Korporativna varnost

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

Letnik 2022, maj • št. 29



Slovensko združenje korporativne varnosti

vključujoča platforma sodelovanja javno-zasebnega partnerstva

Pred nami so pomembni izzivi v elektroenergetiki

mag. Aleksander Mervar, direktor ELES



S SISTEMSKIM VARNOSTNIM PREGLEDOM IN PENETRACIJSKIM (VDORNIM) TESTIRANJEM DO VEČJE KIBERNETSKE VARNOSTI

V okviru instituta deluje Center za informacijsko varnost, ki se v prvi vrsti ukvarja s področjem testiranja v IT okoljih oziroma varnostnimi pregledi.

- ⇒ Prepoznavanje in odkrivanje šibkih točk v organizacijah
- ⇒ Ocena skladnosti varnostnih politik
- ⇒ Ocena skladnosti vse programske in strojne opreme
- ⇒ Preizkusi ozaveščenosti zaposlenih o varnostnih vprašanjih
- ⇒ Odziv v primeru varnostnega incidenta na podlagi realno izvedljivih metod
- ⇒ Ravnamo se po več mednarodno priznanih metodologijah
- ⇒ Uporabljamo vrsto različnih programov in pripomočkov
- ⇒ Rezultat varnostnega testiranja so pisna poročila in so ključnega pomena pri zagotavljanju najvišjih standardov organizacije
- ⇒ Organizacijam priporočamo opravljanje varnostnega pregleda in testiranje v letnem intervalu ali po vsaki večji implementaciji oz. spremembi v IT okolju.

Ekipa strokovnjakov Instituta za korporativne varnostne študije, ki je specializirana za kibernetsko varnost, bo s poglobljenim tehničnim znanjem ter pridobljenimi certifikati poskrbela za strokovno in neodvisno testiranje, ki vam bo razkrilo ranljivosti vašega informacijskega sistema.

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

Kontakt: info@ics-institut.si / telefon: 05 90 54 300
spletna stran: www.ics-institut.si

EC-Council CHFI CERTIFIED
EC-Council CPENT CERTIFIED
EC-Council CEH CERTIFIED
EC-Council ECIH CERTIFIED
OFFENSIVE security OSCP

ISO 27001

CERTIFIKAT O USPEŠNO OPRAVLJENEM IZPITU ZA VODILNEGA PRESOJEVALCA ZA PODROČJE PR320: ISMS ISO 27001:2013

BUREAU VERITAS 1828

DPO

CERTIFIKAT O USPEŠNO OPRAVLJENEM ZAKLJUČNEM IZPITU NA SEMINARJU ZA POOBLAŠČENO OSEBO ZA VARSTVO OSEBNIH PODATKOV



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:
maj 2022

Izvod revije je brezplačen

Naslovnica in slike:
Illustration 125486217 © Nmedia | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

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

Pred nami se nahaja številka revije Korporativna varnost, ki jo vsako leto posebej posvetimo najpomembnejšemu letnemu dogodku Dnevi korporativne varnosti. Glede na dejstvo, da nas mednarodno varnostno okolje vedno pogosteje preizkuša z novimi kriznimi situacijami, ki potrebujejo učinkovito odzivanje za zagotavljanje neprekinjenega delovanja naših organizacij, so pričujoče vsebine pomemben del posredovanja izkušenj, katere nam pomagajo, da skupaj rastemo kot strokovna skupnost. Krize si v zadnjem obdobju praktično ne sledijo več v nekih dokaj predvidljivih cikličnih amplitudah, temveč so postale stalnica, ki se razlikuje samo po stopnji kompleksnosti in obsegu vpliva. Poleg navedenega zahtevnega mednarodnega okolja je bil v zadnjem času fokus slovenske javnosti usmerjen predvsem v parlamentarne volitve, ki so nepotrebno odvračale pozornost od realnih problemov s katerimi so soočene naše organizacije in država. Seveda je stabilnost nacionalnega političnega okolja nujna za nemotenost delovanja širše družbene skupnosti. V tem okviru še vedno nekoliko pogrešamo zmožnost političnih akterjev, da presežejo različnost pogledov in pristopov pri uveljavljanju na področju vitalnih interesov Republike Slovenije. V tem okviru ima poseben pomen kontinuiranost vodenja organizacij, ki upravljajo s kritično infrastrukturo v Republiki Sloveniji. Določen vpliv na nepredvidljivost ustvarja tudi nedorečenost in nezmožnost sprejemanja tistih nujnih zakonskih predpisov, ki so pomembni za zagotavljanje pravne predvidljivosti in podlag za normalno delovanje teh družbenih sistemov. Krizne situacije v mednarodnem okolju nam ne dopuščajo več časa za počasno odraščanje demokratične skupnosti. Vedno večja potreba bo usmerjena v iskanje soglasja, kateri so tisti ključni procesi v družbi, ki ne morejo biti predmet različnih političnih pristopov vsakokratne izvršilne politike. V zadnjem obdobju smo tudi s pomočjo razprav in stališč objavljenih v tej strokovni reviji prispevali k dvigu zavedanja o pomembnosti delovanja kritične infrastrukture in zagotavljanju potrebe po njenem neprekinjenem delovanju. Poleg strokovne javnosti imajo tukaj ključno mesto ravno strateški odločevalci v nacionalnem in gospodarskem okolju. Temu področju je bilo v zadnjem obdobju namenjeno zelo veliko pozornosti, kar se odraža tudi v pričujoči številki, ki prinaša intervjuje s pomembnimi strateškimi odločevalci in njihove poglede na pomen zagotavljanja nacionalne in korporativne varnosti sistemov in organizacij, katere tudi s svojim vodenjem pomembno oblikujejo. Pomembna ugotovitev pa je, da smo uspeli, tudi s trudom Slovenskega združenja za korporativno varnost, zagotoviti dojemanje korporativne varnosti, kot enega izmed ključnih orodij v organizacijah, ki zagotavljajo učinkovitejše obvladovanje tveganj. Deloma je k temu pripomoglo tudi obdobje, kot že rečeno, v katerem se krize vrstijo ena za drugo. Organizacije, ki temu ne posvečajo dovolj pozornosti vedno težje zagotavljajo svoje preživetje v zahtevnem globalnem gospodarskem okolju.

Ravno zaradi tega smo v tokratni številki revije želeli vsebinsko osvetliti dovolj širok spekter strokovnih prispevkov. 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
g. Cvetko Sršen, predsednik uprave Telekoma Slovenije, d.d.

DINAMIČNE SPREMEMBE VARNOSTNEGA IN TEHNOLOŠKEGA OKOLJA POMEMBNI IZZIVI ZA TELEKOM SLOVENIJE

10



INTERVJU
mag. Nada Drobne Popović, predsednica uprave Petrol d.d.

PETROL PROCESOM UPRAVLJANJA TVEGANJ NAMENJA POSEBNO POZORNOST PRI SVOJEM POSLOVANJU

20



INTERVJU
g. Boštjan Šefic, svetovalec predsednika republike za nacionalno varnost

POTREBUJEMO DODATNE SINERGIJE ZA POVEČANJE UČINKOVITOSTI NACIONALNO VARNOSTNEGA SISTEMA

25



INTERVJU
ga. Mojca Prelesnik, informacijska pooblaščenka Republike Slovenije

PROCESI VAROVANJA ZASEBNOSTI V NENEHNEM ISKANJU RAVNOTEŽJA V DRUŽBENI SKUPNOSTI

30



INTERVJU
mag. Tanja Muha, direktorica Agencije za komunikacijska omrežja in storitve Republike Slovenije

REGULATORNI ORGANI IMAJO IZREDNO POMEMBNO VLOGO ZA OHRANJANJE RAVNOVESJA V EKOSISTEMU ELEKTRONSKIH KOMUNIKACIJ

36

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

INTERVJU
mag. Aleksander Mervar, direktor ELES d.o.o.*

PRED NAMI SO POMEMBNI IZZIVI V ELEKTROENERGETIKI

Geopolitična varnostna tveganja in razvoj informacijskih tehnologij bodo pomembno vplivali na zagotavljanje neprekinjenosti delovanja prenosnega omrežja prihodnosti. To bo predstavljalo velik izziv, ki bo poleg ostalega, zahteval tudi sistemski pristop upravljanja korporativne varnosti. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Aleksandrom Mervarjem.

Nahajamo se v zahtevnih časih, ki na energetskem področju prinašajo pomembne dileme in izzive. Kako v ELESU čutite vpliv Ukrajinske krize, ki bo na področju oskrbe z energenti prinesla pomembne spremembe?

ELES je družba slovenske elektroenergetike, ki skrbi za nemoteno delovanje celotnega slovenskega elektroenergetskega sistema. Ne ukvarja pa se s trženjem in prodajo električne energije. Zato so vplivi posredni. Kupuje elektriko za pokrivanje izgub na prenosnem omrežju, kupuje in prodaja elektriko za 15 minutne izravnave ter elektriko za sistemske storitve. Najbolj drastičen primer je ocena stroškov izgub na prenosnem omrežju za letošnje leto. Povprečje zadnjih nekaj let je znašalo okrog 17 mio EUR/letno. Za letošnje leto ocenjujemo, da bodo stroški preko 50 mio EUR. Razlog so ekstremno visoke cene elektrike na borzah. Razlika je, da preko 33 mio EUR pomeni potrebo po 30% zvišanju tarif za uporabo prenosnega omrežja. Povsem odprta pa je situacija za primer, da bi Ukrajina porabljala elektriko, proizvedeno v evropskem sinhronem območju, kamor je bila vključena pred kratkim, zanjo pa nič plačala. Možni sta dve situaciji, prva, da EU ustanovi t.i. »kritni fond«, druga, slabša pa, da se to socializira po nekem ključu, na nivoju držav članic EU oz. za nas še slabše, po sistemskih operaterjih.

Glede na dejstvo, da je elektroenergetika vselej odvisna od nemotenega zagotavljanja prenosnih poti v širšem mednarodnem okolju, kako lahko take krize, kot je Ukrajinska, vplivajo na prenosne zmogljivosti v našem neposrednem regijskem prostoru?

Če odmislim sabotaže, kibernetske napade, vojno stanje izven območja Ukrajine, neposrednega vpliva na prenosne poti ni.

Digitalizacija je proces, ki se ga ne boste mogli izogniti tudi v energetiki. Robustnost in neprekinjenost delovanja sta dva izredno pomembna pogoja za delovanje prenosnega elektroenergetskega omrežja. Kako zagotoviti, da bodo ti procesi digitalizacije postopni in obvladljivi?

Robustnost, digitalizacija! Dajva najprej o teh dveh pojmih. Robustnost pojmujem kot vlaganje v hardware, v omrežje. Digitalizacijo pa pojmujem kot software, kot tisto orodje, s katerim se optimizira vlaganje v robustnost, da ne bo slednje edino posvečeno, še več, pretirano!

Dosedanja praksa je, da potrebujemo za pridobitev vseh okolijsko-upravnih dovoljenj več kot 10 let, kar je nevzdržno. Ne samo to, tudi ne omogoča časovno usklajenega prehoda k obnovljivim virom. Tu bo potrebno bolj pogosto uveljavljanje javne koristi, predvsem pa prevetriti obstoječo zakonodajo s tega področja in procese odločanja pri izdaji teh dovoljenj. Menim, da bo to ena izmed prioritetnih nalog nove Vlade RS.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



V zadnjih desetih letih v ELES dajemo prednost digitalizaciji. Na tem področju smo naredili ogromno, čaka pa nas še veliko izzivov.

Največji izziv so kadri z ustreznimi kompetencami. Tu smo v naši državi, zaradi majhnosti, zelo šibki. Vse nove, sofisticirane naprave, katere implementiramo v naše prenosno omrežje, so visoko digitalizirane. Za vse to potrebujemo kader. Pri digitalizaciji je pomembno, da se ne zaletimo v preširoko fronto, katero z razpoložljivimi resursi ne bomo sposobni obvladovati. Potreben je premišljen pristop in določitev prioritet. Bom dal samo en primer. Security Operations Center (SOC). Na začetku razmišljanja smo bili skoraj prepričani, da bomo imeli svojega. Bolj natančna analiza pa nas je pripeljala do ugotovitve, da to ne bo mogoče. Razlog so kadri, zato smo menjali strategijo. Se pravi, ne vse na »prvo žogo«!

Umeščanje nove prenosne infrastrukture je precej počasen in zapleten proces. Kaj bi bilo potrebno še postoriti, da bi lahko pospešili vnos nujnih prenosnih poti v elektro energetiki?

ELES bo letos maja, če bo vse po načrtih, dal pod napetost nov visoko napetostni daljnovod Cirkovce – Pince 2x400 kV. Naj kar na začetku podam zanimivo primerjavo – termična kapaciteta tega daljnovoda znaša 2.600 MW, kar je enako moči dveh in pol NEK II. S tem daljnovodom bomo povezani z vsemi prenosnimi sistemi sosednjih držav. Do konca leta 2030 zato ne načrtujemo nobenih novih čezmejnih daljnovodov. Tisto, kar je nujno, pa se nanaša na bodoče investicije v priključne daljnovode, ki bodo povezovali velika polja sončnih in vetrnih elektrarn s prenosnim omrežjem. Dosedanja praksa je, da potrebujemo za pridobitev vseh okolijsko-upravnih dovoljenj več kot 10 let, kar je nevzdržno. Ne samo to, tudi ne omogoča časovno usklajenega prehoda k obnovljivim virom. Tu bo potrebno bolj pogosto uveljavljanje javne koristi, predvsem pa prevetriti obstoječo zakonodajo s tega področja in procese odločanja pri izdaji teh dovoljenj. Menim, da bo to ena izmed prioritetnih nalog nove Vlade RS.

Verjetno je še bolj kot zagotavljanje dodatnih prenosnih zmogljivosti na ELES-u pomembno razumevanje, da je potrebno zagotavljati tudi okrepitev prenosnih omrežij na ravni distribucijskega omrežja?

Ja, se povsem strinjam. O tem sem se kar obširno razgovoril v mojem intervjuju 09.04.2022 v Dnevnikovem Objektivu. Obstoječe distribucijsko omrežje v povprečju gledano, ne omogoča priklapljanja večjih moči razpršenih proizvodnih virov OVE, električnih polnilnic za vozila, in pa koncentrirano nameščanje novih toplotnih črpalk. Razumevanje bo potrebno na več straneh. Agencija za energijo bo morala distribucijskim podjetjem priznavati investicije v omrežje »v naprej«. Distribucijske družbe pa bodo morale že enkrat dokončno razumeti metodologijo Agencije za energijo glede reguliranja in ne pričakovati, da bodo investirali v okviru prostega letnega denarnega toka. Morali se bodo zadolžiti, tako kot to počno prenosna in distribucijska podjetja v EU. Slovenski državni holding se bo moral v prihodnje odpovedati izplačilu dividend, ravno tako mali delničarji, ostali deležniki pa bodo morali razumeti, da je omrežnina tako za prenosno kot za distribucijsko omrežje, če želimo zeleni preboj, prenizka.

Premik k uporabi bolj zelene in okolju sprejemljive energetske porabe bo od določenega dela izkoriščanja fosilnih goriv težišče še bolj premikal v smeri uporabe električne energije, ki bo proizvedena s strani alternativnih produkcijskih virov. To verjetno tudi pred ELES postavlja določene izzive

še boljše učinkovitosti uporabe prenosnih omrežij, zmanjšanja izgub in predvsem uvajanja dodatnih tehnologij, ki bodo to razpršenost proizvodnih zmogljivosti spravila v nek obvladljiv sistem?

S to problematiko smo se začeli ukvarjati že pred petnajstimi leti. Pričelo se je z odločitvijo in izvedbo investicije v prečni transformator v Divači, nadaljevalo se je leta 2010 s pričetkom projekta SUMO , krona vsega pa sta projekta NEDO in SincroGrid. O prvem je bilo v medijih napisanega veliko, zato se ne bom ponavljal. Raje se bom osredotočil na drugi projekt. Tehnološko, z vidika delovanja prenosnega omrežja z uporabo novih tehnologij, je slednji izjemen. Zaradi pričakovanega vedno večjega vključevanja decentraliziranih obnovljivih virov energije, tako na območju Slovenije, kot na območju Hrvaške, smo ocenili, da bo primanjkovalo virov prožnosti, ki so potrebni za uravnavanje elektroenergetskega sistema. Operaterji prenosnega omrežja (HOPS in ELES) in distribucijskega omrežja (HEP ODS in SODO) Hrvaške in Slovenije smo zato leta 2014 začeli iskati skupne rešitve. Kot najobetavnejša se je pokazala vzpostavitev mednarodnega sodelovanja pri vzpostavljanju pametnih omrežij in rodila se je ideja za projekt SINCRO.GRID. Projekt je bil najbolj ocenjen projekt EU s področja pametnih omrežij za prenosne sisteme leta 2016. Pridobili smo skoraj 50 mio EUR nepovratnih sredstev in letos ga zaključujemo.

Leta 2020 smo ustanovili konzorcij podjetij iz Slovenije (ELES, Elektro Celje, Elektro Gorenjska, Elektro Ljubljana, GEN-I), Avstrije (KNG-Kärnten Netz GmbH) in Hrvaške (Hrvatski operator prijenosnog sustava, HEP Operator distribucijskog sustava, Hrvatska elektroprivreda), ki ga koordinira ELES. Odločili smo se za oblikovanje skupnega projekta, s katerim želimo optimizirati uporabo obstoječe elektroenergetske infrastrukture in omogočiti vključevanje novih tehnologij in naprednih funkcionalnosti v prenosna in distribucijska omrežja v Avstriji, na Hrvaškem in v Sloveniji. Projekt smo poimenovali GreenSwitch. Ugotovili smo, da bomo izzive, povezane z vključevanjem vedno večje količine nepredvidljivih obnovljivih virov energije, lažje in ekonomsko učinkoviteje rešili s povezovanjem. V okviru projekta bomo vlagali v primarno infrastrukturo ter uvedli različne tehnologije, platforme in funkcionalnosti za razvoj pametnih omrežij. Ti bodo kombinirani z baterijskimi hranilniki električne energije in visoko digitaliziranimi informacijskimi sistemi. Ker sta prilagajanje odjema in proizvodnje ključnega pomena za prihodnji razvoj omrežja in usklajeno optimizacijo na ravni prenosnega in distribucijskega omrežja, bo GreenSwitch potrošnikom omogočil, da postanejo aktivni udeleženci na elektroenergetskem trgu. Projekt smo prijavili na Komisijo EU, slednja je 30.06.2021 sporočila, da je projekt najboljši od vseh prijavljenih. Njegova ocenjena vrednost se giblje okrog 210 mio EUR. Projekt se je lanskega oktobra uvrstil na t.i. PCI listo (angl. »Projects of Common Interest«). Smo v fazi izdelave dokumentacije za prijavo na nepovratna sredstva EU sklada CEF (angl. »Connecting Europe Facility«).

Več o vseh teh projektih si lahko preberete na naši spletni strani (www.eles.si).



ELES je aktiven v celem nizu mednarodnih projektov. Ob tem vam čestitamo za smelost in vizijo na tem področju. Kako najti način, da Agencijo za energijo prepričate, da so taki razvojni napori nujni za izboljšanje kvalitete in učinkovitosti sistema in, da to ne sme biti smatrano kot prihodek organizacije, zaradi katerega jim kasneje odmerja manjšo povprečnino?

Tu moram pohvaliti Agencijo za energijo. Če analiziram regulativno metodologijo za obdobje let 2016 do 2018, 2019 do 2021, z zadnjo veljavno za leto 2022, lahko ugotovim številne spremembe, katere je uvedla Agencija za energijo in katere spodbujajo regulirane družbe, med njimi tudi ELES, da pridobivajo nepovratna sredstva, da prioritetno vlagajo v t.i. »pametna omrežja«, da se vključujejo v mednarodne razvojno-raziskovalne in pilotne projekte. S tem so nam dali nov zagon za vse te aktivnosti.

Regulirane družbe moramo v okviru načrtovanja in poročanja pri letnih poročilih računovodske izkaze razmejevati na postave regulirane in ne regulirane dejavnosti. Agencija za energijo, če so podane pravilne osnove, utemeljitve čistih izplenov iz ne reguliranih dejavnosti ne uvršča med regulirane prihodke. Glede na določila 5. odstavka 45. člena ZOEE (Zakon o oskrbi z električno energijo)

morajo regulirane družbe pridobiti soglasje Agencije za energijo za opravljanje ne reguliranih dejavnosti. To določilo se uporablja od novembra 2021 dalje.

Kakšna je vaša ocena na področju varnostnega zavedanja zaposlenih, ki je bilo še posebej pomembno v času epidemije COVID-19, ko je večina delala izven delovnega okolja? Ste zadovoljni z rezultati dela, ki so jih vaši sodelavci na tem področju korporativne varnosti vlagali v preteklih obdobjih?

Vedenje in zavedanje zaposlenih v družbi Eles d.o.o. o temeljnem apostolatu družbe, kar predstavlja nemoten in neprekinjen prenos električne energije, je na visoki ravni.

Tveganja krovno obvladujemo preko sistemov upravljanja kakovosti, katerega sestavni del je Katalog tveganj na operativni ravni in izvedbeni ravni, s pomočjo obratovalnih navodil in drugih predpisov, ki urejajo obratovanje elektroenergetskega sistema (EES). Neprestano izboljševanje delovnih procesov je naša stalna aktivnost z namenom zmanjšanja tveganj, predvsem tistih najpomembnejših, ki se nanašajo na delovanje najbolj vitalnih delov EES. Kot pomembno tveganje smo, že pred samo epidemijo, med drugim zaznali tveganja nerazpoložljivosti operativnega osebja zaradi bolezni. Tveganja vezana na epidemijo korona-virusne bolezni so zagotovo v preteklih dveh letih vplivala na poslovanje, ne samo Elesa, temveč celotnega spektra gospodarstva, družbe kot take. V tej zvezi smo v Elesu sprejeli in izvajali skupno več kot 330 ukrepov. Z visoko motivacijo in aktivnim sodelovanjem vseh zaposlenih so se tudi v času epidemije Covida-19 izvajale vse načrtovane aktivnosti, s katerimi so bile zagotovljene korporativne varnostne komponente za vzpostavljanje varnega in zdravega delovnega okolja in 100% izvedbo zadanih delovnih nalog. Varno in zdravo delovno okolje pa je zgolj kamenček v mozaiku elementov, ki jih na podlagi zaznave, prepoznave in identifikacije tveganj, načrtujemo, izvajamo in spremljamo, v okviru sistema korporativne varnosti. Če omenim samo integriran sistem zagotavljanja tehnične varnosti, ki smo ga v zadnjih štirih letih zgradili in popolnoma prenovili, da deluje enotno na vseh lokacijah ELES, pa ukrepi za zagotavljanje neprekinjenega poslovanja družbe, ukrepi vezani na področje informacijske varnosti, varovanja ključnih informacij družbe, varnosti zaposlenih in deležnikov družbe, načrtovanje nalog in aktivnosti v izrednih stanjih, vojni, kriznih situacijah, civilna obramba, načrtovanje in izvajanje aktivnosti nalog zaščite, reševanja in pomoči, in še bi lahko našteval. Vsi procesi so nedeljiva celota, kar postavlja poslanstvo korporativne varnosti v širši nepogrešljiv okvir delovanja gospodarske družbe. In samo integrirano izvajanje vseh procesov na koncu pripelje do želenih ciljev. To je neizpodbitno in dokazano tudi v praksi uspešnega delovanja družbe Eles, d.o.o.

Izzivi in tveganja kibernetske varnosti so verjetno tisti, ki nas trenutno najbolj skrbijo, posebej v relaciji neprekinjenega delovanja kritične infrastrukture. Kateri so tisti zadnji koraki, ki bi jih izpostavili na tem področju za grajenje dodatnih kadrovskih in tehnoloških zmogljivosti?

Da, tveganja kibernetske varnosti so v zadnjem času res skrb vzbujajoča, predvsem za sektor kritične infrastrukture in izvajalce bistvenih storitev, saj negativno vplivajo na izvajanja njihovega poslanstva in s tem ohromitev družbe kot celote. Potreba po medsebojnem povezovanju elektroenergetskih deležnikov in s tem odpiranje napram svetu, Epidemija COVID 19 in s tem v večji meri prehod na delo od doma ter konflikt v Ukrajini, so prinesla nova kibernetska tveganja. Da so ta tveganja realna, kaže tudi kibernetski napad na EE infrastrukturo v Ukrajini, ki se je zgodil ta mesec – 8.4.2022 (CERT-UA). Zavedanje, da je evropski EE sistem tako dober, kot njegov najšibkejši člen v verigi, je EU in njene inštitucije (evropska komisija, Acer,... tudi ENTSO-E in DSO) vzpodbudilo k sistemskemu pristopu in vzpostavitvi enotnih pravil, prenovi zakonodaje, vzpodbujanju sodelovanja in usklajevanja v boju proti kibernetskemu kriminalu. Družba ELES se pomena neprekinjenosti poslovanja in vpliva informacijskih tveganj nanj dobro zaveda, zato je že pred leti naslovila to problematiko s sistemskim pristopom. Družba je tako že deseto leto nosilec certifikata ISO 27001. Da se zavedanje o informacijski varnosti krepi, priča tudi dejstvo, da je bila v preteklem letu družba ELES podvržena sedmim zunanjim, neodvisnim pregledom in inšpekcijam, ki so pokazali, da je družba ELES, na področju zagotavljanja informacijske varnosti ubrala pravi pristop. Kibernetska tveganja smo posebej opredelili v katalogu tveganj, nenehno uvajamo nove ukrepe, s katerimi jih obvladujemo, spremljamo realizacijo ukrepov ter o tem poročamo pristojnim organom.

Konkretnih korakov na področju kibernetske varnosti sicer ne moremo razkrivati, smo pa naša prizadevanja na tem področju usmerili:

- v povečevanje aktivnosti na področju domačega in mednarodnega sodelovanja in izmenjave informacijsko varnostnih informacij (ENTSO-E, Cybersecurity group ENTSO-E, mednarodna vaja CyberCoalition 2021, sodelovanje z URSIV in SICERT,...),

- v povečanje obsega in pogostosti testiranja postopkov neprekinjenega poslovanja (opomba: na podlagi ZinfV smo lani planiranli 22 testov, izvedli 21),

- v aktivnosti za povečanje preglednosti in centralizacije tehničnega upravljanja informacijske varnosti (opomba: izgradnja ad hoc varnostno nadzornega centra in študija za sistemski pristop k vzpostavitvi VOC),

- v željo po dvigu ozaveščenosti med zaposlenimi, v izgradnjo informacijsko varnostne kulture v podjetju, kjer so usposabljanja in preverjanja s področja informacijske varnosti deležni vsi zaposleni (opomba: izobraževanje za vse, izpit po izobraževanju in redno izvajanje ribarjenja med zaposlenimi, strokovna usposabljanja sistemskih inženirjev).

Pri tem vašem vprašanju bi omenil, da bo morala Agencija za energijo primerno ovrednotiti nov regulatorni okvir za prihodnja leta in v njem pripoznati dodatne stroške za kibernetsko varnost.

Katere strateške izzive, ki bodo v naslednjem obdobju pomembno vplivali na razvoj elektroenergetike v Sloveniji, bi izpostavil za konec našega pogovora?

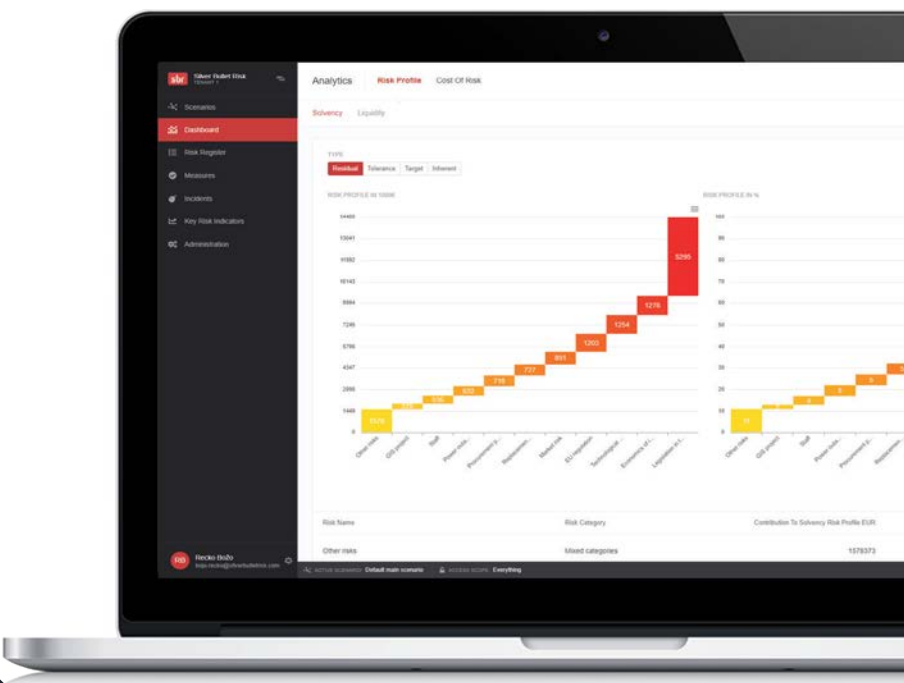
Znanja za uspešen bodoči razvoj slovenske elektroenergetike je pri nas dovolj. Vprašanje je, če smo ga sposobni pravilno uporabiti, predvsem pa, pravočasno. Pomembno je tudi, ali bomo v bodoče elektroenergetsko strategijo gradili na podlagi lokalnih interesov, tako kot sedaj, ali pa bomo končno dali prednost nacionalnim interesom. Ključno pa je, da se bodo vsi deležniki pričeli zavedati, da bo bodoči razvoj elektroenergetike zahteval bistveno večja vlaganja, kar bo povzročilo višje končne cene elektrike. Naj to ne zveni kot pesimizem ali strašenje, gre le za preprosto dejstvo. ■

Foto: arhiv ELES

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

INTERVJU
g. Cvetko Sršen, predsednik uprave Telekoma Slovenije, d.d.*

DINAMIČNE SPREMEMBE VARNOSTNEGA IN TEHNOLOŠKEGA OKOLJA POMEMBNI IZZIVI ZA TELEKOM SLOVENIJE

Telekom Slovenije s pomembno mero ambicioznosti razvoja novih poslovnih in tehnoloških pristopov, ki v Slovenijo in širši regijski prostor prinašajo nujno potrebne nove modele za zagotavljanje kibernetske varnosti, stopa naproti izzivom dinamičnega varnostnega okolja. Ob tej priložnosti smo se o izzivih razvoja in smelih korakih na področju kibernetske varnosti pogovarjali z g. Cvetkom Sršenom, predsednikom uprave Telekoma Slovenije.

S svojim poslovanjem ste močno prisotni v nacionalnem, kakor tudi širšem regijskem področju telekomunikacijskih storitev, kjer so varnostna tveganja še posebej specifična. Zadnje obdobje je prežeto z globalnimi krizami, ki močno vplivajo tudi na vaš sektor. Kako v teh zahtevnih razmerah iščete cilje za nadaljnji razvoj podjetja?

Panoga telekomunikacij se nenehno spreminja. V 30-ih letih, kolikor je v letu 2021 minilo od uvedbe mobilne telefonije in interneta v Sloveniji, smo naredili ogromen tehnološki preskok in razvoj. V vsem tem času se je veliko spremenilo, navdušujejo nas vedno nove in nove tehnologije in storitve, tako da lahko rečem, da smo v telekomunikacijah na nenehne spremembe navajeni. In čeprav bo morda zvenelo kot oguljena fraza, je vsaka krizna situacija resnično lahko tudi priložnost. Tako je, na primer, pandemija covid-19 izrazito pospešila digitalizacijo gospodarstva in družbe nasploh ter dodatno izpostavila pomen, ki ga imajo zanesljive, sodobne, hitre in varne komunikacije in komunikacijske rešitve. Pandemija je v Sloveniji povzročila množično in hitro transformacijo dela in učenja na daljavo, skladno s tem so se spremenili tudi prometni tokovi in obremenitve našega omrežja. Soočili smo se z velikim porastom obremenitev in količin prometa govornih, podatkovnih in video storitev, in sicer za več kot polovico glede na običajno situacijo ter beležili velik porast prometa pri dostopu do

Skratka, naša naloga je, da z lastnim znanjem razvijamo najsodobnejše komunikacijske rešitve, ki poenostavljajo življenje. In ta razvoj na različnih področjih se bo nadaljeval tudi v prihodnje. Na ta način vsak dan udejanjamo svojo vizijo, ki se glasi - digitaliziramo svet priložnosti.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

globalnega interneta omrežij in IPTV. Na okoliščine, v katerih smo se skupaj znašli, smo se sistematično in pravočasno pripravili tako z vidika tehnologije, zagotavljanja varnosti omrežja in storitev kot z vidika kadrov in procesov. In to je po mojem mnenju ključno – da se znamo vedno znova hitro odzvati in prilagoditi.

Na ravni Skupine Telekom Slovenije imamo sprejet strateški poslovni načrt za naslednje petletno obdobje, ki ga ravno zaradi tehnološkega razvoja in hitrih sprememb, ki se v telekomunikacijah dogajajo, vsako leto posodabljamo in pripravljamo letni poslovni načrt. To je način našega delovanja.

Nekatere analize ocenjujejo, da je čas korona krize za področje digitalizacije in informatizacije v družbi naredil poseben pospešek. Kot ste že omenili, pa so lahko te krize tudi dejavnik za iskanje novih tehnoloških in poslovnih priložnosti.

Drži, digitalizacija je aktualna tema že vrsto let, s pandemijo covid-19 pa je dobila velik pospešek, saj se je v določenem obdobju velik del poslovanja in življenja prenesel v digitalni svet. V Telekomu Slovenije spremljamo tako globalne trende kot potrebe podjetij in uporabnikov pri uporabi IKT-storitev. Skladno s tem uvajamo novosti in izkoriščamo priložnosti, ki jih digitalizacija prinaša. Med pandemijo smo kot nacionalni operater vsem – uporabnikom, podjetjem, gospodarstvu ter državnim institucijam in organom – dokazali, da smo zanesljiv in močan partner, na katerega se lahko zanesejo. Hkrati pa smo tudi v tem obdobju skrbeli za tehnološki razvoj, tako da smo kot prvi v Sloveniji uvedli peto generacijo mobilnih omrežij (5G) in nadaljevali s širitvijo in nadgradnjo največjega dostopovnega optičnega omrežja v državi. Priklop nanj trenutno omogočamo že več kot polovici slovenskih gospodinjstev. To so pomembni mejniki digitalizacije Slovenije.

> Podpora predsedovanju Slovenije Svetu EU je bila za nas izjemno pomembna izkušnja, ki je zahtevala izredno veliko logističnih, materialnih in človeških resursov. Rezultat je bil, s kibernetskega aspekta, brezhibno predsedovanje in s tem smo zelo zadovoljni.

V Telekomu Slovenije veliko sredstev vlagate v lasten razvoj novih tehnoloških rešitev. Nam lahko zaupate svojo vizijo na tem področju za prihodnje obdobje?

Ob povečani digitalizaciji ter delu in šolanju na daljavo posebno skrb namenjamo varnosti, in sicer tako z razvojem storitev za zasebne in poslovne uporabnike kot z najsodobnejšim Operativnim





centrom kibernetske varnosti, v katerem razvijamo prilagojene rešitve za podjetja vseh velikosti. Kot sem že omenil, je v letu 2021 minilo natanko 30 let od uvedbe mobilne telefonije in interneta v Sloveniji. Nosilec razvoja v vsem tem obdobju je bil in je Telekom Slovenije oziroma njegove odvisne družbe. Minilo je tudi natanko tri leta, odkar smo v slovenske domove vstopili z glasovnim upravljanjem vsebin in naprav pametnega doma in to v slovenskem jeziku. Glasovno upravljanje je postalo izjemno priljubljeno – platformo NEO je konec leta uporabljalo že več kot 130.000 uporabnikov, v enem letu pa se je število uporabnikov povečalo za tretjino. Uporabniki pametne denarnice VALÚ, s katero smo v letu 2019 nadgradili svoj portfelj finančnih storitev, so v letu 2021 opravili že več kot dva milijona transakcij, število uporabnikov pa se je povečalo za več kot 40 %, tako da je konec leta VALÚ uporabljalo več kot 100.000 uporabnikov. Razvili in omogočili smo tehnično rešitev, prek katere Zavarovalnica Sava našim naročnikom mobilnih storitev omogoča edino turistično zavarovanje s plačilom glede na dejansko število dni, ko je posameznik v tujini. Vedno večje je povpraševanje po naši storitvi E-oskrba, širimo tudi mrežo, v kateri ponujamo rešitve telemedicine. Ob tem pa razvijamo in nenehno nadgrajujemo tudi trajnostne rešitve za pametna mesta, pametne tovarne in skupnosti.

Skratka, naša naloga je, da z lastnim znanjem razvijamo najsodobnejše komunikacijske rešitve, ki poenostavljajo življenje. In ta razvoj na različnih področjih se bo nadaljeval tudi v prihodnje. Na ta način vsak dan udejanjamo svojo vizijo, ki se glasi - digitaliziramo svet priložnosti.

Bili ste prvi, ki ste v Sloveniji smelo stopili na področje uvajanja tehnologije 5G. Se vam na tem področju že kažejo rezultati teh korakov?

Letos bo minilo že dve leti, odkar smo kot prvi v Sloveniji vzpostavili nacionalno omrežje pete mobilne generacije. Razvoj omrežja 5G kot evolucijska nadgradnja 4G je kompleksen in dolgo-

ročen tehnološki projekt, ki zahteva napredno tehnologijo omrežja ter poznavanje in testiranje celotne njegove verige. V primerjavi z obstoječimi mobilnimi omrežji je 5G uporabnikom prinesel veliko večje hitrosti prenosa podatkov v obeh smereh (od in do uporabnika) in veliko krajši odzivni čas z izjemno nizko zakasnitvijo. Ob tem pa tudi hkratno učinkovito povezovanje velikega števila naprav, kar omogoča razvoj pametne industrije, pametnih mest in skupnosti ter preko možnosti rezinjenja omrežja uvedbo številnih navideznih namenskih omrežij, kar bo gospodarstvu omogočilo nadaljnjo digitalizacijo. Mobilno omrežje pete generacije načrtujemo na način, da se znotraj ene fizične infrastrukture omogoči virtualna namenska omrežja za različne vertikale, kot so energetika, transport, logistika, industrija, pametna mesta, zdravstvo, zaščita in reševanje (javna varnost) in podobno.

V zadnjem obdobju kibernetski varnosti posvečate ogromno svoje strokovne pozornosti. Vaš Operativni center kibernetske varnosti je postal vodilna zmogljivost varnostno operativnih centrov na področju zagotavljanja kibernetske varnosti v širšem regijskem prostoru. Podpora predsedovanju Republike Slovenije Svetu EU je bila še dodatna preizkušnja za vaše delovanje. Ste bili zadovoljni s prikazanim učinkom?

Kibernetski varnosti namenjamo zelo veliko pozornosti, tako da smo v zadnjih letih razvili napredne kibernetske rešitve v vseh treh segmentih kibernetske varnosti: preventivna kibernetska varnost, reaktivna kibernetska varnost in prediktivna kibernetska varnost. Naš Operativni center kibernetske varnosti danes aktivno varuje institucije v Sloveniji, regiji in celo na drugih celinah. Varnostne dogodke 24/7 podrobno spremljamo, analiziramo in ocenjujemo informacije, ki jih z različnih virov prejemamo glede potencialnih groženj. Na globalnem nivoju sodelujemo z različnimi organizacijami, sprejemamo dodatne ukrepe za povečevanje varnosti tako lastnih storitev kot storitev, ki jih zagotavljamo naročnikom, v stalni pripravljenosti je tudi kibernetska odzivna skupina. Vse naše aktivnosti so usmerjene v zagotavljanje najvišje stopnje varnosti, zanesljivosti in zaupnosti. Podpora predsedovanju Slovenije Svetu EU je bila za nas izjemno pomembna izkušnja, ki je zahtevala izredno veliko logističnih, materialnih in človeških resursov. Rezultat je bil s kibernetskega aspekta brezhibno predsedovanje in s tem smo zelo zadovoljni.

V preteklosti smo morali spodbujati podjetja, naj več vlagajo v varnost, danes pa nas podjetja in ostali deležniki vse pogosteje kontaktirajo sami. Stopnja zavedanja o pomenu ustrezne kibernetske in informacijske varnosti se je izjemno povečala.

Kako ocenjujete evolucijo slovenskega trga na področju zagotavljanja kibernetske varnosti?

Še pred nekaj leti je bilo na splošno bolj malo govora o kibernetski varnosti, danes pa je to popolnoma drugače, tako da so posamezniki, podjetja in ustanove že precej ozaveščeni. Zagotovo so k temu pripomogle aktivnosti vseh, ki skrbimo za varnost, k vse boljši osveščenosti pa prispevajo tudi medijsko izpostavljeni primeri vdorov v informacijske sisteme. V preteklosti smo morali spodbujati podjetja, naj več vlagajo v varnost, danes pa nas podjetja in ostali deležniki vse pogosteje kontaktirajo sami. Stopnja zavedanja o pomenu ustrezne kibernetske in informacijske varnosti se je izjemno povečala.)

V zadnjem obdobju iščete sinergije na področju delovanja tudi z ostalimi organizacijami. Ena od takih je tudi nakup podjetja Actual IT, ki je s svojimi storitvami pomemben deležnik na trgu IKT-rešitev. Katera so bistvena pričakovanja pri dvigovanju dodane vrednosti skupnega nastopa na področju zagotavljanja kibernetske varnosti v pomembnih infrastrukturnih sektorjih?

Telekom Slovenije tržni delež in pozicijo vodilnega operaterja ohranja s celovito ponudbo najsodobnejših IKT-storitev in rešitev. Skladno z zastavljeno strategijo pa bomo rast na IKT-trgu dosegali tudi s konsolidacijo slovenskega trga. Več v tem trenutku ne morem povedati, saj, kar se tiče nakupa podjetja Actual IT, vsi postopki še niso zaključeni.

Telekom Slovenije je na področju raziskav in razvoja zelo aktiven tudi v okviru mednarodnih projektov. Med drugimi ste usmerjeni v projekte zaščite kritične infrastrukture in kibernetske varnosti. Kateri so tisti potenciali, ki jih črpate iz teh inovativnih pristopov?

V Telekomu Slovenije vseskozi sodelujemo v razvojnih projektih, nenazadnje kot edini slovenski operater že vrsto let sodelujemo tudi v evropskih projektih, namenjenih razvoju 5G. Raziskovalni projekti, v katerih smo udeleženi na področju varnosti, nam skozi inovativne pristope dajejo novo in drugačno perspektivo na varnostne izzive, še posebej v kombinaciji fizične in kibernetske varnosti. Gre za raziskovanje vpliva kibernetskih napadov na fizični svet in obratno ter seveda hibridnih groženj. Če k temu dodamo še kaskadne učinke, ki nastajajo med več infrastrukturnimi sistemi, postane naloga že zelo kompleksna. Skozi sodelovanje v tovrstnih projektih pridobivamo znanja, izkušnje in nove pristope k reševanju kompleksnih izzivov. Ta znanja uporabljamo pri izboljševanju procesov in storitev za naše naročnike.

Telekom Slovenije je eden izmed pomembnih korporativnih članov Slovenskega združenja za korporativno varnost. Veliko napora je v zadnjem obdobju namenjenega razumevanju strateškega managementa o pomenu korporativne varnosti za poslovanje organizacij. Menite, da dosedanji trud že prinaša rezultate na tem področju?

Absolutno. Podjetja so vedno bolj osveščena in imajo o kibernetskih varnostnih tveganjih ter odzivih nanje vedno več znanja in izkušenj. Varnost je vedno pomembnejša tema. ■

Foto: arhiv Telekom Slovenije

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.

Občina Slovenska Bistrica · tuš · Melamin · telemach · SIEMENS · CAA · SMART COM · URSIV · 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

Avtor: Vojko Volk / veleposlanik



KOLUMNA

UJETNIKI VOJNE

„Izbirali ste med vojno in sramoto, izbrali ste sramoto in zdaj boste imeli še vojno“.

/Winston Churchil, leta 1938, ob odločitvi Chamberlainove vlade, da Hitlerju v zameno za mir prepusti Sudete/

Ob začetku agresije na Ukrajino nismo vedeli, zakaj je Rusija napadla in kaj hoče. Razumeli smo le, da je Ukrajina žrtev agresije in se uspešno brani. Po skoraj treh mesecih vojne še vedno ne vemo, kaj Rusija hoče, le da nam poslej ni več jasno niti to, kaj natanko hoče Ukrajina. Hoče premirje, konec žrtev in nasilja, ali pa hoče vojaško zmago? V obeh primerih na koncu nastopi diplomacija, ki sklene mirovni sporazum. V prvem primeru ima Ukrajina popolno podporo zahoda skozi politično in denarno zaslombo in s pošiljanjem orožja. Pošiljanje orožja seveda ni sodelovanje v vojni, ampak je oblika pomoči žrtvam agresije, ki imajo legitimno pravico do samoobrambe. Zahod še bolj pomaga Ukrajini s sankcijami, ki že močno hromijo rusko gospodarstvo ter Putinovo sposobnost financiranja vojne. Ta vojna z nič uspeha in ogromno žrtvami, škode in sramote, Rusijo neizmerno veliko stane in to v čisto vseh pogledih, posebej materialnem in moralnem. Prav zaradi poloma ruske vojske v Ukrajini je Putin obrnil svojo retoriko in zdaj razlaga, da je Rusija v vojni z Natom. V drugem primeru, ko Ukrajina načrtuje poraz ruske vojske, pa se postavi vprašanje, kaj bi v Ukrajini šteli za zmago; izgon ruskih sil iz vseh delov Ukrajine razen Krima in Donbasa ali izgon ruskih sil iz čisto vseh delov Ukrajine? Na misel pride še tretja možnost, ki bi tudi lahko bila zmaga za Zelenskega, in sicer razpis referenduma v Donbasu, na katerem bi se ljudje res svobodno izrekli o tem, komu želijo pripadati in bi bil izveden pod mednarodnim nadzorom. Vsekakor se v tej dilemi zahodna javnost vse bolj nagiba k čim prejšnji zaustavitvi nasilja, ter vzpostavitvi premirja in dialoga in se odvrača od spodbujanja Ukrajine, da s pomočjo zahodnega orožja vojaško porazi Rusijo. Gre za položaj, ki je za demokracije običajen, ker si ljudje želijo miru in napredka, Putin pa to izkorišča za svoje interese in z vsemi sredstvi, obveščevalnimi in propagandnimi, koplje prepad med evropskimi politiki in javnostjo. Nedavna izjava Putinovega zunanjega ministra Lavrova o tem, da je bil Hitler v resnici Žid, in da so Židje sami sebi največji sovražniki, je bilo sporočilo vsem anti-evropskim skrajnežem v državah EU, da je Rusija edina, ki dekadentni zahod lahko reši pred vladavino Judov, gejev in Amerike. Vsekakor je dilema izbire med vojaško pomočjo Ukrajini in prizadevanji za takojšnji mir za ljudi v Evropi strahotno realna in jo čutijo ‚v kosteh‘ in v resnici gre za odgovor na preprosto vprašanje; je mogoče premagati silo, ki ima jedrsko orožje?

Res je, da o marsičem lahko danes samo ugibamo, je pa enako res, da bo prihodnost Evrope posledica naših današnjih ravnanj. Ključna odgovornost Evrope, in v prvi vrsti EU, bo zagotovo v tem, da Evropa ohrani enotnost in z njo trdnost v odnosu do Putinove Rusije.

Tako kot vse na tem svetu je tudi vojne med seboj težko enačiti in celo primerjati zato, da bi v njih poiskali poduke o človeški norosti. A podobnost Putinovih vojn s tistimi, ki jih je začel Milošević na Balkanu je res velika. Gre za arhaični etnični pristop, v katerem je treba združiti vsa ozemlja, kjer živijo Rusi oziroma Srbi. Leta 1998 se je Milošević odločil za vojaško kazensko ekspedicijo na Kosovu z izgovorom zaščite Srbov pred nasiljem albanskih nacionalistov. V samo nekaj dneh je povzročil ogromno žrtev in v beg spravil 800 tisoč kosovskih Albancev. Svet je bil zgrožen, ker je minilo manj kot 5 let od srbskega obleganja Sarajeva in genocida v Srebrenici. Takoj zatem, ko je NATO bombardiral srbske položaje okrog Sarajeva, je bilo doseženo premirje in zelo hitro še Daytonski sporazum. Zaradi te izkušnje zahod ni

okleval in je po petih poskusih, da preko Varnostnega sveta doseže poseg za preprečitev humanitarne katastrofe na Kosovu (vse je z vetom blokirala Rusija), stvari vzel v svoje roke. Po brezštevilnih pozivih Miloševiću, naj ustavi delovanje vojske na Kosovu, je jeseni 1998 prišlo do prve resne grožnje z vojaškim posegom, potem pa je do tega zares prišlo marca 1999. Zahod se je zaradi preprečitve ponovne humanitarne katastrofe na Balkanu odločil za vojaški poseg, ki ga je opravil NATO. Odločitev je bila težka, o razlogih pa dvoma ni bilo; zahodna javnost ni bila več pripravljena trpeti novih zločinov Miloševićevega režima, ki je v BiH in na Hrvaškem povzročil skoraj 200 tisoč žrtev. Poseg NATO se je končal z Miloševićevim porazom po tem, ko mu je postalo dokončno jasno, da mu Rusija ne bo stopila v bran. V resnici je Putin v Kosovu že takrat zaznal model, ki mu je bil kasneje priročen pri ustanavljanju ‚samooklicanih' republik na obrobjih nekdanjega sovjetskega imperija, kjerkoli je to potreboval za domnevno zaščito ruskega prebivalstva. V nedavnem pogovoru z generalnim sekretarjem ZN Gutteresem je Putin to tudi javno priznal in globoko prizadel Srbe, ki so naivno verjeli v bratsko Rusijo. Vprašanje se torej glasi; je mogoče Putina premagati na način, kot je bil poražen Milošević? Ali še drugače, bi Milošević še pred porazom uporabil jedrsko orožje, če bi ga imel? Bi ga, če bi ga imela, tik pred svojim padcem jedrsko orožje uporabila Hussein in Gadafi? In kje je točka, kjer bi jedrski gumb lahko stisnil Putin?

Evropa je medtem vse bolj sama v soočanju s Putinovo vojno in vse bolj je videti, kot da Amerika in Rusija med seboj obračunavata preko hrbtov Evropejcev. A se Evropa, močno preizkušena od Trumpove vladavine, brexita in Covida presenetljivo dobro drži in vzdržuje enotnost. Ameriški predsednik Biden se mukoma bori za javno podporo tik pred vmesnimi volitvami, kjer mu ne kaže najbolje. Vse kar izreče in počne je bolj v korist njegovih političnih interesov kot interesov Evrope. Na drugi strani je Kitajska, ki je vse bolj utrujena od čakanja, da Putin nekako zmaga in konča vojno. Poznavalci so celo zaznali cinizem kitajskih predstavnikov oblasti ob objavi vesti, da so Ukrajinci potopili križarko Moskva, ponos ruske mornarice. Putin je postal absolutni protagonist svetovnih dogajanj in vseh medijskih poročil, Kitajska pa je s svojimi interesi in ambicijami potisnjena v vlogo, da dogodkom zgolj sledi. Tega pa Kitajska že dolgo ni več navajena in to zagotovo ne koristi njenim geopolitičnim in še manj gospodarskim interesom, še zlasti v Evropi, ki je za Kitajsko daleč največji in najpomembnejši trg na svetu.

> V vojnah so pesimisti in optimisti nekoristni, realisti pa nastopijo, ko se vojne končajo, da se doseže mir. Tokrat doseči mir, pomeni doseči prihodnost. Dotlej pa bomo vsi, Evropejci pa še posebej, ujetniki Putinove vojne.





Prepričljiva volilna zmaga Macrona je dobra vest za EU, a verjetno prinaša obnovo tlečega spora z Nemčijo, ki se nekoliko presenetljivo odloča za pošiljanje „obrambnih tankov“ v Ukrajino medtem, ko utegne Macron pod pritiskom javnosti zagovarjati zmanjševanje napetosti in dosego premirja. Podobno velja za Italijo, kjer skoraj polovica javnosti že zdaj nasprotuje pošiljanju orožja Ukrajini in se delež samo še krepi. A gre za lažno dilemo, ker se v resnici vojaška podpora Ukrajini in mirovna prizadevanja v celovitem odnosu EU do Rusije ne izključujejo, ampak dopolnjujejo. Vprašanje je samo, koliko so realne naše ocene o dejanskih razmerah v Rusiji. Zanesljivo vemo le, da je rusko gospodarstvo realno že upadlo za vsaj 15 odstotkov, in da ruska mesta že trpijo pomanjkanje dobrin. A bolj pomembno je vedeti, koliko je v resnici prizadeta sposobnost ruske vojske, da vztraja pri napadih v Ukrajini, koliko je zaradi sankcij prizadet ruski finančni sistem, koliko standard prebivalstva in predvsem koliko sposobnost Putina, da ohranja politično podporo naroda. Da vsi Rusi stojijo za Putinom, je seveda zgolj videz, pogojen s popolno medijsko nesvobodo in cenzuro. S pozivi na patriotizem za obrambo pred zahodom, bo Putin od Rusov že to jesen prisiljen zahtevati odrekanje. A kako bo ljudem pojasnil, zakaj Rusija trpi pa ni na ruskih tleh nobenih žrtev, nobenega Stalingrada in nobenega Nato vojaka? In kaj bodo obubožani Rusi dobili v zameno za huda odrekanja, mar razrita ukrajinska polja, obubožani Donbas, povsem izolirani Krim, razrušeni Mariupolj in predvsem obsodbe sveta za zločine zoper človeštvo, ali celo za genocid?

Res je, da o marsičem lahko danes samo ugibamo, je pa enako res, da bo prihodnost Evrope posledica naših današnjih ravnanj. Ključna odgovornost Evrope, in v prvi vrsti EU, bo zagotovo v tem, da Evropa ohrani enotnost in z njo trdnost v odnosu do Putinove Rusije. Edino, česar si Evropa ne more privoščiti, je popuščanje Putinu, ker bi vsako popuščanje razumel kot našo slabost. Seveda ob hkratnem zavedanju, da Putina ni mogoče vojaško poraziti na način, kot je to bilo v vseh dosedanjih vojnah tega sveta. Ostane nam spretnost kombiniranja naše vojaške podpore Ukrajini, vojaških sposobnosti Ukrajine, ter diplomacije s pogajanji in priznavanjem realnosti. V vojnah so pesimisti in optimisti nekoristni, realisti pa nastopijo, ko se vojne končajo, da se doseže mir. Tokrat doseči mir, pomeni doseči prihodnost. Dotlej pa bomo vsi, Evropejci pa še posebej, ujetniki Putinove vojne. ■

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
mag. Nada Drobne Popović, predsednica uprave Petrol d.d.*

PETROL PROCESOM UPRAVLJANJA TVEGANJ NAMENJA POSEBNO POZORNOST PRI SVOJEM POSLOVANJU

Pričujoča energetska kriza zahteva od najpomembnejše energetske družbe v Sloveniji še dodatno skrbnost pri obvladovanju varnostnih tveganj. S tem zagotavljajo večjo odpornost družbe in neprekinjenost delovanja ključnih operativnih procesov ne glede na nenehne dinamične izzive varnostnega okolja. Nekaj ključnih misli o izzivih, ki stojijo pred Petrolom, nam je zaupala njegova predsednica uprave mag. Nada Drobne Popović.

Petrol je v svoji osnovi še vedno najpomembnejša energetska družba v Sloveniji in ima pomemben tržni delež tudi v bližnji regiji. Konflikt v Ukrajini je ponovno izpostavil Evropsko odvisnost od Ruskih energentov. Kje trenutno vidite največje izzive, ki stojijo pred Petrolom za zagotavljanje neprekinjene oskrbe z energenti, ki jih ponujate svojim uporabnikom?

Družba Petrol ima vzpostavljene učinkovite nabavne procese, razpršene oskrbne vire za goriva in energente, celovito ponudbo goriv in energentov. Vse to so pomembni elementi, s katerimi zaenkrat uspešno obvladujemo tveganja, povezana z energetsko krizo.

Kot največja energetska družba v Sloveniji smo zaenkrat uspeli z učinkovitim nabavnim procesom in pravočasnim vnaprejšnjim nakupom dovoljšnjih količin goriv in zakupom dovoljšnjih količin energentov, za prihodnje obdobje zagotoviti konkurenčne cene goriv in energentov in zanesljivo oskrbo z njimi. Družba Petrol ima tako trenutno dovoljšnje zaloge za običajne potrebe slovenskega prebivalstva po pogonskih gorivih. Ocenjujemo, da bo v primeru, da bodo povpraševanja po gorivu ostala na običajni ravni, oskrba strank v Sloveniji in v ostalih državah, kjer je Petrol prisoten, potekala brez večjih motenj. Ocenjujemo, da zanesljivost dobave

Že dejstvo, da je trenutna uprava pod mojim vodstvom ustanovila konkretno službo in jo ustrezno organizacijsko umestila v naš sistem korporativnega upravljanja, potrjuje, da služba z moje strani uživa vso potrebno podporo ter zaupanje. Pri izvajanju postopkov in ukrepov pa je v celoti avtonomna.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



pogonskih goriv ob normalnih pogojih (običajnih nivojih povpraševanja) v prihodnosti ne bo ogrožena, zagotovo pa se bodo zaradi situacije v Ukrajini spremenile dobavne poti pogonskih goriv.

Za leto 2022 ima družba Petrol zagotovljene dolgoročne nabavne pogodbe za naftne derivate v obsegu, ki odraža dosedanjo dinamiko rasti mobilnosti na predkovidne ravni, kot je opredeljeno v poslovnem načrtu za leto 2022. Tudi v primeru morebitnega embarga na rusko nafto bodo podpisane dolgoročne pogodbe realizirane, pojavijo se lahko zgolj zamude v dobavah in rast nabavnih cen. Zaradi situacije v Ukrajini in s tem zaostrenih varnostnih razmer smo že doslej opažali zamude v oskrbnih verigah, vendar lahko potrdimo, da ima družba za mesec maj potrjene vse načrtovane dobave naftnih derivatov.

Energetska kriza in potrebe po zmanjšanju emisij toplogrednih plinov verjetno vplivajo tudi na smer razvoja Petrola v prihodnosti. Boste zaradi energetske krize še pospešili svoj razvoj na področju pridobivanja energije iz obnovljivih virov?

V skupini Petrol smo že pred leti sprejeli odločitev, da postanemo sodobna trajnostno naravnana energetska družba. Pri tem ima posebno strateško mesto proizvodnja elektrike iz obnovljivih virov. Zaveza prehodu na zeleno energijo pomeni, da bo skupina Petrol v strateškem obdobju 2021 – 2025 za naložbe v energetsko tranzicijo namenila 35 % od skupnega investicijskega potenciala v višini 698 mio EUR, od tega največji del za investicije v pridobivanje energije iz obnovljivih virov.

Skupina Petrol je na področju proizvodnje elektrike iz obnovljivih virov prisotna že dalj časa, saj je prepoznala potrebo po zagotavljanju trajnostne, zelene energije za prehod v nizkoogljično družbo. Večino projektov proizvodnje električne energije iz obnovljivih virov energije Petrol izvaja na Hrvaškem, v Bosni in Hercegovini ter v Srbiji , kjer je velik naravni potencial vetra, sonca in vode. Skupno v okviru skupine Petrol trenutno obratujejo: 2 vetrni elektrarni, 30 manjših sončnih elektrarn in 6 malih hidroelektrarn.

Naslednji velik korak je investicija v prve tri velike sončne elektrarne skupne inštalirane moči 22 MW ter s pričakovano proizvodnjo električne energije v višini 29 GWh. Gre za tri elektrarne na območju Šibeniško Kninske županije

V skupini Petrol se zavedamo, da informacijske varnosti ne sestavljajo samo tehnološke rešitve in strokovnjaki, ki jih upravljajo, ampak so pomembni prav vsi uporabniki informacijskega sistema, saj le celovit pristop lahko zagotovi varnejšo prihodnost.



na Hrvaškem. Sončne elektrarne bodo s proizvodnjo elektrike pričele v začetku leta 2023. Skupna vrednost investicije je ocenjena na 17 mio EUR.

Skupina Petrol je imela konec leta 2021 skupno inštalirano moč za proizvodnjo elektrike iz obnovljivih virov v višini 68,9 MW. Do leta 2025 pa želimo z razvojem in izvajanjem projektov na področju proizvodnje električne energije iz OVE, tako za lastne potrebe kot vire pri prodaji električne energije, preseči 160 MW inštalirane moči.

Z gradnjo lastnih proizvodnih kapacitet za proizvodnjo elektrike iz obnovljivih virov energije Petrol sledi strateški usmeritvi postati prepoznaven regionalni ponudnik celovitih energetskih in okoljskih rešitev ter partner za prehod v nizkoogljično družbo.

V svoji dolgoletni karieri ste delovali v različnih organizacijskih sredinah v katerih ste se srečevali z različnimi vidiki vodenja. Nam lahko zaupate katere izkušnje preteklih organizacijskih okolij so vam najbolj pomagale pri obvladovanju izzivov, ki ste jih našli v Petrolu?

Vsaka organizacija, v kateri sem delovala doslej, je imela svoje posebnosti in mi je dala specifične dragocene izkušnje. Na začetku svoje poklicne poti sem več kot 10 let delovala v uspešnem zasebnem podjetju in spoznala delovanje zasebnega sektorja. Kasneje sem pridobila izkušnje z vodenjem večjih organizacij v javnem sektorju. Družba Petrol ima spet svoje posebnosti: je zasebna družba, a tudi v državni lasti. Poleg tega gre za matično družbo v veliki regijski skupini podjetij. Oboje prinaša posebne dimenzije korporativnega upravljanja in strateškega vodenja ob upoštevanju številnih deležnikov in njihovih raznolikih interesov.

Obvladovanje tveganj je za nepreki-njenost delovanja tako kompleksne organizacije, kot je Petrol, izrednega pomena. V preteklem obdobju ste na novo organizacijsko in procesno osmislili Službo za korporativno varnost in nadzor poslovanja. Katere so tiste dodane vrednosti, ki jih kot strateška voditeljica pričakujete od tega mehanizma v vaši organizaciji?

Družba Petrol je po sprejetju ambiciozne strategije januarja lani izvedla tudi reorganizacijo določenih delovnih procesov. S postavitvijo samostojne štabne službe za korporativno varnost in nad-

zor poslovanja smo na enem mestu združili upravljanje in obvladovanje ključnih varnostnih tveganj, ki nedvomno vplivajo na neprekinjenost poslovanja. Glavni namen in naloge novo nastale službe so predvsem v zagotavljanju varnega okolja za poslovanje skupine Petrol, učinkovitost pri zaščiti delovnih procesov, varnosti zaposlenih in objektov ter pravočasno zaznavanje oz. preprečevanje odklonskih pojavov, ki negativno vplivajo na poslovno uspešnost ali krnijo ugled naše družbe.

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

Že dejstvo, da je trenutna uprava pod mojim vodstvom ustanovila konkretno službo in jo ustrezno organizacijsko umestila v naš sistem korporativnega upravljanja, potrjuje, da služba z moje strani uživa vso potrebno podporo ter zaupanje. Pri izvajanju postopkov in ukrepov pa je v celoti avtonomna.

Digitalizacija poslovanja in dejstvo, da vaši pomembni infrastrukturni procesi temeljijo na informacijsko komunikacijski tehnologiji, so pomen informacijske varnosti postavili v popolnoma novo dimenzijo. Kaj so po vaši oceni tisti potrebni izzivi na tem področju, ki jim boste morali v prihodnosti nameniti posebno pozornost?

V zadnjih nekaj letih se je izpostavljenost kibernetskim napadom na globalni ravni močno povečala, zato je uspešnost zaščite, zaznave in hitrega odziva na varnostne incidente ključna. Še posebej je to pomembno za informacijske sisteme, ki so bistvenega pomena za nemoteno delovanje države, med katere spadata tudi energija in promet. Zagotavljanje varnosti informacijskega sistema je zato eden od ključnih elementov strategije razvoja informacijske tehnologije v družbi Petrol. Popolne varnosti seveda ni mogoče doseči, zato je treba poiskati pravo mero obvladovanja tveganja. To pa zahteva poznavanje poslovnega okolja in trendov na področju digitalizacije ter mora biti del korporativnega upravljanja z informacijsko varnostjo. V skupini Petrol se zavedamo, da informacijske varnosti ne sestavljajo samo tehnološke rešitve in strokovnjaki, ki jih upravljajo, ampak so pomembni prav vsi uporabniki informacijskega sistema, saj le celovit pristop lahko zagotovi varnejšo prihodnost.

Trenutne varnostne razmere na globalnem nivoju nedvomno vplivajo na vsa družbena okolja. V danih razmerah učinkovito strateško upravljanje podjetja ali poslovne organizacije, podobne naši, ni možno brez ustrezno organiziranega sistema korporativne varnosti.

Petrol je za Republiko Slovenijo ena od najpomembnejših družb tudi v smeri zagotavljanja kritičnih procesov in blagovih rezerv goriva. To pomeni, da je potreba po učinkovitem sodelovanju z različnimi državnimi institucijami zelo pomembna. Kako bi ocenili to sodelovanje in ali so še priložnosti, kjer bi lahko državne institucije s strokovnimi ukrepi še dodatno podprle vašo organizacijo?

Glede na dejavnost družbe Petrol in glede na njeno lastništvo so država in državne institucije pomemben deležnik, ki s svojim delovanjem vplivajo na uspešnost podjetja. V družbi Petrol se trudimo z vsemi deležniki razvijati odnos sodelovanja in partnerstva pri zasledovanju skupnih interesov, tudi z državnimi institucijami.

Petrol je zelo močno prisoten tudi v okviru različnih mednarodnih raziskovalnih projektov. Predvidevamo, da je vaša strateška usmeritev temu področju namenjati pomembno pozornost? Katere so tiste bistvene kvalitete, ki jih dobite skozi tako sodelovanje?

Naša dejavnost je kompleksna in razvejana, še posebej v kontekstu zahtevne tranzicije v nizkoogljično prihodnost, kateri je zavezana tudi skupina Petrol. Skladno s tem kontinuirano stremimo k razvoju novih poslovnih modelov in iščemo nove priložnosti za razvoj in partnerstva. Eden od najboljših načinov je sodelovanje v mednarodnih razvojnih projektih.

Koristi in priložnosti, ki jih prinese sodelovanje v tovrstnih partnerstvih so dolgoročne in multiplikativne. Pozitivnega vpliva nimajo samo na sodelujoče partnerje, ki lahko skozi sodelovanje razvijejo tudi dolgoročnejša poslovna razmerja, ampak tudi na strokovni razvoj posameznikov, ki sodelujejo v tovrstnih projektih, pa tudi na širšo družbo in okolje.

V raziskovalne in razvojne projekte se vključujemo na različnih področjih, od kibernetske varnosti, do pametnih mest in skupnosti, pametnih zgradb in doma, razvoja zelenih tehnologij, mobilnosti in podobno. Trenutno smo partnerji v projektih X-Flex, Compile, CyberSeas, InfraStress, za več projektov, s katerimi smo kandidirali na javnih razpisih za nepovratna sredstva (Atlantis, Seamless, CarFulesBio) čakamo še na končne rezultate razpisa. V prihodnje bomo aktivnosti na tem področju še intenzivirali in s tem pospešili energetsko tranzicijo družbe.

Petrol je eden izmed pomembnih korporativnih članov Slovenskega združenja za korporativno varnost. Veliko napora je v zadnjem obdobju namenjenega v smeri, kako strateški management v organizacijah dodatno osvestiti o pomenu korporativne varnosti za poslovanje organizacij. Menite, da tudi razmere v zahtevnem varnostnem okolju vplivajo na povečanje tega zavedanja o pomenu korporativne varnosti?

Trenutne varnostne razmere na globalnem nivoju nedvomno vplivajo na vsa družbena okolja. V zadnjih dveh letih smo se tako soočali s posebnimi varnostnimi izzivi, ki jih je povzročala epidemija covid-19 in trenutno s posledicami še trajajoče vojne v Ukrajini. Poleg posledične gospodarske škode smo se vsi znašli v posebnih varnostnih okoliščinah, v katerih se je zavedanje o pomenu korporativne varnosti samo še okrepilo. V danih razmerah učinkovito strateško upravljanje podjetja ali poslovne organizacije, podobne naši, ni možno brez ustrezno organiziranega sistema korporativne varnosti. ■

Foto: arhiv Petrol

VARNOSTNI PREHODI ZA KONTROLO DOSTOPA V NADZOROVANA OBMOČJA

Visoka in nizka vrtljiva vrata ter hitri avtomatizirani prehodi kot dodatna kontrola točka za vstop v omejena območja.

Primerno za zunanjo ali notranjo namestitev in za območja z velikim pretokom uporabnikov.
Možnost integracije z obstoječimi VNC sistemi in uporabo enega medija znotraj kompleksa.
Zvočni in svetlobni alarmi v primerih neavtoriziranega prehoda.
Možnost avtomatiziranih plačljivih prehodov ter dodatnih modulov po meri naročnika (biometrija, ticketing – avtomatizirano preverjanje vstopnic, štetje obiskovalcev,...).



ID SHOP – ZANESLJIV PARTNER ZA ZAGOTAVLJANJE KONTROLE PRISTOPA V VAŠIH OBJEKTIH

Varnostni prehodi na kritičnih območjih pomenijo več, kot zgolj povečano varnost!

- Nižji stroški fizičnega varovanja.
- Bolj kontroliran pretok ljudi.
- Večja izkoriščenost varnostno-nadzornega centra.
- Učinkovita integracija z obstoječo kontrolo pristopa v stavbi.
- Doseganje višjih varnostnih standardov.



ID Shop zagotavlja celovite rešitve za zagotavljanje kontrole pristopa:

Mehanski sistemi zaklepanja • Elektronski sistemi zaklepanja (pametne ključke, digitalni cilindri, mehatronske komponente) • Varnostni prehodi (visoka, nizka vrtljiva vrata, hitri prehodi in zapore)

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

cominfo Security First

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Boštjan Šefic, svetovalec predsednika republike za nacionalno varnost

POTREBUJEMO DODATNE SINERGIJE ZA POVEČANJE UČINKOVITOSTI NACIONALNO VARNOSTNEGA SISTEMA

Nacionalna varnost Republike Slovenije se nahaja pred pomembnimi dilemami, ki jih pred nas postavlja vedno bolj kompleksno mednarodno varnostno okolje. O ključnih izzivih in o možnih sinergijah za povečanje učinkovitosti delovanja celovitega nacionalno varnostnega sistema, smo se pogovarjali z g. Boštjanom Šeficem.

Novi varnostni izzivi za nacionalno varnostni sistem Republike Slovenije predstavljajo pomembno dilemo ali je ustrezno ustrojen za učinkovito odzivanje? Kako vi ocenjujete trenutno stanje učinkovitosti?

Večkrat sem izrazil prepričanje, da je slovenski nacionalno varnostni sistem dobro zasnovan in da smo tudi po njegovi zaslugi oziroma posameznih subjektih, država z eno najvišjih varnosti v Evropi in svetu. Se pa varnostne razmere v naši bližnji in daljni okolici spreminjajo, pojavljajo se nove grožnje in povečujejo tveganja. Zato se mora tudi sistem kot celota stalno prilagajati tem spremenjenim okoliščinam. V zadnjem obdobju se soočamo z vrsto novih groženj in tveganj, ki predstavljajo izziv za nacionalno varnostni sistem. V mislih imam kibernetske grožnje, hibridne grožnje, mednarodni organizirani kriminal, nasilni ekstremizem, radikalizem, soočamo se z obsežnejšimi migracijami in različnimi krizami. Tem okoliščinam se mora ves čas pravočasno in ustrezno prilagajati tudi nacionalno varnostni sistem. To mora biti stalen proces. Pri tem ne smemo zaostajati, temveč najmanj biti v koraku z intenzivnostjo posameznih groženj oziroma tveganji.

Osebno ocenjujem, da trenutne razmere narekujejo odpravo nekaterih vrzeli s ciljem biti v največji meri pripravljen na obstoječe in prihajajoče varnostne izzive. Izhajajoč iz tega vidim nekaj področij, ki bi jih bilo potrebno spremeniti in nadgraditi. Predvsem pa moramo kadrovske, materialne in finančne vire, ki so nam na razpolago, optimalno uporabiti.

Kateri so tisti segmenti tega sistema, ki mogoče še kličejo po določenih prenovah ali spremenjenih podlagah o pristojnostih, ki bi stanje dvignili na višji nivo učinkovitosti?

Osebno ocenjujem, da trenutne razmere narekujejo odpravo nekaterih vrzeli s ciljem biti v največji meri pripravljen na obstoječe in prihajajoče varnostne izzive. Izhajajoč iz tega vidim nekaj področij, ki bi jih bilo potrebno spremeniti in nadgraditi. Predvsem pa moramo kadrovske, materialne in finančne vire, ki so nam na razpolago, optimalno uporabiti.



V mislih imam predvsem obveščevalno, protiobveščevalno in varnostno področje, kjer nujno potrebujemo nekatere spremembe. Zanesljivi podatki in informacije so ključne pri sprejemanju odločitev. Po drugi strani moramo zapolniti vrzeli, ki so nastale in še posebej izstopajo v zadnjem obdobju. To so ekstremizem, radikalizem in terorizem. V tem bi bilo potrebno narediti nekaj posegov v zakonodajo glede pristojnosti, organizacije in pooblastil posameznih subjektov.

Usklajenost delovanja in usmerjanje vseh podsistemov in subjektov je prav tako izjemno pomembna in zagotavlja višjo stopnjo učinkovitosti. Tu so bili v preteklosti narejeni nekateri premiki, ki niso zadostni in v celoti ustrezni.

Ob preudarnem in premišljenem definiranju nujno potrebnih pooblastil za uspešno soočanje z grožnjami in tveganji pa mora biti zagotovljen tudi ustrezen nadzor, tako strokovni kot politični oziroma parlamentarni. To področje bo potrebno vsekakor nadgraditi, jasno razmejiti pristojnosti in jih definirati ter oblikovati tako, da ne bo prihajalo do prekrivanja. Zlasti pri parlamentarnem nadzoru je potrebno vzpostaviti sistem, da se prepreči morebitna zloraba za doseganje političnih ciljev. Po drugi strani pa mora prav preprečevati morebitne poskuse zlorabe s strani izvršne veje oblasti. Nenazadnje, to potrjujejo številni primeri in ekscesi zadnjih let.

Pri Slovenski vojski in celotnem obrambnem področju so prav tako potrebne nekatere prilagoditve novo nastalim razmeram in potrebam. Pri tem imam v mislih poslabšanje varnostnih razmer v Evropi, spremembe na področju skupne varnostne in obrambne politike EU ter spremembe znotraj Nata. Ključno pa je, da Slovenska vojska še naprej ostaja učinkovit garant naše suverenosti in ključni subjekt slovenske nacionalne obrambe. Zato sta njen premišljen vsestranski razvoj in krepitev nujna.

Izjema ni niti odlično delujoč sistem zaščite in reševanja. Namreč, tudi na tem področju se pojavljajo novi izzivi. Naj samo omenim pomembno vlogo, ki jo je imel ta podsistem v času množičnih migracij s katerimi se bomo zelo verjetno v prihodnosti srečevali pogosteje. Ne glede na to, da načeloma ne zagovarjam sprememb, zlasti hitrih, tam, kjer stvari tečejo dobro, pa sem prepričan, da bi bilo smiselno v nekem srednjeročnem obdobju razmišljati o zaščiti in reševanju, kot nekoliko okrepljenem in samostojnejšem podsistemu nacionalne varnosti z nadgrajeno vlogo.

Ali lahko z nivoja Urada predsednika Republike Slovenije pričakujemo določene pobude, ki bi še okrepile razprave znotraj nacionalno-varnostnega sistema, predvsem pa izgradile most za diskusijo med ključnimi državnimi institucijami in civilno družbo?

V zvezi s tem sem že jeseni preteklega leta opravil vrsto pogovorov z nekaterimi ključnimi deležniki in uglednimi domačimi strokovnjaki o tem, kako spodbuditi konstruktivno razpravo o vseh navedenih vprašanjih. Zamisel je bila oblikovana, vendar smo ocenili, da gre za pomembno tematiko, ki potrebuje umirjeno, strokovno in argumentirano razpravo, za kar pa zadnji meseci niso bili najbolj primerni. Upam, da bo interes in priložnost nekatere pogovore ter preveritev posameznih razmišljanj opraviti s predstavniki nove Vlade in vsemi zainteresiranimi še do konca tega leta.

Kriza v Ukrajini je pred nas postavila bistvena vprašanja o učinkovitosti obrambnih sistemov v državah članicah EU. Po podatkih lahko vidimo, da članice EU skupaj namenjajo

več sredstev za obrambne sisteme, kot na primer Rusija, pa je vendarle ocena, da ti vložki niso najbolj učinkovito implementirani v neposredne obrambne zmogljivosti. Kje so po vašem mnenju na tem področju še določene rezerve?

Države članice Evropske unije se zavedamo tega dejstva. Verjamem, da so tudi največji skeptiki prepoznali dejstvo, da so se varnostne razmere v nam bližjih regijah in tudi v nekoliko bolj oddaljenih območjih, bistveno spremenile. Žal, tako vsaj kaže v tem trenutku, bodo trendi prej negativni kot pozitivni. Rezultat tega so resna razmišljanja nekaterih držav, da se aktivno vključijo v Nato. Zavedajo se, da je to pravzaprav najboljša garancija za zagotavljanje njihove varnosti in obrambe. V preteklosti nam je sicer marsikdo očital, da opozarjamo na slabšanje varnostnih razmer zgolj kot izgovor za zagotavljanje več sredstev in investicije v varnostni in zlasti obrambni sistem. Seveda, sredstva za obrambo morajo biti uporabljena premišljeno in na način, da z njimi dosežemo največji učinek, tako z vidika nacionalne kot kolektivne obrambe. In tisto, kar vlagamo mora biti komplementarno z obrambnimi interesi ter ambicijami EU in potrebami Nata. S tega zornega kota je potrebno zagotoviti dvoje. Načrtovanje obrambnih struktur in zmogljivosti mora odgovarjati na zastavljene cilje, ki se morajo med seboj dopolnjevati. In drugo, dogovorjene in sprejete obveze morajo biti uresničene v dogovorjenem obsegu in času. Na obeh področjih moramo narediti še veliko. To velja za našo državo, kot tudi vrsto drugih članic. Samo tako bomo postopno dosegli stanje, ki bo zagotavljalo visoko stopnjo varnosti.

Digitalizacija je proces, ki se mu ne bomo mogli izogniti niti na področju nacionalne varnosti. Kako gledate na uvajanje novih tehnoloških rešitev v sisteme nacionalne varnosti?

Vsa področja morajo slediti sodobnim tehnologijam. To velja tudi za nacionalno varnost. Z njihovim uvajanjem v sistem nacionalne varnosti moramo biti pravočasni. Zamujanje pomeni tveganje za našo varnost. To velja za vse podsisteme in subjekte nacionalne varnosti. Brez posodabljanja, tako na ofenzivnem kot defenzivnem področju, ne moremo uspešno obvladovati razmer. Pa naj bo to obveščevalno področje, področje zagotavljanja notranje varnosti, protiobveščevalne zaščite, obrambe ali zaščite in reševanja. Pri uvajanju pa moramo izhajati iz realnih ocen ogroženosti in potreb. Zelo jasno morajo biti opredeljeni učinki in koristi za nacionalno varnost.

> Korporativna varnost je pomemben del zagotavljanja varnosti v družbi. V posameznih elementih je sestavni del nacionalne varnosti, saj je zagotavljanje visoke stopnje varnosti in zaščita interesov v gospodarskih in drugih dejavnostih v nacionalnem interesu.

Pri uvajanju novih tehnoloških rešitev se najpogosteje srečujemo z dvema ključnima izzivoma. Prvič, finančnimi sredstvi, saj nove tehnologije praviloma predstavljajo velik finančni zalogaj. In drugič, še pogosteje je ključna težava predvsem skrb glede morebitne nenamenske uporabe oziroma zlorabe teh sistemov, poseganje v človekove pravice in varovanje osebnih podatkov. Zato je pomembno, da ob dobro premišljenih potrebah upoštevajoč nevarnosti, vedno nadgrajujemo tudi sistem nadzora in predvsem izobraževanja in osveščanja vseh, ki uporabljajo sodobne tehnologije pri zagotavljanju naše varnosti.

Kibernetski prostor v modernem varnostnem okolju prestavlja posebno komponento, ki vedno bolj pridobiva na pomembnosti. Ali v Republiki Sloveniji temu področju namenjamo dovolj pozornosti?

V današnji globalni povezanosti in ob tendenci po digitalizaciji praktično vseh procesov postajamo bolj učinkoviti, vendar hkrati tudi ranljivi za grožnje in tveganja usmerjena v kibernetsko okolje. Zavedanje o razširjenosti in obsežnosti kibernetskega prostora je prišlo relativno pozno. Ocenjujem, da je bilo daljše obdobje, ko smo temu namenjali odločno premalo pozornosti in se preprosto večina ni zavedala, kako zelo je to področje poseglo v naše vsakodnevno življenje. Zato smo zelo podcenjevali tudi področje kibernetske varnosti. Posledica tega je, da danes v marsikaterem pogledu nismo na nivoju, kjer bi morali biti. Menim, da je del zasebnega sektorja naredil velik oziroma bistveno večji premik, medtem ko je v javnem sektorju drugače. Morda ni prepozno, vsekakor pa smo glede tega v precejšnjem zaostanku. Na pomembnost ranljivosti, gro-



ženj in tveganj v kibernetskem prostoru, nas vsak dan opozarja vojna v Ukrajini.

Zato so nekateri koraki v smeri vzpostavitve celovitega sistema kibernetske varnosti in varovanja kibernetskega prostora tako pomembni. Poleg organizacijskih ukrepov, tehničnih ukrepov za obvladovanje kibernetskih groženj in povečevanje odpornosti vseh subjektov je pomembno izobraževanje, usposabljanje in osveščanje o grožnjah, tveganjih in varnosti. Po mojem prepričanju je pomembno, da vse aktivnosti vodimo premišljeno in sistematično, ker se pri tem ne sme preskakovati posameznih faz. To je tudi področje, kjer je sodelovanje javnega in zasebnega sektorja izjemno pomembno.

Če se vrnem k vprašanju. Menim, da posvečamo več pozornosti kot v preteklosti, vendar še vedno premalo glede na njegovo izjemno pomembnost, zahtevnost in dejstvo, da ima lahko vsaka pomanjkljivost velike posledice za delovanje posameznih sistemov in hude neposredne posledice na delovanje celotne družbe, na naše vsakdanje življenje. To se je pokazalo ob nekaterih, vsaj zaenkrat, relativno manj kritičnih primerih. Zato je varovanje kibernetskega prostora in krepitev kibernetske varnosti ena izmed ključnih prioritet. V to bomo morali vložiti več znanja, angažirati in usmeriti v skupno delovanje vse razpoložljive potenciale.

Kritična infrastruktura je bila v obdobju COVID-19 krize zelo pogosto omenjena beseda. Ali smo po vaši oceni uspešno zagotavljali neprekinjenost delovanja ključnih infrastrukturnih zmogljivosti?

Po moji oceni je ta kriza pokazala, da smo sposobni zagotoviti delovanje kritične infrastrukture v zelo težkih razmerah. Če dobro premislim, v vsem času se nismo soočili z razmerami, ko posamezni segmenti ne bi bili sposobni opravljati svoje dejavnosti. Pravzaprav so se vsi ključni subjekti zelo hitro odzvali in se prilagodili v marsičem povsem novim in zahtevnim razmeram. Vsem, ki so zagotavljali delovanje je potrebno izreči iskreno priznanje in zahvalo.

Seveda, pokazale pa so se tudi pomanjkljivosti. Navkljub izjemnim naporom zdravstvenega sistema, medicinskega in drugega osebja se je pokazalo, da je v tem sistemu že v normalnih razmerah veliko težav, ob tako veliki krizi pa so te še bolj izrazite. Pri tem imam v mislih, tako organizacijski vidik kot ustrezno opremljenost in zadostno število kadra, ki je še posebej izpostavljen v takšnih razmerah. Dobro je, da bodo takšna zagotovila, in celovita ureditev razmer v zdravstvenem sistemu ena ključnih nalog nove Vlade. Zaradi sprememb v okolju in tveganjih, ki izhajajo iz morebitnih drugih kriz, lahko takšne in podobne epidemije pričakujemo tudi v prihodnje. V tem okviru bo potrebno premisliti in sprejeti potrebne ukrepe za boljše obvladovanje razmer na področju socialno varstvenih storitev.

Sedanje izkušnje morajo biti izhodišče za temeljito analizo v posameznih sektorjih s ciljem odprave posameznih pomanjkljivosti, vpeljavo dobrih praks iz pretekle krize in nadgradnje načrtov za posamezne krize.

Moje osebno mnenje je, da je krizno upravljanje na vseh nivojih izjemno zahtevno. Sistem, ki je vzpostavljen na podlagi preteklih izkušenj je dober. Zato bi bilo morda še manj težav, če bi ga v celoti upoštevali in izvajali.

V času pandemije se je posebej izpostavil še en dejavnik in sicer ključni človeški viri, ki so pomembni za neprekinjenost zagotavljanja delovanja kritične infrastrukture. Katere so tiste izkušnje, ki jih moramo v relaciji do ključnega kadrovskega potenciala upoštevati v organih nacionalne varnosti?

Človek je vedno ključen dejavnik. Vse ostale pomanjkljivosti lahko v veliki meri presežemo z dobro usposobljenimi in motiviranimi ljudmi. Kriza je pokazala, da imamo glede tega izjemen potencial. Menim, da se je ogromna večina ljudi, angažiranih v nacionalno varnostnem sistemu, izkazala s svojim delom in motiviranostjo. Pri tem moram posebej izpostaviti sistem zaščite in reševanja in Civilno zaščito, ki je v ključnih trenutkih odločno in odlično podprla zdravstveni sistem, odigrala pomembno vlogo pri oskrbovanju starejših v domovih starejših občanov in tudi v okolju, kjer sicer živijo.

Izkazalo se je, da so tisti subjekti in sistemi, ki več vlagajo v pripravo svojih pripadnikov za delovanje v krizah, veliko usposabljajo in nasploh posvečajo delu z ljudmi, takšne krize še bolje obvladovali. Za to so odgovorna predvsem vodstva. Tako, z distanco, bi ocenil, da so nekatera vodstva s tem imela malenkost več težav.

Kot sem že omenil, pa vidim pomanjkljivosti na področju kriznega upravljanja in strateškega komuniciranja. Tu so vrzeli večje, tako na nivoju celotnega sistema, kot posameznih podsistemov ali subjektov. Pomanjkljivosti in napake so vplivale tudi na ljudi v sistemu nacionalne varnosti in odnos do njih v javnosti. Zato bo potrebno vložiti veliko dela v usposabljanje za uspešnejše krizno upravljanje. Če povzamem, ustrezna pripravljenost in usposobljenost ter motiviranost so ključni elementi, ko govorimo o človeških virih.

Kje so po vašem mnenju še mogoče izboljšave in rezerve v razmerju sodelovanja nacionalnih institucij in segmentov korporativne varnosti v pomembnih gospodarskih organizacijah za boljše zagotavljanje varnostnih procesov delovanja pomembnih infrastrukturnih zmogljivosti?

Korporativna varnost je pomemben del zagotavljanja varnosti v družbi. V posameznih elementih je sestavni del nacionalne varnosti, saj je zagotavljanje visoke stopnje varnosti in zaščita interesov v gospodarskih in drugih dejavnostih v nacionalnem interesu. Zato je tesno sodelovanje ključno. In to ne sme biti zgolj fraza, ki se lepo sliši. To mora biti del našega skupnega vsakdanjega dela. V mislih imam skupno delo na področju regulative, človeških virov, pretoka znanja, varnostnega osveščanja, ki je v Sloveniji še poseben izziv, in izkušenj. Prepričan sem, da bi lahko marsikateri deficit pri strokovnih kadrih v nacionalno varnostnem sistemu zapolnili z bolj fleksibilnim sistemskim pristopom in s tem povečali učinkovitost nacionalno varnostnega sistema ter povečali stopnjo varnosti.

Slovensko združenje za korporativno varnost je primer dobre prakse sodelovanja državnih, javnih in gospodarskih institucij. Kakšno je vaše mnenje o tem okolju sodelovanja in kje bi lahko našli še dodatne sinergije, ki bi krepile to platformo sodelovanja in izmenjav dobrih praks?

Če odgovorim zelo kratko in izhajam iz prejšnjega odgovora. Združenje s svojim vsestranskim potencialom ima lahko še večjo vlogo, kot pomembno stičišče za vsa področja, ki sem jih omenil malo prej. Če bo ustrezno razumevanje pri tistih, ki vodijo sistem nacionalne varnosti, in bodo videli priložnosti v skupnem delu, potem lahko v relativno kratkem času dosežemo napredek pri vseh izzivih o katerih je bilo govora v tem pogovoru. ■

Foto: arhiv Urada predsednika RS

ZARJA ELEKTRONIKA

Varno v nov dan.



- razvoj
- inženiring
- proizvodnja
- projektiranje

sistemov za tehnično varovanje

60 LET TRADICIJE

www.zarja.com

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
ga. Mojca Prelesnik, informacijska pooblaščenka Republike Slovenije*

PROCESI VAROVANJA ZASEBNOSTI V NENEHNEM ISKANJU RAVNOTEŽJA V DRUŽBENI SKUPNOSTI

Zahtevne družbene razmere ob nenehnih spremembah, ki so postale stalnica modernega varnostnega okolja, na področje varovanja zasebnosti prinašajo nove in nove izzive. O ukrepih, ki zagotavljajo tiste potrebne standarde na področju zagotavljanja varovanja zasebnosti, smo se pogovarjali z gospo Mojco Prelesnik.

Danes si praktično težko predstavljamo katerikoli organizacijski proces, da ob tem ne pomislimo na varovanje osebnih podatkov. To je verjetno določen pokazatelj, da se je to področje uspelo uveljaviti, in da je postalo pomemben segment evropske družbe. Kakšna je vaša strokovna ocena dinamike razvoja? Ste zadovoljni z dosežen im v Republiki Sloveniji?

Prvi zakon o varstvu osebnih podatkov je bil sprejet že leta 1990, torej pet let pred evropsko direktivo (95/46). Konec leta 2005 je nastal Informacijski pooblaščenec, za katerega lahko po odzivu ljudi rečem, da se je skozi leta uveljavil kot zaupanja vreden neodvisni organ. Obenem pa se je skozi leta dvigovala tudi ozaveščenost posameznikov in družbe glede pomena varovanja osebnih podatkov in zasebnosti. Seveda tudi ta razvoj ni bil premočrten – za mnoge smo varuh njihovih pravic, tudi številni odločevalci se obrnejo na nas. Vseeno pa imam občutek, da moramo nekatere temeljne postulate vedno znova ponavljati, tako politikom kot državljanom, a to je verjetno del našega poslanstva. Varovanja zasebnosti namreč ni enostavno razumeti. Tako vedno znova vidimo primerjave, kako Google nekaj počne, naši državi, policiji pa IP tega ne dovoli, pa izjave češ, da nimamo kaj za skrivati, česa bi se bali, kraje identitete se dogajajo le drugim in podobne. Žal pogosto pomembnosti varovanja naših podatkov ne razumemo, dokler sami ne doživimo zlorabe. Še težje za razumeti pa je, če nas zloraba ne doleti – zakaj toliko pravil, ko pa se mi ni nikoli nič zgodilo? Dejstvo pa je, da brez zasebnosti ni svobode in ni demokracije, in včasih je dobro pokukati čez naše meje in videti, kaj lahko pomeni izguba te svobode. Kitajska nam npr. s primeri biometričnega nadzora, »točkovanjem« državljanov in blokadami svobodnih komunikacij daje zelo zgovorna svarila. Z razvojem pri nas smo v grobem lahko zadovoljni, je pa varovanje zasebnosti prav gotovo nikoli končano delo in lahko bi rekli, da smo šele na začetku res množičnega zbiranja in uporabe naših podatkov.

Poudariti pa moram, da zadnji dve leti sodeč po analizi dela Informacijskega pooblaščenca, nista osvetlili le pomena zasebnosti. Izkazalo se je tudi, kako bistvena sta transparentna javna uprava in učinkovit dostop do informacij javnega značaja v časih, ko so temeljne pravice drastično omejene.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

V Sloveniji imamo na zakonodajnem področju določene izzive predvsem, ko govorimo o sprejemu ZVOP-2? Ste zadovoljni s pripravljenim predlogom, ki je bil posredovan v proceduro sprejema v Državni zbor?

V Sloveniji nikakor ne moremo biti zadovoljni že zato, ker je več kot 6 let po sprejemu Splošne uredbe o varstvu podatkov in 4 leta po začetku njene uporabe, Slovenija edina država Evropske unije, ki še vedno nima izvedbenega zakona za njeno izvajanje. To med drugim pomeni, da Informacijski pooblaščenec, kot nacionalni nadzorni organ za varstvo podatkov ne more izrekati upravnih glob zaradi kršitev Splošne uredbe, pač pa le prekrške za kršitev posameznih določb nacionalnega Zakona o varstvu osebnih podatkov. Hkrati pa to pomeni za pravno varnost povsem nevzdržno situacijo, ko se ne ve točno, kakšna je pravna ureditev tako pomembnega področja. Obstoječi Zakon o varstvu osebnih podatkov oz. ZVOP-1 namreč v delu še vedno velja in se uporablja, noben zakon pa ne določa v katerem delu točno.

To naj bi odpravil ZVOP-2, ki pa še ni bil vložen v zakonodajni postopek v Državni zbor. Informacijski pooblaščenec je svoje zadnje mnenje podal v okviru strokovnega usklajevanja maja lani. Izpostavili smo zlasti nujnost strokovne uskladitve in jasne ureditve pritožbenega postopka, pa tudi naše pristojnosti glede izvajanja pravic posameznikov. Posebej želimo, da ne pride do nižanja standardov glede na veljavne določbe ZVOP-1. Posebne dodatne pozornosti mora biti nujno deležna tudi ureditev kazenskih določb, zlasti pri opredelitvi izrekanja upravnih glob in sodelovanja IP v čezmejnih postopkih nadzora. Ves čas opozarjamo, da so kazenske določbe glede predpisane višine in razpona glob izdelane pomanjkljivo in površno, ter niso skladne z določbami Splošne uredbe. Opozorili pa smo tudi na nekatere neustreznosti ureditve videonadzora in biometrije. Zadnji javno objavljen predlog ZVOP-2 s februarja 2022, ki naj bi bil v obravnavi na vladi, teh pomanjkljivosti v pretežnem delu ne odpravlja. Informacijski pooblaščenec ni seznanjen, ali je vlada od takrat zakon še dopolnjevala in kakšna bo nadaljnja usoda predloga ZVOP-2, zato podrobneje nadaljnjega postopka priprave zakona ne morem komentirati.

Predvsem obdobje epidemije COVID-19 je prinesel zahtevne razmere vezane tudi na varovanje osebnih podatkov državljanov. V določenih primerih ste se javno in odločno postavili v bran tej osnovni pravici po ustreznem varovanju osebnih podatkov državljanov. Kako ocenjujete to obdobje?

Obdobje zadnjih dveh let je bilo nedvomno eno najzahtevnejših, tudi na področju varstva obeh ustavnih pravic, ki ju Informacijski pooblaščenec varuje. Na področju varstva podatkov so bile najbolj množične prijave, ki smo jih prejeli v preteklem letu, povezane zlasti z ukrepi države povezanimi z epidemijo. Poudariti pa moram, da zadnji dve leti sodeč po analizi dela Informacijskega pooblaščenca, nista osvetlili le pomena zasebnosti. Izkazalo se je tudi, kako bistvena sta transparentna javna uprava in učinkovit dostop do informacij javnega značaja v časih, ko so temeljne pravice drastično omejene.

Pokazalo se je, kako krhka so ravnovesja med posameznimi pravicami in kako življenjsko pomembno je, da vsaka institucija dosledno in odgovorno uresničuje Ustavo RS tudi v praksi. Prav zato smo ves čas opozarjali na nujnost jasnih, ustavno skladnih in razumljivih predpisov. Na podlagi zaprosil za mnenja, prijav in stikov z ljudmi smo namreč na področju varstva podatkov zaznali velike stiske posameznikov, podjetij, šol, in drugih organizacij prav zaradi nejasnih, hitro spreminjajočih in ustavno spornih predpisov. Z žalostjo ugotavljam, da zakonodajalec v preteklem letu ni izkoristil priložnosti, da bi odpravil številna neskladja, ki jih je Ustavno sodišče že ugotovilo.





Skoraj pri nobenem projektu digitalizacije ne gre brez osebnih podatkov, zato je pravočasna naslovitev tveganj bistvena za njihovo obvladovanje in predpogoj za zakonitost projekta ter upoštevanja temeljnih načel varstva osebnih podatkov.

Upam, da bo država naredila analizo izkušenj preteklih dveh let in se bomo vsi skupaj iz tega kaj naučili o pomenu iskanja pravih ravnovesij pri skrbi za dobrobit vseh. To je lepo razvidno na primeru uporabe modernih tehnologij. Države so kot eno temeljnih orodij za učinkovito obvladovanje epidemije prepoznale obdelave osebnih podatkov s pomočjo najrazličnejših aplikacij in tehnologij. Nadzorni organi smo ves čas opozarjali, da varstvo zasebnosti ni in ne sme biti razumljeno kot ovira pri varovanju interesov javnega zdravja, ampak mora biti sestavni del snovanja aplikacij. Eno zmed poročil nevladnih organizacij z decembra 2021 zdaj jasno kaže na posledice neupoštevanja teh vidikov. Nevladne organizacije so namreč poudarile, da je bilo zaradi pomanjkljive komunikacije vlad in ne transparentnosti glede uporabe aplikacij in podatkov porušeno zaupanje v aplikacije, posledica pa nižje število uporabnikov.

.

Kako uspešna je po vaši oceni integracija mreže pooblaščencev za varovanje osebnih podatkov v različnih organizacijskih okoljih? Je s sistemskega stališča to prava pot za dvigovanje nivoja zaščite osebnih podatkov v Sloveniji?

Glede na dosedanje izkušnje se je institut pooblaščenih oseb za varstvo osebnih podatkov izkazal kot učinkovit. Seveda tako kot drugje obstajajo primeri dobrih in slabih praks – kjer so te osebe dojete kot interni varuhi pred kršitvami, zlorabami in sankcijami, tam imajo na voljo ustrezne pogoje za delo, dostop do vodstva, znanja in primeren položaj v organizaciji. Po drugi strani pa, kjer te osebe jemljejo zgolj kot birokratsko dolžnost, od njih ni prave koristi. Podobno velja za zunanje ponudnike tovrstnih storitev, saj vidimo primere zelo usposobljenih, zagnanih in učinkovitih ponudnikov, medtem ko nekateri poročajo o takšnih, ki ponujajo standardne obrazce in le osnovno pomoč za mesečne pavšale. Informacijskemu pooblaščencu je kontakte pooblaščenih oseb do sedaj sporočilo že okrog 2500 organizacij. Mi jih dojemamo kot neke vrste »podaljšano roko Informacijskega pooblaščenca«, saj izvajajo tako nadzorne kot svetovalne in ozaveščevalne naloge, zelo pomembno pa je tudi njihovo medsebojno povezovanje in izmenjava izkušenj ter dobrih praks.

Digitalizacija procesov močno vpliva tudi na varovanje osebnih podatkov in ukrepe, ki jih je potrebno zagotavljati v tej povezavi. Tukaj je še kar nekaj dilem in izzivov, ki jih je potrebno ocenjevati v vsakem konkretnem primeru. Menite, da imate s tega naslova kaj več vprašanj in dilem, ki prihajajo s strani različnih organizacijskih okolij?

Digitalizacija prav gotovo tudi na področju varstva osebnih podatkov prinaša nove izzive. Nadzor parkirišč s pomočjo bralnikov registrskih tablic, merjenje potovalnih časov z blu-

etooh signali, covid aplikacije in sledilniki, orodja za delo od doma in nadzor tega, e-storitve državne uprave in še dolgo bi lahko naštevali. Na pot digitalizacije ni primerno stopati brez dobro zavezanih čevljev, oz. kot nedvomno drži - pot v pekel je tlakovana z dobrimi nameni. Vsakokrat posebej se pokaže, da kolikor projekte digitalizacije peljejo zgolj IT-jevska zagnanost, politična všečnost ali ekonomska računica, pri tem pa se ne upošteva tveganj, ko govorimo o osebnih podatkih, potem projekti trčijo ob težave. Zlasti gre za potrebne in vnaprejšnje pravne podlage, pravočasno in celovito obveščanje posameznikov ter upoštevanja minimizacije obdelave že v samem dizajnu rešitev, torej tako imenovana načela vgrajenega in privzetega varstva podatkov. V tej luči se kot učinkovito orodje kažejo pravočasne in celovite ocene učinka na varstvo osebnih podatkov (DPIA). Skoraj pri nobenem projektu digitalizacije ne gre brez osebnih podatkov, zato je pravočasna naslovitev tveganj bistvena za njihovo obvladovanje in predpogoj za zakonitost projekta ter upoštevanja temeljnih načel varstva osebnih podatkov. Kakovostna ocena učinka lahko prihrani veliko stroškov, popravljalnih ukrepov in izgube zaupanja – če je seveda narejena pošteno in ne zgolj kot propagandni material z namenom dokazovanja ali zavajanja, da bo vse v redu.

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

Menim, da je v prvi vrsti pomembno zavedanje, da vrednost organizacije leži v njenih podatkih, ti se pa le še v manjšem delu obdelujejo na papirju. Kibernetska varnost tako predstavlja ključen gradnik v varovanju naše vrednosti, zaupanja v nas, našega dobrega imena. S tega vidika bi morala biti deležna ustreznih sredstev, usposobljenih kadrov in sistemskih pristopov. Splošna uredba o varstvu podatkov tukaj žogico vrže upravljavcem podatkov, sami se morajo sprofilirati: oceniti tveganja in sprejeti potrebne ukrepe, pri tem pa seveda uporabljati mednarodne standarde, dobre prakse in priporočila.

V praksi se pojavljajo nevarni precedensi, kjer zagovorniki t.i. »Red teamov« zagovarjajo stališča, da lahko pri naročenih vdornih testih v informacijske sisteme vdirajo in pregledujejo elektronsko pošto zaposlenih. Kako odgovarjate na taka stališča?

Pri katerem koli naročanju storitev, naj gre za obdelavo podatkov, storitve s področja informacijske varnosti ali kaj tretjega velja osnovno pravilo, da naročnik na izvajalca ne more prenesti pooblastil, ki jih tudi sam nima oziroma jih izvajalcu neposredno ne daje zakonodaja. V Republiki Sloveniji imamo zelo strogo varovanje komunikacijske zasebnosti, ki zajema tudi komunikacije v delovnih okoljih. Delodajalci bi morali izpolniti stroge pogoje, ki jih določa Ustava v 37. členu, če bi želeli posegati v komunikacijo zaposlenih po elektronski pošti ali telefonu in prav gotovo ne smejo kar tako vdirati in pregledovati predalov elektronske pošte zaposlenih – ne sami, ne s pomočjo zunanjih izvajalcev; nenazadnje bi s tem lahko posegli tudi v pravice tretjih oseb, torej pošiljateljev izven organizacij naročnika ter bili na meji storitve kaznivih dejanj. Kolikor je namen naročnika preveriti varnost sistema elektronske pošte bi se tako lastni, kot zunanji izvajalci varnostnega preverjanja morali ustaviti na točki, ki izkazuje ranljivost(i) sistema in ne izkazovati jih s pregledovanjem elektronskih sporočil.

> Pravica dostopa do informacij javnega značaja je temeljna človekova pravica, ki vsakomur omogoča pridobitev informacij o pomembnih družbenih temah. Obenem pa omogoča tudi nadzor nad delom organov javnih oblasti in porabo javnega denarja, s čimer se preprečuje slabo gospodarjenje z javnimi sredstvi in korupcija. Tu smo v zadnjih dveh letih žal zaznali izrazito povečanje števila pritožb, tudi zaradi molka organa. To kaže na to, da se je transparentnost delovanja javnega sektorja v teh dveh letih zmanjšala.

V zadnjem obdobju so bile pomembne razprave tudi na področju priprave ustreznega pravnega akta vezanega na zaščito oseb, ki anonimno razkrivajo nepravilnosti. So bili v tem procesu priprave zakona upoštevani tudi vaši pomisleki in predlogi rešitev?

Prenos direktive o zaščiti žvižgačev je za vse države Evropske unije velik in pomemben zalogaj. Informacijski pooblaščenec je podal pripombe na predlog zakona o zaščiti žvižgačev, ki so bile v velikem delu upoštevane. Vendar ne gre le za vprašanja zakonskega urejanja ali varstva podatkov, pač pa predvsem za spreminjanje utrjenih vzorcev razmišljanja. Zato je zakon šele prvi korak, ki naj bi pripomogel k ustvarjanju okolja, v katerem se bo posameznik, ki v svojem delovnem okolju dobronamerno zazna kršitev, počutil dovolj varnega, da o njej poroča najprej v okviru svojega podjetja oziroma organizacije. Zunanja prijava, ki je dejansko že zdaj na voljo, je namreč šele drugi korak. Gre za to, ali smo kot družba zreli in sposobni odgovorno in samokritično pogledati na lastne napake.

Različni nadzorni organi dejansko v skladu z Zakonom o inšpekcijskem nadzoru in področno zakonodajo že obravnavamo zunanje prijave in pomembno je, da nov sistem temelji na izkušnjah, ki jih že imamo. Ključna naloga v praksi bo za vse vzpostavitev varnih poti prijav in usposabljanje zaposlenih, ki so v stiku s strankami o možnostih svetovanja v primeru grožnj povračilnih ukrepov. V delu zavarovanja in podpore žvižgačem glede povračilnih ukrepov pa bo največjo vlogo imela Komisija za preprečevanje korupcije. Informacijski pooblaščenec neredko prejmemo prijave ali pritožbe posameznikov, ki domnevnih kršitev niso uspeli razrešiti v okviru lastnih delovnih okolij. Nimamo pa veliko izkušenj s konkretno zaščito prijaviteljev, saj se posamezniki v tem delu običajno ne obračajo na nas po pomoč. To bo vsekakor izziv tudi na nas.

Katera težišča in nove pristope lahko v prihodnje pričakujemo s stališča EU, vezano na področje varstva osebnih podatkov? Verjetno je še vedno svojevrsten izziv regulacija velikih korporacij, ki imajo sedež izven EU in množično obdelujejo naše podatke, kot npr. Google, Twitter in podobni.



Splošna uredba o varstvu podatkov je velik korak naprej pri zagotavljanju možnosti za čezmejni nadzor na ravni Evropske unije, hkrati pa resen poskus, kako k varovanju pravil varstva podatkov prisiliti tudi velike korporacije, ki so izven EU. Vendar moramo biti pri slednjem realni. Nadzorni organi iz držav članic EU imamo pravno gledano in v praksi zelo omejene možnosti za ukrepanje, če ima podjetje zgolj predstavnika v EU, ne pa tudi podružnice.

Za učinkovitejši čezmejni nadzor sta nedvomno revolucionarni zlasti dve novosti, ki ju je prinesla Splošna uredba. Prva izredno pomembna novost je bila ustanovitev Evropskega odbora za varstvo podatkov, ki je organ EU, katerega odločitve so pravno zavezujoče. Druga nič manj pomembna novost pa je vzpostavitev postopka čezmejnega nadzora ‚vse na enem' mestu. Preko tega vodilni nadzorni organ v nadzornih postopkih glede podjetij, ki imajo več podružnic v EU, usklajuje delo ostalih nadzornih organov. Taki postopki tečejo in so se že zaključili tudi z večmilijonskimi globami. Primeri takega čezmejnega nadzora ne vključujejo le storitev priljubljenih spletnih velikanov, kot so npr. Facebook, Google, Amazon, in drugi, ampak tudi neustrezna ravnanja z osebnimi podatki drugih akterjev, tudi ponudnikov bančnih storitev, spletnih ponudnikov različnih storitev, ponudnikov pretočnih storitev, povezanih vozil itd. iz številnih držav članic EU. Praksa nadzorov kaže, kako velik izziv je usklajevanje čezmejnih postopkov zaradi različne postopkovne zakonodaje v državah članicah, zato čezmejni postopki trajajo dlje, kot bi si želeli.

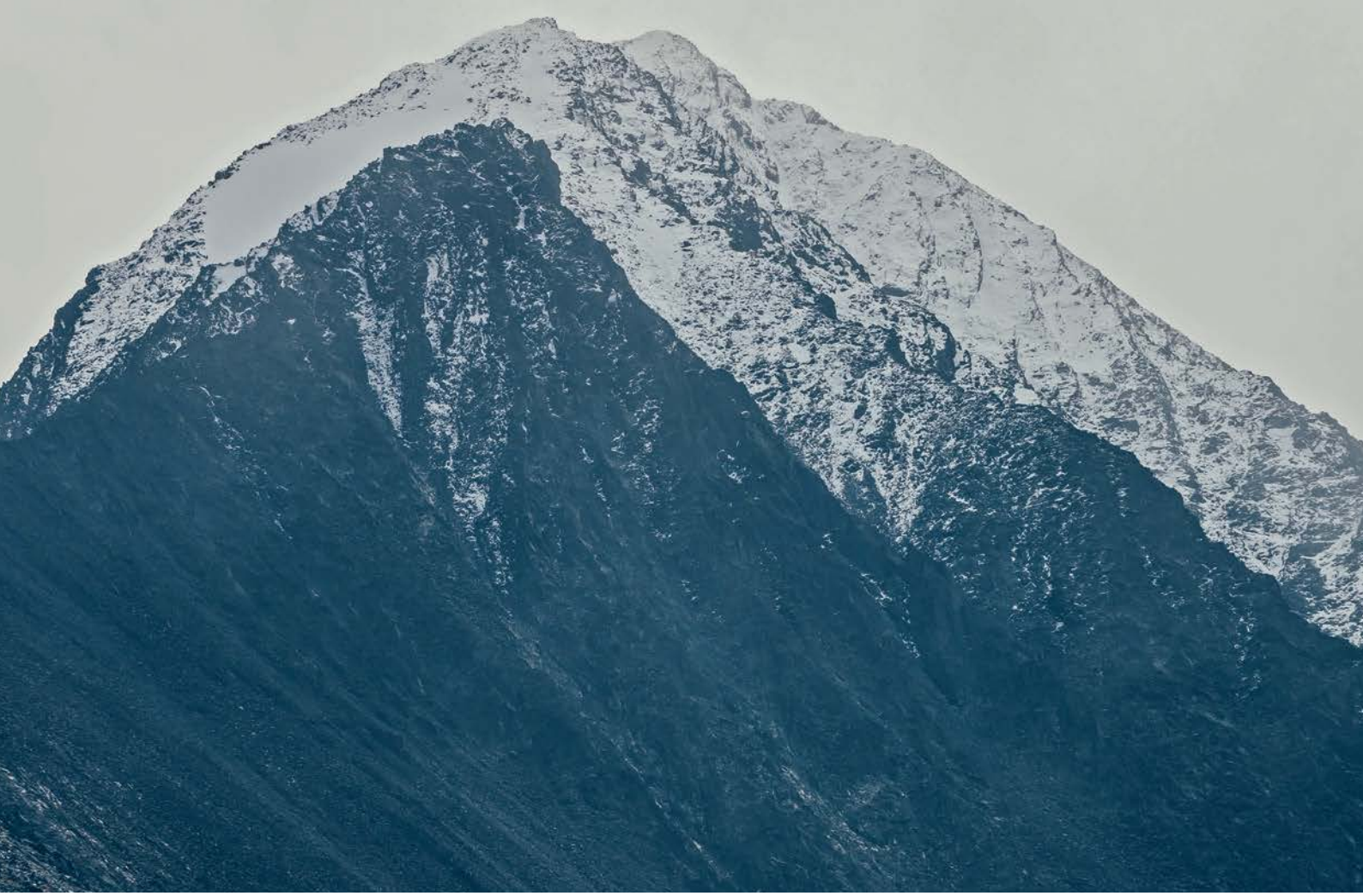
Vsekakor pa nas čaka na ravni EU ob svetlobno hitrem razvoju tehnologije tudi nadaljnji nujni razvoj pravnih okvirjev. Eden takih velikih zakonodajnih projektov Evropske unije je mega paket 6 ‚digitalnih' zakonov s področja obdelav podatkov, ki pokriva tudi urejanje umetne inteligence in e-zasebnosti. Pomembno pa bo vplival tudi na razvoj mehanizmov varstva osebnih podatkov ter izvajanje nadzora.

Kakšno je stanje procesov na drugem pomembnem področju, ki ga pokrivate in sicer dostop do informacij javnega značaja. V zadnjem obdobju ste se v javnosti velikokrat oglasili tudi s potrebnimi obrazložitvami s tega področja. Je preglednost delovanja države pomembna v smeri nadzora državljanov nad njenim delom?

Pravica dostopa do informacij javnega značaja je temeljna človekova pravica, ki vsakomur omogoča pridobitev informacij o pomembnih družbenih temah. Obenem pa omogoča tudi nadzor nad delom organov javnih oblasti in porabo javnega denarja, s čimer se preprečuje slabo gospodarjenje z javnimi sredstvi in korupcija. Tu smo v zadnjih dveh letih žal zaznali izrazito povečanje števila pritožb, tudi zaradi molka organa. To kaže na to, da se je transparentnost delovanja javnega sektorja v teh dveh letih zmanjšala. Zlasti zaskrbljujoče je naraščanje števila pritožb zoper državne organe, torej v glavnem zoper državno upravo, ministrstva in organe v sestavi. Naraščajo pa tudi primeri, kjer so prosilci za informacije mediji, ki imajo v demokratični družbi posebno vlogo tako imenovanih psov čuvajev. To pomeni, da bi jim morale biti informacije dostopne hitro in na čim učinkovitejši način. Žal v praksi ni tako.

V času epidemije pa je narastlo tudi število primerov, kjer so prosilci zahtevali informacije o epidemioloških ukrepih, javnem zdravju in s tem povezano porabo javnega denarja. Ukvarjali smo se npr. s primeri različnih statistik o obolelosti in smrtnosti, nabavo zaščitne opreme, cepljenjem, izplačili dodatkov za delo v posebnih pogojih, plačami javnih uslužbencev... Ker gre večinoma za informacije, ki so v širšem javnem interesu, smo se zato večkrat odločili, da jih zavezanci morajo posredovati javnosti. ■

ZAVEZANI SMO H GRADNJI OMREŽIJ, KI SO VARNA, STABILNA IN ZANESLJIVA



VARNOST, BREZ KOMPROMISOV

HUAWEI

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
mag. Tanja Muha, direktorica Agencije za komunikacijska omrežja in storitve Republike Slovenije*

REGULATORNI ORGANI IMAJO IZREDNO POMEMBNO VLOGO ZA OHRANJANJE RAVNOVESJA V EKOSISTEMU ELEKTRONSKIH KOMUNIKACIJ

Izredno hiter razvoj modernih komunikacijskih tehnologij na eni strani, in izpostavljena potreba po urejenosti sistema delovanja elektronskih komunikacij na drugi strani, nas postavlja pred pomembne izzive, kako zagotavljati uravnoteženost tega krhkega sistema. Če v ta okvir dodamo še dinamična varnostna tveganja, imamo več kot dovolj izzivov, o katerih smo se pogovarjali z mag. Tanjo Muha.

Strateški varnostni izzivi pred katerimi, kot del mednarodnega okolja stoji tudi Slovenija, bodo imeli pomemben vpliv na delovanje AKOS. Nam lahko zaupate, kje pričakujete največje izzive, ki sledijo področjem, ki jih upravljate v vaši agenciji?

Na področju elektronskih komunikacij na agenciji ugotavljamo, da vsi operaterji niso enako dobro pripravljeni na vse te izzive. Potrebno bo vzpostaviti regulatorno okolje, ki bo zagotovilo varne storitve končnim uporabnikom, hkrati pa bo tudi vzdržno na strani operaterjev. Tako na strani operaterjev, kot tudi agencije, pa bo velik izziv zagotoviti dovolj ustrezno število tudi ustrezno kvalificiranih kadrov, s primernim strokovnim znanjem. Še naprej pa bo ključnega pomena tesno sodelovanje z drugimi regulatornimi organi v državah članicah, tako znotraj Organa evropskih regulatorjev elektronskih komunikacij BEREC kot tudi znotraj ENISA, za izmenjavo informacij in za iskanje dobrih praks ter enotnih pristopov.

Uvedba 5G tehnologije pomeni pomemben korak v smeri digitalizacije družbe. S trendom digitalizacije se bo 5G omrežje, zaradi tehničnih karakteristik, uporabljalo na vseh segmentih družbe in sektorjev, tudi tistih, ki se do sedaj v teh zgodbah niso pojavljali. S povezovanjem velikega števila sistemov in naprav, ter posledičnega zbiranja ogromnega števila podatkov, se veča tudi možnost različnih zlorab.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Korona kriza je izpostavila pomen kritične infrastrukture, zlasti varnosti in odpornosti komunikacijskih sistemov. Menite, da so se operaterji informacijsko-komunikacijskih storitev ustrezno odzvali na izzive te krize?

V času korona krize se je zaradi velikega obsega dela in šolanja od doma bistveno povečala potreba po višjih kapacitetah omrežja. Prav tako pa se je, kot pomembna izkazala varnost in celovitost komunikacijskih omrežij in storitev. Na agenciji smo tudi v tem obdobju, poleg nadzorstvene vloge, dajali velik poudarek preventivno usmerjenemu delovanju in imeli smo vzpostavljeno tesno sodelovanje z operaterji komunikacijskih storitev. V okviru tega je potekalo redno izmenjevanje informacij o delovanju omrežij in storitev, vključno s spremljanjem uspešnosti odzivanja operaterjev na že omenjene bistveno višje potrebe po kapacitetah priključkov na strani končnih uporabnikov. V tem okviru je agencija operaterjem, v kolikor se je to izkazalo za potrebno, nudila tudi ustrezno podporo in imela pripravljene scenarije za primere, ko operaterji z razpoložljivimi resursi ne bi zmogli slediti tem zahtevam. Ugotavljamo, da so se operaterji ustrezno odzvali na izzive te krize in vlagali znatne napore v optimizacijo in nadgradnjo omrežja, v smeri zagotavljanja višjih kapacitet in varnosti tega. Posledično zato v Sloveniji nismo bili postavljeni pred izzive, kot v nekaterih drugih državah članicah, kjer so dejansko morali poseči po dodatnih ukrepih, kot npr. začasni dodelitvi dodatnega radio-frekvenčnega spektra operaterjem.

Spremembe Zakona o elektronskih komunikacijah (ZEKom-2) še vedno niso zagledale luč sveta. Kdaj menite, da lahko pričakujemo sprejem te pomembne zakonske podlage?

Na agenciji si želimo, da se ZEKom-2 čim prej sprejme in se s tem ustrezno prenese določbe Evropskega zakonika na področju elektronskih komunikacij tudi v slovenski pravni red. V tej luči bo agencija za dosego tega cilja, še naprej nudila vso potrebno strokovno podporo zakonodajalcu. Zakon je bil v državnem zboru že tik pred sprejemom, kar pa se iz znanih razlogov na koncu ni realiziralo. Na hitrost sprejema ZEKom-2 bo vsekakor pomembno vplivala tudi njegova vsebina. Osebno menim, da bi bil lahko zakon z ustreznimi popravki sprejet hitro. Sploh ob upoštevanju kazni, ki bodo Slovenijo doletele, zaradi nepravočasne implementacije evropskih direktiv v nacionalni pravni red.

Ste kot direktorica tega pomembnega regulatornega organa zadovoljni z zadnjimi spremembami in dopolnitvami, ki jih je bil deležen osnutek zakona, skozi postopek medresorskega usklajevanja in parlamentarne procedure?

Agencija je že od leta 2018 bila aktivna članica delovne skupine, ki je pripravljala predlog ZEKom-2 in v okviru tega nudila ministrstvu obsežno strokovno podporo. Kljub temu pa so se kasneje v predlogu predmetnega zakona pojavila določila, ki so po mnenju agencije zelo sporna, saj so v evidentnem nasprotju z evropskimi direktivami. Na to je agencija, pa tudi jaz sama, kot direktorica agencije, pristojne javno in z dopisi tudi večkrat opozorila. Žal pa problematičnih členov, tudi v času popravljanja vsebine zakona v postopku njegovega sprejemanja, niso ustrezno prilagodili. Problematični so predvsem trije členi, ki v obliki, kot so napisani, pomenijo poseganje v neodvisnost delovanja agencije, kot regulatornega organa. Kako pomembna je neodvisnost regulatorja potrjuje dejstvo, da tako kot evropski zakonik za elektronske komunikacije, tudi vse ostale evropske področne direktive iz področij delovanja agencije poudarjajo, da sta za sektorske regulatorje bistvena njihova neodvisnost in samostojnost, kar je potrebno s strani držav članic tudi zagotoviti. Neodvisnost in samostojnost zajema, tako neodvisnost od dnevne politike, kakor tudi od reguliranih subjektov na trgu. Slednje velja še toliko

Agencija pozdravlja novo vlogo URSIV, kot nosilca sektorja »informacijsko-komunikacijskih omrežij in sistemov«. Obveznosti operaterjev omrežij na področju elektronskih komunikacij bodo skladno z ZEKom-2 še vedno pod nadzorom agencije, pri čemer pa URSIV prevzema pomembno vlogo koordinatorja celotnega ekosistema vseh sektorjev.

bolj, v kolikor ima država prevladujoče lastninske deleže v podjetjih, ki jih preko sprejetih ukrepov regulira agencija.

Obstoječa verzija predloga ZEKom-2 posega v rok za izvajanje tržnih analiz, s tem pa tudi v regulatorni cikel, na način, da se kljub temu, da je jasno določen 5-letni cikel v direktivi, lahko na zahtevo operaterja ta rok skrajša na 3 leta. Navedeno poleg tega, da pomeni poseganje v avtonomnost delovanja agencije, pomeni tudi bistveno oteženo ustrezno planiranje dela agencije oz. realizacije plana dela agencije za posamezno leto. V drugem delu ZEKom-2 že vnaprej opredeljuje upoštevni trg na podlagi zmogljivosti različnih tehnologij, kljub dejstvu, da direktive jasno določajo, da se upoštevni trg



definira s strani agencije na podlagi analize trga in na podlagi zamenljivosti storitev, ter tehnološko nevtralno. Od vseh določb zakona, pa pomeni najbolj grob poseg v neodvisnost delovanja člen, ki vpeljuje dodaten razlog za predčasno razrešitev direktorja agencije, in sicer zamudo zakonskih rokov pri odločanju agencije. V Sloveniji ne obstaja niti en primer agencije, organa ali organizacije javnega sektorja, kjer bi bil uzakonjen takšen razlog za razrešitev direktorja. Evropski zakonik za elektronske komunikacije in tudi ostale področne direktive, kot pomembnejšo varovalko za zagotavljanje neodvisnosti regulatornih organov, poleg finančne in kadrovske neodvisnosti, določa tudi zagotavljanje neodvisnosti vodstva.

V preteklem obdobju je bilo tudi nekaj poskusov Vlade Republike Slovenije usmerjenih v racionalizacijo delovanja določenih regulatornih organov. Posegu v avtonomnost institucije, ki jo vodite, ste argumentirano zelo močno nasprotovali. Kateri so bili tisti glavni argumenti, ki s strokovnega stališča ne dopuščajo možnosti zmanjševanja avtonomnosti AKOS?

V primeru poskusa sprejema predloga Zakona o Javni agenciji Republike Slovenije za trg in potrošnike in Javni agenciji Republike Slovenije za finančne trge, je prav tako šlo za vsebino zakona, ki je bila v nasprotju z več evropskimi direktivami, katere poudarjajo samostojnost oz. čim večjo neodvisnost agencije od ustanovitelja, pri čemer se neodvisnost nanaša, tako na financiranje, kot na organizacijo in notranje postopke. V predlogu zakona ni bilo jasno, kje bo sedež novonastale agencije, niti ni predvidel organizacijske strukture. Agencija je ugotavljala, da ima mehanizme, ki jih je predlagatelj navajal, kot prednosti povezovanja regulatorjev v agencijo, že vzpostavljene (denimo Sektor za ekonomske analize, zgledno urejen informacijski sistem, vzpostavljen nadzor ministrstev in sodišč nad delom in odločitvami agencije, ter vzpostavljeno pregledno financiranje). Glede skladnosti z evropskimi pravili, neodvisnosti in samostojnosti, bolj preglednega financiranja ter večje učinkovitosti in fleksibilnosti, pa agencija meni, da bi s predlaganim zakonom bil dosežen ravno obraten učinek. Agencija je po področjih dela že danes eden največjih regulatorjev v Evropi, saj pokriva kar pet (5) vsebinskih področji: elektronske komunikacije, radio-komunikacije, pošta, elektronski mediji in železnice, obenem pa je četrti najmanjši regulator po številu zaposlenih. Pet področij je tudi sicer največje število različnih področij, ki jih pokrivajo regulatorni organi v državah EU. Agencija s kar devetimi področji, kot jo je predvideval predlog zakona, bi tako predstavljala tudi bistven odmik od praks v Evropi.

Kaj pomembnega se je dogodilo na ravni EU, ki bo imelo pomembne vplive tudi na vaše delovanje in na splošno na delovanje sektorja telekomunikacij?

Agencija bo po implementaciji EECC z ZEKom-2 v nacionalni zakonodaji prenovila pripadajoče splošne akte, kjer si bo prizadevala za konkretnost in določnost zakonskih in podzakonskih aktov, kar bo pripomoglo k pravni varnosti in posledično tudi k predvidljivim in čim krajšim postopkom na področju regulacije telekomunikacij. Z uvedbo ZEKom-2 bo na področju varnosti omrežij in storitev prišlo do precej vsebinskih sprememb, saj predlog zakona vključuje, tako določbe novega evropskega zakonika o elektronskih komunikacijah, kot tudi druge strateške usmeritve Evropske komisije za zagotovitev višje ravni kibernetske varnosti v Evropi. V luči novih strategij Evropske komisije s področja zagotavljanja kibernetske varnosti, bo tudi agencija morala povečati nadzor

nad zavezanci, še posebej nad tistimi, ki nudijo svoja omrežja in storitve upravljalcem kritične infrastrukture, izvajalcem bistvenih storitev, organom državne uprave in nosilcem ključnih delov nacionalno-varnostnega sistema. Nadzor in preverjanje ravni varnosti se bo povečalo tudi pri zavezancih, ki bodo uvedli mobilna omrežja 5G, saj bodo s svojo infrastrukturo podporni komunikacijski steber za marsikatero gospodarsko panogo ali storitev, ki je ključna za delovanje države in družbe. ZEKom-2 bo pri zavezancih povzročil kar precej sprememb na tem področju. Prišlo bo namreč do vsebinskih sprememb zakonskih določb, posledično bodo te povzročile spremembe tudi pri splošnih aktih agencije.

Marca 2021 je Evropska komisija objavila digitalni kompas, ki predstavlja vizijo in poti za digitalno preobrazbo Evrope. Pol leta kasneje je predlagala še pot do digitalnega desetletja - konkreten načrt za digitalno preobrazbo družbe in gospodarstva Evropske unije do leta 2030. Evropska komisija si s predstavitvijo poti do digitalnega desetletja prizadeva dokončati predlog skupne „Izjave o digitalnih načelih“. Ta govori o zagotavljanju evropskih vrednot in pravicah, ki se odražajo v digitalnem prostoru, da bodo lahko vsi državljani uživali prednosti digitalnih priložnosti, kot so univerzalni dostop do interneta, transparentni algoritmi, ki zagotavljajo pošteno in ne diskriminatorno odločanje, ter varno in zaupanja vredno spletno okolje. Gigabitna povezljivost, podprta z varnimi optičnimi in 5G omrežji, je nepogrešljiva za ustrezno digitalizacijo vseh segmentov družbe. Tega se zavedamo tudi članice BEREC, kjer se je prav tako prepoznalo potrebo po skupnem delovanju, tudi na področju kibernetske varnosti. BEREC in ENISA bosta tako okrepila medsebojno sodelovanje in še bolj podpirala NIS kooperativno skupino pri vseh aktivnostih, povezanih z vzpostavljanjem kibernetske varnosti v EU. V te aktivnosti je agencija še posebej aktivno vključena, saj sopredsedujemo ekspertni skupini BEREC, ki se ukvarja z vprašanji kibernetske varnosti 5G omrežij. O vsem aktualnem dogajanju na tem področju bo agencija tudi v prihodnje deležnike in zainteresirano javnost sproti seznanjala.

Kako ocenjujete uspešnost uvajanja rešitev 5G v neposredno operativno okolje. Ali tukaj zaznavate kakšne dodatne izzive, ki bi jim veljalo posvetiti več pozornosti?

Uvedba 5G tehnologije pomeni pomemben korak v smeri digitalizacije družbe. S trendom digitalizacije se bo 5G omrežje, zaradi tehničnih karakteristik, uporabljalo na vseh segmentih družbe in sektorjev, tudi tistih, ki se do sedaj v teh zgodbah niso pojavljali. S povezovanjem velikega števila sistemov in naprav, ter posledičnega zbiranja ogromnega števila podatkov, se veča tudi možnost različnih zlorab. In zlorabe se v takem okolju lahko dogajajo, tako na strani naprav pri končnih uporabnikih, kot tudi na samem omrežju. Za ustrezno naslavljanje tovrstnih izzivov je potrebna, tako ustrezna pravna ureditev, kot tudi intenzivno ozaveščanje uporabnikov, tako poslovnih kot tudi rezidenčnih, v smeri sprejemanja ustreznih preventivnih ukrepov in vpeljevanjem preventivnega delovanja. Dodaten poudarek pa je potrebno dati zagotavljanju ustrezne kakovosti, varnosti in celovitosti omrežja na strani operaterjev teh omrežij, saj ti postajajo z digitalizacijo platforma, na kateri bo vse delovalo. Zagotavljanje informacijske in kibernetske varnosti, ter varnosti samih omrežij tako postaja še pomembnejše. Pri tem bo zagotovo pomembna tudi ustrezna implementacija t.i. orodja za povezljivost in sprejem ZEKom-2. Zelo pomembno bo tudi nadaljnje tesno sodelovanje vseh pristojnih organov in nudenje ustrezne podpore dolžnikom na trgu. Z vidika pristojnosti agencije, pomeni uvajanje 5G rešitev v operativno okolje širok nabor aktivnosti, tako na področju same gradnje omrežij in njihovo umeščanje v prostor, kot tudi na področju zagotavljanja storitev uporabnikom in varnosti, ter celovitosti omrežij in storitev. Na podlagi obveznosti, ki so jih operaterji sprejeli v okviru pridobitve frekvenc, je rok za implementacijo 5G omrežja na območju celotne države do leta 2025. V tem času bo potrebnih veliko aktivnosti in dela, kar bo pripomoglo k uspešnosti uvajanja rešitev 5G. Zaenkrat uvajanje poteka v pričakovanih okvirih.

Agencija je aktivna članica Slovenskega združenja korporativne varnosti. Na agenciji menimo, da je navedeno sodelovanje pomembno, saj združenje povezuje predstavnike podjetij in institucij iz različnih sektorjev.

Kibernetska varnost postaja vedno bolj pereči izziv za organizacije, državo in tudi mednarodno skupnost. Na področju kritične infrastrukture so se pred kratkim uveljavile določene spremembe, kjer je naloge nosilca sektorja »informacijsko-komunikacijskih omrežij in sistemov« prevzel Urad za informacijsko varnost. Kaj pričakujete od te spremembe in ali pričakujete krepitev sodelovanja pri urejanju tega pomembnega sektorja?

Agencija ima z URSIV že sedaj vzpostavljeno konstruktivno in zgledno sodelovanje. Agencija pozdravlja novo vlogo URSIV, kot nosilca sektorja »informacijsko-komunikacijskih omrežij in sistemov«. Obveznosti operaterjev omrežij na področju elektronskih komunikacij bodo skladno z ZEKom-2 še vedno pod nadzorom agencije, pri čemer pa URSIV prevzema pomembno vlogo koordinatorja celotnega ekosistema vseh sektorjev. Slednje je še posebej pomembno z vidika prepoznavanja celostne slike in usklajenih pristopov. ZEKom-2 bo formalno uredil odnose med vsemi pristojnimi organi: agencijo, URSIV in SI-CERT. V prihodnje pričakujem nadaljnjo krepitev sodelovanja in vzpostavitev dodatnih mehanizmov. Agencija si že več let prizadeva za vzpostavitev enotnega sistema za poročanje operaterjev, ki bi pomenil zmanjšanje administrativnih ovir, tako za zavezance kot tudi za agencijo in druge pristojne organe.

Kako ste zadovoljni z vašim delovanjem v okviru Slovenskega združenja korporativne varnosti? Kateri so tisti dejavniki, ki bi jih pri tem sodelovanju želeli posebej poudariti?

Agencija je aktivna članica Slovenskega združenja korporativne varnosti. Na agenciji menimo, da je navedeno sodelovanje pomembno, saj združenje povezuje predstavnike podjetij in institucij iz različnih sektorjev. S tega vidika vidimo navedeno združenje, kot pomembno mesto za seznanjanje s trendi in dogajanjem na področju informacijske in kibernetske varnosti ter za izmenjavo dobrih praks. Na agenciji pozdravljamo tudi organizacijo vsakoletne strokovne konference Dnevi korporativne varnosti, ki jo organizira združenje, na njej pa vsako leto s strokovnim prispevkom sodeluje tudi agencija. ■

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: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Pavle Jazbec, glavni izvršni direktor in član upravnega odbora skupine Actual I.T.

NEPREKINJENOST DELOVANJA KRITIČNE INFRASTRUKTURE NAM JE POMEMBEN STROKOVNI IZZIV

Kritična infrastruktura v energetiki in transportni logistiki je posebej izpostavljena skozi prizmo dveh pomembnih sektorjev, ki močno vplivata na učinkovitost delovanja moderne družbe globaliziranega sveta. Ob vse zahtevnejši intenziteti kriz, ki se pojavljajo v dinamičnem varnostnem okolju, je zaščita kritične infrastrukture postala poseben imperativ, ki ne zaposluje samo strokovnjakov s tega področja, temveč vedno bolj tudi strateške odločevalce na nacionalni in tudi mednarodni ravni. O izzivih in priložnostih na tem področju smo se pogovarjali z g. Pavlom Jazbecem, glavnim izvršnim direktorjem družbe Actual I.T.

Strateško varnostno okolje postaja vedno bolj zahtevno. Energetika in logistične dobavne verige so vedno bolj na udaru vplivov kriz s katerimi smo soočeni. Kako iz vašega strateškega pogleda ocenjujete trenutno stanje in kakšen vpliv bo to imelo na vašo organizacijo?

Kritična infrastruktura je od nekdaj zahtevna. Posamezni sektorji so na različnih zrelostnih ravneh in nekateri imajo implementiranih že veliko mehanizmov, ki povečujejo odpornost. Na primer finančni sektor ima zelo dobro urejeno regulativo, ki posamezne organizacije sili k enovitemu pristopu menjave podatkov, načinih avtentikacij, načrtov za okrevanje idr.

Sektor energetike je trenutno zahtevnejši zaradi več tehnoloških omrežij, ki zahtevajo ločene obravnave, a morajo delovati med sabo preko izmenjave podatkov.

Tudi logistične verige tvorijo več deležnikov, ki niso nujno na isti zrelostni ravni, zanje so značilni tudi manj standardizirani procesi. To za nas ni novost. Še naprej moramo ohranjati in graditi domensko znanje posameznega sektorja in krepiti odnose s partnerji, specialisti na posameznem področju. Vsekakor zahtevnejša okolja za nas pomenijo dodaten izziv in večanje naše konkurenčne prednosti, saj prodajamo predvsem znanje in s tem izstopamo med ponudniki, ki prinašajo zgolj rešitve na zahtevo brez svetovanja.

S pojavom novih poslovnih modelov ponujanja npr. alternativnih pogonskih energentov, električnih polnilnic, polnilnic vodika, več manjših zasebnih elektrarn, vključenih v celovito omrežje, povezovanje različnih ponudnikov idr., se pojavljajo čisto novi izzivi, ki zahtevajo povezovanje s specialisti oz. partnerji za posamezno področje.



Vedno bolj ste s svojimi rešitvami in znanjem prisotni v organizacijah, ki upravljajo s kritično infrastrukturo. Predvsem ste usmerjeni v področje energetike in logistike? Kje vidite posebej izpostavljene izzive v teh konkretnih področjih, ki jih bo potrebno začeti ustrezno naslavljati, če bomo želeli zagotavljati ustrezno neprekinjenost delovanja?

Naša skupina je od nekdaj delovala na področju kritične infrastrukture. Je pa res, da je čedalje več organizacij in vertikal skozi digitalizacijski moment tako ali drugače vpeto v kritično infrastrukturo. Tako vse naše stranke obravnavamo kot del kritične infrastrukture, saj je njihov osnovni proces zanje kritičen in zahteva določeno raven nemotenega poslovanja.

Vsekakor nismo prisotni v vseh sektorjih enako, saj je potreba po domenskem znanju, ki zagotavlja strokoven pristop. Kot tudi nismo prisotni samo na energetiki ter logistiki, temveč še na javni upravi, telekomunikacijah, kritični infrastrukturi državnega in zasebnega pomena, itd.

Na področju energetike vidimo izzive enovitega in celovitega upravljanja z varnostnimi tveganji. Težava niso rešitve, saj le te že obstajajo. Več izzivov je na področju kadrov in novih tehnologij, ki jih bodo morali nasloviti. S pojavom novih poslovnih modelov ponujanja npr. alternativnih pogonskih energentov, električnih polnilnic, polnilnic vodika, več manjših zasebnih elektrarn, vključenih v celovito omrežje, povezovanje različnih ponudnikov idr., se pojavljajo čisto novi izzivi, ki zahtevajo povezovanje s specialisti oz. partnerji za posamezno področje. Izrednega pomena so vaje izvedbe načrtov neprekinjenosti poslovanja, ki jih izvaja premalo organizacij.

Tudi sektor logistike je podvržen podobnim izzivom, saj se srečujejo s sistemi, ki so ločeno nastajali, in vse več je zahtev po celoviti storitvi od izvora do ponora, ne glede na izzive med procesom. Dodaten izziv je vsebina logistike, saj se produkti med seboj lahko zelo razlikujejo in potrebujejo drugačna naslavljanja za dosego istega cilja, tj. dostava od izvora do ponora. Vsekakor na neprekinjenost poslovanja zelo vpliva dober pregled nad blagom v procesu in tako prihaja do mikro pozicioniranja vseh deležnikov, da upravljavec točno ve, kje se nahaja določen produkt, določeno vozilo s prediktivnimi metodami napovedovanja morebitnih sprememb v procesu. Prav tako imajo velik vpliv na neprekinjenost poslovanja tudi rezervni scenariji ob odpovedi določenih sistemov, kar nas ponovno vodi do izvajanja vaj izvedbe načrtov neprekinjenosti poslovanja.

Digitalizacija je eno izmed osrednjih težišč, ki ga vse moderne organizacije poskušajo v čim večjem obsegu implementirati v svoje organizacijske in poslovne procese. Kje vidite dodano vrednost, ki jo prinašate v ta segment s svojimi novimi informacijskimi rešitvami?

Vsa naša ponudba je oblikovana tako, da strankam dodajamo vrednost. To je cilj notranjega razvoja rešitev in storitev, kar prinaša uspeh tudi nam. Zavedamo se, da dolgoročnost sodelovanja pomeni, da moraš ponuditi nekaj, česar drugi nimajo. Tako zagotavljamo strankam celovitost ponudbe od svetovanja, implementacije, zagotavljanja obratovanja in uporabniške podpore na varen in skladen način. Seveda ni nujno, da vse stranke koristijo celoten proces, a le ta jim zagotavlja hiter odziv na spremembe, ki so stalnica poslovnega okolja naših strank. Ponujanje celovitih rešitev stranki pomeni poznavanje življenjskega cikla posamezne rešitve.

Da pa ne izgubimo strokovnosti na posameznem področju, smo organizirani v družbe, ki so osredotočene na svojo osnovno dejavnost. Le tako lahko strankam zagotavljamo napredne rešitve, ki so plod sodelovanja med posameznimi specialisti.

Naš cilj je biti najboljši v okviru, ki ga naslavljamo, in trga nikakor nočemo naslavljati samostojno, temveč v sodelovanju s partnerji. Skupaj smo namreč vedno močnejši »#strongertogether ni naključno naš moto«.

Kibernetska varnost je verjetno področje, ki se zaradi zahtev varnostnega okolja najhitreje razvija. Kako boste v vaši organizaciji sledili tempu razvoja storitev in procesov, ki jih pričakujejo organizacije v nacionalnem in mednarodnem okolju?

Z eno besedo – težko. Verjetno ni veliko ponudnikov, ki bi tako odgovorilo, saj je kibernetska varnost del naše specializacije in s tem ponudbe. Je pa izziv dojemanje področja kibernetske varnosti, ko so tveganja manjša. Namreč stranke se še premalo zavedajo nevarnosti oz. vrednosti za neprekinjenost poslovanja do prve večje težave. Potem žal večinoma ne moremo zagotavljati takšne podpore, kot jo prizadeti pričakuje, saj je prizadetih več segmentov. Od posameznih fizičnih implementiranih rešitev do načrtov neprekinjenosti poslovanja, ki se izkažejo za pomanjkljive.

Rešitev vidimo v sodelovanju, povezovanju z drugimi ponudniki, saj imamo ekipe, ki ob morebitnih težavah lahko in morajo sodelovati, da zagotovimo stranki čim hitrejše okrevanje. Izmenjava podatkov in sodelovanje na skupnih projektih zagotavljata višjo stopnjo varnosti, tako stranki kot ponudnikom storitev. Navezava na zunanje vire informacij pa so dodatno zagotovilo, da smo skupaj bolje pripravljeni na dogodke, ki zadevajo kibernetski prostor.

Delovanje lokalno pa ob vpetosti organizacij v mednarodno okolje pomeni ščitenje le teh z vseh strani. Imamo več strank, ki delujejo v več državah, in celovito naslavljanje varnosti je mogoče le s sodelovanjem vseh. Tudi uporabnikov z njihovo osveščenostjo.

Imate občutek, da bi se dalo na tem področju v Sloveniji z določenimi skupnimi koraki in sinergijami doseči boljše rezultate in višjo stopnjo zagotavljanja kibernetske varnosti?

Vsekakor. Ravno o tem sem govoril. Znanja, kot jih imate posamezni specialisti, se med seboj dopolnjujejo. Tisti, ki si še ni priznal, da sam ne zmore vsega, bo v današnjem hitro razvijajočem se svetu ostal na ravni, ki mu ne bo omogočala preživetja. Predvsem v Sloveniji moramo sodelovati med seboj, saj je naš trg majhen, zaradi vpetosti v globalno okolje pa moramo zagotavljati visoko raven varnosti. Povezovanje je prednost, ki jo lahko izkoristimo v mednarodnem okolju.

Ste močno usmerjeni v mednarodno okolje in tudi prisotni v pomembnih infrastrukturnih sistemih. Katere so tiste izkušnje in dobre prakse, ki jih lahko prinesete v slovensko okolje?

Mednarodno okolje ni več tako drugačno odkar živimo v povezanem svetu. Je pa res, da so razlike v dojemanju posameznega področja, odvisne od poslovne kulture. Zavedanje, da je digitalizacija smer, ki zagotavlja konkurenčno prednost našim strankam, je ponekod večje. Pri tem tudi razumevanje, da določene rešitve zahtevajo več sredstev tako finančnih kot človeških virov. Ena izmed dobrih praks, ki bi jo radi prenesli v lokalno okolje, je, da najnižja cena projekta ni edino merilo za sodelovanje.

Vsekakor pa je dobra praksa marsikje, da ločijo svetovalno fazo pred izvedbo projekta in nato samo implementacijo le tega. Obe fazi sta plačljivi in tako stranke dobijo kakovostnejše informacije za pripravo projekta in zagotovilo, da se ponudnik strokovno posveti izvedbi posamezne faze.

Zelo močno ste prisotni tudi v procesih uvajanja energetsko učinkovitih rešitev in tehnologij, ki podpirajo na zeleni prehod naših organizacij. Kateri so tisti projekti, na katere v prihodnosti posebej stavite, da bodo prinašali ustrezno dodano vrednost v smeri učinkovitosti?

Pri uvajanju zelenih rešitev smo previdni, saj se skupaj s strankami še učimo, kako ovrednotiti učinkovitost takšnih implementacij. Vemo, da omogočamo zeleni prehod, ni pa primerljivih kazalnikov, ki bi jasno pokazali, kaj neposredno prinaša dodano vrednost.

Že vrsto let imamo rešitve večih naših strank v lastnem podatkovnem centru, kar vsekakor zagotavlja boljši energetski izkoristek. Smo tudi dolgoletni nosilci certifikata 14001. To je vsekakor en korak v pravo smer. Sicer pa razvijamo projekte

Zavedanje, da je digitalizacija smer, ki zagotavlja konkurenčno prednost našim strankam, je ponekod večje. Pri tem tudi razumevanje, da določene rešitve zahtevajo več sredstev tako finančnih kot človeških virov. Ena izmed dobrih praks, ki bi jo radi prenesli v lokalno okolje, je, da najnižja cena projekta ni edino merilo za sodelovanje.

umetne inteligence, uporabe vizualne prepoznave in analitičnih orodij s prediktivnimi napovedmi. Pri omenjenih področjih znamo oceniti prihranke in dodano vrednost za stranke.

Področje raziskav in razvoja je posebej izraženo v vaši poslovni viziji. Zakaj se vam zdi pomembno, da temu področju namenjate toliko energije in pozornosti?

Za zagotavljanje konkurenčne prednosti naših strank moramo biti sami več korakov pred njimi glede poznavanja novih tehnologij in poslovnih modelov. Vsekakor pa raziskave in razvojno okolje pomenijo zaposlenim rast in spodbudno okolje, v katerem lahko prispevajo k osebni rasti in razvoju celotne družbe. Le učeča se družba napreduje in verjamemo, da to cenijo tudi naše stranke in partnerji.

Iz medijev smo bili seznanjeni o sprejemu vaše odločitve, da boste skupaj s Telekomom Slovenije dosegli pomembne sinergije v poslovanju in razvoju. Kateri so tisti poudarki, ki so vas prepričali, da krenete po tej poti?

Same lastniške spremembe do sedaj niso neposredno vplivale na naše delo. Kar smo pridobili, je anorganska rast v preteklosti, s tem lažje povezovanje družb s komplementarnimi programi in posledično večja dodana vrednost za naše stranke. Seveda pa so tako dobre kot slabše posledice lastniških sprememb.

Zadnja odločitev o delovanju v skupini Telekom Slovenije je prišla z logičnim razvojem dogodkov, saj smo že sodelovali na več projektih in smo prav tako komplementarni na več področjih. Zagotovo bo poleg Telekoma Slovenije in skupine Actual IT s tem pridobila največ slovenska družba, saj bo skupina ponovno v slovenski lasti. Skupina Telekom bo pridobila enega najmočnejših IT partnerjev v regiji, skupina Actual IT pa dostop do trga s povezanimi storitvami in rešitvami.

Na Dnevih korporativne varnosti ste tradicionalno prisotni in podpirate ta dogodek. Katera so tista težišča, zaradi katerih je ta dogodek pomemben za vašo organizacijo?

Dogodek je pomemben, saj strokovno naslavlja vprašanja, ki se jih komercialni ponudniki ne dotikajo preveč. To se sklada z našo vizijo. Vsekakor pa je to priložnost, da strokovnjakom in javnosti predstavimo svoje dosežke tudi vsebinsko in s tem odpremo dodatne izzive. Na tem področju smo dejavni vse leto, ne le ob tem dogodku. ■

Foto: arhiv Actual I.T.



OKREPITE VARNOST

4-dnevni tečaj

KIBERNETSKA VARNOST ICS/OT/IoT OKOLIJ

Kibernetski napadi na kritično infrastrukturo predstavljajo 5. največje globalno tveganje.

V obdobju enega leta od 2020 do 2021 so bila podjetja v povprečju 536-krat na teden tarča hekerjev.

Spoznajte, kako učinkovito vzpostaviti zaščito pred zlorabami in hekerskimi napadi za zagotovitev neprekinjenega delovanja industrijskih okolij in kritične infrastrukture.

Skenirajte za prenos programa

https://bit.ly/program-OT

info@smart-com.si

01 561 16 06

SMART COM

Zanesljiv, tehnološko napreden partner za kibernetsko varnost, informacijsko-komunikacijska omrežja in podatkovne centre.

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Peter Ceferin, tehnični direktor, Smart Com*

POMEMBNOST NOVIH PERSPEKTIV ZA UČINKOVITEJŠE OBVLADOVANJE KIBERNETSKIH TVEGANJ

Usmerjenost v upravljane storitve za specializirane tehnološke rešitve, pomeni korak naprej v učinkovitejšem obvladovanju ključnih procesnih in informacijskih sistemov, med katerimi imajo tisti v organizacijah kritične infrastrukture še posebej pomembno mesto. O priložnostih, ki jih prinašajo novi izzivi na področju kibernetske varnosti, smo se pogovarjali z g. Petrom Ceferinom, tehničnim direktorjem podjetja Smart Com.

Opravljate funkcijo tehničnega direktorja, ki v vsaki organizaciji pomeni operativno srce tehnološkega razvoja. Katere strateško razvojne vidike, ki vam bodo v prihodnjem obdobju zagotovili konkurenčne prednosti pred ostalimi organizacijami, bi v vaši organizaciji posebej izpostavili?

Naše poslovne usmeritve, ki se odražajo v vseh procesih znotraj organizacije, se skozi celotno 32 letno zgodovino delovanja podjetja Smart Com vedno osredotočajo na trg. Pri tem so naročniki v centru naše pozornosti in igrajo pomembno vlogo, saj prisluhnemo njihovim potrebam in zahtevam. Po drugi strani, interno vedno spodbujamo in izvajamo aktivnosti, ki so korak pred neposrednimi zahtevami naročnikov. Saj na konkurenčnem trgu tehnoloških rešitev s področja IT velja pravilo, da konkurenčnost vzdržuješ le tako, da naročnikom ponudiš napredne rešitve in storitve, ki jim pomagajo reševati tudi tiste izzive, ki se jih morda niti še ne zavedajo. Kljub hitremu tehnološkemu razvoju, je pri uvajanju takšnih rešitev vseeno potreben določen čas, da predlogi dozorijo in da se vpeljujejo premišljeno in strukturirano. V naši organizaciji tako tehnološki razvoj vodimo preko t. i. strateških iniciativ, ki so namenjene oblikovanju novih rešitev in storitev. Te iniciative so dolgoročno zasnovane aktivnosti, ki potekajo v večletnem obdobju. Znotraj njih se oblikujejo razvojni projekti, ki prinašajo konkretne rešitve in storitve. Tako smo identificirali strateške

> V kontekstu glavnih smernic našega tehnološkega razvoja je ravno z vidika povečevanja odpornosti organizacij na kibernetske grožnje ena ključnih usmeritev in priložnosti, ki jo vidimo, usmeritev v zagotavljanje namenskih storitev s področja upravljanja različnih tehnoloških rešitev.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



iniciative, ki posegajo na področje kibernetske varnosti, še posebej na področje industrijskih ICS/OT sistemov v kritični infrastrukturi in industrijskih okoljih, namenska privatna brezžična omrežja 5G z integriranimi mehanizmi kibernetske varnosti, ter podatkovni centri v kombinaciji s t. i. hiper-konvergenčno infrastrukturo in pa sisteme avtomatizacije na področju upravljanja komunikacijskih omrežij. Naš tehnološki razvoj usmerjamo na zaznane razmere na trgu, zato smo pred kratkim lansirali obsežnejši nabor t. i. upravljanih storitev, ki jih izvajamo na obeh naših ključnih tehnoloških področjih – kibernetski varnosti in komunikacijskih omrežjih. Vseprisotno pomanjkanje IT strokovnjakov in zavedanje, da zgolj tehnologija ne rešuje izzivov, s katerimi se organizacije srečujejo, nas je vzpodbudilo k razvoju in vzpostavitvi Smart Centra upravljanih storitev. V Centru ekipa kompetentnih strokovnjakov s področja kibernetske varnosti in komunikacijskih omrežij preko razdelanih postopkov zagotavlja in izvaja za naše naročnike prilagojene storitve upravljanja različnih segmentov kibernetske varnosti in omrežnih rešitev. Vse večja kompleksnost IT sistemov bo tako tudi v prihodnje zahtevala še intenzivnejše odzivanje in oblikovanje dodatnih storitev upravljanja. Pri tem moram omeniti, da storitve upravljanja s področja kibernetske varnosti niso nadomestek ali konkurenca storitvam Varnostno operativnih centrov, pač pa gre za komplementarne storitve. V Smart Comu se usmerjamo predvsem v upravljane storitve za specializirane tehnološke rešitve, kot so npr. sistemi za spremljanje in zaznavanje kibernetskih groženj in incidentov v procesnih (OT) in informacijskih (IT) sistemih, s katerimi se navezujemo na delovanje sektorskih Varnostno operativnih centrov. Pravilnost naših usmeritev potrjuje tudi trg in rezultati, ki jih beležimo.

Globalno varnostno okolje od nas zahteva popolnoma novo paradigmo zavedanja pomena varnosti delovanja informacijskih okolij. Kje v vaši organizaciji na tem področju vidite glavne priložnosti?

V kontekstu glavnih smernic našega tehnološkega razvoja je ravno z vidika povečevanja odpornosti organizacij na kibernetske grožnje ena ključnih usmeritev in priložnosti, ki jo vidimo, usmeritev v zagotavljanje namenskih storitev s področja upravljanja različnih tehnoloških rešitev. Organizacije čedalje več naporov in sredstev usmerjajo v posodobitve in digitalizacijo poslovnih in procesnih sistemov. Po drugi strani pa morajo nasloviti pereče vprašanje, ki je sistemske narave – pomanjkanje kadrov s področja IT tehnologij in kibernetske varnosti. Kot primer lahko navedem področje komunikacijskih omrežij – to področje je bilo pred časom zelo »popularno« in zaželeno področje dela za mlade inženirje. Če se danes na dogodkih s tega področja ozre-



mo naokrog, in poskusimo oceniti starostno strukturo strokovnega osebja, lahko hitro ugotovimo, da se ta populacija stara. To pomeni, da je dotok mladih inženirjev premajhen, da bi uravnovesil in zagotovil zadostno število potrebnega kadra za izvajanje obsežnejših in zahtevnih IT operacij, začenši z načrtovanjem in kasneje implementacijo ter upravljanjem. Zato smo ravno zaradi naših dolgoročnih usmeritev uspeli vzpostaviti ter ohranjati ekipo strokovnjakov z obeh področij – omrežij in kibernetske varnosti. Z ekipo tako zagotavljamo strokovni potencial za izvajanje različnih storitev, tudi storitve upravljanja, ki so časovno daljnosežne in zahtevajo ustrezno kritično maso primerno usposobljenega in strokovnega kadra v organizaciji.

Kje prepoznavate največje izzive pri integraciji različnih rešitev naprednih omrežij IT, ki podpirajo in so namenjena avtomatizaciji tehnoloških in poslovnih procesov?

Izzivi, s katerimi se srečujemo, so čedalje bolj vezani na obsežne možnosti, ki jih trg IT rešitev ponuja. Danes namreč ni več problem tehnologija ali rešitve, ki jih je moč kupiti na trgu, pač pa kako možnosti, ki so na voljo, čimbolj optimalno izkoristiti. Pri tem pa je potrebno vsako novo rešitev gledati in analizirati iz več zornih kotov. Poleg tehnološkega vidika moramo identificirati tudi konkurenčne prednosti, kako rešitev umestiti v specifiko tržnih vertikal, ki jih naslavljamo, ter zagotoviti ustrezen nabor strokovnega kadra za obvladovanje konkretnih tehnoloških rešitev. Te izzive uspešno naslavljamo, saj stalno namenjamo znaten del sredstev za strokovna in tehnološka usposabljanja ter osebni razvoj naših zaposlenih. Saj skrb za profesionalni razvoj naših zaposlenih in upravljanje s kadri obravnavamo kot pomemben element uspešnosti podjetja.

Razvoj informacijskih tehnologij, predvsem z uvajanjem storitev 5G, prinaša pomembne spremembe na področju operativnega informacijsko-procesnega okolja. Kje so po vašem mnenju tisti pomembni izzivi, ki jih bomo morali urediti, da bodo ti sistemi še naprej zagotavljali ustrezno neprekinjenost delovanja?

> Zelo intenzivno se ukvarjamo s področjem kibernetske varnosti, predvsem kako naše tehnološko znanje prenesti v kontekst storitev. Saj opažamo čedalje večji razkorak pri zagotavljanju strokovnega kadra v organizacijah, glede na čedalje večjo kompleksnost pri izvajanju nalog, ki so pomembne za zanesljivo delovanje informacijske tehnologije.

Spet se navezujem na vprašanje, kdo in kako bo upravljal z infrastrukturo in tehnologijami v operativnih procesnih okoljih. Velika razlika je namreč med uporabo 5G tehnologije v javnih omrežjih in uporabo te tehnologije v industrijskih okoljih ali kritični infrastrukturi. V javnih omrežjih je vedno na prvem mestu – koncept CIA (Confidentiality, Integrity, Availability), a v operativnih procesnih okoljih je ta koncept ravno obraten – AIC (Availability, Integrity, Confidentiality). To pomeni, da je na prvem mestu vedno razpoložljivost pred ostalimi elementi. Razpoložljivost pa je odvisna od spleta dejavnikov, med katerimi je ključna odpornost na kibernetske napade in zagotavljanje neprekinjenega delovanja tudi v smislu upravljanja takih omrežij. Kljub temu, da je s tehnološkimi rešitvami 5G že ne-

Slovensko združenje korporativne varnosti predstavlja zelo pomembno obliko platforme za povezovanje med različnimi akterji, ki delujemo na področju kibernetske varnosti. Nadvse pomembna je tudi možnost, ki jo združenje nudi za izmenjavo pretoka informacij in dobrih praks.

ločljivo povezana kibernetska varnost, je občutek, da smo pri 5G za operativna procesna okolja šele na začetku poti. Vendar ne toliko s tehnološkega vidika, temveč predvsem v smislu potrebnega zavedanja, kot je to že precej časa prisotno v IT okoljih.

Kibernetski varnosti namenjate izredno veliko pozornosti. Smo v obsežnem procesu digitalizacije širše družbene skupnosti. Kateri so tisti izzivi, ki jih s tega področja velja posebej izpostaviti?

Na področju kibernetske varnosti bi izpostavil predvsem dejstvo, da se bomo različni akterji – naročniki, raziskovalne in akademske institucije ter ponudniki – morali na tem področju še bolje povezovati, čeprav ugotavljam, da je v zadnjih letih že prišlo do pomembnega napredka na tem področju. Je pa to dolgoročen proces, na katerem je treba vztrajati. Pri tem, po našem mnenju, združenja, kot je Slovensko združenje korporativne varnosti, igrajo zelo pomembno vlogo pri krepitvi kibernetske varnosti v širšem družbenem pomenu. Zelo pomembno je tudi, da se lahko konkurenti povezujemo in tudi tako zagotovimo ustrezne vire in znanja na trgu. Krepitev kibernetske varnosti je namreč proces podoben povezovanju zavezniških vojaških enot, saj obramba pred kibernetskimi napadi marsikje že prehaja na področje hibridnega vojskovanja. Nedavna vaja Locked Shields 22, na kateri je sodelovala tudi naša ekipa, je dokaz, kako pomembno je organizirano delovanje in združevanje strokovnega ter organizacijskega potenciala različnih akterjev.

Razvojna usmerjenost vaše organizacije ni bila nikoli vprašljiva. Katerim tehnološkim procesom trenutno namenjate največ raziskovalne pozornosti?

Zelo intenzivno se ukvarjamo s področjem kibernetske varnosti, predvsem kako naše tehnološko znanje prenesti v kontekst storitev. Saj opažamo čedalje večji razkorak pri zagotavljanju strokovnega kadra v organizacijah, glede na čedalje večjo kompleksnost pri izvajanju nalog, ki so pomembne za zanesljivo delovanje informacijske tehnologije. Z letošnjim letom smo trgu predstavili Smart Center upravljanih storitev, v katerem in okrog katerega poteka največ naših aktivnosti. V Center vlagamo, tako razvojna sredstva kot strokovna znanja z namenom zagotoviti našim naročnikom in partnerjem zanesljivo in kakovostno delovanje sistemov s področja kibernetske varnosti in omrežnih tehnologij.

Kadrovski potencial in njegovo pomanjkanje je verjetno v zadnjem obdobju tema, ki zaposluje vse nivoje v naših organizacijah. Ste prišli do kakšnih posebnih pristopov, ki vam v podjetju zagotavljajo svež kadrovski potencial z informacijsko- tehničnega področja?

Tudi za nas in naš razvoj je ključnega pomena ustrezen kadrovski potencial. Mi smo se s temi izzivi srečevali že dlje časa, zato smo tudi v obdobje vsesplošnega primanjkljaja strokovnega kadra vstopili dobro pripravljeni. Bodoče sodelavce identificiramo že v fazi študija na različnih fakultetah in jim nudimo praktična usposabljanja, prek katerih se spoznajo z našo dejavnostjo. Ključnega pomena pa je, da spoznamo drug drugega, da ugotovimo, ali jim področje, na katerem delujemo predstavlja profesionalni in osebni izziv ter ali se poistovetijo z našimi vrednotami, ki jih živimo v podjetju. Na ta način uspemo tudi zagotavljati zdravo mešanico strokovnega kadra s svežimi idejami na eni strani ter preizkušenimi pristopi na drugi strani.

Bi po vaši oceni več sredstev iz paketa za okrevanje po epidemiji morali nameniti krepitvi robustnosti informacijskega okolja v ključnih organizacijah, še posebej tistih, ki upravljajo s kritično infrastrukturo?

Če se malo pošalim - teh sredstev ni nikoli dovolj. Dejstvo pa je, da bodo za dvig odpornosti informacijskih okolij, predvsem v sistemih kritične infrastrukture, pri čemer ciljam na operativne procesne sisteme (OT), potrebne večje investicije. Podjetja se tega zavedajo, kar se je potrdilo tudi ob nedavni pripravi vlog za pridobivanje sredstev iz paketa za okrevanje, saj so podjetja ravno s področja kibernetske varnosti pripravila največ projektov. Bojim pa se, da razpisana sredstva ne bodo dovoljšna za obseg potreb, ki jih zaznavamo na trgu.

Katere so vaše lastne rešitve, ki zagotavljajo prepoznavnost vaše organizacije kot ponudnika, ki je sposoben učinkovito, zanesljivo ter varno reševati poslovne in tehnološke izzive vaših partnerjev?

Smart Com je že vrsto let prepoznaven na področju razvoja rešitev za komunikacijska omrežja ter kibernetsko varnost. Zaradi dolgoročnega sodelovanja z našimi partnerji smo razvili kompetence in poznavanje specifičnih okolij, kot so npr. okolja kritične infrastrukture, industrijskih okolij, finančnih institucij ter sistemov javne uprave. Zato lahko naše rešitve in storitve bistveno bolje optimiziramo in prilagodimo tem okoljem, kar nam naši partnerji tudi priznavajo. Kot tipičen primer bi tukaj navedel rešitve omrežnih sistemov in kibernetske varnosti za področja operativne tehnologije, ki so pomembna za kritično infrastrukturo, kot so elektrogospodarstvo in industrijska okolja.

Vrsto let ste kot podporniki prisotni na pomembnem dogodku Dnevi korporativne varnosti. Kaj vam pomeni sodelovanje na dogodku in kako ocenjujete priložnosti nagovarjanja ključne strokovne javnosti, predvsem iz organizacij kritične infrastrukture?

Slovensko združenje korporativne varnosti predstavlja zelo pomembno obliko platforme za povezovanje med različnimi akterji, ki delujemo na področju kibernetske varnosti. Nadvse pomembna je tudi možnost, ki jo združenje nudi za izmenjavo pretoka informacij in dobrih praks. Dogodek Dnevi korporativne varnosti pa s poglobljenimi vsebinskimi prispevki predstavlja veliko dodano vrednost, ne samo za člane združenja, ampak tudi za strokovno javnost v širšem pomenu. Tudi organizacije kritične infrastrukture, ki so vključene v dejavnosti združenja, pomembno prispevajo k širitvi zavedanja pomena kibernetske varnosti, kar ima velik vpliv na nadaljnjo krepitev in razvoj odpornosti organizacij. ■

Foto: arhiv Smart Com

HSI
VARNOSTNE REŠITVE

CAPTIS®
Upravljanje avtomatiziranega vstopa/izstopa vozil na območju podjetja

Captis® je **napreden**, **prilagodljiv pametni sistem upravljanja s parkirišči,** primeren tako v manjših kot večjih podjetjih, mejnih prehodih, transportu in logistiki.

CAPTIS®

- Glasovni klic/VoIP
- Avtentikacija
- Najave
- ANPR
- RFID

AVTENTIKATORJI · POVEZLJIVOST · APLIKACIJE · EDINSTVENOST

- Povezljivost z drugimi sistemi
- Možnost povezave v oblaku
- Spletni način upravljanja
- Digitalni podpis
- API integracija

- Merjenje hitrosti
- Kontrola dostopa
- Lokacija vozil – cone
- Upravljanje s parkirišči
- Usmerjanje po parkirišču
- Potek dela v realnem času

- RoI
- Hibrid
- Večjezičnost
- GDPR skladnost
- Popolna prilagodljivost
- Ultimate privacy način delovanja

HSI d.o.o., Ljubljanska cesta 28, 8000 Novo mesto · +386 7 600 1960 · info@hsi.si · podpora@hsi.si · www.hsi.si

DOBRODOŠLI
PRI NAS
NA POTI

www.petrol.si/na-poti

PETROL
Energija za življenje

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
prof. dr. Aleš Ahčan, predavatelj na Ekonomski fakulteti v Ljubljani

UPRAVLJANJE S TVEGANJI JE KLJUČNO ZA NEPREKINJENO DELOVANJE ORGANIZACIJ

Organizacije v zadnjem obdobju vse več pozornosti namenjajo iskanju pravih odgovorov kako učinkovito upravljati s tveganji v dinamičnem poslovnem okolju. Kako lahko aplikacija Silver Bullet Risk olajša preglednost tega zahtevnega procesa smo povprašali dr. Aleša Ahčana, predavatelja na Ekonomski fakulteti v Ljubljani.

Globalne krize so postale stalnica, ki močno vpliva tudi na delovanje organizacij v tem povezanem poslovnem okolju. Kakšna je vaša ocena prihodnjih trendov. Se bodo razmere v naslednjih letih zaostrovale ali lahko v nekem doglednem času pričakujemo stabilizacijo?

Globalne krize bodo postale vedno bolj pogoste. Razlogi so, da je strukturno svet vedno bolj zadolžen, da so surovine omejene in da je vedno več ljudi v smislu multilateralne diverzifikacije centrov moči. To bo vodilo v enem delu do večjih tarif, v drugem delu pa do večjih transakcijskih stroškov, kar bo povzročalo, da bodo krize bolj pogoste, daljše in obdobja volatilnosti močnejša. Vmes bodo obdobja žepov stabilnosti, ki bodo omogočala nadpovprečno velike zaslužke tistim, ki bodo preživeli, torej tistim, ki bodo dobro upravljali s tveganji. Vsekakor pa bo svet bistveno bolj dinamičen, cikel razvoja in propada produktov se bo močno skrajšal. Povedano *še bolj neposredno,* gremo v smeri džungle in preživeli bodo le najbolj pripravljeni.

Upravljanje s tveganji je v takih razmerah za organizacijo eden od pomembnejših, če ne celo najpomembnejši poslovni proces. Vas lahko prosim za oceno stanja v kakšni kondiciji so na tem področju poslovne organizacije v Republiki Sloveniji?

Vezano na prejšnje vprašanje je logično, da bodo obdobja volatilnosti, ko so ovire bistveno večje in realizacije tveganj za podjetja bolj pereča, lažje preživela podjetja, ki tveganja bolje upravljajo. To pomeni, da so bolje pripravljena na različne scenarije in dejavnike realizacije posameznih tveganj. Glede tega je stanje v Sloveniji dokaj zaskrbljujoče. Tveganja se bolj ali manj upravljajo pro forma in toliko, da se odkljuka nujno potrebno za izpolnitev birokratskih zahtev. Medtem, ko vsebinsko pravega upravljanja s tveganji praktično ni, razen v redkih podjetjih, ki jih lahko preštejemo na prste dveh rok.

Glede tega je stanje v Sloveniji dokaj zaskrbljujoče. Tveganja se bolj ali manj upravljajo pro forma in toliko, da se odkljuka nujno potrebno za izpolnitev birokratskih zahtev. Medtem, ko vsebinsko pravega upravljanja s tveganji praktično ni, razen v redkih podjetjih, ki jih lahko preštejemo na prste dveh rok.

Kateri so tisti ključni dejavniki procesa upravljanja s tveganji, ki bi jih posebej izpostavili kot ključne, da tak proces lahko ustrezno deluje znotraj organizacijskega okolja?

Ključni dejavniki za uspešno upravljanje s tveganji so nedvomno t.i. povratna zanka. To pomeni, da se tveganja ocenijo v posameznih pristojnih delih organizacije, ki

imajo največji vpogled v vsebino in realizacijo tveganja, s strani vodij posameznih oddelkov. Na podlagi njihovih ocen se nato spremlja vpliv realizacije tveganja na poslovni izid ter se popravi, poveča ali zniža, glede na dejanski razvoj dogodkov, ocena t.i. maksimalne škode oziroma najslabšega možnega realističnega *škodnega* dogodka. Le na ta način preko povratne zanke, s katero se spremlja vpliv na poslovni izid in se hkrati sprejema poslovne odločitve o ščitenju ali izpostavljenosti dejavnikom tveganja, lahko pridemo do smiselne integracije tveganj v poslovno odločanje. Tveganja imajo namreč svoj strošek. Znižanje vrednosti rublja, porast vrednosti nafte, naraščanje cene elektrike, neplačila kupcev, vse to ima finančni učinek, ki lahko zamaje stabilnost in likvidnost ter v skrajnem primeru povzroči smrt podjetja.

Ste zelo priznan član akademske skupnosti, imate pa tudi bogate poslovne izkušnje. Kaj po vašem mnenju je v Sloveniji potrebno spremeniti, da bomo pri strateškem managementu vzpodbudili višje zavedanje o pomenu učinkovitega upravljanja s tveganji?

Odgovor je povsem enostaven. Dokler ne bo sankcij, da bodo odgovarjali, tako nadzorni sveti kot uprave za neuspešno oziroma neadekvatno upravljanje s tveganji, ali pa bodo banke sankcionirale podjetja, ki ne bodo uspešno upravljala s tveganji, z višjimi obrestnimi merami. Torej, dokler ne bo finančnega stroška iz naslova slabega upravljanja s tveganji, tožb, ali penalizacije v višjem strošku zadolževanja oziroma višjem strošku kapitala, do takrat ne bo spremembe.

Velikokrat se v strokovni javnosti poraja spoznanje, da strateški management področju finančnih tveganj daje prednost pred ostalimi pomembnimi področji. Gre tukaj za problem predhodnega znanja in izkušenj ali gre preprosto za nerazumevanje kompleksnosti okolja in dejavnikov v katerem delujejo poslovne organizacije, ki jih vodijo?

Ne bi se povsem strinjal s takšno ugotovitvijo. Številna podjetja dajejo prednost operativnim tveganjem, vsaj kvalitativno. Finančna tveganja so dejansko najlažja za oceno oziroma kvantifikacijo in s tega vidika morda najlažja za upravljanje v smislu evrskih vrednosti. Medtem ko so le korak stran ali dlje operativna tveganja, ki z malo vloženega truda lahko vodijo do boljših in globljih spoznanj, saj imajo običajno večji vpliv na poslovanje podjetja. Zato spodbujam premik od finančnih k operativnim tveganjem podjetja.



Skupaj s podjetjem Silver Bullet Risk sodelujete tudi pri razvoju istoimenske aplikacije za upravljanje varnostnih tveganj. Kvaliteta in uporabnost aplikacije je bila že v preteklosti prepoznana tudi v strokovnih okoljih. Katero dodano vrednost po vaši oceni prinaša v realno okolje ta aplikacija pri učinkovitejšem upravljanju s tveganji?

Največja dodana vrednost aplikacije Silver Bullet Risk (SBR) je, da je vse na enem mestu in napredna metodologija, ki omogoča upravljanje vseh tveganj z enakimi vatli, preko enake prizme in hkrati prenos znanja v podjetje. Takšen pristop nedvomno že srednjeročno in seveda dolgoročno pripomore k manjši kompleksnosti in večji transparentnosti upravljanja s tveganji. Glede na krize, ki prihajajo in pomen tveganj, ki ga bodo imela v krizah, bo takšen pristop postal nujen. S podjetjem Silver Bullet Risk bo ta prehod v smiselno upravljanje s tveganji z jasnimi cilji in rezultati bistveno manj boleč, hitrejši in cenejši.

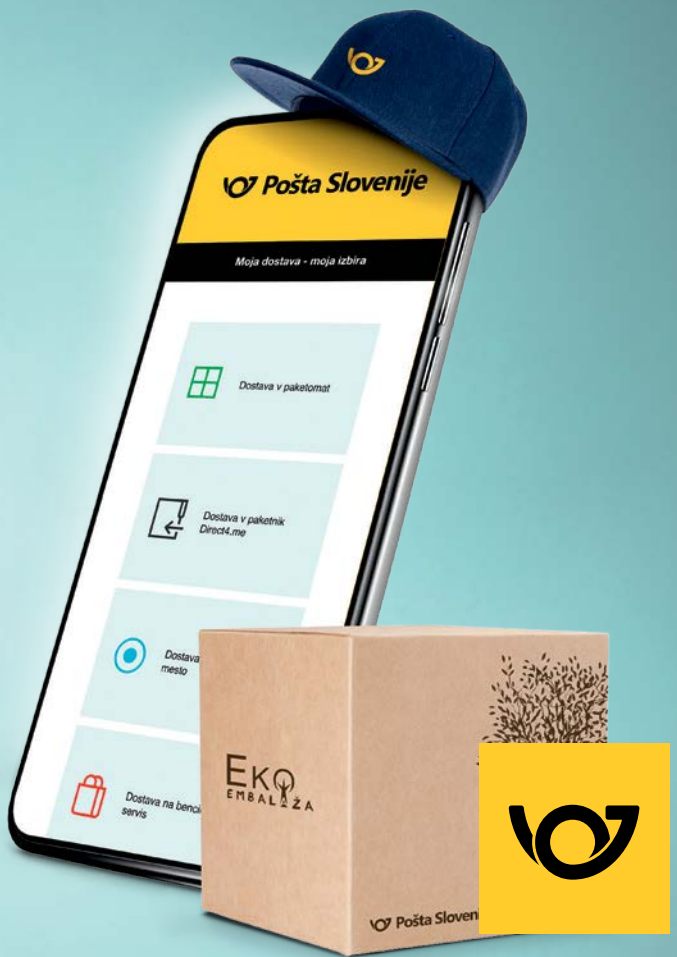
Lahko ta aplikacija in z njo povezani pristopi zagotovijo potrebne odgovore na vedno večjo kompleksnost tveganj globalnega poslovnega okolja in njihovo boljše upravljanje?

Sama aplikacija brez angažiranja zaposlenih seveda ne reši problema. Vsekakor pa ob ustreznemu namenu znatno olajša delo in poenoti pristop, ter že srednjeročno prinese rezultate v krajšem času, kot bi brez sistematičnega pristopa in programske podpore. Prav tako se z uporabo SBR in vgrajenih rešitev za upravljanje s tveganji zmanjša kompleksnost in izboljša razumevanje tveganj. Kot rečeno, brez sodelovanja zaposlenih ne gre, je pa pot s SBR lažja, bolj natančna, ter predvsem stroškovno in časovno bolj učinkovita. ■

Foto: osebni arhiv

Izberi dostavo po meri!

- 7 načinov dostave
- Več kot 1.100 prevzemnih mest
- Dostava tudi v roku 1 ure



POENOSTAVI SPLETNO NAKUPOVANJE Z IZBIRO DOSTAVE, KI TI NAJBOLJ USTREZA

Izberi enega od več kot 1.100 alternativnih prevzemnih mest in s spletnim orodjem "Sledenje pošiljk" spremljaj, kako blizu je tvoj paket.

Več nasvetov za enostavne spletne nakupe na www.posta.si/enostavna-dostava

KRAFT&WERK

Poskrbite za varnost na spletu pri vašem poslovanju.

Zavarovanje kibernetske zaščite za podjetja

Vse bo v redu.

triglav

triglav.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Boštjan Pavlin, mag., sekretar, Ministrstvo za obrambo

NEDAVNO KONČANA VAJA »LOCKED SHIELDS« JE POKAZALA POMEMBNE MOŽNOSTI ZA RAZVOJ KIBERNETSKE OBRAMBE

Mednarodna vaja »Locked Shields« je ena izmed dveh ključnih vadbenih aktivnostih v NATO na področju kibernetske obrambe. O izzivih na področju kibernetske obrambe in ravnokar končane mednarodne vaje smo se pogovarjali z g. Boštjanom Pavlinom, ki je bil nacionalni predstavnik za vajo kibernetske obrambe in strateškega odločanja Locked Shields v Sloveniji ter hkrati nosilec celotne izvedbe in pomočnik vodje vaje v 2022.

Ukrajinska kriza je ponovno pokazala, da je področje kibernetskih groženj postalo eden od pomembnih delov spektra s katerimi se morajo soočati države in njihova kritična infrastruktura. Kaj menite o tem?

Mednarodno varnostno okolje se spreminja in nova mednarodna varnostna arhitektura, bo morala zagotavljati globalno sodelovanje držav, tudi v kontekstu dolgoročnega naslavljanja njihovih skrbi glede varnostnih vprašanj. Zavedanje glede potrebe po t.i. 360 stopinjskem pristopu glede zaznavanja in odzivanja na grožnje je zelo prisotno v EU in Natu, ki v teh okoliščinah aktivno oblikujeta nove strateške smernice svojega delovanja - t.i. Strateški kompas in nov strateški koncept Nata. Pretekli konflikti npr. v Siriji, Libiji, med Azerbajdžanom in Armenijo, v Afriki in na Krimu so pokazali različne načine hibridnega delovanja ter uresničevanja interesov velikih sil. Slednje se seveda odkrito odraža tudi v vojni v Ukrajini, kjer lahko rečemo, da gre za hibridno vojno – torej poleg vojaških sredstev gre za uporabo različnih orodij, kot so dezinformacije, kibernetski napadi, vplivanje na javno mnenje, ekonomski

Vaja Locked Shields je vaja kibernetske obrambe in strateškega odločanja, in naj izpostavim, da smo po letošnji aktivnosti izredno zadovoljni. Uspeli smo namreč realizirati zelo ambiciozne cilje na področju kibernetske obrambe, razumevanje strateškega odločanja izhajajoč iz prekinitve delovanj, ki so posledica težiščno kibernetskih napadov in hkrati celotno aktivnost obravnavati kot upravljanje hibridne grožnje.



pritiski, psihološko in informacijsko bojevanje, obveščevalne aktivnosti, oviranje dostopa do dobrin in storitev ključnih za življenje, šibitev kredibilnosti politične oblasti in podobno. Zaščita kritične infrastrukture je pri tem bistvenega pomena. Če se osredotočim le na kibernetske grožnje je cilj jasen – v kombinaciji kibernetskih in vojaških delovanj prekiniti delovanje ukrajinskih oblasti, oboroženih sil, storitev in infrastrukture. Zaradi posebne občutljivosti posamezne infrastrukture, kot so npr. jedrske zmogljivosti ali sistem distribucije električne energije so ključni celoviti ukrepi na celotnem spektru – zaznavanja, preprečevanja, odzivanja, upravljanja kibernetskega incidenta ali napada ter ponovne vzpostavitve delovanja. Da je to mogoče, pa mora biti seveda vnaprej oblikovan trden sistem upravljanja kibernetske varnosti z zmogljivostmi, viri, opredeljenimi ukrepi ter rednim preverjanjem stanja in uvajanjem sprememb oz. prilagoditev ob ugotoviti pomanjkljivosti. In to velja na vseh področjih – v državni upravi, gospodarstvu, zdravstvu, šolstvu, energetiki, finančnemu sektorju itd.

Pred kratkim se je končala pomembna mednarodna vaja na področju kibernetske obrambe in strateškega odločanja »Locked Shields«, kjer ima tudi Slovenija vedno pomembnejšo vlogo. Ste ob prvih analizah z doseženim zadovoljni?

Naj uvodoma povem, da Nato kibernetsko obrambo vidi širše, ne le kot strogo zaščito lastnih omrežij in aktivnosti v kibernetskem prostoru v okviru skupne obrambe, ampak tudi kot podpora krepitvi nacionalnih zmogljivosti posameznih zaveznic oz. njihove odpornosti na kibernetske napade, ki mora biti celovita in ta odpornost seveda ne zadeva le obrambni resor. Zato je včasih pojem kibernetska obramba lahko zavajajoč. Omenjena celovitost se v primeru Nata odraža v podpori zaveznicam za izgradnjo zmogljivosti, izmenjavi informacij, zagotavljanju odzivnih timov, vključevanju kibernetike v vse domene Natovega delovanja in v posebnih oblikah sodelovanja z EU, OZN in OVSE. Na nacionalni ravni pa je z vidika odpornosti pomemben celovit sistem upravljanja kibernetske varnosti z vsemi relevantnimi deležniki v Sloveniji - nacionalnim organom, državnimi organi, akademsko sfero, gospodarstvom, državljani. Zadnje seveda ni pristojnost obrambnega resorja, je pa obrambni resor pomemben del v tem mozaiku.

Če se vrnem nazaj, Nato preko izobraževanja, usposabljanja in vaj prispeva k bolj odpornemu delovanju Nata kot celote, preko krepitve posameznih zaveznic. Skladno s tem so za Slovenijo zelo pomembne redne vaje iz več zornih kotov. V njih lahko preizkusimo svoje zmogljivosti in usposobljenost. Vaja Locked Shields je vaja kibernetske obrambe in strateškega odločanja, in naj izpostavim, da smo po letošnji aktivnosti izredno zadovoljni. Uspeli smo namreč realizirati zelo ambiciozne cilje na področju kibernetske obrambe, razumevanje strateškega odločanja izhajajoč iz prekinitve delovanj, ki so posledica težiščno kibernetskih napadov in hkrati celotno aktivnost obravnavati kot upravljanje hibridne grožnje.

Najbolj smo zadovoljni z izjemnim sodelovanjem ministrstva za obrambo z gospodarskimi družbami, ki imajo izredne strokovnjake na področju kibernetske varnosti. Tu nedvomno obstaja potencial za nadaljnje sodelovanje.

Na tem dogodku je bil dan velik poudarek sodelovanju med državnimi organi in gospodarskimi družbami, kar je zaradi omejenih kadrovskih resursov na kibernetskem področju v Sloveniji zelo pomembno. Kako bi ocenili sodelovanje in povezovanje teh deležnikov na vaji?

Kot sem že omenil je kibernetska varnost povezana z vsemi navedenimi subjekti – državnimi organi, gospodarskimi subjekti, kritično infrastrukturo, akademsko sfero in državljani. Pri

vaji Locked Shields sicer zaradi koncepta in scenarija niso bili vključeni vsi subjekti, ki bi jih lahko šteli v kibernetski ekosistem v Sloveniji, smo pa vključili največji možni del gospodarskih družb, samostojnih podjetnikov in drugih posameznikov, ki imajo ekspertna znanja, kakor je omogočal koncept vaje. Sodelovanje med deležniki je bilo odlično, kar je pokazatelj profesionalnosti in kompetentnosti vseh sodelujočih. Ministrstvo za obrambo se je trudilo zagotoviti vse pogoje za kvalitetno izvedbo. Naše sodelovanje z gospodarsko zbornico je pokazalo, da so rešitve vedno v povezovanju različnih znanj in kompetenc. Kot izjemen doprinos k sodelovanju pa je potrebno izpostaviti tudi gospoda Spagnola, ki je kot tehnični direktor vodil slovensko ekipo kibernetske obrambe.

Pri zagotavljanju kibernetske varnosti države in njenih različnih segmentov je pomembno razumeti, da potrebujemo učinkovito podporo in povezovanje v ekspertne skupine na strateški in operativni ravni, ki se lahko kot skupina bistveno bolj učinkovito odzivajo kot posamezniki.

Takšni dogodki poleg pridobivanja novih izkušenj in znanj omogočajo tudi določeno vrednotenje zmogljivosti in znanj strokovnjakov. Glede na to, da je metodološko vaja postavljena na način, da se delovanje vseh ekip tudi točkuje, je to verjetno pomembna informacija za vas, da znate oceniti kje smo v tem trenutku?

Določene vaje imajo natančno točkovanje delovnega procesa in doseženih rezultatov. Locked Shields je v svoji specifičnosti najzahtevnejša. Točkovanje vseh ekip predstavlja merjenje kompetenc hkrati pa tudi sposobnosti ali boljše uigranosti v sodelovanju celotne ekipe. Takšne vaje zelo realno pokažejo tudi to, da so poleg kibernetskega tehničnega znanja v takih situacijah izjemnega pomena poročanje, nadzor nad celotnim dogajanjem, pravni aspekt in načini komuniciranja. Vse to so področja, ki podajo celovitost upravljanja in kvalitetno odzivnost.

Na ministrstvu za obrambo se zavedamo internega manjka ekspertnih znanj, ki pa jih gospodarstvo ima. In če ocenjujem kje smo, je potrebno v prihodnje opraviti veliko dela in narediti vse, kar je v naši moči, da bomo vzdrževali visoko tehnološki razvoj in zadrževali znanja. Ker pa so sinergije povezovanja odlične sem prepričan, da smo na dobri poti. Tu je potrebno omeniti manjko normativnih dokumentov in predvsem uvajanje dobrih praks iz tujine, ključno je tudi izgrajevanje zmogljivosti v obliki javno zasebnih partnerstev.

Veliko je razprav v katero smer bi morali v Sloveniji razvijati kibernetske zmogljivosti. Kakšna je vaša ocena glede na vaše izkušnje, kompetence in analize, ki jih dobite skozi tovrstne mednarodne vaje?

Odzivanje na kibernetske grožnje zaradi horizontalne narave te grožnje zahteva celovit pristop. Rad bi pa izpostavil dejstvo, da bomo lahko celovito kibernetsko varnost v Sloveniji zagotavljali le z institucionalnim / sistemskim sodelovanjem med državnimi organi in gospodarsko sfero, seveda pa je treba vključevati tudi akademsko in raziskovalno sfero ter z vidika ozaveščanja tudi državljane. Zaradi velikosti države, resursov, ki so na voljo, specifičnih znanj in zagotavljanja ustreznih pogojev za razvoj kadra lahko le povezovanje zagotovi najvišjo raven varnosti. Gospodarski sektor je ključni deležnik v kibernetskem prostoru in nosilec tehnoloških inovacij ter specifičnega znanja. Zato mora država na tem področju iskati sinergije in povezovanje. Nedvomno pa je obojestranski interes izmenjava informacij glede kibernetskih groženj, krepitev odpornosti omrežij in in-

Odzivanje na kibernetske grožnje zaradi horizontalne narave te grožnje zahteva celovit pristop. Rad bi pa izpostavil dejstvo, da bomo lahko celovito kibernetsko varnost v Sloveniji zagotavljali le z institucionalnim / sistemskim sodelovanjem med državnimi organi in gospodarsko sfero, seveda pa je treba vključevati tudi akademsko in raziskovalno sfero ter z vidika ozaveščanja tudi državljane.

formacijskih sistemov ter učinkovito preprečevanje, odzivanje in okrevanje po morebitnem kibernetskem napadu. Slednje je še toliko bolj pomembno spričo dejstva, da bo na področju kibernetske varnosti prišlo do širših zakonskih sprememb na ravni EU in s tem Slovenije, ki se bodo nanašale na finančne institucije, kritično infrastrukturo ter različne gospodarske subjekte in subjekte, ki zagotavljajo različne storitve. Velik premik in prilagoditve za subjekte z vidika zaščite podatkov je v tem oziru že predstavljala Splošna uredba EU o varstvu podatkov (t.i. GDPR), podobno lahko tako pričakujemo s paketom napovedane EU zakonodaje. Pri tem pa ne smemo, z vidika razvoja področja kibernetske varnosti v Sloveniji, prezreti tudi velikih možnosti povezovanja v mednarodnem okolju, kjer obstaja mreža podobnih kompetenčnih skupnosti ali pa v okviru mednarodnih organizacij. Vse več je tudi poskusov harmonizacije oz. standardizacije določenih segmentov kibernetske varnosti bodisi pri produktih, storitvah ali pri upravljanju tako z namenom učinkovitejšega zagotavljanja varnosti, kot z vidika zagotavljanja varnega delovanja enotnega trga EU. Torej razvojnih možnosti je ogromno, ključno v prihodnje pa bo še močnejše sodelovanje in povezovanje deležnikov v Sloveniji.

Kaj po vaši oceni lahko še izboljšamo na naslednjih mednarodnih vajah s področja kibernetske obrambe, ki nam bo zagotavljalo, da bomo v primeru realnih kibernetskih napadov bolje pripravljeni na učinkovito odzivanje?

Da bomo naredili korak naprej moramo naprej določiti skupne cilje. V tem trenutku se cilji oblikujejo ločeno v posameznih državnih organih, ministrstvih in podobno, drugi del pa v gospodarstvu. Potreben je premislek o skupnih ciljih, kjer bomo našli dodano vrednost v povezovanju vseh kvalitet in zmogljivosti na strateški in operativni ravni. Zagotovo mora biti eden prvih skupnih ciljev zagotovitev kvalitetnega izobraževanja kibernetske varnosti na fakultetah v Sloveniji. Posledično morajo kadri imeti pogoje in ustvarjati v slovenskem prostoru. Iskati je potrebno sinergije visoko tehnoloških podjetij z nacionalno varnostnimi subjekti in akademsko sfero.

Hkrati pa je tudi pri kibernetskih napadih in grožnjah ključen dejavnik varnostne percepcije posameznika in družbe. Močno upam, da bo družba dvignila odnos do varnosti na vseh področjih, tudi na področju kibernetske varnosti. Gre namreč za področje, kjer lahko škoda, ko se zgodi napad, zelo presega vlaganje v preventivne aktivnosti in seveda onemogoči delovanje ključnih družbenih podsistemov. ■

Dobrodošli v novi dimenziji

MOBOTIX

BeyondHumanVision

Nove Kamere



D71 Q71

Nove aplikacije

Irisity IRIS Core AI - Detekcija Vdora

Vaxtor LPR - Prepoznava tablic na dveh objektivih.

Vaxtor AIN – Identifikacija letal

In še več

tend

ORG. Tend d.o.o
Kraljeviča Marka ulica 19
SI-2000 Maribor

MOBOTIX
Authorized Distributor 2022

E: mobotix@tend.si W: www.tend.si

smartis
PAMETNI INFORMACIJSKI SISTEMI

Kako do varne infrastrukture za digitalno preobrazbo

Preizkušene varnostne rešitve Smartis za kritične infrastrukturne ter industrijske sisteme tlakujejo pot vašemu napredku in poslovni uspešnosti.

Vsi si želimo učinkovitih in kakovostnih storitev, ki temeljijo na informacijah iz kritičnih infrastrukturnih in industrijskih sistemov. Vendar so ti sistemi zaradi izpostavljenosti kibernetskim varnostnim tveganjem **neprodušno zaprti.** V resnici pa ni več razlogov za to! **Podatke iz vaših kritičnih sistemov** na primer brez slabe vesti uporabite v pametnih rešitvah za odločanje in poročanje, za upravljanje in vzdrževanje sistemov, obvladovanje človeških virov, za obračunavanje storitev in obveščanje deležnikov. **Z inteligentno zaščito in varovanjem** komunikacijskega omrežja za dostop do vaših produkcijskih sistemov (OT – Operational Technologies) in senzorjev (IoT - Internet of Things) vzpostavite temelj **digitalne transformacije vaše osnovne dejavnosti** – v skladu s standardi industrije **4.0 in 5.0.**

Poskenirajte kodo za več informacij o zaščiti kritične infrastrukture!

Smartis d.o.o.
Ameriška ulica 8
1000 Ljubljana

info@smartis.si
01 601 0650
www.smartis.si

Avtor: doc. dr. Brane Bertoncelj / Slovensko združenje za korporativno varnost



VARNOST ZAPOSLENIH NA SLUŽBENI POTI

Zaskrbljenost za varnost zaposlenih na službeni poti je prednostna naloga uspešnih organizacij in dolžnost skrbnosti poslovanja. Mnogi komercialni vodje bodo brez dvoma potrdili: »Službena srečanja v živo so ključna za uspeh posla«.

Uvod

Kljub porastu števila videokonferenc po letu 2020, ta v celoti niso nadomestila pristnih poslovnih srečanj. Za mnoge organizacije, ki delujejo na mednarodni ravni, so službena potovanja neizogibna in potrebna za širitev na nove trge ali nove stranke. Sedanja ekonomska vojna s sankcijami vpliva tudi na svetovno ekonomijo, cene surovin in na dobavne verige. To pa zahteva tudi iskanje novih poslovnih partnerjev in posledično tudi večje število službenih potovanj. Svet postaja vse bolj globaliziran in povezan, narašča pa tudi število držav, v katere potniki potujejo, kar posledično povečuje število tveganj, s katerimi se bodo lahko srečali.

Mednarodna organizacija za standardizacijo (ISO) je septembra 2021 izdala ISO za obvladovanje potovalnih tveganj (Travel risk management, ISO 31030:2021). Ta standard je koristen za določitev številnih vidikov organiziranja potovanj, ki jih mora organizacija smiselno upoštevati. Trenutno je, bolj kot kdaj koli prej, potrebno zmanjšati zaznana potovalna tveganja za organizacijo in zaposlene, ki morajo v teh razmerah znova potovati, hkrati pa se počutiti varne in vedeti, da obstajajo ukrepi in postopki za zagotavljanje podpore, če bo to potrebno.

ISO standard 31030:2021

Standard se nanaša na »novo normalno« razmišljanje o potovanjih skozi spekter tradicionalnih in novih potovalnih tveganj. Spodbuja obravnavanje potovalnih tveganj z ustreznimi viri in upravlja aktivnosti. Prepoznane so naslednje prednosti:

- zaščita zaposlenih, večja informacijska varnost, boljša zaščita intelektualne lastnine in drugo premoženje organizacije;
- zmanjša finančna in pravna tveganja;
- omogoča poslovanje tudi na tveganih lokacijah;
- poveča organizacijsko kulturo in ugled organizacije;
- izboljša zaupanje zaposlenih na področju varnosti in zdravja pri delu;
- poveča odpornost organizacije za neprekinjeno poslovanje.

Politika potovanj

Vodstvo organizacije mora vzpostaviti politiko potovanj, ki določa splošna načela, namen in usmeritev za doseganje ciljev. Le ta mora biti primerna za potrebe in sredstva organizacije. Postati mora sestavni del politike upravljanja organizacije. Poleg tega mora biti usklajena z upravljanjem tveganj organizacije, neprekinjenim poslovanjem, potovalnimi naročili in trajnostno politiko. Sklicevati se mora na ustrezno zakonodajo, standarde, politike in kodekse ravnanja. V okviru tega je potrebno tudi določiti načela za postopek ocene tveganja, kar pomeni, da upošteva (ali določi) merila tveganja organizacije, opredeljuje vloge in odgovornosti, ter odgovornosti vseh deležnikov, vključno z njihovo usposobljenostjo. Določati mora politiko organizacije glede časa (izven delovnega časa ali osebnega dopusta), povezano s katerim koli potovanjem in upoštevati politiko več potnikov in spremljevalcev, kadar je to potrebno.

Cilj usposabljanja za varnost potovanj v organizaciji je ustrezno pripraviti potnike na izogibanje, prepoznavanje in ublažitev nevarnosti in groženj na poslovnem potovanju. Če potnikom zagotovimo potrebno znanje za soočenje z morebitnimi izrednimi dogodki, se lahko organizacija počuti bolj samozavestno pri pošiljanju zaposlenih na službene poti.

Tveganja

Organizacija mora izdelati pisni načrt odzivanja na izredne dogodke na službenih potovanjih, ki določa organe in odgovornosti ključnih zaposlenih, vključno z ekipo za upravljanje izrednih dogodkov. Ta ekipa mora biti predhodno ustanovljena, z ustreznimi viri za obvladovanje razmer.

Analiza tveganja naj se nanaša na:
- tveganje osebne poškodbe in bolezni (vključno povezano z delom), napad, pridržanje, ugrabitev, krajo, rop, smrt;
- pravno tveganje: kazenski pregon ali civilnopravne posledice ali oboje;
- poslovno tveganje: tveganje kontinuitete za upravljanje izrednih dogodkov in/ali ponovno normalno poslovanje;
- tveganje ugleda: neustrezen odziv na izredne dogodke ali neupoštevanje potovalne politike lahko povzroči finančne in pravne posledice ter izgubo (zmanjšanje) ugleda;
- finančno tveganje: neuspešna izvedba poslovne naloge, prekinitev potovanja, obdavčitev, status vizumskega delovnega dovoljenja, civilni zahtevki, stroški zavarovanja, stroški evakuacije, zdravstvena repatriacija;
- tveganje za podatke, intelektualno lastnino in informacijska sredstva: kršitev zaupnosti in dosegljivosti podatkov, vdor v omrežje, sistem ali izguba sredstev, vohunjenje;
- tveganje za produktivnost/učinkovitost potovanja: neuspeh potovanja, zamude, neuspeh korporativnega dogodka.

Analiza tveganja mora upoštevati dejavnike, kot so:
- verjetnost dogodkov in posledic;
- narava in velikost posledic;
- zapletenost in povezljivost;
- dejavniki, povezani s časom in nestanovitnostjo;
- učinkovitost obstoječih kontrol;
- razponi občutljivosti in zaupanja.

Priporočila za operativne aktivnosti

Potovalna politika: Pri organiziranju službenih potovanj je treba upoštevati veliko dejavnikov, zato je smiselno izdelati poslovno politiko potovanj. Določanje vseh ustreznih ukrepov in postopkov bo pomagalo zaščititi potnike in zmanjšati potne stroške organizacije.

Opredelitev ciljev potovanj: Ti vključujejo, poleg doseganja poslovnih ciljev, standarde zagotavljanja varnosti in udobja potnikov ter pomoč pri odločanju o potovanju. Od potnikov se pričakuje, da upoštevajo varnostne smernice, vključene v potovalno politiko, da zagotovijo lastno varnost, v skladu z lokalnimi zakoni.

Določanje standardov rezervacij potovanj: Imenovati je potrebno zaposlenega, ki bo vodil postopke rezervacij za organizacijo. Razmisliti je potrebno o najpogostejših destinacijah za potnike in najboljši način, da ta pride do njih ter ali obstajajo posebne potrebe ali pomisleki, povezani z dejavnostmi organizacije.

Dajte potnikom možnosti: Vsak ima rad izbiro, zato potnikom ponudite izbiro hotelov ali letalskih družb. Stroške lahko znižate tako, da omejite hotelsko oceno zvezdic ali razred letalske karte.

Določite smernice za vse vidike potovanj: Potovalna politika mora biti vseobsegajoča, tako da ne pušča prostora za dvome; to vključuje vse, od pravil letalskih rezervacij do pravilnika o povračilih stroškov potovanj in dodatnih stroškov do sprejemanja daril.

Zagotoviti je potrebno, da potniki vedo, kakšna je potovalna politika: Vsi ustrezni dokumenti morajo biti na voljo zaposlenim prek intraneta ali potovalne platforme. Politiko je treba jasno sporočiti vsem, vključno z vodstvom, da jo lahko uveljavlja.

Vodje, odgovorni za usposabljanje, bi morali:
- zagotoviti, da bodo vsi potniki prejeli potrebno usposabljanje, znanje in izkušnje;
- njihova delovna dodelitev mora biti varna;
- oceniti, ali potniki razumejo zagotovljene informacije, navodila in usposabljanje zaradi kakršnih koli težav;
- zagotovite, da se povratne informacije usposabljanja nanašajo tudi na izvajalca usposabljanja kot del ocene.

Zaključek

Potovalna tveganja moramo obravnavati v okviru ključnih sprememb paradigme, konceptualizacije in novejšega definiranja pojma tveganja. Ta ni več samo »možnost ali verjetnost izgube«, ampak tudi »učinek negotovosti na cilje«. To pomeni, da se beseda »tveganje« nanaša na pozitivne posledice negotovosti, pa tudi negativne.

Cilj usposabljanja za varnost potovanj v organizaciji je ustrezno pripraviti potnike na izogibanje, prepoznavanje in ublažitev nevarnosti in groženj na poslovnem potovanju. Če potnikom zagotovimo potrebno znanje za soočenje z morebitnimi izrednimi dogodki, se lahko organizacija počuti bolj samozavestno pri pošiljanju zaposlenih na službene poti. Žal pa so tudi primeri, ko potnik zaradi spleta izrednih dogodkov ostane sam (zlasti v tujini), brez sredstev, kontaktov ipd. in mora samoiniciativno »po zdravi pameti« odreagirati za uspešno realizacijo ciljev potovanja.

Ta članek je treba razumeti kot pripomoček in vzpodbudo za sistematični pristop k upravljanju potovalnih tveganj za vodje korporativne varnosti, vodje potovanj organizacij, vodje upravljanja tveganj, pooblaščence za skladnost in vodje kadrov.

Za lastno varnost na potovanju pa je v prvi vrsti odgovoren potnik sam. Ostanite varni in potujte varno. ■


Telecom security
for a connected world
As the world goes digital, mobile networks are becoming the open platform of innovation serving business, society and mission critical use cases. 5G gives communication service providers the ability to serve these use cases with secure and resilient connectivity, connecting everything from enterprises, smart factories and critical public safety infrastructures.
www.ericsson.com/en/security
ERICSSON



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.