkovitega in hitrega odzivanja na varnostne dogodke. Telekom Slovenije ima Varnostno nadzorni center standardiziran skladno s standardom EN 50518:2013. Menim, da bi morale družbe, ki v državi zagotavljajo ključne procese in storitve, svoje varovanje zagotavljati le s standardiziranim varnostnim



Proaktivnost Slovenskega združenja korporativne varnosti, ki s svojimi rednimi oblikami združevanja strokovnjakov k temu prispeva največ v slovenskem prostoru, je lahko zgled tudi drugim panogam.



nadzornim centrom, saj lahko le na ta način zagotavljamo enotnost in ustrezen nivo varnosti.

Kako pristopate k preprečevanju kibernetskih tveganj, ki so v vaši dejavnosti zelo izpostavljena?

Kibernetska varnostna tveganja sodijo med najpomembnejša operativna tveganja, zato temu področju namenjamo zelo veliko pozornosti. Vzpostavljen imamo najsodobnejši Operativni center kibernetske varnosti, ki je prejel tudi nagrado za najbolj inovativno varnostno rešitev, v katerem storitve izvajamo tako za lastne potrebe kot za ostale organizacije in podjetja. Center je certificiran tudi po mednarodnem standardu za informacijsko varnost ISO 27001.

Področje kibernetske varnosti sicer nenehno krepimo tako, da vlagamo v nadgradnjo tehnologij za natančnejše zaznavanje dogodkov, poglobljeno analitiko, povečanje stopnje avtomatizacije operativnih procesov, ter opravljamo različna varnostna in vdorna testiranja. V prihodnje bomo vlagali tudi v varnostne rešitve tehnologije umetne inteligence. Med naše redne aktivnosti sicer sodijo osveščanje, izobraževanje in širjenje kompetenc zaposlenih, posodabljanje pravil in protokolov (tudi s pomočjo zunanjih pregledov) ter re-certifikacija.

Kakšno je vaše sodelovanje s tujimi operaterji na področju zagotavljanja varnosti in predvsem preprečevanja zlorab informacijskih poti?

Za učinkovito preprečevanje zlorab je potrebno sodelovanje vseh deležnikov. Telekom Slovenije pri tem aktivno sodeluje v združenju GSMA (Global System for Mobile Communications Association) in znotraj njega v skupini za zlorabe in varnost (Fraud and Security Group). Prav tako smo partnerji agencije Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj – Europol, kjer strokovnjaki aktivno sodelujejo v okviru European Cybercrime Centre (EC3), kot člani svetovalne skupine ponudnikov komunikacijskih storitev (Advisory Group Communication Providers). S sodelovanjem v teh skupinah, katerih člani so tudi ostali večji evropski operaterji in ponudniki storitev, pridobivamo ter si izmenjujemo informacije, izkušnje in dobre prakse pri zgodnjem zaznavanju in preprečevanju novih načinov zlorab in napadov v telekomunikacijskih sistemih in omrežjih.

Pri zagotavljanju varnosti in preprečevanju zlorab je pomembna tudi vloga BEREC (Body of European Regulators for Electronic Communications).

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

Zagotovo. Znanje je poleg izkušenj eden od osnovnih pogojev za uspešno delovanje v katerikoli dejavnosti. Zato mora biti kontinuirano izobraževanje ter pridobivanje novih znanj in kompetenc, sestavni del posameznikovega karierenega razvoja. V Telekomu Slovenije se tega zavedamo in imamo vzpostavljen celovit sistem izobraževanj za razvoj zaposlenih. Da smo na tem področju uspešni, nenazadnje potrjuje tudi priznanje TOP Employer, ki ga je Telekom Slovenije prejel za leto 2022. Priznanje Top Employer predstavlja mednarodni strokovni standard na področju prepoznavanja odličnosti praks, ki jih podjetja izvajajo za svoje zaposlene. V to je vključeno tudi skrbno in odgovorno upravljanje s kadri na področju izobraževanja.

Telekom Slovenije s svojimi izkušenimi strokovnjaki v okviru Izobraževalnega centra izvaja izobraževanja tudi za druge organizacije in podjetja. Aktivno sodelujemo tudi z Institutom za korporativne varnostne študije.

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

Zavedanje o pomenu varnosti je vedno boljše, kljub temu pa skozi pogovore še vedno kdaj dobim občutek, da se na področju varnosti v nekaterih podjetjih ali organizacijah varčuje. Vsi, ki se ukvarjamo z varnostjo, moramo krepiti zavedanje o pomenu varnosti in to zavedanje dvigniti še na višjo raven. Z varnostjo se ne smemo pričeti ukvarjati takrat, ko jo izgubimo. Nenazadnje – v zadnjem obdobju smo bili priča kar nekaj odmevnim kibernetskim napadom tako pri nas kot v naši okolici. Varčevanje na področju zagotavljanja varnosti nas lahko stane ogromno.

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

Združevanje strokovnjakov s področja korporativne varnosti je neprecenljivo, saj omogoča izmenjavo dobrih praks in inovativnih rešitev pri zagotavljanju varnosti ter tako skupen napredek na tem področju. Proaktivnost Slovenskega združenja korporativne varnosti, ki s svojimi rednimi oblikami združevanja strokovnjakov k temu prispeva največ v slovenskem prostoru, je lahko zgled tudi drugim panogam. ■

Foto: arhiv Telekom Slovenije

13. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

31. MAJ - 1. JUNIJ 2022



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!

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Thomas Tomsich, direktor Zarja Elektronika d.o.o.*

PODROČJE TEHNIČNEGA VAROVANJA IMA ŠE VEDNO POMEMBNO MESTO V SISTEMU INTEGRALNE VARNOSTNE ZAŠČITE

Sistemi tehničnega varovanja, med katerimi imajo pomembno mesto protipožarni sistemi, predstavljajo pomemben temelj vsakega integralno varnostnega sistema v različnih organizacijah. Sinergija in priložnosti na tem področju predstavljajo dodatno motivacijo za razvojne korake podjetja Zarja Elektronika.

Najprej vam izrekamo čestitke ob ponovnem imenovanju na mesto direktorja Zarja Elektronika. Zarja Elektronika je v svojem razvoju prehodila pomembne razvojne korake. Kateri so tisti razvojni momenti, ki bi jih skozi preteklo obdobje izpostavil kot tiste ključne, na katerih bo temeljil tudi nadaljnji razvoj vašega podjetja?

Zahvaljujem se vam za čestitke. Zarja Elektronika je v vseh letih svojega obstoja oziroma delovanja dosegla pomembne razvojne cilje. Z vztrajnim delom, lastnim znanjem in razvojem, nenehnim strokovnim izpopolnjevanjem, sledenjem svetovnim trendom in izvedbo tehnično najzahtevnejših projektov se je razvila v dinamično vodilno strukturo z več kot 90 zaposlenimi.

V zadnjem obdobju je prišlo tudi do lastniških sprememb v Zarji Elektroniki. Take spremembe po navadi za seboj potegnejo tudi določene spremembe pri strategiji razvoja podjetja. Kje bodo tista nova težišča, ki bodo naredila podjetje še bolj prodorno na zahtevnem tržišču?

Kakor veste je pred kratkim prišlo do prevzema s strani skupine MSIN d.o.o., družbe za svetovanje in investiranje, ki preko upravljavskih deležev oziroma mreže lastništva in na podlagi skrbno načrtovane strateške politike, med drugim obvladuje tudi znani CETIS d.d., družbo ŽIMA tovarna ščetk d.d. in družbo KREMEN d.o.o., industrija in rudniki nekovin. Skupaj s povezanimi slovenskimi in tujimi gospodarskimi subjekti družba MSIN d.o.o. zaposluje preko 1000 delavcev. Prošnjo novih lastnikov po nadaljnjem sodelovanju sem z veseljem sprejel, saj tukaj vidim veliko izzivov, priložnosti in novih projektov za naprej in sicer ne samo v Sloveniji, ampak tudi v mednarodnih vodah.

Boste na podlagi nove strategije širili svoje delovanje tudi na druge segmente poleg sistemov požarne varnosti ali boste poskušali slediti še večji specializaciji in tržnemu deležu na tem specifičnem segmentu?

Zarja Elektronika je v Sloveniji znana kot ena od vodilnih družb na področju tehničnega varovanja. Kot proizvajalec in ponudnik storitev tehničnega varovanja se prilagaja uporabnikovim željam in potrebam »po meri kupca«.

Ena od ključnih strategij je, še dodatno ojačati naš položaj h kupcu usmerjenega podjetja z oblikovanjem prijaznih, dostopnih, preglednih in učinkovitih stori-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



tev na vseh segmentih tehničnega varovanja, vključno z ustreznimi deležniki ter hkratnim izkoriščanjem možnosti digitalizacije, ki predstavlja ključen premik k večji konkurenčnosti.

Verjetno lahko pričakujemo, da bo Zarja Elektronika vedno bolj usmerjena tudi v širjenje svoje dejavnosti v širšem regijskem prostoru izven Slovenije? Boste v novi viziji temu segmentu namenili dodaten strateški potisk?

Osebno pričakujem konsolidacijo naše panoge v celotni regiji in v Evropi. Trendi v zadnjih 3 letih (Covid-19 in Ukrajinska kriza) kažejo na korenite spremembe zlasti v demografskih gibanjih, pritiskih na dobavne verige, tekmovanju za svetovne vire in gospodarskem razvoju.

Spoprijemamo se z grožnjo strukturnega upočasnjevanja svetovne gospodarske rasti, zato je nujna pospešena rast produktivnosti, razvoja novih modelov poslovanja in delovnih mest, kar zahteva razvoj novih znanj in veščin ter prilagoditve na številnih področjih gospodarskega, družbenega in okolijskega razvoja.

Z lanskim letom smo postali 100% lastniki hrvaškega podjetja za tehnično varovanje Tehnomobil Elsting s katerim nadaljujemo strategijo širitve naše prisotnosti v regiji. V prihajajočem obdobju bomo v podjetju dali še več poudarka na strateško povezovanje s partnerji na različnih področjih tako doma kot v tujini, s ciljem širjenja našega razvoja in poslovanja. Visoko rast izvoza planiramo predvsem v Veliko Britanijo in v Avstrijo.

Sodelovanje, odprtost in povezanost na nacionalni, regionalni in evropski ravni so tako čedalje pomembnejša. Naše poslanstvo je postati quality leader na področju tehničnega varovanja.

Tehnološki razvoj bo verjetno tudi v prihodnje izredno pomemben temelj vaše konkurenčnosti. Nam lahko zaupate kakšne smele korake boste izvajali na tem področju?

Drzni koraki – v tem trenutku pripravljamo razvojni načrt na podlagi potreb trga, kamor vključimo naše poslovne partnerje, ki nam dajejo dragocen »input« na podlagi njihovih izkušenj in na podlagi prihodnjih načrtov. Preučujemo tudi razvojno partnerstvo s portugalsko firmo Global Fire Equipment, prav tako z naše panoge.

Kadri so tisti ključni del vsake organizacije. Pri določenih transformacijah podjetja nas vedno najbolj skrbi kako zadržati ključne kadrovske vire. Verjamemo, da boste temu področju tudi v prihodnosti namenili posebno pozornost?

Res je, dobro počutje je naša dnevna skrb, zadovoljstvo in razvoj vseh zaposlenih pa prioriteta, če želimo realizirati visoko zastavljene cilje razvoja podjetja. Ker smo pred kratkim postali del skupine MSIN, nam je trenutno najbolj pomembno, da delovanje organiziramo z novo sistemizacijo in novim plačnim modelom, ki bo predvideval tudi ciljno vodenje in razvoj kompetenc zaposlenih. Kot del skupine, bomo spremljali zadovoljstvo zaposlenih in na podlagi dobljenih rezultatov planirali in izvajali potrebne programe in aktivnosti, ki bodo omogočali rast, razvoj in s tem zadržali sodelavce.

Zarja Elektronika je že vrsto let pomembna članica v Slovenskem združenju za korporativno varnost. Kaj tako strokovno združevanje prinaša vašemu podjetju in ali boste tudi vnaprej tako aktivni pri sodelovanju in razvoju te asociacije?

ICS vidimo kot enega najpomembnejših partnerjev. Z ICS sodelujemo že več let in pričakujemo, da bomo tudi vnaprej tesno sodelovali. Veliko eminentnih podjetij, kot je na primer ELES d.o.o., ki je tudi naš dolgoletni poslovni partner, je včlanjenih v to združenje, zato smo ponosni, da imamo tudi mi možnost sodelovanja. ■

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.

INFORMATIKA



Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

Med elementi ključne infrastrukture je energetika druga najbolj izpostavljena panoga, trendi intenzivne digitalizacije poslovanja in integracije operativnih in poslovnih sistemov pa izpostavljenost kibernetskim napadom še povečujejo.

Vplivi kibernetskih napadov na različna področja v energetiki:

PROIZVODNJA
Prekinitve storitev in napadi z izsiljevalsko programsko opremo (ransomware) na elektrarne in alternativne proizvajalce energije.

Možni vzroki:
zastareli sistemi za proizvodnjo in razvijajoča se infrastruktura čiste energije, zasnovana brez upoštevanja varnosti.

PRENOS
Hude motnje v dostavi energije odjemalcem s prekinitvami delovanja storitev na daljavo.

Možni vzroki:
pomanjkljivosti fizičnega varovanja omogočajo dostop do sistemov za nadzor omrežja.

DISTRIBUCIJA
Motnje v delovanju razdelilnih postaj, ki vodijo do regionalnih motenj v distribuciji in prekinitve delovanja storitev za odjemalce.

Možni vzroki:
porazdeljeni energetski sistemi in omejeni mehanizmi varnosti vgrajeni v SCADA sisteme.

PORABNIKI
Kraja podatkov o uporabnikih, prevare na področju podatkov o porabi in motnje v delovanju storitev.

Možni vzroki:
veliko tarč za napade z razširjeno mrežo različnih IoT naprav, vključno s pametnimi števci in električnimi vozili.

ČAS JE ZA ODLOČILEN KORAK

INFORMATIKINI strokovnjaki lahko pomagamo pri vzpostavitvi sodobnega sistema aktivne zaščite pred kibernetskimi in drugimi grožnjami, ki temelji na ključnih storitvah **VOC**:

- zaznavanje in obravnavanje incidentov kibernetske varnosti,
- odkrivanje ranljivost v informacijskih sistemih,
- izvajanje testov vdorov,
- vzpostavitev sistemov vab,
- modeliranje groženj,
- preverjanje izvorne kode,
- definiranje varnostnih izhodišč za informacijske sisteme,
- preverjanje prisotnosti in analiza škodljive kode,
- poročanje incidentov deležnikom ter
- ozaveščanje in usposabljanje.

VOC zagotavlja skladnost z zakonodajo, zmanjšanje škode v primeru incidenta in podporo neprekinjenem poslovanju podjetja. Združevanje okrog sektorskega varnostnega operativnega centra zagotavlja vzpostavitev domensko specifičnih načinov varovanja, ki so bolj prilagojeni panogi in so zato bolj učinkoviti.

VOC INFORMATIKE temelji na najnovejših tehnoloških rešitvah in vrhunskih produktih vodilnih svetovnih proizvajalcev.

www.informatika.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Franc Pavlin, direktor Službe za korporativno varnost in nadzor poslovanja, Petrol d.d.*

UČINKOVITOST ORGANIZACIJE POVEZANA Z USTREZNO ORGANIZIRANOSTJO KORPORATIVNE VARNOSTI

Korporativna varnost in nadzor poslovanja predstavljata ključno orodje za obvladovanje tveganj v kompleksnih poslovnih organizacijah. O glavnih izzivih varnostnega okolja v katerem posluje naša najpomembnejša energetska družba smo se pogovarjali z g. Francom Pavlinom.

V svoji dolgoletni karieri ste delovali v različnih organizacijskih sredinah, v katerih je bilo obvladovanje varnostnih tveganj pomemben segment vaših strokovnih prizadevanj. Nam lahko zaupate katere izkušnje preteklih organizacijskih okolij vam bodo najbolj pomagale pri nadaljnjih izzivih, ki ste jih našli v Petrolu?

Upam si trditi, da sem v svoji 31-letni policijski karieri, skozi operativno delo na različnih delovnih področjih, pridobil veliko izkušenj in strokovnih kompetenc. Kariero sem začel kot policist na največji policijski postaji v Republiki Sloveniji, nadaljeval kot kriminalist na področju organiziranega kriminala in preprečevanja korupcije ter jo zaključil na delovnem mestu vodje Sektorja za notranje preiskave in integriteto. Dolga leta dela v policiji sem bil tudi pripadnik Posebne policijske enote in sem veteran osamosvojitvene vojne. Na novi karierni poti mi bodo prišle prav vse operativne izkušnje, ki sem jih skozi leta operative pridobival v policiji. Najbolj pa definitivno zadnje trinajstletno vodenje službe notranje varnosti na Generalni policijski upravi.

Ob vašem prihodu ste v Petrolu tudi resno postavili glavne strateške temelje za Službo korporativne varnosti. Kateri so tisti glavni procesi s katerimi bo v svojem delokrogu upravljala vaša služba?

Ključni procesi, ki jih zagovarjamo in postavljamo z ekipo, temeljijo na zagotavljanju varnosti naših zaposlenih in naših poslovnih partnerjev, zaščiti naših objektov oz. premoženja in omogočanju uspešnega ter transparentnega poslovanja naše družbe. Specifičnost naše službe se odraža skozi izvajanje nadzorne dejavnosti, in sicer tako nad poslovanjem samim, kakor tudi preko nadzora transportne verige. Pri izvajanju nadzorne dejavnosti si pomagamo s postopki notranjih preiskav. Namen le teh je pravočasno preprečevanje odklonskih pojavov in zagotavljanju visokih standardov osebnostne integritete zaposlenih, organizacijske integritete ter preprečevanju krnitve ugleda naše družbe. Nenazadnje mi je poslovodstvo, poleg vodenja štabne službe Korporativna var-

> Obvladovanje tveganj v trenutno poslabšanih varnostnih razmerah bo zame in moje sodelavce velik izziv. V tem trenutku si želim še boljšega medsebojnega sodelovanja in izmenjave podatkov s kolegi, ki se ukvarjamo s korporativno varnostjo.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

nost in nadzor poslovanja, zaupalo tudi mandat pooblaščenca za integriteto za celotno skupino Petrol.

Na področju notranjih preiskav imate bogate izkušnje. Bo temu procesu tudi v Petrolu namenjen določen del vaših strokovnih naporov?

Vsekakor. Kot sem omenil, smo z ekipo sodelavcev v policiji v trinajstih letih naredili ogromno. Tako na področju preiskovanja kaznivih ravnanj, ki so jih bili osumljeni uslužbenci policije, kakor tudi na področju preprečevanja odklonskih pojavov. Z našim delom smo veliko doprinesli k dvigu standardov policijske integritete in ugledu slovenske policije, tudi v tujini. Moram biti pošten in povedati, da je k naši uspešnosti pripomoglo tudi delo naših predhodnikov, ki so pred nami izvajali notranjo zaščitno dejavnost. In ja. V proces zagotavljanja korporativne varnosti v skupini Petrol, skozi izvajanje nadzorne dejavnosti in notranjih preiskav, že prenašam strokovne izkušnje oz. operativno prakso zagotavljanja notranje varnosti. To je bil tudi moj namen ob prihodu v povsem novo organizacijsko okolje. Večina kolegov, ki izvaja to dejavnost, sicer nima operativnih izkušenj, ki so potrebne za uspešno izvajanje posameznih postopkov in ukrepov, če želimo, da je neka preiskava učinkovita. Vendar bomo ta primanjkljaj z različnimi oblikami usposabljanja, predvsem pa ravno s prenosom operativnih izkušenj s časom odpravili.

> V začetku si nisem predstavljal takšne vsebinske veličine in takšne strokovne širine združenja. Ključno poslanstvo združenja je ravno to, kar sem že omenjal, strokovno povezovanje in medsebojna izmenjava izkušenj.

Ustrezno sodelovanje in podpora strateškega vodstva je ključna za učinkovitost delovanja korporativne varnosti. Ocenjujete, da imate ustrezno podporo za izvajanje svojega poslanstva?

Samo v okolju, kjer ima takšna služba podporo strateškega managementa, je lahko delovanje korporativne varnosti oz.



zagotavljanje notranje varnosti učinkovito. V kolikor vodstvo podjetja v organizaciji, jasno in konkretno ne podpira takšne službe, ali da je do njenih postopkov pasivno, potem je služba sama sebi namen in ni učinkovita. Pa naj si bo to gospodarska družba ali državni organ. Lahko povem, da z ekipo trenutno uživamo popolno zaupanje poslovodstva in smo pri svojem delu popolnoma avtonomni.

Kadri so eden od pomembnih izzivov s katerimi se v zadnjem obdobju ukvarjajo praktično vse organizacije. Kakšna je vaša vizija pri kadrovski krepitvi Služb za korporativno varnost?

Ocenjujem, da smo po obsegu in po vsebini procesov, ki so, če se lahko tako izrazim, v skrbništvu naše štabne službe, s trenutno kadrovsko zasedbo učinkoviti pri zagotavljanju notranje varnosti v celotni skupini Petrol. Obseg in območje dela sta se nam samo na ozemlju R Hrvaške znatno povečala, kar je posledica nakupa družbe Crodux. Po procesu integracije smo s prvim marcem pričeli s priklapljanjem Croduxovih prodajnih mest v Petrolov informacijski sistem. Ključno vlogo pri tem je imela tudi naša služba. Zaradi logičnosti povečanja tveganj smo trenutno v fazi povečevanja strokovnega teama korporativne varnosti na hrvaškem trgu, ki bo tudi v prihodnje strokovno usmerjan neposredno iz naše službe in voden po modelu funkcijske odgovornosti. Glede na strategijo naše družbe in pričakovanemu širjenju oz. povečevanju poslovanja tudi v R Srbiji, R BIH in Črni gori, bomo na področju korporativne varnosti sorazmerno potrebam, krepili tudi kadrovski potencial. Dosedanja analiza tveganj in trenutni potencialni viri ogroženosti našega poslovanja, mi že sami po sebi ponujajo odgovor, da bom v prihodnje potrebne kadre verjetno poskušal pridobiti iz policije ali iz preostalih struktur nacionalno varnostnega sistema. Verjetno podobno razmišljajo tudi moji kolegi v podobno velikih gospodarskih družbah. Trenutne globalne varnostne razmere bodo to potrebo samo še bolj potrjevale.

Mreža poslovalnic s katerimi upravlja Petrol je zelo razvejana. Zelo močno ste razširjeni tudi v regiji. Kateri so tisti izzivi obvladovanja tveganj, katerim bo v prihodnjem obdobju potrebno posvetiti posebno pozornost?

Samo za predstavo, da smo res veliki. Na območju Slovenije in na prej omenjenih območjih JV trgov imamo skupaj 594 prodajnih mest oz. bencinskih servisov. Večje število celinskih in morskih skladišč fosilnih goriv, več skladišč utekočinjenega naftnega plina, lasten laboratorij ter številne druge objekte. Naši posamezni objekti se uvrščajo pod t.i. državno kritično infrastrukturo. Naša prioriteta bo v prvi vrsti še vedno zagotavljanje varnosti zaposlenih, visok nivo zaščite omenjenih objektov in varovanje poslovnih podatkov ter zagotavljanje neprekinjenega poslovanja. Obvladovanje tveganj v trenutno poslabšanih varnostnih razmerah bo zame in moje sodelavce velik izziv. V tem trenutku si želim še boljšega medsebojnega sodelovanja in izmenjave podatkov s kolegi, ki se ukvarjamo s korporativno varnostjo.

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

Kibernetski varnosti dajemo v skupini Petrol velik poudarek. Imamo posebej formiran team, ki se brez prestanka ukvarja zgolj in samo z informacijsko varnostnimi procesi. V Petrolu si namreč ne moremo in ne smemo privoščiti izpada naše informacijske mreže, preko katere upravljamo celotno preskrbovalno verigo z gorivi. Do pred kratkim smo zagotavljanje informacijske varnosti ocenjevali kot visoko učinkovito. Da ne bo pomote, jo tudi sedaj. Vendar trenutne varnostne razmere in informacije, ki jih dnevno dobivamo, kažejo na to, da je grožnja kibernetskih napadov na območju Evropske unije na žalost vedno bolj pričakovana realnost. Tudi na tem varnostnem izzivu pričakujem maksimalno sodelovanje in sprotno izmenjavo ključnih podatkov, tudi s pristojnimi službami nacionalno varnostnega sistema RS.



Ste tudi zelo močno vpeti v raziskovalne projekte na področju zaščite kritične infrastrukture in kibernetske varnosti. Kakšno dodano vrednost vam prinaša tako sodelovanje?

Odkar sem v Petrolu, sodelujem v drugem raziskovalnem projektu, ki ga financira EU. Tako imenovani Infrastress projekt je v celoti usmerjen ravno k iskanju izboljšav, odpornosti in učinkoviti celoviti zaščiti kritične infrastrukture. Ravno nabor strokovnjakov iz različnih delovnih področij in iz različnih podjetij, ki so skrbniki kritične infrastrukture, njihova oz. naša medsebojna izmenjava različnih izkušenj pri zagotavljanju varnostnih izzivov, meni osebno in verjetno tudi kolegom, ki sodelujejo v istem projektu, predstavlja največjo dodano vrednost zaščite kritične infrastrukture. Jasno je, da nas vse ogrožajo enaki viri, enaka tveganja in v primeru ranljivosti se bomo prav vsi srečali z enakimi posledicami.

Kako ocenjujete vaše dosedanje delovanje v okviru Slovenskega združenja korporativne varnosti?

Sodelovanje v okviru združenja ocenjujem za več kot odlično. Kmalu po mojem prihodu na Petrol, sem se hitro odzval povabilu in se vam pridružil. V začetku si nisem predstavljal takšne vsebinske veličine in takšne strokovne širine združenja. Ključno poslanstvo združenja je ravno to, kar sem že omenjal, strokovno povezovanje in medsebojna izmenjava izkušenj. In če zaključim. Mi je v čast, da sem lahko eden izmed vas. Hvala vam za vso vašo dosedanjo pomoč. ■

Foto: Boštjan Vihtelič

DIGITALNI SISTEM ZAKLEPANJA ZA KRITIČNO INFRASTRUKTURO

Lastno napajanje – mobitel kot ključ in vir energije (NFC tehnologija) ali digitalni ključ (kinetična energija).

Oddaljeno upravljanje avtorizacij, časovnih profilov in drugih funkcij preko SaaS iLOQ Manager programske opreme.
Visoka varnost prenosa in enkripcije podatkov (PKI in AES–256 šifriranje).
Odpornost na ekstremne vremenske razmere.
Centralizirano upravljanjem oddaljenih objektov v realnem času.



BREZ BATERIJ IN KABLOV • BREZ STROŠKOV VZDRŽEVANJA • ZELENA REŠITEV

Na voljo širok nabor komponent: digitalni cilindri, polcilindri, pohištvene ključavnice, obešanke, zidni trezorji ter RFID in PIN čitalci za celovito kontrolo pristopa na vseh vrstah objektov.



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

iLOQ

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
David Krajnc, direktor Službe korporativne varnosti in nadzora v Pošti Slovenije*

POŠTA SLOVENIJE PRIPRAVLJENA NA NOVE VARNOSTNE IZZIVE PRIHODNOSTI

Pošta Slovenije na temelju tradicije smelo koraka v smeri novih izzivov in poslovnih priložnosti. O ključnih težiščih obvladovanja tveganj, ki jih za poslovanje Pošte Slovenije prinaša dinamično varnostno okolje, smo se pogovarjali z g. Davidom Krajncem.

V svoji dolgoletni karieri ste delovali v različnih organizacijskih sredinah, v katerih je bilo obvladovanje varnostnih tveganj pomemben segment vaših strokovnih prizadevanj. Nam lahko zaupate katere izkušnje preteklih organizacijskih okolij vam bodo najbolj pomagale pri nadaljnjih izzivih, ki ste jih našli v Pošti Slovenije?

Deloval sem v policiji, na različnih delovnih mestih, kjer dejansko spoznaš vse osnovne oblike dela, od zbiranja informacij, opravljanja razgovorov, spremljanja aktualnih problematik, intervencije, kazniva dejanja, uporaba prisilnih sredstev, ter podobno. Spoznaš osnove, kjer se dejansko seznaniš, kaj vse zajema varnost... Oblike dela sem spoznaval skozi delo policista, pripadnika posebne policijske enote, inštruktorja samoobrambe, preiskovalca računalniške kriminalitete... Po 17-tih letih sem z delom nadaljeval na Zavarovalnici Triglav d.d., kot preiskovalec zavarovalniških prevar in goljufij. Tu se je pokazala nova specifika oblike dela, zato so se odprla vrata polna novih izzivov. Kljub bogatim izkušnjam, se na Pošti Slovenije d.o.o. srečujemo z novimi oblikami tveganj in izzivi, saj smo eno največjih podjetij v Sloveniji, število zaposlenih skupaj z Intereuropo presega število 8.000.

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

Sodobna organizacija je trenutno postavljena v globalno in tehnološko usmerjeno okolje, ki postaja v čedalje večji meri odvisno od infrastrukture informacijsko-komunikacijskih tehnologij. Potenciali elektronskega komuniciranja, intenzivnost in nepredvidljivost razvoja ter zlasti otežen nadzor nad uporabo IKT-ja vplivajo na to, da postajajo vprašanja povezana z varnostjo mrežnih okolij in zaščito pred nedovoljenimi posegi v temeljne človekove pravice in svoboščine, kot tudi razprave o morebitnih tveganjih, vse pomembnejše. Ob predpostavki, da razpolagamo s tehnološko dovršenimi

> Ob predpostavki, da razpolagamo s tehnološko dovršenimi orodji in da lahko na spremembe v zunanjem okolju vplivamo le bolj ali manj uspešno, je posamezen zaposleni, verjetno eden izmed šibkejših elementov v organizacijskem sistemu.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Usmerjenost k posamezniku oziroma k socialnemu kapitalu predstavlja mejnik med »organizacijo včeraj« in »organizacijo jutri«.

orodji in da lahko na spremembe v zunanjem okolju vplivamo le bolj ali manj uspešno, je posamezen zaposleni, verjetno eden izmed šibkejših elementov v organizacijskem sistemu. Dovzetnost za vplive, kot ena izmed osebnih značilnosti ljudi, lahko dolgoročno zmanjšuje sposobnosti in kompetence ter vpliva na to, koliko posameznik osebno prispeva k celotni informacijski varnosti v določeni organizaciji. Usmerjenost k posamezniku oziroma k socialnemu kapitalu predstavlja mejnik med »organizacijo včeraj« in »organizacijo jutri«. Slednja temelji na zavedanju, da je uspeh ali neuspeh organizacije v veliki meri odvisen od tega, kar zaposleni naredijo dobro oz. od tistega, kar je bilo narejeno slabo.

Nujno je nenehno vlaganje v zaposlene, njihovo izobraževanje ter ozaveščanje. Mislim, da je to na dolgi rok edina pot do uspeha.

Pošta Slovenije je v obdobju zadnjih desetih let podvržena pomembnim spremembam v svojih poslovnih procesih. Vsekakor pa ostaja organizacija z najbolj obsežno mrežo poslovalnic v Republiki Sloveniji. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Obvladovanje tveganja je proces prepoznavanja, ocenjevanja in nadzora groženj pri profitu posamezne organizacije. Ta tveganja izvirajo iz različnih virov, vključno s finančnimi negotovostmi, zakonskimi odgovornostmi, tehnološkimi vprašanji, napakami pri strateškem upravljanju, nesrečami, naravnimi nesrečami in podobno. Uspešen program za obvladovanje tveganj pomaga organizaciji, da preuči celoten nabor tveganj, ki jih ima. Obvladovanje tveganj preučuje tudi razmerje med tveganji in kaskadnim vplivom, ki bi ga lahko imeli na strateške cilje organizacije. Ta celovit pristop k obvladovanju tveganja je včasih opisan kot upravljanje tveganja podjetij zaradi njegovega poudarka na predvidevanju in razumevanju tveganja v organizaciji.

Veliko število poslovalnic vsekakor vpliva na obvladovanje tveganj, saj je v veliki meri odvisno od zaposlenih, ter vlaganja vanje. Glede na situacijo, katero nam je prinesel COVID, so se spremenila tudi tveganja v našem podjetju, predvsem se je povečal obseg dela za isto število zaposlenih, kjer pa je posledično prihajalo do različnih varnostnih dogodkov.

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

Digitalizacija, vpeljava novih tehnologij v poslovne procese, ter hkrati varno poslovanje je bistvenega pomena za naše podjetje. Ozaveščanje in izobraževanje zaposlenih je predpogoj, kako se izogniti vsem varnostnim tveganjem v kibernetski varnosti. 100% varnosti ni. Za samo informacijsko varnost mislim, da je v Pošti Slovenije dobro poskrbljeno. Nenehno vlaganje, ozaveščanje in izobraževanje je le predpogoj, da bo za to dobro poskrbljeno.

V celovitem procesu upravljanja varnostnih tveganj lahko zavarovanje določenih tveganj predstavlja enega od orodij za učinkovito obvladovanje le teh. Kakšni so vaši

pogledi na uporabnost tega orodja v procesih zagotavljanja korporativne varnosti?

Zavarovalna tveganja so tveganja nastanka izgube ali neugodne spremembe v vrednosti. Kibernetsko tveganje predstavlja vse večjo skrb za institucije, gospodarske družbe, posameznike in finančne trge. Vedno večje je število kibernetskih incidentov, kjer ravno zavarovanje predstavlja eno od rešitev pri morebitni izgubi. Pri tem si lahko olajšamo lastno izgubo, odškodninske zahtevke tretjih oseb, ali pa krijemo izgube škode kot so na primer obratovalni zastoj, prekinitve poslovanja, lahko tudi kibernetsko izsiljevanje, stroški odkupnine in samo kritje nezakonito odvzetih denarnih sredstev.

Uvajanje novih tehnologij je bilo vedno v strateški usmeritvi Pošte Slovenije. V zadnjem obdobju smo videli, da ste aktivni pri poskusu uvajanja brezpilotnih letal v svoje procese prenosa določenih vrst pošiljk. Kako uspete v organizaciji združevati te tehnološke ideje in varnostne izzive, ki se porajajo ob uvedbi novih tehnologij?

Vsekakor je potrebno slediti trendom, času ter inovacijam. Brezpilotni letalniki imajo prihodnost, samo vprašanje časa je, kdaj bodo stopili v »ospredje« ter nam olajšali vsakodnevne obveznosti. V Pošti Slovenije smo testno opravljali avtonomne polete dronov, prav tako jih bomo skušali umestiti v pomoč pri doseganju korporativne varnosti in nadzoru. Gledano za celotno Slovenijo bi lahko imeli vidno vlogo pri umestitvi dronov v procese poslovanja ter postavitve tako imenovanega U - space koridorja za drone.

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

Glede na število poslovalnic in zaposlenih je posledično tudi veliko različnih varnostnih dogodkov, tako da prepričevanje strateškega managementa ni potrebno, saj sledijo našim željam in potrebam, da zagotovimo čim bolj varno okolje. Skušamo v najboljši meri slediti novim trendom, vpeljavi novih tehnologij, inovacij, katere nam olajšajo delo ter hkrati poskrbijo za nujne kriterije varnosti.

Nam lahko zaupate kako pomemben je za delovanje tako kompleksne organizacije, kot je Pošta Slovenije, učinkovit sistem varovanja ključnih poslovnih informacij. Je v tem pogledu dvigovanje varnostnega zavedanja med zaposlenimi pomemben dejavnik zagotavljanja ustrezne ravni varovanja teh informacij? Kakšni so vaši pogledi in koraki na tem področju?

V slovenskem gospodarskem prostoru je prej opaziti uhajanje konkurenčnih poslovnih podatkov zaradi neustreznega zavedanja vrednosti in posledično premajhne ali nikakršne zaščite, kot pa iz zlonamernih nagibov npr. nadaljnje preprodaje informacije o sestavini mešanice novega materiala. Tudi naša slovenska podjetja razvijajo izdelke in materiale, ki so lahko tako dobri, da začnejo resno ogrožati svetovno konkurenco. Slovenci smo zelo marljivi, inovativni, ter tehnološko dobro podkovani. Ob vsakem »problemu« že imamo rešitev... Samo uhajanje poslovnih informacij predstavlja veliko varnostno tveganje, kjer se veliko dela lahko opravi z neprestanim ozaveščanjem in izobraževanjem zaposlenih.

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



Korporativna varnost se identificira kot dejavnost, ki izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju, organizaciji. V Sloveniji, se le tega zavedajo v mnogih podjetjih, kjer imajo skrb za zagotavljanje varnosti opredeljeno kot zaščito premoženja in poslovnih procesov. Gre za eno od osnovnih funkcij delovanja podjetja in se za njegovo učinkovito delovanje nujno izvaja v tesnem sodelovanju z vsemi ključnimi funkcijami podjetja.

Cilj sistema je zagotavljanje notranje varnosti podjetja, le to pa se doseže z vrsto ukrepov. Ukrepi se uveljavljajo na pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ravneh, morajo pa biti skladni s spoštovanjem zakonov in internih zapisov ter z zagotavljanjem varnosti ljudi in premoženja v podjetju.

Vaše podjetje je tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Kako vi osebno ocenjujete potrebnost in učinkovitost tega strokovnega združevanja?

Ocenjujem kot nujno potrebno, ter zelo dobrodošlo. Samo povezovanje podjetij med seboj, deljenje izkušenj, mnenj, ter dobrih praks pripomorejo k reševanju posamezne tvegane varnostne situacije. V pomoč ti je pri reševanju varnostno tvegane situacije, da si nanjo lahko predhodno pripravljen, oz. ti nudi smernice, kako v dani situaciji odreagirati. ■

Foto: arhiv Pošta Slovenije

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*



KIBERNETSKA VARNOST IN PRAVNI OKVIR V EU

Za razumevanje zakonodajnega okvira v Republiki Sloveniji, ki je vezan na zagotavljanje informacijske varnosti, moramo poznati predvsem poizkuse zakonske regulative na nivoju EU. Dinamično varnostno okolje in izvajanje različnih družbenih procesov, med katerimi pa je proces digitalizacije tisti, ki ima še dodatni vpliv na hitrost uveljavljanja določenih pravnih rešitev zagotavljanja informacijske varnosti.

Za pravilno razumevanje tega področja predlagam, da si najprej pogledamo primarne korake, ki jih je EU poskušala celovito urediti skozi sprejem **EU strategije o zagotavljanju kibernetske varnosti (EU Cybersecurity Strategy)**. Cilj strategije EU za kibernetsko varnost je podpreti kolektivno odpornost Evrope na kibernetske grožnje in zagotoviti, da imajo vsi državljani in podjetja koristi od uporabe zaupanja vrednih in zanesljivih digitalnih storitev, aplikacij in orodij. Ukrepi so usmerjeni v ustrezno zaščito, ki bo omogočala nadaljnjo zagotovitev globalnega in odprtega interneta. To pa bo podlaga za zagotavljanje varnosti in zaščite evropskih vrednot in temeljnih pravic vsakogar. Strategija EU za kibernetsko varnost obravnava tri glavna področja delovanja EU:

- Odpornost, tehnološka suverenost in vodstvo[1].

Vključuje reformo varnostnih pravil v zvezi z omrežnimi in informacijskimi sistemi. S tem se bo zagotovila povečana raven kibernetske odpornosti kritičnih javnih in zasebnih sektorjev, kot so bolnišnice, energetska omrežja, železnice, podatkovni centri, javne uprave, raziskovalni laboratoriji in proizvodnja kritičnih medicinskih naprav ter zdravila. V ta okvir pa so vključene tudi druge kritične infrastrukture in storitve. Takšna infrastruktura mora ostati ustrezno zaščitena in robustna v hitro spreminjajočem in zapletenem varnostnem okolju. Ti ukrepi se neposredno izvajajo na podlagi revidirane direktive o "NIS" ali "NIS 2", ki nosi normativni okvir za visoko skupno raven kibernetske varnosti v EU.

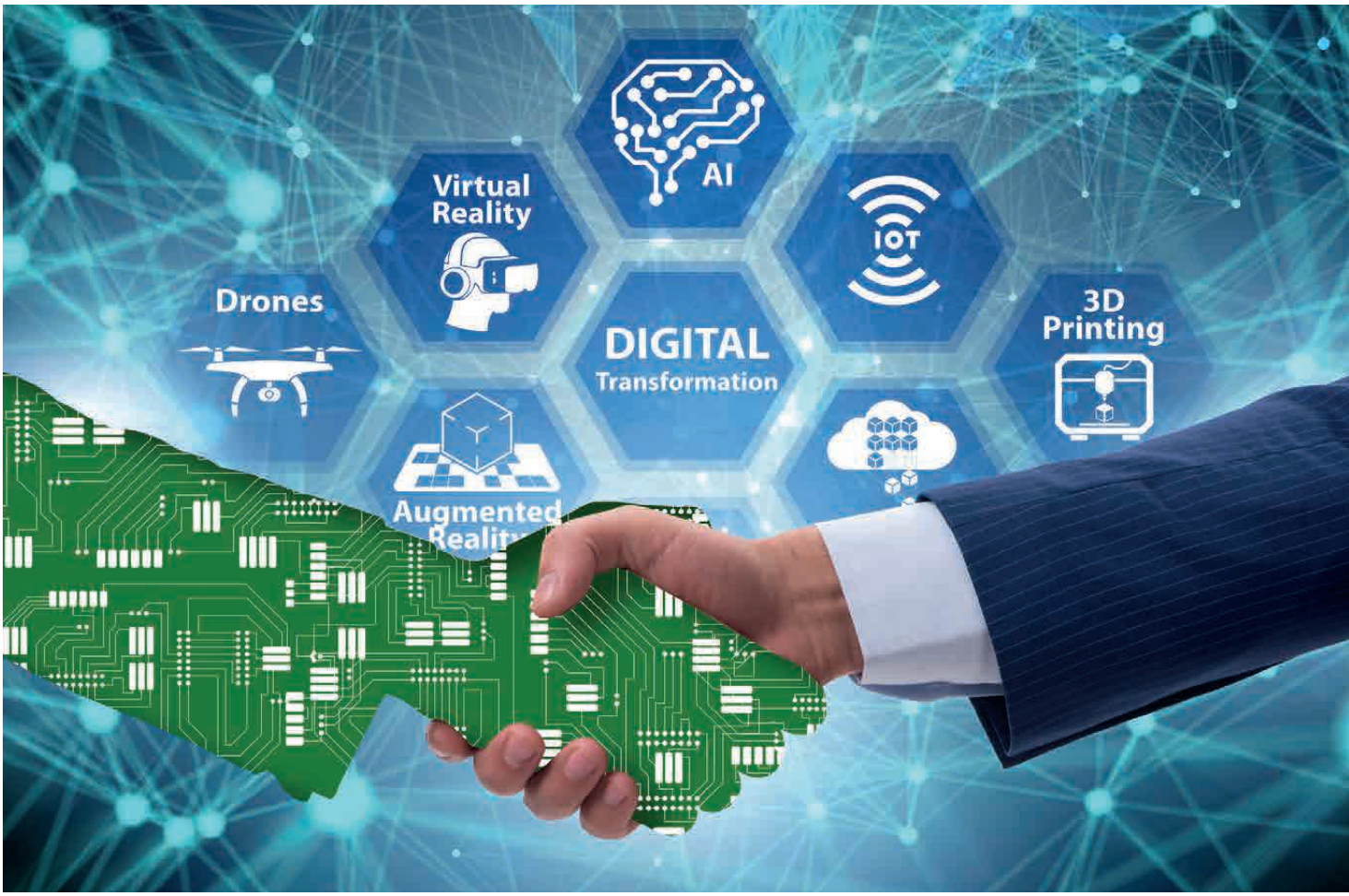
Predlaga pa se tudi vzpostavitev mreže varnostnih operativnih centrov (SOC) po vsej EU, kjer bi uporabljali umetno inteligenco (AI). To omrežje SOC bo oblikovalo „ščit za kibernetsko varnost" za celotno EU, ki bo lahko dovolj zgodaj odkril znake kibernetskega napada in na drugi strani omogočil ustrezne proaktivne ukrepe. Dodatni ukrepi bodo vključevali namensko podporo malim in srednje velikim podjetjem, usposabljanje in osveščanje zaposlenih, privabljanje in zadrževanje strokovnjakov za kibernetsko varnost ter vlaganje v raziskave in inovacije. Te zadnje pa morajo biti ustrezno dostopne, konkurenčne v okviru tehnoloških rezultatov in temeljiti na odličnosti.

Direktiva o varnosti omrežnih in informacijskih sistemov – Direktiva NIS predstavlja pomemben normativni okvir na področju kibernetske varnosti, ki velja za celotno EU, katere cilj je zagotoviti zmogljivosti kibernetske varnosti na enaki ravni razvoja v vseh državah članicah EU. Zagotavlja učinkovito izmenjavo informacij in sodelovanje, vključno s čezmejno izmenjavo informacij, s čimer prispeva k ustvarjanju višje ravni kibernetske varnosti v EU.

- Operativna zmogljivost za preprečevanje, odvračanje in odzivanje[2].

V pripravi je nova skupna kibernetska entiteta, ki bo vzpostavljena skupaj s postopnim in vključujočim procesom z državami članicami. Cilj je zbližati in okrepiti sodelovanje med orga-

*avtorica je članica Slovenskega združenja korporativne varnosti



ni EU in organi držav članic, ki so odgovorni za preprečevanje, odvračanje in odzivanje na kibernetske napade. Poleg tega so predlagani ukrepi za preprečevanje, odvračanje in učinkovit odziv na zlonamerne kibernetske dejavnosti. V tem okviru je fokus zlasti na tiste, ki vplivajo na kritično infrastrukturo, dobavne verige, demokratične institucije in procese. Tudi EU si prizadeva za nadaljnjo krepitev sodelovanja na področju kibernetske obrambe in razvoj najsodobnejših zmogljivosti za kibernetsko obrambo, pri čemer se osredotoča na delo Evropske obrambne agencije in spodbuja države članice, da v celoti izkoristijo stalno strukturirano sodelovanje in Evropski obrambni sklad.

- Sodelovanje za razvoj globalnega in odprtega kibernetskega prostora[3].

EU nadalje podpira sodelovanje z mednarodnimi partnerji za krepitev svetovnega reda, ki temelji na pravilih, spodbujanju mednarodne varnosti in stabilnosti v kibernetskem prostoru ter zaščito človekovih pravic in temeljnih svoboščin na spletu. Za napredek mednarodnih standardov, ki odražajo te temeljne vrednote EU, bo EU spodbujala tudi sodelovanje z Združenimi narodi in drugimi ustreznimi forumi, okrepila mehanizme za kibernetsko diplomacijo EU in z razvojem zunanje kibernetske zmogljivosti EU povečala prizadevanja za izgradnjo kibernetskih zmogljivosti v tretjih državah.

EU je prav tako zavezana podpreti novo strategijo kibernetske varnosti z večjo ravnjo naložb, predvidenih v naslednjih sedmih letih, prek programa Digitalna Evropa in Horizon Europe ter načrta za oživitev Evrope. Cilj je doseči do 4,5 milijarde evrov skupnih naložb iz EU, držav članic in industrije v okviru kompetenčnega centra za kibernetsko varnost in mreže koordinacijskih centrov ter zagotoviti, da bo večji del namenjen organizacijam, ki se ekspertno ukvarjajo s kibernetsko varnostjo.

Poleg tega je namenjen krepitvi industrijskih in tehnoloških zmogljivosti EU na področju kibernetske varnosti s projekti, ki jih skupaj podpirajo proračun EU in nacionalni proračuni. V zvezi s tem ima EU priložnost, da v skladu z vrednotami in prednostnimi nalogami EU, združi svoja sredstva za okrepitev svoje strateške avtonomije in uveljavi svojo vodilno vlogo na področju kibernetske varnosti v celotni digitalni dobavni verigi.

Uredba Evropskega parlamenta in Sveta EU o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti)

Uredba EU o kibernetski varnosti [4] je začela veljati 27. junija 2019. Gre za obsežen paket ukrepov, katerih cilj je okrepiti odpornost proti kibernetskim napadom v Evropski uniji (EU). Gre za pomemben korak k varnosti na enotnem evropskem digitalnem trgu in večjemu zaupanju v internet stvari (IoT). Gre za pravni okvir, ki usklajuje postopke testiranja za certificiranje izdelkov, storitev in procesov na ravni EU.

Natančneje, Uredba o kibernetski varnosti vključuje:
(1) Stalni mandat za Agencijo EU za kibernetsko varnost (ENISA), ki predvideva znatno povečanje finančnih in člo-

veških virov agencije. V zvezi s tem lahko ENISA poveča zmogljivosti za kibernetsko varnost v Evropski uniji in spodbuja pripravljenost. ENISA naj bi delovala tudi kot neodvisen kompetenčni center. Cilj je dvojen, ozaveščanje državljanov in podjetij ter podpora institucijam EU in državam članicam pri izvajanju političnega okvira in ustreznih pogojev na področju kibernetske varnosti.

(2) Oblikovanje okvira EU za certificiranje varnosti izdelkov, storitev in procesov IKT. To vključuje obsežen sklop pravil, tehničnih zahtev, standardov in postopkov na ravni EU za ocenjevanje lastnosti kibernetske varnosti izdelkov, storitev ali procesov. Certifikati so veljavni v vseh državah članicah EU in zagotavljajo informacije o izpolnjenih varnostnih zahtevah IKT. Podjetja, ki poslujejo v EU, bodo imela koristi od tega, da bodo svoje izdelke, postopke in storitve IKT certificirala samo enkrat in da bodo njihovi certifikati priznani po vsej EU. ENISA bo imela ključno vlogo pri vzpostavitvi in vzdrževanju evropskega certifikacijskega okvira za kibernetsko varnost s pripravo tehnične podlage za posebne sheme certificiranja. ENISA bo zadolžena za obveščanje javnosti o certifikacijskih shemah in izdanih certifikatih prek namenskega portala.

Na podlagi novih telekomunikacijskih pravil (Kodeks elektronskih komunikacij) morajo države članice zagotoviti, da se ohranjata celovitost in varnost javnih komunikacijskih omrežij, ter da operaterji sprejmejo tehnične in organizacijske ukrepe za obvladovanje morebitnih varnostnih tveganj v omrežjih in storitvah. Prav tako določa, da imajo pristojni nacionalni regulativni organi pooblastila, vključno s pooblastili za izdajanje zavezujočih navodil in zagotavljanje njihove skladnosti. Poleg tega lahko države članice določijo pogoje v zvezi z varnostjo javnih omrežij pred nepooblaščenim dostopom do splošnih dovoljenj za operaterje z namenom varovanja zaupnosti komunikacij.

Uredba EU o kibernetski varnosti prvič določa mehanizme kot sta „Security by Design“ in „Security by Default” kot regulativni načeli za izdelke, ki so pomembni za varnost. V zvezi s tem spodbuja proizvajalce ali ponudnike, ki sodelujejo pri načrtovanju in razvoju izdelkov, storitev ali procesov IKT, da izvajajo ukrepe v najzgodnejših fazah procesa načrtovanja in razvoja. To omogoča zaščito teh izdelkov, storitev ali procesov na najvišji možni ravni, tako da se predvideva in čim bolj zmanjša pojav kibernetskih napadov.



Pričakuje, da bodo imeli koristi od navedene Uredbe o kibernetski varnosti EU, različni segmenti družbene skupnosti in sicer:
- Državljani in končni uporabniki, ki jim bo omogočeno bolj pregledno odločanje glede izdelkov in storitev, ki jih uporabljajo.
- Ponudniki in ponudniki izdelkov in storitev, ki bodo imeli prihranke pri stroških in času, saj bodo opravili enoten postopek za pridobitev evropskega certifikata, ki je veljaven in jim omogoča konkurenčnost v vseh državah članicah.
- Vlade, ki bodo bolje opremljene za sprejemanje bolj informiranih odločitev o nakupu izdelkov in storitev IKT.

Treba je opozoriti, da certifikacijske sheme temeljijo na prostovoljni odločitvi posamezne organizacije in ponudnika. To praktično pomeni, da se prodajalci lahko odločijo, ali želijo, da so njihovi izdelki certificirani ali ne. Vendar Uredba predvideva, da lahko Komisija oceni učinkovitost in uporabo sprejetih evropskih sistemov certificiranja kibernetske varnosti. Na ta način lahko oceni, ali bi morala posebna evropska shema certificiranja kibernetske varnosti z ustrezno normativno ureditvijo v EU postati obvezna. Odločitev bo temeljila na potrebi, da se zagotovi ustrezna raven kibernetske varnosti izdelkov, storitev in procesov IKT.

V skladu z Uredbo o kibernetski varnosti EU se uveljavljata vloga in odgovornosti Agencije EU za kibernetsko varnost (ENISA). Glavne naloge ENISE v okviru novega mandata so:
- Podpora izvajanja politik na področju kibernetske varnosti, zlasti direktive o omrežjih in informacijskih sistemih (NIS), kot tudi drugih političnih pobud z elementi kibernetske varnosti v različnih sektorjih (npr. energetika, promet, finance).
- Ustvarjanje strokovnega znanja na področju kibernetske varnosti, da bi pomagali izboljšati zmogljivosti javnih organov EU in nacionalnih organov (na primer z usposabljanji).
- Analiza trga glede standardizacije in certificiranja kibernetske varnosti.
- Zagotavljanje operativnega sodelovanja in kriznega upravljanja z namenom krepitve obstoječih preventivnih operativnih zmogljivosti in podpore operativnemu sodelovanju kot sekretariat mreže CSIRT. ENISA bo državam članicam nudila tudi pomoč pri obravnavanju incidentov in izvajala pomembno vlogo pri usklajenem odzivu EU na obsežne čezmejne incidente kibernetske varnosti.
- Usklajeno razkrivanje ranljivosti, kjer bo državam članicam in institucijam, agencijam in organom Unije pomagalo pri prostovoljnem oblikovanju in izvajanju politik razkritja ranljivosti.

Direktiva o varnosti omrežnih in informacijskih sistemov – Direktiva NIS (The Directive on Security of Network and Information Systems – The NIS Directive)

Direktiva o varnosti omrežnih in informacijskih sistemov – Direktiva NIS[5] predstavlja pomemben normativni okvir na področju kibernetske varnosti, ki velja za celotno EU, katere cilj je zagotoviti zmogljivosti kibernetske varnosti na enaki ravni razvoja v vseh državah članicah EU. Zagotavlja učinkovito izmenjavo informacij in sodelovanje, vključno s čezmejno izmenjavo informacij, s čimer prispeva k ustvarjanju višje ravni kibernetske varnosti v EU.

Direktiva NIS izvajalcem bistvenih storitev (IBS) in ponudnikom digitalnih storitev (PDS) nalaga nove zahteve glede varnosti omrežja in informacij. Oba sta odgovorna za poročanje o

večjih varnostnih incidentih. Tudi če IBS in PDS vzdrževanje svojih informacijskih sistemov oddajo tretjim osebam, Direktiva NIS od njih zahteva, da so odgovorni za morebitne varnostne incidente. Poleg tega morajo IBS in PDS poročati o vseh pomembnih incidentih pristojnim organom ali skupinam za odzivanje na računalniške varnostne incidente (CSIRT). Pomemben incident v zvezi s kibernetsko varnostjo je določen s številom uporabnikov, ki jih je prizadela varnostna kršitev, pa tudi z dolžino in geografskim dosegom incidenta.

Države članice EU morajo poleg nacionalnih pristojnih organov (NSA) in enotnih kontaktnih točk (EKT) vzpostaviti strategijo direktive NIS, ki vključuje ustanovitev CSIRT. Takšni deležniki so odgovorni za obravnavo kršitev kibernetske varnosti na način, ki zmanjšuje negativne vplive. Poleg tega se vse države članice EU spodbuja k izmenjavi informacij o kibernetski varnosti.[6]

Na splošno direktiva NIS zagotavlja pravne ukrepe, ki povečujejo raven kibernetske varnosti v EU z zagotavljanjem:
- Izmenjave informacij, saj morajo države članice ustanoviti CSIRT in pristojni nacionalni organ (NSA).
- Sodelovanja z ustanovitvijo skupine za sodelovanje za podporo in krepitev strateškega sodelovanja ter izmenjave informacij med državami članicami.
- Dvigovanja zavesti o varnosti s spodbujanjem varnostne kulture v ključnih sektorjih za gospodarstvo in družbo EU, ki so močno odvisni od IKT, kot so energija, promet, voda, bančništvo, infrastruktura finančnih trgov, zdravstveno varstvo in digitalna infrastruktura.

Direktiva NIS 2 (The NIS 2 Directive)

Evropski ministri so ob koncu leta 2021 na zasedanju Sveta za promet, telekomunikacije in energijo, ki mu je predsedoval minister za javno upravo Boštjan Koritnik, soglasno potrdili splošni pristop pri direktivi NIS 2, kar bo močno prispevalo k odpornosti in zmogljivosti odzivanja na kibernetske incidente. Direktiva NIS 2 se trenutno nahaja v fazi pogajanj z Evropskim parlamentom. Zaključek pogajanj in sprejem, pa se pričakuje v maju 2022.

Natančneje, NIS 2 se osredotoča na razširitev direktive NIS in zagotavlja:

(1) Večje zmogljivosti
- Uvaja strožje nadzorne ukrepe in izvrševanje.
- Predvideva seznam upravnih sankcij, kot so globe za kršitev obvladovanja tveganja kibernetske varnosti in obveznosti poročanja.

(2) Povečano sodelovanje
- Vzpostavi evropsko mrežo organizacij za povezavo pri soočanju s kibernetskimi krizami (EU-CyCLONE) za podporo usklajenemu upravljanju obsežnih incidentov in kriz kibernetske varnosti na ravni EU.
- Spodbuja izmenjavo informacij in sodelovanje med organi držav članic z okrepljeno vlogo skupine za sodelovanje.
- Vzpostavlja usklajeno razkritje ranljivosti za novo odkrite ranljivosti po vsej EU.

(3) Okrepljeno upravljanje tveganja kibernetske varnosti
- Povišane varnostne zahteve s seznamom osredotočenih ukrepov, vključno z odzivom na incidente in kriznim upravljanjem, obravnavanjem in razkritjem ranljivosti, testiranjem kibernetske varnosti in učinkovito uporabo šifriranja.



- Povečana kibernetska varnost dobavne verige za ključne informacijske in komunikacijske tehnologije.
- Uvaja odgovornost vodstva družbe za skladnost z ukrepi za obvladovanje tveganja kibernetske varnosti.
- Poenostavljene obveznosti poročanja o incidentih z natančnimi določbami o postopku poročanja, vsebini in časovnici.

Poleg tega NIS 2 razširja področje uporabe direktive, da vključuje več sektorjev in storitev, kot so:
- Ponudniki javnih elektronskih komunikacijskih omrežij ali storitev
- Digitalne storitve, kot so platforme storitev družbenih omrežij in podatkovni centri
- Odpadne vode in ravnanje z odpadki
- Vesolje
- Proizvodnja nekaterih kritičnih izdelkov (kot so farmacevtski izdelki, medicinski pripomočki, kemikalije)
- Poštne in kurirske storitve
- Hrana
- Javna uprava.[7]

1 Resilience, technological sovereignty and leadership

2 Operational capacity to prevent, deter and respond

3 Cooperation to advance a global and open cyberspace

4 "EU Cybersecurity Act - Regulation (EU) 2019/881 of the European Parliament and of the Council," 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

5 "NIS Directive, European Parliament," 2016. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

6 Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System version 3.1: Specification Document," June 2019. [Online]. Available: https://www.first.org/cvss/specification-document. [Accessed January 2022].

7 https://slovenian-presidency.consilium.europa.eu/sl/novice/slovenija-s-potrditvijo-direktive-nis-2-mocno-prispevala-h-krepitvi-kibernetske-varnosti-v-evropski-uniji/ ■

Avtor: Mihael Nagelj / Gospodarska zbornica Slovenije, Združenje za informatiko in telekomunikacije*



URESNIČEVANJE UKREPOV KIBERNETSKE VARNOSTI V PROCESIH DIGITALNE TRANSFORMACIJE

Ni novost, da se kibernetske grožnje nenehno razvijajo, saj o tem pogosto poročajo novinarji. Pred kratkim smo videli, da ne gre samo za izsiljevalsko programsko opremo ali lažno predstavljanje, temveč tudi za ranljivosti v glavnih knjižnicah programske opreme (npr. Log4J). V povezavi s človeškim faktorjem (kulturo kibernetske varnosti) pa so možnosti ogrožanja še večje. Pri upravljanju kibernetskih groženj gre za obvladovanje tveganj, ki pa zahteva poznavanje kompleksnosti vsakega sistema, tako z vidika vpliva tehnik napadalcev, možnosti izvedbe protiukrepov in posledic, ki jih uspešno izveden napad lahko ima na poslovanje podjetij. Kibernetska tveganja so pomemben dejavnik, ki ga podjetja morajo upoštevati pri vseh programih digitalne transformacije, s čimer bodo prednosti le te lahko učinkovito izkoristila.

V zadnjih letih se podjetja in družba v celoti soočajo z digitalno transformacijo, ki so jo še posebej pospešili zadnji dogodki v zvezi s COVID-19 in porastom digitalnih rešitev (digitalne platforme, spletne storitve, ...) v vseh sektorjih družbe. Tak pospešen digitalni prehod je povečal obseg storitev za potrošnike in specialiste, kar je zelo spremenilo procese dela in istočasno bistveno povečalo število tveganj in stopnjo ogrožanja neprekinjenosti poslovanja in s tem zmanjšanja učinkov investicij v digitalno transformacijo.

Večina kibernetskih tveganj ni novih, vendar sta velika odvisnost od digitalnih tehnologij, še posebej v povezavi z drugimi tveganji, razkrila nove izzive, ki zahtevajo posebno pozornost izboljšanja upravljanja virov za zagotavljanje ustrezne varnosti v kibernetskem prostoru. Ob kibernetskem incidentu predpostavke o tveganjih postanejo realnost, podjetje spozna ranljivost svojega sistema, slabosti varnostnih ukrepov in posledice v stroških in ugledu podjetja. Zaradi kompleksnosti napadov in varnostnih ukrepov, ki niso samo tehnološki, je ključnega pomena zavedanje vodilnih o stanju tveganj poslovanja podjetja in s tem tudi možnost izvajanja organizacijskih ukrepov. Ob uresničevanju digitalne transformacije podjetja bi morali biti tudi vidiki varnosti delovanja podjetja ustrezno upoštevani. Kar pa pomeni celovite (organizacijske in tehnološke vidike) digitalne rešitve na vseh ravneh organizacije.

Obstajajo splošna kibernetska varnostna tveganja, npr. klasični virusi in kripto virusi, zlonamerna koda razširjena v medmrežju, avtomatizirana zloraba storitev, katerim so izpostavljena vsa področja. Obstajajo tudi specifična tveganja za posamezno domeno, organizacijo ali storitev, ki med drugim vključuje ciljane napade, onemogočanje storitev, socialni inženiring z namenom pridobivanja ključnih informacij za izvedbo vdora, ki jim je potrebno dodati kibernetske konflikte na regionalni ali globalni ravni.

Na splošno je digitalna transformacija kontinuiran proces radikalnejših sprememb, inoviranja produktov, procesov ali poslovnega modela, z izkoriščanjem lastnosti modernih informacijskih in komunikacijskih tehnologij. Nobena strategija digitalne transformacije ni bila uspešno uresničena brez bistvenih sprememb v miselnosti in spreminjanju organizacijske kulture. Nedvomno je del sprememb tudi varnostna kultura, saj zaposleni z ozaveščenim in odgovornim

* Poleg navedenega tudi predsednik ZIT SeKV in IKT Hm Kibernetska varnost – Koordinator področja



ravnanjem lahko preprečijo dnevne poskuse vdorov v informacijske sisteme ali pa s strateškimi odločitvami zagotovijo potrebne ukrepe za obvladovanje kibernetskih tveganj že od samega začetka procesa digitalne transformacije podjetja.

Varnost in zasebnost sta ključni zahtevi modernih informacijskih in komunikacijskih sistemov. Razvoj novih digitalnih produktov in storitev, kot dela digitalne transformacije podjetja, si praktično ne moremo zamisliti brez ustreznih varnostnih rešitev in storitev, ki morajo biti v izdelke in storitve vključene že v fazi načrtovanja. Varnost in zasebnost naslavljajo in zahtevajo pomembne evropske uredbe in direktive, kot so GDPR, direktiva NIS in njeni delovni dokumenti, Splošne uredbe o varstvu podatkov ter uredbe eIDAS, ki urejajo skupni evropski digitalni trg. Uporabniki storitev in rešitev pričakujejo doseganje varnostnih standardov, kot je družina standardov ISO 27000.

Na zagotavljanje varnosti in zasebnosti bistveno vplivajo raznovrstnost prihodnjih naprav, ki se vse bolj intenzivno vključujejo v omrežja in oblačna okolja, razdrobljenost nadzora in upravljanja modernih ekosistemov ter raznorodnost zahtev ciljnih domen. Samodejna skladnost z zahtevami ter standardi, modernost in primernost uporabljenih mehanizmov, zmožnost povezovanja ter souporabe in združljivost z različnimi produkti so tisti dejavniki, ki bodo transformacijskim projektom zagotovili kompetenčne prednosti.



Za celovito zagotavljanje kibernetske varnosti je potrebno začeti že v fazi načrtovanja. Že v tej fazi je potrebno narediti analizo tveganj in razjasniti, katere so potencialne ranljivosti in kakšen nivo varnosti pričakujemo od končnega produkta. Tako lahko ustrezne varnostne mehanizme načrtujemo že dovolj zgodaj, da so primerno integrirani v zasnovo arhitekture transformiranega sistema ali novih produktov.



Le tako se lahko izognete stroškom odprave pomanjkljivosti ugotovljenih ob koncu razvojnega cikla projekta digitalne transformacije.

V fazi razvoja in izgradnje produkta, sistema ali storitve se vzporedno z glavno funkcionalnostjo razvija in testira tudi funkcionalnost varnostnih mehanizmov, zagotavljanje zanesljivosti in zaščite (npr. varnostno preverjanje programske kode, varnostna utrditev sistemskega okolja, namestitev specifičnih varnostnih elementov in funkcionalnosti, definiranje in uveljavitev varnostnih postopkov in kontrol, usposabljanje osebja itd.) transformiranega področja v podjetju. Tu je glavni poudarek na aplikacijski varnosti. Pred prehodom v operativno uporabo transformiranih rešitev je potrebno, ne le funkcionalno in integracijsko, ampak tudi varnostno preverjanje izdelka ali transformirane rešitve. Vse bolj se uveljavlja koncept certificiranja z namenom vzpostavljanja zaupanja in varnosti izdelkov, storitev in procesov za kibernetsko varnost. Tako uporabniki kot ponudniki storitev morajo biti sposobni določiti raven varnostnega zagotovila za izdelke, storitve in procese, ki jih nabavljajo, dajejo na voljo ali uporabljajo.

V produkcijski fazi se bodo zaznavale pomanjkljivosti, ki so bile spregledane v prejšnjih fazah. Poleg tega se bo transformirana rešitev še naprej prilagajala spremembam v okolju, uporabnikom in načinu uporabe. Tu je potrebno vključevati neprekinjeno analizo novih groženj v okolju in vrednotenje, za katere je transformirana rešitev ranljiva in jo je potrebno dodatno zaščititi. S procesom vzdrževanja in stalnega izboljševanja zagotavljamo, da rešitev ohranja načrtovan nivo varnosti, ki ga po potrebi še okrepimo in dvignemo. Ne smemo pozabiti pomena stalnega ozaveščanja uporabnikov in vzdrževanja ustrezne ravni varnostne kulture. Ne le, da znajo uporabljati osnovno funkcionalnost produkta – zavedati se morajo, kakšni napadi jim grozijo in ponotranjiti osnove varne uporabe produkta, sistema in IKT tehnologij nasploh, v primeru incidenta pa morajo znati hitro in primerno ukrepati.

Opisan proces zagotavljanja varnosti je cikličen – nobena faza ni zadnja, saj moramo identificirane pomanjkljivosti takoj vključiti v načrt in kolo se ponovno zavrti. S celovitim obvladovanjem celotnega cikla, namesto samo delnem izpostavljanju preverjanja varnosti, se bo podjetje lahko izognilo potencialnim napadom, v primeru napada pa bo sposobno ustrezno ukrepati. Poleg tega problem kibernetske varnosti ni samo tehnični, katerega lahko razrešijo inženirji, pač pa je njegovo razreševanje odvisno od spreminjanja varnostne kulture v podjetju. Del te kulture je tudi povezanost s podjetji, ki izvajajo digitalne ali varnostne storitve v celotnem življenjskem ciklu, ali pa organi države, ki zagotavljajo informacije o aktualnih grožnjah. Le tako bodo izboljšane možnosti obvarovanja uspeha digitalne transformacije podjetij pred grožnjami iz kibernetskega prostora.

Digitalna transformacija je kompleksen proces s katerim podjetje zagotavlja svojo konkurenčno prednost na trgu. Napadi iz kibernetskega prostora lahko učinke teh procesov pomembno ogrozijo, zato je v digitalno transformacijo potrebno vključiti tudi vidike kibernetske varnosti. V prvi vrsti je podjetje samo odgovorno za stanje kibernetske varnosti, ki jo lahko zagotavlja le z uvajanjem celovitih ukrepov, ter tako zmanjša vpliv groženj na učinke digitalne transformacije. ■

KOMU ZAUPATI
VARNOST NEPREKINJENEGA POSLOVANJA?

Izzivi za poslovna in informacijska okolja

S pravimi partnerji, rešitvami in storitvami je neprekinjeno poslovanje možno uresničiti v vsakem podjetju. To pa je v praksi velik izziv za vsako podjetje, saj zahteva nadvse zanesljive storitve in IT-infrastrukturo. »Informacijska varnost in natančneje kibernetska varnost sta v zadnjem času postali ključni besedi vseh, ki želijo primerno naslavljati tveganja vsakodnevnega poslovanja podjetja. Prav je, **da se zavedamo groženj,** ki lahko povzročajo prekinitve poslovanja. Prav gotovo pa je najbolj smiselno takemu zavedanju dodati še primerno **pripravljenost na nepredvidene, predvsem krizne dogodke,** ki lahko ohromijo poslovanje in pa vse **ukrepe za okrevanje** v primeru kakršnekoli prekinitve poslovanja.« ***poudarja Rony Plevnik, direktor podjetja PRO.ASTEC d.o.o.***

V ta namen je treba pristopiti k oblikovanju načrtov neprekinjenega poslovanja. Ti ne obsegajo samo zaznave dogodka oziroma incidenta, pač pa še množico vseh ostalih aktivnosti, s katerimi se lahko podjetje lažje in z manj izgubami vrne v običajno poslovanje.

Kako standard ISO 22301 pomaga upravljati neprekinjeno poslovanje

Primerna osnova za pripravo načrtov neprekinjenega poslovanja so mednarodne dobre prakse in med njimi prav gotovo standard **ISO 22301.** Ta določa pogoje, ki jih organizacije potrebujejo za oblikovanje načrtov, izvajanje, delovanje, spremljanje, pregledovanje, vzdrževanje in pripravo na zmanjševanje tveganj ter za razvoj dokumentiranega sistema upravljanja za zagotovitev kontinuitete poslovanja.

V pridobivanju **certifikata skladnosti s standardom ISO 22301** je ob pomoči strokovnjakov iz podjetja PRO.ASTEC tudi **partnersko podjetje Stelkom,** ponudnik telekomunikacijskih storitev z 18-letno tradicijo.

V podjetju Stelkom se bo tako po dogodku, ki lahko privede do motenj kontinuitete poslovanja, sposobnost organizacije za zagotavljanje izdelkov ali storitev nadaljevala na vnaprej določenih sprejemljivih ravneh.



Neprekinjeno poslovanje je potrebno načrtovati vnaprej

Obvladovanje neprekinjenega poslovanja zahteva kakovostno in celovito podporo

Neprekinjeno poslovanje moramo primerno načrtovati, širiti poznavanje načrta in kasneje tudi po njem vaditi. V določenem trenutku, ko varnostni incident preraste običajne dimenzije, je tako treba:

- sprejeti odločitev, da gre za krizno situacijo,
- o tem obvestiti izvajalce poslovnih procesov,
- pričeti izvajati odziv na katastrofo,
- obvestiti tiste, ki so odgovorni za poslovanje,
- nadomestiti izpadla sredstva,
- sanirati primarne lokacije in
- vzpostaviti običajno delovanje.

Podjetja namreč spoznavajo, da **skupina Actual IT** kot specializiran ponudnik, z ekipo strokovnjakov poskrbi za informacijsko varnost z dolgoletnimi kompetencami in ustreznimi rešitvami.

Skupina Actual

Skupina Actual IT je del mednarodne skupine, v Sloveniji obsega štiri družbe: **Actual I.T. d.d., PRO.Astec d.o.o., Unistar LC d.o.o., Itelis d.o.o..** Strankam kritične infrastrukture, javnim in zasebnim podjetjem ter drugim organizacijam različnih velikosti kot skupina nudimo in zagotavljamo celovite informacijske rešitve in storitve za digitalno poslovanje, storitve in rešitve s področja IKT-infrastrukture ter informacijske in kibernetske varnosti.

PRO.Astec d.o.o., Dunajska cesta 158 - 1000 Ljubljana
Telefon: +386 1 3207 133, E-mail: info@astec.si

Avtor: Albert Nabernik, CFE /
Pomočnik vodje Službe za nadzor pri Komisiji za preprečevanje korupcije



VZPOSTAVITEV POTI ZA NOTRANJE PRIJAVE IN ZAŠČITA ŽVIŽGAČEV

Direktiva (EU) 2019/1937 Evropskega parlamenta in Sveta z dne 23. oktobra 2019 o zaščiti oseb, ki prijavijo kršitve prava Unije (v nadaljevanju: Direktiva), od držav članic med drugim zahteva, da uredijo poti za obravnavo notranjih prijav, informiranje prijaviteljev in zaščito pred povračilnimi ukrepi.

Direktiva zahteva poseben režim obravnave in zaščite prijaviteljev, ki bodo prijavili kršitve s področij javnega naročanja, finančnih storitev, preprečevanja pranja denarja in financiranja terorizma, varnosti izdelkov, varnosti v prometu, varstva okolja, zaščite pred sevanjem in jedrske varnosti, varnosti hrane, javnega zdravja, zdravja živali, varstva potrošnikov, varstva zasebnosti, varnosti omrežij in informacijskih sistemov, kršitve, ki vplivajo na finančne interese Unije, kršitve, ki se nanašajo na notranji trg, vključno s kršitvami pravil Unije o konkurenci in državni pomoči, ter kršitve, ki se nanašajo na notranji trg v zvezi z dejanji, ki kršijo pravila o davku od dohodkov pravnih oseb (v nadaljevanju: stvarno področje uporabe).

Poseben režim obravnave in zaščite bo potrebno zagotoviti osebam, ki bodo prijavile kršitve, o katerih so se seznanile v okviru zaposlitve, kot kandidati za zaposlitev, pogodbeni sodelavci, bivši zaposleni, delničarji, člani organa upravljanja ali nadzora (v nadaljevanju: osebno področje uporabe). Na podlagi Direktive bodo zaščite deležni zlasti posamezniki, ki se na delovnem mestu seznanijo s sumi kršitev. Glede na sprejeto osebno področje uporabe Direktive lahko te posameznike imenujemo tudi žvižgači. Svet Evrope je namreč že leta 2014 ob sprejemu priporočil CM/Rec(2014)7, kot žvižgača opredelil vsakogar, ki v kontekstu delovnega razmerja v javnem ali zasebnem sektorju prijavi ali razkrije informacije, ki ogrožajo ali škodijo javnemu interesu.[1]

Zaupnost identitete je prva obrambna linija, ki je najbolj preprosta in hkrati najbolj učinkovita pri preprečevanju možnosti nastanka povračilnih ukrepov. Največkrat se ravno zaradi strahu pred razkritjem posamezniki bojijo prijaviti nepravilnosti.

Državam članicam je prepuščeno, da lahko stvarno področje uporabe Direktive razširijo, in zagotovijo zaščito tudi prijaviteljem, ki bodo delodajalcu ali pristojnim organom prijavili informacije o sumih kršitev z drugih področij (npr. postopki zaposlovanj, podelitve koncesije in sklepanje javno zasebnih partnerstev, darila, donacije,..).

Neodvisno od odločitve o minimalnem ali širšem prenosu Direktive, ki je lahko še predmet širše razprave, v nadaljevanju podajam nekaj minimalnih zahtev oziroma dodatnih obveznosti, ki jih za pravne subjekte v zasebnem sektorju določa Direktiva. Te obveznosti še niso pravno zavezujoče, saj bo potrebno počakati na sprejem zakona in drugih predpisov, potrebnih za uskladitev z Direktivo.

V zasebnem sektorju bodo poti za notranje prijave morali vzpostaviti vsi pravni subjekti s 50 ali več zaposlenimi, ne glede na naravo njihove dejavnosti. Teh je okoli 1700.[2] Zlasti v zasebnem sektorju imajo večja podjetja že danes vzpostavljena delovna mesta ali organizirane posebne notranje organizacijske enote za sprejem in obravnavo prijav (npr. pooblaščenec za skladnost poslovanja, pooblaščenec za korporativno integriteto, Služba za preprečevanje in obravnavo prevar, Služba za korporativno varnost,...). Pri teh zavezancih ni skrbi, da ne bi pravočasno izpolnili tudi dodatnih obveznosti, ki jih bo podrobneje določal Zakon o zaščiti prijaviteljev, ki je še v medresorskem usklajevanju.

Podjetja, ki imajo 50 ali več zaposlenih in še nimajo vzpostavljenih poti za prijavo, bodo morala v določenem prehodnem obdobju: (1) urediti poti za sprejem notranjih prijav, (2) dolo-



čiti zaupnika za sprejem in obravnavo kršitev ter (3) zagotoviti informiranje prijavitelja o zaščiti.

Ureditev poti za notranjo prijavo

Pred vzpostavitvijo poti za notranjo prijavo bi bilo potrebno vse zaposlene, vključno s poslovodstvom, ozavestiti o pomenu žvižgaštva in pravni podlagi zanj. Sporočanje sumov kršitev ni dejavnost z negativnim predznakom (špecanje, ovaduštvo, cinkanje...), ampak dejanje lojalnosti do podjetja. Prej, ko bo delodajalec seznanjen z nepravilnostmi, manjša bo škoda za podjetje, saj bo njihovo nadaljnje izvajanje ustavilo, sprejelo popravljalne ukrepe ter s tem zmanjšalo tudi nadaljnjo škodo, ki jo le te povzročajo njegovemu poslovanju. Pravna podlaga za sporočanje informacij o nepravilnostih delodajalcu, pristojnim organom ali za javno razkritje, je urejena v prvem odstavku 39. člena Ustave Republike Slovenije in v 10. členu Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin, in sicer je to pravica do svobode izražanja, ki je ena od temeljnih človekovih pravic in temeljnih svoboščin.

Podjetja bodo z internimi akti določila možne poti za notranjo prijavo (preko spletnega obrazca, po pošti, telefonu ali osebno...). Pri odločitvi o izbiri poti bo treba upoštevati potrebo po zagotavljanju zaupnosti identitete prijavitelja. Zaupnost ne bo zagotovljena, če bo kot edina možnost za prijavo določena osebna prijava pooblaščencu za skladnost poslovanja, saj bi lahko drugi zaposleni, in med njimi tudi prijavljena oseba, na podlagi obiskov pooblaščenca za skladnost ugotovili identiteto prijavitelja. Primerna pot za prijavo tudi ne bo nezaščiten poštni nabiralnik, ki z malo napora omogoča, da se seznanimo z njegovo vsebino. Tudi zaradi navedenih razlogov se vedno več podjetij že danes odloča za programske rešitve, ki ob zagotavljanju anonimnosti prijavitelju omogočajo varno dvosmerno komunikacijo med prijaviteljem in uslužbencem ali službo, ki obravnava prijavo. Večje korporacije zaposlenim dodatno omogočajo, da lahko prijavo podajo odvetniškim družbam (varuhom), ki so vstopne točke za sprejem in nadaljnje pošiljanje prijav. Zaradi varstva poklicne tajnosti oziroma zaupnosti razmerja med odvetnikom in stranko, je pri tem zagotovljena zaupnost identitete prijavitelja.[3] V skladu z Direktivo bodo vsi pravni subjekti, ki imajo vsaj 50 zaposlenih, morali imenovati posameznika za sprejem in obravnavo prijave, dodatno pa bodo lahko v sistem zaščite prijaviteljev implementirali še druge kanale in zunanje strokovnjake (zunanje svetovalce, revizorje, predstavnike sindikatov ali predstavnike zaposlenih, a le pod pogojem, da bodo zagotavljali ustrezna jamstva glede neodvisnosti, zaupnosti, varstva podatkov in tajnosti).

Zaupnost identitete bo treba zagotavljati prijaviteljem, ki bodo na podlagi utemeljenih razlogov menili, da so bile prijavljene informacije o kršitvah ob prijavi resnične in da take informacije spadajo na področje uporabe Direktive. Zaupnost identitete pomeni, da brez soglasja prijavitelja ni dovoljeno razkriti njegove identitete ali naveznih okoliščin (vsebine prijave, ki razkriva identiteto prijavitelja) nepooblaščenim osebam. Zaupnost identitete je prva obrambna linija, ki je najbolj preprosta in hkrati najbolj učinkovita pri preprečevanju možnosti nastanka povračilnih ukrepov. Največkrat se ravno zaradi strahu pred razkritjem posamezniki bojijo prijaviti nepravilnosti. Drugi razlogi, da posamezniki ne spregovorijo, so tudi percepcija, da bo nezakonito ravna-

Žvižgači v podjetjih niso le generatorji dodane vrednosti in ne predstavljajo le stroška dela, ampak so tudi branik etičnosti in zakonitosti. Ker se prvi in neposredno seznanijo z nepravilnostmi, je njihova informacija praviloma verodostojnejša in lahko bistveno prispevajo k ohranjanju ugleda, zmanjšanju izdatkov za razne inšpekcijske postopke, zmanjšanju odškodnin zaradi nevarnih izdelkov ali na primer zmanjšanju škode zaradi prevar.

nje težko dokazati, da ne bo nič storjenega, ali ker ne vedo komu ali kaj prijaviti.[4]

Zagotavljanje zaupnosti ni enako zagotavljanju anonimnosti. Pri zagotavljanju zaupnosti gre za postopke in ukrepe, ki preprečujejo razkritje identitete posameznika, medtem ko gre pri zagotavljanju anonimnosti za odločitev podjetja ali pristojnega organa, da sprejema in obravnava tudi anonimne prijave.

Čeprav Direktiva omogoča, da se države članice same odločijo ali morajo pravni subjekti v zasebnem ali javnem sektorju in pristojni organi sprejeti tudi anonimne prijave kršitev in na podlagi teh nadalje ukrepati, pa je potrebno upoštevati, da so anonimne prijave že močno usidrane v našo kulturo. Nacionalni predpisi s področij, ki jih omenja Direktiva, ne prepovedujejo sprejema anonimnih prijav. Analiza, ki smo jo opravili na Komisiji za preprečevanje korupcije (v nadaljevanju: Komisija) pa je pokazala, da zadnjih 6 let konstantno beležimo več kot 30 % delež anonimnih prijav. Vsaka tretja prijava, ki jo prejmemo je anonimna. Ko smo podrobneje analizirali koristi anonimnih prijav smo ugotovili, da smo na podlagi vsake pete anonimne prijave opravili odstop prijave drugemu pristojnemu organu, zaznali korupcijsko tveganje ali uvedli preiskavo. Največ odstopljenih anonimnih prijav se je nanašalo na področje javnih naročil, postopkov zaposlovanj v javnem sektorju, delovno-pravno področje, finančno področje, izobraževanje, šolstvo in šport. Navedeno nakazuje na pomembnost obravnave anonimnih prijav, zato velja priporočilo, da podjetja obravnavajo tudi anonimne prijave. Bojazni, da so zlasti anonimne prijave prežete z neresničnimi (zlonamernimi) prijavami in da bodo podjetja z njimi administrativno preobremenjena, so neutemeljene. Na Komisiji smo v zadnjih 6 letih identificirali zgolj 1 zlonamerno prijavo. Anonimna prijava, ki bo vsebinsko pomanjkljiva, ki bo izražala zgolj slabo mnenje o določenem posamezniku, ne bo pa ponujala dokazov o nepravilnostih, v večini primerov niti ne bo primerna za nadaljnjo obravnavo, zato ne gre računati, da bo prihajalo do administrativnih obremenitev. Ob tem je treba pojasniti, da prijava posameznika z namenom maščevanja po definiciji iz Direktive ni zlonamerna prijava, če je prijavitelj na podlagi utemeljenih razlogov menil, da so



bile informacije o kršitvi ob podani prijavi resnične. Direktiva se torej odmika od iskanja motivov za prijavo. Pomembna je le še verodostojnost informacije o kršitvi. Zlonamerni prijavitelj bo zgolj tisti prijavitelj, ki bo delodajalcu, pristojnim organom ali javnosti vedoma razkril neresnične (lažne) informacije o sumu kršitve.

Določitev zaupnika za prejem in obravnavo kršitev

Ob vzpostavitvi notranjih poti za prijavo bodo podjetja imela priložnost izkazati iskreno in pošteno namero glede zaščite prijaviteljev. Podjetje, ki bo želelo zakonito poslovanje ter bo z zgledom vsakodnevno med zaposlenimi utrjevalo pozitivne vrednote, bo kot zaupnika za prejem in/ali obravnavo kršitev imenovalo zaupanja vredno osebo. To je zagotovo posameznik, ki ima lastnosti, kot so osebna integriteta, nepristranskost in načelnost. Oseba, na katero se lahko obrnejo zaposleni po nasvet, ne da bi bili v strahu, da bo razkrita njihova identiteta.

Zaupnik za prejem in/ali obravnavo kršitev bo vsako prijavo moral skrbno preučiti, v sedmih dneh po prejemu pa prijavitelju izdati potrdilo o prejemu prijave ter najkasneje v treh mesecih po potrditvi prejema podati povratne informacije o izvedenih ukrepih. Podatke o prijavitelju, o prijavljeni osebi in tretjih osebah, navedenih v prijavi, bo moral skrbno varovati pred ostalimi sodelavci, ki niso pooblaščeni za sprejem in obravnavo prijav.

Informiranje prijavitelja o zaščiti

Zaupnik bo prijavitelje informiral zlasti o možnih postopkih in poteh za notranjo in zunanjo prijavo ter na splošno o podpornih ukrepih za zaščito, vključno s posebnim statusom in pravicami prijavitelja v sodnih postopkih. Če bo obveljala odločitev iz osnutka Zakona o zaščiti prijaviteljev, bo zaupnik na zahtevo prijavitelja izdajal tudi potrdilo o upravičenosti do zaščite.

Nobeno podjetje ni imuno na prevare, kršitve zakonskih obveznosti in razna neetična ravnanja, ki krnijo ugled in zaupanje javnosti, poslovnih partnerjev, strank in delničarjev.

Prijavljanje nepravilnosti ni nezakonita dejavnost, zato prijavitelji ne bi smeli biti deležni povračilnih ukrepov. Realnost je na žalost mnogokrat drugačna. Že večkrat so bili posamezniki zaradi podanih prijav ali javnih razkritij neutemeljeno izolirani, ignorirani, degradirani, diskriminirani in v sklepni fazi tudi odpuščeni iz krivdnih ali poslovnih razlogov.

Sistem zaščite prijaviteljev bo na preizkušnji vsakič, ko bodo prijave (notranje ali zunanje) podane proti poslovodstvu, svetovalcem uprave in drugim vplivnim posameznikom, ki uživajo zaupanje vodstva. Za preprečitev takšnih situacij bi bilo smiselno, da bi sistem zaščite prijaviteljev v podjetjih (zlasti v sistemih korporativnega upravljanja) oblikovali predstavniki ustanovitelja, nadzorni svet in uprava. Prijavo, podano zoper člane uprave, lahko neodvisno obravnava zgolj nadzorni svet, po drugi strani pa lahko prijavo zoper člane nadzornega sveta neodvisno obravnavajo zgolj predstavniki ustanovitelja, ki imajo pristojnosti za odpoklic v primeru kršitev.



Ne glede na zagotovljeno sodno varstvo, ki mora biti toliko učinkovito, da prijavitelja opogumi, da stopi naprej in zaupniku ali pristojnemu organu sporoči informacijo o sumu kršitve, bi lahko delodajalci razmislili še o dodatnih vzpodbudah, kot so nagrade, priporočila, plačana odsotnost, izleti in podobno.

Žvižgači v podjetjih niso le generatorji dodane vrednosti in ne predstavljajo le stroška dela, ampak so tudi branik etičnosti in zakonitosti. Ker se prvi in neposredno seznanijo z nepravilnostmi, je njihova informacija praviloma verodostojnejša in lahko bistveno prispevajo k ohranjanju ugleda, zmanjšanju izdatkov za razne inšpekcijske postopke, zmanjšanju odškodnin zaradi nevarnih izdelkov ali na primer zmanjšanju škode zaradi prevar.

Zaradi ekonomske odvisnosti od delodajalca se v primeru razkritja žvižgači znajdejo v neugodnem položaju, hkrati pa ne gre spregledati položaja sodelavcev, sorodnikov in drugih posameznikov, ki bodo nudili (četudi zgolj) moralno podporo prijavitelju, ter zaupnikov, ki bodo sprejemali in/ali obravnavali te prijave, zato bo potrebno sprejeti ne le jasne poti za notranjo prijavo in povečati usposobljenost zaupnikov, ampak zlasti sprejeti takšne zakonodajne rešitve, ki bodo učinkovito preprečevale nastanek povračilnih ukrepov zoper ključne deležnike v procesu podaje, sprejema in obravnave prijav.

1 Glej Priporočilo CM/Rec(2014)7 Komiteja ministrov državam članicam o zaščiti žvižgačev, dostopno na https://rm.coe.int/16807096c7>.

2 Po podatkih iz Poslovnega registra Slovenije na dan 28. 2. 2022.

3 https://www.ombudsmen-of-volkswagen.com/

4 Transparency International, Global corruption barometer, 2016, str. 23 in 24. ■

Avtorica: mag. Ana Robnik / svetovalka za raziskave in strateški razvoj, Iskratel, d.o.o., Kranj*



PRIMERI UVAJANJA SISTEMA JAVNEGA OPOZARJANJA V EU

EU je sprejela normativno podlago za uvedbo sistema javnega opozarjanja (angl. Public Warning System s kratico PWS), ki ga bo potrebno uveljaviti v državah Evropske unije do 21.junija 2022. V tem prispevku bo posebej prikazana mednarodna primerjalna praksa izbranih evropskih držav.

Uvod

Svetovna skupnost, države in njihove povezave se vse pogosteje soočajo z raznorodnimi oblikami groženj, od vse obsežnejših in pogostejših naravnih nesreč, kot so požari, poplave, velika neurja in potresi, do terorističnih in ostalih digitalnih napadov, izbruhov bolezni in virusnih pandemij, do dogodkov z množično udeležbo ter industrijskih in drugih nesreč, ki jih povzroči človek ali stroj. Ker imajo te grožnje izjemno velik vpliv na javno varnost, zaščito in reševanje, je zakonska obveza uvedbe Sistema javnega opozarjanja (angl. Public Warning System s kratico PWS) v državah Evropske unije do 21.junija 2022 več kot na mestu. V tem prispevku obravnavamo značilnosti v procesu načrtovanja, implementacije in uvajanja sistema v Grčiji, Nemčiji, Romuniji, Franciji in Belgiji. Vsaka od teh držav uporablja eno ali več tehnoloških možnosti, kot so oddajanje prek mobilnih baznih postaj (angl. Cell Broadcast s kratico CB) po standardu EU-ALERT (ETSI TS 102 900), pošiljanje kratkih sporočil na podlagi lokacije končne naprave (angl. Location Based SMS s kratico LB-SMS) ali prek mobilne aplikacije, ki temelji na storitvi dostopa do interneta (angl. Internet Access Service PWS z oznako IAS-PWS).

Rešitev GR-IPAWS v Grčiji

V Grčiji je implementiran Sistem integriranega javnega alarmiranja in opozarjanja (angl. Integrated Public alert and warning system z oznako GR-IPAWS) [1], ki je odprt za nadgradnje z novimi komunikacijskimi kanali. Pri načrtovanju so uporabljali interdisciplinarni pristop strokovnjakov s področja družboslovja ter s področja ukrepanja v primeru izrednih dogodkov in tehnologij IKT.

GR-IPAWS je enovit sistem, ki uporablja primarni komunikacijski kanal CB, poleg tega pa je na voljo tudi LB-SMS, elektronska pošta, povratni klic 112 na stacionarne telefone; v prihodnosti pa načrtujejo še komunikacijska kanala do družbenih omrežij in do naprav s protokolom CAP (angl. Common Alerting Protocol). Vmesna verzija sistema v letu 2019 je temeljila na komunikacijskem kanalu LB-SMS in bila uporabljena pri obsežnem požaru, vključno s podporo procesu evakuacije. V nadaljevanju so prešli na tehnologijo CB, ki ima manjši vpliv na preobremenjenost omrežja, opozarjanje je na podlagi lokacije in ne na podlagi podatkovne baze številk, prijava in registracija nista potrebni, telefoni imajo vključeno funkcionalnost, ki pa jo lahko uporabniki tudi izključijo (angl. opt-out), poskrbljeno je za zasebnost. Januarja 2020 so hkrati z uvajanjem sistema IPAWS sprejeli tudi Zakon o upravljanju v izrednih razmerah (angl. Emergency Management Act), ki je prestrukturiral civilno zaščito in helenske gasilske enote, ter vzpostavil Nacionalni center za usklajevanje operacij in krizno upravljanje, katerega del je Enota 112, znotraj nje pa je poleg NG 112 PSAP tudi oddelek za IPAWS.

Rešitev IAS-PWS v Nemčiji

V Nemčiji uporabljajo nestandardne aplikacije Katwarn, Nina und Biwapp, ki so bile razvite že pred leti, niso odprto-kodne in so zanje po javno dostopnih informacijah potrebne izboljšave [2]. Temeljijo na centralnem modularnem opozorilnem sistemu (nemško Modulares Warnsystem z okrajšavo MoWaS). Opozorila se posredujejo aplikacijam v mobilnih napravah, ki so povezane preko omrežja WLAN ali mobilne internetne povezave. Dogodek “Warntag” [3] in zadnje velike poplave so pokazale na pomanjkljivosti teh aplikacij. Na prvem dogodku “Warntag” so zaznali probleme pri preizkušanju siren in pri obremenitvi sistema MoWaS, kar je bil vzrok, da številni alarmi niso dosegli uporabnikov aplikacije

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



ali pa jih niso dosegli pravočasno. Skupina, ki je analizirala celotno situacijo [4], je priporočila uporabo standardiziranega komunikacijskega kanala CB, opozorilne aplikacije pa kot koristen dodatek. Zadnje velike poplave v letu 2020 so bile resno opozorilo, zato je nemška vlada predlagala spremembo Zakona o telekomunikacijah (nem. Telekommunikationsgesetz), ki utira pot tehnologiji CB [5]. Znani so tudi rezultati triletnega projekta Warning of the Population [6], ki prinašajo posodobljen sistem MoWaS in izboljšan dostop do sistema po javnem internetu, ki je cenovno ugodnejši od dosedanjih satelitskih povezav. Hkrati so dodali nove opozorilne kanale, kot so sodobne opozorilne aplikacije ali digitalne oglasne table v mestnih središčih.

Rešitev RO-Alert v Romuniji

Realna potreba po sistemu PWS je nastala po nesreči leta 2016, ko je Vlada ustanovila delovno skupino, ki so jo sestavljali romunski regulator, državna telesa, mobilni operaterji in sistemski integrator Special Telecommunication Service (STS) [7].

V Romuniji je implementirana rešitev RO-Alert [8], ki temelji na tehnologiji CB. Pri procesu implementacije velja poudariti časovno dimenzijo, ki je pokazatelj kompleksnosti posameznih delov implementacije [7]. Tehnološki del je bil zaključen septembra 2017 in je trajal 3 mesece, operativni del je bil zaključen aprila 2018 in je trajal 8 mesecev, regulatorni del pa je bil zaključen po treh letih in vključuje zakonsko podlago v zvezi z implementacijo iz leta 2017, z obveznostmi mobilnih operaterjev iz leta 2019 in s prepovedjo mobilnih telefonov brez CB iz leta 2020.

Mobilni operaterji so dali na voljo podatke o baznih postajah na podlagi podpisanih dogovorov o ne razkrivanju. Georedundančna postavitev Centra za celično oddajanje (angl. Cell Broadcast Centre z oznako CBC) zagotavlja visoko razpoložljivost. CBC je centraliziran za vse operaterje in se nahaja pri GIES (angl. General Inspectorate for Emergency) in ne pri posameznem operaterju. Ta odločitev je bila sprejeta na podlagi ocene, da je to najhitrejši način implementacije, kajti noben od operaterjev ni imel pred tem svojega lastnega CBC. Pri mobilnih terminalih so zahtevali združljivost terminala s CB, ki mora biti vgrajen v pametne telefone in prilagojen za državo, podprta sta CMAS 4371 in GSMA 919, uporabnik ima možnost izključiti opozorila (opt-out). V Romuniji so namenili politiki varnosti [7] veliko pozornost od samega začetka. Uvedli so tudi aplikacijo DSU, ki omogoča dvosmerno komunikacijo, uporabniki pa poleg javnih opozoril na območju, ki ga določijo sami, prejmejo tudi ostale informacije. Zanimiva rešitev je javno opozarjanje preko visokega stolpa, ki ga upravlja STS.

Rešitev FR-ALERT v Franciji

V Franciji so izbrali dve tehnologiji, in sicer CB in LB-SMS [9], ki bosta uporabljeni po celotni državi, razen otokov. Zagotovljeno bo množično in hitro pošiljanje. Proizvajalec je izbran zaradi optimalne kombinacije obvladovanja natančnosti lokacije in hitrosti pošiljanja opozoril, ter razumevanja potreb države in mobilnih operaterjev. Sistem je zaživel v drugi polovici leta 2021 na prioritetnih področjih z visoko stopnjo tveganja za nesreče, do junija 2022 pa bo implementiran na ozemlju celotne države.



Rešitev Be-Alert© v Belgiji

Rešitev Be-Alert© [10] je bila uvedena junija 2017 s kraljevim odlokom, in sicer po terorističnih napadih v Bruslju konec leta 2016. Trije glavni telekomunikacijski operaterji (Proxima®, Télémet® in Orange®) so neposredno integrirani v enotno platformo Be-Alert©. Komunikacijski kanal je LB-SMS, prilagojen na velikost države, opozorila se pošiljajo po SMS, kot glasovna sporočila na stacionarne telefonske linije ali po elektronski pošti. Na storitev Be-Alert© se je mogoče naročiti. Opozorila Be-Alert© se sprožijo glede na lokacijo, glede na kontekst in glede na čas dogodka. Izziv je še vedno optimizirati sporočila za ljudi, ki se niso naročili na Be-Alert©.

V Belgiji je še vedno obvezna odobritev javnih opozoril s strani lokalnih oblasti, lokalnega odbora za varnost ali župana. Zato županom ponujajo usposabljanje za uporabo opozorilne platforme skupaj s praktičnimi vajami. Operaterji so dolžni proti plačilu, če tako zahteva center za krizno upravljanje, poslati opozorilna sporočila lokalnim skupnostim, ki so naročene na to storitev. Center za krizno upravljanje plačuje operaterjem glede na število poslanih sporočil in glede na število opozoril.

Zaključek

Za konec omenimo, da je v procesu izbire rešitve, implementacije in uvajanja Sistema javnega opozarjanja v omenjenih državah članicah, moč zaznati naslednje skupne značilnosti:

- celosten in celovit pristop k tehnološkim, organizacijskim in normativnim konceptom ter tesno sodelovanje vseh deležnikov od samega začetka, od ministrstev, regulatorja do operaterjev in ponudnikov mobilnih naprav,
- jasen načrt opozarjanja in alarmiranja z oblikovanimi vsebinami opozoril, vključno z opozorili v več jezikih in s prilagoditvami za osebe z motnjami zaznavanja, pri čemer so vključevali tudi stroko z družboslovnega področja,
- raba več tehnologij opozarjanja za največji možni doseg je zaznana kot prednost, vendar je potrebna pazljivost pri opozorilih, ki vključujejo povezave na druge informacije,
- vgrajena zasebnost in varnost je bila pravilo v mnogih državah,
- izobraževanje, ozaveščanje in informiranje javnosti je izjemno pomembno,
- praktične vaje in preizkušanja so nujni del uvajanja,
- uskladitve organizacijskih pravil in pravno-regulatornega okvira je dolgotrajnejše od tehnološke implementacije,
- pomembna je trajnostna naravnanost rešitve z jasno usmerjenostjo na končnega uporabnika.

Literatura in viri

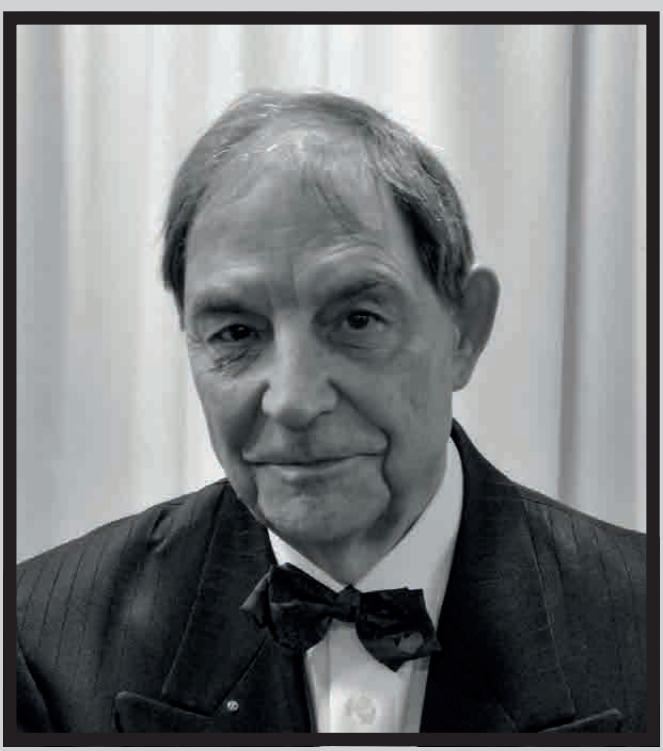
1. Grčija: Georgios Marios Karagiannis, Deputy Secretary General for Civil Protection, General Secretariat for Civil Protection, Greece, videoposnetek na domači strani (https://rb.gy/wqmpyo)
2. Nemčija: Katwarn oder NINA: Welche Warn-App ist besser?, dostopno na povezavi (https://rb.gy/tirmhp)
3. Nemčija: Nationalwide Alert Day, dostopno na povezavi (https://rb.gy/lqnsew)
4. Nemčija: How (not) to set up a public warning system, dostopno na povezavi (https://rb.gy/a2bhre)
5. Nemčija: Cell Broadcast readied in Germany's post flood re--build, dostopno na povezavi (https://rb.gy/yhm3wi)
6. Nemčija: Warning of the Population, dostopno na povezavi (https://rb.gy/1cw84t)
7. Romunija: Konferenca EENA 2021, Riga, sekcija Public Warning Systems
8. Romunija: RO-Alert, dostopno na povezavi (https://rb.gy/3o-1hun)
9. Francija: Network operators follow Mol lead in partnering with Intersec to deliver €50 million public warning system, dostopno na povezavi (https://rb.gy/qykjek)
10. Belgija: Be-Alert, dostopno na povezavi (https://rb.gy/k8jlnb) ■

INGU V SPOMIN IN SLOVO

Pred časom nas je pretresla novica, da nas je za vedno zapustil naš član Ingo Falk Pasch Wallersberg.

Gospod Ingo je s svojim neumornim strokovnim delom v svoji več kot 40 letni karieri bistveno pripomogel k dvigovanju ugleda korporativne varnosti v slovenskem in mednarodnem okolju. V svoji dolgoletni karieri je opravljal ključne funkcije, med katerimi je potrebno posebej izpostaviti ministrovanje v času prelomnih časov osamosvajanja RS, več let pa je bil tudi predsednik Zbornice za razvoj slovenskega zasebnega varovanja. Na tem področju je s svojimi pronicljivimi idejami in visokim strokovnim znanjem zagotavljal, da se je dejavnost razvijala v smeri potreb, ki jih je prinašalo novo poslovno in varnostno okolje. Hkrati je pomembno pripomogel tudi k razvoju kvalitete korporativne varnosti, kot krovne strateške dejavnosti. Ingo je užival visok ugled tako v širšem nacionalnem kot tudi v mednarodnem okolju.

V zadnjem obdobju se je posvetil delovanju znotraj Slovenskega združenja za korporativno varnost, kjer je bil eden od pomembnih članov. S svojimi bogatimi izkušnjami je pomembno pripomogel k rasti ugleda omenjenega združenja in s tem posledično tudi korporativne varnosti kot profesije. Seveda pa je bil njegov neutrudni duh izražen tudi skozi družbene aktivnosti, ki so pokazale njegovo strokovno širino in pripravljenost razdajanja na različnih družbeno pomembnih področjih povezanih z varnostjo. Med drugim je bil tudi prejemnik nagrade za življenjsko delo, ki jo podeljujeta Institut za korporativne varnostne študije in Slovensko združenje korporativne varnosti.



Naj počiva v miru.

13. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

31. MAJ - 1. JUNIJ 2022



DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

SPROŠČENO VZDUŠJE, ODLIČNI PREDAVATELJI, MEDIJSKA ODZIVNOST,
IZMENJAVA NAJNOVEJŠIH SPOZNANJ IN DOBRIH PRAKS.
STROKOVNJAKI KORPORATIVNE VARNOSTI,
KI VLAGAJO V ZNANJE, BODO Z NAMI.
PRIDRUŽITE SE NAM TUDI VI!

WWW.ICS-INSTITUT.SI