Korporativna varnost

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

Letnik 2023, maj • št. 32

Slovensko združenje korporativne varnosti vključujoča platforma sodelovanja javno-zasebnega partnerstva

Strateški varnostni izzivi Republike Slovenije

Dr. Andrej Benedejčič, državni sekretar za nacionalno in mednarodno varnost

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 2023

Izvod revije je brezplačen

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

ISSN 2232-6170

Pred nami se nahaja številka revije Korporativna varnost, ki jo vsako leto posebej posvetimo najpomembnejšemu letnemu dogodku Dnevi korporativne varnosti. Glede na potrebo po učinkovitem odzivanju na prihajajoče krizne situacije in v povezavi z zagotavljanjem 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 v dogodke strelskih pohodov, ki so se začeli dogajati v naši neposredni bližini. Posebej pa velja poudariti tudi potrebo po stabilnosti strokovnega okolja v organizacijah, ki je nujna za nemoteno in varno delovanje naših organizacijskih okolij. V tem okviru še vedno nekoliko pogrešamo zmožnost političnih akterjev, da presežejo različnost pogledov in pristopov pri uveljavljanju na področju vitalnih interesov Republike Slovenije. Tukaj je potrebno posebej izpostaviti pomen kontinuiranosti 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 veliko 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 o pomenu 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. Kot že rečeno je k temu deloma pripomoglo tudi obdobje, 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, ki izhaja ob najpomembnejšem letnem dogodku na področju korporativne varnosti, 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
mag. Vesna Prodnik, članica uprave,
Telekom Slovenije d.d.

DIGITALIZACIJA IN HITRO SPREMINJAJOČE GLOBALNE RAZMERE POMEMBEN IZZIV IN PRILOŽNOST ZA TELEKOM SLOVENIJE

KOLUMNA
izr. prof. dr. Denis Čaleta, Institut za
korporativne varnostne študije

JE ČLOVEK NAJŠIBKEJŠI ALI NAJMOČNEJŠI DEL VARNOSTNEGA SISTEMA?

INTERVJU
dr. Dragan Kovačić, dr. med.,
direktor Splošne bolnišnice Celje

RAZVOJ POMEMBNIH ZDRAVSTVENIH ORGANIZACIJ NI MOGOČ BREZ USTREZNEGA ZAGOTAVLJANJA VARNOSTI

STRATEGIJA DIGITALNA SLOVENIJA 2030

Po izteku prejšnje (Digitalna Slovenija 2020) smo novo strategijo digitalne preobrazbe pričakovali v letu 2020. Kljub poskusom v prejšnji in še eni vladi pred tem, predlog nikoli ni ugledal luč sveta, zato smo res veseli in ponosni, da lahko rečemo da je 23. marca letos Vlada Republike Slovenije sprejela strategijo Digitalna Slovenija 2030, ki je krovni strateški dokument Vlade Republike Slovenije na področju digitalne preobrazbe.

VESOLJSKE INDUSTRIJE IN PRILOŽNOSTI ZA SLOVENSKE ORGANIZACIJE

V prispevku želimo podrobneje predstaviti korake, ki jih Republika Slovenija in preko tega tudi slovenske organizacije, izvajajo na področju sektorja vesoljske industrije. Prehojena pot predstavlja odlično odskočno desko za razširitev sodelovanja in izvajanja smelejših korakov na tem zahtevnem in visoko konkurenčnem področju.

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

INTERVJU
dr. Andrej Benedejčič, svetovalec predsednika Vlade RS za nacionalno in mednarodno varnost

STRATEŠKI VARNOSTNI IZZIVI REPUBLIKE SLOVENIJE

Dr. Andrej Benedejčič je v pogovoru z nami analiziral stanje in izzive na področju zagotavljanja nacionalne in mednarodne varnosti. V pogovoru je med drugim posebno težišče namenil varnostnim izzivom pred katerimi se nahaja nacionalna varnost Republike Slovenije.

Na začetku pogovora se nikakor ne moremo izogniti Ukrajinski krizi, ki je močno zaznamovala evropsko in tudi svetovno varnostno okolje. Kaj bi z vašega zornega kota izpostavili kot ključne varnostne izzive pred katerimi se je znašla EU?

Ukrajinska kriza brez dvoma predstavlja točko dokončnega preloma za evropsko varnostno arhitekturo. Ta je bila sicer pod pritiskom že dlje časa. Če govorimo o treh stebrih nadzora nad oborožitvijo v Evropi, potem se velja spomniti, da je Rusija že leta 2007 uvedla moratorij na izvajanje Pogodbe o konvencionalnih silah v Evropi, od leta 2011 naprej blokira poskuse za posodobitev Dunajskega dokumenta za krepitev varnosti in zaupanja, leta 2021 pa je izstopila iz Pogodbe o odprtih zračnih prostorih.

Za Evropsko unijo, kot tudi zvezo Nato – navsezadnje se članstvo obeh integracij v veliki meri prekriva – to pomeni, da sta soočeni z vrnitvijo konvencionalnega vojskovanja v Evropi, ki naj bi sicer že pripadalo preteklosti. Nova realnost zato zahteva prilagoditev prejšnjega pristopa, ki je bil predvsem usmerjen v izgradnjo zmogljivosti za ekspedicijsko vojskovanje. Tudi zato so se v zadnjih letih nekatere evropske države celo odpovedale svojim oklepnim silam. Zdaj pa je potrebno te kapacitete obnoviti, obenem pa tudi zagotoviti ustrezne industrijske zmogljivosti za proizvodnjo ne le opreme, temveč tudi streliva, še posebej težkega artilerijskega. Poraba slednjega v Ukrajini je namreč astronomska.

Vse to, seveda, zahteva usklajen pristop in še več evroatlantskega sodelovanja med EU in Natom. Prav tako je pomembno, da se dodatne zmogljivosti v čim večji meri zagotovi z vlaganjem v evropsko industrijsko bazo. Zato bi želel posebej izpostaviti nedavni obisk evropskega komisarja za notranji trg Thierryja Bretona pri nas. Z gostiteljem, predsednikom vlade dr. Robertom Golobom, se je namreč strinjal, da je v primeru Slovenije obrambne izdatke smiselno povečevati tudi skozi podporo domačim visokotehnološkim podjetjem, še posebej na področju zračne obrambe, nenazadnje tudi zato, ker je večina teh izdelkov in tehnologij dvojno uporabna tudi v drugih panogah.

Republika Slovenija je jasno moralno podprla Ukrajino pri njenih naporih za obrambo države in bila tudi ena izmed prvih držav, ki je zelo jasno artikulirala potrebo po skupnem Evropskem pristopu obsodbe Ruske agresije. Z določene časovne perspektive, več kot leto trajajočega konflikta, je bil to vsekakor pogumen in pravi pristop. Kakšna je vaša strokovna ocena?

Ruka invazija na Ukrajino predstavlja grobo kršitev določb mednarodnega prava, med drugim tudi načel Ustanovne listine OZN. Kot takšna je preprosto nesprejemljiva za Sloveni-

> Gre predvsem za vprašanje dviga odpornosti na ravni celotne družbe, nekako po vzoru nekdanjega pristopa »Nič nas ne sme presenetiti«. Zato je tako pomembno, da se zavest o tem, da živimo v drugačnem svetu od tistega, ki smo ga pričakovali po koncu hladne vojne, čim prej ponotranji.

*avtor je član Slovenskega združenja korporativne varnosti

jo, ki varnost vidi predvsem v svetovni ureditvi, ki temelji na moči pravil in ne na pravu močnejšega. Vsekakor pa dodaten šok in razočaranje predstavlja ruska odločitev, da svojo agresijo stopnjuje z napadi na civilne objekte. Vlada je zato že novembra lani ostro obsodila sistematično uničevanje kritične infrastrukture, še posebej energetske, in pozvala rusko stran naj s takšnim delovanjem nemudoma preneha.

Ali menite, da je Slovenija in njen nacionalno-varnostni sistem ustrezno organiziran in dovolj robusten za učinkovito soočanje z vedno novimi grožnjami, ki jih prinaša dinamično varnostno okolje?

Slovenski nacionalno-varnostni sistem ni od včeraj, temveč se je razvijal skozi desetletja. V začetku devetdesetih se je izkazal za dovolj robustnega, da je v desetdnevni vojni porazil takrat tretjo najmočnejšo armado v Evropi. Danes se na nove grožnje odziva v okviru EU in Nata, pač v skladu z referendumsko odločitvijo Slovenk in Slovencev, da svoje varnosti ne zagotavljajo le na nacionalni ravni, temveč tudi v okviru širših sistemov kolektivne varnosti. V praksi to med drugim pomeni, da, kot članica Nata od leta 2016, prepoznavamo kibernetski prostor kot operativno domeno, od leta 2019 pa tudi vesolje.

Nacionalno varnostni sistem je sestavljen iz celega spektra procesov in subjektov. Kaj bi se po vašem mnenju dalo še dodatno izboljšati na področju koordinacije tega sistema, da bi dosegli večjo učinkovitost?

Dejansko gre pri nacionalno varnostnem sistemu za kompleksno in soodvisno strukturo. Tudi zato jo je treba redno preverjati, med drugim v okviru vaj, tako na nacionalnem kot tudi mednarodnem nivoju. Ena takšnih je potekala pred kratkim. Gre za Nato vajo kriznega upravljanja, znano pod kratico CMX, ki se je v prvi polovici marca odvila hkrati v vseh članicah zavezništva. Poleg skupnega je vsebovala tudi ločene nacionalne scenarije. Ena od ugotovitev na naši strani je potreba po tem, da se zaščiten komunikacijsko informacijski sistem, ki ga imamo v Sloveniji, razširi na vse resorje in ne ostane omejen samo na državotvorna ministrstva in službe.

Kako vidite nadaljnji razvoj nacionalno-varnostnega sistema v teh zahtevnih gospodarskih in družbenih okoliščinah?

Tako, kot smo na vojaškem področju soočeni z nujo po ponovni vzpostavitvi zmogljivosti in praks, povezanih s kolektivnim odvračanjem in obrambo, tako se tudi na širši nacionalno-varnostni ravni ukvarjamo z obnovo institucionalnega spomina. Gre predvsem za vprašanje dviga odpornosti na ravni celotne družbe, nekako po vzoru nekdanjega pristopa »Nič nas ne sme presenetiti«. Zato je tako pomembno, da se zavest o tem, da živimo v drugačnem svetu od tistega, ki smo ga pričakovali po koncu hladne vojne, čim prej ponotranji. Soočeni smo namreč s konvencionalno vojno velikih razsežnosti v Evropi in strateškim rivalstvom na globalni ravni. V zvezi s tem bi še posebej izpostavil nevarnost, ki jo za nacionalno kohezivnost in medzavezniško solidarnost lahko predstavljajo dezinformacije.

Svetovalec predsednika vlade za nacionalno varnost ima v večini držav izredno pomembno vlogo pri usklajevanju in koordinaciji aktivnosti na področju nacionalne varnosti. Kakšne so vaše dosedanje izkušnje o vlogi, ki jo trenutno opravljate pri predsedniku Vlade Republike Slovenije?

Vloga svetovalca za nacionalno varnost se je v našem sistemu z leti ne le uveljavila, temveč tudi sistemsko dorekla. Pri tem mislim predvsem na okvir, ki ga ponuja Svet za nacionalno varnost. Njegov sekretar je namreč ravno svetovalec za nacionalno varnost, ki je obenem vodja sekretariata Sveta za nacionalno varnost. V tej vlogi tudi vodi srečanja operativne skupine sekretariata, ki v skladu z veljavnim odlokom vključuje direktorja Sove, generalnega direktorja Policije, državnega sekretarja zunanjega ministrstva, generalnega direktorja Obveščevalno varnostne službe obrambnega ministrstva in direktorja Urada za informacijsko varnost. Skupina se sestaja tedensko, kar pomeni, da že sama po sebi zagotavlja usklajenost in koordinacijo aktivnosti na področju nacionalne varnosti. Sicer pa bi izpostavil tudi dobro izkušnjo z Nacionalnim centrom za krizno upravljanje, ki mi pri mojem delu nudi vso potrebno administrativno in tehnično pomoč.

Kritična infrastruktura je nujna za nemoteno delovanje družbe. Kako na ravni nacionalne-varnosti organizirati sistem obvladovanja tveganj, da bo zagotavljal ustrezno varnost za nemoteno delovanje te infrastrukture?

Ruska agresija na Ukrajino je jasno izpostavila pomen kritične infrastrukture, kot tudi energetske varnosti kot takšne. Naj zato poudarim, da se je glede tega zelo vidno in zelo zgodaj angažirala tudi slovenska stran. Že junija lani je namreč predsednik vlade dr. Golob na Evropskem svetu dosegel, da se je v sklepe zapisala zaveza, da bodo države članice tesneje sodelovale na področju energetike pred prihajajočo zimo. Na podlagi slovenskih predlogov je bila tako med drugim sprejeta Uredba Sveta Evropske unije o nujnem posredovanju za zajezitev volatilnosti cen energentov.

Sicer pa smo se na možen vpliv ruske agresije na nestanovitnost energetskih trgov pripravili tudi na nacionalni ravni. Kot veste, bi takratne motnje v oskrbi s plinom, zmanjšana razpoložljivost nekaterih elektrarn ter posledični učinki na cene energentov lahko pomenili težave pri oskrbi z elektriko. Zato je bila v skladu z Zakonom o kritični infrastrukturi jeseni sklicana vrsta usklajevalnih sestankov z vsemi deležniki s ciljem zagotovitve neprekinjenega delovanja kritične infrastrukture in njene segmentacije glede na morebitne redukcije. Vse te aktivnosti so potekale ob vednosti sekretariata Sveta za nacionalno varnost.

Vloga svetovalca za nacionalno varnost se je v našem sistemu z leti ne le uveljavila, temveč tudi sistemsko dorekla.

Sistem za odzivanje na kibernetske grožnje imamo torej vzpostavljen. Seveda pa imamo v današnjem svetu na tem področju opravka z vse bolj sofisticiranimi in sposobnimi akterji. Zato je tem bolj pomembno sodelovanje z našimi partnerji v okviru EU in Nata.

Kateri so po vašem mnenju tisti koraki, ki jih lahko storijo manjše države, kot je npr. Slovenija, za učinkovito zavarovanje pred temi kompleksnimi grožnjami? Primer napada na MZZ je sam po sebi dovolj zgovoren, da nismo varna oaza sredi razburkanega oceana.

Področje varnosti omrežij in informacijskih sistemov pri nas ureja Zakon o informacijski varnosti. Gre za prenos EU direktive s področja informacijske varnosti, tako imenovane direktive NIS oz. Network and Information Security iz leta 2016. Zakon med drugim določa, da morajo izvajalci bistvenih storitev priglasiti incidente s pomembnim vplivom na neprekinjeno izvajanje njihovih dejavnosti. Pristojni nacionalni organ, ki je Urad Vlade Republike Slovenije za informacijsko varnost, pa o incidentih, ki bi lahko imeli večji medpodročni vpliv ali vplivali na varnost države, nemudoma obvesti sekretariat Sveta za nacionalno varnost, Policijo in Nacionalni center za krizno upravljanje.

Sistem za odzivanje na kibernetske grožnje imamo torej vzpostavljen. Seveda pa imamo v današnjem svetu na tem področju opravka z vse bolj sofisticiranimi in sposobnimi akterji. Zato je tem bolj pomembno sodelovanje z našimi partnerji v okviru EU in Nata. Napad, ki ga omenjate, zato po eni strani predstavlja razlog za skrb, po drugi pa priča o tem, da praksa medsebojnega obveščanja in opozarjanja deluje. To pa ne pomeni, da se zadev ne bi dalo še izboljšati. Pravzaprav je bila zaradi vse večjih izzivov na področju kibernetske varnosti na ravni EU že sprejeta nova direktiva, znana kot NIS 2, ki določa strožje nadzorne ukrepe nad zavezanimi subjekti. V nacionalno zakonodajo jo je treba prenesti do oktobra 2024.

Sicer pa bi rad opozoril, da od lanske jeseni pri nas beležimo občuten porast t. i. phishing napadov. Te poskušamo omejevati s tehničnimi ukrepi in rednim opozarjanjem uporabnikov prek medijev in drugih kanalov. V zvezi s tem sta še posebej pomembna programa ozaveščanja na področju kibernetske varnosti *Varni na internetu* in *Center za varnejši internet*. Prvega izvaja Nacionalni odzivni center za kibernetsko varnost oz. SI-CERT, namenjen pa je splošni javnosti ter mikro, majhnim in srednje velikim podjetjem. Drugega pa izvaja konzorcij pod vodstvom Fakultete za družbene vede Univerze v Ljubljani in je namenjen ozaveščanju otrok, mladostnikov, njihovih staršev in učiteljev. Oba programa financira Urad Vlade za informacijsko varnost.

Slovenske organizacije so zelo aktivne na različnih EU projektih s področja kritične infrastrukture in kibernetske varnosti. Menite, da lahko operativno raziskovalna spoznanja pomagajo pri iskanju novih rešitev za izboljšanje normativnih in koordinativnih ukrepov v Republiki Sloveniji? Postavlja se glavno vprašanje, kako pravilno usmeriti in integrirati vso pridobljeno znanje v različne dele nacionalno-varnostnega sistema?

Ne le, da sem prepričan v pomen takšnih raziskav, temveč tudi vem, da so uporabne za naš nacionalno varnostni sistem. Naj v zvezi s tem izpostavim dve.

Prva je raziskovalna monografija E-armagedon, ki je izšla lani pri Založbi FDV in se ukvarja z družbenimi posledicami večjih izpadov električne energije. Moram reči, da se redko zgodi, da avtorji začutijo duh časa tako dobro, kot v tem primeru, in obenem s teoretične perspektive tako pronicljivo osmislijo in osvetlijo praktične izzive, tudi na nacionalni ravni. Do same predstavitve knjige pa je prišlo ravno še pred novembrskim

zasedanjem Sveta za nacionalno varnost, ki je bil posvečen obravnavi nacionalno varnostnih implikacij nadaljnje ruske agresije proti Ukrajini, pri čemer tudi s perspektive energetske varnosti.

Druga takšna raziskava pa je identifikacija in pregled vseh metodologij za izdelavo ocen ogroženosti, ki ga izvaja Fakulteta za varnostne vede Univerze v Mariboru. Sekretariat Sveta za nacionalno varnost se je že decembra lani seznanil z modelom za ocenjevanje varnostnih razmer in ogroženosti v Republiki Sloveniji ter predlogi za izboljšave, ki ga je pripravila raziskovalna projektna skupina. V zvezi s tem je bil tudi sprejet sklep, da se v prihodnje opravi razpravo o vseh obstoječih metodologijah za izdelavo ocen ogroženosti. Gre torej za raziskovalna spoznanja, ki so vsekakor uporabna za naš nacionalno varnosti sistem.

Strokovna združenja imajo pomembno mesto pri zagotavljanju uveljavljanja posamezne stroke. Slovensko združenje korporativne varnosti je tukaj izredno aktivno, kar s svojo vedno večjo včlanitvijo prepoznavajo tudi ključne državne institucije. Menite, da je ta strokovno-povezovalna pot lahko ena od možnosti tesnejšega sodelovanja vseh deležnikov pri iskanju učinkovitih rešitev za kompleksne grožnje, katerim je izpostavljena Republika Slovenija?

Naj odgovorim na kratko: da. Tudi sicer bi rad poudaril, da izzivi s katerimi se soočamo zahtevajo čim bolj celosten pristop k varnosti. Do konca zgodovine, ki so jo ob koncu hladne vojne nekateri napovedovali, pač ni prišlo. Vizija svobodne, demokratične, skupne in nedeljive varnostne skupnosti od Vancouvra do Vladivostoka, kot je bila leta 2010 formulirana na zadnjem vrhu Organizacije za varnost in sodelovanje v Evropi, se prav tako ni uresničila. Soočeni smo s svetom, v katerem se po eni strani razvijajo najbolj napredne vojaške tehnologije, vključno s hipersonično, po drugi pa se praktica tudi podtalno hibridno vojskovanje. Ravno zato potrebujemo čim več zavedanja o tem v kakšnem okolju živimo, kot tudi čim več medsebojnega sodelovanja. Vloga strokovnih združenj, kot je Slovensko združenje korporativne varnosti, je zato nepogrešljiva. ■

Foto: arhiv kabineta Vlade RS

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

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.

Melamin, Mercator, telemach, SIEMENS, NIJZ Nacionalni inštitut za javno zdravje, ELEKTRONČEK, Telekom Slovenije, Pošta Slovenije, AKRAPOVIČ, 4AIPES, INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O. INFORMATIKA, smartis PAMETNI INFORMACIJSKI SISTEMI, Elita i.b. d.o.o., ZARJA ELEKTRONIKA, UNISTAR PRO, CINKARNA, Slovenske železnice

GEN SKUPINA, Občina Slovenska Bistrica, Onkološki inštitut Institute of Oncology Ljubljana, CAA, SMART COM, URSIV, Ministrstvo za infrastrukturo, Javni medobčinski stanovanjski sklad Maribor, GENERALI, Mestna občina Ljubljana, PETROL Energija za življenje, interblock LUXURY GAMING PRODUCTS, triglav, SPICA, DARS, NovaKBM, LON, energetika ljubljana

www.ics-institut.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Vesna Prodnik, članica uprave, Telekom Slovenije d.d.*

DIGITALIZACIJA IN HITRO SPREMINJAJOČE GLOBALNE RAZMERE POMEMBEN IZZIV IN PRILOŽNOST ZA TELEKOM SLOVENIJE

Telekom Slovenije z novimi tehnološkimi pristopi na področju obvladovanja in upravljanja informacijskih tveganj prinaša pomembne novosti v širši strokovni prostor. Ob tej priložnosti smo se o izzivih razvoja in smelih korakih na področju kibernetske varnosti pogovarjali z mag. Vesno Prodnik, članico uprave odgovorno za tehnologijo v Telekomu Slovenije.

Pospešena digitalizacija in hitro spreminjajoče globalne razmere povečujejo varnostna tveganja v kibernetskem okolju. Kako se v Telekomu Slovenije odzivate na te spreminjajoče se varnostne izzive?

S pospešeno digitalizacijo in vseprisotnim delom na daljavo ter ob hkrati spreminjajočih se geopolitičnih razmerah se povečujejo tudi varnostna tveganja na vseh področjih našega delovanja. Pred kibernetskimi napadi ni varen nihče, zato je ključno, da vsi, pa naj gre za posameznike, podjetja ali organizacije, poskrbimo za ustrezno preventivo in za dobro zaščito na vratih svojega digitalnega sveta.

V Telekomu Slovenije neprestano vlagamo v tehnologije za učinkovito in natančno zaznavanje dogodkov, poglobljeno analitiko, povečanje stopnje avtomatizacije operativnih procesov, različna varnostna in vdorna testiranja ter testiranja ranljivosti.

V Telekomu Slovenije neprestano vlagamo v tehnologije za učinkovito in natančno zaznavanje dogodkov, poglobljeno analitiko, povečanje stopnje avtomatizacije operativnih procesov, različna varnostna in vdorna testiranja ter testiranja ranljivosti. Na globalnem nivoju sodelujemo z različnimi organizacijami in sprejemamo dodatne ukrepe za povečevanje varnosti tako lastnih storitev, kot storitev, ki jih zagotavljamo naročnikom. Vse s ciljem zagotavljanja večje odpornosti omrežja in storitev Telekoma Slovenije.

Ob tem ves čas skrbimo za posodabljanje internih pravil in protokolov (tudi s pomočjo zunanjih pregledov) ter re-certifikacijo procesov in storitev skladno s standardoma ISO 23001 oz. ISO 27001. Širimo in krepimo ekipo, skrbimo za

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

izobraževanja in nadgradnjo kompetenc svojih strokovnjakov ter aktivno sodelujemo na mednarodnih vajah s področja kibernetske varnosti, s čimer pridobivamo dragocene izkušnje. Telekom Slovenije je kot edino podjetje v Sloveniji akreditiran član mednarodne organizacije Trusted Introducer; poleg nas je akreditiran član le še Nacionalni odzivni center za kibernetsko varnost (SI-CERT).

Ste podjetje, ki veliko sredstev vlaga v lasten razvoj novih tehnoloških rešitev. Nam lahko zaupate svojo vizijo na tem področju za prihodnje obdobje?

Telekom Slovenije želi ohraniti pozicijo vodilnega tehnološkega podjetja v panogi, pri čemer so vlaganja v razvoj novih tehnoloških rešitev in povečevanje kompetenc naših strokovnjakov ključna za doseganje tega cilja. Varnosti našega omrežja, storitev in uporabnikov namenjamo popolno pozornost. Zagotavljanje varnosti je in bo ostala naša strateška prioriteta. Nenazadnje smo tudi v svoje poslanstvo zapisali – varujemo vaš svet. Z namenom zagotavljanja celovite kibernetske odpornosti se bomo tudi v prihodnje osredotočali na nadaljnje preventivne aktivnosti za preprečevanje kibernetskih napadov, avtomatizacijo z ustrezno stopnjo umetne inteligence, krepitev kompetenc in ekipe strokovnjakov ter optimizacijo procesov in orodij za učinkovito zaznavo, omejevanje in hiter odziv na napade. Na varnost pa se seveda osredotočamo tudi pri razvoju aplikacij, rešitev interneta stvari, oblačnih storitev in kontejnerskih tehnologij.

V zadnjem obdobju kibernetski varnosti posvečate ogromno svoje strokovne pozornosti. Posebej vaš Operativni center kibernetske varnosti postaja eno izmed pomembnih orodij za zagotavljanje višje stopnje kibernetske varnosti tudi pri velikem številu slovenskih organizacij, ki jim nudite to podporo? Kako ocenjujete evolucijo slovenskega trga na področju zagotavljanja kibernetske varnosti?

Tehnologija, telekomunikacije, trg in varnostne grožnje se nenehno razvijajo. Odvisno od posameznega trga pa je evolucija različna. V Telekomu Slovenije aktivno spremljamo najnovejše smernice in dogajanje na področju kibernetske varnosti. Na vseh segmentih omrežij in storitev uvajamo varnostne rešitve, ki vključujejo tehnologije umetne inteligence.

Zelo spodbudno pa je, da se je stopnja zavedanja glede pomena ustrezne kibernetske zaščite v zadnjem obdobju bistveno povečala. Za varnostne storitve se odloča vedno več organizacij in podjetij, pri tem pa so storitve kibernetske varnosti, ki jih izvaja Operativni center kibernetske varnosti, namenjene tako naši lastni zaščiti kot drugim podjetjem vseh panog in velikosti ter organizacijam kritične infrastrukture in ostalih bistvenih dejavnosti. Ravno prilagodljivost upravljane storitve kibernetskega varovanja in zaščite je ena naših ključnih prednosti.

V segmentu večjih podjetij se spremembe dogajajo zelo hitro, v segmentu manjših in srednjih podjetij pa malce počasneje. Prav zato smo razvili celoten portfelj ponudbe, ki je namenjena različnim tržnim segmentom. Ponudba kibernetske zaščite je raznolika in zajema od varnostnih pregledov, raznih testiranj, priporočil za spremembe do rednega spremljanja varnostnih dogodkov in ukrepanja, če je to potrebno, s

K boljši kibernetski varnosti prispeva tudi zavezanost modelu ničelnega zaupanja (zero trust). Tovrstni model preverja vsako zahtevo za dostop do podatkov na način, kot da izvira iz odprtega omrežja, torej potencialno tveganega okolja.

strani strokovnjakov Operativnega centra kibernetske varnosti. Skrbimo tudi za usposabljanja in izobraževanja ekip pri uporabnikih, poleg tega veliko pozornosti namenjamo ozaveščanju tako podjetij kot uporabnikov.

Kje v teh sistemskih korakih vidite pomen zagotavljanja celovite kibernetske odpornosti širšega kibernetskega prostora v Republiki Sloveniji?

V dvigu kibernetske odpornosti na vseh segmentih tako na strani podjetij, upravljalcev kritične infrastrukture in javne uprave. V večji pripravljenosti in boljši usklajenosti vseh ob morebitnem odzivu na kibernetski incident. Dvigniti je potrebno nivo kompetenc, zaupanja in ozaveščenosti. Pri tem pa je izredno pomembno sodelovanje med posameznimi ključnimi deležniki na varnostnem področju, kot so SICERT, URSIV, AKOS, gospodarska združenja, fakultete in seveda operaterji.

Kako pristopate k prenosu lastnih varnostnih standardov v produkte, ki jih ponujate kot podporo delovanju drugih pomembnih organizacij? Verjetno je to pri storitvah zagotavljanja kibernetske varnosti ključnega pomena, saj jih zagotavljate med drugim tudi za deležnike kritične infrastrukture?

Telekom Slovenije nastopa v treh vlogah - skrbimo za delovanje in varnost lastnih informacijsko-telekomunikacijskih sistemov, skrbimo za varnost sistemov za zagotavljanje telekomunikacijskih storitev ter zagotavljamo IKT in varnostne rešitve pri uporabnikih. Ker želimo biti tehnološko na visoki ravni, se pogosto prvi v Sloveniji spopademo z novimi tehnologijami. S proizvajalci sistemov imamo partnerski odnos, tako da skupaj iščemo dobre prakse pri uvajanju novih tehnologij. Z deležniki bistvene in kritične infrastrukture uspešno sodelujemo, saj jim pogosto pomagamo pri integraciji podobnih rešitev, kot jih uporabljamo tudi sami. Že v fazi načrtovanja poleg funkcionalnosti vedno zasledujemo tudi naše dobre prakse pri zagotavljanju kibernetske varnosti. Poleg mednarodnih standardov moramo seveda pri tem upoštevati tudi lokalno zakonodajo. Ta na področju kibernetske varnosti z zakonom o informacijski varnosti uveljavlja EU direktivo NIS oziroma kmalu novo direktivo NIS-2, ki bo še povečala nabor izvajalcev bistvenih storitev.

Prosim, če nam razložite, kako vi razumete potrebo po zagotavljanju modela ničelnega zaupanja, ki ga v zadnjem obdobju v Telekomu Slovenije zelo izpostavljate?

K boljši kibernetski varnosti prispeva tudi zavezanost modelu ničelnega zaupanja (zero trust). Tovrstni model preverja vsako zahtevo za dostop do podatkov na način, kot da izvira iz odprtega omrežja, torej potencialno tveganega okolja. Ničelno zaupanje nas uči, naj nikoli ne zaupamo in naj vedno preverimo, ne glede na izvor zahteve ali vrsto vira, do katerega se dostopa.

Ko govorimo o ničelnem zaupanju, po navadi najprej pomislimo na obstoječo varnostno arhitekturo: ko se nekdo prijavi v podjetje, lahko dostopa do celotnega omrežja. S tem pristopom je varovan manjši del podjetja. Obstoječi model ne zagotavlja visoke varnostne zaščite dela na daljavo in izpostavlja podjetje tvega-

nju, saj lahko nekdo, ki pridobi poverilnice (uporabniška imena, gesla), dostopa do večine podatkov v podjetju.

Arhitektura modela ničelnega zaupanja pa ne varuje le vstopa do organizacije, temveč varuje vsako datoteko, e-pošto in omrežje ali aplikacijo s preverjanjem pristnosti vsake identitete in naprave. Ne varuje le enega omrežja, temveč pomaga zavarovati tudi oddaljen dostop, osebne naprave in aplikacije tretjih oseb. Pomembno je preverjanje identitet, naprav, upravljanje dostopa do naprav in omrežij, dovoljenj za aplikacije na napravah, dovoljenj za dostope do podatkov (tudi šifriranje), nadzor nad celotno infrastrukturo, korelacijo dogodkov in seveda posodabljanje celote. Če podjetje uporablja model ničelnega zaupanja, bo hitreje zaznalo grožnje kot sicer. S tem bo zasnovalo tudi boljši odziv, ne glede na to, ali so grožnje posledica nepooblaščenega dostopa, zlonamerne komunikacije ali zastarele programske opreme. Model ničelnega zaupanja lahko pomaga tudi pri preprečevanju kršitev zasebnosti in omogoča boljši nadzor podatkovnih tokov.

Pridobivanje ustreznega kadrovskega potenciala je eden od najpomembnejših izzivov, s katerimi se v zadnjem obdobju srečuje večina organizacij. Področje kibernetske varnosti je v tem pogledu še posebej izpostavljeno. Kakšne pristope uporabljate na tem zahtevnem področju?

Drži, na kadrovskem področju ima kibernetska varnost mnogo izzivov. Trenutni izobraževalni sistem nima programa, ki bi omogočal ciljno izobraževanje strokovnjakov na tem področju. To bo v prihodnje potrebno spremeniti. V Telekomu Slovenije kadrovski izziv rešujemo na način, da veliko pozornosti namenjamo interni mobilnosti, skrbimo za redna izobraževanja, prenos izkušenj in kompetenc. Na ta način znotraj družbe strokovnjakom, ki jih področje zanima, omogočamo dostop do zahtevanega znanja in njegovo neprekinjeno nadgrajevanje. Zaposleni se izobražujejo na mednarodno priznanih institucijah, katerih certifikati so standard za dokazovanje kompetenc (npr. SANS certifikacija). Izobražujemo se tudi pri ponudnikih opreme in rešitev. Poleg tega na trgu iščemo strokovnjake s primernimi znanji in certifikati, žal je tudi teh omejeno število. Ker se področje širi in potrebujemo vedno več specializiranih strokovnjakov, je še toliko bolj pomembno tesno sodelovanje s strokovnimi srednjimi šolami in fakultetami, kjer mlade navdušujemo za poklice prihodnosti, kar področje kibernetske varnosti zagotovo je. Skratka, pridobivanje in razvoj strokovnjakov na področju kibernetske varnosti je kompleksen in dolgoročen proces, v Telekomu Slovenije pa se zavedamo tudi svoje odgovornosti na tem področju.

Slovensko združenje za korporativno varnost je ključna organizacija, ki se osredotoča na povezovanje, izobraževanje in ozaveščanje podjetij ter posameznikov na področju korporativne varnosti, zato takšno sodelovanje med deležniki ocenjujemo kot pomemben prispevek k večji odpornosti slovenskega gospodarstva in družbe nasploh.

Menite, da slovenski izobraževalni sistem zagotavlja zadosten kompetenčni okvir za pridobivanje bodočih strokovnjakov na področju informacijske varnosti?

Mislim, da se vsi skupaj vedno bolj in vedno bolje zavedamo naraščajočega pomena informacijske varnosti in potreb po ustrezno usposobljenih strokovnjakih na tem področju. V zadnjih letih je bilo narejenih nekaj pomembnih korakov za izboljšanje kompetenčnega okvira, so pa seveda še vedno priložnosti za izboljšave.

Eno izmed ključnih področij, kjer slovenski izobraževalni sistem lahko naredi več, je razvoj specialističnih smeri in predmetnikov, ki bi se osredotočali na informacijsko varnost. Trenutno je večina študijskih programov, ki vključujejo informacijsko varnost, splošna in študentom nudi le osnovno razumevanje varnostnih konceptov. Za bolj poglobljeno in praktično znanje, ki bi bilo neposredno uporabno v industriji, pa bodo potrebni posebej oblikovani študijski programi.

Telekom Slovenije je zelo aktiven tudi v okviru mednarodnih projektov. Kako uspete v podjetju zagotavljati uravnoteženost med, na eni strani zelo restriktivnimi varnostnimi zahtevami varovanja ključnih informacij organizacije in na drugi raziskovalni iniciativnosti, ki je včasih zelo občutljiva na prevelike omejitve delovnega okolja?

Telekom Slovenije sodeluje v evropskih razvojno-raziskovalnih projektih; s tem sledimo svojim strateškim usmeritvam tehnološko naprednega operaterja, ki aktivno deluje na področju razvoja in uvedbe sodobnih telekomunikacijskih rešitev. Zavedamo se, da je raziskovalna iniciativnost gonilo napredka in inovacij. Zaposleni potrebujejo ustvarjalno in spodbudno delovno okolje z dostopom do potrebnih virov in opreme, kar restriktivne varnostne zahteve varovanja ključnih informacij lahko v določenih situacijah tudi zavirajo. Zato je pomembno, da aktivno uravnavamo pravo razmerje med zagotavljanjem ustreznega varovanja ključnih informacij družbe in razvojem. Na nivoju podjetja imamo jasno definirano varnostno politiko, ki opredeljuje vlogo in odgovornosti zaposlenih ter smernice in pravila za dostop, shranjevanje in posredovanje informacij. Hkrati skrbimo za redno usposabljanje in ozaveščanje zaposlenih o pomenu varnosti.

Telekom Slovenije je eden izmed pomembnih korporativnih članov Slovenskega združenja za korporativno varnost. Kakšen vpliv ima lahko omenjeno strokovno povezovanje na dvigovanje varnostnega zavedanja v širši družbeni skupnosti?

Slovensko združenje za korporativno varnost je ključna organizacija, ki se osredotoča na povezovanje, izobraževanje in ozaveščanje podjetij ter posameznikov na področju korporativne varnosti, zato takšno sodelovanje med deležniki ocenjujemo kot pomemben prispevek k večji odpornosti slovenskega gospodarstva in družbe nasploh. Združenje pomembno prispeva k ozaveščanju deležnikov, izjemno pa je pomembna in koristna tudi izmenjava informacij in dobrih praks. To je pomemben dejavnik krepitve skupne varnosti. Sodelovanje in medsebojna podpora omogočata hitrejši odziv na kibernetske grožnje in boljše razumevanje tveganj ter potrebnih ukrepov za njihovo obvladovanje. ■

Foto: arhiv Telekom Slovenija

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

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

KOLUMNA

JE ČLOVEK NAJŠIBKEJŠI ALI NAJMOČNEJŠI DEL VARNOSTNEGA SISTEMA?

Ob vseh informacijah o tehnoloških prebojih na področju umetne inteligence in drugih sodobnih tehnologijah, ki so in bodo korenito spremenile našo sedanjost in prihodnost, smo pozabili na domačo nalogo, ki jo, kot družba na področju vzpostavitve vrednostnega modela mlade generacije, ki prihaja, nismo naredili.

Pred kratkim nas je pretresla novica o strelskem pohodu v osnovni šoli v Beogradu, ki mu je v kratkem obdobju sledilo še nekaj povezanih strelskih incidentov s tragičnimi posledicami. V zelo kratkem trenutku se je na hitro razblinilo utopično mišljenje, da smo v evropski družbi imuni na pojave, ki so na primer v Združenih državah Amerike postali stalnica vsakdana. Vrh ledene gore se je začel odkrivati že z brutalnim umorom in nerazumnimi dogodki medvrstniškega nasilja, ki so se zgodili v Nemčiji in kjer so bili storilci predstavniki mladoletne generacije. Prepogosto smo postali priča indikatorjem medvrstniškega nasilja, kateremu, razen nekaj medijske, ne posvečamo večje pozornosti. So taki primeri mogoči v Sloveniji, je naša mlada generacija drugačna od splošne svetovne populacije, so razmerja v družinah, kot naših osnovnih celicah drugačna, kot na splošno v drugih družbenih skupnostih? Upravičeno se lahko vprašamo, ali so to samo posamezni, v nebo vpijajoči primeri, ali gre za rak, ki se je razlezel skozi družbeno tkivo mlade generacije in je samo vprašanje, kdaj bo začel resno hromiti nadaljnji razvoj družbe z resnimi varnostnimi implikacijami. Seveda so prvi odzivi politike usmerjeni v poskuse populističnih odgovorov v smeri zaostritve zakonodaje, povečanja represivnih mehanizmov, nesistemskih pristopov za zagotavljanje varnosti, nihče pa se noče dotakniti realnih izvorov nastalih težav. To je z njihovega stališča deloma razumljivo, saj so to ukrepi, ki so dolgoročni in ne prinašajo kratkoročnih političnih točk, vendar gre v tem primeru za družbeno odgovornost, ki presega mandate vlad, županov, ravnateljev in drugih položajev. Najbolj odgovorni za to stanje pa smo starši. Torej generacija, ki vzgaja svoje potomce, jim daje vrednostni okvir, kot osnovna celica vsake družbene skupnosti. Ta odgovornost je neodtujljiva, predvsem pa neprenosljiva na nikogar izven te osnovne družbene celice. Seveda so negativni vplivi okolja, ki pa jih bo generacija, ki prihaja lažje obvladovala, če bodo imeli ustrezen vrednostni okvir in podporo v svojih družinskih okoljih. Naj v nadaljevanju pojasnim nekaj pomembnih vidikov, ki bodo mogoče lahko deloma pripomogli k drugačnemu razumevanju resnosti situacije, v kateri smo se znašli kot družba, in zaradi katerih bomo imeli lahko v prihodnje resne varnostne izzive.

Pomen vzgoje v družini je ključnega pomena za ustrezen razvoj mlade generacije. Čeprav je Kahlil Gilbran nekoč napisal, da »Vaši otroci niso Vaši otroci, so sinovi in hčere želje po

Najbolj odgovorni za to stanje pa smo starši. Torej generacija, ki vzgaja svoje potomce, jim daje vrednostni okvir, kot osnovna celica vsake družbene skupnosti. Ta odgovornost je neodtujljiva, predvsem pa neprenosljiva na nikogar izven te osnovne družbene celice.

*avtor je član Slovenskega združenja korporativne varnosti

življenju«, »Na svet so prišli po Vas in ne za Vas«, »Lahko jim daste svojo ljubezen, a ne svojih misli, ker imajo lastne misli, ki so drugačne od Vaših«, »Doma imate njihova telesa, a ne njihovih duš. Njihove duše bivajo v hišah jutrišnjega dne.« so starši izredno pomemben dejavnik podlag za njihovo nadaljnjo pot in razvoj. Starši so tisti, ki morajo svoje otroke naučiti empatije, odgovornosti, strpnosti in spoštljivega komuniciranja. Čeprav je življenje postalo dinamično z večjo mero obremenjenosti, kot smo ji bili priča v preteklosti, to ne sme biti izgovor, da preostanek časa ne preživljamo z otroki. Seveda govorimo o kvalitetnem preživljanju časa, kjer se z otroki ustrezno komunicira, jih vzpodbuja, postavlja meje predvsem pa, da jim s svojim zgledom postavlja vrednostni okvir. Razumevanje, da naši otroci niso v vsem najboljši in, da je za sobivanje potrebno znati poiskati kompromise je največja vrednost, ki jo lahko predamo naslednji generaciji in bo v večini primerov rešila veliko konfliktnih situacij, travm in agresije. Starši smo tisti, ki dajemo zgled. Otrokom omejimo dostop do komunikacijskih naprav, socialnih omrežij, neustreznih televizijskih oddaj, ne pridrvimo v šolo z odvetnikom, ko nekdo upravičeno postavlja meje dopustnega ravnanja v šolskem okolju in še bi lahko naštevali. Preživljanje kvalitetnega skupnega časa v družinah ne sme biti, da so vsi člani družine vsak na svoji telefonski napravi, temveč v neposredni pristni komunikaciji. Nekdo bo lahko argumentiral, da se zatekamo k poenostavljanju, vendar na žalost govorimo o osnovah, na katere smo po poti že povsem pozabili. Že star slovenski pregovor velja »Kar se Janezek nauči, to Janezek zna«.

> Ko bodo problemi vrednostnega okvirja, ki ga sedaj ustvarjamo pri generaciji katera prihaja, v celoti eskalirali tudi v korporativnih okoljih, za seboj prinesli zelo izpostavljeno tveganje, ki ga nobena nova tehnologija ne bo mogla preprečiti.

Druga pomembna raven je šola oz. širše izobraževalni sistem, kjer je vključena celotna pot sekundarnega postavljanja vrednostnega sistema od vrtca pa vse do visokošolskega izobraževanja. Šolski sistem ni samo sistem za oblikovanje in podajanje znanja, temveč je tudi sistem, ki postavlja naslednji nivo vrednot in oblikuje mlado generacijo v razmišljujoče, predvsem pa strpne in racionalne posameznike. To pomeni, da imajo učitelji in vsi ostali sodelujoči v tem sistemu pomembno vlogo usmerjevalcev, podpornikov in motivatorjev. Poleg tega pa tudi dve pomembni funkciji postavljavcev mej in tistih, ki morajo zaznavati določena odklonska vedenja in jih v ustreznih postopkih skupaj s starši in drugimi institucijami v in izven šole ustrezno naslavljati. Pasivni položaj, kamor so se v zadnjem obdobju umaknili učitelji, je slaba usluga tako otrokom, staršem in nenazadnje izobraževalni profesiji. Seveda mora šolski sistem ustrezno zagotavljati podporo, zaščito in pomoč učiteljem pri izvajanju njihovega poslanstva, tudi pri ustvarjanju vrednostnega okvira v šolah.

Tretja pomembna raven so vsekakor institucije, ki so namenjene obravnavi primerov posameznikov, ki zaradi različnih fizioloških, psiholoških ali socialnih dejavnikov izstopajo iz tega okolja in za normalno socialno pot potrebujejo določen strokovni potisk in pomoč. V tem delu smo priča visoko zbi-

rokratiziranosti sistema, ki deluje sam za sebe in ne v podporo vseh deležnikov, ki so potrebni pomoči ali pa določenega discipliniranja v smeri razumevanja meja, ki jih je širša družbena skupnost postavila za ustrezno sobivanje. Da ne bo pomote, tukaj ne govorimo samo o posameznikih ali družinah, ki imajo eksistenčne probleme, iz katerih se kasneje razvije tudi cel niz drugih vzgojnih in vedenjskih težav. V tem delu govorim tudi o pristopu do tistih družinskih okolij, kjer je vsega v izobilju in iz tega nastajajo psihološki in socialni problemi neustreznih vedenjskih vzorcev, ki postanejo moteči oz. nevarni.

Naslednja raven so seveda mediji, ki se sicer sami poimenujejo četrta veja oblasti, ki je poklicana za nastavljanje ogledala in izvrševanje nadzora prvim trem vejam oblasti (izvršilni, zakonodajni in sodni). Na žalost je razvoj neoliberalističnega modela globalnega razvoja sveta pripeljal do trenutka, ko si mediji niso sposobni sami postaviti ogledala in je bolj kot kvaliteta programov in vsebin pomemben indikator gledanosti. Vse to je pripeljalo do nevarnega stanja, da so mediji tisti kanal, ki v vsako poro družbe prenaša nestrpen in agresiven govor, izpostavljanje slabih primerov, različne vsebine, ki vrednostni okvir v družbi popolnoma izkrivlja. Če to dejstvo pogledamo iz oči mladoletne generacije, kjer odpovedujejo nadzori že v vseh prej navedenih primarnih nivojih, si lahko samo mislimo kakšno eksplozijsko mešanico dajemo v možgane mladi generaciji.

Kibernetski prostor s socialnimi omrežji smo namerno izvzeli iz medijskega okvirja, saj sama po sebi predstavljalo poseben izziv, kateremu je izpostavljena družba na sploh, še posebej pa mlada generacija, ki je najmočnejši uporabnik. Izzivi, ki jih predstavlja nadzor nad ustreznostjo vsebin, ki se širi preko socialnih omrežij, pa vse do omejenosti dostopov v zaprta omrežja, so tisti izzivi, na katere danes na različnih odzivnih nivojih nismo našli ustreznega odgovora. Prvenstveno pa bo družba na tem področju uspešnejša, če bosta delovala oba pola te premice in sicer primarna celica (družina) in družba kot celota s svojim ustreznim vrednostnim okvirjem ter nadzornimi mehanizmi organov, ki so na podlagi zakonodaje za to poklicani.

Vidik, ki ga je v okviru tega potrebno posebej izpostaviti in največkrat tudi zelo vpliva na pojavnost takih dogodkov, ki bi jih strokovno vsekakor lahko umestili med AMOK situacije, pa je dostopnost do orožja in drugih eksplozivnih sredstev. Sprejeta družbena norma je, da ima samo država pooblastilo uporabe represivnih sredstev in še to pod točno določenimi zakonskimi okvirji. Posedovanje in uporabo orožja izven teh mehanizmov pa zelo podrobno predpiše z ustreznimi normativnimi akti. Restriktivni pristop do posedovanja orožja se je do sedaj v praksi, glede na različne družbene modele, pokazal kot ustreznejši za obvladovanje tovrstnih dejanj povezanih s strelskimi pohodi ali drugimi AMOK situacijami. Seveda se je potrebno v tem okviru zavedati problematike, ki jo predstavlja črni trg za orožje in nelegalno posedovanje oborožitve, do katerih pa mora imeti družba nično stopnjo tolerance. Poleg vsega navedenega poseben izziv predstavljajo tudi nove tehnologije, kot so 3D printerji in celoten globalni logistični sistem, preko katerega se lahko naročajo in posredujejo določeni deli, kateri bi služili za izdelavo orožja. Skupaj z idejami in navodili, ki jih je možno najti na spletu, to ponovno predstavlja nevarno zmes za tragedijo. Seveda se bodo hitro našli zagovorniki in opravičevalci, ki bodo posedovanje nelegalnega orožja pripisali kulturi, tradiciji, bližini kriznih žarišč, varnostnega stanja v družbi, kjer se pojavljajo ideje o vaških

Odgovornost, ki je v naših rokah in ni samo deklarativna, temveč dejanska neodtujljiva dolžnost, ki ji ne moremo ubežati ali jo prevaliti na nikogar drugega, je izredno velika! Trenutno stanje kaže, da na tej poti nismo naredili svoje domače naloge.

stražah ali milicah, vendar mora ustrezno razumska družbena skupnost narediti vse, da to ne postane del vrednostnega sistema družbe in še posebej mlade generacije, ki prihaja. Če pa zadevo spet pripeljemo do osnovne celice, se v veliki večini zadeve preprečujejo že na tej primarni stopnji delujočega vrednostnega sistema, ki ga starši prenašamo na mladostnike.

Po zapisanem se boste verjetno vprašali dve ključni stvari in sicer zakaj v reviji, ki se ukvarja z varnostjo v korporativnem okolju odpiramo probleme varnostnih implikacij mlade generacije, ki še ni neposredno vpeta v korporativno varnostno okolje in drugič si boste verjetno rekli, da so v pričujočem prispevku napisane splošne resnice, ki so jasne vsakemu posamezniku te družbe.

V odgovor je potrebno zapisati naslednje, da ob vseh tehnoloških dognanjih in razvoju kateremu je podvržena družba, še posebej pa mlada generacija, ki prihaja, smo v celoti pozabili na pomembnost vedenjskega okvira, da prekomeren individualizem vodi v povečevanje konfliktnih situacij na vseh družbenih nivojih. Ko bodo problemi vrednostnega okvirja, ki ga sedaj ustvarjamo pri generaciji katera prihaja, v celoti eskalirali tudi v korporativnih okoljih, za seboj prinesli zelo izpostavljeno tveganje, ki ga nobena nova tehnologija ne bo mogla preprečiti. Še posebej v tem okviru izpostavljamo organizacije, ki upravljajo s ključno infrastrukturo, ki je pomembna za delovanje naše družbene skupnosti. Si zamislite, da bomo v to okolje začeli dobivati generacijo bodočih sodelavcev s popačenim vrednostnim modelom, ki v osnovi temelji na popolni individualnosti. Na drugi strani tudi družba popolnega nadzora z detektorji na vhodih naših šol ali organizacij, obsežnem video nadzornem sistemu podprtim z umetno inteligenco ali neskončnem številu angažiranega varnostnega osebja, ne bo prinesla bližnjice do zagotavljanja ustreznega nivoja varnosti. Varnost namreč generira najprej vsak posameznik in nato ožja ter širša družbena skupnost. Posameznik je s svojim psihološkim, fiziološkim in predvsem sociološkim smislom tisti člen našega sistema, ki ga lahko gledamo skozi prizmo najšibkejšega ali najmočnejšega člena. Od vseh nas pa je odvisno kateri vidik bo prevladal.

Za konec pa še odgovor po odpiranju splošno znanih dejstev pomena vloge posameznika in družine. Vsak del primarne skupnosti, predvsem pa starši sami naj si v odgovor nastavimo ogledalo ali svojim zanamcem s svojimi ravnanji, zgledom in spoštljivo komunikacijo prenašamo vrednostni model, ki bo omogočal normalno in varno sobivanje. Odgovornost, ki je v naših rokah in ni samo deklarativna, temveč dejanska neodtujljiva dolžnost, ki ji ne moremo ubežati ali jo prevaliti na nikogar drugega, je izredno velika! Trenutno stanje kaže, da na tej poti nismo naredili svoje domače naloge. ■

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

SMART COM

Zagotovite varno, zanesljivo in odgovorno digitalno prihodnost

Smart Center upravljanih varnostnih in omrežnih storitev

Kibernetska varnost v poslovnem in industrijskem okolju in okolju kritične infrastrukture

Sodobna omrežja nove generacije za odlično uporabniško izkušnjo

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
dr. Dragan Kovačić, dr. med., direktor Splošne bolnišnice Celje*

RAZVOJ POMEMBNIH ZDRAVSTVENIH ORGANIZACIJ NI MOGOČ BREZ USTREZNEGA ZAGOTAVLJANJA VARNOSTI

O izzivih, ki jih prinaša potreba po zagotavljanju obvladljivega in varnega delovnega okolja v modernih zdravstvenih organizacijah, smo se pogovarjali z dr. Kovačićem, direktorjem Splošne Bolnišnice Celje.

Pred kratkim ste nastopili polni mandat na položaju direktorja Splošne bolnišnice Celje za kar vam iskreno čestitamo. Bodite tako prijazni in nam zaupajte, kaj so tista glavna vodila, ki so vas motivirala, da se poleg interne medicine posvetite upravljanju te pomembne zdravstvene ustanove?

Šlo je predvsem za skrb, da bi lahko imenovanje osebe, ki ne pozna dobro delovanja naše bolnišnice ter istočasno aktualnega dogajanja v zdravstvu na državnem nivoju, oviralo strokovni razvoj naše ustanove, kot tudi dokončanje osrednjega strateškega projekta naše bolnišnice, in sicer projekta Novogradnje. V svoji osnovi tako ostajam zdravnik, moja motivacija za prevzem te odgovorne funkcije pa je izključno vezana na nadaljnji razvoj in napredek Splošne bolnišnice Celje.

Pospešena digitalizacija močno prodira tudi v zdravstveni sektor. Kako po vašem mnenju najti neko ustrezno razmerje uvajanja teh rešitev v poslovne procese zdravstvenega sektorja, da zaradi prehitrih odločitev ne ogrožate varnosti vaših pacientov?

Digitalizacija v zdravstvu bo smiselna in možna šele takrat, ko bodo njeni iniciatorji in operativci dojeli, da jo lahko uvajajo zgolj in edino v sodelovanju z medicinsko stroko. Vodstvu zdravstvenih ustanov pa mora postati digitalizacija pomagalo pri delu in ne zgolj še ena dodatna naloga in breme poleg vseh že obstoječih. V preteklosti so bile motivacije za vzpostavitev digitalizacije v zdravstvu različne, v glavnem finančne in na strani dobaviteljev opreme. Sistemi, ki so bili uporabljeni pa so v glavnem zastareli in brez kakršnekoli povezave z realno situacijo na deloviščih v zdravstvu. Ponovitve podobnih pristopov bodo po mojem mnenju tudi v prihodnje obsojeni na propad oziroma na popolnoma neracionalno porabo javnega denarja.

Digitalizacija v zdravstvu bo smiselna in možna šele takrat, ko bodo njeni iniciatorji in operativci dojeli, da jo lahko uvajajo zgolj in edino v sodelovanju z medicinsko stroko. Vodstvu zdravstvenih ustanov pa mora postati digitalizacija pomagalo pri delu in ne zgolj še ena dodatna naloga in breme poleg vseh že obstoječih.

V zadnjem obdobju smo bili v zdravstvenih ustanovah priča primerom

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Kot vodilni delavec javnega zavoda sem seveda dolžan zagotavljati politiko ničelne tolerance do korupcije, kar v praksi pomeni, da vzpostavljam in skrbim za mehanizme, ki podobno ravnanje oziroma tveganja zmanjšujejo.

fizičnih napadov na zaposlene v bolnišnici. Tak primer se je zgodil tudi v vaši ustanovi. Kako ste se lotili reševanja teh izpostavljenih varnostnih izzivov?

Predvsem smo ta nevarni dogodek obravnavali z vso resnostjo, ki mu po našem prepričanju pripada. Izkušnje iz nedavnih dogodkov doma in po svetu nas namreč učijo, da lahko negativna klima v populaciji preko podobnih dogodkov signalizira realno možnost in nevarnost mnogo resnejšega izgreda s hujšimi posledicami. Zato smo ravnali preventivno, se povezali s strokovnimi inštitucijami s področja korporativne varnosti, pridobili njihova mnenja, okrepili varovanje ljudi in premoženja, obnovili programe edukacije naših uporabnikov glede varnosti, ter sprejeli številne druge ukrepe, ki bodo zagotavljali večjo varnost tako bolnikov kot zaposlenih, kar je po našem mnenju osnovni pogoj za izvajanje našega poslanstva oziroma za opravljanje dela, ki ga od nas pričakujejo ljudje.

Menite, da je izobraževanje s področja dvigovanja varnostnega zavedanja vseh zaposlenih v vaši organizaciji lahko pomemben korak k višji stopnji varnosti? Boste na tem področju poskušali narediti kakšen korak k povečanju teh izobraževalnih vsebin tudi za zdravstveno osebje?

Absolutno. Naše globoko prepričanje je, da je ravno edukacija osnovni način postopnega spreminjanja ravnanja katerekoli populacije, tudi naših bolnikov ali zaposlenih, zato temu že namenjamo veliko pozornosti. Za zaposlene imamo na voljo spletne edukacije, informativne filme za naše uporabnike predvajamo na monitorjih po vsej bolnišnici, na voljo so edukacijski pisni materiali, itd. V prihodnosti pa bomo temu področju namenili še več pozornosti.

Korupcija je v zadnjem obdobju dvajsetih let verjetno eden od najbolj problematičnih izzivov Slovenskega zdravstva. Kako se v vaši ustanovi spoprijemate s temi problemi?

Korupcija je problem vseh družbenih in gospodarskih podsistemov, ki s pomanjkanjem regulatornih mehanizmov ali pa s pomanjkljivo oziroma nepravilno uporabo le-teh slednjo dopuščajo. Osebno menim, da je tovrstno ravnanje z vzpostavitvijo kontrolnih mehanizmov in ustreznega nagrajevanja najproduktivnejših zaposlenih možno v celoti izkoreniniti. Vprašanje je le, če je to vsem, ki se s tem področjem ukvarjajo, dejansko v interesu, ali pa gre zgolj za všečno postavljanje pred množicami potencialnih volivcev, v ozadju pa hudo pomanjkanje vsebine. Kot vodilni delavec javnega zavoda sem seveda dolžan zagotavljati politiko ničelne tolerance do korupcije, kar v praksi pomeni, da vzpostavljam in skrbim za mehanizme, ki podobno ravnanje oziroma tveganja zmanjšujejo.

Menite, da so lahko izkušnje, ki jih prinašajo mednarodni evropski projekti pot za večjo učinkovitost na tem področju? Pred kratkim ste se skupaj z močnim mednarodnim konzorcijem prijavili na evropski razpis, ki je v center postavil ravno uporabo rešitev umetne inteligence pri preprečevanju korupcijskih tveganj.

Absolutno. V Sloveniji vse prevečkrat odkrivamo toplo vodo sami in to vedno znova, namesto, da bi že preverjene rešitve enostavno uvozili od drugod. Evropski projekti slovijo po svoji zelo strogi regulativi in nadzoru, kar korupcijska tveganja močno zmanjšuje. Ne

vidim težav v tem, da se učim od nekoga, ki zna bolje, hitreje in bolj racionalno. Umetna inteligenca hitro postaja naša realnost. Poišče nam lahko hotele, letala, piše govore, pesmi in prezentacije. Zakaj ne bi njenih potencialov uporabili pri iskanju koruptivnih tveganj?

Informacijskim tveganjem se ne more izogniti niti zdravstveni sektor. Tem tveganjem so podvrženi, tako ključni podatki o pacientih, kakor tudi delovanje pomembnih tehnoloških naprav, ki jih uporabljate v zdravstvenem sektorju. Kakšen pomen boste v času svojega upravljanja Splošne bolnišnice v Celju namenili temu pomembnemu področju?

V času mojega vodenja bomo okrepili sektor za korporativno varnost, saj vsakodnevno operiramo z zelo občutljivimi osebnimi podatki. Pri vsakodnevnem delu s toliko zaposlenimi in uporabniki se dogajajo izredni dogodki in zato je potrebno slediti novostim. Da vse to zagotovimo in ob tem našim bolnikom zagotavljamo tudi najvišjo možno kakovost storitev, je potrebno uporabljati sodobno tehnologijo, ki seveda s seboj prinaša nova tveganja. Ker se le-teh zavedamo, bomo tudi nadzor nad njimi in protokole, ki bodo preprečevali napake ali zlorabe sproti razvijali, dopolnjevali in koordinirali z ustreznimi državnimi in mednarodnimi institucijami.

V zdravstvu se veliko govori o pomanjkanju zdravnikov in drugega medicinskega osebja, redko pa slišimo o problemih pomanjkanja drugih strokovnjakov, ki so ravno tako pomembni za nemoteno delovanje zdravstvenega sistema, kot na primer pomanjkanje informatikov ali strokovnjakov s področja korporativne varnosti. Kako razumete te izzive in katere pristope boste udejanjili na tem področju?

S pomanjkanjem navedenih profilov smo se v naši bolnišnici srečali že takoj ob prevzemu vodenja in takoj odreagirali z dodatnim zaposlovanjem. S tem smo pomanjkanje ublažili, ne pa popolnoma odpravili. Problem glede informatike je v javnem sistemu. To je popolnoma nekonkurenčen in neustrezen način plačevanja v katerem najproduktivnejši posamezniki prejmejo mesečno nekajkrat manjšo plačo, kot v zasebnih podjetjih. Na tem področju čakamo na napovedane spremembe na državni ravni.

V vaši bolnišnici je bil v operativno uporabo dan nov helidrom, ki predstavlja možnost hitrejše oskrbe pacientov. Kaj za vas pomeni ta pridobitev?

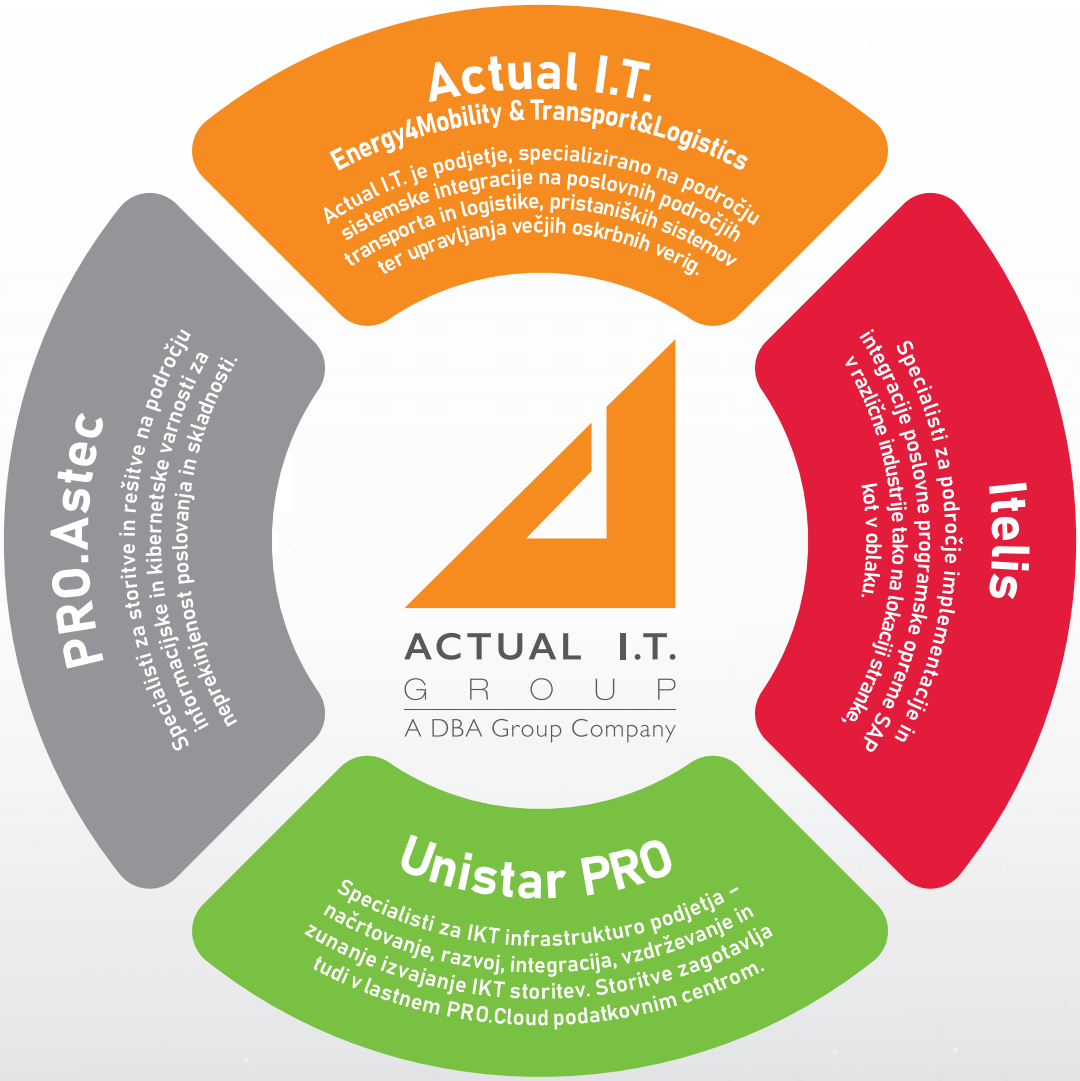
Gre za velik strokovni napredek, saj je sedaj možna urgentna dostava bolnikov v našo bolnišnico iz nedostopnih točk na terenu, ki nas obdaja, kot tudi premestitev nujnega bolnika iz naše bolnišnice v ustrezno terciarno ustanovo, v kateremkoli delu dneva in ne glede na razmere na cestah. Gre za možnost, ki se je v rednem kliničnem delu že prijela in jo vsakodnevno uporabljamo. Gre za pridobitev, ki rešuje življenja, istočasno pa za pridobitev, ki povečuje razvojni potencial bolnišnice v prihodnosti in v smereh, ki morda v tem trenutku še niso povsem očitne.

Splošna bolnišnica Celje je eden izmed pomembnih korporativnih članov Slovenskega združenja za korporativno varnost. Kakšen vpliv ima lahko omenjeno strokovno povezovanje na dvigovanje varnostnega zavedanja v širši družbeni skupnosti?

Skupnosti in združenja imajo po načelu, da več glav več ve, vedno večjo moč in vpliv kot posameznik. Povezava z ljudmi, ki se z varnostjo ukvarjajo poklicno, predstavlja preskok iz amaterske zaskrbljenosti v poklicno identifikacijo dejavnikov tveganja, opredelitev konkretnih nevarnosti in sprejem ustreznih ukrepov, ki bodo tveganja za naše bolnike in zaposlene zmanjšale na minimum. Gre za jasen odmik od učenja preko poskusov in napak, na akademski pristop, z uporabo jasnih principov varnostnih znanosti. Zavedamo se, da tako na področju zdravja, kot tudi na področju varnosti, znanost ni popolna, obenem pa tudi, da je znanost največ, kar v tem trenutku imamo. In to skušamo uporabiti v vsakodnevni praksi. ■

Foto: arhiv Splošna bolnišnica Celje

Povezava z ljudmi, ki se z varnostjo ukvarjajo poklicno, predstavlja preskok iz amaterske zaskrbljenosti v poklicno identifikacijo dejavnikov tveganja, opredelitev konkretnih nevarnosti in sprejem ustreznih ukrepov, ki bodo tveganja za naše bolnike in zaposlene zmanjšale na minimum.



ACTUAL I.T. astec ITELIS UNISTAR PRO

IT360°

www.actual-it.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Matija Repina, vodja Službe varovanja v družbi BTC d.d.*

KORPORATIVNA VARNOST NI MOGOČA BREZ STROKOVNIH POSAMEZNIKOV

V dinamičnem poslovnem okolju je zagotavljanje odpornosti in s tem neprekinjenosti delovanja velikih organizacij nujna za poslovno učinkovitost. Korporativna varnost ima v tem okviru posebej izraženo vlogo in odgovornost.

Gospod Matija Repina je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2022«.

Obvladovanje varnostnih tveganj je zelo pomembna nit vaše strokovne kariere. Katera področja so posebej zaznamovala vaš karierni razvoj?

V tako velikem in raznolikem ekosistemu, kot je družba BTC, se pri zagotavljanju varovanja srečujemo s številnimi kompleksnimi varnostnimi tveganji, ki se ob tem pojavljajo. V družbi, kjer delam že več kot 15 let je moj karierni razvoj tesno povezan z varnostnimi tveganji, ki izhajajo iz diverzificiranih dejavnosti družbe. V sklopu posameznih poslovnih enot se srečujemo s popolnoma drugačnimi tveganji in pristopi, zato težko izpostavim posamezno področje. Pri vseh pa je ključno, da smo nanje dobro pripravljeni in imamo vzpostavljene procese na področju zagotavljanja varovanja, s katerimi se lahko hitro in prilagodljivo odzivamo na dogajanje. Pri zagotavljanju neprekinjenega delovanja velikega sistema, kot ga upravlja družba BTC, ne gre brez povezovanja in sodelovanja. Varno okolje BTC City-jev namreč soustvarjamo skupaj, tako zaposleni kot naši poslovni partnerji in tudi obiskovalci. Pri tem je pomembno izobraževanje in ozaveščanje, da znajo posamezniki ob tveganjih primerno ravnati, hkrati pa se zavedajo, da varnost ni samoumevna.

V zadnjem obdobju ste zelo močno vpeti v upravljanje varnostnih tveganj v BTC. Menite, da je ustrezno razumevanje sprememb kompleksnega varnostnega okolja lahko konkurenčna prednost podjetij?

Ustrezno razumevanje varnostnega okolja in sprememb je nuja in hkrati konkurenčna prednost podjetij. Organizacija mora obvladovati tveganja, da se lahko posveča prepoznavanju trendov in razvijanju novih poslovnih priložnosti. V družbi BTC se zavedamo pomena učinkovitega in kakovostnega sistema varnosti, ki je podlaga za izvajanje drznih naložb, inovativnih poslovnih rešitev, trajnostnega razvoja in našo nadaljnjo visoko rast.

BTC je eden izmed največjih poslovno-zabaviščnih kompleksov v tem delu Evrope in je zaradi obsega različnih dejavnosti in površine zelo kompleksna organizacija za obvladovanje varnostnih tveganj. Kako uspete zagotavljati potrebno koordinacijo z različnimi deležniki, ki sobivajo v okviru BTC?

Varnost v najširšem smislu je eden izmed temeljev za uspešno poslovanje družbe BTC. V naših središčih BTC City dajemo poseben poudarek zagotavljanju splošne, požarne in prometne varnosti

Gospod Matija Repina je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2022«.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

ter varnosti premoženja, tako družbe kot njenih zaposlenih, poslovnih partnerjev in obiskovalcev. Družba BTC je že pred leti z namenom zagotavljanja varnosti organizirala lastno službo varovanja, katere naloga je ustvarjanje podlage za prijazno in urejeno okolje, v katerem se vsi počutijo varno. Res pa je, da se potencialna tveganja z vse večjim obiskom – samo BTC City Ljubljana ima letno več kot 21 milijonov obiskov – novimi objekti in programi, ter zaradi aktualnih gospodarskih in političnih razmer spreminjajo. Kot sem že omenil je pri zagotavljanju varnosti potrebno sodelovanje in izobraževanje tako zaposlenih, poslovnih partnerjev in obiskovalcev. Morda samo kot primer omenimo, da smo v lanskem letu ob ostalih investicijah v BTC City Ljubljana postavili tudi nove oglaševalske zaslone, ki ozaveščajo mimoidoče obiskovalce središča o varnosti in temeljnih postopkih oživljanja, štirje pa imajo ob strani nameščen tudi avtomatski zunanji defibrilator. Pri tem velja poudariti, da varnost na območju pravzaprav soustvarjamo vsi.

BTC vsak dan delovanja obišče veliko število obiskovalcev in uporabnikov vaših storitev. S tega stališča je zagotavljanje njihove varnosti verjetno poseben izziv?

BTC City Ljubljana je območje z visoko dnevno frekvenco obiskovalcev, zato je skrb za zagotavljanje varnosti izredno pomembna. Zagotavljanje varnosti vsem na tako velikem območju s tako raznolikimi dejavnostmi ne dopušča napak. Dnevno namreč beležimo velik obisk območja, poleg tega iz naših skladišč vsak dan pripravimo in odpremimo kar nekaj tovornih vozil, ki oskrbujejo poslovne partnerje na lokacijah po celi Sloveniji. Veseli smo, da skupaj s poslovnimi partnerji uspešno skrbimo za varnost območja.

BTC je eden od pomembnih partnerjev EU projekta APPRAISE, ki je usmerjen ravno v zaščito ti. »mehkih tarč«. Katera so vaša glavna pričakovanja od sodelovanja na tem zahtevnem projektu?

Raziskovalni projekt APPRAISE je izjemno kompleksen, saj se v prvi vrsti osredotoča na zagotavljanje varnosti »mehkih tarč« in varnostnih scenarijev ob morebitnih izrednih dogodkih, a hkrati naslavlja veliko izzivov, s katerimi se dnevno srečujemo pri zagotavljanju varnosti. S sodelovanjem v projektu želimo pridobiti nova znanja in izkušnje, utrditi sodelovanje z Policijo in poglobiti stike z mednarodnimi strokovnjaki in tujimi partnerji ter pridobiti vpogled v nove tehnologije, ki bi jih lahko vpeljali v naše varnostne sisteme in bi zaposlenim omogočili lažje, hitrejše in boljše odločanje, hkrati pa bi jih razbremenili. V projektu sodeluje kar 27 partnerjev iz 10 držav. S sodelovanjem v projektu bomo lahko preverili tudi naše obstoječe varnostne protokole, pridobili ideje za njihovo izboljšanje skupaj z različnimi deležniki pri zagotavljanju varnosti.

Opažam, da se nivo prepoznavanja pomena korporativne varnosti in obvladanja tveganj v zadnjem času krepi. Verjamem, da je to tudi plod aktivnosti Slovenskega združenja korporativne varnosti.

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

Z veseljem lahko povem, da vodstvo družbe BTC in služba za varovanje dobro sodelujemo. Vodstvo se na strateškem nivoju zelo dobro zaveda pomena varnosti za nemoteno delovanje in razvoj družbe, zato ob konstruktivnih in utemeljenih predlogih za izboljšave in posodobitve na tem področju nimamo težav s podporo.

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

Dejstvo je, da okvir zagotavljanja varnosti v posamezni organizaciji presega zgolj samo službo, ki je za to direktno zadolžena, ampak varnost soustvarjamo vsi deležniki v poslovnem procesu. Drži, da je ob pospešeni digitalizaciji in enormnemu pretoku informacij, varnost v vseh pogledih vedno bolj pomemben sestavni del vseh organizacij, ki mora biti za njihovo uspešno delovanje integriran v vsakdan podjetij – to ne pomeni zgolj urejenega požarnega, tehničnega, fizičnega in kibernetskega varovanja, ampak tudi vpeto v vsakodnevne procese. Opažam, da se nivo prepoznavanja pomena korporativne varnosti in obvladanja tveganj v zadnjem času krepi. Verjamem, da je to tudi plod aktivnosti Slovenskega združenja korporativne varnosti.

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

Zagotovo. Razvoj kompetenc in krepitev zavedanja o pomenu varnosti so ključna. Sam sem zagovornik celovitega pristopa – ne zgolj tehnike, temveč tudi ustrezno usposobljenega kadra, saj ob rapidnem razvoju tehnologij človek (p) ostaja najšibkejši člen v sistemu varovanja. Človek je tisti, ki se kljub pomoči tehnologije, mora odločiti kako reagirati, ko pride do tvegane situacije. In to ne samo posamezniki, ki delajo na področju varovanja, ampak vsi. Varnost je odgovornost vseh in ni samoumevna, zato je tudi vložek vanjo neizbežen. Prepoznavanje teh dejstev in izvajanje izobraževanj loči uspešna podjetja od povprečnih. Pomembno vlogo ima tudi spremljanje novih tehnologij in trendov na področju varovanja ter uvajanje tistih tehnologij, ki nam bodo pomagale izboljšati procese in razbremeniti naše zaposlene. V prihodnje bo predvsem na področje izobraževanja in tudi uvajanja novih tehnologij potrebno usmeriti še več virov s ciljem zmanjševanja in obvladovanja tveganj.

Varnost je odgovornost vseh in ni samoumevna, zato je tudi vložek vanjo neizbežen. Prepoznavanje teh dejstev in izvajanje izobraževanj loči uspešna podjetja od povprečnih.

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

Vesel sem, da smo v družbi BTC že dolga leta korporacijski člani združenja. Kot pravi eno od poslanstev združenja, „Ustvarjamo vezi, ki bogatijo, ter tako gradimo pot do uspeha!“, in to lahko potrdim iz prve roke. Združenje in povezovanje strokovnjakov, ki prihajajo z zelo različnih področji in se ukvarjajo z varovanjem, je velika dodana vrednost za člane ter pomembna priložnost za pridobivanje novega znanja, izmenjavo izkušenj in dobrih praks.

Kaj vam pomeni prejeta nagrada Slovenian Grand Security Award v kategoriji »korporativno varnostni manager leta«?

Ob seznanitvi s podeljeno nagrado sem bil izjemno počaščen. Nagrada mi v prvi vrsti pomeni motivacijo in zavezo za kvalitetno izvajanje dela tudi v prihodnje. Bi se pa želel ob tem zahvaliti svojim predanim in odločnim sodelavcem, s katerimi skupaj skrbimo za zagotavljanje varnosti v družbi BTC, saj kot rad poudarjam, varnost s sodelavci soustvarjamo skupaj, zato tudi njim pripada del te nagrade. ■

Foto: arhiv BTC

Ključavnice za pametne sisteme pisarniških in garderobnih omaric v sodobnih delovnih prostorih

Za varne možnosti shranjevanja osebnih stvari, dokumentov, garderobe, paketov, delovne opreme zaposlenih ali obiskovalcev.

Minimalistične ključavnice, ki se zlahka zlijejo z dizajnom vašega prostora, brez težav pa jih lahko namestite tudi na obstoječe omarice in odklepate z obstoječimi mediji.

- Različni načini odklepanja (RFID medij, koda, mobitel) in napajanja (baterije ali On-line).
- Upravljanje preko centralnega terminala ali vsake omarice kot samostojne enote.
- Dodatne funkcije: USB polnjenje, osvetlitev, svetlobni in zvočni alarmi,...

IDealni partner za identifikacijo in varnost

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

Gantner
www.gantner.com

Avtorica: Mojca Štruc / vodja Sektorja za digitalno vključenost, Ministrstvo za digitalno preobrazbo

STRATEGIJA DIGITALNA SLOVENIJA 2030

Po izteku prejšnje (Digitalna Slovenija 2020) smo novo strategijo digitalne preobrazbe pričakovali v letu 2020. Kljub poskusom v prejšnji in še eni vladi pred tem, predlog nikoli ni ugledal luč sveta, zato smo res veseli in ponosni, da lahko rečemo da je 23. marca letos Vlada Republike Slovenije sprejela strategijo Digitalna Slovenija 2030, ki je krovni strateški dokument Vlade Republike Slovenije na področju digitalne preobrazbe. Je izjemnega pomena: ne samo zato, ker smo nanj dolgo čakali, temveč predvsem zaradi vsebine.

Strategija je odgovor Vlade Republike na razvojne izzive digitalizacije in je namenjena strateškemu načrtovanju spodbujanja digitalne preobrazbe Slovenije v razvojnem obdobju do leta 2030.

Pri tem je treba razumeti, da se potrebe različnih segmentov družbe oziroma različnih ciljnih skupin med seboj razlikujejo ter, da je potrebno poskrbeti tako za gospodarski razvoj, napredek in konkurenčnost, kakor tudi javnim institucijam, lokalnim skupnostim in posameznikom zagotoviti potrebna sredstva in vire, da bomo skupaj vstopali v digitalno napredno družbo in izkoristili prednosti digitalnih tehnologij.

Ključno je, da se tako vladni predstavniki kakor tudi širši deležniki zavežemo, da bomo imeli redno medsebojno komunikacijo in usklajevanja, saj smo le skupaj, kot enotna skupnost, lahko dovolj hitri in kompetentni za uspešno digitalno preobrazbo.

Ker vsebuje Digitalna Slovenija 2030 (v nadaljevanju: DSI2030) tako široke strateške usmeritve, ne vsebuje podrobnosti specifičnih področij (npr. zdravstva, kmetijstva, okolja itd.) – te so ali pa še bodo opredeljene v področnih strategijah ali akcijskih načrtih oz. programih.

Ker je Slovenija članica EU, so pri pripravi naših strategij izjemno pomembne strateške usmeritve Evrope. Te so na področju digitalne preobrazbe zelo ambiciozne.

Vizijo, cilje in možnosti za uspešno digitalno preobrazbo Evrope do leta 2030 je Evropska komisija marca 2021 predstavila v dokumentu Evropsko digitalno desetletje: digitalni cilji za leto 2030, kjer je predlagan dogovor o sklopu digitalnih načel za hitro uvedbo pomembnih več državnih projektov in pripravo zakonodajnega predloga, ki določa trden okvir upravljanja, za spremljanje napredka – digitalni kompas.

Ta temelji na štirih glavnih točkah:
1. Digitalno usposobljeno prebivalstvo in visoko kvalificirani strokovnjaki na digitalnem področju
2. Varne, učinkovite in trajnostne digitalne infrastrukture
3. Digitalna preobrazba podjetij
4. Digitalizacija javnih storitev

Za vsako od naštetih področij je EK predvidela konkretne kazalnike, ki jim sledimo tudi v Sloveniji.

V središče DSI2030 smo postavili posameznika: pri digitalnem preoblikovanju je treba upoštevati uporabniške potrebe (ang. user needs) in potrošniške pravice (ang. consumer rights) ter ustrezno zaščititi človekove pravice (ang. human rights). Ob tem je na mestu tudi posebna skrb za okolje, v katerem posameznik živi.

Upoštevali smo načela EU: ljudje v središču, solidarnost in vključenost, svoboda izbire, sodelovanje, varnost in zaščita, trajnost. Ob teh načelih pa smo v strategiji posebej izpostavili še nekatera druga, za nas ključna in za naše okolje morda specifična načela: splošno zavedanje o pomenu digitalne pre-

Skupna pot je edina pot naprej k učinkoviti digitalni preobrazbi v vse hitreje spreminjajoči se družbi, zato se vsem, ki so doslej kakor koli sodelovali pri pripravi strategije Digitalna Slovenija 2030, na tem mestu zahvaljujemo za konstruktivno sodelovanje doslej in se veselimo sodelovanja tudi v prihodnje.

obrazbe; internet kot strateško orodje digitalne preobrazbe; zaščita svobodnega odprtega interneta; zasledovanje medsektorskih sinergijskih razvojnih učinkov; uporaba slovenskega jezika in ohranjanje kulturne identitete; spodbujanje raziskav in razvoja digitalnih tehnologij in njihove uporabe; strateška avtonomija, enotni digitalni trg in digitalna suverenost; demokratična digitalna družba; doseganje razvojnih ciljev Slovenije z digitalno preobrazbo.

Digitalna Slovenija 2030 torej upošteva ambicije in načela EU, obenem pa se usmerja v bistvene izzive Slovenije na področju digitalne preobrazbe in tako prepoznava šest prednostnih vsebinskih področij digitalne preobrazbe. Na tem mestu prednostna vsebinska področja naštevamo in izpostavljamo ključne cilje s kazalniki pri vsakem od njih:

1. Gigabitna infrastruktura

Strateški cilji v DSI2030 so določeni skladno z Načrtom razvoja gigabitne infrastrukture v Sloveniji do leta 2030, in sicer na treh področjih:

- zagotovljena pokritost vseh gospodinjstev z gigabitnim omrežjem
- zagotovljena pokritost vseh podjetij in drugih spodbujevalcev družbeno-gospodarskega razvoja z gigabitnim omrežjem
- zagotovljena pokritost vseh naseljenih območij z omrežjem 5G

2. Digitalne kompetence in vključenost

- Vsaj 80 odstotkov prebivalcev z vsaj osnovnimi digitalnimi kompetencami
- Vsaj 10 % zaposlenih IKT strokovnjakov
- Vsaj 25 % zaposlenih žensk glede na odstotek vseh zaposlenih v IKT

3. Digitalna preobrazba gospodarstva

Vlada Republike Slovenije je januarja 2022 sprejela Strategijo digitalne transformacije gospodarstva, v juniju 2021 pa Slovensko industrijsko strategijo 2021 – 2030. V DSI2030 opredeljujemo ključne usmeritve in cilje na področju digitalne preobrazbe gospodarstva. Kot ključno vidimo nadaljnjo usmeritev v družbo znanja in s tem blaginjo vseh prebivalcev Slovenije ter spodbujanje vlaganj v digitalne tehnologije. Tudi pri digitalni preobrazbi gospodarstva Slovenija sledi ciljem Digitalnega kompasa:

- Dodana vrednost na zaposlenega (2030: 88.000 EUR)
- Odstotek podjetij, ki najema umetno inteligenco* (2030: več kot 75 %)
- Odstotek podjetij, ki najema storitve računalništva v oblaku* (2030: več kot 75 %)
- Odstotek podjetij, ki uporabljajo velepodatke* (2030: več kot 75 %) – *zvezdica pomeni, da je cilj doseči enega od teh kazalnikov*

- Stopnja digitalizacije v podjetjih z več kot 10 zaposlenimi (2030: 53 %)
- Delež MSP, ki dosega vsaj osnovno stopnjo digitalne zrelosti (2030: 90 %)
- Odstotek podjetij, ki izvajajo usposabljanja za IKT (2030: 90 %)
- Odstotek MSP z internetno prodajo (2030: več kot 30 %)
- Odstotek MSP prihodka prek e-prodaje (2030: več kot 30 %)
- BDP na prebivalca glede na kupno moč je 95 % (glede na povprečje EU)

4. Pot v pametno družbo 5.0

Izpostavljamo, da nameravamo prehod v Pametno družbo 5.0 doseči z vključevanjem naprednih tehnologij v različne panoge in družbene dejavnosti ter spodbujanjem inovacij za ustvarjanje nove vrednosti.

V tem poglavju so določeni naslednji kazalniki spremljanja:

- Število zaposlenih, ki so opravili vsaj eno usposabljanje s področja podatkov je 5.000
- Število skrbnikov podatkov je 150
- Izvedba ukrepov iz NpUI je 100 %
- Vrednost lokalnega DESI-ja (indeks digitalnega gospodarstva in družbe na ravni občin, sestavljen iz različnih indikatorjev: človeškega kapitala, povezljivosti, integracije digitalnih tehnologij in digitalnih javnih storitev, trenutna vrednost: 23,44).

5. Digitalne javne storitve

Vlada Republike Slovenije je decembra 2022 sprejela Strategijo digitalnih javnih storitev 2030, katere vizija je, da bodo digitalne javne storitve, osredotočene na državljane in poslovne subjekte, omogočale integrirano, usklajeno, varno in učinkovito interakcijo državljanov in podjetij z javno upravo. Kazalniki na tem področju so sledeči:

- 100 % ključnih javnih storitev je zagotovljenih na spletu in dostopnih vsem uporabnikom
- 80 % ključnih javnih storitev, ki so dostopne digitalno, je tudi opravljenih digitalno
- 80 % uporabnikov javnih storitev uporablja digitalno identiteto.

6. Kibernetska varnost

Za uspešno digitalno preobrazbo je nujna tudi skrb za kibernetsko varnost. V DSI2030 kot eno od prioritetnih področij naslavljamo tudi to vsebino, pri čemer želimo zagotoviti varen, odporen in zanesljiv kibernetski prostora za vse ter s tem dvigniti raven kibernetske varnosti v Republiki Sloveniji v vseh segmentih družbe. Cilj DSI2030 na področju kibernetske varnosti je uvrstitev Slovenije med prvih dvajset najboljših držav po Nacionalnem indeksu kibernetske varnosti.

Krovni cilj strategije je spodbujanje digitalne preobrazbe Slovenije v vseh segmentih - družba, država, lokalne skupnosti in gospodarstvo.

Kazalnika doseganja cilja v DSI2030 nismo določili krovno, saj ugotavljamo, da DESI indeks ne vključuje nekaterih področij, ki so za nas izjemno pomembna. Cilje tako DSI2030 določa pri posameznih prednostnih vsebinskih področjih.

Naša vizija je, da z digitalno preobrazbo izboljšamo kakovost življenja prebivalcev na trajnosten in zaupanja vreden način.

Ker je digitalna preobrazba izjemno (ampak res izjemno) horizontalno področje, je za uspešno naslavljanje tega izziva ključno sodelovanje različnih deležnikov. DSI2030 določa, da je za upravljanje izvajanja strategije DSI2030 odgovorno ministrstvo, pristojno za digitalno preobrazbo. Za horizontalno in medresorsko usklajevanje digitalne preobrazbe pa Vlada Republike Slovenije imenuje posvetovalno telo, tj. strateški svet za digitalno preobrazbo.

Za učinkovito medresorsko koordinacijo projektov digitalne preobrazbe in za zasledovanje multiplikativnih sinergijskih razvojnih učinkov, imenuje ministrstvo, pristojno za digitalno preobrazbo, medresorsko delovno skupino za projekte digitalne preobrazbe.

Ob tem je pomembno dodati, da bo učinkovitost izvajanja in vrednotenja strategije ter iskanja priložnosti za dodatno izboljšanje proučevala tudi Evropska komisija, ki bo spremljala nacionalne programe projektov držav članic EU in jim po potrebi svetovala, kako ukrepati za vidnejši napredek k zastavljenim ciljem.

Predvidoma do letošnje jeseni bo pripravljen pripadajoči akcijski načrt strategije Digitalna Slovenija 2030. V njem bo določena pot (letne vrednosti) k doseganju v strategiji določenih ciljev s kazalniki. Opredeljeni bodo ukrepi in njihov pričakovani učinek na doseganje ciljev ter načrtovana javna finančna sredstva za ta namen.

To je lahko velik izziv ... Skupna pot je edina pot naprej k učinkoviti digitalni preobrazbi v vse hitreje spreminjajoči se družbi, zato se vsem, ki so doslej kakor koli sodelovali pri pripravi strategije Digitalna Slovenija 2030, na tem mestu zahvaljujemo za konstruktivno sodelovanje doslej in se veselimo sodelovanja tudi v prihodnje. ■

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

VARNOST, BREZ KOMPROMISOV

HUAWEI

Avtor: Vencel Cserháti / Vodja za kibernetsko varnost in varstvo zasebnosti
Huawei Technologies Madžarska in regija Adriatik

ZAGOTAVLJANJE VARNOSTI VAŠE OSKRBOVALNE VERIGE: NAJBOLJŠE PRAKSE ZA OBRAMBO PRED KIBERNETSKIMI NAPADI

Kibernetski napadi na oskrbovalne verige se krepijo. To pa viša stroške podjetjem, draži izdelke, poslabša uporabniške izkušnje ...

Dobavne in oskrbovalne verige so zadnja leta velike tarče kibernetskih napadalcev. Očitno je, zakaj. Če so kibernetski napadalci uspešni, bodo skoraj zagotovo dobili plačano visoko odkupnino, saj si podjetja ne morejo privoščiti izpada poslovanja in izgube ugleda. Lahko pa tudi ne plačajo zahtevane odkupnine in upajo na najboljše.

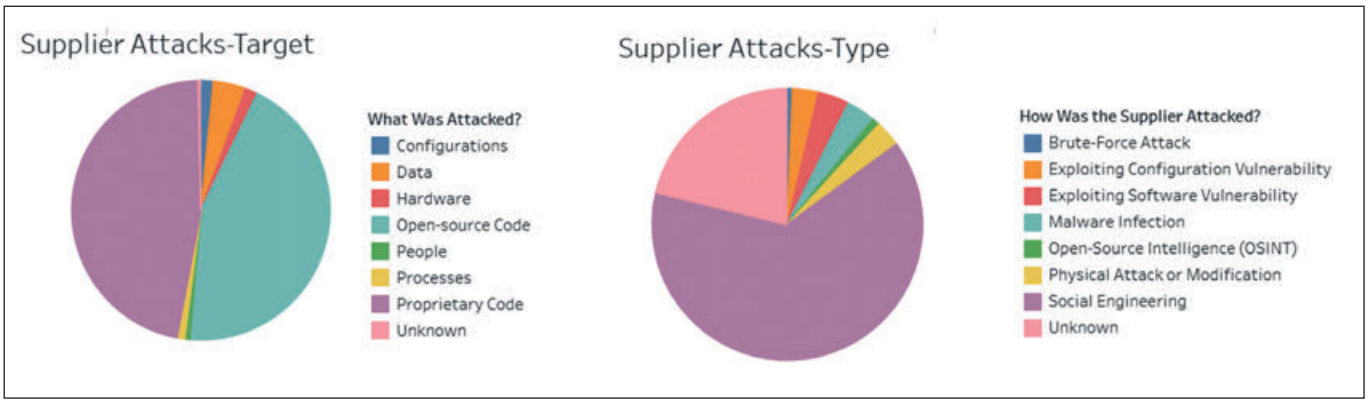
Ta scenarij se ni dobro končal za velikega dobavitelja v avtomobilski industriji. Napad z izsiljevalsko programsko opremo je lani za dlje časa povsem ohromil podjetje Kojima Industries Corporation, enega od glavnih dobaviteljev globalnega proizvajalca vozil. Ta je moral ustaviti proizvodnjo v 14 tovarnah (28 proizvodnih linij). Posledice so bile res hude: zaradi izpada delovanja sistemov je bilo podjetje primorano zmanjšati letno proizvodnjo za pet odstotkov, kar v številkah pomeni 13.000 ključnih sestavnih delov za vozila.

Stanje na področju zagotavljanja kibernetske varnosti v dobavnih verigah ni rožnato, a podjetja vendarle niso nemočna. Proaktivna pa mora postati celotna veriga, saj je ta močna le toliko, kolikor je močan najšibkejši člen.

Oskrbovalne verige zahtevajo celovito zaščito

Lansko poročilo o krajini digitalnih groženj, ki ga je objavila Agencija Evropske unije za kibernetsko varnost (ENISA), razkriva, da so napadi na oskrbovalne verige še vedno na seznamu 10 najpogostejših napadov. Ne le posamezna podjetja, težave se pojavljajo tudi pri ponudnikih programske opreme, saj napadalci skušajo že pri njih okužiti programsko opremo, ki jo uporabljajo podjetja v posamezni oskrbovalni verigi. S tem, ko okužijo programsko kodo, se lahko »pretihotapijo« v številna podjetja in izvedejo precej bolj nevarne in ciljno usmerjene napade.

Kompleksnost dobavne verige in odvisnosti od tretjih oseb oziroma drugih podjetij se bodo v sodobnem poslovnem svetu samo še povečevale, zato bodo morala podjetja pridobiti večji nadzor in pregled nad svojimi povezavami in odnosi z dobavitelji in odjemalci.



Slika 1: Vrste napadov na dobavne verige in najpogostejše tarče[1]

Napadalci izkoriščajo predvsem ranljivosti v programski opremi podjetij in tehnike socialnega inženiringa.

Glede na raziskavo družbe PricewaterhouseCoopers (PWC) je le 40 % vprašanih podjetij odgovorilo, da razumejo tveganja tretjih oseb in lastna kibernetska tveganja in tveganja v zvezi z zasebnostjo. Podobno ugotavlja raziskava podjetja BlueVoyant, kjer je 38 % vprašanih odgovorilo, da nimajo niti možnosti vedeti, kdaj in ali sploh pride do težav s kibernetsko varnostjo dobavitelja, torej tretje osebe v oskrbovalni verigi.

Varnostna tveganja velja kar najbolj zmanjšati

Stanje na področju zagotavljanja kibernetske varnosti v dobavnih verigah ni rožnato, a podjetja vendarle niso nemočna. Namesto, da podjetja zapoznelo reagirajo na varnostne incidente, ko ti že povzročijo veliko škodo, bi morala napadalce in škodljive kode proaktivno iskati in blokirati. Proaktivna pa mora postati celotna veriga, saj je ta močna le toliko, kolikor je močan najšibkejši člen. Na podlagi najnovejših rezultatov različnih študij in raziskav lahko podjetja izboljšajo svojo odpornost proti napadom in napadalcem v dobavni verigi na več načinov, in sicer:

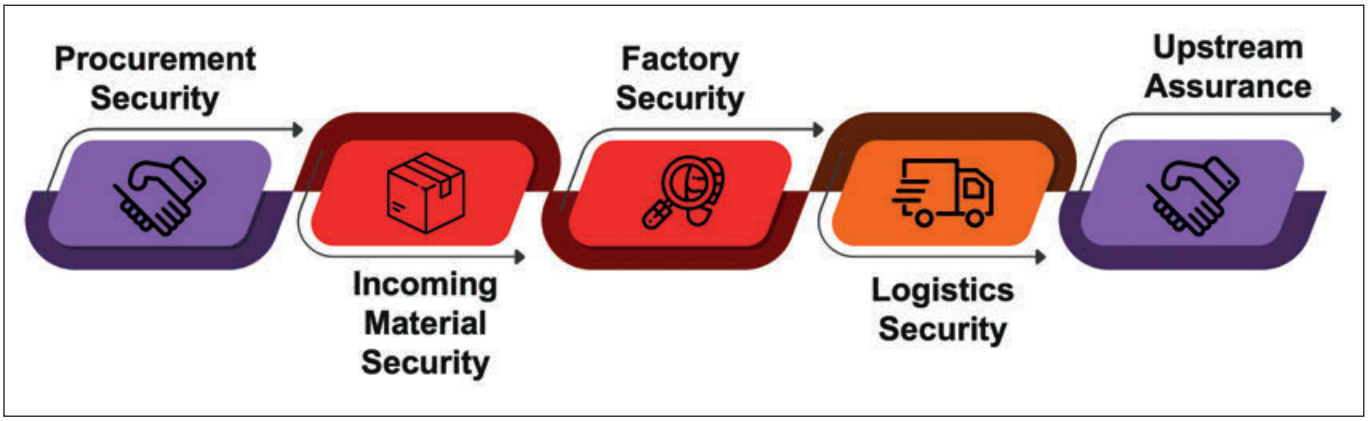
- **Večja osredotočenost na upravljanje tveganj.** Namesto, da podjetja zapoznelo reagirajo na varnostne incidente, ko ti že povzročijo veliko škodo, bi morala napadalce in škodljive kode proaktivno iskati in blokirati. Proaktivna pa mora postati celotna veriga, saj je ta močna le toliko, kolikor je močan najšibkejši člen. Preprosti vprašalniki, ali dobavitelj skrbi za kibernetsko varnost, niso dovolj, podjetja morajo zahtevati tehnične certifikate in potrdila o preverjanju varnosti.
- **Strožji, vendar pravični in nediskriminatorni predpisi.** Nekatere države že izvajajo strožje predpise za izboljšanje varnosti dobavne verige, zlasti na področju kibernetske varnosti in zasebnosti podatkov. Evropska komisija je utrla pot direktivi NIS2, ki tudi obravnava varnost dobavnih verig, in predstavila svojo strategijo kibernetske varnosti s predlogi za okrepitev obrambe in izboljšanje odzivanja na zlonamerne dejavnosti, ki vplivajo na dobavne verige. Oktobra lani so vlade EU pozvale k oblikovanju »evropske zbirke varnostnih orodij IKT za dobavne verige«, katere osnutek naj bi bil pripravljen v prvi polovici letošnjega leta.
- **Ozaveščanje glede t. i. notranjih groženj.** Podjetja bi se morala bolj zavedati tveganj, ki jih predstavljajo osebe z dostopom do notranjih informacij, kot so zaposleni, izvajalci in dobavitelji. Izobraževanje in ozaveščanje sta tako nuja, na ključnih položajih v podjetjih pa naj delujejo le ustrezno varnostno usposobljeni in tudi preverjeni kadri.
- **Diverzifikacija dobavnih verig za zmanjšanje tveganja nastanka motenj.** Podjetja naj preučijo alternativne možnosti pridobivanja virov, pa tudi lokalno ali bližnjo proizvodnjo oziroma dobavo, ki bi zmanjšala zapletenost dobavne verige in olajšala njeno varovanje.
- **Sodelovanje in izmenjava informacij sta ključnega pomena.** Sodelovanje med podjetji, vladami, ponudniki varnostnih rešitev in drugimi zainteresiranimi stranmi postaja vse pomembnejše za izboljšanje varnosti dobavne verige. To vključuje izmenjavo informacij o morebitnih grožnjah in najboljših praksah za obvladovanje tveganj, podobno kot že danes delujejo panožni varnostno-operativni centri.

Veriga mora biti zaščitena od začetka do konca

Danes so ocene tveganja sestavljene večinoma le iz preproste zahteve dobaviteljem, da izpolnijo vprašalnik glede varnostnih ukrepov, kar seveda ni dovolj. Podjetja, s katerimi posamezno podjetje sodeluje, izmenjuje podatke in gradi verigo, ki bi morala poskrbeti za redna varnostna preverjanja procesov in upravljanja informacij. To sicer traja dlje časa, vendar lahko pri tem podjetjem pomagajo tudi tehnični certifikati, opravljeni varnostni pregledi in t. i. penetracijski testi, ki dokazujejo naprednejšo raven varnostnega preverjanja. Tovrstna preverjanja bodo podjetjem dala ne le seznam razpok v njihovem digitalnem ščitu, temveč jih tudi usmerila v smer odprave ranljivosti.

Ker kibernetski napadalci vedno pogosteje uporabljajo tehnike socialnega inženiringa, s katerimi vedno uspešneje pretentajo oziroma prevarajo zaposlene, velja uvesti tudi varnostne rešitve, ki spremljajo aktivnosti zaposlenih. Obenem velja uvesti jasna varnostna pravila, gledati pod prste tudi morebitnim strokovnjakom, kot so zunanji izvajalci in vzdrževalci, ter jim takoj po opravljenih nalogah ukiniti vse dostope do IKT-virov podjetja.

Zgolj namestitev požarnih zidov in protivirusne programske opreme že dolgo ni več ustrezna kibernetska obramba. Žal podjetja na kibernetsko varnost gledajo le kot na strošek, ki ga želijo minimizirati, to pa pomeni vedno nove težave. Nekaj je jasno. Podjetja se proti napadalcem ne morejo braniti sama, vseeno pa morajo tudi na področju IKT in kibernetske varnosti poiskati sposobne in zaupanja vredne partnerje.



Slika 2: Huaweiev celostni pristop varnosti oskrbovalne verige[1]

Pred leti je direktorica informatike ameriške vesoljske agencije NASA zavrnila podpis pogodbe z velikim dobaviteljem opreme IKT v ZDA zaradi varnostnih težav pri dobavitelju. Nepodpis pogodbe bi lahko ogrozil njen položaj v agenciji NASA, vendar se je zavestno odločila za to potezo, saj je bil tako dobavitelj primoran kibernetsko varnost obravnavati prednostno. Ta primer ponazarja pomen kibernetske varnosti in skladnosti kot ključnih dejavnikov za doseganje zadovoljstva strank in pridobivanja zaupanja. V trenutku, ko lahko prodajalce in dobavitelje doletijo resne denarne posledice, vključno s prekinitvijo pogodbe, ti začno informacijsko in kibernetsko varnost jemati zelo resno. Vsak dobavitelj mora poskrbeti, da infrastruktura, ki se uporablja za načrtovanje, razvoj, proizvodnjo in dobavo izdelkov, sestavnih delov in storitev, upošteva dobre prakse glede kibernetske varnosti. Tudi postopki razvoja, vzdrževanja in podpore izdelkov morajo vključevati varnost in zasebnost podatkov.

Veriga je močna le toliko, kolikor je močan najšibkejši člen

Poleg tega dobavitelji ne smejo pozabiti na svoje lastne dobavitelje. Zagotavljanje kibernetske varnosti ne sme ostati le na papirju – s podpisom dogovorov glede varnosti in zasebnosti – temveč velja izvesti tudi preverjanje vseh odgovorov na vprašalnike, zahtevati ustrezne certifikate ter izvajati redne in priložnostne revizije (ob upoštevanju ravni tveganja dobavitelja). Čeprav se nekatere tehnične zahteve uporabljajo glede na kategorijo izdelkov in tveganja, na splošno upoštevanje znanih standardov, kot ISO/IEC 27001, IEC 62443-4-1, IEC 62443-4-2 (ali posebnih, kot je matrika kontrol v oblaku CSA), izboljšuje raven zaupanja v dobavitelje. Spremljanje varnostnih ranljivosti – o katerih poročajo notranji in zunanji viri – ne velja le za dobaviteljeve lastne izdelke in programsko opremo, temveč tudi za komponente tretjih oseb. Ko je ranljivost odkrita, mora podjetje, ki ga ranljivost zadeva, čim prej razviti popravek, ki mora prestati ustrezen postopek testiranja in preverjanja. Zelo pomembno je tudi, kako se taki popravki sporočijo in dostavijo/implementirajo strankam.

Pomembno je zagotoviti celovitost in točnost izvora vhodnih podatkov ali odprtokodne programske opreme, uporabljene v kateremkoli delu izdelka. Dobavitelji morajo uporabljati ustrezne tehnične in organizacijske kontrole za strojno in programsko opremo ter orodja in storitve tretjih oseb, ki so prisotne v procesih razvoja izdelkov ali programske opreme. Takšnega nadzora morda ni preprosto izvajati, vendar obstajajo rešitve, ki ga poenostavijo.

Medtem, ko je preverjanje varnosti zunanjih programskih komponent zaradi samodejnih orodij za preverjanje varnosti programske opreme nekoliko lažje, lahko preverjanje pristnosti in izvora strojnih komponent podjetjem predstavlja večji izziv. Huawei je na tem področju razvil številne dobre prakse in metode preverjanja, kot so razrez elektronskih komponent, rentgensko testiranje in avtomatsko merjenje impedance okvarne zanke strojne opreme.

Standardi in certifikati olajšajo zagotavljanje varnosti

Glede na priporočila strokovnjakov obstajajo trije ključni ukrepi, ki jih lahko upošteva vsako podjetje, da bi okrepilo varnost svoje dobavne verige. Najprej je treba varnostne kontrole vključiti v celoten življenjski cikel dobavne verige. Slednje zahteva sodelovanje in komunikacijo med vsemi vpletenimi stranmi. Drugič, preglednost in sledljivost, vgrajeni v izdelke in procese, pomenita večji ugled dobavitelja. Za kaj takega je najbolje, da se podjetja v dobavni verigi držijo dogovorjenih standardov delovanja. Nenazadnje lahko upoštevanje mednarodnih standardov na področju varnosti dobavne verige zagotovi več koristi, ki presegajo golo certificiranje rešitev in zaposlenih. Takšen pristop kaže zavezanost podjetja k najboljšim praksam pri varovanju dobavne verige, gradi zaupanje pri strankah in partnerjih ter zmanjšuje tveganje za varnostne incidente in motnje v dobavni verigi. Mednarodni standardi lahko obenem zagotovijo skupen imenovalec – skupen jezik in okvir za razpravo in obravnavo varnosti dobavne verige v različnih panogah in regijah. Prav zato so standardi in certifikati še kako dobrodošli. ■

1 Vir: https://www.comparitech.com/software-supply-chain-attacks/

2 Vir: Huawei

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

Varnostno-operativni center – **SOC**

Krepitev kibernetske odpornosti je ključnega pomena pri krepitvi poslovne odpornosti v digitalnem svetu.

Prednosti SOC

- Stroškovna učinkovitost
- Neprekinjena zaščita
- Izkušnje skupnosti z več kot 40.000 uporabniki
- Preprečevanje groženj
- Zabeleženih več kot 1.000 incidentov na leto
- Skladnost in poslovni ugled
- Visoka razpoložljivost varnostnih strokovnjakov

Storitve SOC

- Modeliranje groženj
- Zaznavanje incidentov
- Odziv na incidente
- Odkrivanje ranljivosti
- Vdorni testi in varnostni pregledi
- Varnostno preverjanje izvorne kode
- Avtentikacija in analiza zlonamerne kode
- Opredelitev varnostnih izhodišč
- Ozaveščanje in usposabljanje

s&t ISKRATEL

Avtorica: Tanja Permozer / vodja Slovenske vesoljske pisarne in vodja delegacije RS pri Evropski vesoljski agenciji

VESOLJSKE INDUSTRIJE IN PRILOŽNOSTI ZA SLOVENSKE ORGANIZACIJE

V prispevku želimo podrobneje predstaviti korake, ki jih Republika Slovenija in preko tega tudi slovenske organizacije, izvajajo na področju sektorja vesoljske industrije. Prehojena pot predstavlja odlično odskočno desko za razširitev sodelovanja in izvajanja smelejših korakov na tem zahtevnem in visoko konkurenčnem področju.

Področje vesoljske industrije je zelo obsežno in vanj se lahko vključijo podjetja iz najrazličnejših sektorjev: od prehrane, energije, telekomunikacij in navigacije, novih materialov in 3D tiskanja, kontrolnih sistemov, obdelave in hrambe velikih količin podatkov, novih načinov obdelave materialov, medicine, obrambe in številnih drugih.

Poleg tega ima sektor zaradi visoke stopnje inovativnosti tudi nadpovprečne učinke prelivanja. Primeri takega prelivanja so na primer uporaba laserske tehnologije razvite na področju vesoljske tehnologije za izvedbo očesnih operacij, uporaba infrardečih kamer prvenstveno razvitih za uporabo na satelitih za pametne naprave, uporaba inovativnih materialov razvitih za vesoljske objekte v letalski in avtomobilski industriji itd.

Tudi z vidika digitalnega gospodarstva ima vesolje vedno večjo vlogo, kar je prepoznal tudi Evropski parlament. Podatki, pridobljeni iz vesolja, lahko pomagajo okrepiti vodilno vlogo industrije na področju interneta stvari in avtomatizirane vožnje ter natančneje spremljati emisije toplogrednih plinov, kar bo povečalo učinkovitost podnebnih ukrepov. Tudi razvoj sodobnega, varnejšega, učinkovitega in trajnostnega prometa je tesno povezan z razvojem vesoljske tehnologije. Z navigacijskim sistemom in opazovanjem Zemlje so prometne storitve učinkovitejše. S tem se efektivno zmanjšujejo emisije. Razvoj vesoljskih tehnologij lahko pomaga pri spopadanju s podnebnimi spremembami, izboljšujejo se dostavne in poštne storitve, z boljšimi sistemi sledenja letalom pa se zmanjšuje hrup in število preklicanih letov.

Podatki, pridobljeni iz vesolja, lahko pomagajo okrepiti vodilno vlogo industrije na področju interneta stvari in avtomatizirane vožnje ter natančneje spremljati emisije toplogrednih plinov, kar bo povečalo učinkovitost podnebnih ukrepov.

Sodelovanje z Evropsko vesoljsko agencijo - ESA

Slovenija se je Evropski vesoljski agenciji (ESA) pridružila v letu 2016 s podpisom pridružitvenega sporazuma. V letu 2020 je svoj status nadgradila s podpisom nadgrajenega pridružitvenega sporazuma, ki predvideva postopno približevanje Slovenije k polnopravnemu članstvu v tej mednarodni agenciji.

Sporazum omogoča tudi izvedbo posebnih razpisov zgolj za slovenske deležnike (RPA), katerih namen je dodatno spodbujanje razvoja vesoljskih kapacitet v Sloveniji in zajema možnosti za začetne študije, razvoj tehnologije na področjih izven opcijskih programov, možnosti za pridobitev izkušenj v vesolju, pripravo tržnih aplikacij in razvoj študijskih programov na področju vesolja.

Slovenija je na ministrskem zasedanju Sveta ESA „CM22“, ki je potekalo v Parizu 22. in 23. 11. 2022, povečala finančni prispevek v programe ESA v naslednjih treh letih, in sicer s 3 milijonov EUR na 5,8 milijonov EUR letno.

Slovenija je potrdila sodelovanje v štirih izbirnih programih, v katerih je sodelovala do sedaj (GSTP – splošne tehnologije, EO – opazovanje Zemlje, E3P3 – človeške in robotske raziskave, znanstveni program Prodex) ter dodatno potrdila sodelovanje v programih (Digitalni dvojček Zemlje, InCubed) ter programu telekomunikacij (Artes).

Podjetja so:

- razvijala satelite in inštrumente zanje, kjer bi izpostavili tudi nove rešitve v smeri miniaturizacije in video posnetkov skoraj v realnem času
- razvijala aplikacije za uporabo satelitskih podatkov za najrazličnejše namene med drugim za monitoring stanja voda, suše in invazivnih rastlin, prostorske načrte, opozarjanje v primeru naravnih nesreč.
- Razvijala specialne nadzorne sisteme, sisteme za hitro obdelavo podatkov, še posebej za obdelavo in skladiščenje velikih količin podatkov, ki jih dobimo iz vesolja,
- z uporabo umetne inteligence in strojnega učenja nadgrajevala obstoječe aplikacije in podobno.
- razvijala so nove materiale, 3D tiskanje in postopke za obdelavo materialov, da se omogoči njihova uporaba v težkih razmerah v vesolju.
- septembra 2020 sta iz Francoske Gvajane v vesolje poletela prva dva slovenska satelita – Nemo HD (Vesolje.si) ter TriSat (Skylabs), junija 2022 pa že tretji satelit TrisatR.
- slovenski znanstveniki so na podlagi podatkov Ese raziskovali še neznana področja vesolja,
- v Planici pa se izvajajo »bed-rest« študije vpliva breztežnosti na človeški organizem.

Vesoljski sektor v Sloveniji je sicer še relativno majhen. Podjetja, ki se ukvarjajo zgolj s področjem vesoljske tehnologije so večinoma mala in mikro podjetja. Se je pa število zaposlenih v teh podjetjih od leta 2016, ko se je Slovenija začela intenzivneje ukvarjati s področjem vesoljske tehnologije, povečalo iz takrat 100 na današnjih 182 zaposlenih, kar predstavlja kar 82% rast. V Sloveniji trenutno skupno število podjetij in raziskovalnih inštitucij ter javnih zavodov, ki se ukvarjajo s področjem vesolja, presega 40 akterjev.

Podjetja so v zadnjem obdobju dosegla nekatere pomembne mejnike:

- v letu 2016 je slovensko podjetje Sinergise prejelo glavno nagrado na Copernicus Masters tekmovanju za razvoj orodja Sentinel Hub, ki omogoča enostavno in učinkovito arhiviranje, procesiranje in dostavo satelitskih posnetkov. Njihova rešitev je čas za prikaz in uporabo satelitskih posnetkov skrajšala z nekaj ur na le nekaj sekund. Ta projekt pa jih je tudi uvrstil med najvplivnejša podjetja na področju obdelave satelitskih podatkov v Evropi ter jim omogočil sodelovanje v vrsti najrazličnejših projektov tako v okviru ESE, programa Obzorje 2020 in komercialnih projektov. Podjetje Sinergise je, skupaj s partnerji v konzorciju T-Systems International, 2. decembra 2022 z Evropsko vesoljsko agencijo (ESA) ter Evropsko komisijo (EK) podpisalo šestletno pogodbo za vzpostavitev sistema za shranjevanje, procesiranje in distribucijo podatkov sistema Kopernikus (CDAS) v skupni vrednosti 150 milijonov EUR.
- septembra 2020 sta iz Francoske Gvajane v vesolje poletela prva dva slovenska satelita:

Slovenska vesoljska strategija 2030 je bila pripravljena z namenom, da usmerja in podpira našo hitro rastočo vesoljsko industrijo in raziskovalne dejavnosti na tem področju. To je še posebej pomembno z vidika prizadevanj Slovenije za polnopravno članstvo v Esa, kar je ena izmed prioritet Vlade.

- Nemo HD je mikro satelit Centra odličnosti Vesolje-SI z maso 65 kg za interaktivno daljinsko zaznavanje z visoko natančnostjo. Omogoča zajem multi spektralnih podob zemeljske površine ter snemanje videa visoke ločljivosti. Vesolje-SI je razvil tudi svojo premično zemeljsko postajo, ki se povezuje s satelitom. Zaenkrat je ta satelit še edini v Evropi, ki ima v vesolju delujoč video;
- TRISAT je nano satelit, ki je bil razvit, kot izobraževalna vesoljska misija Univerze v Mariboru, v sodelovanju s podjetjem SkyLabs. Pomemben je zaradi tehnološko-demonstracijskega vidika, saj je bila v okviru projekta razvita inovativna minimizirana vgrajena strojna in programska oprema, ki je po potrditvi delovanja v vesolju komercialno zelo zanimiva za vesoljsko industrijo;
- julija 2022 je bil prav tako iz Francoske Gvajane izstreljen tretji slovenski satelit: TRISAT R je nano satelit, razvit v sodelovanju med Univerzo v Mariboru in podjetjem Skylabs, ki je namenjen opravljanju meritev ionizirajočega sevanja v srednji Zemljini orbiti z namenom modeliranja okolja magnetosfere ter boljšega razumevanja vesoljskega vremena in je eden prvih nano satelitov, ki je letel tako visoko;
- Oktobra 2021 je v Nordijskem centru Planica potekala otvoritev Laboratorija za gravitacijsko fiziologijo Instituta »Jožef Stefan« (IJS) na podlagi instalacije človeške centrifuge, ki jo je ESA prenesla v Slovenijo zaradi uspešno izvedenih »bed rest« študij v hipoksičnem okolju tega centra, ki so jih izvajali predstavniki IJS. Laboratorij prispeva k raziskavam za ohranjanje zdravja in dobrega počutja astronavtov med prihodnjimi misijami v vesolje, hkrati pa tudi za življenje ljudi na Zemlji. S tem je center Planica postal eden od treh znanstveno raziskovalnih centrov ESE za izvajanje tovrstnih študij (poleg centrov v Nemčiji in Franciji) in edini, na katerem je možno izvajati »bed rest« študije v hipoksičnem okolju z uporabo centrifuge.

S ciljem promocije slovenske vesoljske industrije sta bila pripravljena tudi video s področja vesolja ter Katalog slovenske vesoljske industrije in raziskovalnih institucij.

Področje vesolja je bilo vključeno med prioritete slovenskega predsedovanja Svetu EU v drugi polovici l. 2021. V okviru Delovne skupine Sveta EU za vesolje so se pripravljali Sklepi Sveta „Vesolje za vsakogar“ in poročilo predsedstva na področju vesoljskega prometa (STM – Space Traffic Management).

Odbor Združenih narodov za miroljubno uporabo vesolja (Committee on the Peaceful Uses of Outer Space – COPUOS)

V začetku leta 2021 smo vložili uradno kandidaturo za članstvo v Odbor Združenih narodov za miroljubno uporabo vesolja (Committee on the Peaceful Uses of Outer Space – COPUOS). Slovenija je konec leta 2021 postala 100. država članica tega ključnega mednarodnega foruma za področje vesolja.

Ostale ključne mednarodne aktivnosti:

Ker je bilo na EXPO Dubai 2020 med izpostavljenimi temami tudi vesolje, je tudi Slovenija pripravila svojo delegacijo podjetij, ki so aktivna na področju vesolja. S tem se je predstavila kot država, aktivna na področju vesolja ter vzpostavila nove povezave z drugimi akterji na tem izrazito mednarodnem področju.

Tekom priprav na EXPO 2020 je bila Slovenija izbrana za polurno predstavitev v okviru Pre-EXPO 2020 – Space oktobra 2020, skupaj z državami kot so ZDA, Švica, RF.

Junija 2021 je bilo podpisano Pismo o nameri za sodelovanje med MGRT in Italijansko vesoljsko agencijo (ASI). Omenjeni dokument nudi dobro podlago za razvoj sodelovanja med slovenskimi in italijanskimi podjetji in raziskovalnimi institucijami. Tako sta bila organizirana že dva sestanka in s tem več kot 80 bilateralnih sestankov med slovenskimi in italijanskimi partnerji.

Področje sodelovanja na področju vesolja je tudi tema gospodarskih konzultacij med Slovenijo in Francijo. V mesecu juniju pripravljamo izhodno gospodarsko delegacijo v CNES.

Prav tako smo že vzpostavili povezavo z nemško vesoljsko agencijo DLR.

Aprila letos se je Slovenija tudi prvič udeležila največjega vesoljskega simpozija v Coloradu Springs, kjer so se slovenska podjetja s področja vesoljske industrije predstavila na skupni stojnici. Med drugim so se nadaljevali pogovori z NASO o sodelovanju pri različnih projektih in drugimi ameriškimi podjetji. Simpozij je letos gostil cca. 18.000 udeležencev, kar je 40 % več kot lani, kar nakazuje na hitro rast vesoljskega sektorja na globalni ravni.

Priprava nacionalne vesoljske strategije

V mesecu aprilu smo predstavili osnutek Slovenske vesoljske strategije 2030. Gre za prvi tovrstni dokument s področja vesolja.

Strategija zajema obdobje od leta 2023 do leta 2030. Pripravljena je bila na podlagi dokumenta »Analiza in prihodnje pozicioniranje slovenskega vesoljskega ekosistema« iz leta 2022 ter zavez Republike Slovenije na Svetu Ese na nivoju ministrov novembra 2022, kjer je bistveno povečala vplačana sredstva in se pridružila novim izbirnim programom.

Slovenska vesoljska strategija 2030 je bila pripravljena z namenom, da usmerja in podpira našo hitro rastočo vesoljsko industrijo in raziskovalne dejavnosti na tem področju. To je še posebej pomembno z vidika prizadevanj Slovenije za polnopravno članstvo v Esa, kar je ena izmed prioritet Vlade.

Vesoljski sektor je eden izmed najhitreje rastočih sektorjev, tudi v Sloveniji, za katerega so značilni veliki multiplikativni učinki na gospodarsko rast in zaposlovanje, zeleni digitalni prehod in razvoj raziskovalne dejavnosti. Pomen vesoljskega sektorja je prepoznan tudi v okviru EU, saj je področje vesolja vključeno v najrazličnejše programe od varnosti do inovativnosti. Vse to je še posebno pomembno v luči doseganja ciljev »Slovenija. Zelena. Ustvarjalna. Pametna.« Iz tega izhajata tudi vizija strategije: *»Slovenski prostor si prizadeva širiti meje znanja in inovacij ter navdihovati zeleno, digitalno in trajnostno prihodnost«* ter njena misija: *»Slovenija, ki se pozicionira kot dinamično vesoljsko gospodarstvo, želi spodbujati okolje, ki bo omogočalo inovacijski in tehnološki razvoj, da bi se tako povzpela med svojimi globalnimi tekmeci. Slovenska podjetja se zavedajo, da smo na prelomni točki, zato si prizadevajo za korak naprej pri njihovi uveljavitvi na mednarodnem prizorišču, tudi z uporabo lokalnega strokovnega znanja.«*

Naše ambicije iz vizije in poslanstva slovenske vesoljske strategije so se izoblikovale v vrsto dolgoročnih ciljev, ki tvorijo pet strateških stebrov za podporo razvoju sektorja.

Trije stebri so namenjeni reševanju programskih prednostnih področij:

- spodbujanje in razvoj vesoljih tehnologij ter raziskav in razvoja: razvoj tržno uspešnih izdelkov, primernih za vesolje, ki se lahko uporabljajo v tehnologijah na Zemlji ter prenos znanja na ne vesoljske sektorje;
- sodelovanje pri mednarodnem raziskovanju in proučevanju vesolja, kar vključuje tudi znanje in tehnologijo za izvedbo človeških in robotskih raziskovalnih misij, pri čemer tesno sodelujemo s tujimi partnerji; ter
- vesoljske aplikacije: pridobivanje in uporaba podatkov, pridobljenih iz vesolja, za različne namene na Zemlji.

Ostala dva stebra sta opredeljena za krepitev dejavnikov ekosistema:

- spodbujanje izobraževanja na področju znanosti, tehnologije, inženirstva in matematike (STEM) med prihodnjimi generacijami ter
- *širitev zmogljivosti Slovenije za podporo podjetništvu in razvoju programov za vesoljske inovacije z uporabo in nadgradnjo obstoječih shem za podporo podjetništvu ter spin*-offov univerz in raziskovalnih institucij.

Status Slovenije v ESI

Pridružitveni sporazum z ESO poteče konec leta 2024, trenutno potekajo intenzivne priprave na polnopravno članstvo, ki vključujejo tudi sprejem nacionalne vesoljske strategije, ki je eden od formalnih pogojev za polnopravno članstvo; poleg geografskega povračila, ki mora biti vsaj 85% in razmerje projekti industrija/institucije 75%. ■

Avtor: Jure Habbe / operativni direktor, Silver Bullet Risk

OPTIMIZACIJA IN DIGITALIZACIJA UPRAVLJANJA TVEGANJ PRI UPRAVLJAVCIH KRITIČNE INFRASTRUKTURE IN IZVAJALCIH BISTVENIH STORITEV

Upravljavci kritične infrastrukture in izvajalci bistvenih storitev zagotavljajo zmogljivosti, ki so ključnega pomena za našo državo, zato bi imela večja prekinitev njihovega delovanja resne posledice za nacionalno varnost, gospodarstvo in druge pomembne družbene aktivnosti ter zdravje, varnost in blaginjo prebivalcev.

Vendar pa je vsaka organizacija pri svojem delovanju izpostavljena nevarnostim, ki presegajo običajne motnje in lahko resno ogrozijo njene dejavnosti ter v skrajnem primeru celo njen obstoj. Za zmanjšanje in obvladovanje takšnih nevarnosti oziroma tveganj, so upravljavci kritične infrastrukture in izvajalci bistvenih storitev dolžni izpolnjevati zahteve o upravljanju tveganj, ki jih predpisujeta Zakon o kritični infrastrukturi (Ur.l. RS št. 75/17) in Zakon o informacijski varnosti (Ur.l. RS št. 30/18), s pripadajočimi navodili.

V praksi opažamo, da se upravljanje neprekinjenega poslovanja večkrat zamenjuje z varnostnimi načrti, ki so samo njegov del, zato povzemimo bistvo.

Ker se pri sodelovanju z zavezanci na omenjenem področju večkrat srečujemo s podobnimi vprašanji in dvomi, v nadaljevanju predstavljamo nekatere rešitve, s katerimi lahko pri upravljanju tveganj dosežemo boljše in predvsem praktično uporabne rezultate.

Metodologija za analizo tveganj

Temelj za učinkovito upravljanje je analiza tveganj, s katero prepoznamo, ocenimo in razvrstimo tveganja po pomembnosti glede na možne posledice njihove uresničitve.

Usmeritve za analizo tveganj določata Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije (Ur.l. RS, št. 7/19) in Pravilnik o varnostni dokumen-

taciji in varnostnih ukrepih izvajalcev bistvenih storitev (Ur.l. RS, št. 8/23).

Pozornemu bralcu zagotovo nista ušla različna izraza, ocenjevanje in analiza tveganj, pri čemer je primernejši slednji, ker je širši pojem. Vendar to ni edina razlika, ki jih je med obema dokumentoma še precej več. Zato bi upravljavcem kritične infrastrukture in izvajalcem bistvenih storitev izpolnjevanje predpisanih zahtev precej olajšala enotna metodologija za analizo in upravljanje tveganj, ki bi upoštevala tudi smernice standarda za informacijsko varnost ISO 27001 in standarda za upravljanje tveganj ISO 31000.

Tako bi pridobili celovita izhodišča za vsako poslovno okolje, ki bi jih zagotovo upoštevale številne gospodarske in negospodarske organizacije.

Procesni pristop pri analizi tveganj

Navodilo za ocenjevanje tveganj kritične infrastrukture in analiza tveganj v pravilniku za izvajalce bistvenih storitev se razlikujeta že v osnovah. Medtem, ko prvi izhaja iz virov tveganj in posledic njihove uresničitve, so pri drugem v ospredju sredstva ter grožnje in ranljivosti. Zato se pri uvajanju njunih določil večkrat pojavlja vprašanje, ali in kako lahko zadostimo obema hkrati.

Delovanje kritične infrastrukture in bistvenih storitev temelji na ključnih obratovalnih in poslovnih procesih. Za izvajanje procesov potrebujemo sredstva, kot so objekti, kadri, stroji, surovine in materiali, strojna in programska oprema, omrežja, energenti in druga. Uresničitve tveganj, ki vplivajo na ključna sredstva in posledično na procese, pa lahko prekinejo njihovo delovanje in s tem razpoložljivost kritične infrastrukture in bistvenih storitev.

Ob upoštevanju procesnega pristopa lahko osnovno analizo tveganj izdelamo v naslednjih korakih:

- **Procesi:** Določimo procese, ki so ključni za nemoteno delovanje kritične infrastrukture in bistvenih storitev.
- **Sredstva:** Za procese določimo sredstva, ki so ključnega pomena za njihovo delovanje.
- **Tveganja:** Za sredstva opredelimo tveganja, ki lahko bistveno vplivajo na njihovo delovanje, ter jih delimo na grožnje kot zunanje dejavnike, in ranljivosti kot notranje dejavnike.
- **Verjetnost in vpliv:** Za tveganja določimo verjetnost uresničitve in vpliv na celoten proces in ne zgolj na posamezno sredstvo.
- **Stopnja tveganja:** Za tveganja izračunamo stopnje in jih razvrstimo od največje do najmanjše, s čimer pridobimo pregled nad pomembnostjo tveganj.

Na podlagi rezultatov izpolnimo še preostale zahteve in s tem določila obeh navedenih predpisanih usmeritev.

Kvalitativne in kvantitativne metode ocenjevanja tveganj

Kot vemo, imamo za ocenjevanje tveganj na razpolago kvalitativne in kvantitativne metode.

Pri kvalitativnih pristopih verjetnost in vpliv uresničitve tveganj ocenjujemo opisno (npr. malo, srednje, visoko) in/ali številčno (npr. 1 do 3) ter tveganja običajno razvrščamo matrično. Pri kvantitativnih pristopih pa so ocene merljive, kar pomeni izračun verjetnosti in finančni vpliv uresničitve tveganj, pri razvrščanju pa lahko uporabimo t.i. profil tveganj, ki nazorno prikazuje največja tveganja.

Čeprav so mnogo bolj razširjeni kvalitativni pristopi, ker so preprostejši za razumevanje in uporabo, je njihova uporabna vrednost močno omejena, kar je razloženo v številnih člankih in več knjigah. Zato je pomemben napredek pri ocenjevanju tveganj kvantitativni ali merljivi pristop, s katerim določimo finančne ocene tveganj. Ker je denar univerzalni pojem za komunikacijo v poslovnem okolju, tako olajšamo obravnavanje tveganj med poslovnimi in tehničnimi sogovorniki ter lažje poenotimo ocenjevane kriterije na različnih področjih. Hkrati pa prispeva k nazornejšim predstavam o pomenu in predvsem možnih posledicah uresničitve tveganj.

Upravljanje neprekinjenega poslovanja

Pomembno področje in obveznost upravljavcev kritične infrastrukture in izvajalcev bistvenih storitev je upravljanje neprekinjenega poslovanja. Kljub vsem preprečevalnim ukrepom in skrbnemu ravnanju se nekatera tveganja uresničijo ter prekinejo izvajanje procesov in razpoložljivost njihovih storitev. **Namen učinkovitega sistema neprekinjenega poslovanja pa je, da se na prekinitve odzovemo organizirano in sistematično ter, da vsem prizadetim povzročijo čim manj škode.**

V praksi opažamo, da se upravljanje neprekinjenega poslovanja večkrat zamenjuje z varnostnimi načrti, ki so samo njegov del, zato povzemimo bistvo.

Splošno uveljavljene zahteve in smernice za upravljanje neprekinjenega poslovanja opisuje standard ISO 22301, ki je dobro poznan tudi v našem poslovnem okolju. Podobno kot upravljanje tveganj temelji na določitvi ključnih procesov, za katere z analizo vplivov na poslovanje (ang. Business Impact Analysis – BIA) ugotovimo ključne zahteve za okrevanje ob prekinitvah. Poleg tega je del učinkovitega sistema upravljanja neprekinjenega poslovanja tudi obvladovanje tveganj. To nam omogoča preventivno delovanje oziroma zmanjšanje možnosti nastopa prekinitev ter usmeritev aktivnosti načrtovanja neprekinjenega poslovanja v odziv na tveganja, ki jih ne moremo preprečiti.

Dokumentacija sistema neprekinjenega poslovanja obsega tri nivoje. Prvi je krovna politika, ki izraža zavezanost vodstva k doseganju ciljev neprekinjenega poslovanja. Sledi strategija, ki temelji na rezultatih analize vplivov na poslovanje in obravnava različne scenarije uresničitve tveganja ter vzpostavitve razpoložljivosti storitev. Na tretjem nivoju pa so operativni – ali varnostni – načrti za ukrepanje v primeru dejanskih kriznih razmer. Temu sledi uvajanje sprejetih določil v prakso ter redno testiranje, dopolnjevanje in izpopolnjevanje načrtov na podlagi doseženih rezultatov, kot proces stalnih izboljšav.

Digitalizacija upravljanja tveganj

Čeprav govorimo predvsem o analizah, so upravljavci kritične infrastrukture in izvajalci bistvenih storitev dolžni tudi načrtovati in izvajati ukrepe za zmanjševanje tveganj ter evidentirati škodne dogodke, kot uresničena tveganja.

Ukrepe predstavljajo predvidene aktivnosti, odgovorni nosilci in izvajalci, časovni roki ter na primer stopnja izvedbe in učinkovitosti ukrepov. Podobno velja za škodne dogodke oz. incidente, kjer poleg podatkov o incidentih prav tako izvajamo popravljalne (korektivne) in preprečevalne (preventivne) ukrepe, da se ne ponovijo.

Celoten proces upravljanja tveganj vključuje podatke, izračune, preglede in poročila, ki jih težko učinkovito obvladujemo v preprostih preglednicah in tekstovnih datotekah. Zato me ne čudi, da na primer v kompleksnejših organizacijah, za zbiranje in obdelavo podatkov za poročanje nadzornim organom, porabijo veliko časa. Polega tega pa ne moremo zagotoviti ustrezne ravni varnosti podatkov o tveganjih, ki so običajno zaupni.

Učinkovitemu obvladovanju procesov in podatkov pri upravljanju tveganj je namenjena digitalizacija, ki jo omogoča na primer informacijska rešitev Silver Bullet Risk, ki upravljavcem kritične infrastrukture in izvajalcem bistvenih storitev omogoča lažje izpolnjevanje zakonskih obveznosti pri vseh ključnih dejavnostih, kot so analize tveganj, načrtovanje in izvajanje ukrepov ter evidentiranje škodnih dogodkov.

Zaključek

Čeprav upravljanje tveganj pri upravljanju kritične infrastrukture in izvajanju bistvenih storitev ni pretirano zapleteno, potrebujemo za zakonsko skladne in praktično uporabne rešitve določeno znanje in izkušnje. Pridobimo jih lahko samostojno z učenjem na lastnih napakah, kar pa ima lahko občutne posledice. Druga možnost pa je, da poiščemo strokovno pomoč, s katero obveznosti in druge cilje pri upravljanju tveganj dosežemo lažje in hitreje. ■

Praktične rešitve za upravljanje tveganj na področju kritične infrastrukture in izvajanja bistvenih storitev

Zakon o kritični infrastrukturi in Zakon o informacijski varnosti s pripadajočimi navodili od upravljavcev kritične infrastrukture in izvajalcev bistvenih storitev med drugim zahtevajo, da analizirajo tveganja ter izvajajo ukrepe za njihovo obvladovanje in evidentirajo škodne dogodke.

V čem je težava?

V praksi je precej izzivov že pri analizi tveganj sredstev in virov v skladu z načeli celovitosti, razpoložljivosti in zaupnosti.

Nalogo dodatno otežujejo neskladja med navodili, ki se jim običajno pridružujejo še usmeritve in zahteve standardov za informacijsko varnost ISO/IEC 27000.

Nepriročno in varnostno vprašljivo pa je tudi obvladovanje podatkov v preprostih preglednicah in podobnih evidencah, na podlagi katerih poročamo in dokazujemo skladnost nadzornim organom.

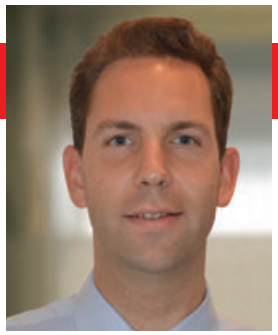
Kako vam lahko pomagamo?

Upravljavcem kritične infrastrukture in izvajalcem bistvenih storitev lahko pomagamo na več načinov, kot so:

- Svetovalna podpora pri izdelavi analize tveganj in vzpostavitvi celovitega sistema upravljanja tveganj, ki upošteva zahteve predpisov in standarda ISO/IEC 27001.
- Informacijska rešitev Silver Bullet Risk za obvladovanje podatkov o tveganjih, ukrepih in škodnih dogodkih ter pripadajoča poročila na enem mestu.
- Sodelovanje pri načrtovanju in uvajanju sistemov neprekinjenega poslovanja v skladu s standardom ISO 22301.

Za več informacij ali pogovor nam pišite na naslov **info@silverbulletrisk.com**.

Avtor: dr. Andrej Bregar / Informatika d.o.o.*



PROCES UPRAVLJANJA PREMOSTITVENIH UKREPOV PROTI KIBERNETSKIM GROŽNJAM

V prispevku bo predstavljeno, zakaj je pomemben in kako ga udejaniti-dobra praksa iz projekta CyberSEAS. Kibernetska varnost postaja v korporativnih okoljih vse kompleksnejša in vse bolj pomembna. Še zlasti to velja za sisteme kritične infrastrukture, ki so nacionalnega pomena in morajo zadostiti najstrožjim zahtevam po neprekinjenem poslovanju.

Uvod

V trenutnih geopolitičnih razmerah so posebej izpostavljeni energetski sistemi, v katerih predstavljajo dodatno raven kompleksnosti integracije informacijskih in procesnih tehnologij, obseg in soodvisnost infrastrukturnih virov ter povezovanje številnih deležnikov v proizvodnih in dobavnih verigah. Zato v tovrstnih sistemih nikakor ne smemo pasivno čakati, da pride do kibernetskega napada ter da le-tega zaznamo, se nanj odzovemo in ga zajezimo. Po statistikah za leto 2022 je namreč povprečni čas do odprave posledic kibernetskega napada kar 277 dni. Takšen odzivni čas je pogosto nesprejemljiv in ostaja na približno enaki ravni kot v preteklem desetletju. Eden obetavnejših in bržkone ključnih pristopov v korporativni in kibernetski varnosti so tako premostitvene strategije in ukrepi, po katerih lahko posežemo, da proaktivno preprečimo ali zmanjšamo učinke varnostnih groženj in povečamo splošno odpornost organizacij, korporativnih in tehnoloških sistemov ter informacijskih, komunikacijskih in procesnih infrastruktur.

Premostitev tveganj je strategija, po kateri lahko organizacije posežejo z namenom prepoznavanja, ocenjevanja in zmanjševanja učinkov poslovnih, varnostnih, kibernetskih ali drugih tveganj, groženj in napadov. Je del procesa upravljanja tveganj in omogoča organizacijam, da se pripravijo na tveganja, povezana z delovnimi procesi, aktivnostmi, storitvami in informacijsko-komunikacijsko infrastrukturo.

Premostitev tveganj

Premostitev tveganj je strategija, po kateri lahko organizacije posežejo z namenom prepoznavanja, ocenjevanja in zmanjševanja učinkov poslovnih, varnostnih, kibernetskih ali drugih tveganj, groženj in napadov. Je del procesa upravljanja tveganj in omogoča organizacijam, da se pripravijo na tveganja, povezana z delovnimi procesi, aktivnostmi, storitvami in informacijsko-komunikacijsko infrastrukturo. Bistveno je, da organizacije izboljšajo razumevanje tveganj, jih sprejmejo in se nanje vnaprej pripravijo. Tako imajo v primeru neželenih dogodkov na voljo ustrezne ukrepe za zmanjšanje negativnih učinkov in posledic tveganj. To omeji škodo, ki lahko nastane v povezavi z viri, delovanjem in ugledom, ter je pomemben dejavnik za zagotavljanje neprekinjenega poslovanja.

Naš cilj naj bo, da se pripravimo na grožnje, ocenimo njihov vpliv in postavimo prioritete glede pristopa ter ukrepov za

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

njihovo omejevanje. Osnovni koncept ni izogibanje grožnjam in popolno preprečevanje kibernetskih incidentov, temveč oblikovanje strategije, ki obravnava posledice incidenta ter vpelje zaporedje akcij, ki jih izvedemo še pred morebitnim varnostnim dogodkom, kar zmanjša kratkoročne in dolgoročne negativne učinke. Pogosto je dovolj, če se organizacije zavedajo, da lahko do incidentov pride, in imajo vzpostavljene mehanizme, s katerimi se le-te soočijo.

V sklopu evropskega razvojno-raziskovalnega projekta Horizon 2020 CyberSEAS smo v skladu s temi izhodišči vpeljali sistematičen proces upravljanja, ocenjevanja in izvedbe premostitvenih ukrepov proti kibernetskim tveganjem in grožnjam. Proces smo primarno zasnovali za sisteme elektroenergetske kritične infrastrukture, vendar je primeren in učinkovit tudi v sklopu drugih korporativnih okoljih.

Ocenjevanje in izbira premostitvenih ukrepov

Kibernetsko odpornost informacijske, procesne ali poslovne infrastrukture je možno zagotoviti z udejanjanjem dveh strategij – proaktivne in reaktivne. Pri prvem pristopu skušamo predvideti in oceniti kibernetska tveganja, grožnje in ranljivosti. Na podlagi teh ocen implementiramo ustrezne premostitvene ukrepe, s katerimi želimo vnaprej preprečiti kibernetske napade, do katerih bi lahko prišlo, oziroma zagotovimo, da imajo ti napadi karseda majhen vpliv, v kolikor se zgodijo. Pri drugi strategiji pa neprenehoma aktivno spremljamo informacije in dogodke, povezane s kibernetsko varnostjo, pri čemer nam lahko izdatno pomagajo sistemi, kakršni so SIEM (Security Information and Event Management) in SOAR (Security Orchestration, Automation and Response). Čim zaznamo kibernetski napad, sprožimo ustrezne premostitvene ukrepe in odzivne procedure, s katerimi omilimo ali odstranimo učinke in posledice napada.

Za obe strategiji velja, da je potrebno izbrati in implementirati enega ali več premostitvenih ukrepov, s katerimi zagotovimo neprekinjenost poslovanja. Ker pa pomeni izvedba vsakega ukrepa strošek in ker utegne imeti ukrep zgolj omejen učinek, je bistvenega pomena oceniti primernost in učinkovitost posameznega potencialnega premostitvenega ukrepa na podlagi več vidikov, ki upoštevajo značilnosti infrastrukture, zrelost razpoložljivih tehnologij in procesov za zagotavljanje kibernetske varnosti, organizacijske omejitve, korporativne cilje in resnost kibernetskih incidentov. Ključno vlogo tako igra sistematičen odločitveni pristop.

Osnovni in običajni pristop k ocenjevanju varnostnih tveganj sloni na uporabi matrike tveganj, ki jo lahko kombiniramo z zaporedjem vprašanj in naborom odločitvenih pravil, ki združujejo odgovore na več hierarhičnih nivojih. Takšen način ocenjevanja praviloma sledi standardu ISO 31000, ki določa proces upravljanja tveganj. Druga možnost je uporaba standardne ocene ranljivosti CVSS (Common Vulnerability Scoring System), ki jo pridobimo iz NIST-ove baze ranljivosti NVD (National Vulnerability Database) na podlagi podatkov o vseh poznanih in zabeleženih ranljivostih. Za kompleksnejše domene, med katere uvrščamo sisteme energetske kritične infrastrukture, pa priporočamo celovitejši pristop. Takšen odločitveni model sledi priporočilom NIST o upravljanju informacijskih varnostnih tveganj, po katerih poteka odločanje na treh nivojih – organizacijskem, poslovnem in informacijskem. Na nivoju informacijskega sistema varnostni analitiki raziščejo in analizirajo informacije o varnostnih dogodkih. Te informacije nato odločevalci na poslovnem in procesnem nivoju uporabijo za izbiro najprimernejših premostitvenih ukrepov in strategij. Odločitev mora upoštevati organizacijske in poslovne zahteve ter tolerančne omejitve ocenjenih organizacijskih tveganj. Organizacijski nivo je zato zadolžen za potrditev ustreznosti odločitve ter mora zagotoviti vire za implementacijo izbranih premostitvenih ukrepov in strategij. Večnivojsko korporativno odločanje tako zahteva sodelovanje skupine odločevalcev. Poleg tega vključujejo kompleksni sistemi množico povezanih informacijskih in infrastrukturnih virov, ki so lahko sočasno ogroženi zaradi medsebojnih odvisnosti in kaskadnih učinkov napadov. Ti viri pogosto pripadajo različnim deležnikom, kar odpira še en nivo skupinskega usklajevanja in odločanja.

> Priporočljivo je, da ocenitev na nivoju informacijskega sistema opravi tehnično osebje, ocenitev na nivoju poslovnega procesa pa je v domeni poslovnih odločevalcev.

Priporočljivo je, da ocenitev na nivoju informacijskega sistema opravi tehnično osebje, ocenitev na nivoju poslovnega procesa pa je v domeni poslovnih odločevalcev. Tehnične zahteve pokrijejo splošni kriteriji za varnost informacijskih sistemov po standardu ISO/IEC 15408. Mednje spada vpliv na korporativno okolje, ki ga določimo na osnovi števila ogroženih virov in medsebojnih odvisnosti teh virov. Pomembno je, da varnostni analitiki presodijo tudi vpliv premostitvenih ukrepov na atribute informacij – razpoložljivost, celovitost in zaupnost.

Želeni učinek premostitvenega ukrepa ali strategije je, da zmanjša vpliv kibernetske grožnje ali napada. Iz tega razloga

Takšen proces smo vpeljali v sklopu projekta CyberSEAS kot dobro prakso varovanja in povečanja odpornosti evropske energetske kritične infrastrukture. Podprli smo ga z odločitvenim orodjem, med njegove sestavne dele pa smo vključili še premostitvena ogrodja in modele za korporativno odločanje.

je potrebno najprej oceniti vplive zaznanih groženj in incidentov na infrastrukturne vire. S tem namenom posežemo po ločenem ocenitvenem modelu, ki upošteva kriterije za ocenjevanje vplivov infrastrukturnih odpovedi po priporočilih organizacije NESCOR. Odločitveni proces tako sestoji iz dveh zaporednih faz. V prvi fazi ocenimo vplive incidentov, v drugi pa učinkovitost premostitvenih ukrepov in strategij za te incidente. Fazi sta korelirani, kar pomeni, da je ocenjena učinkovitost ukrepa odvisna od začetnega vpliva incidenta.

Proces upravljanja premostitvenih ukrepov

Proces upravljanja premostitvenih ukrepov mora biti usklajen s tremi splošnimi procesi – odločanja, upravljanja tveganj in odzivanja na incidente. Prične se s fazo inteligence, v kateri določimo kontekst, identificiramo ogrožene vire in njihove ranljivosti ter zbiramo in obogatimo varnostne informacije. Sledi faza analize in oblikovanja, v sklopu katere identificiramo potencialne premostitvene ukrepe in strategije ter prilagodimo večkriterijske modele za ocenitev in izbiro specifikam naše infrastrukture in korporativnega okolja. Sledi faza ovrednotenja, izbire in odločitve, ki sledi priporočilom, podanim v predhodnem razdelku. Izbrane premostitvene ukrepe na koncu implementiramo. Pomembno je zbrati povratne informacije o učinkovitosti implementacije, t.j. o dejanski izboljšavi odpornosti ter stroških in virih, ki so bili potrebni. To dolgoročno izboljšuje celoten proces in omogoči inteligenco kibernetskih tveganj oziroma širšo izmenjavo informacij o kibernetskih tveganjih med organizacijami in CERT-i.

Izhodišče za odločanje so zaznani ali predvideni varnostni dogodki. Povezani dogodki lahko odražajo enega ali več kibernetskih napadov, pri čemer je v skladu z ogrodjem MITRE ATT&CK posamezen napad realiziran z uporabo ene ali več standardnih tehnik napadov. V tem kontekstu se premostitveni ukrep ali premostitvena strategija nanašata na eno ali več aktivnosti, ki jih je potrebno izvršiti za odpravo ali zmanjšanje vpliva varnostnih dogodkov. Strategija nadgrajuje koncept ukrepa na takšen način, da gre za zaporedje več ukrepov, ki jih s sinergijskimi učinki izvedemo v povezavi.

V sklopu odločitvenega procesa poiščemo potencialno primerne premostitvene ukrepe na podlagi ogroženih infrastrukturnih virov in identificiranih kibernetskih incidentov ali groženj. Premostitveno ogrodje zato vpelje nabor preslikav in pravil, na podlagi katerih je možno pridobiti začetno množico premostitvenih ukrepov, iz katere lahko varnostni strokovnjaki in odločevalci izberejo najprimernejše ukrepe za implementacijo. Množica premostitvenih ukrepov ter pripadajočih preslikav virov, tehnik napadov in zaznanih kibernetskih incidentov tako predstavlja organizacijsko bazo varnostnega znanja. Pri identifikaciji tehnik napadov, splošnih ranljivosti in premostitvenih ukrepov, pa si pomagamo tudi s standardnimi podatkovnimi bazami, kot je baza NVD.

Postopek identifikacije se prične z določitvijo standardne oznake CPE (Common Pattern Enumeration), ki opiše osnovne lastnosti ogroženega infrastrukturnega vira. Le-ta omogoči, da iz baze NVD pridobimo nabor splošno znanih ranljivosti vira, ki so lahko v obliki CVE (Common Vulnerabilities and Exposures) ali v obliki CWE (Common Weakness Enumeration). Za vsako ranljivost je možno poiskati tudi splošno oceno ranljivosti po sistemu CVSS. Ta predstavlja standardno metodo za ocenjevanje stopnje resnosti ranljivosti v IT sistemih z upoštevanjem večjega števila kriterijev, ki zajemajo bazične metrike, časovne metrike in metrike okolja. Oceno CVSS upoštevamo kot enega od objektivnih ocenitvenih kriterijev, vendar pa zaradi splošnosti ni nujno zadostna za samostojno obravnavo, saj ne upošteva značilnosti specifičnega okolja, v okviru katerega implementiramo premostitvene ukrepe. Na osnovi zaznanih incidentov, ali identificiranih ranljivosti, lahko v zadnjih korakih postopka poiščemo standardne tehnike napadov in jih preslikamo v nabor razpoložljivih premostitvenih ukrepov in strategij, med katerimi izberemo najučinkovitejše za implementacijo.

Za učinkovito upravljanje premostitvenih ukrepov je ključno, da uporabimo ustrezno ogrodje, ki vpelje standardno klasifikacijo in nabor premostitvenih ukrepov. Posežemo lahko po nekaterih uveljavljenih ogrodjih, med katerimi velja izpostaviti MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), CIS (Center for Internet Security) Critical Security Controls in strategije ACSC (Australian Cyber Security Centre). Uvedemo pa lahko tudi lastno ogrodje, ki združuje ukrepe in dobre lastnosti omenjenih standardnih premostitvenih ogrodij ter je prilagojeno infrastrukturi, ki jo varujemo.

Sklep

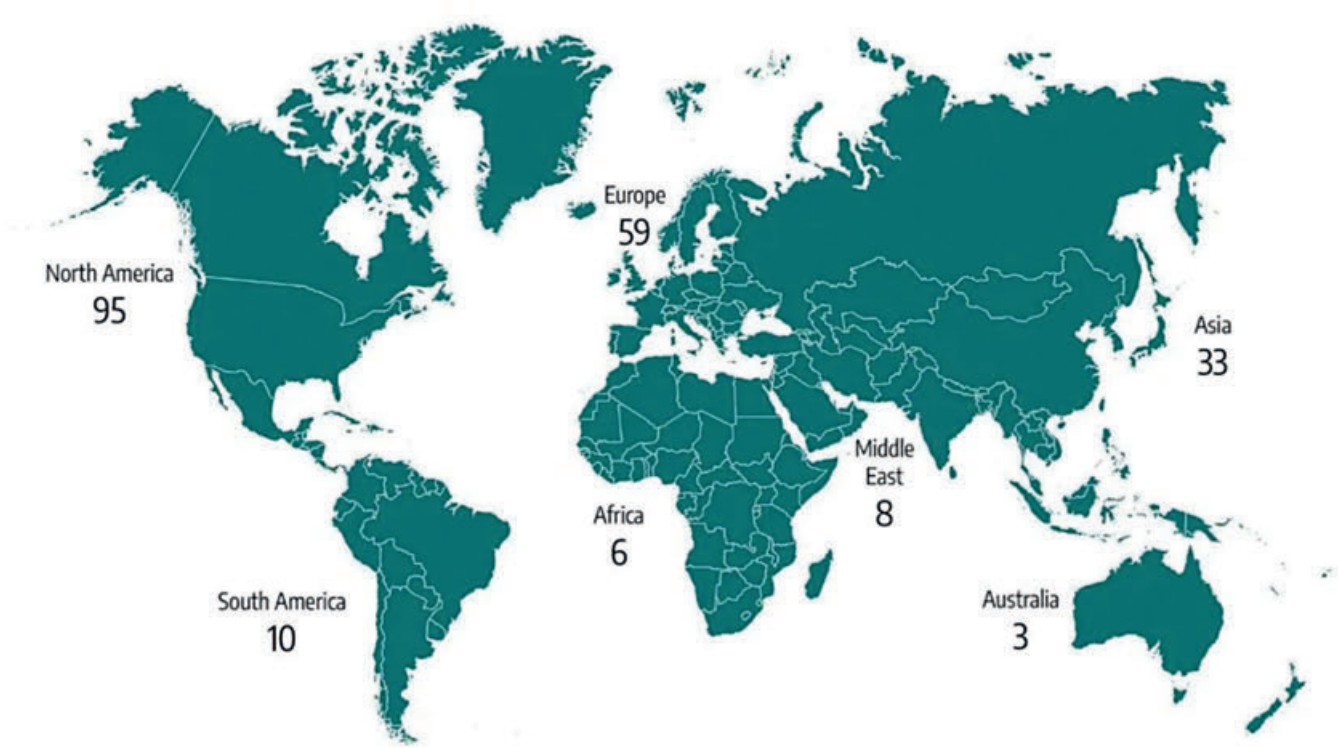
Kibernetska varnost v kompleksnih korporativnih okoljih zahteva vse bolj proaktiven pristop. Ena učinkovitejših strategij je upravljanje in izvedba ukrepov za premostitev tveganj in groženj na podlagi pravočasne inteligence informacij o varnostnih dogodkih in analize stanja, s čimer se na kibernetske napade pripravimo vnaprej. To lahko dosežemo s sistematičnim procesom za ocenjevanje vplivov groženj in izbiro premostitvenih ukrepov, katerih učinkovitost upravičuje stroške in uporabljene vire. Takšen proces smo vpeljali v sklopu projekta CyberSEAS kot dobro prakso varovanja in povečanja odpornosti evropske energetske kritične infrastrukture. Podprli smo ga z odločitvenim orodjem, med njegove sestavne dele pa smo vključili še premostitvena ogrodja in modele za korporativno odločanje. ■

Avtor: Boris Krajnc / specialist za kibernetsko varnost, Telekom Slovenije d.d.*

INDUSTRIJSKA OKOLJA VEDNO POGOSTEJŠA TARČA KIBERNETSKIH NAPADOV

Kibernetski napadalci, ki ciljajo na industrijska okolja, se le-teh lotijo z izsiljevalsko programsko opremo in izkoriščanjem ranljivosti naprav.

Napadi z izsiljevalsko programsko opremo »ransomware« so tudi v prvem četrtletju leta 2023 industrijskim organizacijam in infrastrukturi predstavljali veliko grožnjo. Ta trend poudarja vse večjo prefinjenost skupin, ki uporabljajo izsiljevalsko programsko opremo, zato je ključno, da industrijske organizacije ostanejo pozorne ter sprejmejo in izvajajo zanesljive ukrepe za zaščito svojih dejavnosti in infrastrukture.



Slika: Incidenti z izsiljevalsko programsko opremo po celinah (zaslonski zajem dragons.com)

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Na svetovni ravni:

- 44 odstotkov napadov z izsiljevalsko programsko opremo po vsem svetu je vplivalo na industrijske organizacije in infrastrukturo,
- V ZDA je bilo izvedenih več kot 41 odstotkov vseh napadov z izsiljevalsko programsko opremo,
- Po številu napadov sledi Evropa z 28 odstotki napadov z izsiljevalsko programsko opremo.

Poleg napadov z izsiljevalsko programsko opremo je seveda potrebno biti pozoren tudi na ranljivosti, ki so odkrite na opremi, kot so RTU, HMI, PLC, ki se uporablja v proizvodnem procesu ali za potrebe upravljanja infrastrukture.

Kot primer lahko navedemo kritično ranljivost, ki je bila odkrita na RTU-napravah (Remote Terminal Unit oziroma oddaljena terminalska enota) v maju letos. Z izkoriščanjem odkrite ranljivosti bi lahko hekerji prevzeli popoln nadzor nad upravljanjem procesov, ki bi jih upravljali v industriji ali v infrastrukturi. Ranljivost, ki je dobila oznako CVE-2023-2131 z oceno varnostne ranljivosti CVSS 10, vpliva na RTU-naprave z vgrajeno programsko opremo pred različico 3.36. CVSS označuje skupno ocenjevalno lestvico ranljivosti (Common Vulnerability Scoring System), ki se uporablja za ocenjevanje resnosti varnostnih ranljivosti v računalniških sistemih. Po navedbah CISA (Cybersecurity and Infrastructure Security Agency) se RTU-naprave z omenjeno ranljivostjo uporabljajo v panogah, kot so promet, vodovod in kanalizacija. Ker naprave podpirajo standarde, kot so IEC 60870-5-101/104, ki so uveljavljeni v energetiki, pa je lahko na udaru tudi ta del kritične infrastrukture.

Z izkoriščanjem prej omenjene ranljivosti CVE-2023-2131 lahko napadalec pridobi najvišje »root« privilegije v ciljni enoti RTU, kar mu omogoča popoln nadzor nad to napravo. Potencialni vpliv v resničnem svetu pa je odvisen od tega, za kaj se RTU uporablja. Ko govorimo o RTU-napravah, pomeni, da je to naprava, ki jo upravljamo s sistemom SCADA (Supervisory Control and Data Acquisition), računalniškim nadzornim sistemom, ki se uporablja za nadzor in upravljanje industrijskih procesov. Tisti, ki ima možnost upravljanja RTU, lahko spreminja tako vhode kot izhode. To je odvisno od tega, za kaj organizacija RTU uporablja. Pri tem pa lahko, če se uporablja, na primer, za odpiranje oz. zapiranje črpalk ali vodnih vrat, napadalec nadzoruje tudi to. Napadalec lahko v celoti onemogoči delovanje sistema, kar ima lahko velik vpliv na industrijske procese v organizaciji. Posodobitev programske opreme, ki onemogoča izkoriščanje omenjene ranljivosti, je bila s strani proizvajalca RTU-jev že izdana.

Kaj lahko storimo, da se izognemo ali preprečimo napade z izsiljevalsko programsko opremo oziroma, da napadalcem onemogočimo izkoriščanje ranljivosti na opremi, ki je iz takšnih ali drugačnih razlogov še nismo uspeli ali ne moremo posodobiti?

Potrebno je začeti pri osnovah. Ker se dostava izsiljevalske programske opreme še vedno najpogosteje dogaja preko vektorja napada, največkrat socialnega inženiringa, je ključno, da organizacije (po)skrbijo za ozaveščenost zaposlenih. Nepridipravi namreč izkoriščajo najlažje načine, kot so elektronska pošta, odmetavanje USB ključkov, pošiljanje USB ključkov v imenu zunanjega partnerja, predstavljanje v imenu zunanjih partnerjev s pretvezo podpore in podobno. Če so zaposleni ozaveščeni in poznajo poskuse napadov s socialnim inže-

niringom ter osnove kibernetske varnosti, je veliko manjša možnost, da bo vdor uspel.

K sreči se vedno več organizacij zaveda pomembnosti izobraževanja zaposlenih na tem področju.

Omenimo še zaščito opreme, ki jo imamo v proizvodnem ali infrastrukturnem procesu, kot so že omenjeni PLC, RTU, HMI, aktuatorji in ostalo. Omrežje, ki se uporablja za nadzor in upravljanje industrijskih procesov, kot so elektrarne, tovarne, rafinerije in drugi infrastrukturni sistemi, mora zagotavljati osnovne zahteve, ki so namenjene zagotavljanju stabilnosti, zanesljivosti in varnosti sistema.

Nekaj ključnih zahtev:

Zanesljivost
Industrijsko okolje in okolje kritične infrastrukture zahtevata visoko stopnjo zanesljivosti, saj je neprekinjeno delovanje ključno. To pomeni, da morajo biti omrežni elementi, kot so strežniki, stikala in usmerjevalniki zasnovani tako, da zagotavljajo visoko razpoložljivost in odpornost na napake. Poleg tega je potrebno upoštevati tudi redundanco, ki prepreči izpad celotnega sistema v primeru okvare posameznih komponent.

Varnost
Industrijska okolja in okolja kritične infrastrukture so pogosto tarča kibernetskih napadov, zaradi česar morajo biti omrežne naprave in komunikacijski protokoli varni pred nepooblaščenim dostopom, zlonamerno programsko opremo in vsemi drugimi oblikami kibernetskih groženj. Zagotoviti je treba ustrezno avtentikacijo, avtorizacijo in šifriranje komunikacije v omrežju. Prav tako je treba upoštevati strogo politiko varnosti, ki zajema gesla, nadzor dostopa, varnostne posodobitve in spremljanje omrežnega prometa.

Ločevanje omrežij
Zaradi varnostnih razlogov je v industrijskem okolju pomembno ločevanje omrežij. To pomeni, da se različne komponente omrežja, kot so operativna tehnologija (OT) in informacijska tehnologija (IT) vzdržujejo ločeno. OT-omrežje je namenjeno industrijskim procesom, medtem ko je IT-omrežje namenjeno pisarniškim aplikacijam in podatkom. Ločevanje omrežij pomaga preprečevati nepooblaščen dostop in širjenje napadov med različnimi deli sistema. Z upoštevanjem modela »Purdue« lahko zagotovimo optimalno ločevanje omrežij informacijske in operativne tehnologije ter s tem večjo varnost.

Odpornost na motnje
Industrijsko okolje in okolje kritične infrastrukture morata biti odporna na različne vrste motenj, vključno s fizičnimi napakami, naravnimi nesrečami in kibernetskimi napadi. Zato je ključna redundanca ter izvajanje rednih pregledov sistema, vzdrževanje opreme in izvajanje načrtov za obnovo po izpadu. Prav tako je treba redno izvajati varnostne posodobitve omrežne opreme in programskih komponent, s čimer se zaprejo morebitne varnostne vrzeli.

Nadzor dostopa
V industrijskih okoljih in okoljih kritične infrastrukture je pomembno natančno upravljanje in nadzorovanje dostopa do omrežja. To vključuje dodeljevanje uporabniških pravic in vlog ter vzpostavitev sistema za upravljanje identitet in dostopa (Identity and Access Management - IAM). Dostop do omrežnih virov in funkcij naj imajo le pooblaščeni uporabniki, kar zmanjša tveganje za nepooblaščeno uporabo in zlorabo.

Monitoriranje in zaznavanje
Industrijsko okolje in okolje kritične infrastrukture zahtevata učinkovito spremljanje in zaznavanje morebitnih varnostnih incidentov ter neobičajnih dogodkov v omrežju. Sistem za zaznavanje napadov (Intrusion Detection System - IDS) in sistem za zaznavanje naprednih groženj (Advanced Threat Detection System - ATDS) lahko pomagata pri odkrivanju in odzivanju na morebitne kibernetske napade. Prav tako je vedno bolj v veljavi uporaba ADS naprav (Anomaly Detection System), ki s strojnim učenjem in umetno inteligenco pravočasno opozorijo na anomalije, ki se pojavljajo v proizvodnem procesu, kar omogoča, da hekerje pravočasno odkrijemo in onesposobimo.

Redundanca in obnovitev
V industrijskih okoljih in okoljih kritične infrastrukture je pomembno tudi, da so na voljo rezervne sistemske komponente in načrti za obnovitev v primeru izpada ali okvare. Redundantna arhitektura omrežja omogoča preklapljanje na rezervne komponente v primeru odpovedi primarnih elementov sistema. Prav tako je treba redno izvajati varnostne kopije podatkov ter načrtovati in preizkušati postopke obnovitve sistema.

Vse navedeno so osnovne zahteve, ki so ključne za zagotavljanje stabilnosti, zanesljivosti in varnosti omrežja v industrijskih okoljih in okoljih kritične infrastrukture. Tovrstne zahteve naj se upoštevajo že pri načrtovanju in vzpostavitvi omrežja, redno naj se izvajajo tudi pregledi in posodobitve sistema. ■

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

UVAJANJE UMETNE INTELIGENCE V PROCESE PREPREČEVANJA NELEGALNE TRGOVINE Z DROGAMI - NOV EU PROJEKT ARIEN

Razvoj na področju umetne inteligence širi možnost njene uporabe tudi na področja, ki so zelo pomembna za zagotavljanje nacionalne in mednarodne varnosti. Preprečevanje nelegalne trgovine z drogami je izredno zahteven proces, kjer lahko vsaka uvedba novih tehnologij pomembno pripomore k njegovi učinkovitosti.

V letošnjem letu je EU skozi raziskovalno-razvojni mehanizem HORIZON Europe izbrala in bo financirala pomemben projekt ARIEN - Artificial Intelligence In Fighting Illicit Drugs Production And Trafficking.

Posebej nas lahko veseli, da so slovenske organizacije Institut za korporativne varnostne študije, Ministrstvo za notranje zadeve/Policija, Univerza v Mariboru in Pošta Slovenije del tega pomembnega projekta. To je seveda dokaz odličnosti in prodornosti slovenskega znanja in seveda priznanje za odlično delo v fazi priprave na objavljen razpis. V nadaljevanju si podrobneje oglejmo vsebino in glavne cilje navedenega projekta ARIEN.

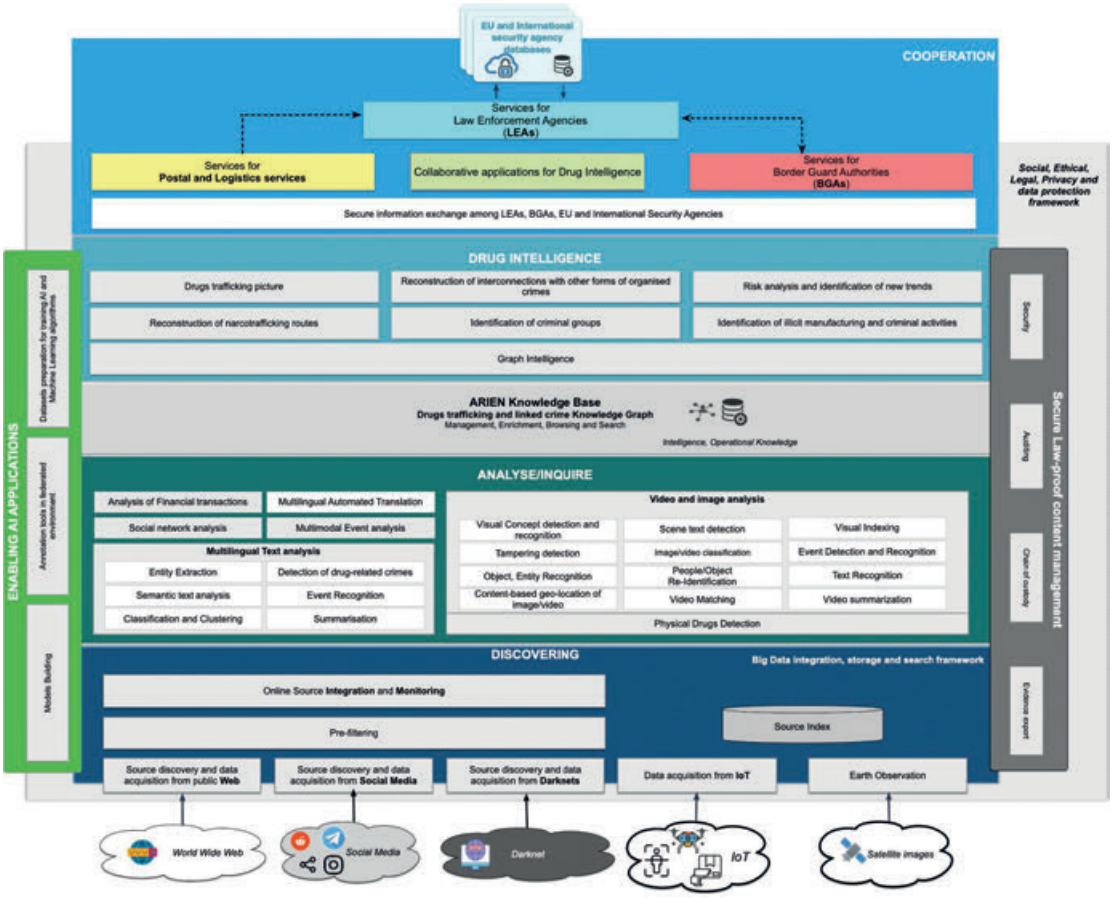
ARIEN

Zavezanost Evropske unije k boju proti nezakonitemu prometu s prepovedanimi drogami je bila ponovno potrjena v strategiji in akcijskem načrtu EU na področju drog za obdobje 2021-2025[12]. Kljub prizadevanjem in dosežkom prejšnjih pobud EU in mednarodnih pobud je promet z nedovoljenimi drogami vse bolj dinamičen pojav, kar zadeva razširjenost in zapletenost, v katerega so vključene tako organizirane kriminalne združbe (OKZ) kot osamljeni storilci kaznivih dejanj, ki skupaj aktivno sodelujejo pri številnih povezanih kaznivih dejanjih.[3]

Neposredni in posredni učinki gojenja nezakonitih pridelkov, proizvodnje drog, uporabe drog in celo odzivov politike na področju drog na okolje, so že prej postali del razprave o trajnosti in podnebnih spremembah. To je ključno vprašanje, vendar so znanstvene raziskave, ki raziskujejo povezave med trgovino s prepovedanimi drogami in okoljem, v primerjavi z drugimi področji preučevanja, povezanimi s prepovedanimi drogami, še vedno razmeroma omejeno in nedavno opravljeno delo. Učinki teh dejavnikov lahko poudarijo pomen na mednarodni, nacionalni in lokalni ravni ter ravni posameznika. Uporaba predhodnih sestavin za proizvodnjo novih psihoaktivnih snovi (NPS) povečuje količino odpadkov, kar je lahko tudi eden izmed pomembnih indikatorjev.

Posebej nas lahko veseli, da so slovenske organizacije Institut za korporativne varnostne študije, Ministrstvo za notranje zadeve/Policija, Univerza v Mariboru in Pošta Slovenije del tega pomembnega projekta. To je seveda dokaz odličnosti in prodornosti slovenskega znanja in seveda priznanje za odlično delo v fazi priprave na objavljen razpis.

*avtorica je članica Slovenskega združenja korporativne varnosti



Shema 1: Logična arhitektura projekta ARIEN

Poslanstvo projekta ARIEN

ARIEN predlaga izvedbo celovitega delovnega načrta, ki temeljito obravnava temo razpisa, usklajeno z akcijskim načrtom EU za boj proti drogam, doseženega s celovitim inovacijskim ukrepom, ki v realnem času ustvarja obveščevalno sliko o pojavnosti trgovine z drogami v EU. Zmogljivosti za odkrivanje, analiziranje in sledenje verigi trgovine s prepovedanimi drogami, tako na spletu kot zunaj njega, podprte z orodji, ki jih poganja umetna inteligenca, so takšna orodja, ki bodo prednostno spodbujala sodelovanje med organi pregona, pristojnimi organi držav članic, carino in poštnimi službami v EU in zunaj nje. Sodelovalno znanje iz mreže agencij bo pomagalo pri odkrivanju poti trgovanja, uravnoteženo z razčlembo zakonodajnih parametrov in vrzeli, ki bodo podlaga za regulativna priporočila za uskladitev zakonov, skladnosti s predpisi in čezmejnim mednarodnim sodelovanjem.

Glavni strateški cilji projekta so:

SC1. [PREISKOVANJE] Izboljšanje preiskovalnih zmogljivosti organov pregona na področju proizvodnje in prometa s prepovedanimi drogami z uporabo inovativnih tehnik umetne inteligence za spremljanje spletnih trgov s prepovedanimi drogami in pridobivanje dragocenih informacij (npr. o fizičnih žariščih preprodaje drog prek družbenih medijev), ki podpirajo učinkovito preiskavo.

SC2. [OBVEŠČEVALNE INFORMACIJE] Izboljšanje obveščevalne slike o proizvodnji in prometu s prepovedanimi drogami, izboljšanje razumevanja celotne verige, njenih finančnih tokov in vloge črnih trgov v globalnem t.i. »dark netu« ter njihovih povezav z družbenimi mediji.

SG3. [ZNANJE] Izboljšanje znanja o načinu delovanja ter novih grožnjah in trendih na področju trgovine z drogami in organiziranega kriminala, povezanega z drogami.

SG4. [SODELOVANJE] Spodbujanje učinkovitih strategij mednarodnega sodelovanja med pristojnimi organi EU in izven EU, carinskimi in mejnimi organi ter oblikovalci politike za povečanje zmogljivosti preiskav proti kriminalnim združbam.

Skozi projekt se bodo metodološki in tehnološki ukrepi testirali skozi štiri glavne pilotne sredine:
Pilot 1: Boj proti nezakonitemu gojenju, proizvodnji in prometu z marihuano in drogami
Pilot 2: Podpora pri razgradnji verige trgovine s prepovedanimi drogami
Pilot 3: Trgovina z novimi psihoaktivnimi snovmi (NPS) in predhodnimi sestavinami za droge
Pilot 4: Metode trgovanja z drogami: Pošta in poštni paketi

Projekt se bo uradno začel s 1. novembrom 2023. O vseh naslednjih korakih vas bomo skozi različne komunikacijske kanale ustrezno obveščali. ■

1 Council of the EU (2020) EU Drugs Strategy 2021-25 - https://www.emcdda.europa.eu/drugs-library/council-eu-2020-eu-drugs-strategy-2021-25_en
2 EU Drugs Action Plan 2021-2025 - https://www.emcdda.europa.eu/system/files/attachments/13933/eu-drugs-action-plan-2021-2025.pdf
3 European Drugs Markets Report - https://www.emcdda.europa.eu/system/files/publications/12078/20192630_TD0319332ENN_PDF.pdf

ARIEN
ARtificial Intelligence in fighting illicit drugs production and trafficking

Avtorica: Kristina Ober / direktorica marketinga, Smart Com d.o.o.*

TEHNOLOŠKO NAPREDNO ELEKTRODISTRIBUCIJSKO OMREŽJE ELEKTRA CELJE ZA ZANESLJIVO OSKRBO TER TRAJNOSTNE STORITVE – PRIMER DOBRE PRAKSE

Elektro Celje d.d. je, kot eno izmed petih elektrodistribucijskih podjetij v državi, del elektroenergetskega sistema Republike Slovenije in tako ključni člen za razvoj stroškovno učinkovitega distribucijskega omrežja države za zagotavljanje kakovostne in zanesljive oskrbe odjemalcev električne energije.

Elektro Celje d.d. skrbi za upravljanje, vodenje in obratovanje distribucijskega sistema ter vzdrževanje, izgradnjo in obnovo elektrodistribucijskih vodov in naprav na območju, ki obsega 4.345 km^2 oz. 22 odstotkov površine Slovenije. Elektroenergetska infrastruktura, preko katere se napaja več kot 173.000 odjemalcev, v celotni dolžini predstavlja drugo najdaljše omrežje v državi. Družba je lastnik elektrodistribucijske infrastrukture, ki zajema 12.994 km nizkonapetostnih omrežij, 1.258 km srednjenapetostnih kablovodov, 72 km 110 kV daljnovodov, 2.440 km srednjenapetostnih daljnovodov, 19 razdelilnih transformatorskih postaj, 16 razdelilnih postaj in 3.593 transformatorskih postaj.

Za nemoteno delovanje tega elektrodistribucijskega sistema je ključno načrtovanje, upravljanje, vodenje in obratovanje distribucijskega omrežja. Zanesljivost in varnost obratovanja omrežja dosegajo tudi z uvajanjem sodobne informacijske in telekomunikacijske podpore, ki sloni na najnovejših tehnoloških rešitvah.

Z leti se je kompleksnost telekomunikacijskega sistema, ki je bil zgrajen na osnovi Ethernet tehnologije, povečevala, s tem pa se je zmanjševala obvladljivost omrežja. Zato so se ob zadnjem ciklu prenove sistema odločili za postopno uvajanje nove tehnologije, in sicer tehnologije matričja oz. fabric ponudnika Extreme Networks. Projekt pa so uspešno izpeljali z dolgoletnim partnerjem Smart Com d.o.o. ki je sodeloval pri razvoju, načrtovanju in vpeljavi rešitve.

Sistem, ki temelji na tehnologiji matričja oz. fabric, jim v povezavi z gradniki avtomatizacije in upravljanja omogoča učinkovito obvladovanje omrežja ob hkratnem povečevanju zahtev uporabnikov in naglo razvijajočem se področju različnih aplikacij in sistemov v pametnih omrežjih.

Zagotavlja jim visoko razpoložljivost, predvsem pa večjo kibernetsko varnost ter omogoča uvajanje storitev po načelih trajnostnega razvoja za širok nabor različnih uporabniških sistemov.

Zanesljivost in varnost obratovanja omrežja dosegajo tudi z uvajanjem sodobne informacijske in telekomunikacijske podpore, ki sloni na najnovejših tehnoloških rešitvah.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Omrežje jim omogoča tudi višjo raven kibernetske varnosti, saj je le-ta vgrajena že na omrežno raven in tako že na samem robu omrežja poskrbijo za večjo odpornost na napredne kibernetske grožnje.

Izziv

V Elektro Celje d. d. je tehnologija Ethernet ključna za delovanje IKT sistema, saj jim omogoča visoko razpoložljivost in varnost ter podpira vse vitalne storitve. Naravni tehnološki razvoj pa je zahteval premislek pri načrtovanju omrežja in varnosti, saj nadgradnja obstoječe tehnologije in vgrajene opreme ni bila več smiselna. Tveganje, da lahko tehnologija ali oprema, ki je stara deset let in več, kadarkoli odpove, je bilo previsoko, in potrebno je bilo pristopiti k nadgradnji oz. prenovi sistema. Dodaten motiv so bili stroški vzdrževanja vgrajenih naprednih naprav višjega cenovnega razreda, ki so se z njihovim staranjem hitro povečevali.

Rešitev

Na voljo je bilo več možnosti, od izbire tehnologije, izbire specifične stojne opreme ter implementacije oz. izbire pravega termina vključitve v produkcijo, ko je potrebno omrežje prekiniti, kar je izjemnega pomena za uspešnost projekta. Po tehtnem premisleku ter opravljeni analizi možnosti in preverjanju zrelosti glede na zmožnosti, učinkovitost in povečanje ravni kibernetske varnosti, se je kot najboljša izbira za nadgradnjo Ethernet omrežja pokazala ravno tehnologija matričja oz. fabric. Ta obsežen projekt so zastavili v več korakih ter migracijo izpeljali v več obvladljivih fazah. Danes imajo v omrežju najnovejšo omrežno tehnologijo, ki je združljiva z ostalimi deli omrežja.

Pozitivni učinki

- Bistveno lažje upravljanje z omrežjem in odpravljanje težav v omrežju preko enovitega in krovnega sistema za nadzor in upravljanje.
- Omogočena visoka razpoložljivost ter zagotovljena samodejna preusmeritev prometnih tokov na obhodno pot v primeru napake v omrežju.
- Prožnost omrežne arhitekture (visoka stopnja prilagodljivosti pri uvajanju storitev...).
- Višja raven kibernetske varnosti na ravni omrežne arhitekture. Možnost vpeljevanja sodobnih mehanizmov kibernetske varnosti tako v poslovni (IT) kot procesni (OT) del.
- Optimizacija delovnih procesov, saj se z vpeljavo avtomatizacije prihrani bistveno več časa pri vsakodnevnem rutinskem delu kot tudi pri odpravljanju težav v omrežju.
- Občutno nižji stroški obratovanja in vzdrževanja omrežja. Nova oprema porabi manj energije, kar je prednost tudi s trajnostnega vidika.

Zagotavlja jim visoko razpoložljivost, predvsem pa večjo kibernetsko varnost ter omogoča uvajanje storitev po načelih trajnostnega razvoja za širok nabor različnih uporabniških sistemov.

Ključna zanesljivost in varnost obratovanja omrežja

Pomembno vlogo pri obratovanju in razvoju elektrodistribucijskega sistema ima v Elektro Celje d. d. Služba za telekomunikacije. Z relativno majhno skupino sodelavcev obvladujejo celoten spekter telekomunikacijskih sistemov, kot tudi sistemov kibernetske varnosti, saj skrbijo za njihov razvoj, implementacijo in obratovanje.

Na področju sistemov kibernetske varnosti pa Služba v celoti upravlja napredne požarne pregrade ter programska orodja za kibernetsko varnost in sistem za detekcijo anomalij za procesno omrežje, ki je podprto z umetno inteligenco in omogoča vidljivost nad storitvami, protokoli in napravami v omrežju.

Uvajanje sodobne informacijsko-telekomunikacijske podpore

Z omrežno zasnovo, ki temelji na tehnologiji matričja oz. fabrica, so povečali stopnjo avtomatizacije v omrežju in poenostavili upravljanje, s čimer se je povečala učinkovitost in hitrost opravljanja administratorskih nalog pri upravljanju in obratovanju omrežja.

Za vzpostavitev storitev v omrežju je sedaj potrebnih bistveno manj korakov, saj storitev kreirajo na robu omrežja (na enem in drugem koncu), vmes pa vgrajeni mehanizmi avtomatizacije poskrbijo za ustrezno povezljivost po najkrajši poti. Pri tem je pomembna visoka razpoložljivost, ki je zagotovljena z avtomatsko preusmeritvijo vsega prometa na rezervno pot v primeru napake, kar pomeni, da storitev za končnega uporabnika vedno deluje. Pri majhni ekipi, ki upravlja omrežje, sta zelo pomembni preglednost in učinkovitost – da so rutinske naloge čim bolj avtomatizirane, brez ročnih posegov v jedro omrežja, kar zmanjša možnost napak pri konfiguraciji praktično na ničelno raven in s tem prepreči možnost nedelovanja storitev.

Omrežje jim omogoča tudi višjo raven kibernetske varnosti, saj je le-ta vgrajena že na omrežno raven in tako že na samem robu omrežja poskrbijo za večjo odpornost na napredne kibernetske grožnje.

Omogočena je hipersegmentacija, prav tako je fizični nivo omrežja popolnoma ločen od storitvenega nivoja, s tem pa so topologija omrežja in naprave nevidni uporabnikom in potencialnim napadalcem. S tem se bistveno poveča odpornost na potencialne kibernetske incidente.

Danes imajo v Elektro Celje d. d. z vpeljavo tehnologije matričja oz. fabrica zelo zanesljivo in robustno omrežje, za katerega v vsakem trenutku vedo, v kakšnem stanju je, pa tudi uporabniki, ki so priključeni v omrežje, so z vidika varnosti veliko bolj varni in nemoteno komunicirajo. ■

»Smo del kritične infrastrukture države in hkrati ponudnik bistvenih storitev, zato smo zavezani strogi zakonodaji, ki vpliva na naše delovanje in poslovanje. Vse naše odločitve zato sprejemamo preudarno in premišljeno.«

Damjan Bobek, vodja Službe za telekomunikacije, Elektro Celje d. d.

Foto: Aleš Rosa

»Verjetno si le malokdo predstavlja, kakšno je naše elektrodistribucijsko IKT omrežje. Gre za 50+ telekomunikacijskih vozlišč v nekaj 10 poslovnih objektih, gre za omrežje izredno velikih razsežnosti.«

Damjan Bobek, vodja Službe za telekomunikacije, Elektro Celje d. d.

Foto: Aleš Rosa

»Kot strokovnjak za kibernetsko varnost v prenovi komunikacijskega omrežja vidim velike prednosti tehnologije matričja oz. fabrica, saj omogoča vzpostavljanje bistveno bolj varnih povezav.«

Tomi Kolar, strokovnjak za omrežne tehnologije in kibernetsko varnost, Elektro Celje d. d.

Foto: Aleš Rosa

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.