

Korporativna varnost



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

Letnik 2021, maj • št. 25



Podelitev prestižnih nagrad
»Slovenian Grand Security Award«

Luka Koper pripravljena na nove izzive prihodnosti
Dimitrij Zadel, predsednik uprave Luke Koper d.d.
Boris Kankaraš mag., vodja področja pristaniške varnosti Luke Koper d.d.



360°

VAŠA 360° VARNOST 365 DNI V LETU

MODRO JE IZBRATI OPERATIVNI CENTER KIBERNETSKE VARNOSTI

360° varnost vam zagotavlja **najsodobnejšo kibernetsko zaščito**. Namobilni, stacionarni, oblaki 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 seznani s pomembnimi dogajanji, ki jih zaznajo. OCKV Telekom 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](https://www.telekom.si/poslovni)

Telekom Slovenije



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

Korporativna
varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne
varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida:
maj 2021

Izvod revije je brezplačen

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

ISSN 2232-6170

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

Počasi vendar vztrajno se izrisuje pot iz stanja epidemije COVID-19, s katero smo se morali soočiti več kot leto dni. Omenjena epidemija je še bolj izpostavila pomen odpornosti (resilience) naših organizacij in sposobnost zagotavljanja nemo-teno delovanje ključnih poslovnih procesov, tudi v najbolj zahtevnih trenutkih. Zaradi soodvisnosti moderne družbe je potrebno odpornost razumeti v širšem kontekstu in se ne pustiti ujeti samo v okvirje naše organizacije. Za uspešnost delovanja naših organizacij je potrebno zavedanje zagotavljanja odpornosti družbe kot celote. Tudi tokrat pride do izraza miselnost, da deluj lokalno in misli globalno, kar tudi na področju zagotavljanja odpornosti pomeni pomemben moment razumevanja, da lahko odpornost vsake posamezne organizacije vpliva tudi na zagotavljanje odpornosti celotne družbe. Še posebej je v tem okviru pomembno izpostaviti tiste organizacije, ki upravljajo s kritično infrastrukturo ali bistvenimi storitvami, ki so pomembne za delovanje širše družbene skupnosti. Čeprav je omenjena epidemija prinesla nekaj pozitivnih stvari in še pospešila digitalizacijo družbe in poslovnih procesov, ne smemo zanemarjati in podcenjevati negativnih vidikov. Ti se bodo v prihodnjem obdobju najbolj odražali na varnostnih izzivih, ki bodo povezani s kadrovskim potencialom v naših organizacijah. Nakopičeni stres in potlačene travmatične izkušnje bodo doživele eskalacijo, ko se bo družba poskušala z vso naglico vračati v približno realnost, ki smo jo poznali pred epidemijo. Dogodek, ki smo ga v javnosti zaznali in je bil povezan z načrtovanim strelskim pohodom, katerega so organi pregona na srečo preprečili, predstavlja samo vrh ledene gore in težav s katerim se bomo srečevali v naslednjem obdobju. Nestrpnost, konflikti in nasilje na delovnem mestu bo postalo tisti varnostni dejavnik, ki se mu bo potrebno v prihodnje, poleg kibernetičnih tveganj, še posebej posvetiti. Pospešena digitalizacija družbe pa tako ali tako kibernetična tveganja že dlje časa postavlja na pomemben vrh varnostnih izzivov, katerim bo korporativna varnost morala namenjati vso potrebno pozornost.

Tokratno številko revije Korporativna varnost tokrat posebej namenjamo prihajajoči vrhunski mednarodni konferenci Dnevi korporativne varnosti 2021 in svečani podelitvi prestižnih nagrad Slovenian Grand Security Award. Zaradi navedenega smo del prostora revije namenili tudi nagrajencem, da z našimi bralci podelijo dobre prakse, katere so jim omogočile prejem teh prestižnih nagrad. Poleg navedenega smo želeli vsebinsko osvetliti dovolj široko, da v tem okviru prenesemo določene nove vidike in izkušnje tudi na področja, ki jih prinaša uvajanje novih tehnologij. Tudi področju kibernetične varnosti namenjamo pomemben spekter prispevkov v sami reviji, prostor pa dajemo tudi ostalim varnostnim vsebinam. Posebej bi želel izpostaviti strateško geopolitično oceno, ki jo prinaša tokratna kolumna. Izkoristili smo priložnost in se pogovorili s pomembnimi strateškimi voditelji in strokovnjaki z različnih področij, ki z nami delijo svoje izkušnje in strateške poglede.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



KOLUMNA

Vojko Volk, veleposlanik

STRATEŠKA VARNOST EVROPE IN EVROPSKE VREDNOTE

10



INTERVJU

Dr. Mitja Štular, član uprave Telekom Slovenije, d.d.

TELEKOM SLOVENIJE SMELO UVAJA NOVE TEHNOLOŠKE REŠITVE

14



INTERVJU

Božidar Dajčman, direktor Oddelka upravljanja fizične
in informacijske varnosti, Nova KBM d.d.

KORPORATIVNA VARNOST JE POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE USTREZNE ODPORNOSTI DELOVANJA ORGANIZACIJE

20



INTERVJU

g. Igor Zgonc, direktor Silver Bullet Risk

UPRAVLJANJE S TVEGANJI KLJUČEN DEJAVNIK ZA USPEŠNO POSLOVANJE ORGANIZACIJ

25



KOMPETEMNCE VARNOSTIH MENEDŽERJEV V PROCESU KRIZNEGA UPRAVLJANJA IN VODENJA V KRITIČNI INFRASTRUKTURI

Namen tega sestavka je, da v sklopu aktualnih kriznih razmer v letu 2021 in ob upoštevanju ostalih tveganj, ki se pojavljajo pri upravljanju kritične infrastrukture, predstaviva kompetence in kompetentnost tistih menedžerjev, ki v kritični infrastrukturi upravljajo posamezna področja korporativne varnosti in integralni varnostni sistem kot celoto.

43

INTERVJU

g. Dimitrij Zadel, predsednik uprave Luke Koper d.d.
Boris Kankaraš mag., korporativno varnostni manager,
vodja področja pristaniške varnosti Luke Koper d.d.*

LUKA KOPER PRIPRAVLJENA NA NOVE IZZIVE PRIHODNOSTI

Luka Koper na temelju tradicije smelo koraka proti novim izzivom in poslovnim priložnostim. Luka Koper je dobitnik prestižne nagrade Slovenian Grand Security Award v kategoriji »najbolj varno podjetje« za leto 2020. Prizadevanja za zagotavljanje neprekinjenosti delovanja bodo predstavljala velik izziv, ki bo poleg ostalega zahteval sistemski pristop upravljanja korporativne varnosti. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z g. Dimitrijem Zadelom in g. Borisom Kankarašem.

g. Dimitrij Zadel

Vodite podjetje, ki predstavlja eno od organizacij, od katere je zelo odvisno strateško logistično delovanje Republike Slovenije, kakor tudi širše regije, zaradi njene kompleksne odvisnosti od strateške lege Luke Koper. Imate občutek, da so ta dejstva dovolj upoštevana pri podpori vseh nacionalnih institucij?

Menim, da so. Že leta 1991 se je država v Resoluciji o pomorski usmeritvi Republike Slovenije zavezala, da bo vodila gospodarsko in razvojno politiko, ki bo tudi pomorsko usmerjena in da bo podpirala razvoj koprškega pristanišča, ter prek njega usmerjenega tranzitnega in kopenskega prometa. S Pomorskim zakonikom je nato vnesla pristanišče v pravni red, ga umestila v prostor z Državnim prostorskim načrtom, v Strategiji razvoja prometa v Republiki Sloveniji pa je začrtala, poleg razvoja pristanišča, tudi izgradnjo sodobne

Zavedamo se namreč, da vlaganja v področje varovanja niso zgolj strošek, ampak investicija v zagotavljanje varnega delovnega okolja, nemoteno delovanje luških procesov in ne nazadnje uspešnega poslovanja delniške družbe Luka Koper.

železniške povezave, ki bo pristanišču omogočila izkoristiti njegove poslovne priložnosti.

Kritična infrastruktura je nujna za nemoteno delovanje družbe. Kako ob tej predpostavki organizirati sistem obvladovanja tveganj, ki bo zagotavljal ustrezno varnost za nemoteno delovanje infrastrukture? Kakšne so vaše izkušnje sodelovanja z državnimi organi zadolženimi za pripravo sistemskih ukrepov za zaščito te infrastrukture?

Država je koprsko pristanišče opredelila kot objekt posebnega pomena ter

ga uvrstila med objekte kritične infrastrukture, saj bi prekinitev njegovega delovanja imela resne posledice za nacionalno varnost, gospodarstvo, in druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi. Kako pomembno je pristanišče za oskrbo ljudi in gospodarstva se je izkazalo prav v času aktualne epidemije, ko naše dejavnosti nismo prekinili niti za trenutek. Ob tem je potrebno še dodati, da je območje pristanišča carinska cona in da ima status mednarodnega mejnega prehoda. Izpostavljeno je torej mnogim tveganjem, zato imamo v Luki Koper izdelan varnostni načrt, ter vzpostavljene varnostne in kontrolne mehaniz-

me, s katerimi zagotavljamo nemoteno odvijanje delovnih procesov, varnost pristaniške infrastrukture in objektov, tovara ter oseb, ki se gibljejo na območju pristanišča. Področju varnosti torej posvečamo vso potrebno pozornost in pri tem tvorno sodelujemo s pristojnimi državnimi organi in inštitucijami.

Varnostna kultura in visoko varnostno zavedanje zaposlenih ločuje uspešne organizacije od slabše uspešnih. Kako vi kot strateški manager v tem hitrem dinamičnem okolju, kjer je mobilnost kadrovskega potenciala zelo visoka, zagotavljate osnovne varnostne vrednote in standarde varnostne kulture?

Učinkovit sistem obvladovanja tveganj zagotavljamo s primernimi kadrovskimi resursi, ki imajo ustrezno znanje in varnostno kulturo ter ozaveščanjem zaposlenih na tem področju. Posebno

pozornost namenjamo usposabljanju ter preverjanju tega sistema, ki ga stalno nadgrajujemo in s tem povečujemo njegovo učinkovitost. Poudariti je tudi potrebno, da ves čas delujemo preventivno, saj s tem vnaprej preprečujemo nastajanje dogodkov, ki bi lahko negativno vplivali na varnost ljudi in premoženja.

Smelo korakate v smeri digitalizacije in uvajanja novih energetske rešitve, ki bodo trajnostno bolj prijazne do okolja in predstavljajo zadostno učinkovitost za nadaljnji razvoj pristanišča. Je pa ta razvoj in odvisnost od informacijske tehnologije, kibernetske grožnje postavila v posebno perspektivo. Kateri so po vašem mnenju tisti koraki, ki jih lahko storite za učinkovito varovanje pred temi kompleksnimi grožnjami?

Slovenija je sprejela Zakon o informacijski varnosti ter s tem naredila velik korak, ker je vzpostavila pravni temelj. Digitalizacija luških procesov je zapisana v naše strateške razvojne usmeritve, zato zagotavljanje informacijske varnosti vse bolj pridobiva na pomenu. Zaradi hitrega razvoja in napredka, ki vodi k vse večji odvisnosti od informacijske tehnologije, metodologije in orodja za varovanje informacijskih sistemov nenehno prilagajamo novim tveganjem s ciljem preprečevanja oziroma zmanjševanja posledic varnostnih incidentov na najmanjšo možno mero ter zagotavljanja neprekinjenega poslovanja ob hkratnem zagotavljanju razpoložljivosti informacijskega sistema njegovim uporabnikom.

Sodelovanje na različnih mednarodnih raziskovalnih projektih so ključ za doseganje boljše učinkovitosti tudi na področju zagotavljanja





obvladovanja tveganj. Nameravate v družbi Luka Koper tudi v prihodnje slediti tej poti?

Preko področja za strateški razvoj se povezujemo z mednarodnimi institucijami in drugimi subjekti tudi na raziskovalnem področju. S tem pridobivamo vpogled v primere dobrih praks, izboljšujemo obstoječe rešitve in sodelujemo s partnerji, ki se ukvarjajo s podobno dejavnostjo tet hkrati pridobivamo EU sredstva. V zadnjih desetih letih smo samo s področja varnosti sodelovali pri 6 projektih, ki so pomembno prispevala k razvoju varnostnega sistema Luke Koper. Zadnji primer je EU projekt Infrastress, ki ima za cilj varnostno zaščito občutljivih infrastrukturnih objektov. V projektu sodeluje 27 partnerjev iz 11 držav, ki bodo s predhodnimi raziskavami iskali rešitve pri odkrivanju tako fizičnih kot kibernetskih groženj, ter pripravili ustrezna

Združenje korporativne varnosti in ICS sta za nas izjemnega pomena. Veliko število vrhunskih strokovnjakov na področju varnosti, z veliko izkušnjami, širokim naborom znanj, razvito znanstveno raziskovalno dejavnostjo so na eni strani neusahljiv vir znanja, na drugi pa promotor in podpora pri razvoju varnosti v našem podjetju.

konkurenčna in uporabnikom prijazna orodja za zaščito.

Ste letošnji prejemniki prestižne nagrade Slovenian Grand Security Award v kategoriji »Najbolj varno podjetje«. Nam lahko zaupate kaj vam pomeni prejem take nagrade?

Nagrada nam pomeni priznanje za dosedanje delo in dobra popotnica za delo

v prihodnje. Še naprej se bomo zavzemali za obvladovanje tveganj in neprekinjeno delovanje koprskega pristanišča. Zavedamo se namreč, da vlaganja v področje varovanja niso zgolj strošek, ampak investicija v zagotavljanje varnega delovnega okolja, nemoteno delovanje luških procesov in ne nazadnje uspešnega poslovanja delniške družbe Luka Koper.

Trenutno opravljate vlogo nosilca procesov korporativne varnosti v podjetju Luka Koper. Nam lahko bolj podrobno opredelite kakšne so strateške naloge vaše službe in njena organizacijska umeščenost?

Vodim Področje pristaniške varnosti, ki v okviru svojih pooblastil in pristojnosti izvaja ključne naloge za zaščito koprskega pristanišča in delniške družbe. Med te naloge spadajo:

- varovanje življenja ljudi in premoženja;
- varnostno nadzorni center;
- varovanje tajnih podatkov in poslovnih skrivnosti;
- krizno upravljanje;
- civilna obramba
- zaščita kritične infrastrukture ter
- neprekinjeno poslovanje;

Področje je podrejeno predsedniku uprave družbe.

Kakšno mesto in vlogo ima v hierarhiji strateških dokumentov v Luki Koper varnostna politika organizacije. Ali tak dokument predstavlja strateški pogled in usmeritve za postavitev in delovanje sistema korporativne varnosti v vaši organizaciji?

Podlaga za izdelavo varnostne politike so strateški razvojni dokumenti družbe, ki določajo njen nadaljnji razvoj in cilje. Tudi zato varnostna politika Luke Koper d.d. spada med strateške dokumente delniške družbe. Je krovni dokument, ki opredeljuje politiko in usmeritve družbe do varnosti v širšem pomenu besede, ter hkrati opredeljuje posamezne vidike varnosti za celotno organizacijo.

Standardizacija sredstev na področju tehničnega varovanja in varnostnih procesov na splošno je v tako razvejanem sistemu verjetno nujno potrebna. Kakšne so na tem področju vaše izkušnje in kakšne pristope uporabljate v Luki Koper?

Luki Koper d.d. ter njeni varnostni službi nalaga obveznosti različna mednarodna, oz. evropska in nacionalna zakonodaja. Pomembno dejstvo je tudi velikost (teritorialno) ter dinamika (obseg in hitrost operativnih procesov) v pristanišču. Ob upoštevanju zakonodajnih zahtev smo v Luki Koper d.d. pozorni na izkušnje in dobre prakse razvitih pristanišč, znanstveno raziskovalnih institucij ter seveda tehnološkemu razvoju na področju varnostno tehničnih sistemov.

Luka Koper je eden izmed korporativnih članov Slovenskega združenja korporativne varnosti. Kakšen pomen pripisujete stanovskemu združevanju na področju korporativne varnosti? Je to dolgoročno lahko pomemben korak k dvigovanju varnostnega zavedanja in predvsem pomena korporativne varnosti?

Izjemen. Združenje korporativne varnosti in ICS sta za nas izjemnega pomena. Veliko število vrhunskih strokovnjakov na področju varnosti, z veliko izkušnjami, širokim naborom znanj in razvito znanstveno raziskovalno dejavnostjo, so na eni strani neusahljiv vir znanja, na drugi pa promotor in podpora pri razvoju varnosti v našem podjetju.

Kje v prihodnosti pričakujete največje varnostne izzive za nemoteno delovanje vaše organizacije?

Luka Koper d.d. izvaja vrsto razvojnih projektov, ki bodo povečali njeno konkurenčno prednost med jadranskimi pristanišči. Tehnološki razvoj v svetovnem merilu postaja vedno hitrejši, s tem pa tudi boj med konkurenco. Osebeno menim, da bo imela Luka Koper d.d. največje izzive na področju kibernetске varnosti, tehnološkega razvoja ter hibridnih groženj. Dolgoročno pa seveda tudi okoljske grožnje oz. podnebne spremembe. ■



Cyber Security Is What We Do



KOLUMNA



STRATEŠKA VARNOST EVROPE IN EVROPSKE VREDNOTE

„Usoda Evrope in prihodnost svobodnega sveta sta v celoti v naših rokah“.

/Simone Veil, 1982/

Vprašanja evropske varnosti se največkrat povezujejo z obrambnimi izdatki, informacijsko in tehnološko varnostjo, zaščito pred informacijskimi vdori, varnostjo pred terorističnimi napadi, raznimi številkami, razpredelnici in organigrami. A to še zdaleč ni vse. Tisto, kar neko povezavo dela zares trdno niso zunanji okopi in obrambni zidovi ampak tisto, kar jo povezuje znotraj in kar je temelj, na katerem povezava obstaja. Ustanovni očetje EU so imeli idealne svobode, miru in blagostanja za vse ljudi. Nekoč strahotno pomembna in sporočilna besedna zveza „svobodni svet“ je v zadnjih dveh desetletjih postala samoumevnost, ki še posebej mladim na zahodu ne pomeni več prav veliko. A odkar smo lahko opazovali delovanje ameriškega predsednika Trumpa in posledice na svet, odkar je Rusija nasilno priključila Krim in odkar je Kitajska pokazala, da nima namena spoštovati niti temeljnih demokratičnih načel, se pomen svobode in demokracije na zahodu na novo vrednoti. Pri mladih še posebej v povezavi z varstvom okolja in trajnostnim razvojem, kjer EU izrazito prednjači pred celim svetom. Zdravo in varno okolje postaja vrednota, ki jo je potrebno varovati. Navsezadnje EU sama po sebi ni ne dobra ne slaba, je le tisto, kar iz nje naredimo.

Dolgoročno povsem nevzdržna politika Bidenovega predhodnika, da bo Amerika znova velika zato, ker se bo odpovedala vsem ključnim mednarodnim sporazumom, oddaljila od zaveznikov in nasploh osamila, se zdaj sistematično preobrača v nasprotno smer.

Prvi tedni delovanja novega ameriškega predsednika v celoti potrjujejo čisto vse, kar je Joe Biden v volilni kampanji napovedoval in kar so pričakovali pozornejši opazovalci mednarodnih odnosov. Tudi pisec teh vrstic je o tem pisal v prejšnji številki pričujoče in meni vedno te, bolj ljube revije. Dolgoročno povsem nevzdržna politika Bidenovega predhodnika, da bo Amerika znova velika zato, ker se bo odpovedala vsem ključnim mednarodnim sporazumom, oddaljila od zaveznikov in nasploh osamila, se zdaj sistematično preobrača v nasprotno smer. V resnici je Amerika postala največja sila sveta prav zato, ker je sklepala mednarodne sporazume, ker je sodelovala z zavezniki in ker je spoznala, da v globalnem svetu tudi v gospodarstvu največ pridobi tisti, ki je karseda vključujoč, spoštljiv do partnerjev in odprt za sodelovanje. Biden bo ta del Trumpove zunanjepolitične dediščine odpravil že v prvem polletju. Ko pa gre za notranjepolitične razmere, kjer je Trump za seboj zapustil socialno in politično povsem razklano ameriško družbo, bo delo trajalo še dolgo. Če je bil Trumpov mandat za kaj koristen je bil prav gotovo za to, da so bile dokončno razgaljene ogromne razlike med ameriško in evropsko družbo. Amerika kljub bogastvu ne premore niti osnovnih orodij socialne države, ne javnega zdravstva, ne šolstva, kot tudi ne solidarnostnega pokojninskega sistema, ostali socialni transferji pa so minimalni. To je z vso silo udarilo na plano prav v času pandemije COVID 19. EU je z zagotovitvijo rekordnega deleža sredstev za pomoč gospodarstvu in predvsem zdravstvu, državljanom EU omogočila dostojno preživetje v času krize. Je pa hkrati EU skoraj povsem odpovedala pri nabavi cepiv, kar je lekcija, ki jo bo treba vzeti skrajno resno, ker se ne sme več ponoviti. Nenazadnje je v vseh krizah ena sama gotovost, da po dežju vselej zasije sonce. In na sonce je treba biti dobro pripravljen.

Simbolično morda najbolj pomemben dokaz, kako različna svetova sta ZDA in EU, pa je bil nedavni poskus oblikovanja evropske nogometne Super Lige. Čez noč in po ameriškem



zgledu so jo hoteli ustanoviti silno zadolženi kitajski, ruski, arabski in ameriški lastniki ducata evropskih nogometnih velikanov, a jim ni uspelo. Prej kot v 48 urah je projekt propadel, pa čeprav je za njim stal svetovni kapital in vsemogočna ameriška banka JPMorgan Chase. Ključni cilji so bili finančni, športni pa obrobni. Zgodilo se je nekaj, kar je v Ameriki povsem nepredstavljivo. Finančnikom so se družno uprli nogometni navijači, evropski politiki, športni delavci in široka javnost. Pri tem so govorili o rečeh, ki v Evropi še vedno veliko pomenijo, v ZDA pa malo ali nič. Uporniki so se sklicevali na navijaške strasti in na čast, na spoštovanje lokalnih tradicij, zgodovinski ugled klubov kot institucij, na nujno zaščito manj bogatih in revnih in njihovih sanj, da tudi manjši in majhni lahko pridejo do vrha! V vsega dveh dneh smo Evropejci dobili materialni dokaz, da nekaj, čemur lahko rečemo evropske vrednote ali pa celo evropski način življenja, še kako obstaja.

Biden skratka obrača vso Trumpovo politiko kot staro nogavico, najbolj uspešen pa je zagotovo pri spopadu s koronavirusom. Iz Amerike, ki je bila pod Trumpom vodilna zanikovalka virusa, Trumpov mandat pa se je končal z najvišjim številom mrtvih žrtev na svetu, je Biden uspel postaviti Ameriko na vrh vseh držav po precepljenosti prebivalstva. Ta uspeh je še toliko večji v državi, ki ima 330 milijonov prebivalcev, nima pa javnega zdravstva.

Svet po Trumpu

Ob Rusiji, ki je bila med najbolj prizadetimi državami zaradi Trumpovega volilnega poraza in ob Kitajski, ki bi raje imela trgovca Trumpa kot pa načelnega Bidena, se Trumpovega po-

raza lahko odkrito veselimo v Evropi. Trump je EU namesto za zaveznico vzel zgolj za tekmico, kar se je zgodilo prvič po drugi svetovni vojni. Še več, Trump se je nenavadno tesno zblizal s Putinovo Rusijo istočasno, ko je Evropi grozil z gospodarskimi sankcijami in uvajal carine na evropske izdelke. Tudi tega nismo videli nikoli prej po drugi svetovni vojni. In še več, Trump je ob stisku rok s Putinom izjavil, da verjame, da Putin z ničemer ni posegel v ameriške volitve. To je bila ena najbolj nenavadnih in najbolj nepotrebnih izjav v Trumpovem mandatu. Biden je že sredi aprila letos podpisal ukaz o dodatnih sankcijah zoper Rusijo prav zaradi „računalniških vdorov in vmešavanja Rusije v ameriške volitve“. Putin je imel vse razloge tega sveta, da podpre Trumpovo zmago v ZDA, tako kot ga zdaj povsem očitno pogreša.

Biden skratka obrača vso Trumpovo politiko kot staro nogavico, najbolj uspešen pa je zagotovo pri spopadu s koronavirusom. Iz Amerike, ki je bila pod Trumpom vodilna zanikovalka virusa, Trumpov mandat pa se je končal z najvišjim številom mrtvih žrtev na svetu, je Biden uspel postaviti Ameriko na vrh vseh držav po precepljenosti prebivalstva.

Na Balkanu so v zadnjih letih, ko je bila EU tam premalo prisotna, politično prevladali Rusi, gospodarsko pa Kitajci. Prisotnost obeh bo treba uravnovežiti z gospodarskim in predvsem političnim vplivom Evrope na Balkanu, ker druge poti enostavno ni.

Nove ameriške sankcije zoper Rusijo, kot tudi možen paket sankcij EU zaradi kršenja človekovih pravic Putinovemu oporečniku Aleksandru Navalnemu, so velika grožnja ruskega gospodarstvu. Putin se tega seveda zaveda a gre očitno za skrben „cost-benefit“ izračun, saj v sporih z zahodom očitno išče razloge za odvrčanje pozornosti od notranje političnih težav. Putinova popularnost upada, ljudje postajajo utrujeni od obljub o boljšem življenju, ki se ne uresničujejo, utrujeni so tudi od nenehnega iskanja sovražnikov, zlasti pa sporov z Evropo. Rusi vsak dan težje razumejo, zakaj je Evropa sovražnik in še manj razumejo, s čim jih lahko Evropa v resnici ogroža? Ko je ruski zunanji minister Lavrov grozil Evropi, da je vstop Črne gore in Severne Makedonije v NATO „strateška grožnja ruskim interesom“ ni bilo jasno v čem konkretno je ta grožnja. Odkar sta ti dve državi članici NATO pa je to jasno še manj. Navsezadnje se svobodne države same odločajo, v katere mednarodne organizacije bodo ali pa ne bodo vstopile, tudi v NATO. Je pa vsem postalo jasno to, da zahodne sankcije niso šala.

Ko sta EU in ZDA leta 2014 uvedli sankcije zoper Rusijo zaradi aneksije Krima se je ruski BDP na letni ravni domala prepolovil. Po podatkih Svetovne banke (tradingeconomy-

cs.com/russia/gdp) je absolutni ruski BDP leta 2013 znašal skoraj 2300 mrd USD, leta 2014 še 2060 mrd, potem pa sledi brutalen padec na vsega 1363 mrd leta 2015. Padec so povzročile finančne sankcije, prepoved dajanja posojil in omejitev ruskih poslov na finančnih trgih ter uvrstitev ruskih vodilnih poslovnih na liste s prepovedjo potovanj na zahod. Rusija si od takratnih zahodnih sankcij še do danes ni povsem opomogla, pa že prihajajo nove. Ruski BDP je leta 2019 dosegel 1700 mrd in na tej ravni pričakovano stagnira zaradi korona-virusne krize.

Iz podatkov o posledicah sankcij je postalo jasno naslednje;

- da je rusko gospodarstvo usodno odvisno od povezanosti z evropskim trgom, ki kupuje večino ruske proizvodnje plina po cenah, ki jih Rusija ne more doseči nikjer drugje;
- da Rusija na mnogih področjih ni dovolj samozadostna, posebej pa ko gre za finančni kapital, za visoko tehnološke izdelke in hrano;
- in da Rusija kot vojaška velesila in gospodarski palček ni konkurenčna v tekmi z EU, ki je gospodarski velikan in vojaški palček.

Iz teh podatkov jasno izhaja, da sta Rusija in EU v resnici sila kompatibilen par, a ne zmoreta političnih korakov v smeri sodelovanja. A večji delež krivde je brez dvoma na ruski strani. Rusija se sooča s sindromom „nekdanje veličine“, s kakršnim se je spopadal Habsburški imperij po koncu prve in Britanski imperij po koncu druge svetovne vojne. Ni se lahko sprijazniti s hudo skrženo veličino nekdanje Sovjetske zveze, je pa soočenje z dejstvi edini izhod. Kdor se ne sooči z dejstvi, se dejstva soočijo z njim, je ugotavljal že Winston Churchill. Namesto partnerstva z EU, ki bi dvignil rusko ekonomijo na višjo raven, se Putin predaja podcenjevanju EU in podpiranju evropskih populistov. Putin še vedno prisega na grožnje z orožjem in osvajanje ozemelj, kar je manira srednjega veka, Rusija pa namesto razvoja pridobiva zgolj dodatne stroške.





Samo okupacija Krima Rusiji prinaša ogromne stroške, v prvi vrsti doplačevanje nizkih pokojnin in prispevkov prebivalstvu priključenega Krima. Hude so tudi politične posledice, ne le sankcije, ampak tudi ugled Rusije v mednarodni skupnosti.

EU in Balkan

Ena od posledic odsotnosti dialoga med Rusijo in EU so tudi razmere na Balkanu. Na Balkanu so v zadnjih letih, ko je bila EU tam premalo prisotna, politično prevladali Rusi, gospodarsko pa Kitajci. Prisotnost obeh bo treba uravnotežiti z gospodarskim in predvsem političnim vplivom Evrope na Balkanu, ker druge poti enostavno ni. EU se je pri širitvi na Balkan že nekajkrat močno utrudila in skoraj povsem ustavila. Posledice za Balkan pa so bile vsakič resnejše, zadnja leta so celo zelo hude. Na Balkanu države praktično nimajo več političnih stikov, nihče jih več niti ne spodbuja k srečevanju za reševanje odprtih vprašanj. Hrvaška in Srbija že vse od konca vojne nista uredili niti osnovnih odprtih vprašanj in niti vprašanja meja. Se pa po Balkanu znova prenašajo grožnje po medijih, s sumljivimi dokumenti po sumljivih diplomatskih in znova tudi (proti)obveščevalnih kanalih. Seveda pa ni vsega kriva EU, ki lahko pripelje konja do vode, ne more pa ga prisiliti, da jo pije. Srbija, ki je ključna za stabilnost celotnega Balkana, je bila že zelo daleč na poti v EU, a se je ustavila pred zidom demonov svoje lastne preteklosti. Srbija se ne zmore prijazniti z dejstvom, da je Kosovo zanj že dve desetletji izgubljeno in ne zmore realno oceniti dejstva, da kot članica EU ne bo mogla sedeti na dveh stolih; na stolu EU in evropske strateške varnosti in še na stolu Rusije, države, ki strateško varnost Evrope ogroža. Tako Srbija, kot tudi vse ostale balkanske kandidatke za vstop v EU, se bodo morale soočiti z dejstvom, da sta se svet in z njim Evropa v zadnjih letih močno spremenila. Rusija in Kitajska sta od gospodarskih tekmi postali nevarni nasprotnici Evrope ravno v času, ko sta obe zagospodarili na Balkanu. Ob teh dveh pa seveda še Turčija, ki je pod Erdoganovo vladavino od nekdaj kandidatke za vstop v EU posta-

Zato nam Evropejcem tudi na Balkanu ne preostane nič drugega kot strpno in mukotrpno zagovarjanje in promoviranje temeljnih človekovih pravic in demokracije, z doslednostjo in dialogom. Ker prav to so temeljne evropske vrednote, na katerih temelji mir, ki ga Evropski narodi uživamo od konca druge svetovne vojne.

la njen nasprotnik, predvsem pa goreči sovražnik evropskih vrednot. Turčija ima sicer največji vpliv med Bošnjaki v BiH, a tudi med albanskim prebivalstvom na Kosovu in v Severni Makedoniji. A vse te verske in nacionalne razlike na Balkanu, ki povzročajo politične napetosti in konflikte, so le navidezne. Tako kot vedno, odkar obstaja svet, se pod njimi skrivajo materialni interesi lokalnih in tujih gospodarjev, ki bolj kot v bogove verjamejo v denar.

Zato nam Evropejcem tudi na Balkanu ne preostane nič drugega kot strpno in mukotrpno zagovarjanje in promoviranje temeljnih človekovih pravic in demokracije, z doslednostjo in dialogom. Ker prav to so temeljne evropske vrednote, na katerih temelji mir, ki ga Evropski narodi uživamo od konca druge svetovne vojne. Če pomislimo, kako pomemben je na Balkanu nogomet, je praktično način življenja, potem je jasno, da smo z obranitvijo evropskega nogometa pred njegovo amerikanizacijo veliko storili tudi za stabilnost Balkana. Ker tudi kadar se politiki na Balkanu sploh ne pogovarjajo, lahko klubi in nacionalne reprezentance nemoteno igrajo vsaj nogomet ■

INTERVJU

Dr. Mitja Štular,

član uprave Telekom Slovenije, d.d.*

TELEKOM SLOVENIJE SMELO UVAJA NOVE TEHNOLOŠKE REŠITVE

Telekom Slovenije izredno velik poudarek namenja uvajanju novih tehnoloških rešitev, ki zagotavljajo večjo poslovno učinkovitost in varnost uporabnikov njihovih storitev. Ob tej priložnosti smo se o pomenu kibernetске varnosti pogovarjali z dr. Mitjo Štularjem, članom uprave Telekoma Slovenije, ki je odgovoren za tehnologijo.

S svojim poslovanjem ste močno prisotni, tako na nacionalnem, kot v širšem regijskem področju telekomunikacijskih storitev, kjer so varnostna tveganja še posebej specifična. Ali svoje odločitve o širitvi poslovanja na določene trge temeljite na strateških analizah varnostnega okolja ali bolj upoštevate poslovne možnosti?

Oboje. Potrebno se je zavedati tako tveganj in specifičnosti posameznih okolij kot tudi poslovnih možnosti. Zavezani smo k zagotavljanju vrhunskih storitev, visoka stopnja varnosti je naš končni cilj. Imamo sodoben lasten Operativni center kibernetске varnosti, v katerem naši strokovnjaki 24 ur na dan spremljajo in upravljajo različne varnostne izzive v informacijsko-komunikacijskem okolju. Storitve izvajamo, tako zase in skrbimo za varnost svoje infrastrukture in

Svojim naročnikom na področju kibernetске varnosti lahko ponudimo najboljše, kar trg v danem trenutku premore – rešitve, ki jih uporabljamo tudi sami. Z visokimi varnostnimi zahtevami in standardi za potrebe lastnega poslovanja smo na ta način sami sebi najboljša referenca.

storitev, kot za mnoga podjetja, ki nam zaupajo takšno ključno področje, kakor je varnost.

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

Digitaliziramo svet okoli nas – z rešitvami, ki morajo biti preproste, navdihujoče, skrbne, prebojne in varne. Digitalizacija pa ne sme biti sama sebi namen – mora zagotoviti, da bo življenje enostavnejše, bolj učinkovito in bolj varno. To delamo na številnih segmentih, od gradnje omrežij, optičnega in mobilnega, do razvoja in ponudbe številnih IKT rešitev za zasebne in poslovne uporabnike. Iščemo partnerstva in želimo biti odličen partner našim uporabnikom, podjetjem in tudi drugim operaterjem, ki uporabljajo naše rešitve. Upravljamo največje dostopovno optično omrežje v državi, priklop nanj trenutno omogočamo več kot 370.000 slovenskim gospodinjstvom, omrežje pa nenehno nadgrajujemo in širimo. Na področju uvajanja 5G tehnologije smo že sedaj vodilni na trgu in tako bo tudi v prihodnje. Po pridobitvi dodatnega frekvenčnega spektra imamo odprta vrata za širitev omrežja ter popoln izkoristek zmogljivosti, ki jih prinaša peta generacija mobilnih omrežij. Uvajamo novosti, razvijamo rešitve pametnih mest, skupaj s partnerji smo pomemben del industrije 4.0, osredotočamo se na področja javne varnosti in zdravstva. Pri vsem tem pa skrbimo tudi za visoko stopnjo kibernetске varnosti, ki je eden izmed temeljev zaupanja v povezanem svetu, kjer smo odprti, a moramo biti hkrati tudi varni.



Aktivno uvajanje tehnologij 5G je postalo realnost. Telekom Slovenije je na našem tržišču prvi začel s tem zahtevnim procesom. Kako bi ocenili dosedanje izkušnje? Se že kažejo pričakovani rezultati?

Biti vodilen v zahtevni in tehnološko-razvojno usmerjeni telekomunikacijsko-informacijski panogi je za nas kot maraton. Ni hitrih zmag, štejejo strokovnost, vztrajnost, strategija in vizija. 5G je del evolucijskega procesa razvoja omrežij, enako kot predhodne generacije. Te med seboj sobivajo, uporabniki prehajajo med njimi, ne da bi se tega sploh zavedali, vse morajo zagotavljati vrhunsko storitev. Uvedbe 5G smo se v Telekomu Slovenije lotili načrtno, strateško in predvsem pravočasno; infrastrukturo in sisteme smo temeljito pripravljali na komercialni vstop na trg. Prvi v Sloveniji smo tako uporabnikom komercialno ponudili omrežje, storitve in mobilne naprave. Dosedanje izkušnje so zelo pozitivne in koristne, usmerjeni pa smo predvsem v prihodnost in na naslednje korake v razvoju 5G, s katerimi bomo omrežje in pokritost širili, nadgrajevali hitrosti, odzivne čase in zmogljivosti, izkoriščali polni potencial tehnologije ter skupaj s partnerji ustvarjali rešitve za industrijo in javni sektor. Uporabniki so v tem času sicer že spoznali nekatere prednosti 5G, velika večina teh pa šele prihaja.

V zadnjem obdobju kibernetiki varnosti posvečate ogromno svoje strokovne pozornosti. Posebej vaš Operativni center kibernetike varnosti postaja eno izmed

pomembnih orodij za zagotavljanje višje stopnje kibernetike varnosti tudi pri velikem številu slovenskih organizacij, ki jim nudite to podporo. Kako ocenjujete evolucijo slovenskega trga na področju zagotavljanja kibernetike varnosti?

Vzporedno se odvija evolucija na strani ponudnikov in uporabnikov. Uporabniki vedo, da je neurejena informacijska varnost poslovno tveganje, ki lahko poruši poslovne procese, vodi k izgubi podatkov, zaupanja trga in denarja. Vedo tudi, da je nabor tveganj tolikšen, da lahko nanje odgovori le specializirana ekipa strokovnjakov, ki ima na voljo vpogled v svetovne trende in ki razpolaga z ustrezno informacijsko opremo. Tovrstni vložki so visoki, zato si jih posamezno podjetje težko privoščijo, k začetni investiciji pa mora priseti še stalna vlaganja v razvoj ekipe, pa programsko in strojno opremo. Zgolj požarni zid in antivirusna programska oprema ne zadoščajo več.

Danes smo v internet povezani ves čas tako prek službenih kot zasebnih naprav, računalnikov, mobilnih telefonov, tablic. Zato je potrebno varnost naslavljanje celovito, prek vseh točk, kjer bi lahko prišlo do poskusov vdora v sisteme. Za večino podjetij in ustanov je bolj smotno, da upravljanje informacijske varnosti zaupajo specialistu, kot smo mi. V Telekomu Slovenije smo se v zadnjih letih močno razvili in okrepili na tem področju.

DIGITALIZIRAMO
SVET
PRILOŽNOSTI

Verjamem, da je področje korporativne varnosti med tistimi, ki jim bodo podjetja namenjala vedno več pozornosti. S hitrim tehnološkim razvojem, pri katerem bo kmalu skoraj vsak predmet v naši okolici že samostojno komuniciral, se nabor tveganj v povezanem svetu nikakor ne zmanjšuje.

V bistvu smo začeli pri sebi, z razvojem informacijsko-komunikacijske varnosti za lastne potrebe in za potrebe uporabnikov naših omrežij. Zaradi številnih potreb na trgu pa je to preraslo v izjemno profesionalen Operativni center kibernetične varnosti, kjer rešujemo tudi varnostne izzive drugih podjetij.

Kako pristopate k prenosu lastnih varnostnih standardov v produkte, ki jih ponujate kot podporo delovanja

drugih pomembnih organizacij? Verjetno je to pri storitvah zagotavljanja kibernetične varnosti ključnega pomena, saj jih zagotavljate med drugim tudi za deležnike kritične infrastrukture?

V vseh primerih gre za enoten pristop. Visoki varnostni standardi so tukaj, tako zaradi nas, kot tudi potreb trga, zato so tudi vključeni v naše produkte kibernetične varnosti. Doseganje skladnosti, na primer z GDPR, ZinfV, ISO, ENISA nabavnimi priporočili, notranjimi pravili in podobno, je sestavni del naših procesov in tržne ponudbe. Imamo ekipo izjemnih strokovnjakov, ki so specializirani za določena področja kibernetične varnosti in ki imajo na voljo najsodobnejše tehnične rešitve. Na ta način zagotavljamo učinkovito delovanje glede na potrebe posamezne organizacije, celostno obravnavo, zanesljivost in transparentnost. Gradimo zaupanje in dolgoročno sodelovanje.

Ob tem smo pomemben člen kritične infrastrukture, tako da se zelo dobro zavedamo pomena varnosti za naše poslovanje in za širše okolje. Svojim naročnikom na področju kibernetične varnosti lahko ponudimo najboljše, kar trg v danem trenutku premore – rešitve, ki jih uporabljamo tudi sami. Z visokimi varnostnimi zahtevami in standardi za potrebe lastnega poslovanja smo na ta način sami sebi najboljša referenca.

Kako uspete v podjetju zagotavljati uravnoteženost med na eni strani zelo restriktivnimi varnostnimi zahtevami varovanja ključnih informacij organizacije in na drugi raziskovalnimi iniciativami, ki so včasih zelo občutljive na prevelike omejitve delovnega okolja?

Drži, varnost lahko včasih prinese tudi določene omejitve, ampak vse z razlogom, zato je ključna visoka stopnja zavedanja te tematike. Varnost je del poslovne kulture. Krepimo jo z načrtnimi usposabljanji vseh sodelavcev, zato v podjetju vlada visoko zavedanje, kako pomembna je informacijska varnost za naše delo, poslovanje in nastop na trgu.

Seveda pa smo tudi prilagodljivi in odprti. Ne glede na to, da pogosto slišimo, da varnosti ni nikdar preveč, je pri tem potrebno biti tudi razumen – zagotavljanje varnosti je spremljajoča dejavnost, katere namen je zmanjševanje varnostnih tveganj pri opravljanju naše osnovne dejavnosti.

Pri tem sledimo tudi dobrim strokovnim praksam, saj sodelujemo s številnimi domačimi in mednarodnimi organizacijami. Ob tem poleg nenehnega izobraževanja, uporabe najsodobnejših orodij, procesov in certifikacij vlagamo tudi v pridobivanje podatkov o morebitnih ranljivostih in grožnjah na področju informacijske varnosti ter sodelujemo z različnimi organizacijami na področju informacijske

varnosti (SI-CERT, Enisa, Europol). Pridobljeno znanje, izkušnje in strokovnost nenehno preverjamo, tako z odzivi na varnostne incidente kot s sodelovanjem v različnih mednarodnih vajah s področja kibernetске zaštite.

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?

Povezani smo učinkovitejši, izmenjujemo izkušnje, dobre prakse, rešujemo izzive. Strokovno povezovanje lahko vodi k vsemu temu, zato je ključno, da smo kot vodilni slovenski operater del tega združenja. Dvig varnostnega zavedanja je proces, v katerem se napredek odraža postopno, s stalnimi vlaganji ter predvsem z ustreznim komuniciranjem glede tveganj za organizacije in možnih rešitev oz. poznavanjem dobrih praks. Verjamem, da je področje korporativne varnosti med tistimi, ki jim bodo podjetja namenjala vedno več pozornosti. S hitrim tehnološkim razvojem, pri katerem bo kmalu skoraj vsak predmet v naši okolici že samostojno komuniciral, se nabor tveganj v povezanem svetu nikakor ne zmanjšuje.

Fotografiji: arhiv Telekom Slovenije. ■



Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij.

Skozi združenje člani organizirano uresničujejo osebne in poslovne interese na področju korporativne varnosti.



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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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



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:

- postavitve 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.



INTERVJU

Božidar Dajčman,

direktor Oddelka upravljanja fizične in informacijske varnosti, Nova KBM d.d.*

KORPORATIVNA VARNOST JE POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE USTREZNE ODPOORNOSTI DELOVANJA ORGANIZACIJE

V današnjem zahtevnem varnostnem okolju je zagotavljanje odpornosti in s tem neprekinjenosti delovanja velikih poslovnih organizacij, nujna za poslovno učinkovitost. Korporativna varnost ima v tem okviru posebej izraženo vlogo in odgovornost.

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

V svet varnosti sem vstopil pred sedmimi leti, najprej na področje informacijske varnosti. Kljub temu, da sem imel takrat že veliko izkušenj z informacijsko tehnologijo, organizacijo in bančništvom, je bil začetek poln presenečenj. Kot bi odprl bomboniero Foresta Gumpa, kjer nikoli ne veš, kaj se skriva v ovitku. Tudi kasneje sem se največ časa ukvarjal s kibernetskimi tveganji, veliko pa tudi s tveganji fizične varnosti in neprekinjenega poslovanja. Ob začetku epidemije COVID-19 smo vsi največ pozornosti posvečali ukrepom za zdravje naših strank in zaposlenih.

g. Božidar Dajčman je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2020«

Vsa ta področja se medsebojno prekrivajo v pojmi kot so »tveganje«, »varnostni ukrepi«, »incident«, »načrt odziva«, »odpornost«, »obrambne linije«. S temi pojmi se srečujem vsak dan, vendar vsakič malo drugače. Na žalost in na srečo moje delo še ne kaže znakov, da bi postajalo rutinsko.

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

Gotovo. Podjetje lahko tudi z omejenim proračunom uspešno zmanjša tveganja, če jih dobro razume. Pomembno je, da denar in energijo posvečamo pravim tveganjem, torej tistim z večjim produktom frekvence in učinka. To ni niti samoumevno niti lahko, saj so nekatera tveganja bolj vidna in razumljiva kot druga. Podjetje, ki pozna tveganja, bo sprejelo boljše odločitve o tem, katerim tveganjem se je treba izogniti, katerim je treba zmanjšati verjetnost ali učinek in katera si deli z zavarovalnico. Na koncu je treba določena tveganja tudi sprejeti. Prave odločitve prinašajo optimalno uporabo virov in obvladana tveganja, s tem pa prednost pred konkurenti.



Bančni sektor je zaradi regulativnih zahtev in varnostnih tveganj, ki se vedno bolj selijo v informacijsko okolje, zelo specifičen pri svojem delovanju. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Bančno poslovanje je obvladovanje in sprejemanje tveganj. Vsakič, ko banka odobri kredit, prevzame tveganje, da denarja ne bo dobila nazaj.

Regulatorji skrbijo, da banka sprejme samo toliko tveganja, kolikor ga lahko z lastnim kapitalom prenese tudi v pesimističnih scenarijih. V prihodnosti se lahko zgodi, da bodo odločilna tudi varnostna tveganja.

Če zelo poenostavimo, sta koraka za obvladovanje tveganj samo dva: analiza tveganj in izvedba ukrepov za njihovo zmanjšanje. V resnici je precej bolj zapleteno. Različne vrste tveganj banka obravnava z različnimi koraki, vendar na koncu pridemo do skupne slike – profila tveganosti banke. Pri izračunu potrebnega kapitala banke so upoštevana vsa tveganja. Za operativna tveganja, kamor sodijo tudi varnostna, uporabljamo poseben okvir upravljanja. Ta opisuje korake, s katerimi zagotovimo, da tveganja ne presežejo sprejemljivih okvirov. Sprejemljivi okviri so tudi formalno opredeljeni v izjavi o nagnjenosti k prevzemanju tveganj.

Sistem obvladovanja tveganj v bankah je za zunanje opazovalce videti precej zapleten in ta videz ne vara. Ne glede na to, pa je osnovni gradnik logično razmišljanje z nekaj matematike.

Informacijska varnost je v vaši dejavnosti izrednega pomena. Še posebej so se ti izzivi izpostavili ob trajanju

Podjetje, ki pozna tveganja, bo sprejelo boljše odločitve o tem, katerim tveganjem se je treba izogniti, katerim je treba zmanjšati verjetnost ali učinek in katera si deli z zavarovalnico. Na koncu je treba določena tveganja tudi sprejeti. Prave odločitve prinašajo optimalno uporabo virov in obvladana tveganja, s tem pa prednost pred konkurenti.

epidemije COVID-19, saj je pomembna večina zaposlenih svoje delo začela opravljati izven svojega rednega informacijskega delovnega okolja. Kako v vašem podjetju ocenjujete izvajanje potrebnih ukrepov na tem kompleksnem področju?

Informacijska varnost je res še posebno poudarjena, saj banke razpolagajo z velikimi finančnimi sredstvi in je zato tudi potencialna korist za napadalca večja. Izpostavljeni so tudi komitenti, oz. njihova sredstva. Tveganja sledijo poslovanju: ker je večina poslovanja preseljena v digitalno okolje, je tam tudi večina tveganj.

COVID-19 je prinesel kup dodatnih izzivov. Na prvem mestu moramo poskrbeti za zdravje svojih strank in zaposlenih. Za tem pride na vrsto dodatna skrb za informacijsko varnost, ki

Vsaka tranzicija že zaradi svoje narave vedno prinaša dodatna tveganja. Pri vsaki spremembi je mogoče, da kakšen vidik zanemarimo ali naredimo napake. Poleg tega so spremembe vedno povezane z nekim prehodnim, začasnim obdobjem, ko je sistem bolj izpostavljen tveganjem. Ko je vmesno stanje mimo, pridejo do izraza prednosti.

je potrebna zaradi spremenjenega načina dela. Spremenila se je količina in vsebina dela na daljavo. Ne gre samo za to, da več ljudi dela od doma, ampak tudi omogočamo oddaljeno izvajanje nekaterih opravil, za katere je bila prej zahtevana fizična prisotnost. Kljub temu ne gre za neke nove rešitve, saj so bili tehnični pogoji za varno delo na daljavo na voljo že prej. Tehnika sama ne zadošča, deluje pa skupaj z drugimi ukrepi, od omejevanja pooblastil do ozaveščanja zaposlenih.

Premik se je zgodil tudi pri naših strankah. Kljub temu, da je bila večina poslovalnic odprta ves čas epidemije, so mnoge stranke na lastno ali našo pobudo prenesle poslovanje na digitalne kanale. Ti kanali so varni pred COVID-om, se pa tam stranke in banke srečujejo z drugačnimi virusi in drugimi tveganji.



Se v Republiki Sloveniji po vaše dovolj zavedamo pomembnosti področja kibernetske varnosti? So ukrepi, ki jih izvaja država na tem področju ustrezni ali pogrešate konkretnejše ukrepe?

Država ne more zagotoviti varnosti namesto posameznikov in podjetij, zato od nje ne smemo pričakovati preveč. Za zdaj smo lahko spremljali nekaj uspešnih in nekaj manj uspešnih zgodb. Med uspešne štejem dosedanje delovanje SI-CERT-a.

Upravi za informacijsko varnost bomo morali dati nekaj časa, da bo lahko opravila svojo vlogo nacionalnega organa za informacijsko varnost in želim, da bi jim to dobro uspelo. Tudi druge akterje v nacionalnem sistemu kibernetske varnosti čaka še veliko dela. Nikakor si ne želim dveh stvari: slabega sodelovanja med različnimi deležniki v sistemu in pretirane regulacije. So pa področja, kjer je regulacija potrebna in vloga države nenadomestljiva. To zagotovo velja za zagotavljanje delovanja kritične infrastrukture in bistvenih storitev, pri čemer ni pomembno samo kdaj in kako pri nas uvedemo direktive in uredbe EU, kot npr. NIS/NIS2, GDPR, ECI/RCA, DORA.

Tako kot v podjetju, so tudi na nivoju države nekatera tveganja bolj vidna in razumljiva, druga manj. Zato moramo razumevanje tveganj nadgrajevati. Pri tem je ceneje, če se učimo na tujih in ne lastnih napakah. V začetku leta smo videli, kakšna je moč internetnih velikanov, ki lahko po lastni presoji enostavno odklopijo družbeno omrežje ali podjetje. Po potrebi bi lahko odklopili tudi celotne države in vsa podjetja, ki v njih delujejo. Za ilustracijo si lahko skušamo predstavljati, kakšne bi bile posledice, če nenadoma nehajo delovati vse rešitve Google v Sloveniji: iskalnik Google, brskalnik Chrome, telefoni z operacijskim sistemom Android, zemljevidi in navigacija, Gmail, Google Drive, Google Docs... In kakšne bi bile posledice, če bi državo v celoti odrezali od interneta? Ne vem, ali ima država pripravljene načrte odziva na takšne dogodke, bi si pa to želel.

V zadnjem obdobju ste izvedli zelo zahteven poslovni proces združevanja dveh pomembnih bančnih ustanov v Republiki Sloveniji. Posebej z varnostnega vidika je bil to verjetno pomemben izziv, ki je prinesel tudi veliko novih izkušenj in dobrih praks. Lahko z nami podelite nekaj najpomembnejših?

Združitev druge in tretje največje banke v Sloveniji je bil zelo zahteven projekt, ki je prinesel velike organizacijske, tehnološke, produktne, kadrovske, lokacijske in druge spremembe. Dodatna okoliščina je bila epidemija COVID-19 v času, ko so potekale ključne naloge na področju operativnega združevanja. Vsaka tranzicija že zaradi svoje narave vedno prinaša dodatna tveganja. Pri vsaki spremembi je mogoče, da kakšen vidik zanemarimo ali naredimo napake. Poleg tega so spremembe vedno povezane z nekim prehodnim, začasnim obdobjem, ko je sistem bolj izpostavljen tveganjem. Ko je vmesno stanje mimo, pridejo do izraza prednosti.

Na področju varnosti je bilo naše izhodiščno načelo preprosto: tam, kjer banki nista imeli enakih rešitev, se uporabi bolj varna možnost, oz. višji standard. Že pred operativno združitvijo smo uvedli enotno varnostno politiko in podrejene dokumente. Potem smo potrebovali še nekaj časa, da smo varnost poenotili tudi na operativni ravni. Pri fizični varnosti to pomeni tudi dodatne in posodobljene sisteme tehničnega varovanja, pri informacijski varnosti pa opustitev nekaterih orodij in uvedbo drugih v povečanem obsegu.

V Novi KBM smo pravočasno pričeli postavljati strukturo in ekipo za upravljanje varnosti v večji banki, zato smo bili na združitev dobro pripravljeni.

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

Uprava Nove KBM se zaveda varnostnih tveganj in je pripravljena sorazmerno s tem tudi dodeljevati vire. Kljub temu ni tako preprosto. Predlogi morajo biti utemeljeni z jasnim vplivom na tveganja. Še posebno morajo biti argumenti močni, kadar gre za izdatke zunaj načrtovanih okvirov. Velja tudi pregovor »daleč od oči, daleč od srca«, zato skušamo izkoristiti vsako priložnost, da so varnostna vprašanja obravnavana na najvišjih nivojih upravljanja. Pomembno je, da je oddelek organizacijsko podrejen neposredno upravi.

Na koncu odloča medsebojno zaupanje, ki smo ga pri dosedanjem delu z upravo že vzpostavili.

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?

Nekaj informacij o stanju korporativne varnosti v okolju dobim od kolegov iz drugih podjetij, nekaj pa lahko sklepam glede na varnostne dogodke, za katere izvem.

V najslabšem primeru se zavedanje dvigne šele ob večjih incidentih. Zunaj finančnega sektorja ni mnogo organizacij, kjer je strateški management jasno ugotovil in opredelil kolikšna tveganja lahko organizacija prenese in kolikšna so pripravljene sprejeti, kar velja tudi za varnostna tveganja.

Po drugi strani tudi na dnevih korporativne varnosti srečujemo predstavnike podjetij, kjer je obvladovanje tveganj in še posebno korporativna varnost na visokem nivoju. To ne bi bilo mogoče brez podpore strateškega managementa.

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

Po mojih izkušnjah lahko najhitreje in najceneje zmanjšamo varnostna tveganja ravno z izbiro in oblikovanjem pravih kadrov. Še posebno na področju kibernetске varnosti poznam več primerov, ko so organizacije investirale velike zneske v tehnične rešitve, zmanjkalo pa je denarja ali volje za vzpostavitev ekipe, ki bi te rešitve izkoristila. Prodajalci varnostnih rešitev poznajo nešteto takih zgrešenih projektov (ni pa nujno, da o njih govorijo potencialnim kupcem).

Varnostna ozaveščenost ni le vprašanje informiranosti, ampak gre za del organizacijske kulture. Na žalost je včasih lažje zamenjati zaposlene, kot spremeniti njihov način razmišljanja in obnašanja. To še najbolj velja za nas managerje, saj je organizacijsko kulturo treba graditi od zgoraj navzdol.

Vaše podjetje je tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s



Skupaj s sodelavci v Novi KBM smo naredili že veliko, nikoli pa ne bo zmanjkalo izzivov na področju varnosti. Za pravi odziv na te izzive ni dovolj en človek. Imamo izredno ekipo, s katero je pravi užitek delati.

področja korporativne varnosti potrebna in lahko prinesejo v naš prostor dodatno kvaliteto?

Združevanje je potrebno, da lahko kot vsebinsko močna skupina prispevamo pri oblikovanju okvirjev varnosti v državi. Potrebno je tudi zaradi prenosa znanj in izkušenj. Sam sem se na srečanjih s kolegi že veliko naučil, vendar to ni edini razlog, da se udeležujem dogodkov združenja. Pridem predvsem zato, ker je zanimivo in prijetno.

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

Počaščen sem. To je elitna nagrada za področje korporativne varnosti. Kdor pozna dosedanje nagrajence, ve da je tako. Lepo je biti v taki družbi.

Skupaj s sodelavci v Novi KBM smo naredili že veliko, nikoli pa ne bo zmanjkalo izzivov na področju varnosti. Za pravi odziv na te izzive ni dovolj en človek. Imamo izredno ekipo, s katero je pravi užitek delati. ■

Tveganja povežite s poslovnimi kazalniki uspešnosti

Kulturo upravljanja tveganj pa vpeljite v čisto vse organizacijske procese

**SVETOVANJE O
UPRAVLJANJU
TVEGANJ**

**CELOVITO
UPRAVLJANJE
TVEGANJ**

**UPRAVLJANJE
ŠKODNIH
DOGODKOV**



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

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

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

UČINKI IN IZBOLJŠAVE ZA VAŠO ORGANIZACIJO

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

INTERVJU

g. Igor Zgonc, direktor Silver Bullet Risk

UPRAVLJANJE S TVEGANJI KLJUČEN DEJAVNIK ZA USPEŠNO POSLOVANJE ORGANIZACIJ

Aplikacija za upravljanje tveganj Silver Bullet Risk je letos na mednarodni konferenci Dnevi korporativne varnosti prejela najvišje priznanje - Slovenian Grand Security Award«, v kategoriji »Najbolj inovativna varnostna rešitev«. Ob tej priložnosti smo se o pomenu upravljanja s tveganji pogovarjali z g. Igorjem Zgoncem, direktorjem podjetja.

Podjetje Silver Bullet Risk predstavlja eno od vodilnih slovenskih podjetij na področju rešitev upravljanja s tveganji. Nam lahko prosim podrobneje pojasnite katera so glavna težišča vaših rešitev, ki na trg varnostnih rešitev prinašajo dodano vrednost?

Čeprav so tveganja neločljivo povezana z (uspešnim) poslovanjem vsakega podjetja in organizacije, je sistematično in predvsem učinkovito upravljanje tveganj dejavnost, ki se pri nas šele dobro razvija.

Razmeram na slovenskem trgu so prilagojene tudi naše rešitve, ki obsegajo tako izobraževanje in svetovanje podjetjem in organizacijam na področju upravljanja tveganj, kot tudi informacijski sistem oziroma orodje Silver Bullet Risk (SBR), ki jim procese upravljanja tveganj pomaga digitalizirati in s tem učinkoviteje nadzorovati ter upravljati.

Glavna dodana vrednost vseh treh stebrov našega poslovanja je osredotočenost na pomoč vodilnim kadrom in upravljalcem tveganj pri sprejemanju preudarnih poslovnih odločitev in posledično doseganju boljših poslovnih rezultatov, vključno s povečanjem varnosti.

S svojim poslovanjem želite biti prisotni tudi v širšem regijskem prostoru, kjer so varnostna tveganja še pose-

bej specifična. Ali svoje odločitve o širitvi poslovanja na določene trge temeljite tudi na strateških analizah varnostnega okolja ali bolj upoštevate poslovne možnosti?

Varnost, ki je širok pojem, je zagotovo eden izmed pomembnih dejavnikov poslovne uspešnosti nekega podjetja oziroma organizacije, vendar naši pristopi tveganja obravnavajo širše, torej celostno in procesno.

To pomeni, da jih spremljamo na vodstvenem in izvedbenem nivoju ter jih blažimo z različnimi ukrepi, vključno z var-

Glavna dodana vrednost vseh treh stebrov našega poslovanja je osredotočenost na pomoč vodilnim kadrom in upravljalcem tveganj pri sprejemanju preudarnih poslovnih odločitev in posledično doseganju boljših poslovnih rezultatov, vključno s povečanjem varnosti.

nostnimi. Tudi zato so uporabniki naših rešitev iz različnih področij, tako iz gospodarstva in negospodarstva kot državne uprave in kritične infrastrukture. Glede tujine pa je naš glavni cilj v tem obdobju uspešna prodaja orodja za upravljanje tveganj SBR, za katerega smo se prepričali, da je med vodilnimi tudi v mednarodnem merilu.

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

Razvojna vizija je zelo jasna in preprosta – rešitve vseskozi nadgrajujemo s tesnim sodelovanjem z našimi končnimi upo-

rabniki in sprotim prilagajanjem njihovim zahtevam. Pri tem so ključne povratne informacije o njihovih potrebah in pričakovanjih, ki jim prilagajamo tempo razvoja. Na tak način lahko zagotovimo, da rešitev praktično odgovarja na različne poslovne izzive, s katerimi se naše stranke soočajo danes in tudi na tiste, ki se bodo pojavili jutri.

Kako so po vašem mnenju pomembne ključne informacije podjetja v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču. Ali varovanju teh informacij v SBR namenjate veliko pozornosti?

Za uspešnost na globalnih trgih so ključne tri vrste informacij: kdo so končni kupci, kdo konkurenčni ponudniki ter, kako se kot podjetje razlikuješ od ostalih. Odgovor na slednje seveda izveš prek poznavanja lastnih prednosti in slabosti, ki jih posledično lahko pretvoriš v svoje prednosti in hkrati blažiš potencialna tveganja na trgu.

Glede na našo dejavnost se ukvarjamo predvsem z informacijami o dejavnostih, ki v podjetjih in organizacijah lahko upočasnijo ali celo preprečijo doseganje njihovih ciljev. Zato njihovem varovanju razumljivo posvečamo veliko pozornosti tako pri opravljanju svetovalnih storitev, kakor tudi pri zagotavljanju visoke stopnje varnosti naše informacijske rešitve SBR.

Ste letošnji prejemniki prestižne nagrade Slovenian Grand Security Award v kategoriji »Najbolj inovativna varnostna rešitev«. Nam lahko zaupate kaj vam pomeni prejem take nagrade?

Predvsem veliko in pomembno priznanje našemu delu. Z upravljanjem tveganj se namreč ukvarjamo že več kot deset let, pri čemer smo ves čas stremeli k rešitvi, ki bi bila primerna za širok krog poslovnih uporabnikov in bi jim omogočila učinkovitejše obvladovanje procesov na omenjenem področju. Zato nas veseli, da je njena kakovost dosegla ustrezno prepoznavnost za prestižno nagrado, ki si jo zagotovo zasluži. Poleg priznanja pa je seveda tudi velika odgovornost in spodbuda za delo v prihodnosti.

Kje v prihodnosti pričakujemo največje spremembe vezano na uvajanje novih tehnologij na področju obvladovanja varnostnih tveganj? Rešitve t. i. pametnih mest in digitalizacije so postale realnost. Vedno večjo pomembnost pa dobivajo tudi organizacije, ki upravljajo kritično infrastrukturo.

Najšibkejši člen pri varnostnih tveganjih vedno je in bo človeški dejavnik. Velik tehnološki napredek smo nedvomno dosegli z avtomatizacijo, informatizacijo in digitalizacijo varnosti na vseh področjih. V prihodnosti pa lahko pričakujemo vedno več rešitev, ki bodo temeljile na umetni inteligenci; pri čemer je pandemija, ki bo očitno še



nekaj časa naša realnost, spremembe na vseh teh področjih le še dodatno pospešila. Hkrati je razkrila tudi veliko ranljivosti in aspektov, ki se jim do sedaj tako na nivoju družbe, držav in podjetij nismo dovolj posvečali. Tudi zato smo lahko prepričani, da se bomo vprašanju učinkovitega upravljanja tveganj v vseh teh strukturah v bodoče morali bolj posvetiti, da bomo razpolagali z ustreznimi varnostnimi mehanizmi in protokoli in s tem pravočasno blažili morebitne posledice, saj smo videli, da so slednje lahko izredno hude.

Vaše rešitve presegajo samo področje obvladovanja varnostnih tveganj. V katerih segmentih, vezano na optimizacijo poslovnih procesov, lahko vaše rešitve najdemo?

Poslovanje je vsak trenutek in na vseh področjih povezano tudi z določenimi tveganji, saj se nam nesreča, vdor v informacijski sistem ali odpoved proizvodne linije lahko zgodi kadarkoli. Zato se posvečamo vsem področjem in procesom, ki pa se v različnih podjetjih, organizacijah in dejavnostih, seveda razlikujejo. V osnovi jih delimo na vodstvene procese, kjer se sprejemajo poslovne in strateške odločitve ter izvedbene procese, kjer potekajo temeljne dejavnosti. Naše poslanstvo pa je, da vodilnim iz množice notranjih in zunanjih podatkov oblikujemo razumljive in uporabne informacije za odločanje in preprečevanje uresničitve tveganj.

Glede na to, da ste visoko tehnološko podjetje ste vi in posredno vaše stranke v svoji dejavnosti zelo izpostavljene informacijskim tveganjem. Kakšne ukrepe v podjetju izvajate na področju zagotavljanja informacijske varnosti?

Z informacijsko varnostjo smo se začeli ukvarjati že leta 2003, ko smo postali svetovalci in revizorji za skladnost s standardom ISO27001. Temu je bila namenjena tudi naša prva informacijska rešitev, ki jo ponekod uporabljajo še danes. Vse od takrat znanje in izkušnje prenašamo v naše rešitve in jih upoštevamo pri svojem delu. Zato imamo seveda vpeljane tudi postopke za obdelavo in zaščito občutljivih podatkov, še posebej podatkov naših naročnikov. Informacijska varnost torej je in bo ostala eden od temeljev našega poslovanja.

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?

Pri tem upoštevamo dva dejavnika, in sicer človeškega in tehnološkega. Prvi temelj so zanesljivi in usposobljeni sodelavci, ki se zavedajo odgovornosti in pomena upoštevanja pravil za zagotavljanje informacijske varnosti. Zato vse občutljive podatke najprej anonimiziramo in šele nato obdelujemo v razvojnih in raziskovalnih procesih. Drugi temelj pa je tehnologija sama. Zavezani smo uporabi najvišjih varnostnih standardov pri prenosu, obdelavi, shranjevanju in upravljanju s podatki nasploh. Vendar, kot vemo, popolne varnosti ni; še več, to je tudi izziv sodobnega časa, s katerim se vseskozi soočamo tudi v vseh podjetjih in organizacijah, s katerimi sodelujemo.

Vaše podjetje bo verjetno v prihodnosti postalo eden od korporativnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s področja korporativne varnosti potrebne in lahko prinesejo v naš prostor dodatno kvaliteto?



Menimo, da je Slovensko združenje korporativne varnosti eno izmed najbolj aktivnih in prodornih v našem okolju, kar potrjuje tudi nenehna poslovna in strokovna dejavnost, ki jo izvajajo.

Menimo, da je Slovensko združenje korporativne varnosti eno izmed najbolj aktivnih in prodornih v našem okolju, kar potrjuje tudi nenehna poslovna in strokovna dejavnost, ki jo izvajajo. Zato je brez dvoma pomemben dejavnik pri izobraževanju, osveščanju in dvigu varnostne kulture nasploh. Svet se danes spreminja veliko prehitro, da bi lahko vse vedeli, znali in še posebej naredili sami. Poleg tega smo Slovenci precej znani tudi po vrtilčkanju, kar je na poslovnem področju zagotovo slabost. Osebnostno sem prepričan, da smo lahko uspešni samo s širjenjem znanja in sodelovanjem, saj bo tako tudi naš vrtilček postal večji in bolj rodovit.

Fotografiji: arhiv SBR. ■

Ustvarjamo popolnoma povezan,
pametni svet

HUAWEI IdeaHub

Nov stil **Pametna pisarna**

3 v 1 Tabla | Projektor | Spletni sestanek



INTERVJU

mag. Gorazd Ažman,

pomočnik direktorja Področja za strateške inovacije v družbi ELES*

POMEN INOVACIJ V OKVIRU ENERGETSKE TRANZICIJE

O pomenu inovacij na področju energetske tranzicije in določenih izzivih, med katerimi so posebej izpostavljena kibernetika tveganja, smo se pogovarjali z mag. Gorazdom Ažmanom. Elesovi ekipi se je pridružil maja 2017. Na Elesu se ukvarja s Strateškimi inovacijami in je član delovne skupine digitalizacija v okviru evropskega združenja sistemskih operaterjev ENTSO-E. Vodi tudi delovni sklop evropskega projekta OSMOSE, kjer se ukvarjamo s trgovanjem z električno energijo zelo blizu realnega časa.

S čim se ukvarjate pri vašem delu?

Osredotočam se predvsem na vsebine in naloge povezane z digitalizacijo, novimi poslovnimi modeli in trgi. Pomemben del aktivnosti predstavlja tudi povezovanje z drugimi sektorji, predvsem s plinskim, kjer mi pridejo prav izkušnje in poznavanje delovanja na področju plina.

Pri svojem delu na področju strateških inovacij spremljam trende in dogajanje tako v Sloveniji kot tudi v širšem mednarodnem prostoru. V ekipi, kjer delujem, snujemo inovacijske projekte, s katerimi rešujemo izzive v elektroenergetskem sistemu, povezane z vključevanjem vedno večjega deleža obnovljivih virov energije, aktivnejšo vlogo odjemalcev, širitvijo e-mobilnosti.

Kakšen je pomen inovacij pri prehodu na t. i. zeleno družbo, v okviru energetske tranzicije?

Na pomen energetske tranzicije ne gledamo samo znotraj elektroenergetskega sektorja, ampak tudi širše. Zato v zadnjem času veliko energije vlagamo v prizadevanja za vzpostavitev sodelovanja z drugimi sektorji, kot so npr. transport in plinski sektor ter sektor toplote. Z elektrifikacijo namreč prihaja do močnejšega povezovanja med sektorji. Posebej bi omenil ogrevanje in e-mobilnost, ki bosta pomembno vplivala tudi na delovanje elektroenergetskega sistema.

Pri našem delovanju se usmerjamo tako navznoter kot navzven. To pomeni, da pri določenih vsebinah in projektih vključujemo različna področja znotraj Elesu, ker z inovacijskimi projekti rešujemo njihove izzive. Po drugi strani pa, kot sem že prej omenil, s povezovanjem z drugimi sektorji naslavljamo prava vprašanja. Predvsem je pomembno, da pri svojem delu vključujemo tako sodelavce kot zunanje partnerje in z uporabo ustreznih znanj, izkušenj in kompetenc zmoremo celostno gledati na stvari in na ta način priti do optimalnih celovitih rešitev za sistem. Važno pa je tudi, da uspemo akterje na drugih področjih usmeriti tako, da s svojim delovanjem podpirajo energetske tranzicije.

Lahko izpostavite katere spremembe povezane z energijsko tranzicijo že zaznavate?

Vredno je omeniti, da je bil elektroenergetski sistem v preteklosti, če poenostavim, enosmerna cesta. Električna energija

Na osnovi močnejšega povezovanja z ostalimi sektorji, pa bomo uporabljali pri odločanju tudi podatke eden od drugega in se tudi na te vedno bolj zanašali. To bo zahtevalo dobro in zanesljivo usklajevanje in sodelovanje med nami.



proizvedena pri velikih proizvajalcih je bila preko prenosnega omrežja prenesena do operaterjev distribucijskih omrežji in preko njihovega omrežja do končnih odjemalcev.

To se sedaj že spreminja z večjim številom razpršenih proizvodnih virov. Na distribucijskem nivoju se v določenih obdobjih zaradi proizvodnje električne energije iz sončnih elektrarn zmanjša odjem, ki ga zaznamo tudi mi na prenosnem sistemu, saj se posledično zmanjša tudi odjem električne energije med prenosnim in distribucijskim omrežjem. Poleg tega na elektriko postopoma prehaja dodaten odjem, toplotne črpalke in e-vozila. Na tem nivoju se in se bodo v večji meri pojavljale dodatne potrebe. Potrebno jih bo nasloviti tudi tako, da čim bolj učinkovito izkoristimo obstoječo infrastrukturo in ne zgolj z novimi investicijami – tu imam v mislih pametna omrežja in seveda sodelovanje z drugimi sektorji. Z informacijsko podporo se usmerjam v to, kako čim bolj učinkovito povezati in uskladiti delovanje sistema, razpršene proizvodnje in fleksibilnega odjema, ob vsem zavedanju izzivov.

Poleg tega je Slovenija tranzitna država tudi v smislu elektroenergetskega sistema. Slovenski prenosni sistem, ki ga upravljamo na Elesu, je eden najbolje povezanih s sistemi sosednjih držav. Zato v našem sistemu dobro »čutimo« kdaj je zaradi vetra na severu Nemčije več proizvodnje iz vetrnih elektrarn, pa tudi kdaj je v Italiji ob sončnem vremenu več proizvodnje iz sončnic in ne le kdaj je višek proizvodnje iz hidro elektrarn na Balkanu. S projektom SINCRO.GRID v sodelovanju s partnerji v Sloveniji in na Hrvaškem tako naslavljamo prav te iz-

zive, na način, da izboljšamo vključevanje obnovljivih virov v sistem in bolj usklajeno obvladujemo pretoke energije.

Hkrati moramo razumeti, da se bodo vse aktivnosti upravljale vedno bližje realnega časa in na podlagi čim bolj točnih in zanesljivih podatkov. Tako bomo lažje sprejemali boljše odločitve. Na osnovi močnejšega povezovanja z ostalimi sektorji, pa bomo uporabljali pri odločanju tudi podatke eden od drugega in se tudi na te vedno bolj zanašali. To bo zahtevalo dobro in zanesljivo usklajevanje in sodelovanje med nami.

Torej ne bo ključna le izmenjava energetskih podatkov ampak tudi neenergetskih podatkov. Kje vidite izzive, tudi na področju kibernetične varnosti, v povezavi z izmenjavo teh podatkov?

O pomenu podatkov iz drugih virov sem že nekaj povedal, če sem nekoliko bolj konkreten. Na Elesu smo razvili in v polni meri začeli uporabljati sistem za ugotavljanje meja obratovanja naših daljnovodov. To izvajamo ob upoštevanju tehničnih parametrov oziroma omejitev daljnovodov, pretokov v omrežju in tudi vremenskih podatkov. Če upoštevamo vreme, mora biti vir zanesljiv, oziroma si zagotovimo celo več različnih virov podatkov. Govorim o tem, da zunanji vir vpliva na naše odločitve – vzpostavili smo zaupanje, da so rezultati našega obratovanja še boljši. Del tega izziva bomo dodatno naslovili skozi evropski projekt CyberSEAS.

Na nivoju razpršene proizvodnje in prožnega odjema, pa seveda zasledujemo cilj, da je infrastruktura optimalno obremenjena. En primer je počasno vodeno polnjenje e-vozil ali pa dostop do prožnosti. Tukaj govorimo o dostopu do vsake naprave. Želim izpostaviti ranljivost na nivoju naprave – ne le na nivoju odjemalca. Čas velikih sprememb je tudi čas velikih priložnosti in v te segmente vstopajo različni igralci. Tu so seveda razlike med resnimi uveljavljenimi igralci in manjšimi zagonskimi podjetji. Izhodiščno domensko znanje je različno, posledično tudi pristopi. Ampak če se odmaknem od tega, imamo in bomo imeli v sistemu naprave, ki niti ne želijo biti vodene, ampak imajo proizvajalci omogočen daljinski dostop zaradi vzdrževalnih posegov. Torej ne govorimo niti o celovitih sistemih, lahko so samo nastavki, ki omogočijo dostop do naprave. Če na tem nivoju pride do vdora, lahko nekdo preko vklopa in izklopa najprej samo opazuje kaj se v sistemu dogaja, kako sistem na to odreagira ali pa to zlorabi. Spet na drugi strani zato vidim priložnost za podjetja, katera bodo razvila sisteme, ki bodo takšne nenavadne aktivnosti opazili in nanje opozorili oziroma jih celo onemogočili.

Torej do naprav bo na podoben način dostopalo več akterjev. Bodisi z namenom upravljanja odjema ali pa z namenom dostopa do podatkov za potrebe odločanja. Seveda vse na zanesljiv in zaupanja vreden način. Moramo se namreč zavedati, da bo sistem ranljiv toliko kot njegov najšibkejši člen. Torej ne govorimo le o varnosti zaprtih SCADA sistemov, ampak bodo v prihodnje vpliven del sistema številčne in razpršene naprave, ki bodo povezane preko recimo 5G omrežij. Spremljam dogajanje na tem segmentu in vidim, da strokovnjaki s področja kibernetske varnosti že danes tudi temu delu posvečajo veliko pozornosti.

Če se spet vrneva na vaše primarno področje dela, kakšno vlogo ima ELES na področju izvajanja raziskav, razvoja in inovacij?

ELES zelo dobro sodeluje z drugimi družbami, raziskovalnimi institucijami in univerzami. Sodelujemo pri razvoju novih rešitev in produktov ter jim s tem pomagamo. Z oblikovanjem pravih vsebin za naše projekte namreč aktiviramo tudi zunanje okolje. Tako se podjetja, raziskovalne ustanove in univerze lotevajo novih tem in s tem dosežemo širši vpliv na širšo družbo kot bi ga v primeru, če bi projekte izvajali zgolj znotraj Elesu in samo zase. Skozi evropske in druge investicijske projekte uspešno vključujemo zunanje deležnike iz Slovenije, pa tudi izven naših meja. Tako pomagamo nekaterim slovenskim podjetjem, da razvijejo določene rešitve ali pridobijo reference, ki jim pomagajo pri njihovem nadaljnjem delu ali širjenju poslovanja.

Zdi se mi ključno, da ostajamo precej odprti za nove ideje, da spremljamo dogajanje in se tudi naučimo kakšne nove stvari, da imamo široko razumevanje področij tako znotraj elektroenergetskega sistema kot tudi izven, ter da znamo poiskati prave rešitve za nas.

Kaj še nameravate storiti, da bi bili v prihodnje še uspešnejši na področju strateških inovacij?

V aktivno inovacijsko delovanje želimo vključiti še več sodelavcev in zunanjih deležnikov ter aktivno sodelovati pri uspešnem energetskega prehodu v nizkoogljično družbo. Tako v zadnjem času precej pozornosti namenjamo vzpostavitvi širše kulture inoviranja v podjetju. Trenutno pripravljamo poseben pristop zbiranja tem za nove inovacijske projekte



Zdi se mi ključno, da ostajamo precej odprti za nove ideje, da spremljamo dogajanje in se tudi naučimo kakšne nove stvari, da imamo široko razumevanje področij tako znotraj elektroenergetskega sistema kot tudi izven, ter da znamo poiskati prave rešitve za nas.

znotraj Elesu, ki jih nameravamo podpreti na pravi način. Če želimo biti še bolj inovativni, to lahko dosežemo samo tako, da vključimo več sodelavcev. Potem pa skozi ideje, ki pridejo od vseh nas, poiščemo vsebine in rešitve, ki jih najbolj potrebujemo pri svojem delu za naslavljanje izzivov, ki so pred nami. Na ta način želimo preoblikovati ELES v še bolj učinkovito in inovativno podjetje.

Fotografiji: arhiv ELES. ■



iLOQ 5 Series

Digitalni sistem zaklepanja za kritično infrastrukturo

- Prvi digitalni sistem zaklepanja na svetu z lastnim napajanjem
- Brez baterij in kablov
- Mobitel kot ključ in vir energije (uporablja tehnologijo NFC) ali digitalni ključ (kot vir energije uporablja indukcijo)
- Brez stroškov vzdrževanja
- Oddaljeno upravljanje avtorizacij z iLOQ Manager programsko opremo v oblaku
- Revolucionarna rešitev za zahtevna varnostna okolja z veliko dislociranimi enotami
- Visoka varnost (PKI in AES – 256 šifriranje)
- Odpornost na ekstremne vremenske razmere
- Zmanjšani stroški življenjskega cikla sistema zaklepanja
- Zelena, trajnostna rešitev



Digitalni sistem zaklepanja iLOQ 5 Series je možno nadgraditi v kontrolo dostopa iLOQ Online, ki jo lahko v celoti upravljamo na daljavo in dodajamo časovne profile. V isti sistem lahko dodamo digitalne cilindre, obešanke, pohištvene ključavnice, zidne trezorje za ključe ter RFID in PIN čitalce.



Dealni partner za
identifikacijo in varnost

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





NOVI EVROPSKI PREDPISI V ZVEZI Z UPORABO BREZPILOTNIH ZRAKOPLOVOV

Republika Slovenija je prvo zakonodajo s področja brezpilotnih zrakoplovov sprejela leta 2016. Pristojnost za izvajanje nalog je tedaj podelila Javni agenciji za civilno letalstvo Republike Slovenije. V letu 2018 in 2019 pa je bil sprejet paket evropske zakonodaje s področja brezpilotnih zrakoplovov, s katero je nadzor, nad izvajanjem določil te zakonodaje po državah članicah, prevzela Agencija EU za letalsko varnost.

Uvod

Področje brezpilotnih zrakoplovov tako po novem urejata dva evropska predpisa. Izvedbena uredba Komisije (EU) 2019/947 z dne 24. maja 2019 o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov (v nadaljevanju: Uredba 2019/947/EU) določa pravila za upravljanje sistemov brezpilotnih zrakoplovov, pa tudi za osebe, vključno s piloti na daljavo, in organizacije, ki izvajajo navedene operacije. Kot pristojni organ za izvajanje te uredbe in za nadzor nad navedenim predpisom, je določena Javna agencija za civilno letalstvo Republike Slovenije, v manjšem obsegu pa nadzor vršijo tudi Policija in občinska redarstva. Delegirana Uredba Komisije (EU) št. 2019/945, z dne 12. marca 2019 o sistemih brezpilotnega zrakoplova in operatorjih sistemov brezpilotnega zrakoplova iz tretjih držav, določa zahteve za proizvajalce, uvoznike, distributerje itd. brezpilotnih zrakoplovov. Zahteve se nanašajo zlasti na določitev tehnične dokumentacije glede proizvoda in njegovo ustrezno označevanje (oznaka CE, izjava ES o skladnosti, serijska številka proizvoda itd.). Uredba določa tudi ob-

veznost nadzora trga glede brezpilotnih zrakoplovov, ki naj jo izvaja organ, pristojen za nadzor trga. Pristojnost na tem področju si zato delita Tržni inšpektorat Republike Slovenije in Ministrstvo za infrastrukturo.

Bistvena razlika med »staro« slovensko uredbo in Uredbo 2019/947/EU je zlasti v tem, da je domača zakonodaja temeljila na ločitvi operacij, ki se izvajajo za namen dejavnosti in pa operacijami, ki se izvajajo za šport in rekreacijo. Tisti, ki so z brezpilotnimi zrakoplovi izvajali dejavnost, so morali izpolniti več zahtev v primerjavi s tistimi, ki so brezpilotne zrakoplove uporabljali v prostem času. Po drugi strani so bili slednji tudi s predpisom bolj omejeni. Nova EU zakonodaja pa take delitve ne pozna. Tveganost

operacije definira količino zahtev, ki jih morata izpolniti operator in pilot na daljavo. Bolj, ko je tvegana operacija, več zahtev je treba izpolniti in obratno.

Uredba 2019/947/EU

Operacije brezpilotnih zrakoplovov se v skladu z Uredbo 2019/947/EU delijo na tri kategorije, in sicer na odprto, posebno in certificirano.

V odprto kategorijo sodijo brezpilotni zrakoplovi, ki tehtajo od 250 gramov do 25 kilogramov, letijo v vidni liniji in do višine 120 metrov, ter ne prevažajo tovar ali ljudi. Posamezne kategorije se naprej delijo na podkategorije, ki natančno določajo, kateri brezpilotni zrakoplovi

Bistvena razlika med »staro« slovensko uredbo in Uredbo 2019/947/EU je zlasti v tem, da je domača zakonodaja temeljila na ločitvi operacij, ki se izvajajo za namen dejavnosti in pa operacijami, ki se izvajajo za šport in rekreacijo.

Pomembna novost, ki jo prinaša nova zakonodaja, je pristojnost izvajanja nadzora s strani Policije in občinskih redarjev. Ti so po novem pristojni za postopke v zvezi s preverjanjem listin, ki jih morata imeti operator in pilot na daljavo, torej bodo preverjali, ali so operatorji registrirani in piloti na daljavo ustrezno usposobljeni.

sodijo vanje, kakšni so pogoji za njihovo uporabo in kje je uporaba dovoljena. Odprta kategorija se zaradi svoje obsežnosti deli na tri podkategorije: A1, A2 in A3. Če katera od zahtev za odprto kategorijo ni izpolnjena oziroma je presežena, na primer letenje z brezpilotnim zrakoplovom višje od 120 m nad zemeljskim površjem, izven vidnega polja, nad zborom ljudi ali z brezpilotnim zrakoplovom, težjim od 25 kg, mora operator izpolniti zahteve za posebno kategorijo in pridobiti ustrezna dovoljenja. Znotraj posebne kategorije se operacije namreč lahko izvajajo v različnih stopnjah na podlagi različnih dovoljenj oziroma operativnih omejitev.

Če bo operacija vključevala prevoz ljudi ali nevarnih snovi, če znaša premer brezpilotnega zrakoplova več kot 3 metre, gre za operacijo v certificirani kategoriji. Glede te kategorije EU pripravlja dodatne predpise, ki bodo uredili letenje

brezpilotnih zrakoplovov v tej kategoriji. Gre namreč za kategorijo, ki je po obsegu zahtev izenačena z zrakoplovi s posadko: piloti na daljavo bodo morali pridobiti licenco, operator spričevalo letalskega prevoznika, certifikacija brezpilotnega zrakoplova pa bo izvedena s strani Evropske agencije za letalsko varnost.

Novi predpisi vzpostavljajo obveznost registracije operatorjev sistemom brezpilotnih zrakoplovov. V okviru odprte kategorije se morajo registrirati operatorji sistemov brezpilotnih zrakoplovov, če upravljajo kateregakoli od naslednjih brezpilotnih zrakoplovov:

- zrakoplov z največjo vzletno maso 250 g ali več ali zrakoplov, ki lahko v primeru trčenja na človeka prenese več kot 80 joulov kinetične energije;
- zrakoplov, opremljen s senzorjem, ki lahko zajame osebne podatke, razen če je v skladu z Direktivo 2009/48/ES.

V okviru posebne kategorije se registrirajo brezpilotni zrakoplovi s katerokoli maso. Lastnik brezpilotnega zrakoplova, katerega zasnovo je treba certificirati (certificirana kategorija), registrira brezpilotni zrakoplov v skladu s Prilogo 7 k Čikaški konvenciji (nacionalnost in registracijska oznaka brezpilotnega zrakoplova se določita tako, kot to velja za zrakoplove s posadko).

Predpisi EU nalagajo tudi obvezno usposabljanje za vse pilote na daljavo.

Registracija operatorjev in usposabljanje pilotov na daljavo, ter izpit v odprti kategoriji A1/A3, se opravi preko spletne aplikacije, imenovane UAS repozitorij. Spletna aplikacija služi kot spletni priročnik, ki vsebuje zbirko znanj, nasvetov in uporabnih informacij iz področja letalstva za vse pilote na daljavo. Dostopna je 24 ur na dan, 7 dni v tednu, 365 dni v letu. Bistvo nove zakonodaje v delu, ki se nanaša na množično uporabo, oziroma tako imenovano odprto kategorijo, je torej: kupim – se registriram – se usposobim – letim.

Za profesionalno uporabo, kamor spadajo v odprti kategoriji podkategorija A2, in zlasti posebna kategorija, pa bodo morali operatorji pridobiti ustrezna dovoljenja s strani agencije, piloti na daljavo bodo morali poleg osnovnih znanj, ki jih je mogoče pridobiti preko spletne



aplikacije, osvojiti še dodatna praktična in teoretična znanja.

EU je državam članicam naložila, da določijo geografska območja, v katerih je letenje z brezpilotnimi zrakoplovi prepovedano ali omejeno. Republika Slovenija je ta območja opredelila z izvedbenim predpisom. Javna agencija za civilno letalstvo Republike Slovenije, pa je na podlagi tega pripravila interaktivni zemljevid, v katerega je možno vsak čas vpogledati, katero območje je prepovedano ali omejeno. Ta območja so določena glede na zagotavljanje letalske varnosti, na primer okolica letališč, pa tudi glede na zaščito drugih interesov, kot so okolje, obramba države, zasebnost in podobno, pri čemer morajo v slednjih primerih obseg omejitve ali prepovedi določiti področni predpisi ali odloki lokalnih skupnosti. Kot omejeno ali prepovedano območje, pa je možno določiti tudi območja kritične infrastrukture. Zavezanec za obvezno organiziranje varovanja predlaga določeno območje kot geografsko območje, kjer je letenje z brezpilotnimi zrakoplovi prepovedano ali omejeno.

Pomembna novost, ki jo prinaša nova zakonodaja, je pristojnost izvajanja nadzora s strani Policije in občinskih redarjev. Ti so po novem pristojni za postopke v zvezi s preverjanjem listin, ki jih morata imeti operator in pilot na daljavo, torej bodo preverjali, ali so operatorji registrirani in piloti na daljavo ustrezno usposobljeni. Republika Slovenija se je z dodelitvijo pristojnosti navedenim organom zgledovala po primerjalno pravnih ureditvah večine držav članic EU, hkrati pa je napravila korak naprej k učinkovitosti izvajanja nadzora.

Nova EU zakonodaja iz svojega področja uporabe izključuje državne aktivnosti z brezpilotnimi zrakoplovi. Kar seveda pomeni, da morajo države članice sprejeti svoje lastne predpise, s katerimi uredijo letenje vojaških, policijskih, gasilskih in podobnih brezpilotnih zrakoplovov. V Sloveniji to področje še vedno ni ustrezno urejeno, čeprav navedeni deležniki pri svojem delu brezpilotne zrakoplove uporabljajo.

Kako naprej?

Države članice EU so imele pred sprejemom nove EU zakonodaje svoje lastne ureditve, urejanja brezpilotnih zrakoplovov se je vsaka od njih lotila na svoj način. V Sloveniji smo področje urejali



Zaradi občutno povečanega števila operacij v zračnem prostoru pa se že v letu 2023 pričakuje uveljavitev predpisa, ki bo določal zahteve za zračni prostor. Gre za ureditev tako imenovanega posebnega zračnega prostora (ang. U – space airspace), v katerem se izvajajo operacije z brezpilotnimi zrakoplovi, zrakoplovi s posadko pa vanj vstopajo le redko.

podobno, kot sta to uredili Hrvaška in Avstrija. Pri pripravi nove EU zakonodaje pa je Evropska unija izhajala iz španske in francoske nacionalne zakonodaje. Zakonodaja EU zato državam članicam do leta 2023 daje določena prehodna obdobja, veljavnost »starih« domačih dovoljenj, izdanih na vsebinsko popolnoma drugačnih podlagah, pa je omejena na konec leta 2021. Tako pristojni organi kot tudi imetniki teh dovoljenj, pa se posledično soočamo z zmedo, ki so jo ustvarila predmetna prehodna obdobja.

Na glede na težave, s katerimi se bomo soočali na poti k popolni implementaciji EU zakonodaje, je regulacija brezpilotnih zrakoplovov potrebna. Ali bo dovolj hitro sledila tehnološkemu razvoju, na tem mestu ni mogoče odgovoriti.

Vsekakor pa danes lahko rečemo, da bo v prihodnje urejeno področje prevoza to-

vora in ljudi z brezpilotnimi zrakoplovi. Zaradi občutno povečanega števila operacij v zračnem prostoru pa se že v letu 2023 pričakuje uveljavitev predpisa, ki bo določal zahteve za zračni prostor. Gre za ureditev tako imenovanega posebnega zračnega prostora (ang. U – space airspace), v katerem se izvajajo operacije z brezpilotnimi zrakoplovi, zrakoplovi s posadko pa vanj vstopajo le redko. Po mnenju Evropske komisije pomeni vzpostavitev takega zračnega prostora prvi korak k popolni integraciji brezpilotnih zrakoplovov v zračni prostor.

Vsekakor se danes v Sloveniji lahko pohvalimo s proizvajalci, ki imajo na opisanem področju vizijo in, ki to svojo vizijo udejanjajo. ■

Tel: +386 1 8317 488

Service tel.: + 386 1 8317 452

Web: www.zarja.com

E-mail: info@zarja.com

ZARJA ELEKTRONIKA

se ponša s projektiranjem in izvedbo tehnično najzahtevnejših varnostnih sistemov, ki so plod lastnega znanja, razvoja in sledenja svetovnim trendom.

INTEGRACIJSKI SISTEMI:

- Sistem samodejnega odkrivanja in javljanja požara;
- Sistem javljanja vloma;
- Videonadzorni sistem;
- Grafično nadzorni sistem z vizualizacijo dogodkov;
- Sistem javljanja plina;
- Stabilni gasilni sistem;
- Načrtovanje varnostnih sistemov (tehnično projektiranje);
- Registracija delovnega časa;
- Nadzor dostopa in elektronski nadzor nad ključi.

"IZDELAVA SISTEMOV PO MERI KUPCA"

NAPREDNE TEHNOLOGIJE VAROVANJA

Smo ekskluzivni zastopnik za profesionalno opremo najvišjega kakovostnega razreda 

VSAK VAREN DAN SE ZAČNE KOT VSAK SKRBNO NAČRTOVAN VARNOSTNI SISTEM



**ZARJA
ELEKTRONIKA**



ZLIVANJE IT IN OT SISTEMOV V KRITIČNI INFRASTRUKTURI

Zlivanje področij IT (ang. Information Technology) in OT (ang. Operational Technology) je proces, kateremu smo priča že dlje časa, a je njegova intenzivnost opazna šele v zadnjih nekaj letih, kar je posledica potreb po uvajanju sodobnih digitalnih rešitev in avtomatizacije v t. i. procesne sisteme, kakor se tudi označuje OT področja.

Uvod

OT področja so specializirana informacijsko-komunikacijska okolja, ki so namenjena izvajanju procesov. V industriji je to lahko upravljanje avtomatiziranih proizvodnih linij v kritični infrastrukturi, kot so elektroenergetika, pa upravljanje elektroenergetskega omrežja ter merilna infrastruktura. Z razvojem pametnih omrežij pa se v elektroenergetsko infrastrukturo vpeljuje tudi množica novih sistemov. V cestnem prometu je takšen primer upravljanje namenskih sistemov v prometni infrastrukturi, kot so npr. video nadzorni sistemi ali upravljanje s krmilnimi sistemi v avtocestnih predorih, v železniškem sistemu pa npr. vodenje železniškega prometa ali pa upravljanje signalnovarnostnih sistemov.

Našteti je le nekaj primerov, saj ima vsaka vertikala kritične infrastrukture ali različne veje industrije za svoje specifične potrebe vzpostavljeno t. i. OT infrastrukturo. S pričetkom vzpostavljanja OT sistemov ni bilo načrtovanega povezovanja z zunanjimi sistemi, v osnovi so bile to fizično ločene domene, v angleškem jeziku takšno ločitev označujejo z "air gapped". Običajno so to sistemi, ki so v obratovanju dlje časa, kot je življenjska doba v poslovnih oz. IT sistemih, zato pogosto v OT sistemih naletimo na gradnike in naprave, ki so starejšega izvora. V sistemih vodenja elektroenergetskega omrežja (SCADA) tako operacijski sistem Windows XP ni nobena posebnost, kar pa po drugi strani vnaša kibernetika varnostna tveganja, saj za ta operacijski sistem že dolgo ni več varnostnih nadgradenj in tako povečuje tveganja za kibernetiske incidente.

Zlivanje IT in OT kot evolucija ter z njim povezani izzivi

Vzroki za čedalje intenzivnejše zlivanje IT in OT okolij so različni in jih ne moremo enačiti za vse gospodarske panoge t. i. vertikalne. V industriji oz. proizvodnih organizacijah so motivi za digitalizacijo in uvajanje informacijsko-komunikacijskih sistemov v procesna omrežja in posledično zlivanjem z IT predvsem vezani na zahteve po povečanju dobičkonosnosti, zagotavljanje konkurenčnosti na trgu, učinkovitosti, lansiranjem novih produktov ali uvajanjem novih poslovnih modelov. V kritičnih infrastrukturnih sistemih so motivi za zlivanje IT in OT segmentov vezani na potrebo po izmenjavi informacij/podatkov med napravami v procesnem delu ter aplikacijami, ki so po svoji naravi bližje poslovnemu IT segmentu. Tak primer je izmenjava podatkov med

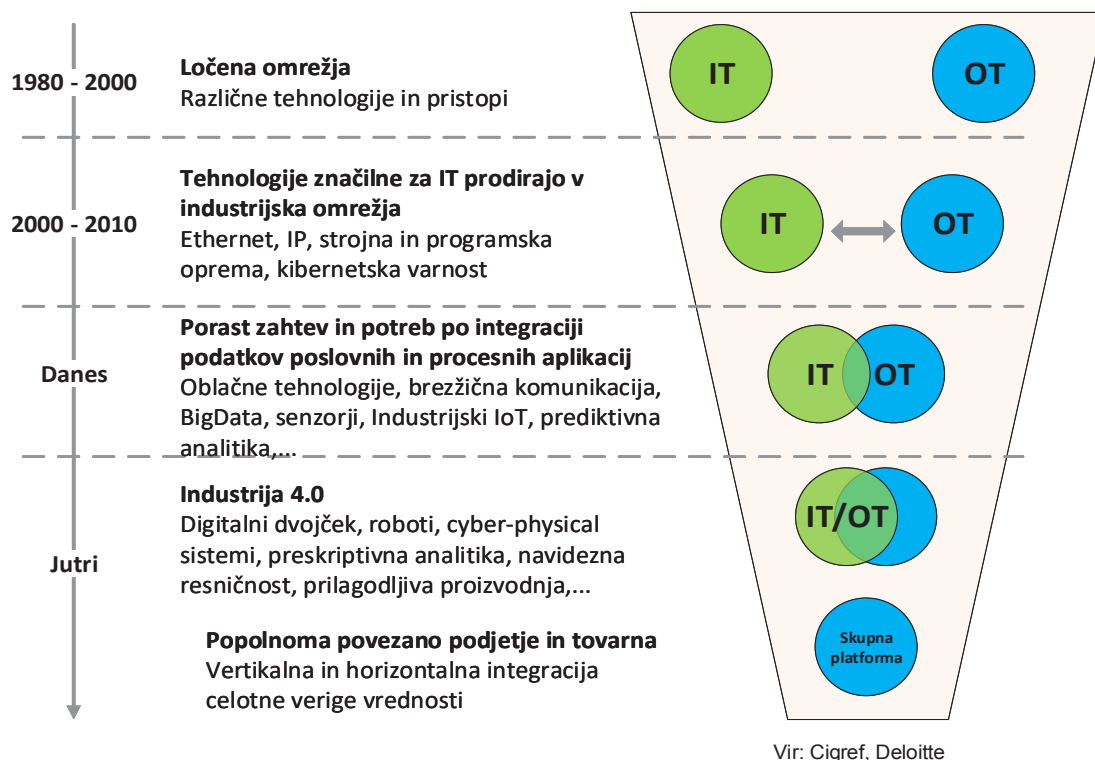
Pomanjkanje strokovnega kadra, kot posledica dolgoletnega upadanja tehničnih in naravoslovnih strokovnjakov, predstavlja velik problem, ne samo za podjetja, ki se ukvarjajo z IT tehnologijo, pač pa za vsa podjetja, ki se modernizirajo in uvajajo kopico novih informacijsko-komunikacijskih orodij in aplikacij.

sistemi za upravljanje s sredstvi (ang. Asset Management) in sistemi, ki se nahajajo na RTP postajah.

V elektroenergetskih sistemih je v prihodnje pričakovati tudi rast t. i. IoT (ang. Internet of Things) naprav in senzorjev, ki so namenjeni merjenju ali zaznavanju različnih veličin. V prihodnjih letih bo potreba po velikih posodobitvah elektrodistribucijskih omrežij, saj bo prehod na nizkoogljeno družbo prinesel elektrifikacijo prometa in ogrevanja ter dodatno rast razpršenih virov proizvodnje električne energije. Vsi ti sistemi brez podpore informacijsko-komunikacijskih sistemov ne bodo možni, zato bo prepletanje IT in OT (ter IoT) sistemov še bolj intenzivno.

Spodnja slika prikazuje proces postopnega zlivanja IT in OT sistemov skozi čas. Danes je že prisoten znaten del prepletanja obeh segmentov, glede na napovedi pa je sčasoma pričakovati, da se bosta oba segmenta zlila v skupno platformo. Digitalizacija v globino procesov oz. t. i. Industrija 4.0. bo pomenila veliko širitev perimetra informacijsko-komunikacijskih sistemov, ki pa mora biti ekonomsko vzdržna, zato dveh vzporednih sistemov enostavno ne bo več možno obvladovati, saj že zdaj prihaja tako do investicijskih in kadrovskih omejitev.

Evolucija konvergence IT in OT



Vse naštetu pa pred organizacije postavlja nove izzive, ki se sicer tako kot celoten proces postopoma rešujejo, stopnja zavedanja in posledično vzpostavitev ustreznih mehanizmov pa je različna glede na vertikale in organizacije.

Ključni izzivi, ki so pri tem prisotni, so trije:

- **Podatkovni** – se nanaša na dilemo, kako izkoristiti moč podatkov, ki jih z vsemi tehnologijami pridobimo, in kako bomo te možnosti izkoristili za povečanje dodane vrednosti v naših procesih. To ni nujno dobičkonosnost v finančnem smislu, v kritičnih sistemih je dodana vrednost predvsem v povečanju zanesljivosti, izboljšanju kakovosti, zagotavljanju neprekinjenega poslovanja, ob ekonomsko zdržni porabi sredstev.

Povečanje odpornosti vsake organizacije podjetij v kritični infrastrukturi je proces, ki ga je potrebno skrbno načrtovati. Ključno spoznanje, ki je potrjeno v praksi, je, da se zavedanje o tem začne na strateški ravni vsake organizacije, kjer uprava oz. vodstvo organizacije poda ustrezne smernice in navodila ter organizira interne procese in področja za krepitev kibernetske varnosti.

- **Kompetence** – zavedati se je potrebno, da združujemo glede obstoječih človeških virov in njihovi percepciji IT tehnologije, ki se seli tudi v OT del dva, v tem času po razvitosti neenakovredna segmenta.

- **Kibernetska varnost** – le-ta v veliki meri vpliva na odpornost organizacij, ki upajajo vse večji delež informacijsko-komunikacijskih sistemov. V zadnjem obdobju pa se je pomembno spremenil tudi način dela, ki ga narekuje pandemija COVID-19, in velika verjetnost obstaja, da se bo tudi v post-pandemični družbi ohranil velik del “virtualnih” delovnih navad, pridobljenih med pandemijo. To vnaša dodaten element, ki ga je potrebno upoštevati pri načrtovanju kibernetske varnosti in z njo povezane odpornosti organizacije.

Kibernetska varnost, kot temelj odpornosti organizacij v kritični infrastrukturi

Različna poročila analitskih hiš in proizvajalcev informacijsko-komunikacijske tehnologije že vrsto let objavljajo izsledke in poročila o gibanju kibernetskih varnostnih incidentov glede na oblike, vertikale in geografsko razpršenost. V zadnjem obdobju so v porastu spodaj navedene vrste kibernetskih napadov, ki vplivajo na odpornost katerekoli organizacije, v kritičnih sistemih pa tovrstni incidenti lahko pomembno zmanjšajo razpoložljivost delovanja osnovnih sistemov:

- kraja intelektualne lastnine,
- lažno predstavlanje (ang. phishing attack) in usmerjeno lažno predstavlanje (ang. spear-phishing attack),
- OT/IoT napadi,
- napadi na verige dobaviteljev,
- izsiljevalsko programje (ang. ransomware),
- zlonamerno programje (ang. malware).

Nekatera poročila o kibernetskih napadih v letu 2020 kažejo sicer na zmanjšanje števila t. i. "malware" (zlonamerno programje) napadov, kar je sicer pripisati pandemiji, saj se je število osebja v organizacijah zaradi sprejetih omejitev izredno zmanjšalo. Kljub zmanjšanju obsega, pa gre za varljivo dejstvo, saj so po drugi strani tovrstni napadi postali še bolj učinkoviti, specializirani ter usmerjeni na določene vertikale, kar pomeni, da je potrebno številčno manj napadov, da se doseže enake ali večje učinke v primerjavi s preteklimi obdobji.

Povečanje odpornosti vsake organizacije podjetij v kritični infrastrukturi je proces, ki ga je potrebno skrbno načrtovati. Ključno spoznanje, ki je potrjeno v praksi, je, da se zavedanje o tem začne na strateški ravni vsake organizacije, kjer uprava oz. vodstvo organizacije poda ustrezne smernice in navodila ter organizira interne procese in področja za krepitev kibernetske varnosti. Odvisno od dejavnosti je sicer potrebno gledati na širšo sliko, saj področja korporativne varnosti zajemajo, tako kibernetsko varnost, kot fizično varnost. Izzivi kibernetske varnosti v organizacijah kritične infrastrukture pa niso izključno tehnološke narave, ampak je potrebno graditi in ustrezno povezovati tri segmente: vire (zaposlene), procese in tehnologijo.

Največji izziv v današnjem času predstavlja prav človeški potencial. Pomanjkanje strokovnega kadra, kot posledica dolgotrajnega upadanja tehničnih in naravoslovnih strokovnjakov, predstavlja velik problem, ne samo za podjetja, ki se ukvarjajo z IT tehnologijo, pač pa za vsa podjetja, ki se modernizirajo in uvajajo kopico novih informacijsko-komunikacijskih orodij in aplikacij. Tudi v podjetjih, kjer osnovna dejavnost ni IT, se potrebe po strokovnem kadru, predvsem s področja zagotavljanja kibernetske varnosti, povečujejo. Še večji primanjkljaj strokovnega kadra s področja kibernetske varnosti je v dani situaciji opaziti v OT okoljih, kjer dosedanja znanja in kompetence večinoma niso zajemala kibernetsko varnostnih sistemov. Na drugi strani pa "klasičen" IT kader ne pozna specifične procesnih sistemov in okolij, kjer je potrebno poznavanje ne samo omrežnih struktur in sistemov, pač pa tudi višje nivojskih protokolov, ki jih zasledimo izključno v OT sistemih. Primera iz kritične infrastrukture elektroenergetskega sistema sta protokola: IEC 60870-5-104 (eden ključnih protokolov za vodenje elektroenergetskega sistema), in IEC



Organizacije morajo predvsem najprej vzpostaviti rešitev za zaznavanje in odkrivanje varnostnih incidentov. S tem bodo spoznale, s katerimi grožnjami se soočajo in nato poskrbeti za rešitve za obvladovanje in odpravo varnostnih incidentov, ki jih po potrebi integrirajo v nadzorno-operativni center ali varnostno-operativni center.

61850 (zbirka različnih protokolov, kot je npr. GOOSE protokol, ki se uporablja za medsebojno komunikacijo t. i. IED naprav – inteligentnih elektroenergetskih naprav).

Za sistematski pristop pri načrtovanju in povečevanju odpornosti v kontekstu kibernetске varnosti se je smiselno nasloniti na t. i. zrelostni model, ki omogoča pogled na vse tri komponente, ki jih moramo upoštevati, in omogoča postopno uvajanje posameznih ukrepov v razvojne načrte vsake organizacije kritične infrastrukture. V nadaljevanju se osredotočimo na zrelostni model v OT okolju. Podoben model velja sicer tudi za IT okolja, vendar je potrebno poudariti, da je stopnja zrelosti kibernetске varnosti v OT v današnjem času še vedno nižja od stopnje zrelosti v IT okoljih.

Zrelostni model IT/OT okolja

Spodnja slika prikazuje zrelostni model, ki nam služi pri načrtovanju ukrepov povečanja odpornosti na kibernetске grožnje v kritični infrastrukturi. Kljub temu, da je dandanes na trgu na voljo ogromno različnih tehnoloških rešitev kibernetске varnosti, je potrebno sisteme uvajati na način, ki bo v

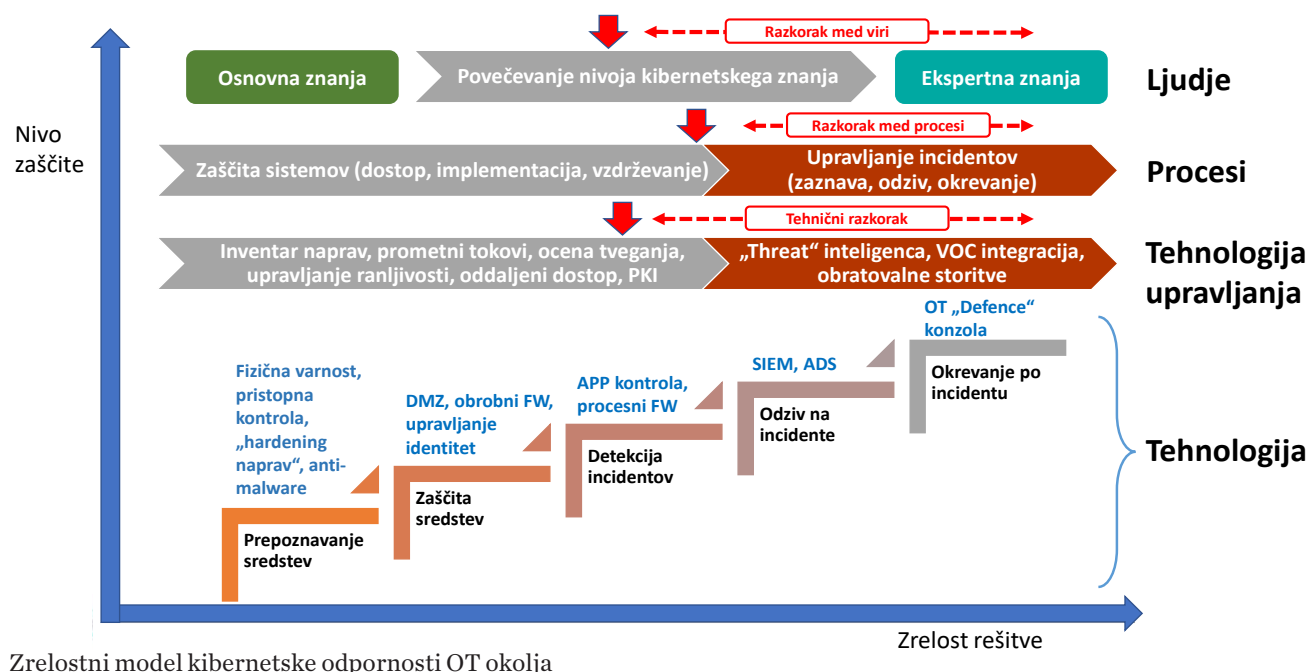
danem trenutku najbolj doprinesel k povečanju odpornosti. Ni nujno, da so to najboljše sistemi, odvisno je od stanja v določenem trenutku, zato je predhodno smiselno izvesti analizo trenutnega stanja, da ugotovimo, na kateri točki zrelostnega modela po vseh treh dejavnikih se organizacija nahaja. Na podlagi takšne analize lahko opredelimo nadaljnje korake povečevanja zrelostnega nivoja in posledično odpornosti organizacije na kibernetске grožnje.

Pri načrtovanju proračunskih sredstev za kibernetčko varnost v IT in OT okolju, je treba upoštevati in hkrati preveriti obstoječe rešitve – na kakšen način in katere varnostne grožnje naslavljajo. Večinoma so te rešitve komplementarne in se medsebojno dopolnjujejo. Ob tem je smotno preveriti, ali lahko z obstoječo rešitvijo organizacija reši še kakšen drug izziv. S konsolidacijo rešitev lahko organizacija prihrani znatna sredstva, ki jih nameni razvoju in vpeljevi novih rešitev, ki rešujejo težave, za katere še nima ustrezne rešitve, in tako dvigne zrelostni nivo kibernetске varnosti in odpornost na kibernetске grožnje.

Pri zagotavljanju celovitega odziva na napredne kibernetске grožnje je potrebno vzpostavljati partnerstva s strokovnjaki za kibernetčko varnost v IT in OT okoljih s ciljem izvajanja naprednih storitev obratovanja na vseh nivojih, tako z vidika arhitekture, kakor zagotavljanja varnosti IT in OT okolja. Na ta način organizacije lahko bistveno zmanjšajo problem pomanjkanja virov, saj specializirana podjetja lahko ponudijo obratovalne storitve, ki dopolnjujejo in optimizirajo delovanje specializiranih kibernetčko varnostnih aplikacij in orodij, ter s tem razbremenijo sistemske inženirje, ki se tako lahko osredotočajo na strateški nivo zagotavljanja storitev in temeljne kompetence organizacije.

Organizacije morajo predvsem najprej vzpostaviti rešitev za zaznavanje in odkrivanje varnostnih incidentov. S tem bodo spoznale, s katerimi grožnjami se soočajo in nato poskrbeti za rešitve za obvladovanje in odpravo varnostnih incidentov, ki jih po potrebi integrirajo v nadzorno-operativni center ali varnostno-operativni center. ■

Zrelostni nivo organizacije



Okrepite kibernetško varnost v kritični infrastrukturi



Obvladovanje kibernetških tveganj za neprekinjeno delovanje



Vpeljava avtonomnih omrežij z uvedbo konceptov umetne inteligence



Celovito upravljanje, avtomatizacija in orkestracija varnostnih in omrežnih rešitev



Zagotavljanje vidljivosti in zaznave anomalij v omrežju ter hiter odziv



Stalno izobraževanje in ozaveščanje uporabnikov

Poglejte si video

Kako zagotoviti kibernetško varnost v kritični infrastrukturi



<http://bit.ly/ot-varnost>

Secured 5G Networks

Ericsson's evolved network security is the pioneer of a simpler yet more robust era of telecom security. Our market-leading solutions equip service providers with autonomous, end-to-end telecom security – built in to each layer of the network and securing all connected things everywhere, all the time.

www.ericsson.com/en/security



ERICSSON



KOMPETENCE VARNOSTIH MENEDŽERJEV V PROCESU KRIZNEGA UPRAVLJANJA IN VODENJA V KRITIČNI INFRASTRUKTURI

Namen tega sestavka je, da v sklopu aktualnih kriznih razmer v letu 2021 in ob upoštevanju ostalih tveganj, ki se pojavljajo pri upravljanju kritične infrastrukture, predstaviva kompetence in kompetentnost tistih menedžerjev, ki v kritični infrastrukturi upravljajo posamezna področja korporativne varnosti in integralni varnostni sistem kot celoto. To so menedžerji korporativne varnosti oziroma (krajše) varnostni menedžerji, ki so v procesu upravljanja kritične infrastrukture eden od ključnih deležnikov zagotavljanja neprekinjenega poslovanja in delovanja kritične infrastrukture ter obvladovanja izrednih dogodkov, krajših kriznih stanj, kompleksnih kriz in posledično kriznega vodenja.

1. Pregled ključnih segmentov kriznega upravljanja in vodenja

1.1 Kompetence in kompetentnost

Kompetence posameznika se izkazujejo skozi izobraževanje pridobljena splošna in strokovna znanja, razne sposobnosti, spretnosti in veščine, vzorce razmišljanja, vrednote, komuniciranje in druge pokazatelje obnašanja, vedenja in izvajanja konkretnih delovnih, poslovnih, projektnih ter drugih funkcij, procesov in nalog. Če ima posameznik vse potrebne kompetence za opravljanje določene vodilne, vodstvene ali operativne funkcije za upravljanje določenega procesa, za določeno delovno mesto ali za določen projekt, pravimo, da je kompetenten za to, kar mu je poverjeno. Drugo vprašanje pa je, ali je fizično, psihološko, socialno in komunikacijsko zmožen udeležati posamezne kompetence in seveda, če ima zadosti volje, poguma in čustvene inteligence za doseganje strategij, načrtov ter lastnih in delodajalčevih ciljev. Če posameznik

določenih kompetenc nima se mora zavedati, da si jih mora pridobiti, če želi konkurirati na trgu delovne sile, ter uspešno in učinkovito izvajati zaupane naloge.

1.2 Kritična infrastruktura

To so tiste gospodarske in druge dejavnosti, ki morajo državi, gospodarstvu, civilni družbi in prebivalstvu svoje proizvode in storitve neprekinjeno zagotavljati tudi v kriznih razmerah. To izhaja iz zakonskega določila, ki pravi, da morajo upravljavci kritične infrastrukture zagotavljati neprekinjeno de-

V proces upravljanja tveganj pri posameznem upravljavcu kritične infrastrukture je torej nujno potrebno vključiti tudi kritične dobavitelje in ključne odjemalce.



lovanje posameznih sektorjev kritične infrastrukture v vseh razmerah (19. čl. ZKI).

Kritično infrastrukturo sestavljajo naslednji sektorji: energtika, promet, prehrana, preskrba s pitno vodo, zdravstvo, finance, varovanje okolja, informacijsko-komunikacijska infrastruktura. Vsak sektor ima svojega nosilca (ministrstvo) in upravljavca (gospodarsko družbo, zavod, državni organ). Za nemoteno oziroma za čim manj moteno delovanje države, gospodarstva, civilne družbe in prebivalstva sta ključna (prioritetna) sektor energetike in sektor informacijsko-komunikacijske infrastrukture.

Pri tem ne smemo zanemariti dejstva, da nujni in neločljivi del kritične infrastrukture pri posameznem upravljavcu kritične infrastrukture predstavljajo na eni strani kritični (ključni, strateški) dobavitelji, ki morajo v kritičnih razmerah neprekinjeno zagotavljati s pogodbami določene dobave, ter na drugi strani ključni odjemalci (kupci, stranke), ki s svojimi zahtevami postavljajo normative za neprekinjenost delovanja posameznega upravljavca kritične infrastrukture. V proces upravljanja tveganj pri posameznem upravljavcu kritične infrastrukture je torej nujno potrebno vključiti tudi kritične dobavitelje in ključne odjemalce.

1.3 Izredni dogodki

Med izredne dogodke velikih razsežnosti in posledic uvrščamo: potrese, poplave, večje plazove, letalske, rudniške, železniške in cestnoprometne nesreče, delovne nesreče, ekološke nesreče, organizirani kriminal, korupcije, mafije, afere, stavke, izgrede na javnih krajih, vlome in roparske napade, sabotaže, diverzije, atentate, teroristična dejanja, izpade in razpade elektroenergetskega sistema (»električne mrke«),

izpade informacijsko-komunikacijske infrastrukture, vdore v računalniška in komunikacijska omrežja, razlitja ogromnih količin nevarnih snovi v morje, vodovje ali v zemljo (ogrožanje podtalnice), velike gozdne požare in požare ter eksplozije na industrijskih objektih in objektih z velikim številom ljudi (poslovne zgradbe, kinodvorane, gostinski lokali, hoteli, gledališča, športna igrišča, vlaki, avtobusi), itd. Posledice vsakega izrednega dogodka so praviloma neugodne, ker se izražajo v materialni, finančni, poslovni, človeški in moralni škodi in hkrati izgubi. Če so materialne, finančne, poslovne, obratovalne (proizvodne) in človeške posledice šokantne, opredelimo tak izredni dogodek kot havarijo oziroma katastrofo za konkretnega upravljavca kritične infrastrukture, celotni sektor v katerega je vpet posamezni upravljavec kritične infrastrukture ter za gospodarstvo, civilno družbo, lokalno skupnost in državo.

1.4 Krizna stanja

V kritični infrastrukturi morajo nosilci sektorjev in posamezni upravljavci kritične infrastrukture obvladovati tudi krizna stanja in krizne okoliščine ter konkretne krize, ki nastanejo zaradi neobvladovanja ali neučinkovitega obvladovanja tveganj in zaradi nenadnih, nepričakovanih ali presenečenih izrednih dogodkov. Za obvladovanje krize mora imeti upravljavec kritične infrastrukture na operativnem nivoju in nosilec sektorja na strateškem nivoju izdelan načrt neprekinjenega delovanja, krizni načrt za delovanje na osnovni in/ali rezervni lokaciji, vzpostavljen krizni štab in pripravljen načrt kriznega komuniciranja. Sestavni del kriznega vodenja je tudi predhodno preizkušanje scenarijev verjetnih izrednih dogodkov in posledično kriznih stanj. Govorimo o t.i. kriznem menedžmentu, ki izhaja iz delovanja kriznega štaba kot ključnega izvajalca kriznega vodenja (nekaj o tem Allen 2019, Phelps 2018).

Posebna krizna stanja so t. i. »kompleksne krize« (več o tem Malešić 2004 in Beršak 2016), ki terjajo kompleksen pristop k razreševanju, zahtevajo angažiranje vseh družbenih sil, veliko materialnih, finančnih in človeških virov ter zavedanje o dolgoročnosti razreševanja. Aktualni primer kompleksne krize je »koronavirus«, ki je dobesedno presenetil ves svet in ki povzroča negotovost, prepletanje pravih in lažnih informacij, omejevanje gibanja in s tem posledično poseganje v temeljne človekove pravice in svoboščine, družbeni nemir in čakanje na izboljšanje stanja. Vse pa vodi v splošno znano ugotovitev »da nikoli ne bo več tako, kot je bilo«.

1.5 Varnostni menedžerji

Varnostni menedžerji, kot eden od ključnih deležnikov upravljanja s tveganji v kritični infrastrukturi in kriznega vodenja, so tiste odgovorne osebe, ki v sistemu korporativne varnosti in procesu upravljanja s tveganji na različnih organizacijskih nivojih, upravljajo:

- zakonodajno in normativno področje
- integralni varnostni sistem
- ranljivost, ogroženost (grožnje) in varnostna tveganja
- kibernetsko varnost (informacijsko varnost in elektronske komunikacije)
- poslovne skrivnosti, osebne in tajne podatke
- varstvo okolja, požarno varnost ter varnost in zdravje pri delu
- zaščito in reševanje (civilno zaščito)
- varnostne standarde
- notranjo kontrolo in revizijo
- krizni štab.

Upravljanje integralnega varnostnega sistema in kriznega štaba (kriznega vodenja) poteka na strateški ravni (uprava, direktorji), ostale poslovno-varnostne funkcije pa na operativni ravni. Upravljanje posameznih poslovno-varnostnih funkcij (ocenjevanje ranljivosti, ogroženosti in varnostnih tveganj, kibernetska varnost, zaščita in reševanje, idr.) izvajajo vodje s potrebnimi oziroma (od delodajalca) zahtevanimi kompetencami.

2. Splošne kompetence

Navajamo deset top kompetenc (znanj, spretnosti, sposobnosti in veščin), ki bi jih moralo posedovati vodilno in vodstveno osebje v državnih, gospodarskih in drugih družbah. Te kompetence so (World Economic Forum 2016, Cabrić 2015, Verte/Markič 2012):

- Reševanje problemov
- Kritično razmišljanje
- Ustvarjalnost
- Upravljanje s človeškimi viri
- Organizacijske sposobnosti
- Čustvena inteligenca
- Etična presoja in razumno odločanje
- Sposobnost osredotočiti se na stranke
- Pogajalske sposobnosti
- Kognitivna fleksibilnost.

Splošne kompetence so sestavni del opravljanja vseh vodilnih in vodstvenih del ter nalog in zagotavljajo, da bodo dela in naloge opravljene kakovostno, pravočasno in stroškovno ustrezno. Poleg tega je od posameznikov pričakovati razmišljanje o var-

V kadrovskih politikah in pri konkretnem kadrovanju na posamezne poslovne in druge funkcije, ter na vodilna in vodstvena delovna mesta, se posveča premalo pozornosti kompetencam. Zaradi tega je vse preveč primerov, ko posamezniki ne obvladujejo strategij, sprememb, tveganj, inovativnih pristopov in konkretnih delovnih nalog.

nostnih in drugih izboljšavah, spoštljiv odnos do drugih, visoko stopnjo odgovornosti in obvladovanje čustvene inteligence.

3. Posebne kompetence varnostnih menedžerjev v procesu kriznega vodenja

Za obvladovanje kriznih razmer v kritični infrastrukturi pa splošne kompetence ne zadostujejo, ker katerakoli kriza (finančna, gospodarska, socialna, zdravstvena, psihološka, itd.) terja vzpostavitev kriznega vodenja, ki ga lahko poimenujemo kar z izrazom »eksplozivno vodenje« proizvodnje, poslovanja, logistike, poslovnih partnerjev, pogodbenih izvajalcev in človeških virov. To pomeni, da nosilci sektorjev kritične infrastrukture in upravljalci kritične infrastrukture povečajo pozornost na splošne in posebne kompetence varnostnih in drugih menedžerjev s ciljem celovitega obvladovanja kriznega vodenja.

Ključno izhodišče za posebne kompetence varnostnih menedžerjev je upravljanje varnostnih tveganj v kritični infrastrukturi, ki jih prepoznamo v oceni ranljivosti, ogroženosti in varnostnih tveganj in v katalogu tveganj kot operativnem dokumentu tekočega upravljanja tveganj (več o tem Čaleta in drugi 2019, Vršec in Vršec 2019).

V nabor posebnih kompetenc varnostnih menedžerjev v procesu obvladovanja kriznega vodenja uvrstimo naslednje kompetence:

- poznavanje kritične infrastrukture in bistvenih storitev sektorja in konkretne organizacije,
- prepoznavanje scenarijev verjetnih izrednih dogodkov, ki jih ugotovimo z oceno ranljivosti, ogroženosti in varnostnih tveganj,
- skozi izvedbo vsakoletnih vaj spoznavanje specifik posameznih scenarijev prepoznanih izrednih dogodkov,
- poznavanje načrta neprekinjenega poslovanja, kriznega načrta in načrta kriznega komuniciranja,
- delovanje v skladu z zakonodajo in drugimi predpisi, varnostnimi standardi in standardi upravljanja tveganj,
- spreminjanje varnostnih strategij na podlagi nastalih sprememb in izrednih dogodkov,
- oblikovanje in izvajanje dodatnih kriznih ukrepov, ki jih terjajo spremembe in nastala krizna situacija,

- poznavanje kriznega štaba in njegovega delovanja,
- poznavanje rezervne lokacije delovanja lastne organizacije,
- komuniciranje s kritičnimi dobavitelji in ključnimi odjemalci z vidika zagotavljanja pogodbenih obveznosti in izvajanja dodatno dogovorjenih kriznih ukrepov in s ciljem zagotavljanja neprekinjenih dobav in neprekinjenosti delovanja procesov,
- poznavanje ključnih služb in vodstvenega osebja, od katerih je odvisno obvladovanje izrednih dogodkov, nastalega kriznega stanja in kriznega vodenja,
- zagotavljanje stalne dosegljivosti v kraju bivanja in/ali v službi in/ali na terenu,
- redna skrb za vzdrževanje fizične in psihične kondicije ključnih kadrov za naporno delo v procesu kriznega vodenja,
- prepoznavanje lažnih informacij,
- odločanje na bazi analiziranih informacij,
- hitro operativno odzivanje na izredne dogodke,
- usklajevanje ukrepanja v okviru sektorjev kritične infrastrukture,
- spremljanje dogajanj in varnostnih razmer v lokalnem, regionalnem in svetovnem okolju,
- razreševanje nastalih internih in eksternih konfliktov.

To je samo nekaj ključnih kompetenc, s katerimi varnostni menedžerji prispevajo k učinkovitemu obvladovanju kriznega vodenja. Večino kompetenc si varnostni menedžerji pridobijo v procesu stalnega usposabljanja, torej v pripravah na krizno vodenje. Zaradi tega kar naprej poudarjamo, da se naj nosilci sektorjev in upravljalci kritične infrastrukture nenehno pripravljajo na predvidene in manj predvidene izredne dogodke, ki izhajajo iz narave, gospodarskega in poslovnega sveta, še posebej pa iz kriminalnega in terorističnega ozadja.

4. Zaključna misel

V kadrovske politike in pri konkretnem kadrovanju na posamezne poslovne in druge funkcije, ter na vodilna in vodstvena delovna mesta, se posveča premalo pozornosti kompetencam. Zaradi tega je vse preveč primerov, ko posamezniki ne obvladujejo strategij, sprememb, tveganj, inovativnih pristopov in konkretnih delovnih nalog. Težava je tudi v tem, da si večino kompetenc ni možno pridobiti v rednem izobraževalnem sistemu temveč v dodatnem načrtnem usposabljanju, ki pa je dokaj šibko. S tega zornega kota bi morali razvojni premik narediti tudi nosilci sektorjev in upravljalci kritične infrastrukture, da bi izboljšali odzive in obvladovanje izrednih dogodkov, sprememb, tveganj, in negotovosti, ter posledično povečati učinkovitost kriznega vodenja.

Viri

- Allen, M. (2019). *The Chief Security Officer's Handbook: Leading Your Team into the Future*. Oxford. Cambridge-Academic Press.
- Bernšak, J.V. (ur.) (2016). *Upravljanje kompleksnih kriz v Republiki Sloveniji*. Ministrstvo za obrambo.
- Cabric, M. (2015). *Corporate Security Management Challenges, Risk and Strategies*. Oxford. Butterworth-Heinemann.



- Čaleta, D., Vršec, M. in Vršec, M., Bertoncelj, B., Kandžič, A., Podgoršek, Ž. (2019). *Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture*. Inštitut za korporativne varnostne študije, Ministrstvo za obrambo.
- Grasser, B. (2020). *Managing Competences, Research, Practice, and Contemporary Issues*. Taylor&Francis.
- Halibozek, E.P., Kovacich, G. (2017). *The Manager's Handbook Security. Establishing and Managing a Successful Assets Protection Program*. Butterworth.
- Malešič, M. (2004). *Krizno upravljanje in vodenje v Sloveniji: izzivi in priložnosti*. Fakulteta za družbene vede.
- Phelps, R. (2018). *Crisis Management: How to develop a powerful program*. Chandi Media.
- Resolucija o strategiji nacionalne varnosti Republike Slovenije (Ur. l. RS, št. 59/2019).
- Uredba o kriznem upravljanju in vodenju ter Nacionalnem centru za krizno upravljanje (Ur. l. RS, št. 28/2018).
- Verte, K., Markič, M. (2012). *Kompetence vršnih managerjev in organiziranost kot osnova uspešnosti organizacije*. Koper, Fakulteta za management.
- Vršec, M. in Vršec M. (2019). *Proces upravljanja tveganj v kritični infrastrukturi na bazi standardov. Korporativna varnost*, št. 19. Inštitut za korporativne varnostne študije.
- World Economic Forum (2016). *The Future of Jobs Employment, Skiles and Workforce Strategy for the Fourth Industrial Revolution*. Annual Miting 20-23 January 2016. Davos. World Economic Forum.
- Zakon o kritični infrastrukturi ZKI (Ur. l. RS, št. 75/2017). ■

HSI

info@hsi.si
+386 7 600 19 60

CAPTIS®

License plate management solution



Sledljivost
ROI v kratkem času
Stalna razpoložljivost
Brez neavtoriziranih vstopov
Velika prepustnost na vhodu
Več varnosti za vaše podjetje
Samodejno odpiranje zapornice
Enostavno upravljanje parkirnih mest
Olajšanje in razbremenitev zaposlenih



OUR MANAGED SECURITY SERVICES

100+ ZAHTEVNEJŠIH PROJEKTOV

150+ ZAHTEVNEJŠIH CERTIFIKATOV

100+ PENETRACIJSKIH TESTOV V ZADNJIH 2 LETIH

PRO.SOC DOSTOPNOST 24/7/365

SVETOVALCI PRI PISANJU ZAKONODAJE NA STRANI GOSPODARSKE ZBORNICE



UNISTAR PRO





IZZIVI INFORMACIJSKE VARNOSTI V OKOLJU OPERATIVNIH TEHNOLOGIJ

Na področju IT je možno za informacijsko varnost skrbeti z zagotavljanjem zaupnosti, celovitosti in dostopnosti do informacij. V poslovnem svetu je prva skrb običajno zaupnost in celovitost informacij, če je potrebno občasno tudi na račun dostopnosti do informacij. V proizvodnji oz. v OT pa je zaradi posebnosti industrijskih procesov običajno drugače. Prva skrb je tipično neovirano delovanje proizvodnje, za kar je potrebna dostopnost do informacij. V očeh OT lahko za doseganje tega cilja občasno trpita celovitost in zaupnost.

Uvod

Zaradi različnih razlogov, ki niso tema tega članka, je v podjetjih vedno več strojev vključenih v računalniško omrežje. Tako so tveganja povezana z informacijsko varnostjo vedno večja, a žal tudi nepoznana strokovnjakom na področju upravljanja teh strojev, ki je v angleščini dobilo ime »Operational Technology« oz. »v nadaljevanju OT« kar bi lahko prevedli z izrazom »operativna tehnologija«. V tem članku bom poskusil opisati nekaj posebnosti skrbi za informacijsko varnost na področju OT pa tudi organizirati možen pristop za vpeljavo informacijske varnosti na tem področju.

Dodaten problem pa je dejstvo, da so OT naprave dostikrat dosti bolj trpežne in dolgotrajne od IT naprav in da tipično ne potrebujejo in ne dopuščajo tako pogostih sprememb, kot je ustaljeno v IT. Posledica tega je, da imamo v proizvodnji danes veliko starejših naprav, ki so bile izdelane v času, ko napadov na IT opremo še ni bilo. Tako je OT okolje brez primerne zaščite zelo ranljivo.

Opis problema

Informacijska tehnologija (IT) že dolgo časa omogoča boljše upravljanje, izvajanje in nadziranje raznih vrst poslovnih procesov.

Drugo področje, kjer so uporabljane IT tehnologije, je področje upravljanja industrijskih procesov. V zadnjem času je prevladujoča oznaka za to področje »operativna tehnologija« in predstavlja, kot so definirali v podjetju Gartner, vso strojno in programsko opremo, ki povzroča in zaznava spremembe v industrijskih procesih z neposrednim spremljanjem in/ali nadzorom industrijske opreme, naprav, procesov ali dogodkov. Primeri tehnologije (z bolj prepoznanimi angleškimi izrazi) so PLC in SCADA.

V zadnjem času mnogo podjetij ugotavlja, da je smiselno omogočiti pretok informacij od poslovnih sistemov (npr. ERP) vse do strojev in nazaj. Tak pristop ima kar nekaj prednosti, ki, kot rečeno, niso tema tega članka, a seveda prinaša nove izzive. Tudi na področju zagotavljanja informacijske varnosti.

Na področju IT je možno za informacijsko varnost skrbeti z zagotavljanjem zaupnosti, celovitosti in dostopnosti do informacij. V poslovnem svetu je prva skrb običajno zaupnost in celovitost informacij, če je potrebno občasno tudi na račun dostopnosti do informacij. V proizvodnji oz. v OT pa je zaradi posebnosti industrijskih procesov običajno drugače. Prva skrb je tipično neovirano delovanje proizvodnje, za kar je potrebna dostopnost do informacij. V očeh OT lahko za doseganje tega cilja občasno trpita celovitost in zaupnost.

Za doseganje celovite informacijske varnosti, na nivoju celotnega podjetja, je seveda nujno sodelovanje članov obeh skupin – OT in IT. Ker zaradi različnih delnih prioritet ni možno poenotiti ciljev na najnižjem nivoju (je bolj pomembna zaupnost ali dostopnost?), morajo vsi sodelavci razumeti posebnosti svojega in »drugega« področja. Usklajeno razumevanje je jasno potreben pogoj za doseganje varnosti tudi na organizacijski ravni.

Druga pogosta razlika je tudi v znanju in IT orodjih, ki jih uporabljata obe skupini. Razlog za to razliko je običajno izobraževalna pot strokovnjakov. V IT je ta dostikrat pridobljena v šolah in fakultetah informacijskega področja, v OT pa strojnega področja. Končna posledica te razlike je, da so v OT uporabljene IT rešitve, ki sicer delujejo, a je zelo verjetno, da je zrelost teh rešitev na nižji ravni. Dober primer slabe posledice bi bil lahko varnostno kopiranje podatkov, ki sicer izvaja svojo nalogo, a kopiranje ni izvedeno za vse naprave na enak način, mesto hranjenja pa ni centralizirano. S takim pristopom ne moremo doseči najvišje stopnje varnosti.

Dodaten problem pa je dejstvo, da so OT naprave dostikrat dosti bolj trpežne in dolgotrajne od IT naprav in da tipično ne potrebujejo in ne dopuščajo tako pogostih sprememb, kot je ustaljeno v IT. Posledica tega je, da imamo v proizvodnji danes veliko starejših naprav, ki so bile izdelane v času, ko napadov na IT opremo še ni bilo. Tako je OT okolje brez primerne zaščite zelo ranljivo. Dodaten izziv so tudi druge posebnosti OT, kot so dostikrat izredno omejeni časi dovoljene nedostopnosti, nedostopnost razvojnega in testnega okolja itn.

Opisane razlike tako zahtevajo drugačen, oz. vsaj prilagojen pristop in en izmed ključnih izzivov zagotavljanja informacijske varnosti je dobro razumevanje problematike oz. posebnosti in razlik v primerjavi z IT.

Ena izmed posledic naštetega je, da v OT okolju tipično ne moremo izvesti sprememb na obstoječi opremi ali opreme preprosto zamenjati. Namesto tega pa lahko obstoječo opremo obdamo z dodatnimi varnostnimi mehanizmi. Tak pristop je zato najbolj pogosto uporabljeno orožje za doseganje cilja.

Kako zagotoviti varnost?

Poglejmo ključna področja, ki jih je potrebno nasloviti. Zatečemo se lahko k preverjenemu pristopu za obvladovanje sprememb: najprej moramo razumeti trenutno stanje, nato določiti želeno končno stanje in končno še korake, ki nas bodo iz trenutnega stanja pripeljali čim bliže h končnemu stanju. Preprosto, kajne?

V prvem koraku moramo torej spoznati tako opremo, kot tudi njen namen oz. vlogo v proizvodnih procesih. Ker varnost ni absolutna, je potrebno razumeti in obvladovati tveganja ter se osredotočiti na tista, ki bodo najbolj znižala tveganje celotnega podjetja. Nujna je torej usklajenost s poslovnimi potrebami.

Še bolj konkretno: potrebno je vzpostaviti podroben seznam vse opreme, komunikacijskih kanalov (katera naprava komunicira s katero), protokolov, ter izmenjevanih informacij.



Primer: PLC z imenom PLC1 (IP naslov I), ki nadzira stroj S, odlaga podatke P na disk D računalnika R (IP naslov J) preko protokola PR. Dodamo še informacije o skrbniku, vzdrževalcih, kasneje pa še kaj več.

V drugem koraku je potrebno določiti želeno končno stanje. Tem, ki je potrebno nasloviti, je kar veliko. Poglejmo nekaj pglavitnih ciljev in vprašanj:

- Kaj sploh varujemo? Katere proizvodne procese, katere stroje, katere naprave?
- Kdo se pogovarja s kom? Potrebno je zagotoviti, da so omogočene le potrebne komunikacijske poti med elementi in med sistemi. Drugih ne smemo dovoliti, razen izjemoma in za določen čas. Če kakšna komunikacija poteka po omrežju mobilnih operaterjev, jo je skoraj nemogoče nadzorovati in jo je zato večinoma najboljše povsem prepovedati.
- Kako bomo dosegli ponovno vzpostavitev delovanja v primeru odpovedi naprav? Paziti moramo, da imamo shranjeno trenutno stanje sistema (programi, konfiguracija) in zapisan ter preverjen postopek ponovne vpeljave takega stanja. Seveda moramo znati oceniti, če je ponovna postavitve uspešna, zato moramo določiti tudi kriterij, ki nam bo odgovoril na to vprašanje.
- So verzije programske opreme posodabljanje tako, da so čim bolj varne in čim bolj stabilne?
- Za sisteme in naprave, ki jih je možno in smiselno posodabljati, je potrebno vzpostaviti proces tovrstnih aktivnosti. Seveda se moramo prej vprašati tudi, kakšne posledice ima taka sprememba tudi na veljavnost garancije proizvajalca oz. kdo sme spremembe izvajati.

- Upravljanje sprememb ter izjem naj bo nadzorovano. Spremembe morajo biti premišljene, predvidene, varne, ponovljive. Tveganja in posledice morajo biti znane, sprejemljive in potrjene. Bo sprememba vplivala na varnost uporabe? Bo sprememba lahko vplivala na veljavnost garancije? Je v primeru, da spremembe ne moremo izvesti do konca, postopek za povrnitev osnovnega stanja znan?
- Je možno odkriti zlonamerno kodo oz. onemogočiti ali vsaj omejiti njeno delovanje?
- Je odgovornost dobaviteljev, ki dobavljajo, vpeljujejo in vzdržujejo OT opremo, znana? So njihovi zaposleni izobraženi in imajo dovolj znanja iz področja IT, OT ter informacijske varnosti? Velja enako tudi za vzdrževalce v našem podjetju?
- So vsi zaposleni in dobavitelji v času nabave novih naprav ali sprememb obstoječih naprav seznanjeni z varnostnimi zahtevami? Kdo je preveril, če so ponudbe za vpeljavo in načrti za spremembe skladne z varnostnimi zahtevami?
- Na kakšen način je možno na varen način omogočiti zunanjim in notranjim vzdrževalcem dostop do OT opreme, da jo lahko vzdržujejo in v primeru napake čim hitreje ponovno vzpostavijo proizvodni proces?

Ko smo tako približno določili želeno končno stanje (verjetno zgolj za prvi korak dviga zrelosti in varnosti, saj bo podobnih korakov – po možnosti skladno z Demingovim ciklom – še več), je zelo primerno ta cilj zapisati v dokument, ki bo določal novo arhitekturo OT okolja in dogovorjene pristope oz. postopke. Prednost takega dokumenta, ki mora seveda biti ravno prav stabilen in ravno prav življenjski, je, da uskladi razumevanje vseh udeleženi in mora biti zato njim tudi





namenjen in razumljiv. Če tak dokument vsebuje mnogo zaupnih informacij, je primerno izvlečke zapisati v ločenem dokumentu in v njih strniti vse zahteve za dobavitelje. Tak dokument mora postati obvezen del razpisne dokumentacije za nakup novih naprav.

V tretjem koraku pa je potrebno začeti izvajati spremembo, skladno z našim načrtom. Žal je za ta del težko ponuditi dober splošen pristop, saj je ogromno vprašanj odvisnih od stanja v podjetju.

Vsekakor ne pozabimo na dobro osnovo! Brez podpore vodstva seveda ne bo šlo, zato je nujno njegovo razumevanje in podpora. Mogoče je potrebno pojasniti vpliv nedelovanja OT naprav na poslovanje podjetja. Naslednji korak je zagotoviti skupno razumevanje vseh deležnikov (proizvodnja, vzdrževanje, IT). Če znanja ali razumevanja tu ni dovolj, je tem zaposlenim nujno zagotoviti potrebno dodatno znanje, splošno razumevanje varnosti v OT pa vključiti v redno izobraževanje o informacijski varnosti za vse zaposlene v podjetju.

Ker je izvedba lahko zelo obsežna, je smiselno začeti z obvladljivimi koraki, najboljše po več vzporednih poteh. Te so lahko na primer:

- Nakup naslednjega novega stroja izvesti tako, da bo ta imel potrebne lastnosti
- Poiskati rešitev za stroje, ki uporabljajo najbolj ranljive protokole (na primer SMB 1.0)
- Nadgraditi stroje z novo programsko opremo, če oz. kjer je to možno
- Onemogočiti uporabo USB ključkov
- Omogočiti nadziran in varen oddaljen dostop
- Večji zalogaj pa je splošna ureditev omrežja

**Vsekakor ne pozabimo na dobro osnovo!
Brez podpore vodstva seveda ne bo šlo,
zato je nujno njegovo razumevanje in
podpora.**

- Vpeljati mrežno opremo, ki bo omogočala delitev omrežij na nivoje in na nižjem nivoju vpeljati mrežne celice v katerih bo strojna oprema, ki nadzira eno proizvodno linijo (skladno s ISA/IEC 62443)
- Zagotoviti nadzor prometa med elementi v omrežju tako, da bo možna le potrebna komunikacija

Po določeni prioritetni lestvici skladno s stopnjo tveganja je potem potrebno izvesti še druge izboljšave in stalno razmišljati, če je pristop pravi. Tako kot v IT, tudi v OT ni zaključka teh aktivnosti.

Zaključek

Ker je tema zelo očitno preobširna za tovrstni članek, sem seveda zapisal le nekatere probleme in nekatere rešitve, mnoge pomembne (npr. upravljanje identitete) pa celo povsem izpustil. A pri tovrstnih problemih se lahko zgledujemo po dveh pregovorih: »vsaka pot se začne s prvim korakom« in »slona se poje po kosih«. V ta namen pa je, upam, predstavljenega dovolj materiala za oblikovanje grobega razumevanja, ki bo lahko dovolj za začetek poti k bolj varni proizvodnji in obenem k boljšemu spancu. ■

Odprite vrata od kjerkoli



www.doorcloud.com

Brez kartic, brez čitalcev

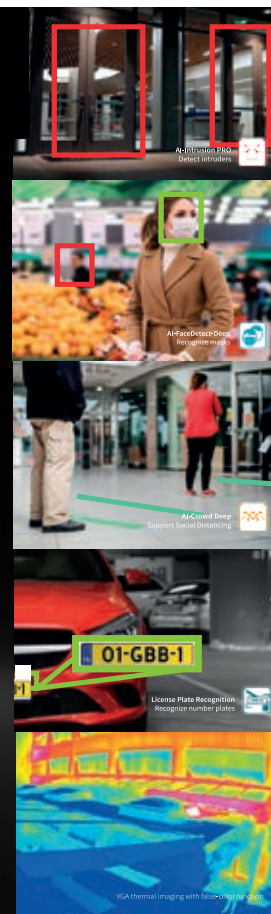
Vrata lahko odprete od kjerkoli s pomočjo pametnega telefona (iOS ali Android) ali Apple pametne ure. Čitalci kartic na račun napredne tehnologije za lociranje niso več potrebni. Identifikacija obiskovalca poteka preko mobilne aplikacije, vrata pa so izbrana s pomočjo lokacije pametnega telefona.

Če so identifikacijske kartice kljub vsemu še vedno potrebne, je mogoče čitalec kartic in mobilni dostop uporabiti skupaj na katerikoli vratih.



S74 Video System

Discreet. Versatile. Outstanding.





RANLJIVOST MICROSOFT EXCHANGE STREŽNIKOV

Ranljivosti posameznih informacijskih sistemov postajajo naša realnost. Pomembno je, da na obvestila o zaznanih ranljivostih v čim krajšem času ustrezno odreagiramo in naredimo vse potrebno, da v naših informacijskih sistemih le te čim hitreje odpravimo.

2. marca je Microsoft objavil opozorila za odpravljanje štirih ranljivosti »zero-day« v strežniku Microsoft Exchange Server, ki so bile izkoriščene v svetu.

Odkriti so bili 4 tipi ranljivosti:

- **CVE-2021-26855** Ponarejanje zahtev na strani strežnika (SSRF)
- **CVE-2021-26857** Nevarna deserializacija
- **CVE-2021-26858** Zapisovanje arbitrarne datoteke
- **CVE-2021-27065** Zapisovanje arbitrarne datoteke

V objavi v blogu Microsoft pripisuje izkoriščanje teh napak skupini, ki jo financira država in jo imenuje HAFNIUM. Skupina je v preteklosti ciljala na ameriške institucije, ki vključujejo „raziskovalce nalezljivih bolezni, odvetniške pisarne, visokošolske zavode, obrambne izvajalce in nevladne organizacije“, piše v Microsoftovem blogu. Raziskovalci v podjetju Volexity so o tem napadu objavili tudi objavo v blogu, ki jo označujejo kot operacijo Exchange Marauder.

Ranljivosti vplivajo na lokalno različico strežnika Microsoft Exchange. Te ranljivosti ne vplivajo na Microsoft Exchange Online.

Analiza ranljivosti

CVE-2021-26855 je ranljivost SSRF v strežniku Microsoft Exchange. Neavtentificirani oddaljeni napadalec bi to napako lahko izkoristil tako, da bi poslal na ranljiv strežnik Exchange posebej izdelano zahtevo HTTP. Microsoft pravi, da mora biti za uspešno izkoriščanje te napake, strežnik Exchange Server sposoben sprejeti nezaupljive povezave prek vrat 443. Uspešno izkoriščanje te napake bi napadalcu omogočilo avtentikacijo na strežniku Exchange.



Volexity, ena od treh skupin, ki so zaslužne za odkritje CVE-2021-26855, je v svojem zapisu v blogu pojasnila, da je opazila, da napadalec izkorišča to ranljivost tako, da ukrade celotno vsebino več uporabniških nabiralnikov. Vse, kar mora napadalec storiti, da izkoristi napako, je, da mora poznati IP naslov ali popolnoma kvalificirano ime domene (FQDN) strežnika Exchange in e-poštni račun, na katerega želi ciljati.

CVE-2021-26857 je v Microsoft Exchangeu nevarna ranljivost pri deserializaciji. Natančneje, napaka je v storitvi Exchange Unified Messaging Service, ki poleg drugih funkcij omogoča tudi funkcijo glasovne pošte. Da bi izkoristil to napako, bi moral biti napadalec overjen na ranljivem strežniku Exchange Server s skrbniškimi pravicami ali najprej izkoristiti drugo ranljivost. Uspešno izkoriščanje bi napadalcu podelilo privilegije za izvajanje poljubne kode, kot pod SISTEMSKIMI pravicami.

CVE-2021-26858 in CVE-2021-27065 sta v Microsoft Exchange ranljivosti pri zapisovanju arbitrarnih datotek. Te napake so lahko izkoriščene po overitvi, kar pomeni, da bi se moral napadalec najprej overiti na ranljivem strežniku Exchange Server, preden bi lahko izkoristil te ranljivosti. To je mogoče doseči z izkoriščanjem CVE-2021-26855 ali z ukradenimi poverilnicami skrbnika. Ko je napadalec overjen, lahko samovoljno piše na katero koli pot na ranljivem strežniku.

Microsoftov blog pravi, da so raziskovalci opazili, da akterji grožnje HAFNIUM izkoriščajo te pomanjkljivosti za uvajanje spletnih lupin v ciljne sisteme z namenom, da bi ukradli poverilnice in podatke o nabiralnikih. Napadalci naj bi lahko za Exchange dobili tudi adresar brez povezave (OAB). Posejdanje teh informacij bi bilo koristno za napadalca, ki izvaja nadaljnje izvidniške dejavnosti na ciljani tarči.

Zaznani vdori segajo vsaj do januarja 2021. Kljub prvotnemu razkritju 2. marca, Steven Adair, predsednik Volexityja, pravi, da je njegova ekipa delala na „več vdorih od januarja“, ki vključujejo te ranljivosti.

Rešitev

Microsoft je 2. marca izdal popravke za strežnik Microsoft Exchange Server, ki obravnavajo vse štiri ranljivosti, izkoriščene v svetu, in tri nepovezane ranljivosti.

Microsoft je izdal tudi namensko aplikacijo Microsoft Exchange On-Premises Mitigation Tool, ki konfiguracijo strežnika spremeni tako, da ranljivosti CVE-2021-26855 ni mogoče več izkoristiti, hkrati pa odstrani posledice do sedaj znanih napadov izkoriščanja. Aplikacija je namenjena manj izkušenim skrbnikom strežnikov, kasneje pa je vseeno potrebna nadgradnja strežnika.

Nekatere organizacije za ublažitev lahko izvedejo določene obvoje, dokler nameščanje varnostnih popravkov ni izvedljivo. Na primer omejevanje nezaupnih povezav na Exchange Server. Vendar močno spodbujamo vse organizacije, ki imajo lokalni strežnik Exchange Server, da čim prej uporabijo ter namestijo te popravke.

Pregled indikatorjev zlorabe (povzeto po SI-CERT)

Ker so se ranljivosti aktivno izkoriščale že pred izdajo popravkov, je potrebno vse Exchange strežnike, ki so imeli odprt dostop do vrat TCP/443, obravnavati kot potencialno zlorabljene. Posledično to pomeni, da je take sisteme potrebno forenzično pregledati za prisotnostjo indikatorjev zlorabe.

Priporočamo uporabo Microsoftovega orodja za preverjanje Test-ProxyLogon.ps1, ki poišče znake zlorab v dnevniških datotekah, ali Microsoft Safety Scanner. Prve zaznave izkoriščanja ranljivosti segajo v začetek januarja 2021, zato je pomembno, da so na voljo dnevniške datoteke vsaj za zadnje 3 mesece, še bolje pa vsaj za zadnjih 6 mesecev. Rezultate preverjanja je potrebno ustrezno interpretirati s pomočjo informacij v članku.

Npr. zaznava dogodkov v datoteki z imenom CVE-2021-26855.csv, kot v spodnjem izpisu, lahko kaže na uspešno zlorabo ranljivosti:

```
„DateTime“,“RequestId“,“ClientIpAddress“,“UrlHost“,“UrlStem“,“RoutingHint“,“UserAgent“,“AnchorMailbox“,“HttpStatus“
```



„2021-03-03T04:28:40.185Z“,“[RequestId]“,“[ClientIpAddress]“,“[redacted].si“,“/ecp/y.js“,“X-BEResource-Cookie“,“ExchangeServicesClient/0.0.0.0“,“ServerInfo-a)@[redacted].si:444/autodiscover/autodiscover.xml?#“,“200“

V tem primeru je potrebno dodatno preveriti dnevniške datoteke v mapi %PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging v času zaznave, da se ugotovi dostope do webshell skript in morebitne druge aktivnosti napadalcev.

Dodatno je potrebno preveriti odložene WebShell skripte, ki se običajno nahajajo v eni od spodnjih map:

```
inetpub\wwwroot\aspnet_client\inetpub\wwwroot\aspnet_client\system_web\%PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Exchange\FrontEnd\HttpProxy\owa\auth\
```

Imena skript so lahko naključna (npr. KGyIWEA.aspx, h7rlykkO.aspx ipd.) ali generična (npr. HttpProxy.aspx, shell.aspx, discover.aspx ipd.).

Za pomoč pri iskanju odloženih WebShell skript priporočamo uporabo orodja detect_webshells.ps1, ki so ga izdelali pri latvijskem CERTu.

Ukrepi po zaznani zlorabi (povzeto po SI-CERT)

V primeru, da se na strežnikih identificira znake, ki bi lahko kazali na zlorabo, pošljite prijavo na SI-CERT. Prijavi priložite izpise skripte Test-ProxyLogon.ps1, zašifriran arhiv odloženih datotek (webshell skript), ter izvleček iz logov o dostopih do teh datotek (iz C:\inetpub\logs\logfiles\).

Priporočeni ukrepi po potrditvi zlorabe:

- restavriranje strežnika na stanje pred zlorabo
- ponastavitev gesel vseh uporabnikov (v primeru dokazane zaznave uporabe WebShell skript)
- opcijsko: zajem delovnega pomnilnika (full memory dump) in izdelava slike sistema (disk image) za namen morebitne forenzične analize

Nove ranljivosti

Mesec dni po razkritju štirih »zero-day« ranljivosti v Exchange Serverju, je Microsoft odpravil štiri dodatne ranljivosti, ki jih je odkrila Nacionalna varnostna agencija (NSA).

CVE-2021-28480 in CVE-2021-28481 sta ranljivosti v sistemu Microsoft Exchange Server pred avtentikacijo. Ranljivost pred avtentikacijo pomeni, da se je napadalcu potrebno avtentificirati na ranljivi strežnik Exchange Server, da bi lahko izkoristil ranljivost. Vse, kar mora napadalec storiti, je izvidnica predvidenega cilja in nato poslati posebej izdelane zahteve ranljivemu strežniku Exchange.



Obe ranljivosti bi delovali podobno kot CVE-2021-26855, znan tudi pod imenom ProxyLogon, ki je ločena ranljivost pred overjanjem v strežniku Exchange Server, ki je bila vključena kot del popravkov iz varnostne posodobitve OOB (ang. Out-of-Band) marca.

CVE-2021-28482 in CVE-2021-28483 sta ranljivosti po overjanju v strežniku Microsoft Exchange Server. Za razliko od CVE-2021-28480 in CVE-2021-28481 jih je mogoče izkoristiti šele, ko se napadalec avtentificira na ranljivem strežniku Exchange. Vendar bi te napake lahko povezali z ranljivostjo Exchange Server pred avtentikacijo, da bi obšli to zahtevo. Prejšnji mesec so napadalci izkoristili ProxyLogon v kombinaciji z ranljivostmi po preverjanju pristnosti, da bi implementirali spletne lupine na ogrožene strežnike Exchange in ohranili obstojnost le te.

Za odpravljanje teh ranljivosti priporočamo namestitev varnostnega popravka: **KB5001779** ■



CYBER SECURITY

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 kibernetško varnost, bo s poglobljenim tehničnim znanjem ter pridobljenimi certifikati poskrbela za strokovno in neodvisno testiranje, ki vam bo razkrilo ranljivosti vašega informacijskega sistema.

Želite izvedeti več:

ICS Ljubljana / e-naslov: info@ics-institut.si / telefon: 05 90 54 300 / spletna stran: www.ics-institut.si



ISO 27001

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



DPO

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



ZAUPANJE: KAKO GA ZGRADITI, VZDRŽEVATI IN OBNOVITI?

Nova resničnost, ki je posledica epidemije novega koronavirusa, postavlja v organizacijah vprašanje zaupanja. Kitajski pregovor pove veliko: »Ko obstaja zaupanje, ne potrebuješ dokazov. Ko zaupanja ni, noben dokaz ne zdrži!«

Ker je definicija zaupanja izmuzljiva in jo lahko vsak razume malo drugače, je prvi korak, da definiramo zaupanje. Zaupanje je sestavljeno iz karakterja in kompetentnosti.

Preko karakterja komuniciramo z našim notranjim svetom – torej, kakšne namene imamo in kakšno stopnjo integritete izkazujemo. Naši nameni se izkazujejo preko skrbi za druge, transparentnosti in odprtosti, naša integriteta pa se izkazuje preko iskrenosti, poštenosti in avtentičnosti. Kompetentnost nam po drugi strani pove kakšne sposobnosti imamo in kakšne rezultate dela dosežemo. Sposobnosti se izkazujejo preko veščin, znanj in izkušenj, rezultati pa preko ugleda, kredibilnosti in uspešnosti. Kompetentnost je odvisna predvsem od naše inteligentnosti, izobrazbe in znanj.

Doživljanje zaupanja zaposlenih v teoretičnem okvirju se nanaša na vrednote, odnos, čustva in razpoloženje. Raziskovalci se strinjajo, da je zaupanje prepričanje med zaposlenimi, ki temelji na izmenjavi mnenj, stališč in prepričanj, in verjetnosti, da nas sodelavec (zlasti vodilni) ne bo prizadel ali nas izpostavil tveganju njegovih dejanj. Tisti, ki zaupa, je pripravljen biti ranljiv proti tistemu, ki mu zaupa in nad katerim nima nadzora. Zaupanje torej vodi v določena pričakovana vedenja med zaposlenimi z namenom upravljanja tveganj tako, da oblikujejo oblike sodelovanja.

Vrednote so naši splošni notranji standardi in vrednosti. Pomagajo nam določiti, kateri občutki, dogodki, dejanja in sodelavci so zaželeni in kateri ne. Prispevajo k doživljanju zaupanja na splošno in spodbujajo nagnjenost k zaupanju. Vrednote, ki jih delimo s sodelavci, gradijo zaupanje, in obratno. Zaupanje torej temelji na relativno stabilnih karakteristikah (vrednotah, lastnostih) zaposlenih.

Poleg znane formule, ki jo je zapisal pisatelj Stephen R. Covey, ki pravi, da ko se v katerikoli organizaciji zaupanje izboljšuje, se povečajo tudi rezultati poslovanja in znižujejo se stroški. Torej, zaupanje se spleča in obratno.

Pomanjkanje ključnih veščin je največja grožnja poslovanju. Med najbolj iskane veščine, ki jih zahteva poslovno okolje danes, so inovativnost, reševanje problemov, voditeljstvo in prilagodljivost. Da bi lahko pridobili in zadržali te veščine vodilni priznavajo, da morajo biti sposobni ustvarjati takšne organizacije, ki jim ljudje zaupajo.

Merjenje javnega mnenja Edelman Trust Barometer (sve-tovna raziskava v 28 državah in s 33.000 anketirancev) za leto 2021 poroča, da je pandemija povzročila krizo zaupanja javnosti. V tem smislu ugotovitve kažejo na nov mandat organizacije, ki je zdaj institucija, ki ji zaposleni najbolj zaupajo (61%), da igra ključno vlogo pri odzivanju na sodobne družbene izzive. Raziskava razkriva tudi pričakovanje, da bo organizacija v času globalne negotovosti skrbela za neprekinjeno poslovanje. Zlasti vodilni si prizadevajo, da dejavno sodelujejo pri ponovni vzpostavitvi zaupanja in reševanju poslovnih ter socialnih vprašanj, ki bodo opredelila tudi prihodnost zaposlenih.

Pomanjkanje ključnih veščin je največja grožnja poslovanju. Med najbolj iskane veščine, ki jih zahteva poslovno okolje danes, so inovativnost, reševanje problemov, voditeljstvo in prilagodljivost. Da bi lahko pridobili in zadržali te veščine vodilni priznavajo, da morajo biti sposobni ustvarjati takšne organizacije, ki jim ljudje zaupajo.

Ustvarjanje in vzdrževanje zaupanja je velik izziv. A odgovornost je prav na vodilnih, da ustvarjajo pozitiven odnos med delodajalcem in zaposlenimi, ki temelji na zaupanju. Kreativ-



nosti, reševanje problemov in prilagodljivosti se ne da zaukazati. Te so posledica tega, kako zaposleni razumejo, verjamejo in se poistovetijo s tem, za kar se organizacija zavzema in kako močno zaupajo vodilnim. Zaupanje je tudi najmočnejša valuta pri privabljanju in zadržanju najboljših sodelavcev.

Izguba zaupanja se ne razlikuje od večine drugih težav - preden jo lahko rešite, morate najprej razumeti, kako deluje in kakšne so posledice. Zaupanje ima tri sestavine: pristnost, logika in empatija. Ko vse tri stvari sinhrono delujejo, imamo veliko zaupanje, če pa katera od teh treh ne deluje, je zaupanje ogroženo.

Najtežje med temi sestavinami je pristnost. Čeprav je recept preprost - bodite le vi - biti resnični jaz ni vedno lahko, še posebej, če se v kakršnikoli obliki razlikujete od večine sodelavcev. Ampak ne pozabite: izguba zaupanja lahko povzroči vrsto neželenih posledic. Vodstva poziva, naj poskrbijo, da so njihove organizacije varne, dobrodošli prostori in da imajo zaposleni dobro samopodobo ter, da se lahko izkažejo.

Kako razviti zaupanje v organizaciji?

Najboljši pristop je, da začnete pri razvijanju zaupanja pri sebi in znotraj svoje delovne skupine v organizaciji. Zaupanje je obojestranski proces – torej tako, kot želijo sodelavci zaupati vam, si tudi vi želite zaupati sodelavcem.

Zaupanje je psihološko stanje zaposlenih, medtem ko je socialni kapital značilnost organizacijske kulture organizacije. Socialni kapital povzroča odnose z visoko ravno zaupanja, ta pa vpliva na formiranje visoke ravni socialnega kapitala in tako obstaja tesna povezava med zaupanjem in ostalimi viri socialnega kapitala. Značilnosti družbene mreže, skupnih norm, prepričanj in formalnih pravil vplivajo na zaupanje.

Zaposleni, ki se medsebojno ne razumejo in nimajo skupnih interesov oziroma skupnega prepričanja, težko medsebojno sodelujejo in je skoraj nemogoče, da bi bogatili raven socialnega kapitala v organizaciji. Socialni kapital namreč izhaja iz splošnega prepričanja, ki omogoča zaposlenim izmenjevati skupne ideje in daje vrednost skupnim izkušnjam.

Kako lahko organizacija igra ključno vlogo pri ponovni vzpostavitvi zaupanja? Predlagam pet načinov, kako se lahko odzove na poziv k ukrepanju:

- ukrepajte proti dezinformacijam (večina anketirancev Trust Barometer (53%) je menila, da bi morala organizacija aktivno sodelovati pri zagotavljanju natančnih informacij),
- vodilni so odgovorni za transformacijske spremembe (rezultati Trust Barometra razkrivajo, da se od vodilnih pričakuje, da bodo spodbudili družbene spremembe. 86% vprašanih pričakuje, da se bodo javno izrekli o družbenih izzivih),
- sprejmite verodostojni namen (po uničujočih vplivih pandemije na zdravje in gospodarstvo je Trust Barometer ugotovil večjo zavest o ključnih družbenih vprašanjih, kot so dostop do zdravstvenega varstva in izobraževanja, podnebnih sprememb in revščine),
- vzpostavite partnerstvo za spremembe (pandemija je pripeljala do nekaterih najbolj navdihujočih primerov učinkovitih partnerstev. Nujnost in obseg izzivov, s katerimi se soočamo zdaj, bosta zahtevala ustvarjalno sodelovanje za spodbujanje sprememb na sistemski ravni),
- mislite lokalno in se razvijajte na obstoječih odnosih (raziskava kaže, da tudi v organizacijah ni prostora za samozadovoljstvo; zaupanje v vseh poslovnih sektorjih upada). ■



VOC

VARNOSTNO OPERATIVNI CENTER

zagotavljamo kibernetsko varnost v energetiki

INFORMACIJSKE STORITVE IN INŽENIRING, D.D.

INFORMATIKA

Q www.informatika.si

Celovite rešitve
po meri naročnika

Potrjeno najbolj
priljubljen prevzem
paketov

*Več kot

97%

uporabnikov ocenjuje
dostavo v PS Paketomat
kot odlično.

PS PAKETOMAT

Za dostavo izberite PS Paketomat in svoje pošiljke prevzemite
kadarkoli, 24/7 – brez čakanja v vrsti in brez kontakta z drugimi
osebami! Preprosto, hitro in priročno!

www.posta.si/paketomat



The background of the entire page is a photograph of a tall, metal electricity pylon with multiple cross-arms and insulators, supporting several high-voltage power lines. The pylon and lines stretch diagonally across the frame from the bottom left towards the top right. In the foreground, there is a dense field of tall, dry, golden-brown reeds or grasses, some with seed heads, which are slightly out of focus. The sky is a clear, bright blue with a few wispy white clouds. The overall composition suggests a connection between nature and modern infrastructure.

**Prenašamo
energijo,
ohranjamo
ravnovesje.**