Korporativna varnost

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

Letnik 2019, november • št. 21



Tradicionalna 11. mednarodna konferenca »Dnevi korporativne varnosti 2020«

Ljubljana, 11-12. marec 2020

Moderni varnostni izzivi postavljajo neprekinjenost delovanja elektronskih omrežij v poseben položaj

mag. Tanja Muha, direktorica AKOS



Vodilno globalno podjetje na področju varovanja

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

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

CE FC UL RoHS ISO 9001:2000

www.dahuasecurity.com

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



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
november 2019

Izvod revije je brezplačen

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

ISSN 2232-6170

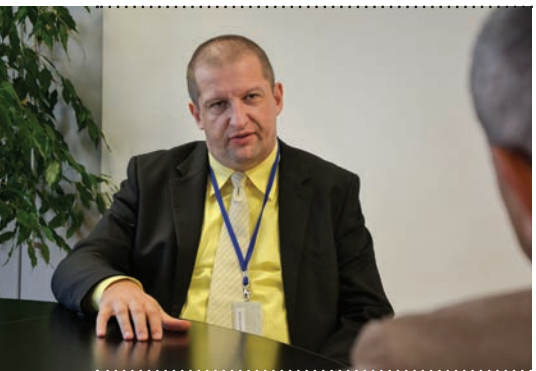
Objavljeni prispevki in njihova vsebina odražajo mnenja in stališča avtorjev, ter predstavljajo v celoti njihovo odgovornost.

Dinamično varnostno okolje, v katerem poslujejo naše organizacije, nam ne dopušča več tistega potrebnega časa, da bi se vedno znova spraševali ali v naših organizacijah potrebujemo ustrezne mehanizme za zagotavljanje varnosti. To je na žalost postalo dejstvo, ki nas sili predvsem v smeri iskanja odgovorov, kako z omejenimi viri zagotoviti čimbolj učinkovit sistem celovitega obvladovanja tveganj. Kompleksnost varnostnih tveganj in groženj pa prinaša nove potrebe po racionalizaciji in predvsem združevanju procesov na določenih segmentih, ki so bili še do včeraj medsebojno močno ločeni. Eden od takih procesov je vsekakor, da se procesi zagotavljanja kibernetske varnosti izključujejo iz področja informatike, in se vedno bolj vključujejo v proces korporativne varnosti. Seveda bo za stabilizacijo in učinkovitost integracije teh dveh pomembnih procesov potrebno kar nekaj časa, ki pa nam ga na žalost zahtevno varnostno okolje ne daje na razpolago. Drugo pomembno dejstvo, katero mora v naših procesih najti določeno prioriteto, je vsekakor iskanje odgovorov, kako čimprej v praksi implementirati zahteve Zakona o informacijski varnosti. Smo v trenutku, ko imamo na trgu vedno več ponudnikov, tako imenovanih Varnostno operativnih centrov (Security Operational Centre), ki pa bodo na tako majhnem in razdrobljenem tržišču vsi težko preživeli. Vsekakor velja ubrati pot združevanja in dviga kvalitete. V tem konkretnem primeru, zaradi izredno omejenih virov, tako manj predstavlja več. To pomeni manjše število centrov in centralizacija virov ter dvig kvalitete, ki bo omogočala tudi prodor na mednarodno tržišče. Pri naročnikih pa nujno potrebujemo dvig zavedanja, da prenos določenega dela zagotavljanja kibernetske varnosti na ponudnike Varnostno operativnih centrov ne pomeni, da v svojih organizacijah ne potrebujejo več izvajati ključnih in osnovnih ukrepov na področju informacijske varnosti. Za konec pa bo potrebno nujno poudariti, da so strokovne oči uprte v korake, ki jih bo naredila država po ustanovitvi Uprave za informacijsko varnost. Le ta se mora predvsem znajti v zahtevnem področju povezovanja vseh razdrobljenih deležnikov javnega in zasebnega okolja, ter akademske sfere pri poenotenju smeri razvoja kibernetske varnosti na nacionalnem in posledično tudi na vseh ostalih ravneh.

V tokratni številki zato ponovno odpiramo pomembne teme, ki so tudi tokrat zelo tesno povezane z različnimi procesi zaščite kritične infrastrukture in zagotavljanjem kibernetske varnosti. Revija pa, kot je že v navadi, prinaša zanimive intervjuje z odločevalci strateškega okolja. Posebej želimo omeniti dva ključna strateška sogovornika, ki prihajata iz Agencije za komunikacijska omrežja in storitve Republike Slovenije ter novoustanovljene Uprave za informacijsko varnost. Revija pa prinaša tudi druge odlične in strokovno informativne teme, ki bodo strokovnjakom različnih profilov pomagale pri širitvi njihovega strokovnega razumevanja varnostnega okolja in procesov, ki stojijo pred njimi.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
dr. Uroš Svete, v.d. direktorja Uprave RS za informacijsko varnost

VZPOSTAVITEV SISTEMA KIBERNETSKE VARNOSTI KOT NUJNI PREDPOGOJ ZA NORMALNO DELOVANJE REPUBLIKE SLOVENIJE 15



ODGOVORNOST MENEDŽMENTA KORPORATIVNE VARNOSTI V KRITIČNI INFRASTRUKTURI

Ocenjevanje, upravljanje in obvladovanje tveganj za delovanje kritične infrastrukture (v nadaljevanju: KI) je kompleksno in interdisciplinarno zahtevno delo. Pristop k ocenjevanju tveganj je metodično zasnovan na principih sistemskega inženiringa, vsebinsko na preprečevanju možnih škod in izgub, operativno pa na sodobnih rešitvah upravljanja in obvladovanja tveganj. 19



KIBERNETSKA VARNOST V KRITIČNI INFRASTRUKTURI

Kibernetska varnost zadeva vse sektorje. Kljub temu pa se kritične infrastrukture soočajo z velikim izzivom na področju kibernetske varnosti. Digitalna preobrazba med drugim zahteva večjo zaščito kibernetske varnosti za kritično infrastrukturo, z drugimi besedami, vsa infrastruktura, katere sistemi, viri in storitve so temeljni za razvoj družbe, in ki zagotavljajo kontinuiteto pri normalnem delovanju storitev, katere zagotavljata država in javna uprava. 33



INTERVJU
Ana Struna Bregar,
direktorica Centra energetsko učinkovitih rešitev (CER)

PODNEBNI VPLIVI NAS SILIJO V RESNO SPREMEMBO KONCEPTOV DOJEMANJA POSLOVANJA NAŠIH ORGANIZACIJ 43



KIBERNETSKA VARNOST MOBILNIH OMREŽIJ 5G

Mobilna telekomunikacijska omrežja so postala ključna javna infrastruktura, mobilne telekomunikacijske storitve pa enako pomembne, če ne celo bolj, kot dobava elektrike, vode, plina... Pomen infrastrukture iz leta v leto narašča, spreminja pa se tudi njena vloga. Pred leti je bila namenjena prvenstveno govornim komunikacijam, danes pa mora biti načrtovana za vedno večje potrebe uporabnikov po mobilnih podatkovnih storitvah. 47

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

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

VARNOSTNI IZZIVI POSTAVLJAJO NEPREKINJENOST DELOVANJA ELEKTRONSKIH OMREŽIJ V POSEBEN POLOŽAJ

Moderno in dinamično varnostno okolje pred nas prinaša vedno nova tveganja in izzive, na drugi strani pa tehnologija napreduje z nesluteno hitrostjo. Če v ta okvir dodamo še vedno pogostejše pojavljanje različnih kibernetskih tveganj, lahko z gotovostjo potrdimo, da je to področje trenutno podvrženo velikim izzivom, ki jih je potrebno ustrezno uravnavati. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Tanjo Muha.

Vodite Agencijo za komunikacijska omrežja in storitve Republike Slovenije, ki ima zelo obširen nabor pristojnosti. Nam lahko na kratko opišete na katerih področjih vse ima AKOS pomembno vlogo.

Agencija kot regulatorni organ obstaja že vse od leta 2001, ko je bila primarno pristojna na področjih telekomunikacij, pošte in upravljanja z radiofrekvenčnim spektrom. Danes bi lahko pristojnosti agencije razdelili na pet glavnih področij, to so: elektronske komunikacije, pošta, elektronski mediji, železniški promet in upravljanje z radiofrekvenčnim spektrom. Znotraj teh sektorjev, pa ima agencija več pristojnosti, med drugim tudi na področju zagotavljanja celovitosti in varnosti telekomunikacijskih omrežij in storitev, ter varstva končnih uporabnikov.

Operaterji morajo skladno z zakonodajo sprejeti ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj omrežij in storitev, prav tako pa tudi ukrepe za zagotavljanje celovitosti omrežij, da se zagotovi neprekinjeno izvajanje storitev.

Izredno aktivno sodelujete v okviru mednarodnih organov EU. Nam lahko kratko predstavite te aktivnosti agencije.

Agencija je članica združenj evropskih regulatorjev na vseh področjih njenega dela in pristojnosti, v okviru katerih aktivno sodeluje pri pripravi dokumentov, in s tem sooblikuje regulatorne politike na evropskem nivoju. Predstavniki agencije se redno udeležujejo sestankov ekspertnih delovnih skupin ter plenarnih zasedanj. Agencija pa redno sodeluje tudi z Evropsko komisijo in Agencijo evropske unije za varnost omrežij in informacij - ENISO. V letošnjem letu je agencija na tem področju še posebej aktivna, saj sem sama podpredsednica združenja evropskih regulatorjev za elektronske komunikacije BEREC, vodja sektorja na agenciji Katja Kmet Vrčko

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

pa je sopredsednica ekspertne delovne skupine, ki se ukvarja z vprašanjem kibernetske varnosti v 5G omrežjih.

Kibernetska varnost postaja eden od najpomembnejših izzivov modernega varnostnega okolja. Kako v tem okviru zagotavljati ustrezno varno in neprekinjeno delovanje telekomunikacijskih operaterjev?

Prvi pogoj za to je zakonodaja, ki zavezuje operaterje k določenim ravnanjem. Drugi pogoj pa je dejansko izvajanje zakonodaje v praksi. Obveznosti operaterjev na tem področju določa Zakon o elektronskih komunikacijah. Operaterji morajo skladno z zakonodajo sprejeti ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj omrežij in storitev, prav tako pa tudi ukrepe za zagotavljanje celovitosti omrežij, da se zagotovi neprekinjeno izvajanje storitev. Operaterji morajo tudi redno obveščati agencijo v primerih kršitev varnosti ali celovitosti, če so te pomembno vplivale na delovanje omrežij ali izvajanje storitev. Agencija lahko zahteva revizijo varnosti in sprejem ter izvajanje varnostnega načrta, v kolikor se to izkaže za potrebno. Agencija pa je pripravila in sprejela tudi Splošni akt o varnosti omrežij in storitev, ki podrobneje določa način vzpostavitve sistema upravljanja varovanja informacij (SUVI) in sistem upravljanja neprekinjenega poslovanja (SUNP). V zakonu so predpisani tudi ukrepi v primeru izjemnih stanj. Agencija izvaja nadzor nad spoštovanjem teh zahtev na strani operaterjev in v primeru nespoštovanja tudi ustrezno sankcionira kršitelja. Se pa agencija zaveda, da je mogoče marsikaj rešiti še preden agencija uvede nadzorne postopke. Z namenom, da operaterji spoštujejo zakonodajo, agencija tako z operaterji redno sodeluje in jim nudi podporo pri ustrezni implementaciji zahtev zakonodaje. Pomembno je tudi seznanjanje operaterjev z novostmi oziroma dogajanjem na teh področjih, tako da si bo agencija tudi v prihodnje prizadevala tudi za preventivno delovanje in ustrezno informiranje, ter izmenjavo znanja z operaterji in tudi drugimi pristojnimi institucijami in organi.

Pred nami stoji še zahtevna implementacija določil Zakona o informacijski varnosti, kot posledica evropske NIS direktive. Kako sodelujete z nosilno institucijo za uveljavitev omenjenega zakona in predvsem procesov kibernetske varnosti?

Pristojnosti agencije na področju zagotavljanja varnosti in celovitosti omrežij in storitev segajo že skoraj 10 let nazaj. V tem času je agencija pridobila veliko dragocenih izkušenj na tem področju, ki so sedaj dobrodošle pri sami implementaciji NIS direktive. Že v preteklosti je agencija z vsemi ostalimi resornimi organi na področju zagotavljanja varnosti imela vzpostavljeno zgledno sodelovanje, ki se sedaj nadaljuje z vključitvijo novih organov. Agencija ima vzpostavljeno redno sodelovanje tudi z Upravo za informacijsko varnost, ki je bila ustanovljena letos. Tako je bila agencija vključena v delovno skupino za pripravo Zakona o informacijski varnosti, ki jo je vodilo pristojno ministrstvo, skupaj pa smo pripravljali tudi oceno tveganj 5G omrežja z vidika kibernetske varnosti v Republiki Sloveniji, ki jo je zahtevalo Priporočilo Evropske komisije o kibernetski varnosti 5G omrežij. Kaže se, da je agencija pomemben člen pri oblikovanju pristopov in politik na teh področjih, ravno zaradi večletnih izkušenj, aktivnega delovanja in nekaterih že vzpostavljenih pristopov. Tako namerava agencija tudi v prihodnje sodelovati in nuditi podporo s svojim strokovnim znanjem, v kolikor bo k sodelovanju povabljena s strani pristojnih organov.



Kako bi ocenili izzive, ki jih prinašajo geopolitične napetosti med glavnimi svetovnimi velesilami in Evropo? Veliko je bilo napisanega o prepovedi kitajskih ponudnikov tehnologije 5G. V katero smer bodo po vaših izkušnjah in informacijah šle evropske države, med njimi tudi Slovenija?

To je zelo kompleksno vprašanje, ki buri dogajanje tako na nacionalnem, evropskem, kot tudi svetovnem nivoju, in vključuje več vidikov preučevanja, med drugim varnostni, ekonomski in zunanjepolitični. In temu primerno je potrebnega tudi več časa za iskanje ustreznega enotnega odgovora. 5G omrežje bo preoblikovalo našo družbo in gospodarstvo ter odprlo nove priložnosti za ljudi in posel. Je pa zato nujno potrebna vzpostavitev ustrezne oblike mehanizma zagotavljanja varnosti. Evropska komisija se je tega lotila na način, da je sprejela Priporočilo o kibernetski varnosti 5G omrežij, na podlagi katerega so države članice morale do konca meseca junija pripraviti svoje ocene tveganj 5G omrežij z vidika kibernetske varnosti. Trenutno pa, v sodelovanju z Evropsko komisijo in ENISO, BEREC v okviru delovne skupine, kateri naša agencija sopredseduje, pripravlja usklajeno oceno tveganj držav članic, ter na podlagi tega orodje za definiranje nabora ustreznih, učinkovitih in sorazmernih možnih ukrepov za obvladovanje tveganj pri 5G omrežju. V tem času so nekatere države članice že sprejele individualne odločitve glede uporabe opreme kitajskega proizvajalca opreme Huawei. Tako se je na primer Nemčija odločila, da ne bo prepovedala Huaweijeve opreme pri gradnji omrežij 5G. Za sodelovanje pri gradnji omrežja 5G s Huawei pa se dogovarja tudi Italija. Francija je trenutno edina država, ki je uzakonila možnost podaje veta na uporabo določene vrste opreme. Končne odločitve glede tega v Sloveniji še ni, je pa dejstvo, da so že obstoječa mobilna omrežja v Sloveniji grajena z opremo Huawei. Zato je potrebno o morebitnih prepovedih resno razmisliti, saj bi to lahko imelo resne posledice na vračanje že investiranih sredstev in tudi višino bodočih investicij operaterjev.

Kje vidite glavne varnostne izzive, ki jih prinaša pričakovana uveljavitev tehnologije 5G?

Kot že rečeno bo 5G omrežje preoblikovalo našo družbo in gospodarstvo ter odprlo nove priložnosti za ljudi in nove poslovne priložnosti. Zaradi tehničnih karakteristik 5G omrežij in posledično možnosti njegove uporabe se bo to



omrežje uporabljalo na vseh segmentih družbe in na sektorjih, ki se sedaj v to zgodbo še niso vključevali. Govorimo o pametni industriji 4.0, širjenju obsega e-storitev na področju zdravja, izobraževanja, poslovanja, povezovanja pametnih naprav M2M in internetu stvari, pametnih omrežjih (smart grid), upo-

Kot že rečeno bo 5G omrežje preoblikovalo našo družbo in gospodarstvo ter, odprlo nove priložnosti za ljudi in nove poslovne priložnosti. Zaradi tehničnih karakteristik 5G omrežij in posledično možnosti njegove uporabe se bo to omrežje uporabljalo na vseh segmentih družbe in na sektorjih, ki se sedaj v to zgodbo še niso vključevali.



rabi dronov in samovozečih vozil, in nenazadnje o možnostih uporabe za javno varnost, ter zaščito in reševanje (PPDR). S povezovanjem velikega števila sistemov in naprav, ter posledičnega zbiranja ogromnega števila podatkov, se veča tudi možnost različnih zlorab. In zlorabe se v takem okolju lahko dogajajo tako na strani naprav pri končnih uporabnikih, kot tudi na samem omrežju. Zato je potrebno poleg mehanizmov in zakonodaje, ki skrbijo za varstvo osebnih podatkov in zasebnosti, poskrbeti tudi za ustrezne mehanizme in zakonodajo, za zagotavljanje informacijske in kibernetske varnosti, ter varnosti samih omrežij. Še vedno velik del tveganj pa predstavljajo uporabniki storitev sami, ki se ne zavedajo svojega dela odgovornosti v tem okolju. Treba je osveščati tudi uporabnike.

Kakšen pomen v AKOS namenjate procesom izobraževanja in usposabljanja? Je to z vaše perspektive učinkovit vzvod za dvigovanje splošnega zavedanja, posebej med operaterji?

Kot zelo pomemben dopolnilni del k sami regulaciji vidimo tudi samoregulacijo, pri spodbujanju katere pa veliko lahko pripomore ozaveščenost končnih uporabnikov, ki se posledično bolj zavedajo svojih pravic in obveznosti. Zato agencija veliko pozornost namenja tudi opismenjevanju na področju varnosti na svojem novem portalu za medijsko in informacijsko pismenost – MIPI, pri čemer se je dogovorila za sodelovanje tudi z drugimi organi, ki se ukvarjajo s tovrstnimi vprašanji. V kolikor se izkažejo potrebe, agencija organizira tudi različne delavnice za operaterje, kar se je prav tako izkazalo za koristno.

Ste tudi inšpekcijski organ, ki predvsem skrbi za uveljavitev in izpolnjevanje določil Zakona o elektronskih komunikacijah (Zekom). Kakšni so vaši generalni občutki in ocena glede stanja v praksi med operaterji? Je to zavedanje po ustrezni implementaciji varnostnih zahtev na dovolj visokem nivoju?

Vsi operaterji morajo na podlagi nacionalne zakonodaje sprejeti takšne varnostne ukrepe, ki so primerni predvidenemu tveganju oz. izhajajo iz analize tveganj, pri čemer morajo upoštevati značilnosti svojega poslovanja, velikosti organizacije, pomembnosti funkcij in storitev, ki jih zagotavljajo. Zavedanje

Združenje omogoča, da se srečujejo na enem mestu strokovnjaki s področja zagotavljanja varnosti, ki izmenjujejo dobre prakse, tako da lahko vsi člani pridobimo z vključenostjo v to združenje. Pri tem ni nezanemarljivo, da združenje povezuje tako deležnike iz različnih panog privatnega sektorja, kot tudi javnega sektorja.

potrebnih varnostnih zahtev je pogojeno tudi z zrelostjo operaterja. Večji operaterji so za svojo usposobljenost začeli pridobivati certifikate, kot so za sistem upravljanja neprekinjenega poslovanja (ISO 22301) ali za sistem vodenja varovanja informacij (ISO 27001). Nadalje so nekateri že vzpostavili operativne varnostne centre, ki bdijo nad dogajanjem v omrežju in imajo vzpostavljene procese ravnanja v primeru določenih varnostnih incidentov, ali v primeru napak ali okvar v omrežju. Izvajajo redne ocene tveganja, ter posodabljajo svojo varnostno politiko in politiko neprekinjenega poslovanja glede na tveganja s katerimi se soočajo oz. so jih prepoznali v okviru svojih analiz. Pri manjših operaterjih je to zavedanje na nižjem nivoju oziroma so razpoložljiva finančna sredstva za zagotavljanje visoke varnostne ravni bistveno manjša. Vseeno pa lahko pri tem do določene mere upoštevamo tudi dejstvo, da posamezen negativni dogodek pri manjših operaterjih vseeno nima tako velikega vpliva oz. prizadene manjše število uporabnikov, storitve, ki jih zagotavljajo ti operaterji, pa niso kritične za državo in njene funkcije.

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

Združenje omogoča, da se srečujejo na enem mestu strokovnjaki s področja zagotavljanja varnosti, ki izmenjujejo dobre prakse, tako da lahko vsi člani pridobimo z vključenostjo v to združenje. Pri tem ni nezanemarljivo, da združenje povezuje tako deležnike iz različnih panog privatnega sektorja, kot tudi javnega sektorja.

Menite, da je združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti lahko odgovor na obvladovanje zahtevne varnostne situacije, in ali so lahko taka združenja ustrezen partner državnim institucijam, kot je AKOS, pri zagotavljanju njenega osnovnega poslanstva?

Ko se pogovarjamo o informacijski in kibernetski varnosti v luči digitalizacije družbe in vpeljave 5G omrežja, se obseg vključenih deležnikov zelo poveča. Prihaja do prepletanja sektorjev, ki so se do sedaj bolj redko srečevala, mnoga med njimi pa tudi še niso posvečala potrebne pozornosti zagotavljanju varnosti. Zato je po mojem osebnem mnenju ključno povezovanje in izmenjevanje znanj, izkušenj in dobrih praks, ter seveda ozaveščanje vseh vpletenih. Združenje korporativne varnosti je primer dobrega načina povezovanja, ki zagotovo lahko pripomore k kvalitetnejši razpravi in skupnemu doseganju zastavljenih ciljev.

Agencija bo še naprej proaktivno sodelovala z drugimi pristojnimi organi na področju zagotavljanja varnosti, pri tem pa si bo prizadevala za vzpostavitev enotnega informacijskega orodja za poročanje o incidentih, kar bi poenostavilo tako delo organom, kot tudi zavezancem za poročanje.



Za konec bi vas prosili, da kratko ocenite izzive, ki stojijo pred agencijo v prihodnosti.

V prihajajočih mesecih bo agencija imela zagotovo še veliko dela pri pripravi ustreznih podlag v okviru vodenja delovne skupine v BEREC in pri sodelovanju z Ministrstvom za javno upravo pri implementaciji prenovljenega evropskega zakonika na področju elektronskih komunikacij, ki tudi na področju varnosti omrežij in storitev prinaša kar nekaj novosti. V prihodnje bo zagotovo treba oblikovati ustrezne obveznosti dobaviteljev opreme in posodobiti obstoječe varnostne zahteve za operaterje omrežij na nacioalnem in evrospkem nivoju. Agencija se pripravlja na javni razpis z javno dražbo frekvenc za javne mobilne storitve, med drugim tudi za 5G omrežje. Na podlagi ugotovljenih tveganj bo verjetno treba vključiti pogoje za zagotavljanje varnosti javnih omrežij tudi pri dodeljevanju pravic uporabe teh frekvenc. Veliko bo treba narediti tudi na ozaveščenosti končnih uporabnikov. Tako je agencija v letošnjem letu vzpostavila portal za medijsko in informacijsko pismenost – MIPI. Namenjen je opismenjevanju uporabnikov in posledično njihovemu odgovornejšemu obnašanju. Preko portala želi agencija na poljuden in prijazen način svetovati, uporabnikom dati konkretne napotke, ter opozarjati na novosti, aktualne teme in kakovostne vsebine. Na portalu bo agencija tudi v prihodnje objavljala novičke iz različnih področij svojega delovanja, tako tudi v povezavi z vprašanji povezanimi z zagotavljanjem varnosti. Agencija bo še naprej proaktivno sodelovala z drugimi pristojnimi organi na področju zagotavljanja varnosti, pri tem pa si bo prizadevala za vzpostavitev enotnega informacijskega orodja za poročanje o incidentih, kar bi poenostavilo delo, tako organom, kot tudi zavezancem za poročanje. ■

Slovensko združenje korporativne varnosti

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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

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

www.ics-institut.si

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

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

www.ics-institut.si

Avtor: Vojko Volk, veleposlanik



KOLUMNA

UJETNIKI PRIHODNOSTI

„Zelo verjetno je, da precenjujemo potencial in koristi 5G prihodnosti. Če vam kdo reče, da ve, kaj nam 5G prinaša, se obrnite in odkorakajte stran“.

/Ken Schmidt, ameriški marketinški strokovnjak/

Konec septembra 2019 so ameriški mediji evforično poročali o ameriški zmagi v carinski vojni s Kitajsko, ki je pristala na zahtevo po večjem uvozu iz ZDA. Celo predsedniku Trumpu nenaklonjeni mediji so se strinjali, da gre za uspeh; „Trump je prevladal v trgovinski vojni s Kitajsko“, je zapisal CNN in izpostavil, da je rast kitajskega gospodarstva prvič padla na vsega 5 odstotkov. S tem je bil storjen skoraj popoln obrat od Amerike, ki je svetu vladala z vojaškimi posredovanji, v Ameriko, ki svet namesto z orožjem obvladuje s trgovinskimi pritiski in carinami. Skoraj istočasno je Svetovna trgovinska organizacija (WTO) Ameriki odobrila že vrsto let pričakovano uvedbo carin za seznam izdelkov iz EU v skupni vrednosti dobrih 7 mrd evrov. S tem je bil sklenjen nekakšen prvi krog v carinski vojni ZDA z ostalim svetom in v tem prvem krogu je brez dvoma prevladala Trumpova odločenost, da ukrepa zoper trgovinsko neravnotežje, v katerem je EU že več kot desetletje dosegala ogromne presežke, Kitajska pa še večje. V letu 2018 je presežek EU v blagovni menjavi med ZDA in EU (skupaj slabih 800 mrd evrov) znašal dobrih 150 mrd evrov, pri čemer sta si EU in ZDA drug drugemu prva partnerja, EU pa je prvi trg sveta za ameriški izvoz. Neprimerno bolj pa je neuravnotežena menjava ZDA s Kitajsko, kjer imajo ZDA pri skupni menjavi 590 mrd evrov kar 340 mrd evrov primanjkljaja; pri 110 mrd evrov izvoza imajo ZDA kar 480 mrd uvoza in tem za 370 mrd trgovinskega deficita. Na ravni statistik in številk je skratka vse na dlani; ZDA je ukrepala v zaščito svojega trga, pri čemer ji je bila odločitev olajšana tudi zato, ker je med vsemi svetovnimi trgi prav ameriški daleč najbolj samozadosten in to v vseh pogledih, začenši s surovinami, hrano in energenti. Ameriški trg je edini, ki brez večje škode lahko preživi tudi brez izvoza, kar je prednost, ki se je trgovski duh Amerike še kako zaveda.

Precej očitno je, da ZDA v času predsednika Trumpa na EU gleda predvsem kot na tekmeca in konkurenco, ki jo je treba podrediti ali pa kar premagati, medtem ko Kitajska na EU gleda kot na ključni trg, brez katerega nima alternative za svoj ogromni industrijski potencial in za status vodilne izvoznice sveta.

A številke in statistike niso vse in tako kot pri vsem tudi tu obstaja druga plat medalje, tista, na katero je opozarjal že ustanovni oče ZDA, Thomas Jefferson; „Egoistični trgovski duh ne pozna meja in ne pozna usmiljenja do načel, razen do dobička“. In res si ni težko predstavljati, kako ubogi bi lahko bili dosežki človeštva, če bi bil dobiček edino gonilo in vodilo sveta. Ravno to je težava vseh, ki na dosežke in posledice globalizacije gledajo izključno z očmi nacionalnih interesov in trgovinskih bilanc. Pri tem prednjači ravno sedanji predsednik ZDA Trump, ki ne samo da ne sliši sporočil ustanovnih očetov Amerike, ampak v svojem govoru na skupščini ZN septembra 2019 brez težav izpove vizijo prihodnosti sveta, ki je obče človeško gledano precejšnja regresija od dosežkov zahodne civilizacije, med katere ne sodita samo blagostanje ljudi in sožitje narodov, ampak tudi delovanje po načelih solidarnosti, skupnega delovanja v korist miru in sodelovanja pri zaščiti okolja. V njegovem govoru ni nobenega stavka, ki ne bi odstopal od temeljnega sporočila, ki gre v en sam stavek; Amerika želi, da se vse države brigajo predvsem zase, se zamejijo v svoja ozemlja, potem pa – in to je ključno - vsaka posebej sklepajo trgovinske pogodbe z ZDA. Lahko si predstavljamo kako neprimerno lažje bi se bilo Ameriki o carinah pogajati samo z Nemčijo, namesto z Evropsko komisijo, ki se pogaja v imenu enotnega trga EU in s tem vseh njenih članic. In kaj bi šele bilo, ko bi se z Ameriko morala sama pogajati Slovenija ...

O tem, kako močno Trump verjame, da je z denarjem mogoče doseči vse, priča tudi njegova namera odkupa Grenlandije od Danske, kar je povzročilo zelo resno ohladitev odnosov med državama. Trumpova namera je bila seveda povezana z zaščito interesov Amerike v vse bolj napeti energetski tekmi s Kitajsko, ki se je pred leti razglasila za „državo v bližini Arktike“ in



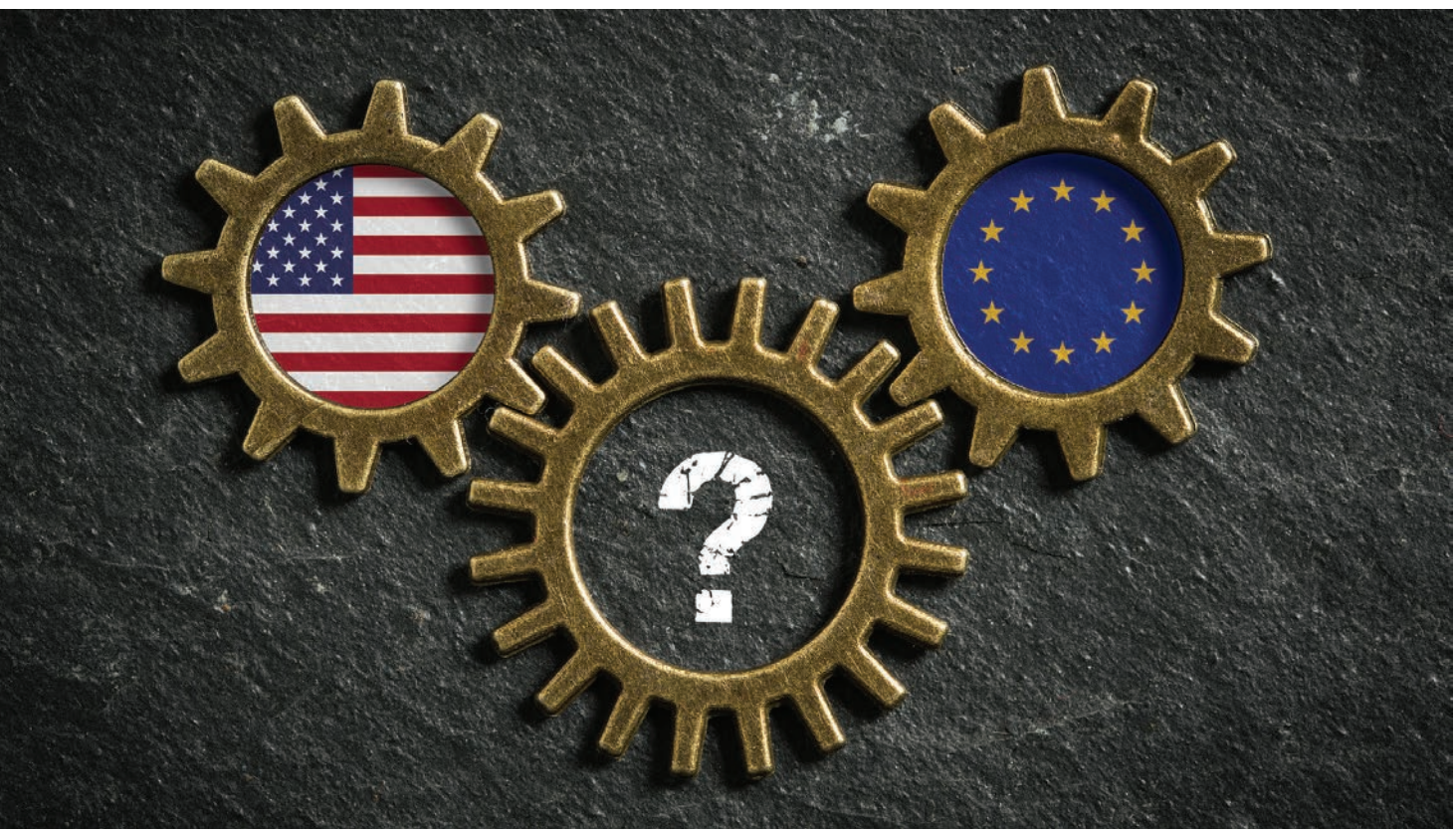
pa seveda Rusije, ki tam res je a nima zadostnih finančnih in strokovnih kapacitet za učinkovito izkoriščanje težko dostopnih surovin. Bolj primeren in 21. stoletju ustreznejši pristop bi bil, da bi se ZDA obrnile na Dansko in tudi na EU s predlogi za skupno zavarovanje energetskih in tudi okoljskih interesov zahoda na Arktiki. Edino to bi bil korak, ki bi Arktiki in vsemu človeštvu prinesel več garancij za ohranjanje okolja in vzdržno poseganje v črpanje arktičnih virov. Arktika je namreč bogata z lantanoidi, redkimi zemljinimi prvinami, na katerih naj bi slonela prihodnost naslednje tehnološke revolucije. O tem, kako je videti brutalno poseganje Rusije v vire Sibirije, Kitajske, v vire osrednje Afrike in Brazilije, v vire Amazonije, pa se je svet lahko prepričal že doslej. Pa ne gre samo za naravne vire. Rusija in Kitajska že v skorajšnji prihodnosti načrtujeta tudi plovbo po ti. arktični svilni poti, ki bi čas plovbe ladje med vzhodom in zahodom skrajšala za najmanj dva tedna. Gre za vprašanje, zakaj lahko Kitajska s svojim strateškim projektom svilne poti oz. „en pas, ena cesta“, ponuja sodelovanje vsem zainteresiranim državam, še posebej Evropi, ZDA pa tega ne zmore in spravi skupaj zgolj zmedeno zahtevo po nakupu Grenlandije?

Precej očitno je, da ZDA v času predsednika Trumpa na EU gleda predvsem kot na tekmeca in konkurenco, ki jo je treba podrediti ali pa kar premagati, medtem ko Kitajska na EU gleda kot na ključni trg, brez katerega nima alternative za svoj ogromni industrijski potencial in za status vodilne izvoznice sveta. In prav v tem je ključni paradoks sedanjih razmer, na katere se Kitajska odziva neprimerno manj politično in predvsem bolj „kapitalistično“ od ZDA in izkazuje več razumevanja za ključno hibo kapitalizma, ki je v tem, da produkti brez trga oz. kupcev nimajo smisla in slej ko prej postanejo breme. Tudi ZDA se ne morejo zanašati na to, da bodo prav vse blago prodale doma, še manj to velja za storitve in usluge, pri katerih so ZDA močno odvisne od izvoza. Ali z drugimi besedami; medtem ko Kitajska počasi sprejema spoznanje, da je globalizacija dvosmerna cesta, na kateri se je treba prilagajati, se v ZDA še vedno spogledujejo z možnostjo, da bi globalizacijo enosmerno zavirali v izključno svojo korist. To pa je približno tako, kot če bi hoteli ustaviti čas.

Še pred 10 leti so bila razmerja v bogastvu oziroma absolutnem BDP med ZDA, EU in Kitajsko močno različna, danes pa so že močno zbližana. Predvsem Kitajska je v desetletju svojih dvomestnih stopenj rasti močno zmanjšala zaostanek za EU, medtem ko se je EU močno približala ZDA. Če bi obveljali sedanji trendi, v katerih Kitajska raste le še za „skromnih“ pet do šest odstotkov na leto, bi v naslednjem desetletju in pol dohitela EU, medtem ko bi distanca med EU in ZDA ostala bolj ali manj enaka. Gotovo je le to, da se v razmerah pospešene globalizacije v obdobju visokih rasti svetovnega gospodarstva razlike hitro zmanjšujejo v korist Kitajske. A iz tega delati strategijo nekakšnega kontroliranega razvoja, kar opažamo v aktualni politiki ZDA, je dvorezen meč. V prvi vrsti zato, ker posledic ni moč natančno predvideti in, ker niso samo ekonomske, ampak tudi politične in socialne. Kadar zunanja politika postane samo izračun stroškov in koristi (cost&benefit) se potem zgodi, da ameriški predsednik oceni, da so stroški miru previsoki in ukaže umik ameriške vojske iz Sirije, svoje dotedanje zaveznike sirijske Kurde pa prepusti maščevalnemu pohodu turških sil. In potem vse skupaj opraviči s tem, da tudi Kurdi niso pomagali Američanom pri izkrcanju v Normandiji ...

S tem pridemo do ključne razvojne zanke, v kateri se bo razviti svet hkrati s povečanim dotokom delovne sile z vseh koncev sveta soočal s temeljno posledico pete tehnološke revolucije, ki bo družba z nizko uporabo delovne sile.

Še večji problem, zgolj ekonomističnih pogledov na prihodnost sveta, je problem migracij, ki postajajo svetovni fenomen, pri čemer je posebej zanimiv položaj Indije. Ta država - kontinent je neke vrste večna pepelka svetovnega gospodarstva, ki nenehno vstaja iz pepela a iz njega nikoli zares ne vstane. V zadnjem desetletju, ki je bilo zanjo znova polno neizpolnjenih pričakovanj, je Indija namesto preboja v prve vrste gospodarskih sil sveta postala ena največjih izvoznic delovne sile, še zlasti v ZDA, kjer so priseljenci iz Indije že nekaj let na prvem mestu, celo pred Mehičani. Globalizacija ob mobilnosti kapitala pač prinaša tudi neprimerno večjo mobilnost prebivalstva in potem je izid jasen; če bodo razlike med bogatimi in revnimi naraščale bo ekonomskih migrantov vedno več, in obratno. S tem pridemo do ključne razvojne zanke, v kateri se bo razviti svet hkrati s povečanim dotokom delovne sile z vseh koncev sveta soočal s temeljno posledico pete tehnološke revolucije, ki bo družba z nizko uporabo delovne sile. Paradoks pri tem pa je, da zahod, še zlasti Evropa, vsaj še naslednji dve desetletji močno potrebuje novo delovno silo, saj so stopnje nezaposlenosti tako v EU kot v posameznih članicah rekordno nizke. V Sloveniji je stopnja nezaposlenosti v letu 2019 prvič padla na zgodovinskih 4.2 odstotka, sta pa pred nami Nemčija s 3 odstotno in Češka z neverjetno, vsega 2 odstotno brezposelnostjo, pa Slovaška s 5.5 odstotno in tako naprej. To pomeni, da je EU lačna delovne sile vseh vrst, kvalificirane in nekvalificirane, a ker EU ni država in ne zmore sprejemati odločitev v smeri zaviranja ilegalnih in spodbujanja legalnih prihodov ljudi v EU, je stanje kritično.



Pričakovanja glede velikih potreb po energentih in redkih surovinah se že zdaj izkazujejo za pretirana in ne kaže, da bodo večji problem od migracij ali celo morebitne prenaseljenosti v razvitem svetu. V 70-letih prejšnjega stoletja je bil svet prestrašen zaradi napovedi in izračunov znanstvenikov slovitega inštituta MIT (Meje rasti, op.vv), ki so napovedovali izčrpanje vseh svetovnih rezerv nafte še pred letom 2000, in skoraj popolno onesnaženje vode in zraka v industrijskih državah zahoda. Danes vemo, da so zaloge nafte in tudi plina domala neomejene, in predvsem vemo, da sta voda in zrak v razvitih družbah neprimerno čistejša kot v manj razvitih. Še več, uspelo nam je celo zaceliti ozonsko luknjo na našem nebu, ki so jo politiki dolga leta zanikali kot znanstveno izmišljotino. Nekaj podobnega velja tudi za že omenjene lantanoide, ki so bili še do včeraj strateški material prihodnosti, zlasti litij, zdaj pa ga v baterijah naših mobilnih telefonov že izpodriva dostopnejši grafen (graphene). Ali z drugimi besedami; izkušnje nas učijo, da kadar stroške varovanja okolja in naravnih virov vključimo v stroške naših proizvodenj, nastane prostor za iskanje rešitev in njihovo financiranje.

Strahovi človeštva o prihodnosti, ki nas bremenijo do te mere, da nas misli na prihodnost spravijo v depresijo, ker kdo ve česa vse nam bo primanjkovalo in bomo umirali žejni, ker ne bo vode, vse se vedno usmeri na materialne reči, ki se potem praviloma izkažejo za manj pomembne in predvsem nadomestljive. V resnici bodo v prihodnosti človeka usodnega pomena predvsem vrednote in temeljna načela sobivanja med ljudmi in narodi. Če bodo vrednote ohranjene, bomo ohranili tudi civilizacijo, če bo prevladalo materialno nad človeškim, pa bo konec neizbežen, tako kot je bil neizbežen za vse doslej izginule civilizacije sveta. ■

V resnici bodo v prihodnosti človeka usodnega pomena predvsem vrednote in temeljna načela sobivanja med ljudmi in narodi.

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
dr. Uroš Svete
v.d. direktorja Uprave Republike Slovenije za informacijsko varnost

VZPOSTAVITEV SISTEMA KIBERNETSKE VARNOSTI KOT NUJNI PREDPOGOJ ZA NORMALNO DELOVANJE REPUBLIKE SLOVENIJE

Uprava RS za informacijsko varnost je ugledala luč sveta in bo v prihodnje ključni tvorec aktivnosti in koordinacije na področju zagotavljanja kibernetske varnosti Republike Slovenije. Izkoristili smo priložnost in se pogovorili z dr. Svetetom, da nam pomaga predstaviti ključne korake na področju delovanja uprave, ki jo trenutno vodi.

Pred nami je vzpostavitev težko pričakovane Agencije za informacijsko varnost. Nam lahko poveste kaj bodo njene osnovne naloge?

Dejansko gre za Upravo Republike Slovenije za informacijsko varnost (UIV), ki kot organ v sestavi deluje v okviru Ministrstva za javno upravo (MJU). V prvi fazi delovanja UIV je potrebno do konca leta 2019 izvesti postopen prenos pristojnosti nad področjem kibernetske varnosti iz Urada za varovanje tajnih podatkov (UVTP), kateremu je bila pristojnost nad tem področjem podeljena s sklepom o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (Uradni list RS, št. 17/17 z dne 10. 4. 2017). Zakon o informacijski varnosti (ZInfV) v 40. členu določa, da UIV v sklopu prenosa pristojnosti od UVTP prevzame naloge, arhive in dokumentacijo, ki se nanašajo na informacijsko varnost, ter javne uslužbence, pravice proračunske porabe, opremo in druge zbirke podatkov oziroma evidence iz prevzetega delovnega področja.

> Majhna država kot je Slovenija, z omejenimi viri na vseh področjih, bi morala povsod, predvsem pa na področjih, pomembnih za nacionalno varnost, bolj stopiti skupaj in narediti več za dobro vseh nas.

Istočasno UIV pripravlja vse potrebno za določitev izvajalcev bistvenih storitev (IBS), ki so ena od skupin zavezancev po ZInfV, kar je pomembno tudi z vidika izvajanja NIS direktive. Kasneje bodo določeni tudi organi državne uprave, ki sestavljajo drugo skupino zavezancev, ki pa je nacionalna specifika v ZInfV.

UIV mora čimprej zagotoviti materialno-tehnične in kadrovske pogoje, da bo lahko z letom 2020 polno operativna pri izvajanju vseh nalog, ki ji jih nalaga ZInfV.

Zakon o informacijski varnosti pred Upravo postavlja zahtevne naloge v zelo napetih časovnih okvirih. Kaj bodo prioritetna področja s katerimi se boste začeli prednostno ukvarjati?

*avtor je član Slovenskega združenja korporativne varnosti



Predvsem je treba povezati vse obstoječe deležnike v nacionalnem sistemu kibernetske varnosti. Tudi tukaj podobno kot še na marsikaterem drugem področju v Sloveniji ni optimalnega sodelovanja. Sicer zelo omejene zmogljivosti na operativni ravni, ki pa glede na vložek še vedno dosegajo nadpovprečne rezultate, bi bilo mogoče bolje povezati in tako izkoristiti sinergije. Vsekakor pa brez resnega dolgoročnega in koordiniranega vlaganja v nacionalni sistem kibernetske varnosti država ne bo mogla zagotoviti primerne stopnje odpornosti na kibernetske grožnje.

Vzpostavitev celovitega sistema vseh deležnikov na področju kibernetske varnosti bo nujen korak. Kako ste si začrtali vzpostavitev tega eko sistema?

Kot že rečeno, je treba deležnike najprej povezati in z njimi navezati partnerske odnose. Res je UIV pristojni nacionalni organ na področju kibernetske/informacijske varnosti, a brez dobrega sodelovanja z organi na operativni ravni (oba CERT-a, nacionalni in vladni, zmogljivosti na MO, MNZ in SOVI) ne more veliko. Prav tako je pomembno dobro sodelovanje z Ministrstvom za izobraževanje, znanost in šport (MIZŠ) in izobraževalnimi ustanovami, če želimo v sistem pripeljati nove strokovnjake oz. dvigniti splošno raven informacijske varnostne kulture v državi preko kurikulumov na različnih stopnjah izobraževanja. Sodelovanje je potrebno seveda tudi z Ministrstvom za gospodarski razvoj in tehnologijo (MGRT), ko gre za podporo in krepitev kibernetske varnosti v podjetjih različnih velikosti. Seznam deležnikov se tukaj seveda ne konča. Zelo pomembno bo sodelovanje z AKOS in posredno z operaterji elektronskih komunikacij, ki zagotavljajo osnovno infrastrukturo za dostop do interneta, od katerega je dandanes odvisno tako rekoč vse, pa tudi z izvajalci bistvenih storitev z različnih področij kritične infrastrukture. Ne smemo pozabiti niti RRI organizacij in strokovnih združenj s področja kibernetske/informacijske varnosti, ki lahko pomembno doprinesejo k uporabi novih tehnoloških rešitev in pristopov za zmanjševanje kibernetskih tveganj. In nenazadnje, kibernetska varnost je postala pomembna tema tudi v mednarodnih odnosih, zato tesno sodelujemo tudi z Ministrstvom za zunanje zadeve

Vsekakor je Združenje lahko pomemben člen pri izmenjavi dobrih praks, novih tehnoloških rešitev in izkušenj, predvsem pa pri zelo pomembni nalogi ozaveščanja o pomenu zagotavljanja kibernetske/informacijske varnosti za celotno družbo pri odločevalcih, tako na nacionalni ravni, kot tudi na ravni podjetij in organizacij.

V Republiki Sloveniji imamo trenutno relativno nekonsistenten zakonodajni pristop, kjer do istih končnih deležnikov država posega z različno zakonodajo, ki bi lahko bila v svoji izvedbeni fazi zahtev bolj usklajena. Kot primer lahko izpostavimo Zakon o kritični infrastrukturi in Zakon o informacijski varnosti. Kako boste pristopili k poenostavitvi zakonske ureditve v smeri boljše učinkovitosti in zmanjšanja birokratskih pristopov ločenega urejanja posameznih področij?

Z vašo trditvijo se je v mnogočem mogoče strinjati. Velikokrat se pozna, da so za pripravo različnih zakonov pristojna različna ministrstva, ki bi lahko med sabo bolje so-

delovala. Tu trčimo ob, lahko bi kar rekli, našo nacionalno hibo, in sicer premajhno medsebojno sodelovanje. Majhna država kot je Slovenija, z omejenimi viri na vseh področjih, bi morala povsod, predvsem pa na področjih, pomembnih za nacionalno varnost, bolj stopiti skupaj in narediti več za dobro vseh nas.

Kako si zamišljate zbiranje ključnih podatkov o kibernetskih incidentih, ki bodo končno podala realno sliko o ogroženosti Slovenije na tem področju?

To je ena od zelo pomembnih nalog UIV, ki bo skupaj z ostalimi deležniki v sistemu morala čim prej vzpostaviti enotno platformo za priglasitev incidentov. Deležnike v sistemu, morda pa tudi širše, je treba povezati v omrežje za izmenjavo in deljenje informacij. Brez tega je v realnem času tako rekoč nemogoče oceniti stopnjo ogroženosti. Hkrati bi deljenje informacij med deležniki omogočilo boljšo preventivo pred kibernetskimi grožnjami, v primeru incidentov pa hitrejšo odpravo posledic in povrnitev v normalno delovanje.

Tako zahtevna uprava za svoje delovanje potrebuje ustrezne vire in kadre. Je tukaj dovolj razumevanja s strani Vlade Republike Slovenije, da bo temu področju namenila več virov, kot jih je namenjala do sedaj?

Za UIV je v predlogu proračuna za 2020/21 predvideno 2,1 in 2,4 mio EUR. V ta zneska je vključen tudi del, namenjen za delovanje SI-CERT. Če se nam bo pri izvedbi načrtovanih ukrepov uspelo povezati z že zgoraj omenjenimi deležniki (npr. z MIZŠ pri vpeljavi tem s področja kibernetske/informacijske varnosti v izobraževalne programe na vseh ravneh izobraževanja, razvoju novih programov na tem področju na naših fakultetah, štipendiranju itd.) in če UIV ne bo dobila kakšnih dodatnih nalog, ocenjujemo, da so načrtovana sredstva primerna. Bo pa za čim večji učinek morda treba ubrati tudi kakšen inovativen pristop, ki ni običajen v javni upravi.

Upravljalci kritične infrastrukture so eden izmed najbolj občutljivih delov eko sistema, večina bo verjetno padla tudi v okvir ponudnikov bistvenih storitev na podlagi Zakona o informacijski varnosti. Bo komunikacija z njimi potekala po kakšnem posebnem sistemu?

Kot že omenjeno, bi si jih želeli povezati v nekakšno omrežje zaupanja, ki bi ga lahko izkoristili tudi v druge namene, ne samo za potrebe ZInfV.

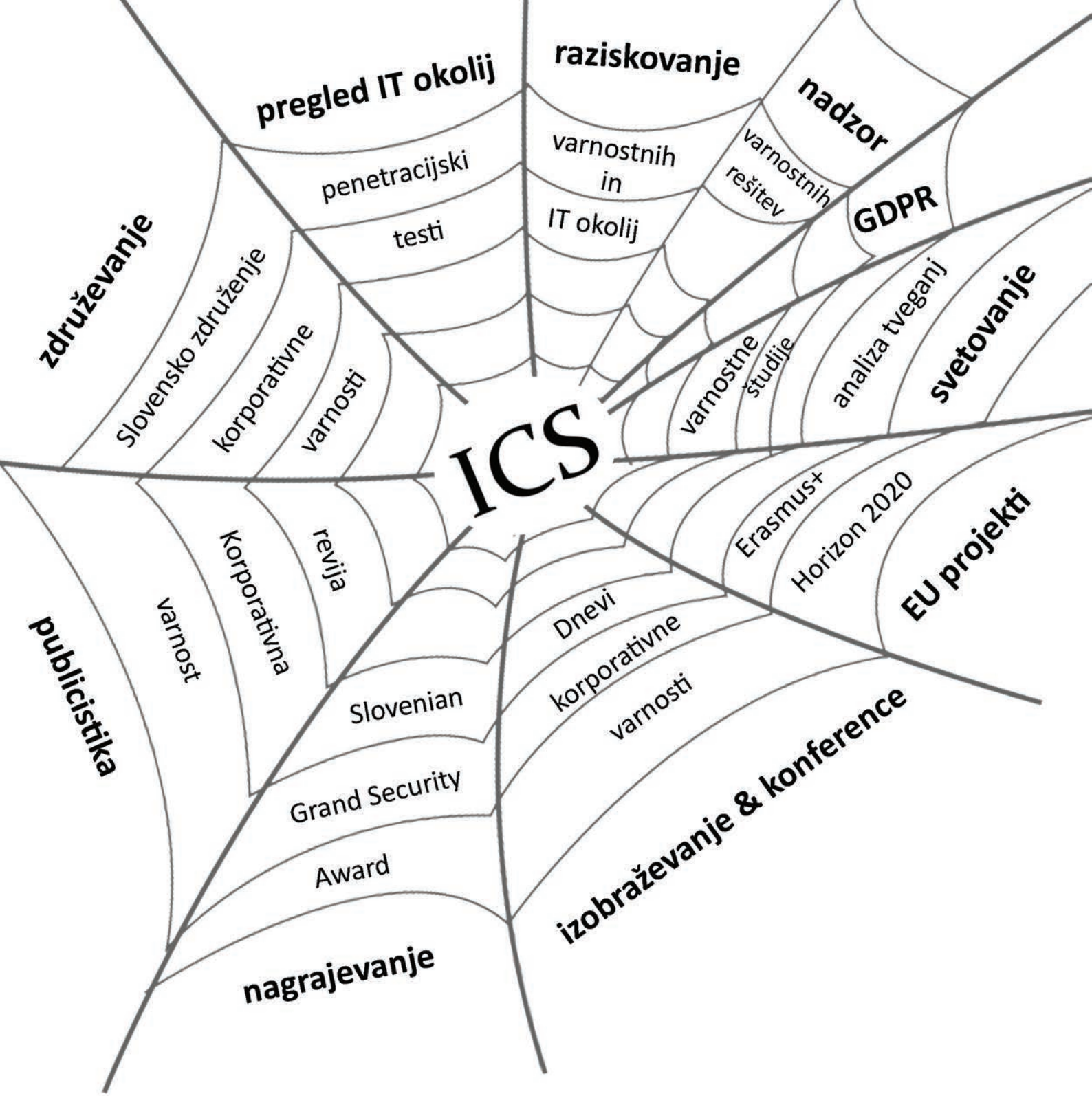
Slovensko Združenje za korporativno varnost združuje pomembno večino organizacij, ki upravljajo kritično infrastrukturo. Je to lahko eden od pomembnih kanalov za izmenjavo nujno potrebnih dobrih praks, novih tehnoloških rešitev in izkušenj?

Vsekakor je Združenje lahko pomemben člen pri izmenjavi dobrih praks, novih tehnoloških rešitev in izkušenj, predvsem pa pri zelo pomembni nalogi ozaveščanja o pomenu zagotavljanja kibernetske/informacijske varnosti za celotno družbo pri odločevalcih tako na nacionalni ravni kot tudi na ravni podjetij in organizacij.

Prihajate iz akademskega okolja zato verjetno lahko pričakujemo, da boste področju raziskav in razvoja namenili določeno mero pozornosti s podpro institucije, ki jo trenutno vodite? Kakšni so vaši načrti in pričakovanja na tem pomembnem področju?

Absolutno. Raziskave in razvoj, pa tudi izobraževalni programi so ključni elementi t.i. preventivnih mehanizmov kibernetske varnosti, ki pa učinkujejo v večji družbeni odpornosti šele na dolgi rok. Pa vendarle si iskreno želim, da bi v Sloveniji prišlo do interdisciplinarnega sodelovanja tako pri raziskovalnih projektih, kot vzpostavljanju izobraževalnih in študijskih programov na področju kibernetske varnosti. Slednja se namreč navezuje na neločljivo povezanost človeka in družbe z informacijsko in komunikacijsko tehnologijo, in njeno raziskovanje mora nujno povezati spoznanja naravoslovno-tehniških ved z družboslovjem in humanistko. Vsekakor pričakujem, da se bo ob našem prizadevanju in skupnih naporih v okviru Evropske unije slovenski akademski in raziskovalni prostor odzval pozitivno. ■





ICS

Institut za korporativne varnostne študije

Cesta Andreja Bitenca 68, Ljubljana

www.ics-institut.si

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



ODGOVORNOST MENEDŽMENTA KORPORATIVNE VARNOSTI V KRITIČNI INFRASTRUKTURI

Morda je pravi trenutek, da nekaj rečemo o menedžmentu korporativne varnosti v kritični infrastrukturi in o njihovi odgovornosti za obvladovanje varnostnih groženj, varnostnih tveganj, ukrepov za zaščito, zagotavljanje neprekinjenega delovanja ter obvladovanja kriznih situacij. Govorimo o menedžmentu, ki je na ravni Vlade odgovoren za varnost, upravljanje in neprekinjeno delovanje kritične infrastrukture, menedžmentu Ministrstva za obrambo, ki ima status usklajevalca in usmerjevalca pri izvajanju nalog, menedžmentu posameznih ministrstev, kot nosilcev sektorjev kritične infrastrukture in menedžmentu upravljavcev kritične infrastrukture, ki so neposredno odgovorni za varnost, neprekinjeno delovanje ter obvladovanje kriznih stanj kritične infrastrukture s katero upravljajo. Se pa najprej postavlja izhodiščno vprašanje ali kritična infrastruktura sploh ima ustrezen (učinkovit) menedžment korporativne varnosti.

Iz naših dosedanjih varnostnih projektov v kritični infrastrukturi je evidentno, da je tovrstni menedžment kadrovsko šibak, nedorečen v kompetencah in z zelo nizkim organizacijskim statusom. Kot tak se ne more učinkovito in usklajeno lotiti prenove upravljanja varnostnih groženj in varnostnih tveganj, kot tudi ne izgradnje učinkovitega sistema ukrepov za zaščito kritične infrastrukture ter ukrepov obvladovanja kriznih okoliščin. Morda kakšna resnejša raziskava, zlasti pa čas, bo pokazal, da je treba menedžment korporativne varnosti v sektorjih kritične infrastrukture in v posameznih gospodarskih družbah, zavodih in drugih organizacijah prenoviti v smeri dviga izobrazbe, znanja, izkušenj in sposobnosti obvladovanja varnostnih izzivov. Prva linija odgovornosti, da se v menedžmentu korporativne varnosti kaj posodobi, je v vladnih ukrepih, ukrepih vodstev pri nosilcih in v ukrepih vodstev pri upravljavcih kritične infrastrukture, katerim dihajo za vrat zakonodaja, resolucije, strategije ter zahteve in potrebe vedno bolj turbulentnega in kompleksnega varnostnega okolja.

Splošno o odgovornosti

V splošnem lahko odgovornost definiramo kot odnos posameznega subjekta do sprejetih pravil vedenja (družbenih norm); to je pravnih, političnih in moralno-etičnih norm. Odnos do teh norm pa je lahko pozitiven ali negativen; zato lahko tudi rečemo, da odgovornost pomeni zavesten prevzem dolžnosti za izvršitev dane naloge in s tem prevzem posledic te dolžnosti, naj si bodo zanj ugodne ali ne. Ko gre za upoštevanje pravnih norm, govorimo o pravni odgovornosti, ko pa gre za spoštovanje političnih in moralno-etičnih norm, govorimo o t.i. nepravni odgovornosti. V sklop pravne odgovornosti sodi kazenska, disciplinska in materialna (odškodninska) odgovornost, v sklop nepravne odgovornosti pa potemtakem spadata (družbeno) politična in moralna odgovornost, (javna kritika, odpoklic, razrešitev). Pravno in nepravno odgovornost v nekem smislu združuje statusna (položajna) odgovornost, za katero je pogosto v rabi tudi izraz pravno-politična odgovornost. Ko gre za iskanje (ne)odgovornosti povsem določene osebe, se rabi izraz osebna (tudi objektivna) odgovornost, ko pa gre za iskanje (ne)

*avtor je član Slovenskega združenja korporativne varnosti

Upravljanje korporativne varnosti kritične infrastrukture zajema: zaznavanje, prepoznavanje, ocenjevanje in upravljanje ranljivosti, varnostnih groženj in varnostnih tveganj, načrtovanje ukrepov zaščite, zagotavljanje neprekinjenega delovanja, obvladovanje izrednih dogodkov in kriznih stanj, varnostno usposabljanje in izmenjavo varnostnih informacij.

odgovornosti celotnega vodstva ali kakega organa, organizacije ali delovnega telesa, pogosto govorimo o kolektivni odgovornosti. Vestno ali nevestno opravljanje strokovnega in specializiranega dela vselej pogojuje tudi zahteve po strokovni odgovornosti; to je odgovornost strokovnjakov kot posameznikov, odgovornost projektnih timov, ekspertnih skupin, strokovnih organov in strokovnih služb itd. V celotnem spletu odgovornosti in neodgovornosti je smiselno obravnavati še horizontalno in vertikalno odgovornost, ter interno in eksterno odgovornost. Horizontalna odgovornost pomeni odgovornost na neki ravni (npr. na ravni določenega organa), vertikalna odgovornost pa pomeni odgovornost nekoga nasproti nekemu višjemu organu. Notranja odgovornost (npr. direktorja) je odgovornost do upravnih organov in do zaposlenih, zunanja (recimo družbeno-politična) odgovornost pa je odgovornost do lokalnih oblasti, ki je sodelovala v oblikovanju in izvrševanju kadrovske politike. Vsak vodja se mora v okviru svojega področja delovanja (področja delovanja organizacije, ki jo vodi) ter v okviru zakonskih določil, standardov in družbenih norm zavedati vseh vrst odgovornosti, da bi na ta način obvladoval dejanske in prikrite slabosti, pomanjkljivosti, nezakonitosti in nasploh škodljive pojave v svojem delovnem in poslovnem okolju.

Aktualni formalnopravni okvir za odgovorno upravljanje korporativne varnosti kritične infrastrukture

Upravljanje korporativne varnosti kritične infrastrukture zajema: zaznavanje, prepoznavanje, ocenjevanje in upravljanje ranljivosti, varnostnih groženj in varnostnih tveganj, načrtovanje ukrepov zaščite, zagotavljanje neprekinjenega delovanja, obvladovanje izrednih dogodkov in kriznih stanj, varnostno usposabljanje in izmenjavo varnostnih informacij. Lahko rečemo, da je za delovanje in razvoj kritične infrastrukture sprejetih kar nekaj pomembnih dokumentov (zakonov, resolucij, strategij), iz katerih lahko razberemo cilje in naloge posameznih pristojnih organov in organizacij kritične infrastrukture. Glavni pristojni organi so, Vlada ter nosilci in upravljavci kritične infrastrukture. Formalnopravni okvir - z vidika sodobnih varnostnih groženj, varnostnih tveganj, zaščite, zahtev po neprekinjenem delovanju in trajnostnemu razvoju kritične infrastrukture - vidimo v naslednjih dokumentih: Strategiji razvoja Republike Slovenije 2030 (2017), Resoluciji o strategiji nacionalne varnosti Republike Slovenije (2010 in 2019), Strategiji kibernetske varnosti (2016), Nacionalnem programu varstva okolja (2018), Zakonu o kritični infrastrukturi (ZoKI 2017), Zakonu o informacijski varnosti (ZinfV 2018), Pravilniku o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (2019), Zakonu o elektronskih komunikacijah (2017), Zakonu o poslovni skrivnosti (2019) in nenezadnje tudi v Splošni uredbi o varstvu osebnih podatkov (GDPR). To so dokumenti, ki veljajo za celotno kritično infrastrukturo ter sledijo novim varnostnim izzivom. Za posamezne sektorje kritične infrastrukture so pomembni še nekateri drugi formalnopravni okvirji, ki jih v tem prispevku ne obravnavam. Vedno bolj kaže realnost in hkrati prevladuje mnenje, da sta najbolj ranljiva in podvržena varnostnim grožnjam sektor energetike in sektor informacijsko-komunikacijskih omrežij in sistemov, ki sta močno ranljiva tudi s tveganji naravnih in drugih nesreč. To vse pa dejansko vpliva tudi na ranljivost in ogroženost drugih sektorjev kritične infrastrukture, ki so bolj ali manj (lahko tudi usodno) odvisni od omenjenih dveh sektorjev.

Odgovornost na ravni vlade

Vlada kot najvišji organ državne uprave izdaja predpise in sprejema pravne, politične, ekonomske, finančne, organizacijske in druge ukrepe, ki so potrebni za razvoj države in za urejenost razmer na vseh področjih v pristojnosti države. Tako je Vlada glavni usmerjevalec tudi na področju upravljanja kritične infrastrukture. Tako na primer 17. člen ZoKI Vladi nalaga izdelavo politike upravljanja kritične infrastrukture, ki bi začrtala vizijo, strategijo, cilje delovanja in razvoja ter zaščite kritične infrastrukture. Po 26. čl. ZinfV pa je Vlada zadolžena za izdelavo Strategije informacijske varnosti kot okvir za izvedbo ukrepov za vzpostavitev učinkovitega nacionalnega sistema zagotavljanja informacijske varnosti. Tako bi ta strategija - skupaj s Strategijo kibernetske varnosti - omogočila učinkovitejše obvladovanje informacijskih in kibernetskih groženj in tveganj tudi pri izvajalcih bistvenih storitev, to je v energetiki, digitalni infrastrukturi, oskrbi s pitno vodo, preskrbi s hrano, zdravstvu, prometu, bančništvu, infrastrukturi finančnega trga in varstvu okolja. Gre torej za kritično infrastrukturo, ki je usodno pomembna tudi za delovanje državnih organov, še zlati pa za delovanje celotnega gospodarstva. S tega zornega kota se postavlja vprašanje, zakaj Vlada nima vzpostavljene posebne službe za kritično infrastrukturo, ki bi, v sodelovanju z nosilci sektorjev kritične infrastrukture, spremljala, usmerjala in nadzirala delovanje in razvoj ter potrebne varnostne mehanizme. V tem kontekstu bi lahko govorili, da ima Vlada vzpostavljen ustrezen menedžment upravljanja kritične infrastrukture, ki bi ga zakoličili v zgoraj navedeni vladni politiki upravljanja kritične infrastrukture.

Odgovornost menedžmenta pri nosilcih sektorjev kritične infrastrukture

Po ZoKI je glavni nosilec kritične infrastrukture Ministrstvo za obrambo, ki ima status koordinatorja in usmerjevalca izvajanja nalog nosilcev sektorjev kritične infrastrukture in izvajanja nalog upravljavcev kritične infrastrukture. Ministrstvo je že izdalo Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenje (2019) in Predlog programa usposabljanja upravljavcev kritične infrastrukture (Direktorat za obrambne zadeve 2018). Vendar pa Ministrstvo pristojno za obrambo čaka še obilo nalog za vzpostavitev procesa ocenjevanja tveganj in usklajevanja predlogov načrtov ukrepov za zaščito kritične infrastrukture. Vzporedno s tem bo treba v



sodelovanju z nosilci sektorjev organizirati ustrezno strokovno pomoč posameznim upravljavcem, ter natančno usmeritev za izdelavo načrtov neprekinjenega delovanja. Ministrstvo ima tudi status kontaktnega organa za sodelovanje med pristojnimi organi kritične infrastrukture.

Vlada je s sklepom (št. 80200-1/2018/10, z dne 5. 7. 2018) določila posamezna ministrstva kot nosilce določenih sektorjev kritične infrastrukture. Tako so posamezna ministrstva odgovorna za delovanje, razvoj in zaščito naslednjih sektorjev:

- Ministrstvo za infrastrukturo je nosilec sektorja energetike in sektorja prometa,
- Ministrstvo za kmetijstvo, gozdarstvo in prehrano je nosilec sektorja prehrane,
- Ministrstvo za okolje in prostor je nosilec sektorja preskrbe s pitno vodo,
- Ministrstvo za zdravje je nosilec sektorja zdravstva,
- Ministrstvo za finance je nosilec sektorja financ,
- Ministrstvo za okolje in prostor je nosilec sektorja varovanja okolja,
- Ministrstvo za javno upravo je nosilec sektorja informacijsko-komunikacijskih omrežij in sistemov.

Navedena ministrstva so po zakonu o kritični infrastrukturi dolžna za svoje sektorje izdelati strokovne usmeritve za izdelavo ocen tveganj. Pri tem je treba upoštevati specifičnost dejavnosti sektorjev, stopnjo ranljivosti in ogroženosti, ter specifiko varnostnih in drugih tveganj. Kajti premoženje, procesi in človeški viri v energetiki so podvrženi povsem drugačnim tveganjem kot denimo v sektorju zdravstva ali v sektorju prometa. Iz tega izhaja, da je za nosilce sektorjev priprava strokovnih usmeritev metodološko in vsebinsko zahtevno opravilo. Prav tako bo zahtevno opravilo potrjevanje ocen tveganj, načrtov ukrepov za zaščito, načrtov neprekinjenega delovanja, kriznih načrtov in pregled, ter potrjevanje letnih poročil o izvajanju načrtov neprekinjenega delovanja pri posameznih upravljavcih kritične infrastrukture.

Odgovornost menedžmenta korporativne varnosti pri upravljavcih kritične infrastrukture

Če bodo vodstva in obstoječi menedžment korporativne varnosti pri upravljavcih kritične infrastrukture, od nosilcev sektorjev pravočasno in strokovno usmerjeni v izdelavo in uporabo dokumentov za zaščito kritične infrastrukture, se obeta metodološko enotnejši in vsebinsko ustreznejši pristop k vzpostavljanju procesa stalnega ocenjevanja tveganj, procesa trajnostnega zagotavljanja neprekinjenega poslovanja in stalne skrbi za obvladovanje morebitnih kriznih stanj. Iz tega izhaja, da upravljavci kritične infrastrukture izdelajo ali prenovijo naslednje dokumente:

> Menedžment korporativne varnosti pri upravljavcih kritične infrastrukture je torej tista »prva linija obrambe«, ki ji je po eni strani izkazano izjemno pomembno poslanstvo in zaupanje, po drugi strani pa s tem prevzema izjemno velike odgovornosti, ki se jih v praksi vse premalokrat zaveda.



- varnostno politiko in politiko upravljanja s tveganji,
- oceno (zaznava, analiza in vrednotenje) tveganj, pri čemer si je treba ustvariti bazo podatkov s pomočjo SWOT analize, s pomočjo drugih analiz in študij ter z uporabo standardov upravljanja s tveganji,
- načrt ukrepov za zaščito kritične infrastrukture, ki mu je podlaga ocena tveganj,
- načrt zagotavljanja neprekinjenega poslovanja, pri čemer je možno uporabiti mednarodni standard za tovrstno načrtovanje,
- krizni načrt s scenariji obvladovanja posameznih izrednih dogodkov in/ali kriznih stanj, z načrtom kriznega komuniciranja, ki mu je podlaga ocena ranljivosti in ogroženosti ter ocena tveganj,
- načrt organiziranega varovanja, v skladu s predpisi, ki urejajo zasebno varovanje.

Po Pravilniku o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev (2019), ki se nanaša na informacijsko varnost, pa je treba izdelati analizo obvladovanja tveganj, politiko neprekinjenega poslovanja, načrt varnostnih ukrepov, načrt odzivanja na incidente in druge dokumente.

Osnovna pripomočka za izdelavo ocene tveganj so strokovne usmeritve nosilcev sektorjev kritične infrastrukture, študija Strokovne podlage za oceno tveganj za delovanje kritične infrastrukture, ki jo je izdelal Inštitut za korporativne varnostne študije, ter zakonske in druge podlage. Upravljavce kritične infrastrukture torej čaka kar zahteven proces vzpostavljanja medsektorsko usklajenega sistema ocenjevanja tveganj, načrtovanja ukrepov za zaščito in trajnostnega zagotavljanja neprekinjenega delovanja. Učinkovitost izvajanja nalog upravljavcev kritične infrastrukture bo v veliki meri odvisna od ažurnosti in kakovosti izvajanja nalog nosilcev sektorjev kritične infrastrukture.

Ne glede na navedena dejstva in zakonske obveznosti nosilcev sektorjev pa je končna odgovornost za izdelavo navedenih dokumentov na upravljavcih kritične infrastrukture, torej na menedžmentu korporativne varnosti, ki je pri upravljavcih kritične infrastrukture neposredno zadolžen in odgovoren za vodenje procesa upravljanja tveganj in izvajanje ustreznih ukrepov za zaščito kritične infrastrukture.

Menedžment korporativne varnosti pri upravljavcih kritične infrastrukture je torej tista »prva linija obrambe«, ki ji je po eni strani izkazano izjemno pomembno poslanstvo in zaupanje, po drugi strani pa s tem prevzema izjemno velike odgovornosti, ki se jih v praksi vse premalokrat zaveda. Zaradi navedenega si mora menedžment korporativne varnost pri upravljavcu kritične infrastrukture izboriti ustrezen pravno-formalni, statusni, organizacijski in ekonomski status, ki mu bo zagotavljal optimalne pogoje za delo, neodvisnost vodenja ter suverenost odločanja. V nasprotnem primeru se bo, vede ali nevede, soočal z večjo (morda celo preveliko) stopnjo tveganja, ki izhaja iz neučinkovitega upravljanja tveganj in neustreznega izvajanja ukrepov za zaščito kritične infrastrukture, s tem pa bo bistveno bolj izpostavljen osebni, kazenski, materialni, moralni, družbeni, politični in še kakšni drugi vrsti odgovornosti.

Sklepna beseda

Za upravljanje varnosti kritične infrastrukture, kamor sodi tudi skrb za vzpostavljanje primernega menedžmenta korporativne varnosti, so odgovorni ključni pristojni organi, ki so: Vlada Republike Slovenije, Ministrstvo pristojno za obrambo, nosilci sektorjev kritične infrastrukture (ministrstva), upravljavci kritične infrastrukture, Nacionalni center za krizno upravljanje in Inšpektorat pristojen za obrambo. Ministrstvo pristojno za obrambo kot koordinator in usmerjevalec upravljanja varnosti kritične infrastrukture bi moralo postaviti kriterije in merila za menedžment korporativne varnosti na ravni nosilcev in na ravni upravljavcev kritične infrastrukture. To je v gospodarskih družbah, zavodih in drugih organizacijah, ki upravljajo s kritično infrastrukturo. Kajti le od izobraženih, usposobljenih in s pravimi kompetencami oboroženih menedžerjev korporativne varnosti lahko pričakujemo in zahtevamo celovito pravno in nepravno odgovornost. V tem kontekstu lahko sklenemo misel, da le profesionalni menedžment korporativne varnosti, ki se zaveda svojega poslanstva in odgovornosti suvereno in trajnostno obvladuje nove varnostne izzive in s tem zagotavlja neprekinjeno delovanje in poslovno odpornost, ter obvladuje morebitna krizna stanja v kritični infrastrukturi.

Viri

- Nacionalni program varstva okolja (2018)
- Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, Ur. l. RS, št. 32/2019
- Resolucija o strategiji nacionalne varnosti v Republiki Sloveniji (2010 in 2019)
- Strategija razvoja Slovenije 2030 (2017)
- Strategija kibernetske varnosti (2016)
- Študija Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture. Inštitut za korporativne varnostne študije (2019)
- Zakon o kritični infrastrukturi. Ur. l. RS, št. 75/2017
- Zakon o informacijski varnosti, Ur. l. RS, št. 30/2018
- Zakon o elektronskih komunikacijah, Ur. l. RS, št. 40/2017
- Zakon o poslovni skrivnosti, Ur. l. RS, št. 22/2019 ■

Gasilnik

2 L / 6 L

Bonpet systems

Zanesljivi gasilni sistemi

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

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

Za gašenje požarov tipa A, B in F.



Prednosti:

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

Tehnične karakteristike 2 L

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

Tehnične karakteristike 6 L

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

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

MPA Dresden

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

www.bonpet.si

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



POMEN DOLOČANJA RANLJIVOSTI KRITIČNIH PROCESOV IN TEHNOLOŠKIH DELOV INFRASTRUKTURNIH SISTEMOV

V procesu določanja kritične infrastrukture se vedno znova znajdemo pred generalizacijo odločanja, kaj je v določenih družbenih okoljih res tako kritično, da je to potrebno opredeliti kot kritična infrastruktura. Seveda pa se je potrebno zavedati, da je to samo prvi korak, ki ga moramo v tem procesu izvesti. Lahko celo ocenimo, da je to lažji del tega procesa. Zaradi pomembnosti procesov in postavljenih kriterijev za določitev kritičnosti teh procesov, ki temeljijo na oceni učinkov v primeru odpovedi, relativno hitro pridemo do organizacij, ki v svojem organizacijskem okolju upravljajo s kritično infrastrukturo. Težji del tega procesa, ki je po naši oceni najbolj pomemben, je z ustreznimi metodološkimi postopki priti do tistih specifičnih delov te kritične infrastrukture, ki je dejansko kritična in bi zaradi izpada delovanja nastale posledice ali škodljivi vplivi na organizacijo, ljudi, okolje ali bi vplivale na delovanje drugih soodvisnih procesov ali organizacij.

Poslovanje organizacij je skoraj vedno povezano z omejenimi kadrovskimi, finančnimi, tehničnimi in organizacijskimi viri. To nas sili v stalno prioritizacijo ukrepov na tiste ključne segmente, ki so zaradi svoje vloge, dejansko pomembni v celotni infrastrukturi naše organizacije. Seveda lahko ta proces generalno prenesemo na vse organizacije poslovnega okolja, še posebej tiste, ki pri svojem delovanju uporabljajo tehnološke ali informacijske zmogljivosti, in ga ni mogoče omejiti samo na področje upravljalcev kritične infrastrukture. Za neko industrijsko organizacijo in za neprekinjeno delovanje njenega tehnološko-poslovnega procesa je ravno tako pomembno razumevanje, kaj je dejansko kritičnega v tem procesu, da bo podjetje uspešno delovalo. V tem delu želimo posebej opozoriti, da so nekateri pristopi preveč usmerjeni samo v tehnično opredeljevanje kritičnih delov infrastrukture, in da človeški potencial vedno bolj postaja tista kritična komponenta naših sistemov, ki lahko pomembno vpliva na kvaliteto delovanja teh kritično infrastrukturnih sistemov. Zaradi tega ga moramo nujno vključiti v opredelitev kritičnih procesov, tehnoloških delov ali zmogljivosti. Za to bi predlagali, da v obseg kritičnih dejavnikov razumemo: (1) Kadre, (2) Material (primer: uporabljene ali proizvedene kemikalije), (3) Informacije, (4) Okolje, (5) Opremo, (6) Objekte in (7) Dejavnosti/operacije/procese.

V nadaljevanju pa bi želeli osvetliti pomemben korak, ki zagotavlja vzpostavitev podrobne ocene stanja in prepoznavanja ranljivosti. Le ta lahko pomembno vpliva na omejitev ali prekinitev delovanja naših kritičnih delov infrastrukture ali procesov.

*avtor je član Slovenskega združenja korporativne varnosti

Proces identifikacije in odkrivanja ranljivosti

Proces identifikacije in odkrivanja ranljivosti je logično nadaljevanje procesa, ko so že definirane kritične zmogljivosti za zagotavljanje neprekinjenega delovanja kritične infrastrukture. V nadaljevanju je pomembna izvedba koraka v katerem izvedemo podrobno opredelitev ranljivosti za vsak definiran kritični del te infrastrukture. Preden se osredotočimo na analizo ranljivosti sistema posamezne kritične infrastrukture, si oglejmo nekaj pomembnih konceptualnih opredelitev ranljivosti in njegove umestitve v celovit sistem upravljanja tveganj.

Ranljivost predstavlja vsako šibkost, ki jo lahko izkoristi nasprotnik za dostop do kritičnih delov našega procesa ali organizacije. Ranljivosti lahko vključujejo, vendar niso omejene zgolj na sestavne značilnosti, lastnosti opreme, vedenje osebja, lokacije ljudi, opreme in zgradb, ali operativne in kadrovske prakse.

Koncept ranljivosti opisuje obsežno lastnost infrastrukture ali tehnološkega procesa, kar smo opredelili kot kritično komponento celovitega sistema (npr. tehničnega sistema, njegovega sestavnega dela, človeka itd.). V tem se ocenjuje zmogljivost odpornosti glede na izpostavljenost določenemu tveganju ali kombinaciji tveganj.

Analiza varnostne ranljivosti predstavlja postopek ugotavljanja verjetnosti, da bo nasprotnik uspešno izkoristil ranljivost in posledično stopnjo škode ali vpliva. Ta proces ne temelji na kvantitativni analizi tveganja, temveč se izvaja z uporabo kakovostne analize, kjer je velik vpliv strokovnosti varnostnih strokovnjakov, da so sposobni učinkovite presoje dejavnikov vplivov na proces zagotavljanja varnosti. Določitev tveganja (kvalitativno) je želeni rezultat analize varnostnih ranljivosti, tako da je osnova za razvrstitev tveganj, povezanih z varnostjo, in s tem določitev prednostnih nalog za uporabo protiukrepov.

Postopek identifikacije oz. prepoznavanja ranljivosti lahko razdelimo na naslednje osnovne štiri korake: 1. korak: Prepoznavanje ranljivosti; 2. korak: Ocenjevanje ranljivosti; 3. korak: Obravnava ranljivosti in 4. korak: Poročanje o ranljivosti.

Ranljivosti predstavljajo obsežne značilnosti sredstva, sistema ali omrežja, zasnove, lokacije, varnostno stanje, postopek ali delovanje, zaradi katerih so le ta dovzetna za uničenje, onesposobitev ali izkoriščanje zaradi tehničnih, organizacijskih ali mehanskih okvar, naravnih nevarnosti, terorističnih napadov, ali drugih zlonamernih dejanj. Proces ugotavljanja ranljivosti posebej opredeli šibkosti, ki bi lahko povzročile zaskrbljujoče posledice pri delovanju kritičnih delov, ob upoštevanju notranjih strukturnih pomanjkljivosti, zaščitnih ukrepov in odpornosti. Potrebno se je zavedati, da ranljivost predstavlja tudi šibkost sistema ali sredstva, varnostnih postopkov sistema, notranjih kontrol ali njenega izvajanja, katerega lahko izkoristi določen vir nevarnosti. Večina ranljivosti sistema je lahko povezana z varnostnimi nadzori, ki bodisi niso bili uporabljeni (namerno ali nenamerno), bodisi so bili uporabljeni, vendar ohranijo nekaj pomanjkljivosti. Pomembno pa je tudi, da se pri analizi vključi razumevanje stalnega spreminjanja okolja in poslovnih procesov. Dinamično okolje, ki obdaja naše sisteme, prinaša nove in nove možnosti za pojavljanje novih ranljivosti, ki lahko nastanejo zaradi sprememb v organizaciji in poslovnih procesih, zaradi spremenjenih okoliščin delovanja ali nastopanja na novih poslovnih okoljih, širjenja in uvajanja novih tehnologij in seveda pojavljanja vedno novih groženj in tveganj.

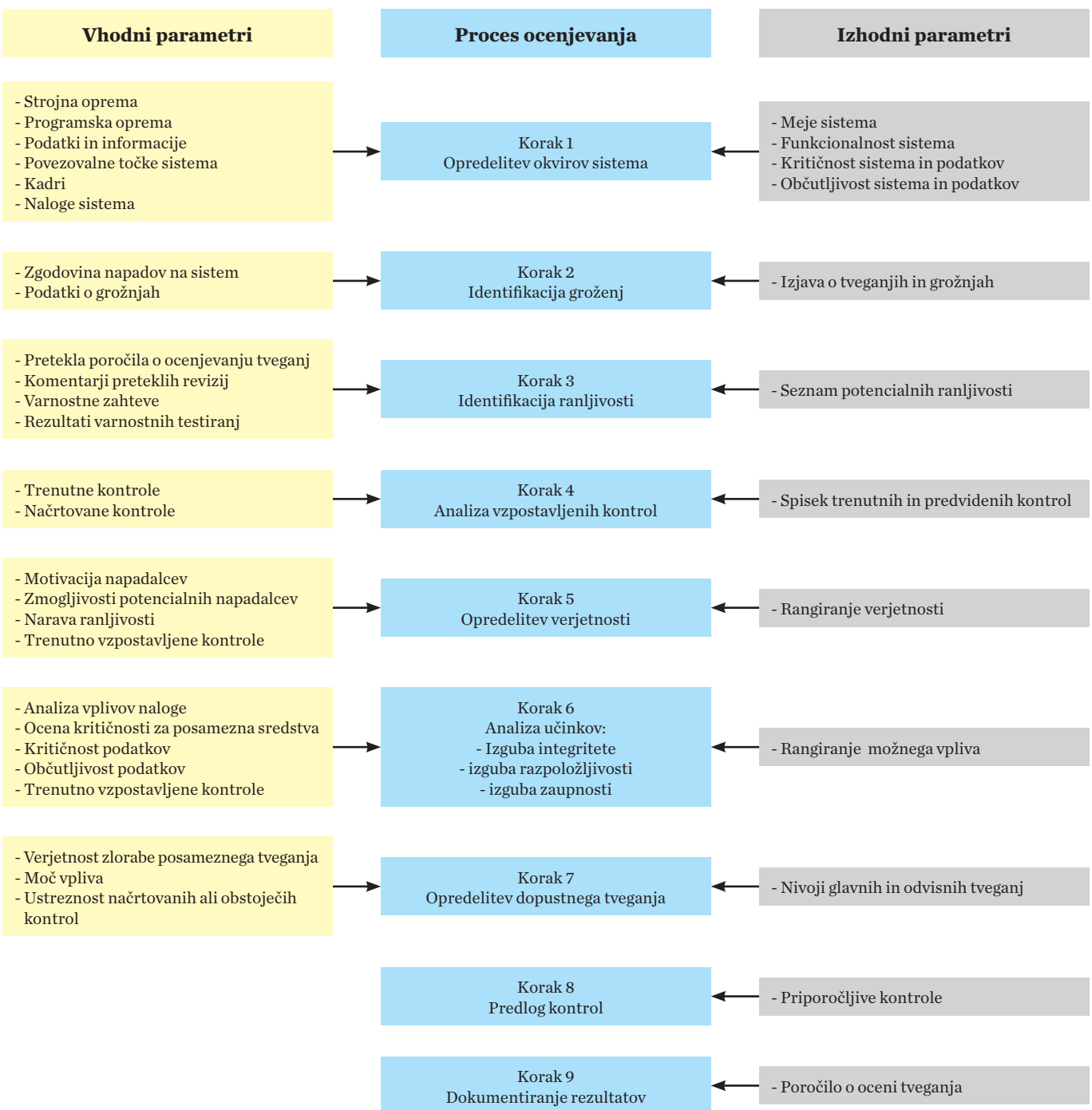
Postopek ocene ranljivosti običajno obsega naslednje ključne korake:
- določitev ustrezne strategije ocenjevanja ranljivosti (npr. samoocena, širša ocena državnih institucij, strokovni pregledi ali neodvisna ocena tretjih oseb);
- določitev metodologije / orodja, primernega za oceno določene vrste sredstva, sistema ali omrežja, ki se obravnava;
- prepoznavanje in razvrščanje ranljivosti z uporabo skupnih scenarijev groženj;
- ugotavljanje odvisnosti in soodvisnosti z drugimi sredstvi in sektorji;



- upoštevanje ranljivosti, povezanih s fizičnimi, kibernetskimi in človeškimi elementi;
- analiza prednosti obstoječih zaščitnih programov; in
- ocena preostalih vrzeli za določitev nerešenih ranljivosti.

Vsak kritično infrastrukturni sistem je sestavljen iz posameznih kritičnih komponent. Kot primer lahko vzamemo elektro-energetsko omrežje v posamezni državi. Dejstvo je, da so samo določeni deli tega sistema res tako kritični, da se ne more zagotoviti nadomestnega obvoda prenosa električne energije oz. bi nedelovanje resno ogrozilo neprekinjenost delovanja tega sistema in seveda posledično vplivalo tudi na vse ostale podsisteme, ki so neposredno odvisni od neprekinjene dobave električne energije. Vsako komponento je treba analizirati z vidika možnih tveganj in varnostnih vidikov. Komponente, namenjene delovanju v varnostno kritičnih okoljih, so običajno zasnovane tako, da naj bi delovale varno. Vendar lahko napadalci izkoristijo varnostne ranljivosti in tako obidejo varnostne mehanizme ter povzročijo omejeno ali obširnejše nedelovanje teh kritičnih delov in s tem posledično tudi celotne infrastrukture. Če to pogledamo v okviru, da vedno več kritične infrastrukture temelji na podpornem delovanju informacijsko-komunikacijskih sistemov, ki so med seboj v določenih okvirih mrežnih povezav, lahko z gotovostjo ugotovimo, da bo temu segmentu, poleg neprekinjenosti delovanja elektro-energetskega sektorja, v prihodnosti posvečeno vedno več pozornosti.

Posamezne pomembne dele kritične infrastrukture je mogoče zaščititi z izvajanjem celovitih ukrepov za zagotavljanje neprekinjenosti njenega delovanja. Proces ocenjevanja ranljivosti pa predstavlja izredno pomemben korak tega procesa,



Shema 1 - Proces podrobnih korakov ocenjevanja tveganj



saj ta analiza predstavlja pomembno osnovo za izdelavo načrtov za preprečevanje groženj in ranljivosti. Seveda pa je vloga načrtovanih aktivnosti za obvladovanje tveganj in groženj usmerjena v odpravo ali vsaj učinkovito obvladovanje le teh. V tem okviru ima odpravljanje ranljivosti pomembno mesto.

V nadaljevanju bomo na celotnem procesu ocenjevanja tveganj (shema -1) pogledali umestitev analize ranljivosti in njeno vlogo v celotnem sistemu.

Zaključek

Za konec si oglejmo nekaj najbolj izpostavljenih ranljivosti, ki jih skozi različne procese ugotavljamo v organizacijah kritične infrastrukture. Ugotovitve, ki jih zaznavamo v nacionalnem okolju so vsekakor primerljive z mednarodnimi trendi, kar smo lahko potrdili skozi analize, ki so bile narejene v okviru mednarodnega projekta INFRASTRESS[1], katerega del je tudi ICS-Ljubljana. Generalno bi lahko najpomembnejše ranljivosti opredelili v naslednja področja:

- Pomanjkljivosti v pripravi ali izvajanju določenih varnostnih politik in postopkov. Na to ima pomemben vpliv nizka varnostna ozaveščenost strateškega vodstva organizacij.
- Človeški dejavniki – tako zaposlenih v organizacijah, kakor tudi zunanjih izvajalcev, ki so vključeni v procese zagotavljanja delovanja kritične infrastrukture (npr. nizka stopnja varnostne kulture, odsotnost ustreznih varnostnih kompetenc itd).
- Organizacijske pomanjkljivosti, še posebej pomanjkanje nadzornih ukrepov in drugih mehanizmov nadzora.
- Merila za načrtovanje in določanje lokacije, ki so bila upoštevana pri prvotni gradnji kritično-infrastrukturnih objektov so se zaradi spremenjenih vplivov varnostnega in družbenega okolja močno spremenila (npr. spremenjeni gradbeni standardi (potresna odpornost), pogostejši hudi naravni pojavi (npr. poplave, ekstremne temperature zaradi globalnega segrevanja), nova izpostavljenost / pomen nasilnih dejanj nekaterih družbenih skupin, npr. terorizma).
- Vedno večja odvisnost kritične infrastrukture od delovanja različnih ITK sistemov, ki sami po sebi prinašajo pomembne ranljivosti v svoji zasnovi.
- Premalo razumevanja pomena in vloge javno-zasebnih partnerskih procesov v postopkih povezanih z zagotavljanjem varnosti.

[1] Improving resilience of sensitive industrial plants & infrastructures exposed to cyberphysical threats, by means of an open testbed stress-testing system – INFRASTRESS, number: 833088 — H2020-SU-INFRA-2018-2019-2020/H2020-SU-INFRA-2018; www.infrastress.eu ■

100-ODSTOTNO PRIPRAVLJENI

Hiter odziv je najboljša obramba pred poslovno škodo.

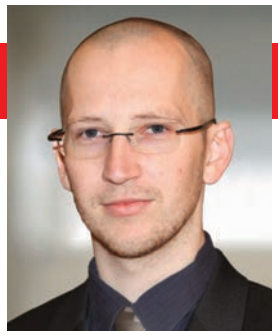
NIL-OV VARNOSTNO OPERATIVNI CENTER



NIL

nil.com

Avtor: mag. Matjaž Drev / Slovensko združenje korporativne varnosti*



ZASEBNOST NA INTERNETU STVARI?

V začetku devetdesetih let so bili nekateri sociologi prepričani, da je internet zaradi svoje razpršenosti in odprtosti odporen proti izvajanju nadzora s strani države ali korporacij (Boyle 1997). Vendar je to veljalo samo na začetku, ko internet še ni bil močno razširjen, zato je za države predstavljal nekaj novega in neobvladljivega.

Z množično rabo se je to spremenilo. Internet je poleg številnih storitev, ki jih omogoča, postal tudi platforma družbenega nadzora, saj se praviloma vsako početje, ki ga izvajamo, zabeleži v obliki elektronskih sledi. Vse večje število medijsko razvpitih primerov (spomnimo samo na Snowdenova razkritja množičnega nadzora telekomunikacij s strani ameriških obveščevalnih služb) kaže, da nadzor uporabnikov na internetu ni izjema, ampak pravilo.



Sicer pa tak nadzor ne temelji več zgolj na spremljanju posameznikov, ki obiskujejo spletne strani, pač pa vse bolj na zbiranju podatkov iz različnih »pametnih naprav«, ki so povezane v internet. Izkazalo se je, da internet kot največje svetovno omrežje ni uporaben le kot platforma za povezovanje strežnikov, odjemalcev in pripadajoče mrežne opreme, ampak tudi najrazličnejših predmetov, ki jih je mogoče posredno ali neposredno prek TCP/IP komunikacijskega protokola povezati v internet. Tako se v vse večjem obsegu z uporabo komunikacijskih tehnologij kot so Wi-fi, Bluetooth, NFC, ZigBee in RFID, v internet povezuje najrazličnejše predmete: GPS naprave, pametne zapestnice, ki zbirajo podatke o posameznikovem zdravju, počutju in telesni aktivnosti, senzorje, ki pridobivajo podatke iz okolja, gospodinjske aparate, sisteme za ogrevanje, industrijske stroje, kmetijske pripomočke, izdelke v trgovinah, igrače, videokamere, osebne pomočnike oziroma katerekoli druge naprave, ki jih je mogoče nadgraditi s prej navedenimi komunikacijskimi tehnologijami in jih tako vpeti v internet. Proces povezovanja predmetov v internet je leta 1999 Kevin Ashton poimenoval »internet stvari«, vendar pa se je izraz začel množično uporabljati šele po letu 2010, ko je tržišče preplavil val predmetov, ki jih je bilo mogoče povezati v internet in na ta način omogočiti komunikacijo med napravami oziroma med napravami in uporabniki (Mattern in Floerkemeier 2016).

Internet je poleg številnih storitev, ki jih omogoča, postal tudi platforma družbenega nadzora, saj se praviloma vsako početje, ki ga izvajamo, zabeleži v obliki elektronskih sledi.

*avtor je član Slovenskega združenja korporativne varnosti

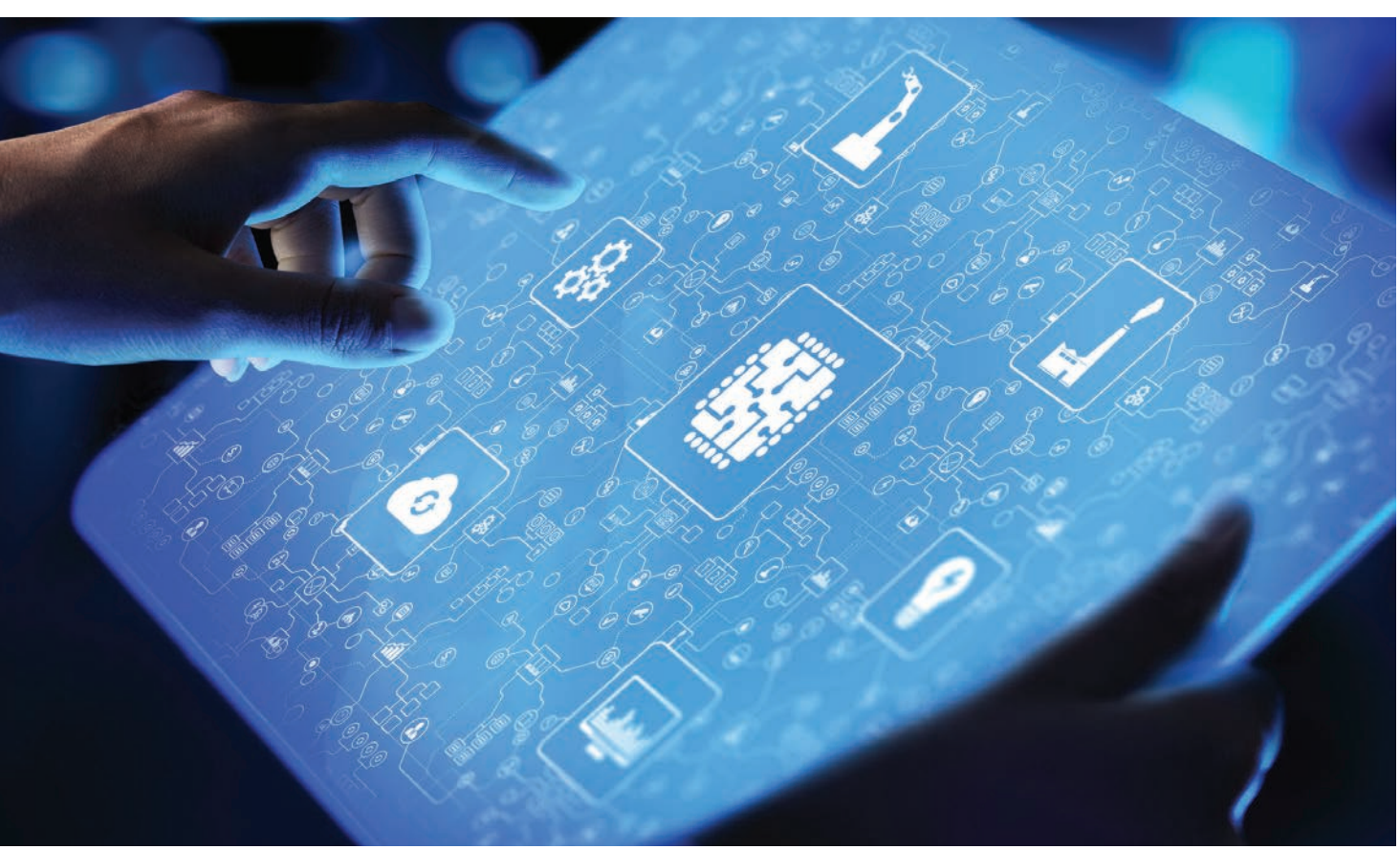
Sicer pa tak nadzor ne temelji več zgolj na spremljanju posameznikov, ki obiskujejo spletne strani, pač pa vse bolj na zbiranju podatkov iz različnih »pametnih naprav«, ki so povezane v internet.

V okviru povezovanja predmetov prek interneta se je kot zelo uporabna izkazala tehnologija radiofrekvenčne identifikacije (RFID), ki deluje na način, da se majhne elektronske etikete namesti na predmet, nato pa se s pomočjo radijskih valov sledi lokaciji označenega predmeta. RFID tehnologija se je zaradi nizke cene in preproste uporabe uveljavila predvsem v logistiki in v trgovinah, saj omogoča enostavno označevanje in spremljanje lokacije izdelkov. Vendar pa se raba RFID tehnologije širi še na druga področja, npr. ugotavljanje identitete s pomočjo dokumentov, ki so opremljeni z RFID etiketami, ali celo spremljanje posameznikov s pomočjo podkožnih RFID vsadkov (Murakami Wood 2006, 25).

V zadnjih letih se je ideja interneta stvari uresničila predvsem skozi vse bolj množično uporabo poceni »pametnih« telefonov, zapestnic, ur, nakita in drugih pripomočkov, ki jih nosimo. Te naprave s pomočjo različnih senzorjev pridobivajo podatke ne le o naši natančni lokaciji, pač pa tudi o našem zdravstvenem stanju, spalnih navadah in (ne)aktivnem načinu življenja. Pametne naprave se večinoma povezujejo prek Bluetooth tehnologije z računalniki oziroma pametnimi telefoni, vzporedno pa prek Wi-fi tehnologije še z internetom. Ob tem velja dodati, da so pogoji uporabe naprav takšni, da nas silijo k deljenju podatkov ne le s ponudniki programske opreme, ki poganja pametne naprave, pač pa tudi s proizvajalci teh naprav. Del zasebnosti je (vsaj v teoriji) mogoče ohraniti z ustreznimi nastavitvami, vendar se v to številni uporabniki ne poglobijo, hkrati pa ni mogoče zanesljivo vedeti ali nastavitve v zvezi z (ne)deljenjem osebnih podatkov dejansko delujejo ali gre zgolj za ustvarjanje iluzije zasebnosti.

Prav poseben izziv zasebnosti v tem kontekstu predstavljajo interaktivne »pametne« naprave kot so »pametni« televizorji, igrače in osebni pomočniki (Amazonova Alexa, Applova Siri in Googlov Asistent). Naštete vrste naprav v okviru osnovnega delovanja izvajajo nenehno obdelavo pogosto zelo občutljivih osebnih podatkov, ki jih pridobivajo tako s spremljanjem načina naše uporabe posamezne naprave, pa tudi z avdio in video snemanjem, kar pomeni, da pametni televizorji in osebni pomočniki podobno kot Telekrani iz distopičnega Orwellovega romana 1984 vse bolj množično vstopajo v intimo bivališč in »velikim bratom« korporacij omogočajo izvajanje množičnega nadzora nad našim vedenjem v realnem času. S tem, ko se število pametnih naprav, ki o nas zbirajo osebne podatke in na podlagi analize teh podatkov sestavljajo vedenjske profile, kar omogoča bolj natančno predvidevanje vedenja posameznikov in posledično učinkovitejše oglaševanje, množi in ko, pametne naprave zaradi medsebojne povezljivosti spodbujajo deljenje podatkov, se ustvarja nov tip ambientalnega nadzora, ki se mu bo čedalje težje izogibati. Hibridni svet interneta stvari, ki povezuje fizično in virtualno realnost, se zato zdi vse bolj podoben panoptičnemu idealu v katerem se razsežnosti pogleda, arhitekture in elektronskih sledi združujejo v novo obliko izpopolnjenega družbenega nadzora.

Ob tem se zastavi vprašanje ali je zasebnost na internetu (stvari) sploh mogoče varovati. Odgovor je v veliki meri odvisen od tega kako široko razumemo





zasebnost. Če jo razumemo zgolj kot seznanitev s tem, kaj naj bi se z našimi osebnimi podatki dogajalo in kako lahko uveljavljamo pravice, ki nam po zakonu pripadajo, potem se lahko brez slabe vesti prepričamo, da smo kot družba dobro zavarovali zasebnosti. Če pa zavzamemo širšo perspektivo in kot zasebnost razumemo predvsem nadzor nad tem kaj se dejansko dogaja z našimi osebnimi podatki, ko uporabljamo v internet povezane »pametne« naprave, je odgovor nikalen – kaj se s podatki dejansko dogaja verjetno vedo zelo redki, če sploh kdo. Toda v tem je svojevrsten paradoks. Internet stvari po eni strani zasebnost krči, po drugi strani pa spodbuja inovativnost na področju razvoja pametnih naprav, ki bodo, vsaj v okviru specifične tržne niše, kot svojo konkurenčno prednost ponudile prav skrb za varnost in (vgrajeno ter privzeto) zasebnost.

Del zasebnosti je (vsaj v teoriji) mogoče ohraniti z ustreznimi nastavitvami, vendar se v to številni uporabniki ne poglobijo, hkrati pa ni mogoče zanesljivo vedeti ali nastavitve v zvezi z (ne)deljenjem osebnih podatkov dejansko delujejo ali gre zgolj za ustvarjanje iluzije zasebnosti.

Viri

Boyle, J. (1997). Foucault in Cyberspace: Surveillance, Sovereignity and Hardwired Censors. University of Cincinnati Law Review 66(1), str. 177-205.

Mattern, F., Floerkemeier, C. (2010). From the Internet of Computer to the Internet of Things. Informatik-Spektrum. 33 (2): str. 107–121.

Murakami, W. D. (ur.) (2006). A Report on the Surveillance Society.

Orwell, G. (2004). 1984. Ljubljana: Mladinska knjiga. ■



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

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

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

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

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

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

C|EH™ Certified Ethical Hacker

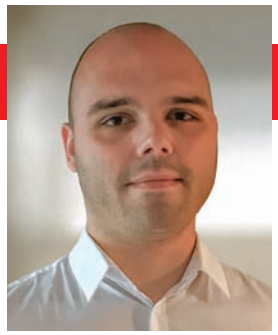
OFFENSIVE SECURITY OSCP

BUREAU VERITAS 1828

DPO

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

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



KIBERNETSKA VARNOST V KRITIČNI INFRASTRUKTURI

Kibernetska varnost zadeva vse sektorje. Kljub temu pa se kritične infrastrukture soočajo z velikim izzivom na področju kibernetske varnosti. Digitalna preobrazba med drugim zahteva večjo zaščito kibernetske varnosti za kritično infrastrukturo, z drugimi besedami, vsa infrastruktura, katere sistemi, viri in storitve so temeljni za razvoj družbe, in ki zagotavljajo kontinuiteto pri normalnem delovanju storitev, katere predstavljata država in javna uprava.

Medtem, ko se na eni strani digitalni svet čedalje bolj povezuje, na drugi strani to lastnikom in upravljalcem kritičnih infrastruktur predstavlja vedno večji izziv pred vedno bolj sofisticiranimi in razvijajočimi se kibernetskimi grožnjami. Raziskovalci odkrivajo nove ranljivosti povezane z varnostjo, ki vplivajo na bistvene dele kritične infrastrukture. Kot na primer na delovanje zaščite pred poplavami, zaznavanje radioaktivnega sevanja, prenos električne energije idr. Izmed vseh odkritih ranljivosti se jih kar nekaj šteje za kritične, kar pomeni, da bi kibernetski napad na te sisteme močno vplival na delovanje kritične infrastrukture in posledično na vse nas.

Znani kibernetski napadi v kritični infrastrukturi

Izpostavimo lahko primer, ki se je zgodil v Ukrajini leta 2015, ko je bilo njihovo električno omrežje (več kot 30 elektrarn v državi) tarča kibernetskega napada. V urah, ki so sledile po napadu, je skoraj četrt milijona ljudi na tistem območju ostalo brez električne energije. Podoben primer se je zgodil prav tako v Ukrajini, leta 2016. Napad je bil opredeljen kot primer lažnega predstavljanja (tehnika socialnega inženiringa), s katero se je širila zlonamerna programska koda, ki je posledično povzročila izpadanje.

Prav tako lahko omenimo kibernetski napad, ki se je zgodil leta 2017, ko so kibernetski teroristi prevzeli dobro poznano petrokemično delovno postajo v Savdski Arabiji, z zlonamerno programsko opremo imenovano Triton ali Trisis. Ta je bila posebno nastavljena za industrijske nadzorne sisteme imenovane tudi operativna tehnologija. Kritična točka je bila v varnostnem krmilniku Triconex francoskega podjetja Schneider Electric. V najslabšem primeru bi napadalci lahko povzročili sproščanje strupenega vodikovega sulfidnega plina ali povzročili eksplozije, kar bi ogrozilo življenje tako v objektu, kot v okolici.

Leta 2017 se je ponovno zgodil napad v Ukrajini, tokrat na finančno, transportno, energetsko in drugo kritično infrastrukturo. Država je bila zopet ohromljena. Letališča niso prikazovala informacij o poletih, na podzemni železnici niso delovali avtomati, ni bilo moč izmeriti černobilskega sevanja in med drugim je bila napadena tudi Centralna banka Ukrajine.

V istem letu je bilo Britansko zdravstvo izpostavljeno kripto virusu, znanemu pod imenom WannaCry. To je najbolj poznana zlonamerna programska koda. Paralizirala je delovanje 16-tih bolnišnic v Veliki Britaniji in tako omejila dostop do zdravstvenih datotek njihovih pacientov.

V letu 2019 lahko izpostavimo zlonamerno programsko kodo imenovano Machete, ki je bila odkrita že leta 2010, vendar se od takrat ni prenehala širiti. Ta koda je namenjena kraji podatkov latinskoameriške vojske iz njenih čet. Po mnenju strokovnjakov se je virus razširil z lažnim predstavljanjem, po 9 letih življenja je še vedno živ in še naprej okužuje opremo latinskoameriške vlade.

Število in resnost kibernetskih učinkov še naprej eksponentno rasteta v čedalje bolj povezanem digitalnem svetu.

Vse naprave povezane v omrežje predstavljajo potencialna zadnja vrata in vstopno točko, ki bi jo lahko hekerji zlorabili in tako pridobili dostop do omrežja in različnih sistemov, na katere je povezana.

Na žalost zgodbe podobne tem le redko dosežejo širšo javnost. Kot rezultat se to pokaže v premajhnem pritisku s strani javnosti na vidik kibernetske varnosti in v podcenjevanju potrebe po operaterjih kibernetske varnosti.

Število in resnost kibernetskih učinkov še naprej eksponentno rasteta v čedalje bolj povezanem digitalnem svetu. Po zadnjih ocenah raziskovalnega podjetja Gartner bo do leta 2020 približno 20,4 milijarde naprav povezanih v internet in približno 37 odstotkov teh ne bo v lasti potrošnikov. To nam da misliti koliko teh bo namenjenih upravljanju in nadzorovanju kritične infrastrukture. Te naprave so nam pripeljale boljšo uspešnost in učinkovitost, polega tega pa so razkrile pred tem nedosegljive sisteme kritične infrastrukture kibernetskim napadom, s strani zlonamernih posameznikov ali skupin z različnimi motivacijami in skupnim ciljem.

Katere so najpogostejše težave v zvezi s kibernetsko varnostjo s katero se soočajo kritične infrastrukture?

Kibernetska varnost se v veliki meri opira na notranje in zunanje dejavnike. Zagotavljanje kakovosti in neprekinjenosti storitev ter izpolnjevanje zakonsko določenih predpisov, sili kritično infrastrukturo, da ponovno preuči svojo strategijo kibernetske varnosti. Potrebno je poskrbeti za sisteme, ki so zastareli ali nimajo ažurne varnostne komponente. Prav tako je potrebno poskrbeti za zastarelo strojno opremo in varnostne vrzeli pri njihovi zasnovi. Zaradi povečanja števila priključenih naprav v omrežje tudi to predstavlja velik izziv. Na eni strani vedno večje število kibernetskih napadov, ki nas na drugi strani silijo k iskanju talentiranih sodelavcev, ki znajo razmišljati kot hekerji.

Omrežje je najprimernejša vstopna točka za kibernetske kriminalce, ki želijo izvesti napad v kritični infrastrukturi. Za izvedbo kibernetskega napada se iščejo načini za vstop preko omrežja. Običajno to storijo z dvema tehnikama; Prva se opira na iskanje ranljivosti v opremi in sistemih, ali na namestitev neke vrste zlonamerne programske kode, da bi pridobili nadzor nad kritično infrastrukturo. Pomembno se je zavedati, da večina organizacij ne ve, da so bile okužene z zlonamerno programsko kodo. To, da ostaja dlje časa okuženo z zlonamerno kodo, predstavlja eno večjih tveganj.



Lastniki, načrtovalci, gradbeniki in finančniki rutinsko usmerjajo veliko virov za zmanjšanje številnih tveganj za kritično infrastrukturo. Kljub temu le redko vložijo toliko pozornosti v predvidevanje morebitnih incidentov kibernetske varnosti. Verjetno obstaja kar nekaj razlogov za pomanjkanje pozornosti do kibernetske varnosti. Tako kot morajo arhitekti upoštevati fizično odpornost in varnost infrastrukturnih sredstev, morajo upravljalci integrirati kibernetsko varnost. Eden od načinov za zagotovitev tega je, da postane kibernetska odpornost sestavni del procesa dizajniranja. Upravljalci kritične infrastrukture bi morali razmisliti o vzpostavitvi jedrne funkcionalnosti, ki je odporna na kibernetske napade ali omogoča, da se lažje prepreči vpliv kibernetskega napada.

Nekateri deli kritične infrastrukture imajo na primer digitalno nadzorovane sisteme za klimatske naprave, vključujoč z vsemi zračniki in okni. Če obstaja možnost obvoda in ročnega posega v delovanje teh krmilnikov, lahko pripomoremo in omogočimo nadaljevanje operacij v primeru kibernetskega napada. V kolikor pa tega nimamo, lahko to predstavlja velik izziv, ko pride do kibernetskega napada, če bi nam na primer nekdo zaprl okna sredi vročega poletnega dne in ugasnil klimatsko napravo oz. jo nastavil na način ogrevanja v strežniški sobi.

Vse naprave povezane v omrežje predstavljajo potencialna zadnja vrata in vstopno točko, ki bi jo lahko hekerji zlorabili in tako pridobili dostop do omrežja in različnih sistemov, na katere je povezana. Zato bi morala biti, kot dokazujejo odmevni kibernetski napadi, za katere se zdi, da se pojavljajo vedno bolj pogosto, kibernetska varnost glavna prioriteta za vse.

Na žalost so vse omrežne naprave in sistemi lahko ranljivi. V našem povezanem svetu pa je kibernetska varnost omrežja le tako močna kot najšibkejša naprava, ki je nanj povezana. Če se te naprave uporabljajo v okolju z visokim tveganjem, kot je kritična infrastruktura, bi bile posledice napada daljnosežnejše s potencialom, da sesujejo veliko več, kot le neko postajo ali drugo zgradbo. Zato je nujno, da omrežne naprave v svojih aplikacijah in konfiguracijah zagotavljajo raven varnosti, ki je potrebna za zaščito celotnega sistema pred potencialno katastrofalnimi učinki napada. Morebitni izpad omrežja na kritičnem infrastrukturnem objektu ali lokaciji je lahko katastrofalen, posledice pa bi se lahko čutile na več segmentih in bi se dotaknile vseh nas.



Pomembna so tudi redna testiranja obstoječih varnostnih kontrol in potrditve, da delujejo kot morajo in če ne, kaj je potrebno storiti, da zadevo spravimo pod nadzor.

Kar se tiče naprav in omrežij, ki se uporabljajo v kritični infrastrukturi, je eden največjih dejavnikov nakup opreme od podjetij, ki se zavzemajo, da bodo zagotavljala najvišjo raven varnosti, in da to v resnici tudi imajo. Najbolj pomembno pri zavarovanju omrežij in naprav je implementacija in uporaba močnih varnostnih politik in postopkov z namenom zmanjšanja verjetnosti, da bi človeška napaka oslabila močno grajeno varnost.

Tudi sektor se razvija z nastankom pametnih mrež povezanih z drugimi sistemi, kot so SCADA, IoT, itd. Zahtevajo večji nadzor varnosti, saj so vstopna točka za kibernetske kriminalce. Kombinacija IT, OT in IoT so vrata hekerjem. Zaradi tega so nujno potrebne učinkovite strategije za zaščito pametnih mrež pred kibernetskimi napadi.

Učinkovita kibernetska varnost pomeni stalno ocenjevanje tveganj in sprejemanje ustreznih ukrepov za ublažitev teh groženj. Gre za delo s pravimi ljudmi, uporabo pravih izdelkov, izkoriščanje ustrezne tehnologije in izvajanje, ter spoštovanje politik in procesov. Pomembna so tudi redna testiranja obstoječih varnostnih kontrol in potrditve, da delujejo kot morajo in če ne, kaj je potrebno storiti, da zadevo spravimo pod nadzor. Če to upoštevamo in se predvsem osredotočimo na kibernetsko varnost, smo lahko veliko boljši pri določanju in zaščiti kritičnih delov kritične infrastrukture. ■

Avtor: Vladimir Ban / Vodilni ekspert za implementacijo ICT rešitev, A1 Slovenija, d.d.*



UMETNA INTELIGENCA JE LAHKO VAŠ NAJBOLJŠI PRIJATELJ

Varnost informacijskih sistemov še nikoli ni bila tako aktualna in pomembna tema, kot je to danes. Napadi na informacijske sisteme so postali vsakdanjost. Ti napadi se ne dogajajo več zgolj na drugem koncu sveta, ampak se vedno bolj dogajajo tudi v našem okolju. Prepričan sem, da je marsikateri bralec tega članka tudi že sam občutil nevarnosti, ki jih sodobne grožnje prinašajo.

Razvoj varnostnih sistemov je zelo dinamičen. Pomemben del razvoja je v zadnjem času povezan z umetno inteligenco, ki na velika vrata trka tudi na to področje.

Okoli umetne inteligence se nam seveda poraja ogromno vprašanj. Kako sploh deluje? Je uporaba zanesljiva? Se moramo bati Skynet efekta?... Na marsikatera vprašanja odgovarja razširjen prispevek, ki je objavljen na naslovu: http://bit.ly/2oSLZuI (*to je naš white paper*). V tem članku pa si bomo odgovorili na vprašanje, kako nam umetna inteligenca pri zagotavljanju varnosti sploh lahko pomaga.

Umetna inteligenca na področje varnosti prinaša dve veliki prednosti. Prva je zmožnost hitre, natančne in učinkovite analitike velikega števila podatkov in identifikacije odstopanj v tej množici podatkov. Druga prednost pa je zmožnost »učenja«. Algoritme umetne inteligence lahko namreč zelo dobro naučimo kako v množici podatkov razpoznati neke vzorce.

Umetna inteligenca na področje varnosti prinaša dve veliki prednosti. Prva je zmožnost hitre, natančne in učinkovite analitike velikega števila podatkov in identifikacije odstopanj v tej množici podatkov. Druga prednost pa je zmožnost »učenja«. Algoritme umetne inteligence lahko namreč zelo dobro naučimo kako v množici podatkov razpoznati neke vzorce.

Če sedaj ti dve prednosti preslikamo v sodobne izzive varnosti, lahko takoj najdemo razloge zakaj nam umetna inteligenca pri tem lahko pomaga. Pri zagotavljanju varnosti se namreč srečujemo z naslednjimi izzivi:

- Napadi so vedno bolj in bolj povezani s t.i. Zero-day napadi. To so napadi, ki v določeni fazi uporabijo nekaj, kar do sedaj ni uporabil še nihče. Približno lahko predvidimo potek napada, ne moremo pa točno v naprej poznati vseh podrobnosti pričakovanih napadov.
- Pri spremljanju dogajanja se neizbežno srečujemo z ogromno količino podatkov v katerih je težko identificirati sporne dogodke
- Nenazadnje je pomembno, da varnost in nadzor delujeta 24/7, kar močno omeji in minimizira zmožnost »ročnih« procesov in vpliva človeške inteligence.

Poglejmo si uporabo sistemov umetne inteligence na konkretnih primerih:

Varovanje elektronske pošte

Preko zlonamernih elektronskih sporočil napadalci želijo uporabnikom ukrasti gesla, jih prepričati, da obiščejo zlonamerne spletne strani in/ali da si namestijo zlonamerno kodo. Praktično je vsak vdor v omrežje, o katerem slišimo danes, povezan z uporabo takšnih metod. Klasični varnostni sistemi so proti tovrstnim napadom dokaj nemočni. Takšni sistemi nas sicer lahko učinkovito zaščitijo pred različno spam e-pošto, težko pa nas zaščitijo pred tistimi najbolj naprednimi in usmerjenimi phishing e-mail napadi.

Vade Secure je primer sistema za zaščito elektronske pošte, ki bazira na algoritmih umetne inteligence. Takšni sistemi

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

niso odvisni zgolj od statičnih filtrov, ampak pri zaznavanju zlonamernosti uspešno uporabljajo sodobne algoritme.

Algoritmi umetne inteligence lahko bistveno bolj učinkovito zaznajo usmerjeno zlonamerno pošto. Namreč Vade Secure sistem spremlja vso vhodno pošto in si pri tem beleži cel kup podatkov. S tem spoznava katera e-pošta je v določenem okolju pričakovana, katera pa ne. Na ta način lahko sistem zelo učinkovito opazi elektronsko pošto, ki je na eni strani nepričakovana – nova. Na drugi strani pa z analizo različnih podatkov išče v elektronski pošti sledi zlonamernosti. Če je elektronska pošta nepričakovana, hkrati pa vsebuje sledi zlonamernosti, je to dober kandidat za filter.

Primer elektronske pošte, ki jo klasični varnostni mehanizmi niso zaznali kot zlonamerno, Vade Secure pa jo je na osnovi dejstva, da pošta na eni strani kaže znake zlonamernosti, na drugi strani pa ima pošiljatelj sumljivo enak ime kot ga ima eden izmed notranjih uporabnikov

Testi so pokazali, da je zelo težko pripraviti zlonamerno pošto, ki jo tak sistem ne bi zaznal.

Identifikacija skrite komunikacije med zlonamerno kodo v omrežju in napadalci

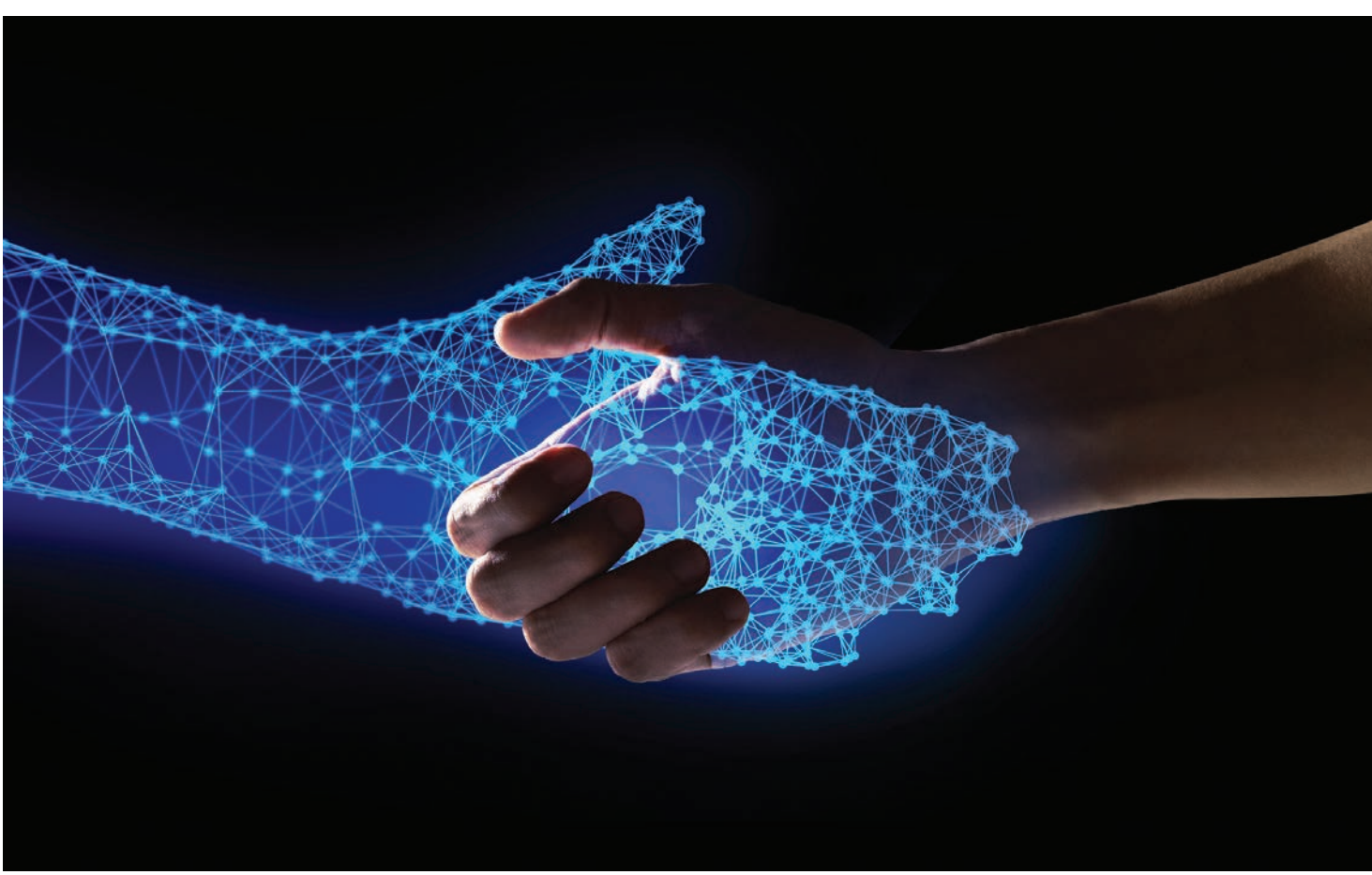
Predpostavimo, da ne uporabljamo Vade Secure sistema in je napadalec uspel prepričati uporabnika, da zažene napadalčevo zlonamerno kodo. V tej točki se sicer lahko zlonamerna koda nato samostojno izvaja, a pri sodobnih napadih je za napadalca ključno, da ta koda vzpostavi stik z njim, s čimer jo napadalec lahko usmerja, ji daje navodila in napad naredi bistveno bolj uspešen.

Pomemben del varovanja okolij je torej biti pozoren na takšne povezave in jih pravočasno preprečiti. To pa ni enostavno. Te povezave so lahko zelo raznolike. Različne so lahko po času, po tipu in po vsebini. Napadalci tu praviloma izkoriščajo klasične načine povezav, ki jih v podjetjih uporabljamo na veliko. Primer je povezava z izhodnim SSL protokolom. V množici vseh izhodnih povezav, ki jih uporabniki vsak trenutek naredijo v Internet omrežje, se takšna zlonamerna povezava hitro lahko »skrije«.

Klasični varnostni sistemi imajo tu velik problem. Če ti nimajo dovolj globokega videnja dogajanj, bodo te povezave za te sisteme neopažene. Če pa uvedemo sistem z dovolj globokim videnjem dogajanj, pa takoj naletimo na ogromno množico lažnih in nepomembnih alarmov.

Uporaba umetne inteligence je tu bistveno bolj učinkovita. **Vectra Cognito** je primer varnostnega sistema, ki tovrstne izzive naslavlja z uporabo tovrstnih algoritmov. Ti algoritmi omogočajo sistemu, da najprej v množici izhodnih povezav učinkovito identificira tiste, ki v statističnem smislu izstopajo (recimo se pojavljajo prvič ali kaj podobnega). Na drugi strani pa ti algoritmi učinkovito identificirajo tiste povezave, ki nosijo znake zlonamernosti. Pri tem se ne naslanjajo na statične metode, kot je recimo reputacija destinacije, ampak predvsem na izgled in potem izhodne komunikacije.

Primer uspešne zaznave skritega HTTPS tunela med zlonamerno kodo in napadalcem. Hkrati je Vectra Cognito varnostni sistem ta tunel uspešno povezal z ostalimi dogodki v omrežju, s čimer je slika grožnje še bolj jasna.





Umetna inteligenca torej neizbežno prihaja. Marsikdo bi rekel, da je že tukaj. Na področju varnosti informacijskih sistemov, tovrstni sodobni sistemi niso del težave, ampak so del rešitve.

Identifikacija zlonamernih aktivnosti na delovni postaji

Predpostavimo, da v dani situaciji Vade Secure in Vectra Cognito sistema nismo uporabili, in je napadalec uspel na delovno postajo namestiti zlonamerno kodo, ki uspešno komunicira z napadalcem. Kljub temu, da je na nek način napad v tej točki že uspel, zadeva še ni čisto dokončana. Namreč, če je okolje žrtve vsaj približno urejeno tako kot bi moralo biti, napadalec še ne more kar tako dokončati svojega dela. Res je prevzel kontrolo nad eno izmed delovnih postaj v omrežju, vendar še vedno nima ustreznih pravic, da bi prišel do tistih pravih podatkov, ali pa da bi zlonamerno zakriptiral tiste najbolj pomembne strežnike.

V tej točki mora napadalec ustrezne pravice še pridobiti. Eden izmed načinov je z eskalacijo pravic na delovni postaji. Tu tipično pridejo na vrsto razni triki, kako na delovnih postajah izvedemo takšno ali drugačno aktivnost, ki bo izkoristila neko ranljivost operacijskega sistema ali programske opreme, ki je nameščena. Možnosti za napadalca je veliko, hkrati pa je vsaj teoretičnih možnosti za skrbnike, da napadalca zaznajo tudi veliko. Vse te aktivnosti napadalca namreč na delovnih postajah puščajo sledi. Tam se sprožajo nenavadni servisi, dogajajo se nenavadne aktivnosti, ipd.

Klasični varnostni sistemi za preprečevanje napadov tej točki niso uspešni. Preveč slonijo na znanih napadih. Praviloma so odvisni od zaznavanja že znanih zlonamernih datotek, procesov in podobnih zadev. Če pa se že lotijo nadzora vsega dogajanja, pa hitro naletijo na problem velikega števila podatkov in če želijo znotraj tega kupa podatkov izbrskati zanimiva opažanja, takoj naletimo na problem velikega števila lažnih in nepomembnih alarmov.

F-Secure RDR je varnostni sistem, ki nadzora dogajanja na delovnih postajah in strežnikih in pri tem uporablja algoritme umetne inteligence. Z algoritmi umetne inteligence namreč nadzor na končnih točkah lahko postane učinkovit. Ti sistemi spremljajo vse kar se na delovnih postajah in strežnikih dogaja. S tem sistem dobi ogromno količino podatkov.

Vendar algoritmi umetne inteligence znajo, znotraj te ogromne količine podatkov, učinkovito identificirati tiste najbolj pomembne. Na eni strani iščejo dogodke in zaporedje dogodkov, ki so nenavadni in nepričakovani. Na drugi strani pa iščejo dogodke in zaporedje dogodkov, ki nosijo sledi zlonamernosti. Tisti dogodki, ki so hkrati nepričakovani in hkrati nosijo sledi zlonamernosti, so tisti dogodki, ki nas zanimajo.

F-Secure RDR sistem je učinkovit zaznal poizkus kreiranja nedovoljenih privilegijev na eni izmed delovnih postaj

Umetna inteligenca torej neizbežno prihaja. Marsikdo bi rekel, da je že tukaj. Na področju varnosti informacijskih sistemov, tovrstni sodobni sistemi niso del težave, ampak so del rešitve. Tehnologija je razvita za potrebe varovanja informacijskih sistemov in ne za potrebe napadov na informacijske sisteme. Tega se v A1 z gotovostjo zavedamo in tem procesom namenjamo posebno pozornost, ter svoje produkte usmerjamo v tej smeri. ■

Varnostni prehodi za kontrolo dostopa v nadzorovana območja



- Visoka in nizka vrtljiva vrata, hitri prehodi, plačljivi prehodi.
- Integracija z obstoječimi sistemi.
- Nižji stroški fizičnega varovanja.
- Zvočni in svetlobni alarmi.
- Primerno za velik pretok uporabnikov.

ID Shop – zanesljiv partner za zagotavljanje kontrole pristopa v vaših objektih!

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

- Znižanje stroškov.
- Bolj nadzorovan pretok ljudi.
- Učinkovita integracija z obstoječo kontrolo pristopa v stavbi.
- Boljša učinkovitost pri doseganju višjih varnostnih standardov.



ID Shop nudi različne nivoje in mehanizme za zagotavljanje kontrole pristopa:

- **Mehanski sistemi zaklepanja** (cilindri, ključavnice, ključi, sistemski, generalni ključi, ...).
- **Mehatronski sistemi zaklepanja** (pametne kljuke, digitalni cilindri, elektronski ščiti, kartični pristop, ...).
- **Varnostni prehodi** (visoke, nizke vrtljive zapore, ...).

IDealni partner za identifikacijo in varnost

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

Avtorica: Mateja Mirtič / skrbnica ključnih kupcev in marketing, ID Shop d.o.o.



KAKŠNO KONTROLO PRISTOPA POSTAVITI NA VHODU V VAROVANA OBMOČJA?

V današnjem okolju zagotavljanje varnosti predstavlja vedno večji pomen za podjetja. Od nevarnosti, ki jih predstavljajo množice brez nadzora na javnih območjih, do tveganj, ki jih predstavljajo vsiljivci in nepooblaščeni vstopi, varnostni strokovnjaki prepoznavajo prednosti vrtljivih prehodov, kot enega najboljših načinov za izboljšanje fizične varnosti in kot sredstvo za nadzor dostopa zaposlenih in obiskovalcev.

Vhod v podjetje je najbolj izpostavljena in kritična točka, ker skozenj vstopajo zaposleni, obiskovalci, dobavitelji, stranke, podizvajalci, zunanji sodelavci, poslovni partnerji, dostavljalci ipd. Na tej točki je torej potrebno zagotoviti najvišjo kontrolo dostopa, da lahko nadzorujemo kdo lahko vstopi, kdo ne sme, ob kateri uri, v katere prostore in nenazadnje zato, da imamo pregled nad gibanjem in zgodovino gibanja zaposlenih in obiskovalcev po naših prostorih. Kompleksnost teh vstopnih procesov pa je vsekakor povezana z določenimi časovnimi obdobji, ko se število prehodov izredno poveča in jih je nemogoče učinkovito in brez nepotrebnih zastojev, obvladovati samo z običajnim fizičnim nadzorom.

Poznamo več nivojev zagotavljanja kontrole pristopa. Fizično varovanje na vhodih v stavbo v večini današnjih podjetij že dolgo ne zadostuje več. To nas sili, da organizacije na različne nivoje uvajajo nove mehanizme kontrole pristopa, med katere sodijo tudi mehanski sistemi zaklepanja s ključi, mehatronski sistemi, kamor spadajo tudi kartični sistemi, pametne

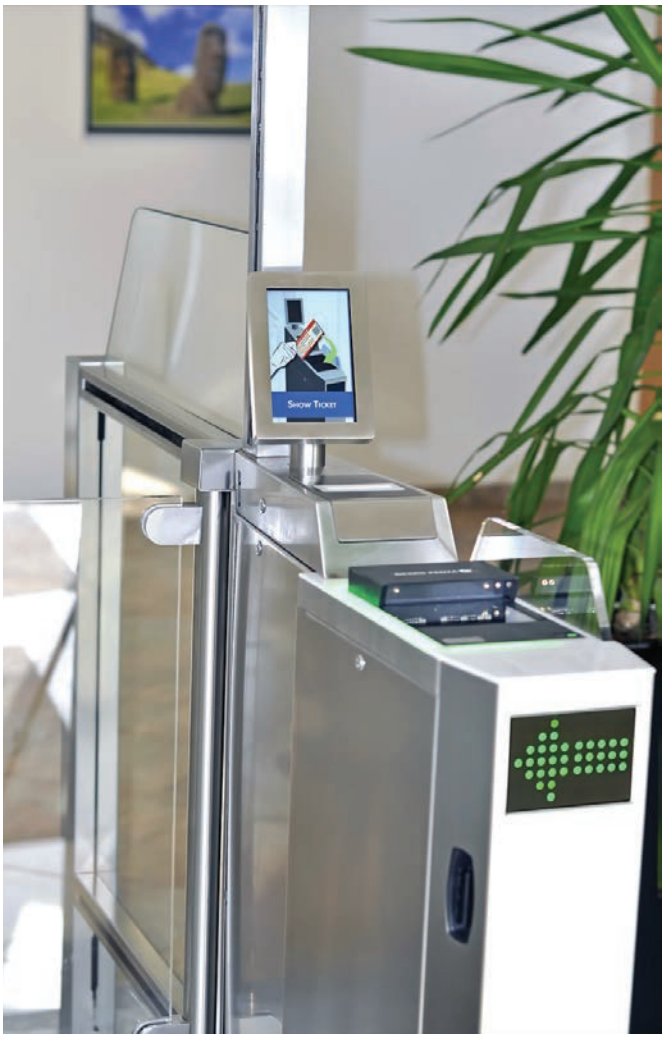


kljuke, digitalni cilindri..., do varnostnih prehodov v obliki vrtljivih varnostnih vrat oz. zapor ali hitrih prehodov za nadzorovana območja.

Podjetja lahko povečajo nivo varnosti, bodisi, ko se odločijo za nadgradnjo obstoječih varnostnih sistemov, bodisi za celovito zamenjavo kontrole pristopa na kritičnih območjih.

Podjetja lahko povečajo nivo varnosti, bodisi, ko se odločijo za nadgradnjo obstoječih varnostnih sistemov, bodisi za celovito zamenjavo kontrole pristopa na kritičnih območjih.

Zakaj je torej dobro, da nadomestimo staro kontrolo pristopa z novejšimi, varnejšimi in bolj naprednimi rešitvami?



Zato, ker z varnostnimi prehodi na nadzorovanih območjih pridobimo veliko več, kot zgolj povečano varnost. Predstavljajo dodane vrednosti, ki se kažejo v znižanju stroškov, večjemu pretoku ljudi, večji fleksibilnosti, izkoriščenosti celotnega varnostno - nadzornega sistema ter boljši učinkovitosti in transparentnosti pri doseganju višjih varnostnih standardov.

Izboljšana varnost

Izboljšana varnost je glavni razlog za namestitev visokih vrtljivih vrat ali hitrih prehodov oziroma t.i. fizičnih barier. Vsi ti sistemi namreč ponujajo vrhunski nadzor dostopa z odvračanjem in odkrivanjem nepooblaščenih obiskovalcev. Krožna vrata omogočajo dostop samo eni osebi naenkrat, kar optimalno upočasni prehod ljudi in varnostnemu osebju omogoči dovolj časa, da opazi morebitne težave in po potrebi posreduje.

Seveda lahko varnostni prehodi omogočajo tudi nadzorovan dostop v povezavi s kartičnim dostopom, biometrije, osebne kode ali drugega medija. Rešujejo tudi vprašanje zlorabe, ko ljudje nepooblaščeno vstopijo preko ovire, se splazijo pod oviro, ali ko skušata vstopiti po dve osebi naenkrat. Krožni varnostni prehodi fizično omejujejo, da bi skozi zaporo lahko hkrati vstopili dve osebi, medtem ko hitri prehodi delujejo na podlagi senzorjev, ki sprožijo vizualna in optična opozorila v primeru nepooblaščenih prehodov ali poskusa zlorabe.

Učinkovita integracija z obstoječo kontrolo pristopa v stavbi

Pomembno je omeniti dejstvo, da lahko varnostne prehode enostavno nadgradimo z obstoječimi varnostnimi in nadzornimi sistemi, ki so v podjetju že prisotni (npr. kamere, alarmni sistemi, požarni sistemi, elektronsko vodena vrata in druga varnostna oprema). Na ta način je možno zagotoviti popoln nadzor nad časom in identiteto vseh, ki vstopajo v stavbo. Prav tako je pomembno vedeti, da varnostni prehodi omogočajo vizualna (svetlobna) in zvočna (alarm) opozorila za lažje usmerjanje in opozarjanje obiskovalcev ter nadzornikov, kot tudi požarno funkcijo, ko se vrata samodejno preklopijo oz. odprejo, časovne okvire, opozorila za nepooblaščene prehode, zlorabe ipd.

Večja prilagodljivost za nemoteno delovanje

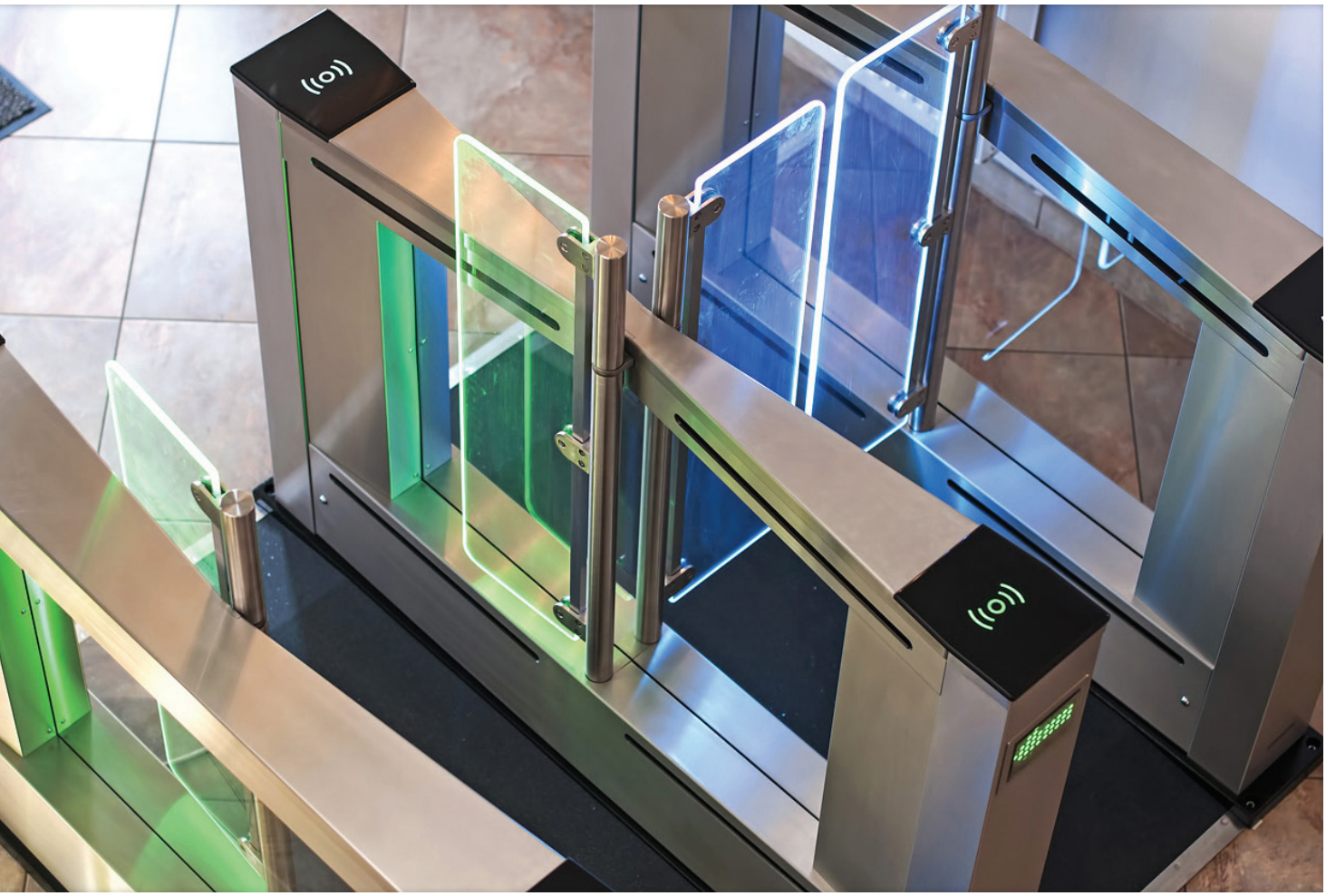
Dejstvo, da je vrtljiva varnostna vrata in hitre prehode možno povezati z drugimi nadzornimi sistemi in posledično z različnimi avtorizacijskimi mediji za hitro validacijo, pomeni, da tak postopek samotestiranja zmanjšuje obremenitev receptorjev in varnostnega osebja, ter prihrani čas in denar.

Sistem je lahko nastavljen na funkcijo „samo za vstop“ zjutraj, na primer, ko večje količine zaposlenih prihajajo in zvečer, ko se ob določeni uri samodejno preklopi na funkcijo „samo za izhod“. Vrata se lahko zaklenejo tudi ponoči ali čez vikend, ko je objekt zaprt. Funkcionalnost teh sistemov je pravzaprav zelo prilagodljiva vašim potrebam.

Varnostne prehode lahko delimo tudi po tipih nadzora

Visoka vrtljiva vrata temeljijo na **fizičnih zaporah**, ki segajo od tal do vrha višine vrat. Idealna za lokacije, ki zahtevajo najvišjo raven varnosti v sklopu podjetij ali na javnih mestih, kot so vojaške baze, skladiščni in distribucijski centri, vhodi v stadione, tematske parke,... Visoke vrtljive zapore so v največji meri primerne za zunanjo namestitev in so učinkovita rešitev v primerih, ko moramo zagotoviti, da več kot ena oseba naenkrat ne more skozi prehod.





Hitri varnostni prehodi poleg fizičnih zapor temeljijo še na **optičnem nadzoru**. To so prehodi, ki uporabljajo infrardeče senzorje za zaznavanje, ko se človek približuje oviri. Idealni so za lokacije, kjer bi visoke fizične ovire veljale za estetsko neprivlačne in vsiljive. Zasedejo minimalno prostora, so nižji in se lahko popolnoma zlijejo s prostorom v katerem se nahajajo. Hitri prehodi so predvideni za uporabo v zaprtih prostorih na območjih, ki potrebujejo nadzor nad velikim pretokom ljudi in vključujejo funkcijo preverjanja ali izdaje kart, računov ipd. Takšne hitre prehode lahko najdemo v objektu Blejski otok za vstop turistov, nameščeni pa so tudi na službenih prehodih, kjer se pojavlja velika količina zaposlenih v kratkih časovnih obdobjih. V takih primerih se v organizacijah za to rešitev odločijo, ker želijo optimizirati nadzorni sistem in se na določenih lokacijah znebiti fizičnega varovanja. Poseben dejavnik pa predstavlja tudi prostorska omejenost, kjer pridejo lahko take rešitve še posebej do izraza.

Pri načrtovanju in sprejemanju odločitev o dvigu ravni varnosti in nadzora je potrebno pred končno odločitvijo pretehtati več ključnih dejavnikov. Eden izmed pomembnih je predvsem izbira pravega sistema in partnerja, ki bo s svojim strokovnim znanjem, referencami in tudi kvalitetnim servisom zagotovil, da bo nameščeni sistem deloval učinkovito, in prinašal željene rezultate, ter ponujal optimalno rešitev za našo organizacijo.

Spomnimo, da je vhodna točka prvo, kar vidijo naši zaposleni in obiskovalci, ter poslovni partnerji naših organizacij. Že sam pogled na vhod lahko vzbudi občutke zaupanja, strokovnosti in varnosti ali pa ravno obratno, česar si v naših organizacijah ne želimo.

Pri načrtovanju in sprejemanju odločitev o dvigu ravni varnosti in nadzora je potrebno pred končno odločitvijo pretehtati več ključnih dejavnikov. Eden izmed pomembnih je predvsem izbira pravega sistema in partnerja, ki bo s svojim strokovnim znanjem, referencami in tudi kvalitetnim servisom zagotovil, da bo nameščeni sistem deloval učinkovito, in prinašal željene rezultate, ter ponujal optimalno rešitev za našo organizacijo. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Ana Struna Bregar
direktorica Centra energetsko učinkovitih rešitev (CER)

PODNEBNI VPLIVI NAS SILIJO V RESNO SPREMEMBO KONCEPTOV DOJEMANJA POSLOVANJA NAŠIH ORGANIZACIJ

Podnebna kriza in negativni vplivi na okolja so nas pripeljali na rob, kjer bo potreben popolnoma drugačen geostrateški pogled na delovanje širših družbenih skupnosti. V tem okviru pa bo to imelo pomemben vpliv na zagotavljanje novih pristopov poslovanja naših organizacij, ki morajo v prihodnosti temeljiti na okoljsko sprejemljivih pristopih. Za pogled na prihodnje izzive smo za komentar povabili ga. Ano Struna Bregar.

Nam lahko na kratko predstavite organizacijo CER, ki jo vodite? Kateri so glavni poudarki omenjene asociacije?

Center energetsko učinkovitih rešitev - CER je mreža naprednih podjetij in organizacij iz različnih sektorjev, ki imajo vodilno vlogo pri spodbujanju podnebno nevtralnega gospodarstva in zelenih tehnologij. Začetki segajo v leto 2012, ko so CER ustanovili Petrol, Knauf Insulation in Jelovica z namenom, da bi kupcem nudili vse za energetsko učinkovito novogradnjo in prenovo na enem mestu. Tekom let se je organizacija preusmerila. Začela je povezovati več sektorjev (energetika, mobilnost, gradnja). Sedaj delujemo kot zavod, ki ima vlogo strokovnega telesa ter sodeluje pri strateško pomembnih odločitvah v interesu širše družbe. Naša vizija je, da bi Slovenija postala stičišče razvoja zelenih tehnologij prihodnosti.

Zaradi podnebne krize, okoljsko energetskih in socialnih izzivov, omejenih naravnih virov ter velikega onesnaževanja okolja, smo priča globalnim in dramatičnim spremembam v čisto vseh sektorjih gospodarstva. Družba se bo v naslednjih desetletjih zaradi dveh globalnih megatrendov – digitalizacije in trajnosti - zelo spremenila. Največje spremembe pa definitivno lahko pričakujemo v mestih.

Fokus naših aktivnosti je usmerjen na spodbujanje orodij za pospeševanje podnebno nevtralnega gospodarstva in zelenih tehnologij, povezovanje različnih sektorjev, ozaveščanje o pozitivnih, mul-

*avtor je član Slovenskega združenja korporativne varnosti



tiplikativnih učinkih podnebno nevtralnega gospodarstva na zdravje, znanje, izobraževanje, zelena delovna mesta, pravičnost, dvig BDP, varnost, prihodnost. Med nalogami CER so tudi promoviranje slovenskega znanja, znanstvenih dosežkov, tehnoloških prebojev na področju zelenih tehnologij, globalno mreženje in internacionalizacija.

V drugi polovici leta 2019 smo imeli 33 članov (podjetij in drugih organizacij), ki dajejo vedno večji poudarek na povečevanju energetske učinkovitosti, uporabe obnovljivih virov energije, zmanjševanju odpadkov in emisij toplogrednih plinov.

Ste tudi izredno aktivni v mednarodnem okolju. Pred kratkim ste podpisali tudi sporazum o bilateralnem sodelovanju s fundacijo Monaškega Princa Alberta II (The Prince Albert II of Monaco Foundation). Kje so glavni poudarki vašega mednarodnega sodelovanja?

Sporazum predstavlja temelj za sodelovanje na področju reševanja podnebno energetskih izzivov. Namen sporazuma je vzpostavitev učinkovitega sodelovanja na poti do uresničevanja skupnih ciljev, ter razvijanje komplementarnih in sinergijskih dejavnosti na področju trajnostnega razvoja. Sporazum nadgrajuje dosedanje sodelovanje in izmenjavo informacij med zavodom CER in Fundacijo monaškega princa Alberta II.

Sodelovanje in povezave asociacij so nujno potrebne in edino logične. Le skupaj nam lahko uspe celovito naslavljati izzive sodobne družbe. Nivo in učinkovitost sodelovanja pa se morata vsekakor izboljšati.

Rezultat podpisa omenjenega dokumenta je sodelovanje in skrb za mednarodne projekte, ki jih bosta organizaciji skupno podpirali. S podpisom sporazuma si obe organizaciji prizadevata za tehnično, znanstveno in metodološko sodelovanje, ki bo omogočilo združevanje ali izkoriščanje posebnega strokovnega znanja in izkušenj pri izbiri, spremljanju in ocenjevanju projektov. Prav tako bosta organizaciji sodelovali pri komuniciranju skupnih vsebin, pripravi skupnih orodij za komunikacijo, kapitalizacijo in razvoj znanja ter pri izmenjavi izkušenj na konferencah, okroglih mizah in simpozijih o temah, ki se nanašajo na glavna področja dejavnosti obeh partneric.

Na mednarodnem nivoju pa sodelujemo tudi s Cambridge University – Insitute for Sustainability Leadership, s katerimi smo letos maja bili sopodpisniki odprtega poziva vladam EU za hitrejše spodbujanje podnebno nevtralnega gospodarstva. Sodelujemo tudi z evropsko platformo za spodbujanje inovacij na področju energetike EIT – InnoEnergy, tujimi gospodarskimi zbornicami in drugimi. Veseli nas, da smo pridobili tudi nove člane SBRA – Slovenian Business and Research Association, ki ima sedež v Bruslju. Vsako leto organiziramo tudi razvojno poslovne delegacije v tujino. Lani smo bili na Danskem in v Angliji, letos v Franciji. Mednarodne aktivnosti bomo v prihodnosti za gotovo še pojačali.

Ko govorimo o inovativnem podnebno nevtralnem krožnem gospodarstvu in zelenih tehnologijah ne moremo mimo razvoja informacijskih rešitev na katerih temeljijo pametna mesta. Kje vidite v prihodnosti glavne izzive razvoja pri uvajanju informacijske tehnologije v zeleno gospodarstvo?

Zaradi podnebne krize, okoljsko energetskih in socialnih izzivov, omejenih naravnih virov ter velikega onesnaževanja okolja, smo priča globalnim in dramatičnim spremembam v čisto vseh sektorjih gospodarstva. Družba se bo v naslednjih desetletjih zaradi dveh globalnih megatrendov – digitalizacije in trajnosti - zelo spremenila. Največje spremembe pa definitivno lahko pričakujemo v mestih.

Neizogibno dejstvo je, da je okoljsko nevtralno – krožno – gospodarstvo edina možna prihodnost in največji projekt naše družbe. Predstavlja številne izzive, hkrati pa nastajajo izjemne nove priložnosti za prilagajanje.

Novi trendi v gospodarstvu, disruptivne inovacije, digitalizacija, umetna inteli-

genca in nove zelene tehnologije (storitve, produkti in procesi) uvajajo nove tržne in vrednostne zakonitosti ter bistveno spreminjajo dinamiko trga, način delovanja podjetij, industrije in navad potrošnika. Pritiski strank, konkurentov, zaposlenih, sodišč, vlagateljev in celotne družbe za preoblikovanje politike in gospodarstva postajajo vedno močnejši.

Za tranzicijo gospodarstva oz. za prilagajanje podnebni krizi bodo potrebne velike investicije, po oceni UN Environment Programme Finance Iniciative bodo letni stroški do leta 2030 znašali 140–300 bilijonov USD, do leta 2050 pa 280–500 bilijonov USD.

Marsikatera podjetja (zlasti tista v energetsko najbolj potratnih sektorjih: energetika, mobilnost, gradnja, kmetijstvo in proizvodnja) so v prehodu na okoljsko nevtralno gospodarstvo že zaznala svoje koristi in prednosti - finančne, okoljske, poslovne, znanje, izkušnje in ugled.

Globalno je opazen porast novih podjetij s področja obnovljivih virov energije in drugih čistih tehnologij (voda, alternativni viri energije, emisije, odpadki ...). Vendar okoljsko nevtralno delovanje podjetij ni omejeno samo na že omenjene sektorje. Čisto vsa podjetja in organizacije bi morali delovati bolj trajnostno (okoljsko, družbeno in ekonomsko).

Informacijska tehnologija bo pri prehodu na zeleno gospodarstvo odigrala zelo pomembno vlogo. Upam, da bo zagotovila transparentnost, sledljivost in, da bo preprečila zlorabe.

Informacijska tehnologija s seboj prinaša določene varnostne izzive, katerim bo potrebno v prihodnosti polagati več pozornosti, tudi na področjih uvajanja novih tehnoloških rešitev za učinkovitejšo izrabo energije. Nameravate tem področjem v prihodnosti namenjati določeno pozornost?

Kar nekaj naših članov se aktivno ukvarja s prestrukturiranjem energetskega sektorja, od katerega smo vsi odvisni. Čista, učinkovita, varna in dostopna energija je tudi eden glavnih ciljev in prioritet Evropske unije. Industrijski in digitalni revoluciji sledi sedaj klimatska. Informacijska tehnologija bo odigrala v tej revoluciji zelo pomembno vlogo. V vsako dnevno življenje prinaša veliko dobrega, a se večina verjetno niti ne zaveda, da prinaša tudi izjemno velike varnostne izzive. Vsekakor se zavedamo, da moramo tudi na tem področju biti zelo aktivni, tako na nivoju ozaveščanja, povezovanja sektorjev.

V zadnjem obdobju zelo tesno sodelujete tudi z Institutom za korporativne varnostne študije, ICS-Ljubljana. Je to po vašem tisto potrebno sodelovanje, kjer bo na vaše področje delovanja pripeljano tudi specialistično znanje s področij obvladovanja varnostnih tveganj, ki bo okrepilo celovitost vašega procesa?

Namen naše organizacije je povezovati različne deležnike in sektorje, saj lahko le s prenosom znanja dosežemo učinkovite rezultate. Da bi bili na področju varnostnih izzivov in tveganj močnejši, in ker imamo sami premalo tovrstnega znanja smo se z veseljem povezali z vašim Institutom za korporativne varnostne študije, ICS-Ljubljana. Čaka nas veliko skupih izzivov.

Izjemno nas veseli, da so letos v CER pristopila tudi podjetja s področja IKT. Za sodelovanje pa se pogovarjamo tudi s predstavniki finančnega ter zavarovalniškega sektorja. Vsi se vedno bolj zavedajo nujnosti povezovanja, izmenjave informacij.

V načrtu je tudi tesnejše povezovanje CER s Slovenskim združenjem za korporativno varnost. So povezave takih asociacij nujno potrebne, če želimo celovito naslavljati izzive, ki so pred nami in našimi člani?

Sodelovanje in povezave asociacij so nujno potrebne in edino logične. Le skupaj nam lahko uspe celovito naslavljati izzive sodobne družbe. Nivo in učinkovitost sodelovanja pa se morata vsekakor izboljšati.

Podnebna kriza naslavlja kritična geostrateška vprašanja, v katerih ni mogoče izključiti možnosti vojn in družbenih prevratov. Čist zrak, voda, zemlja, hrana in zdravi ljudje postaja največja dragocenost. Zato smo pred pomembne izzive postavljeni tudi posamezniki, ki moramo začeti spreminjati svoje navade in zahtevati drugačne – bolj trajnostne rešitve. Od tega je odvisna naša prihodnost. ■



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

PRAVA TEHNIČNA VARNOST SE ZAČNE Z DOBRIM NAČRTOVANJEM LICENCIRANEGA PROJEKTNEGA BIROJA

PET OBMOČIJ VAROVANJA

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

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

VARNOSTNI RAZREDI

Centrala mora nadzirati prenosne poti:

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

UPRAVLJANJE PROTIVLOMNEGA SISTEMA JE PREGLEDNO, PREPROSTO IN UPORABNIKOM PRIJAZNO

NAPREDNE TEHNOLOGIJE VAROVANJA

Vgrajujemo profesionalni sistem najvišjega kakovostnega razreda - Tecnoalarm

ZARJA ELEKTRONIKA

Avtor: Miroslav Štravs / T-2 d.o.o.*

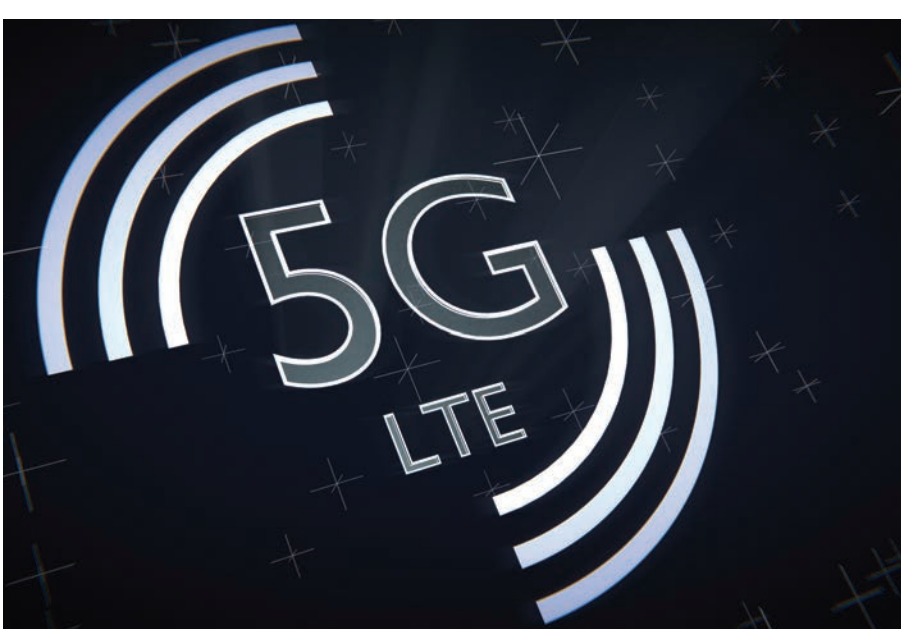


KIBERNETSKA VARNOST MOBILNIH OMREŽIJ 5G

Mobilna telekomunikacijska omrežja so postala ključna javna infrastruktura, mobilne telekomunikacijske storitve pa enako pomembne, če ne celo bolj, kot dobava elektrike, vode, plina... Pomen infrastrukture iz leta v leto narašča, spreminja pa se tudi njena vloga. Pred leti je bila namenjena prvenstveno govornim komunikacijam, danes pa mora biti načrtovana za vedno večje potrebe uporabnikov po mobilnih podatkovnih storitvah. Na obdobje krajše kot dekada se pojavi nova mobilna tehnologija, ki po eni strani omogoča uporabnikom boljšo uporabniško izkušnjo pri uporabi obstoječih storitev, po drugi strani pa jim ponuja nove storitve. V današnjem času se v profesionalnih krogih, pa tudi v javnosti, veliko govori o uvajanju pete generacije mobilne tehnologije, kratko imenovane kar 5G.

Uvod

Operaterji fiksnih in mobilnih telekomunikacijskih omrežij so dolžni v skladu z Zakonom o elektronskih komunikacijah zagotavljati varnost delovanja svojih omrežij. Telekomunikacijski operaterji periodično izvajajo analizo tveganj s katero pripravijo varnostno oceno posameznih sklopov telekomunikacijske in storitvene infrastrukture. Na osnovi ocene določijo ukrepe za zmanjševanje tveganj. Uvedba novih tehnologij sama po sebi ne prinese potrebe po spremembi metodologije izvajanja varnostnih analiz in ukrepov, nove tehnologije pa lahko uvedejo nove grožnje in tveganja, ki jih morajo operaterji prepoznati in upoštevati v analizah varnostnih tveganj in določitvi preventivnih ukrepov. Ocenjuje se, da se nove grožnje pojavljajo tudi zaradi političnih zaostrovanj na globalnem nivoju in strateške pomembnosti obvladovanja tehnologij mobilnih komunikacij vezano na mednarodno standardizacijo, patente, razvoj tehnologije in telekomunikacijske omrežne opreme in sistemov, ter nenazadnje tudi gospodarske učinke.



Kaj prinašajo nove mobilne tehnologije?

V zadnjih treh desetletjih smo priča skokovitemu razvoju mobilnih komunikacij. Začelo se je z analogno mobilno

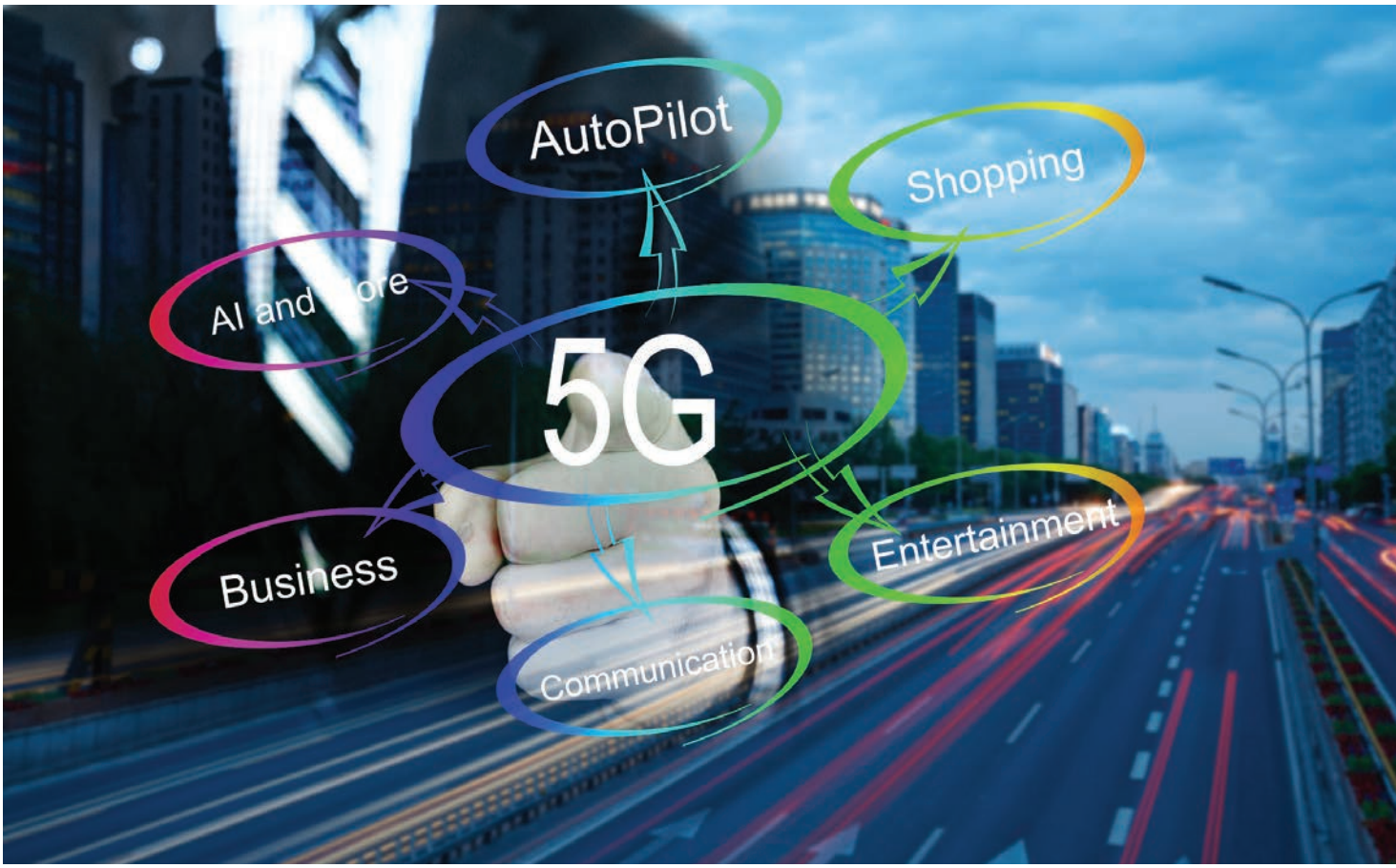
*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Pričakuje se, da bodo omrežja 5G uporabljena za mnoge namene, na začetku uvajanja predvsem za izboljšavo obstoječih storitev: mobilnega dostopa do interneta in izvedbo širokopasovnih povezav do doma z mobilnimi povezavami.

telefonijo, v Sloveniji je bil v uporabi sistem NMT (Nordic Mobile Telephony). Omrežje NMT je bilo v Sloveniji delujoče do konca leta 2005. Drugo generacijo predstavlja GSM (Global System for Mobile Communications), prvi resnično globalni sistem digitalne mobilne tehnologije, čeprav je bil standardiziran s strani evropske institucije ETSI (European Telecommunications Standardis Institute). Nadgradnja standarda poleg govornih storitev omogoča tudi podatkovne storitve, in sicer s tehnologijama GPRS (General Packet Radio Service) in EDGE (Enhanced Data Rates for GSM Evolution). Omrežja GSM so v večini držav delujoča še danes in so namenjena za storitve rezidenčnim in poslovnim uporabnikom. Tretja generacija mobilne tehnologije UMTS (Universal Mobile Telecommunications System) je bila standardizirana s strani 3GPP (the 3rd Generation Partnership Project) in uvaja enakopravno obravnavo govora in prenosa podatkov v omrežju. Omrežja UMTS predstavljajo infrastrukturno podlago za nove uporabniške terminale, pametne telefone, tablice. Nadgradnja podatkovnega prenosa s HSPA (High Speed Packet Access) tehnologijo uvaja širokopasovni mobilni prenos podatkov. Zaradi vedno večjih potreb po podatkovnem prenosu (globalna letna rast mobilnega prenosa podatkov je že vrsto let okoli 60%, medtem, ko rasti mobilnega govornega prometa praktično ni) je bil s strani 3GPP razvit standard četrte generacije mobilnih komunikacij LTE (Long Term Evolution). Standard določa elemente za mobilni podatkovni promet. Mobilna govorna storitev se lahko izvaja le kot podatkovna aplikacija, podobno kot prenos govora v fiksnih internetnih omrežjih, VoIP (Voice over Internet Protocol). Tudi LTE tehnologija je bila nadgrajena in sicer z LTE Advanced in LTE Advanced Pro. Danes običajne potrebe po mobilnih komunikacijah pokrivajo GSM; UMTS in LTE omrežja, ki delujejo paralelno. V zelo gosto naseljenih mestih, ali ob večjih prireditvah (npr. na stadionih), pa mobilna infrastruktura ni več dovolj zmogljiva.

Kapaciteta mobilnega podatkovnega prenosa je sorazmerna širini radio-frekvenčnega spektra, ki je namenjen mobilnim komunikacijam, spektralni učinkovitosti prenosa (koliko bit/s omogoča 1 Hz radio-frekvenčnega spektra) in števila baznih postaj, oz. je obratno sorazmerna z velikostjo področja pokrivanja bazne postaje. Vsaka nova mobilna tehnologija uvaja izboljšave prvih dveh elementov, prav tako peta generacija, 5G. Prva izdaja standardov (Release 15) je bila s strani 3GPP izdana v letih 2017 in 2018, nadaljnji (Release 16) so v izdajanju oz. pričakovanju izdaje. Tehnologija 5G je zasnovana tako, da bi se za desetkrat povečala kapaciteta





podatkovnega prenosa na celico, trikrat povečala spektralna učinkovitost, na desetino znižale zakasnitve v omrežju in omogočilo desetkrat večje število delujočih naprav v omrežju, vse v primerjavi z LTE tehnologijo. Ker se vseh teh parametrov prenosa podatkov ne more doseči sočasno, so bili s strani 3GPP določeni razredi storitev (CoS, Class of Services). Za vsako vrsto prenosa podatkov preko omrežij 5G se določi razred storitev. Razred za napredne mobilne širokopasovne komunikacije, eMBB (enhanced Mobile BroadBand) omogoča velike kapacitete podatkovnega prenosa, določena sta še razreda za visoko zanesljive komunikacije nizkih zakasnitev, URLLC (Ultra Reliable Low Latency Communications) in obsežne komunikacije med stroji, mMTC (massive Machine Type Communications). Izboljšave za doseganje načrtovanih parametrov prenosa se nanašajo predvsem na določitev novega radio-frekvenčnega spektra, ki ga na osnovi razpisa in dražbe v Sloveniji podeli Agencija za komunikacijska omrežja in storitve, kombiniranja radio-frekvenčnega spektra različnih pasov in nove zasnove anten na osnovi tehnologije MIMO (Multiple-input Multiple-output).

Načrtovani primeri uporabe

Razredi storitev se uporabljajo za različne primere uporabe, katerim je v primeru uvajanja tehnologije 5G dan dosti večji poudarek, kot pri uvajanju predhodnih tehnologij. Pričakuje se, da bodo omrežja 5G uporabljena za mnoge namene, na začetku uvajanja predvsem za izboljšavo obstoječih storitev: mobilnega dostopa do interneta in izvedbo širokopasovnih povezav do doma z mobilnimi povezavami. Načrtuje se, da bo tehnologija 5G uporabljena v industriji (npr. za komunikacijo z roboti), za senzorska omrežja (za aplikacije pametnih mest, pametnih vasi, pametnega doma), za potrebe javne varnosti, zaščite in reševanja, na cestah za avtonomno vožnjo, za komunikacijo do brezpilotnih letalnikov in druge danes še neoblikovane poslovne primere. Posameznikom bo omogočena uporaba aplikacij navidezne in razširjene resničnosti, zmogljivih mobilnih računalniških iger in podobno.

Mobilna omrežja 5G bodo skupaj z drugimi sistemi, tudi umetno inteligenco, predstavljala bodočo informacijsko infrastrukturo.

V današnjem času obravnavani zgoraj navedeni primeri uporabe nakazujejo, da bo delovanje družbe in življenje posameznikov še bolj odvisno od mobilnih komunikacij. Zato poudarek na varnosti omrežij 5G ni naključen. Čeprav s tehničnega vidika varnost omrežij 5G ne predstavlja bistveno drugačnega izziva kot varnost mobilnih omrežij predhodnih generacij, je pa pričakovan vpliv omrežij 5G bistveno obsežnejši in je že zato potreben dodaten razmislek o njihovi varnosti.

Varnost elementov mobilne infrastrukture

Sistem mobilnih komunikacij je sestavljen iz več sklopov, in sicer (a) radijske-

Mobilna omrežja 5G bodo skupaj z drugimi sistemi, tudi umetno inteligenco, predstavljala bodočo informacijsko infrastrukturo.



ga omrežja, na katerega se radijsko povezujejo mobilni terminali, (b) mobilnega jedra, ki usmerja govorni in podatkovni promet uporabnikov, (c) medomrežnega povezovanja med operaterji, ki omogoča gostovanje uporabnikov v drugih omrežjih in klice med mobilnimi in fiksnimi omrežji, (d) transportnega omrežja, ki povezuje prej navedene dele sistema in (e) sistema vodenja omrežja in podporne sisteme. Arhitektura sistema se glede na mobilno tehnologijo bistveno ne spreminja, vsaka tehnologija pa zahteva vzpostavitev ločenega sistema. Obravnava varnostnih groženj in tveganj se izvaja za vsak sklop sistema oz. še podrobneje. V okviru izvedbe omrežij 5G se uvajajo novi koncepti izvedbe, npr. omrežna virtualizacija in programsko določena omrežja, kar v izvedbo omrežij 5G vpeljuje dodatna tveganja.

Aktivnosti glede varnosti 5G omrežij

Aktivnosti glede kibernetske varnosti omrežij 5G sta ločeno sprožila Evropska komisija in združenje evropskih regulatorjev elektronskih komunikacij, BEREC (Body of European Regulators for Electronic Communications). Evropska komisija je že podala prvo poročilo, na poročilo BERECa pa še čakamo. Varnost omrežij 5G se obravnava tudi s strani drugih evropskih in nacionalnih institucij.

V juniju 2019 smo vsi evropski mobilni operaterji prejeli vprašalnik Evropske komisije o varnosti 5G omrežij. Vprašalnik v obliki analize tveganj je bil usmerjen v identifikacijo groženj in tveganj, ki se pojavljajo v povezavi z omrežji 5G. Evropska komisija je 9. oktobra 2019 objavila poročilo ‚'EU coordinated risk assessment of the cybersecurity of 5G networks" (dosegljiv na https://europa.eu/rapid/ press-release_IP-19-6049_en.htm) v katerem podaja ugotovitve glede akterjev groženj, ogroženih sredstev, groženj samih, tveganj in obstoječih preventivnih ukrepih.

Poročilo med drugim podaja tri največje akterje groženj, ki so: države ali s strani držav podprti akterji, organizirane kriminalne skupine in posamezniki znotraj operaterjev ali podizvajalcev. Ocenjuje se, da bi v primeru prvih dveh varnostni incident najbolj ogrozil zaupnost komunikacij.

Kibernetska varnost ni edina varnostna skrb glede infrastrukture 5G. Uporaba širšega radio-frekvenčnega spektra in posledično višja izsevana moč elektromagnetnega sevanja, ter uvedba milimetrskih valov za mobilne komunikacije, skrbita družbene skupine in posameznike s področja zdravja in okolja.

Nekatere grožnje v povezavi z infrastrukturo 5G so podobne infrastrukturi 3G in 4G, pri katerih grožnjo predstavljata pomanjkljivo načrtovanje in vodenje infrastrukture. Povečana ogroženost infrastrukture 5G pa temelji na tehnološki kompleksnosti, neprimerna implementacija 3GPP standardov, uporaba 5G specifičnih tehnologij, kot so omrežna virtualizacija, programsko določena omrežja in uporaba sistemov oblaka, ter povezano z naštetim tudi pomanjkanje usposobljenih strokovnjakov. Poročilo posebej poudarja grožnje povezane z dobavitelji. Izpostavljeni grožnji sta odvisnost od dominantnega dobavitelja opreme in sistemov, ter močne povezave med dobaviteljem in vlado tretje države.

Iz groženj izhajajoča tveganja so prav tako obstoječa in nova. Obstoječa tveganja so povezana z napačno konfiguracijo sistemov, pomanjkanjem kontrole dostopa namenjene tehnični podpori s strani pogodbenikov, ki imajo visoke administrativne pravice, slaba kvaliteta opreme tudi zaradi odvisnosti od dominantnega dobavitelja. Če je dominantni dobavitelj iz tretje države, nad katero so uvedene trgovinske sankcije, je operaterju lahko prekinjena dobava opreme in tehnične podpore. Nova tveganja se navezujejo na soodvisnost infrastrukture 5G in druge kritične infrastrukture. Kibernetski napad sovražne države ali kriminalne združbe na infrastrukturo 5G lahko ohromi delovanje druge vrste kritične infrastrukture, npr. elektroenergetskega sistema ali zdravstvenih institucij.

Preventivne aktivnosti se izvajajo na več nivojih, od Evropske komisije navzdol. Pomembno vlogo imajo tudi nacionalne agencije za kibernetsko varnost.

Zaključek

Kibernetska varnost ni edina varnostna skrb glede infrastrukture 5G. Uporaba širšega radio-frekvenčnega spektra in posledično višja izsevana moč elektromagnetnega sevanja, ter uvedba milimetrskih valov za mobilne komunikacije, skrbita družbene skupine in posameznike s področja zdravja in okolja. Zato bo potrebno pred uvedbo mobilnih omrežij in storitev 5G rešiti precej varnostnih izzivov in vprašanj in nekatera področja varnosti verjeto tudi dodatno regulirati. ■

Avtor: mag. Adriana Dvoršak, univ. dipl. pol. /
Mreža nevladnih organizacij za vključujočo informacijsko družbo



INFORMACIJSKA VARNOST BOLNIŠNIC IN KIBERNETSKA OBRAMBA SEKTORJA ZDRAVSTVA

Informacijska varnost v zdravstvu in varnost posebnih osebnih podatkov, kar so podatki o zdravljenju in zdravstvenem stanju vsakega bolnika in tudi vsakega zdravega državljana, postajata prepoznavna pogoja za uspešno digitalizacijo zdravstva.

Razen mnogih koristi, ki jih digitalizacija prinaša bolnikom, zdravnikom, zdravstvenim organizacijam, zavarovalnicam in zdravstvenemu sistemu, postavlja digitalizacija zdravstva pred nas tudi nekatere resne izzive informacijski varnosti in kibernetski obrambi.

- Skoraj v vsaki zdravstveni organizaciji v svetu pride v obdobju dveh let do nepooblaščenega dostopa do informacij.
- Stroški zaradi varnostnih incidentov so med vsemi panogami najvišji prav v zdravstvu.
- Zdravstveni sistemi so posebej ranljivi na nepooblaščen dostop do podatkov, veliko poslovno škodo in so latentno kibernetsko ogroženi, saj so vojaške kibernetske zmogljivosti v glavnem skrite in neznane.

Informacijska varnost kompleksnega informacijskega sistema v bolnišnici

Umni načrtovalci informacijske arhitekture se najprej vprašajo, katerim potrebam bo moral informacijski sistem zadostiti v prihodnosti. Ob tem uporabljajo predvidevanja o prihodnjem tehnološkem razvoju, o razvoju delovnih in poslovnih procesov, ocenjujejo pa tudi, po katerih podatkih in podatkovnih storitvah se bo v prihodnosti dvigovalo povpraševanje. V Sloveniji na primer, se je v zadnjem letu močno povečalo povpraševanje posameznikov v zvezi z obdelavo njihovih podatkov na temelju direktive o varstvu osebnih podatkov. Zaradi velikega števila vlog in obdelane količine podatkov so že tako skromne analitične zmogljivosti slovenskih bolnišnic dodatno obremenjene, tako na tehnološki, kot na kadrovski ravni.

Razen integracije najsodobnejših aparatur, digitalne medicinske opreme in pripomočkov, ki morajo biti neprekinjeno na voljo bolnikom in zdravnikom, informacijsko komunikacijski sistemi zagotavljajo zajem ali vnos podatkov, obdelavo in sledljivost obdelave podatkov, ter predstavitev podatkov bolnikom in zdravnikom v digitalni obliki. Obdelava podatkov v bolnišnicah mora biti hitra, zanesljiva in enostavna za uporabnika. Načrtovanje kliničnih in poslovnih procesov, ki jih podpira informatika, pa se začne že prej, še preden načrtovalci informacijske infrastrukture sploh pričnejo s specifikacijo in izbiro tehnologije.

Ozko gledano informacijsko infrastrukturo bolnišnice sestavljajo strežniška strojna oprema, diskovna polja in sistemi za shranjevanje podatkov, virtualizacija strežnikov in namizij, aktivna mrežna oprema (stikala, usmerjevalniki, brezžične rešitve v zgradbah in izven njih), programske rešitve za

> Bolnišnice so kompleksna delovna okolja v katerih potrebujejo stabilno infrastrukturo, in v katerih vsakodnevno lovijo ravnotežje med kakovostno obravnavo, odličnostjo in profesionalizmom ter stroškovno učinkovitostjo, nižanjem zalog in sanacijo s kronično nezadovoljnimi in podplačanimi zaposlenimi.



shranjevanje, arhiviranje in restavriranje podatkov, namizni, prenosni računalniki, monitorji in tiskalniki, vse podporne storitve, vključno z vzdrževanjem in servisom za več tisoč uporabnikov in več tisoč bolnikov dnevno.

Bolnišnice so kompleksna delovna okolja v katerih potrebujejo stabilno infrastrukturo, in v katerih vsakodnevno lovijo ravnotežje med kakovostno obravnavo, odličnostjo in profesionalizmom ter stroškovno učinkovitostjo, nižanjem zalog in sanacijo s kronično nezadovoljnimi in podplačanimi zaposlenimi. V tem vzdrževanju ravnotežja marsikdo pričakuje, da bo informacijski sistem rešil vse poslovne težave bolnišnice, omogočal hiter, enostaven in točen zajem podatkov, omogočal hiter vpogled v zbrane podatke, ter samodejno skrbel za interakcijo med informacijskimi podsistemi, in za intuitivno interakcijo med sistemom in uporabnikom. Visoka so pričakovanja do poslovnih sistemov, ki sicer podpirajo poslovne odločitve, v zadnjem času pa uporabniki celo pričakujejo, da bodo pravilne poslovne odločitve že avtomatizirane, in da se jim bo poslovna prihodnost tako rekoč prikazala v obliki panela na delovni postaji. Seveda bo potrebno nerealna pričakovanja znižati, saj se realno v informatiki rešujejo urgentna stanja v obliki nujnih posodobitev opreme in podpore uporabnikom.

Poenostavljen prikaz informacijske arhitekture v bolnišničnem okolju

Spletne tehnologije in storitve	Spletne platforme osredotočene na bolnika (vključenost v obravnavo, informiranost, uporabniška izkušnja)	Sistemski deležniki (uporabniki e-zdravja, telezdravja, izmenjava podatkov z Ministrstvom za zdravje, ZZZS, JAZMP, NIJZ, čezmejno zdravstveno varstvo)				**Varnost tehnologij, varnostno vedenje uporabnikov**
Aplikacijska programska oprema	Zdravstvena analitika, registri bolnikov, informacijska podpora zdravstveni dejavnosti (standardizacija procesov in obravnav, prilagajanje storitev in javne zdravstvene mreže)	Klinični informacijski sistemi (RIS/PACS, laboratorijski, lekarniški, reševalna postaja)	Poslovni informacijski sistemi (poslovna analitika, poslovne funkcije, kadrovska analitika, finance, nabava, upravljanje z viri, zalogami, plače)	Kolaboracija, kakovost obravnave, učinkovitost procesov, produktivnost, inovativnost, zasebnost	Lokacijske storitve, sledenje opreme in materiala v realnem času, skladišče, postelje	
Sistemska programska oprema	Uporabniška in sistemska programska oprema (programi za delo s podatkovnimi bazami, razvojna orodja, operacijski sistem)	Podatkovna skladišča, oblačne storitve	Upravljanje z identitetami, in dostopi, varnost (PAM)	Integracija		
Omrežna in strojna oprema, pametne zgradbe	Strežniki in diskovna polja, virtualizacija strežniškega okolja	Mrežna oprema, fiksno in brezžično omrežje	Medicinska oprema, integracija z informacijskimi sistemi	Periferna strojna oprema (delovne postaje, skenerji, multimedijska oprema, tiskalniki), integracija z informacijskimi sistemi	Upravljanje z odpadki, energijo, vodo, zgradbami	

Informacijsko varnost v Sloveniji razumemo kot varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. Informacijsko varnost zagotavlja vsak izvajalec sam, to je vsaka bolnišnica katera mora sama skrbeti za zaupnost, neokrnjenost in razpoložljivost podatkov, ne glede na njihovo obliko: elektronsko, tiskano ali katero drugo. Na kaj se določen tip informacij nanaša in v kakšni obliki se nahaja, pa je implicitno razvidno iz poenostavljenega prikaza informacijske arhitekture v bolnišnici.

Obramba kritične infrastrukture in medicinskih pripomočkov, ki jih imate doma

Nacionalne države same določajo način za varovanje kritične infrastrukture, vključno z informacijskim omrežjem bolnišnic. V Sloveniji so bolnišnice izvajalci bistvenih storitev in so zavezani Zakonu o informacijski varnosti. Aditivno in kumulativno Zakon o kritični infrastrukturi, katerega nosilni resor je Ministrstvo z obrambo, določa sektor zdravstva, kot sektor kritične infrastrukture.

V Sloveniji nas čaka še izvedba stalnih ukrepov za zaščito kritične infrastrukture, predvsem jih v obdobju sanacije ni mogel ustrezno predložiti noben klinični center. Skladno z zakonodajo se stalni ukrepi izvajajo v vseh razmerah; ob po-

> Visoka so pričakovanja do poslovnih sistemov, ki sicer podpirajo poslovne odločitve, v zadnjem času pa uporabniki celo pričakujejo, da bodo pravilne poslovne odločitve že avtomatizirane, in da se jim bo poslovna prihodnost tako rekoč prikazala v obliki panela na delovni postaji.

večani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi, pa se lahko njihovo izvajanje stopnjuje. Izvajajo se lahko še dodatni ukrepi, če stopnjevano izvajanje stalnih ukrepov ne zadošča. Predvideno stopnjevanje zna v realnosti naleteti na dve resni oviri: ustrezno število računalničarjev za implementacijo ukrepov in finančna sredstva za nakup licenčne programske opreme.

V primeru vojaških kibernetskih zmogljivosti in zaščite po mednarodnem (humanitarnem) pravu, danes še ne obstaja čvrsto soglasje o zagotovitvi jasne pravne zaščite civilnega prebivalstva v kibernetskem prostoru. Fizična in informacijska varnost v bolnišnici sta kompleksni, kot je kompleksna informacijska infrastruktura, pogojena s kompleksnostjo delovnih procesov v bolnišnici. Kot nakazano v tem prispevku





informacijski strokovnjaki skrbijo za varnost tehnologij na celotni informacijski arhitekturi, vključno z medicinskimi napravami, ki jih v zdravstvu v grobem ločijo na drago medicinsko opremo, ter na vgradne in nevgradne medicinske naprave. Z vgradnimi medicinskimi napravami je danes veliko bolnikov, ki so uspešno prestali invazivno zdravljenje, torej so bili operirani, ali uporabljalo elektronske naprave za nadzor in upravljanje vitalnih življenjskih funkcij. Tudi te naprave so izpostavljene tveganju za okužbo z zlonamerno programsko kodo. In naprav, ki uspešno nadomeščajo celotne organe ali organske sisteme, je na trgu vsak dan več.

Strokovnjaki Mednarodnega rdečega križa so se novembra 2018 v Ženevi posvetili škodi za ljudi v primeru vojaških kibernetskih operacij. Njihova stališča in skupno poročilo predstavlja korak v razvoju mednarodnega prava za zaščito civilnega prebivalstva v vojaških kibernetskih operacijah. Pozornost so namenili posebnim tveganjem, ki jih predstavljajo biomedicinski pripomočki in naprave, kot so spodbujevalniki in inzulinske črpalke. Ugotovili so prednosti, ki jih ponuja sistemska povezljivost posamičnih pripomočkov, kot je daljinsko spremljanje bolnikovega zdravstvenega stanja ali upravljanja medicinskih pripomočkov. Pri tem se niso ukvarjali z dvomi, ki se občasno pojavljajo v Evropski uniji, ali je visoka tehnologija, ki prihaja iz Kitajske, sprejemljiva za delovanje kritične infrastrukture. Seveda lahko kibernetski napadi, ki so osredotočeni na kritično infrastrukturo, vplivajo na zagotavljanje zdravstvenih storitev na povsem druge, zelo preproste načine, kakršen je bil izsiljevalski virus, ki je zašifriral vse dokumente na računalnikih Ljubljanskih lekarn. Zašifrirati je moč tudi zunanje diske in omrežne pogone, ki jih v mnogih podjetjih uporabljajo za shrambo dokumentacije.

Povabljeni strokovnjaki Mednarodnega rdečega križa so opisali tri faze kibernetskih napadov na industrijske nadzorne sisteme, ki veljajo za kritično infrastrukturo na splošno, in ki vključujejo sektor zdravstva. To so: dostop do IT omrežja, dostop do nadzornih sistemov sektorja zdravstva in povzročanje škodljivih učinkov v procesu zdravstvene obravnave.

Razpravljali so tudi o verjetnosti, zakonitosti in izvedljivosti vojaške sile za poseganje v (vgradno) biomedicinsko napravo sovražnega poveljnika z namenom, da bi ga med spopadom ubili. Ob tem so spomnili, da so ameriškemu podpredsedniku Dicku Cheneyu že pred 20 leti odstranili in zamenjali brezžični srčni spodbujevalnik zaradi bojazni, da bi brezžično tehnologijo lahko kdo izrabil za poskus atentata. Možnosti za kibernetske napade v sektorju zdravstva so številne, poceni in so izvedljive z veliko gotovostjo, njihov psihološki učinek na slovensko prebivalstvo pa bi bil precejšen. ■

11. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 11.—12. MAREC 2020



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

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

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

Avtor: mag. Blaž Ivanc / Slovensko združenje za korporativno varnost*



IZZIVI NA PODROČJU KIBERNETSKIH OPERACIJ V DRŽAVNIH VARNOSTNIH ORGANIZACIJAH RAZVITIH DRŽAV

Namen prispevka je izpostaviti določene izzive, s katerimi se srečujejo državne varnostne organizacije v razviti Evropi in druge globalne organizacije, za katere je značilna močna integracija znanja s področja kibernetskih operacij in razumevanja globalnih varnostnih groženj. Poleg tega je namen opozoriti na dokaj šibko zavedanje o pomenu obveščevalnih informacij v povezavi s kibernetskimi operacijami, v okviru tega pa tudi predstaviti izziv, ki ga predstavlja združevanje groženj po različnih, ponekod še vedno razmejenih varnostnih področjih.

Operacije, ki se izvajajo v kibernetskem prostoru, so skupek širokega nabora opravil in lahko vključujejo tako ofenzivne kot defenzivne ukrepe. Opredelitev kibernetskih operacij je mnogo. Kibernetske operacije opredelimo kot integracijo kibernetskih zmogljivosti z namenom doseganja ciljev v kibernetskem prostoru. Pri tem kot kibernetsko operacijo razumemo kibernetski napad, vendar je hkrati treba povedati, da tudi kibernetski napad vključuje širok nabor možnih razlag. Nadalje vidimo kibernetske operacije kot operacije, usmerjene proti tarči z namenom, da se dosežejo določeni cilji. V tem kontekstu so kibernetske operacije lahko izvedene proti sovražni entiteti v kibernetskem prostoru z namenom doseganja predhodno opredeljenega učinka.

Na področju kibernetskih operacij se države članice Evropske unije danes srečujemo s pomanjkanjem kadra tako na operativni kot na strateški ravni.V splošnem bi bilo možno zapisati, da današnji varnostni izzivi zahtevajo od strokovnjakov, da razumejo vedenje napadalcev in so zmožni razvijati scenarije neželenih dogodkov v kibernetskem prostoru. Še bistveno večji izziv pa predstavlja smiselna organizacija zmogljivosti za širok nabor razvoja kibernetskih operacij. Pri tem je ključnega pomena pravilno upravljanje z znanjem.

V praksi se pri potencialnem vključevanju novega kadra v delovne procese kibernetskih operacij, državne varnostne organizacije srečujejo s pomanjkanjem temeljnih znanj in spretnosti z operativno tehničnih vidikov.

Tako državne varnostne organizacije kakor mednarodna korporativna okolja se srečujejo s pomanjkanjem strokovnjakov različnih strok in specializacij, ki že imajo potrebna znanja in izkušnje na področju kibernetskih operacij. Takšen kader lahko, v pričakovani meri že od svoje vključitve v proces, aplikativno deluje v delovnem procesu organizacije. To še posebej drži za kader na operativni ravni. Z vidika strateškega odločanja pa je, ob nenehno spreminjajoči pojavnosti groženj, prav tako pomembno razumevanje različnih vidikov kibernetskih operacij.

Na področju kibernetskih operacij se države članice Evropske unije danes srečujemo s pomanjkanjem kadra tako na operativni kot na strateški ravni.

*avtor je član Slovenskega združenja korporativne varnosti



Obveščevalna podpora na področju kibernetskih operacij

Obveščevalne informacije o tarčah v kibernetskem prostoru so pomemben dejavnik pri doseganju operativne nadvlade pri kibernetskih operacijah. Pri tem so pomembne pravilne zahteve in smernice, na podlagi katerih se zbirajo in pridobivajo podatki. Poleg strokovnim bralcem že poznanih podatkovnih virov in sovpadajočih metod ter taktik dela obveščevalnovarnostnih služb je smiselno povedati, da tudi analiza družbenih omrežij, skupaj z računalniško analizo stališč, izraženih v besedilih, predstavlja uporabno vrednost pri razumevanju kibernetskih napadov.

Z vidika državnih obveščevalnovarnostnih organizacij je treba poudariti, da se danes srečujemo z združevanjem groženj na različnih, včasih jasno ločenih področjih. Podrobnejša predstavitev slednjega, s ponazoritvijo praktičnih primerov, bi v tem trenutku presegala namen tega članka. Vseeno velja, da pri današnjem pojavu združevanja groženj po različnih kategoriziranih razmejitvah ključno vlogo predstavljata poznavanje nastajajočih tehnologij in deljenje kakovostnih obveščevalnih podatkov.

Če za primer vzamemo kriminalni ekosistem, lahko o njem povemo, da se bo ta vedno prilagodil, pri tem pa sta skupnosti za deljenje informacij s področja kibernetskega prostora ter s področja prevar na različnih stopnjah zrelosti. Prav tako ima področje kibernetskih operacij svoj tip obveščevalnih informacij o grožnjah in metodah analiz ter zaznave. Organizirane kriminalne skupine poskušajo najti šibke točke tako v mednarodnih finančnih sistemih kakor tudi v nastajajočih finančno-tehnoloških storitvah.

> Kibernetski in finančni kriminal sta pogosto povezana, pri čemer nastajajoče tehnologije predstavljajo nove kanale, posledično pa se spreminjata frekvenca in raznolikost izvedbe groženj.

Kibernetski in finančni kriminal sta pogosto povezana, pri čemer nastajajoče tehnologije predstavljajo nove kanale, posledično pa se spreminjata frekvenca in raznolikost izvedbe groženj. Kljub temu se različno razvrščene pojavne oblike groženj še vedno obravnavajo v različnih, med seboj nepovezanih oddelkih in brez skupne točke informacijskega združevanja ter povezovanja. Po drugi strani se varnostne skupnosti pogosto srečujejo s pravnimi ovirami pri deljenju informacij med samimi skupnostmi, z izrazitim pomanjkanjem operativnih modelov za prej opisano delovanje ter z odsotnostjo ali z vsebinsko zastarelostjo regulativ.

Za konec velja poudariti, da velikokrat državne varnostne organizacije velikokrat predstavljajo tisti člen, ki proizvede ali zagotovi premalo uporabnih in časovno ključnih obveščevalnih informacij od pričakovanih. Pri tem se pogosto pojavljajo težave glede sodelovanja med oddelki, poznavanja podatkovnih zahtev in tehnologij, pravilne prepoznave sumljivih aktivnosti, razumevanja izpostavljenosti tveganju ter glede neprimernosti notranjih procesov in orodij. Pri končnih obveščevalnih informacijah pa je pomembno tudi razumevanje okoliščin, relevantnosti in preverljivosti. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Upravljanje s tveganji in korporativna varnost

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

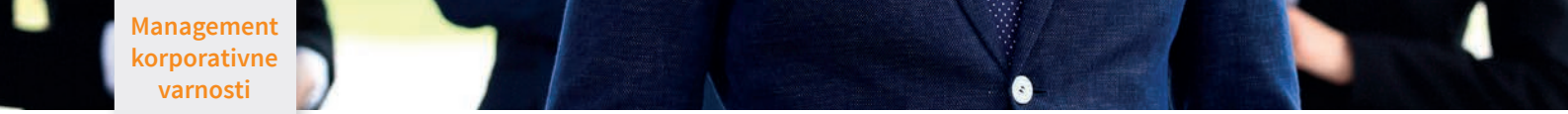
Omogočiti obvladovanje poslovno varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Zakaj Upravljanje s tveganji in korporativna varnost?

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

Komu je študij namenjen?

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



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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



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

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

Predmetnik

I. LETNIK

Skupni obvezni predmeti

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

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

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

Smer Korporativni varnostni manager – podjetnik

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

Izbirni predmeti (študent izbere dva):

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

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

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

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

CENTER VIŠJIH ŠOL

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

FAKULTETA ZA PODJETNIŠTVO

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

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

POSLOVNO-IZOBRAŽEVALNI CENTER

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





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

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo

11. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 11. - 12. MAREC 2020



DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI