Korporativna varnost

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

Letnik 2024, maj • št. 35



Tradicionalna 15. mednarodna konferenca Dnevi korporativne varnosti Brdo pri Kranju, 13.-14. maj 2024

Kibernetska varnost v energetiki: potreba po združevanju, sinergijah in skupnih korakih

mag. Aleksander Mervar, direktor ELES



VAŠA 360° VARNOST 365 DNI V LETU

Odmevni kibernetski varnostni incidenti v preteklem letu so potrdili, da je tudi **Slovenija na radarju kibernetskih kriminalcev**. Ribarjenje oziroma phishing je najbolj razširjena oblika kibernetskega kriminala Zadnje statistike kažejo, da se število tovrstnih napadov tako po svetu kot v Sloveniji iz leta v leto povečuje.

Za vašo varnost in najvišjo stopnjo kibernetske zaščite naj skrbijo **naši visoko certificirani strokovnjaki** iz **Centra kibernetske varnosti in odpornosti**, ki **24 ur na dan in 365 dni v letu** spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske grožnje.

CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

TelekomSlovenije
Vedno na boljše.

Telekom Slovenije, d.d., Ljubljana.



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
tiskano v Sloveniji

Datum izida:
maj 2024

Izvod revije je brezplačen

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

ISSN 2232-6170

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

Slovenija je zaradi svoje vključenosti v ključne mednarodne organizacije, kot so EU, NATO, v zadnjem obdobju pa tudi kot nestalna članica Varnostnega sveta Združenih narodov, deležna vedno večje mednarodne pozornosti v preigravanju geostrateških vplivnih deležnikov. Ta pozornost pa se odraža tudi v povečanju varnostnih izzivov, katerim so podvržene tako državne institucije, kakor tudi najpomembnejše slovenske gospodarske organizacije. V zadnjem obdobju se je močno povečalo število kibernetskih napadov na ključne državne inštitucije, niso pa se jim mogle izogniti niti določene gospodarske organizacije, predvsem tiste, ki upravljajo s pomembno infrastrukturo ali bistvenimi storitvami. To pa niso edina tveganja s katerimi so se v zadnjem obdobju srečevali deležniki nacionalne in korporativne varnosti. Močan medijski vihar smo doživeli ob spletni najavi možnih strelskih napadov v slovenskih šolah. Panični odziv določenega dela družbe je pokazal, da smo relativno nepripravljeni na tovrstne situacije, katerim se na žalost tudi Slovenija ne bo mogla izogniti. Vprašanje ni, ali se bo, temveč kdaj se bo taka situacija zgodila. Ali smo si pripravljeni priznati, da tudi razvoj naše družbe drvi v napačni smeri odtujenosti, prikrite in odkrite agresivnosti in prekomerne individualnosti. Te situacije so možne tudi v korporativnem okolju, zato moramo strokovnjaki korporativne varnosti razumeti izziv, ki ga prinaša to dejstvo in biti pripravljeni na ustrezne preventivne aktivnosti.

Pred nami je največji dogodek s področja korporativne varnosti, ki ga predstavljajo jubilejni 15. Dnevi korporativne varnosti 2024. Omenjeni dogodek je priložnost za izmenjavo dobrih praks in najnovejših spoznanj na področju obvladovanja varnostnih tveganj. Vedno pa je to odlična priložnost, da s podelitvijo prestižnih nagrad »Slovenian Grand Security Awards« izpostavimo tiste, ki so v preteklem obdobju izstopali po svojem delu in prizadevanjih za dvigovanje varnostnega zavedanja v Republiki Sloveniji.

Ravno tem vsebinam je v tokratni številki revije Korporativna varnost namenjena posebna pozornost. Skozi izbrane intervjuje imamo možnost slišati tako strateški nivo odločevalcev, ki upravlja pomembne nacionalne in lokalne organizacije, kakor tudi strokovnjake, kateri neposredno izvajajo svoje aktivnosti v okviru procesa korporativne varnosti. Poseben del v tokratni številki namenjamo kibernetski varnosti, novim zakonskim predlogom, ki so povezani z varnostnimi področji, kakor tudi glavno stvar, ki se rezultira v zaključnih korakih vzpostavljanja varnostno operativnega centra celotnega sektorja energetike. Poleg navedenega smo želeli v tokratni številki revije vsebinsko osvetliti tudi dovolj širok spekter ostalih strokovnih vsebin, ki bodo v pomoč strokovni javnosti pri iskanju potrebnih rešitev in strateške modrosti za ustrezno upravljanje varnostnih tveganj, s katerimi smo dnevno soočeni. V uredništvu revije upamo, da bo tudi 35. 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, direktor Urada Vlade RS za informacijsko varnost

IZZIVI IN NAPREDKI KIBERNETSKE VARNOSTI V PRIHODNOSTI 10



INTERVJU
g. Janez Anžič, direktor Operativno-storitvenega centra Telekoma Slovenije

BREZ PODPORE SODOBNEGA VARNOSTNO OPERATIVNEGA CENTRA SI TEŽKO ZAMIŠLJAMO USPEŠNO DELOVANJE ORGANIZACIJ 15



INTERVJU
g. Robert Bergles in **g. Vladimir Ban**, A1 Slovenija

NOVI IZZIVI NA PODROČJU KIBERNETSKE VARNOSTI - MOČAN DEJAVNIK PRI RAZVOJU SEKTORJA TELEKOMUNIKACIJ 24



INTERVJU
g. Božidar Dajčman, direktor Oddelka upravljanja fizične in informacijske varnosti v Novi kreditni banki Maribor

KONSTANTNOST SPREMEMB JE STALNICA PRI DELOVANJU BANČNEGA SEKTORJA 29



SODELOVALNI VIDIKI KIBERNETSKE VARNOSTI - DOBRE PRAKSE IN REŠITVE IZ PROJEKTA CYBERSEAS

Udejanjanje kibernetske varnosti v korporativnih okoljih postaja vse zahtevnejše, saj se v zadnjem času soočamo z naprednimi tehnikami napadov in porastom izpostavljenosti, kompleksnosti in povezljivosti teh okolij. 52

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

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

KIBERNETSKA VARNOST V ENERGETIKI: POTREBA PO ZDRUŽEVANJU, SINERGIJAH IN SKUPNIH KORAKIH

Glede na dejstvo, da je električna energija osnovna dobrina za zagotavljanje nemotenega delovanja ostalih družbenih procesov, je tudi zagotavljanje neprekinjenosti delovanja energetskega sektorja ključna aktivnost uspešnega upravljanja organizacij. Tudi v Sloveniji se nismo mogli izogniti resnim kibernetskim napadom na energetsko infrastrukturo. Zaradi tega je še toliko močnejše spoznanje, da potrebujemo skupne usklajene korake pri zagotavljanju delovanja sistema kibernetske varnosti v energetskem sektorju. O izzivih in priložnostih smo se pogovarjali z mag. Aleksandrom Mervarjem, direktorjem ELES.

V zadnjem času se vedno bolj krepi spoznanje, da celoten energetski sektor potrebuje pomembne korake v smeri združevanja zmogljivosti na področju obvladovanja kibernetskih tveganj. So dogodki, kot je bil kibernetski napad na HSE, spodbujevalni faktor, da je potrebno na tem področju hitreje izvesti določene korake, ali je to samo eden od dogodkov v nizu izzivov, s katerimi se sooča energetski sektor, predvsem na področju elektroenergetike?

Zanesljiva oskrba z električno energijo je odvisna od vseh skupin deležnikov – proizvajalcev, prenosa in distribucije, trgovcev, ki tvorijo enovit elektroenergetski sistem. Ta sistem bo tako dober in varen, kot bo dober in varen njegov najšibkejši člen. Za usklajeno delovanje in upravljanje elektroenergetskega sistema je potrebno odpiranje in povezovanje kibernetskih prostorov posameznih deležnikov, tako med sabo, kot z zunanjimi partnerji, kar pa prinaša nova informacijsko varnostna tveganja. Na kompleksnost zagotavljanja informacijsko kibernetske varnosti bistveno vpliva tudi heterogenost elektroenergetskega okolja. Zeleni prehod prinaša nove, hitro razvijajoče se tehnologije in z njimi nove informacijsko varnostne grožnje, ki se, kot del istega

> Na področju informacijske varnosti smo priča t. i. »kanibalizmu kadrov«, kjer si deležniki, zaradi izjemnega pomanjkanja strokovnjakov, le-te medsebojno prevzemajo. Za sam strokovni kader je sicer izjemno zanimanje seveda dobrodošlo in jim prinaša dobrobit, za varnost panoge, kjer nastopa izjemna soodvisnost, med deležniki pa je to le prelaganje »iz kupa na kup«.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



elektroenergetskega sistema, prepletajo s komponentami in sistemi z izjemno dolgimi življenjskimi dobami, ki trendom informacijske varnosti ne zmorejo slediti oz. sploh niso bili snovani z mislijo na informacijsko kibernetsko varnost (t. i. »legacy sistemi«).

Ob vseh informacijsko varnostnih izzivih elektroenergetskega področja in ob zavedanju pomena izvajanja bistvene storitve – oskrbe z električno energijo - je proaktivno vedenje in sodelovanje deležnikov nujno potrebno za nemoteno, kakovostno oskrbo z električno energijo.

Glede kibernetskega napada na HSE lahko rečemo, da je bilo opozorilo ob pravem času. Incident HSE je pokazal, da v Sloveniji nismo imuni na tovrstne grožnje in da za napadi na kritično infrastrukturo države stojijo izjemno organizirane in napredne kriminalne združbe, nemalokrat podprte tudi z državno pomočjo. Incident je predvsem potrdil medsebojno prepletenost in odvisnost ter opozoril na potrebo po orkestraciji deležnikov in skupnem nastopu v boju proti kibernetskemu kriminalu. Kibernetski napad na HSE je tako za nekatere deležnike prinesel streznitev, da so na tem področju naredili premalo, drugim pa potrdil pravilnost odločitev za vlaganje naporov v vzpostavljanje učinkovite informacijsko kibernetske obrambe.

Glede na omejenost kadrovskih in finančnih resursov je verjetno logična posledica, da se poišče ustrezne sinergije v združenem varnostno operativnem centru energetskega sektorja.

Zagotovo, z obeh vidikov. Na področju informacijske varnosti smo priča t. i. »kanibalizmu kadrov«, kjer si deležniki, zaradi izjemnega pomanjkanja strokovnjakov, le-te medsebojno prevzemajo. Za sam strokovni kader je sicer izjemno zanimanje seveda dobrodošlo in jim prinaša dobrobit, za varnost panoge, kjer nastopa izjemna soodvisnost, med deležniki pa je to le prelaganje »iz kupa na kup«.

Pri odpravi pomanjkanja kadrov morajo svojo vlogo odigrati tako država kot visokošolske institucije. Ker vemo, da se tak kader ne usposobi »čez noč«, pa moramo deležniki hitro reagirati, združiti znanje na enem mestu in s tem vzpostaviti enotno točko, ki nam bo zagotavljala potrebne informacijsko varnostne storitve.

V prid vzpostavitve enotnega varnostno operativnega centra govori tudi dejstvo, da se področje informacijsko varnostnih rešitev izjemno hitro razvija, tako da posamezne implementirane rešitve dokaj hitro postanejo nezadostne oz. so podvržene razmeroma hitremu staranju. Nenehno dograjevanje kibernetske obrambe, ob pestri izbiri informacijsko varnostnih rešitev, terja dober premislek pred nakupom, tako z vidika visokih stroškov, kot z vidika pravilnosti/ustreznosti odločitve. Posamezne rešitve se zato praviloma najprej preizkusijo (Prove Of Concept – POC), kar pa terja svoje resurse, še dodatno obremeni malo številčen strokovni kader ter podaljša čas do implementacije dodatnih zaščit.

Kako na to potrebo po združevanju gledajo ostali strateški voditelji v energetskem sektorju. Je dozorelo to spoznanje v širšem delu sektorja ali smo še vedno ujeti v določene okvirje čuvanja svojega dvorišča?

Menim, da smo na dobri poti. Zavedamo se, da vsak zase ne bo uspešen. To »čuvanje« pa mogoče ostaja, vendar po moji oceni ni prevladujoče.

Glede na to, da bo energetski sektor pri vzpostavljanju sektorskega varnostno operativnega centra potreboval pomoč vseh nacionalnih deležnikov, verjetno lahko pričakujete pomoč tako državnih institucij kot tudi najmočnejšega nacionalnega telekomunikacijskega operaterja, ki je še ostal v slovenskem lastništvu. Signali, ki jih dobivamo v javnost so več kot pozitivno naklonjeni temu koraku. Kako nadaljevati, da boste uspeli združiti vse deležnike v dinamičen ekosistem?

Brez želje in pomoči države tu zagotovo ne gre. Izhajam iz elektroenergetskega sektorja, vpliv katerega je na delovanje ostalih bistvenih storitev, kritične infrastrukture in s tem delovanja in razvoja družbe, prepoznala EU in je njegovi varnosti posvetila prav posebno pozornost. Prejšnji mesec je Evropska komisija potrdila prvi sektorski akt - nov omrežni kodeks, ki ureja področje kibernetske varnosti (Network Code on Cyber Securty - NCCS) od lokalne pa vse do panevropske ravni. Akt ureja medsebojne relacije, poročanja, odgovornosti, financiranje ter vključuje tako deležnike z elektroenergetskega sektorja kot tudi države. Kot že rečeno, akt je sicer pisan za področje elektroenergetike, vendar se dobre prakse, relacije in principi, ki so v njem zapisani, lahko prenesejo na področje celotne energetike.

Glede na zaznan porast napadov na kritično infrastrukturo in energetski sektor je pravočasna zaznava groženj, informiranje o tveganjih ter o zlonamernih akterjih nuja, katero mora zagotoviti vsak dober gospodar, ne glede na vrsto lastništva – privatno, mešano ali državno. To lahko optimalno zagotovimo le s skupnim pristopom, z vzpostavitvijo sektorskega varnostno operativnega centra. Seveda obstajajo s strani posameznikov tudi pomisleki in strahovi, vendar sem glede na kompleksnost, stroške in pomanjkanje kadra prepričan, da bo ideja vzpostavitve sektorskega varnostno operativnega centra dobro sprejeta, tako s strani države, kot tudi akterjev energetskega sektorja.

Glede na to, da je ELES organizacija, ki je na področju ukrepov za zagotavljanje neprekinjenega delovanja kritične infrastrukture naredila največje korake, boste verjetno ta spoznanja vtkali tudi v zagotovitev delovanja skupnega varnostno operativnega centra energetike?

ELES je glede na svojo poslanstvo – operater prenosnega omrežja - že leta v direktnem stiku z evropskimi informacijsko varnostnimi usmeritvami in zahtevami. Slovenski elektroenergetski sistem je del večjega, evropskega sistema, kjer imajo posamezni večji evropski deležniki izjemno visoko raven informacijsko kibernetske varnosti, pri medsebojnem sodelovanju pa od svojih partnerjev zahtevajo primerljivo informacijsko varnostno raven. V okviru evropskega združenja operaterjev prenosnega omrežja ENTSO-E smo tako oblikovali in sprejeli več informacijsko varnostnih načrtov, katerih spoštovanje je podvrženo rednim neodvisnim pregledom. V preteklih letih, ko so praviloma bolj prevladovali vidiki zagotavljanja funkcionalnosti, so se informacijsko varnostni vidiki marsikomu zdeli razmeroma nepotrebno delo. Danes smo lahko za pridobljene mednarodne informacijsko varnostne izkušnje hvaležni in naša dolžnost je, da jih delimo tudi s preostalimi deležniki.

Kadrovski potencial je v tem trenutku največji izziv vseh organizacijskih okolij. Pri združevanju kadrovskih potencialov bo potrebno verjetno zelo tankočutno izvajati ukrepe, ki bodo ustrezno usklajeni z vsemi deležniki tega sistema?

Tu pričakujem pošten pristop – vsak deležnik ima s področja kibernetske varnosti nekaj kadra in razumem, da bi najboljše rad obdržal zase, vendar če se bo k projektu vzpostavitve energetskega VOC pristopalo na način negativne selekcije kadrov, bo dobrobit za vse odložena oz. je ne bo. Pristop k VOC mora temeljiti na iskrenih namenih, drugače bo projekt zaradi sebičnosti ali pretirane opreznosti vnaprej obsojen na stagnacijo oz. propad. Tu moramo imeti dober pristop in ustvariti ugodne pogoje, da privabimo in zadržimo najboljše strokovnjake. Pozitivno vzdušje in dobri delovni pogoji so temelj za storilnost in dobro počutje zaposlenih. Tu pričakujem pošten pristop – vsak deležnik ima s področja kibernetske varnosti nekaj kadra.

Glavna podpora za korake združevanja pa mora biti verjetno zagotovljena tudi s strani lastnika, ki skozi SDH strateško upravlja z večino energetskih deležnikov. Boste imeli vi, kot direktor ELES-a in predsednik Energetske zbornice Slovenije, pri usklajevanju te podpore ključno vlogo?

Ključno vlogo bo imel SDH. Resorno ministrstvo in mag. Bojan Kumer pa podpirata enotnost elektroenergetike.

Prejšnji mesec je Evropska komisija potrdila prvi sektorski akt - nov omrežni kodeks, ki ureja področje kibernetske varnosti (Network Code on Cyber Securty - NCCS) od lokalne pa vse do panevropske ravni. Akt ureja medsebojne relacije, poročanja, odgovornosti, financiranje ter vključuje tako deležnike z elektroenergetskega sektorja kot tudi države.

Zaradi aktualnosti tematike se nikakor ne moremo izogniti vprašanju potrebe po izgradnji NEK-2. Slovenija za svojo stabilno oskrbo v kriznih časih verjetno nujno potrebuje nov dolgoročno stabilni vir električne energije?

Podpiram, pravilno se projekt glasi JEK 2. Sem pa za pošteno izmenjavo podatkov. O tem sem spregovoril v zadnjih treh intervjujih.

Kje vidite, da lahko ELES največ pridoda k učinkoviti, v zeleno usmerjeni preobrazbi družbe? Verjetno bo za ta prehod zagotavljanje učinkovitih prenosnih zmogljivosti eden od ključnih dejavnikov uspeha?

ELES je pripravljen na zeleni prehod. V letu 2022 smo realizirali projekt SincroGrid, trenutno smo v izvedbi drugega EU projekta GreenSwitch.

Pred nami je jubilejni mednarodni dogodek Dnevi korporativne varnosti, ki postavlja pomembne mejnike za učinkovito obvladovanje tveganj v širšem regijskem prostoru. Glede na to, da ste tradicionalno glavni podpornik dogodka vas prosimo za nekaj osnovnih misli, kaj bi veljalo še posebej izpostaviti v letošnjih razpravah na področju dvigovanja učinkovitosti obvladovanja varnostnih tveganj?

Poleg pomanjkanja kadrov, nezadostnega pretoka informacij in predvsem potrebe po sodelovanju in povezovanju, ki so izjemno pomembni ter že več let prisotni izzivi s področja informacijsko kibernetske varnosti, bi izpostavil odnos do rabe umetne inteligence. O njej se veliko govori, predstavljena je kot »business enabler«, kot pomoč neizmernih razsežnosti. Premalo pa se govori o njeni varni rabi, implementaciji in morebitnih pasteh ter varnostnih tveganjih, ki jih raba te nove tehnologije prinaša, tako na področju zagotavljanja IT storitev kot tudi kibernetske obrambe. ■

Foto: arhiv ELES d.o.o.

Poleg pomanjkanja kadrov, nezadostnega pretoka informacij in predvsem potrebe po sodelovanju in povezovanju, ki so izjemno pomembni ter že več let prisotni izzivi s področja informacijsko kibernetske varnosti, bi izpostavil odnos do rabe umetne inteligence.

Slovensko združenje korporativne varnosti

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

»Ab uno disce omnes (po enem spoznaj vse)«
»Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!«

Namen združenja je uresničevanje interesov članstva, ki so:

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

Združenje ima redne, korporacijske in častne člane.

www.ics-institut.si

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

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

tenzor

GEN SKUPINA

Onkološki inštitut Institute of Oncology Ljubljana

Melamin

Mercator

telemach

SIEMENS

NIJZ Nacionalni inštitut za javno zdravje

ELEKTRONČEK

Telekom Slovenije

Pošta Slovenije

AKRAPOVIČ

AJPES

INFORMATIKA

novakbm

Elita i.b. d.o.o.

ZARJA ELEKTRONIKA

UNISTAR PRO

CINKARNA

Slovenske železnice

CAA

SMART COM

URSIV

MINISTRSTVO ZA INFRASTRUKTURO

JAVNI MEDOBČINSKI STANOVANJSKI SKLAD MARIBOR

GENERALI

Mestna občina Ljubljana

PETROL

Energija za življenje

interblock

triglav

SPICA

DARS

smartis

LON

energetika ljubljana

www.ics-institut.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

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

IZZIVI IN NAPREDKI KIBERNETSKE VARNOSTI V PRIHODNOSTI

Urad za informacijsko varnost dobiva vedno pomembnejšo vlogo pri koordinaciji slovenskega ekosistema informacijske varnosti. Ponovno smo izkoristili priložnost in se ob procesu sprejema novega Zakona o informacijski varnosti pogovorili z dr. Svetetom, da nam podrobneje razjasni vizijo razvoja ekosistema na področju informacijske varnosti.

Priča smo vedno pogostejšim varnostnim izzivom, ki prihajajo iz kibernetskega okolja. Verjetno samo največji optimisti pričakujejo, da se bo v prihodnje zmanjševalo število varnostnih tveganj, realnost pa je verjetno zelo drugačna. Kako vi ocenjujete varnostno dinamiko v naslednjem obdobju?

Dinamika pojavljanja incidentov, tveganj in groženj je vedno bila spremenljiva in taka bo tudi v prihodnje. Če pogledamo leta nazaj, smo nekaj zadnjih let beležili povečano število pojavljanja spletnega ribarjenja prek elektronske pošte. V letu 2023 pa smo zabeležili padec. Kaj se je zgodilo? Predvidevamo, da so bile kampanje glede osveščanja uspešne, saj je omenjene incidente težko dokazati. Ljudje se vedno bolj zavedajo grožnje in tveganj, ki jih ta prinaša. Zato vedno manj odpirajo tovrstna sporočila, hkrati pa jih tudi vedno manj prijavljajo, saj jih prepoznajo in izbrišejo. Po drugi strani pa imamo opravka z vse bolj ciljanimi napadi, ki izkoriščajo ranljivosti informacijskih sistemov, njihovo vse težje nadzorljivo kompleksnost in slabo kibernetsko higieno. Cilji takih napadov so velikokrat trajna prisotnost in eksfiltracija podatkov, zato jih je težje zaznati. Ocenjujemo tudi, da je kljub vsemu še vedno zelo veliko incidentov informacijske varnosti neprijavljenih. Danes imamo v Sloveniji zavezance, ki so po zakonu dolžni prijavljati incidente z resnim vplivom na njihove bistvene storitve, ostali pa jih prijavljajo prostovoljno. V prihodnje, z uveljavitvijo novega zakona o informacijski varnosti, bo zavezancev mnogo več, več kot tisoč, torej bo tudi prijavljenih incidentov več, še vedno pa bodo ostali imeli na voljo prostovoljno prijavo. Zato je zanašanje na statistiko nehvaležno. Hkrati pa se bo zavedanje o pomembnosti zaščite informacijskih sistemov dvignilo, tudi zaradi druge področne regulative – DORA, CER, letalska zakonodaja in drugo, in bo tudi iz tega razloga kakšen incident manj. Seveda pa to ni garant, saj stoodstotne varnosti ni, lahko pa veliko naredimo, da preprečimo marsikatero škodo zaradi incidenta, ali pa le-to vsaj omejimo. Glede groženj, s katerimi se bomo ukvarjali v prihodnje, je treba poudariti, da so orodja in načini izvajanja incidentov

> Glede razkrivanja ranljivosti je treba povedati, da tu ne gre za novo vsebino, ampak gre le za njeno zakonsko ureditev. Nacionalni odzivni center za kibernetsko varnost SI-CERT je že do sedaj prostovoljno prevzemal vlogo koordinatorja odgovornega odkrivanja ranljivosti, kar pomeni, da je kot neodvisen subjekt koordiniral aktivnosti med stranjo, ki je ranljivost odkrila in stranjo, ki je ranljivost imela v svojih informacijskih sistemih.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



vedno bolj izpopolnjeni in inovativni, podprti tudi z uporabo umetno inteligenčnih orodij. Poleg tega pa s prihodom novih tehnologij, prihajajo tudi z njimi povezana tveganja in grožnje. Agencija Evropske unije za kibernetsko varnost v svojih predvidevanjih do leta 2023 na prvo mesto še vedno postavlja grožnje povezane z dobavno verigo, na drugem mestu pa je pomanjkanje veščin povezanih z zagotavljanjem kibernetske varnosti. Med prvih deset groženj je prvič uvrstila sisteme brez varnostnih popravkov in zastarele sisteme v preobremenjenem medsektorskem tehnološkem ekosistemu ter fizične učinke naravnih oziroma okolijskih vplivov na digitalno infrastrukturo. Nekaj izmed teh groženj se je v slovenskem prostoru nedavno že realiziralo.

Pred nami je zelo pomemben korak dokončnega sprejema Zakona o informacijski varnosti in predvsem začetek njegove učinkovite implementacije. Kako ste zadovoljni s pripravo zakonskega predloga in kvaliteto javne razprave? Je le ta pripomogla k izboljšanju končnega predloga zakona?

Priprava omenjenega zakona je precej zahtevna zadeva. Gre predvsem za prenos evropske direktive NIS 2, ki širi, ne-le nabor zavezancev, ampak tudi obseg nalog in nalaga nove. Za nami je prva javna obravnava s katero smo zadovoljni. Prejeti odzivi so pripomogli k jasnosti zakonskih določb. Tu mislimo predvsem na področje varnostne dokumentacije bistvenih in pomembnih subjektov, ukrepov za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov, certificiranja ter področje pristojnosti in teritorialnosti. Ob tem moramo upoštevati, da smo zavezani k prenosu Direktive (EU) 2022/2555 in ne smemo sprejeti rešitev, ki bi nasprotovale zapisanim določbam. Z nekaterimi subjekti smo že stopili v kontakt in opravili uskladitev. Več subjektov je predlagalo, da bi zakon preimenovali v »Zakon o kibernetski varnosti«. Ob dejstvu, da NIS 2 direktiva zahteva pristop upoštevanja vseh groženj, tudi tistih iz fizičnega okolja, menimo, da je naslov zakona ustrezen.

Zakon o informacijski varnosti bo v večini namenjen prenosu evropske direktive NIS 2 v nacionalni pravni red. Je pri nas že dozorelo zavedanje, da se bistveni tektonski premiki dogajajo in usklajujejo v Bruslju in da je sprejem direktiv na evropskem nivoju samo osnovni predpogoj za kasnejše nacionalne korake. Predvsem na področju skupnega pristopa, na področju obvladovanja kibernetskih tveganj in predvsem kibernetske obrambe je to verjetno edina logična pot. Kakšno je vaše mišljenje?

S Slovenskim združenjem za korporativno varnost sodelujemo že vrsto let. To sodelovanje je nujno potrebno, tako z vidika ozaveščanja, izobraževanja različnih javnosti, strokovne razprave o raznovrstnih vprašanjih zagotavljanja kibernetske varnosti in njenega razvoja.

Nov Zakon o informacijski varnosti bo seveda v prvi vrsti sledil ureditvi vsebin, kot jih predvideva direktiva NIS 2. Seveda bodo pa vključene tudi nacionalne vsebine, ki so se do sedaj v praksi izkazale kot potrebne. Ocenjujemo, da je EU pot skupnega pristopa ubrala iz dveh razlogov. Prvi razlog je v dejansko neenotni ureditvi področja. Želela je vzpostaviti enotne minimalne standarde, tako da lahko govorimo o minimalni harmonizaciji. Hkrati pa je področje zagotavljanja kibernetske varnosti prepoznala kot zelo pomembno, saj na letni ravni v EU prihaja do velikih finančnih izgub. Govorimo lahko o milijardnih izgubah, izgubi delovnih mest, izgubi vseh vrst podatkov, osebnih, občutljivih in ne nazadnje tudi o izgubi intelektualne lastnine. Vse to povzroča ogromno gospodarsko škodo, ki jo je treba omejiti in narediti vse potrebno, da se trend povečevanja izgube obrne navzdol. Glede vaše ocene, da se tektonski premiki in usklajevanja dogajajo v prestolnici EU, se strinjamo. A to ne pomeni, da se naš glas ne sliši. Prav v NIS 2 so izpeljane nekatere rešitve, ki smo jih v Sloveniji vpeljali, kot nacionalne določbe že v prvem Zakonu o informacijski varnosti. Tu mislim predvsem na organe državne uprave, nacionalni načrt odzivanja na kibernetske incidente, pomen kriznega odzivanja in vpetosti v kritično infrastrukturo.

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

Lahko potrdim, da se zavedanje glede pomembnosti zagotavljanja informacijske in kibernetske varnosti krepi. Na poti našega razvoja, iz organa v sestavi ministrstva do samostojnega vladnega urada, smo bili deležni razumevanja in podpore, tako glede kadrovskih zahtev kot tudi finančnih virov. Vsako



leto smo uspeli zaposliti nove sodelavce in jih uspešno integrirati v kolektiv. Proces se bo nadaljeval tudi v prihodnje, saj, kot že omenjeno, prihajajo nove zadolžitve.

Trenutno stanje na področju financiranja ključnih projektov informacijske varnosti in kibernetske obrambe, predvsem zaradi popoplavne sanacije, ni najbolj rožnato. Tudi URSIV je bil deležen drastičnega zmanjšanja potrebnih finančnih sredstev. Pričakujete, da bo v prihodnje temu področju namenjeno več finančnih sredstev za zagon in izvajanje nujnih korakov?

Na uradu smo kljub zmanjšanju finančnih sredstev zaradi lanskoletnih poplav uspeli zagotoviti dodatna finančna sredstva, seveda v obsegu, ki smo jih zmožni absorbirati. Nekateri projekti se bodo premaknili naprej in upamo, da nam bo uspelo, kljub temu, da je pol leta že skoraj za nami. Dodatna finančna sredstva pa bodo potrebna tudi za uveljavitev novega zakona o informacijski varnosti, katerega grobo finančno oceno imamo že izoblikovano.

Še vedno se ne moremo znebiti občutka, da pri grajenju dinamičnega in učinkovitega ekosistema nacionalnih deležnikov na področju kibernetske varnosti nismo najbolj uspešni. Menite, da je glavna ovira prekomerno zakoreninjen individualizem v Slovenski družbeni skupnosti ali po vašem mnenju temu botrujejo drugi vzroki?

Grajenje učinkovitega ekosistema zagotavljanja kibernetske varnosti je tek na dolge proge. Gre za dolgoročen proces, kjer je najbolj pomembno medsebojno zaupanje, predvsem pa tudi zavedanje, da so se, tako družbe kot širša geostrateška okolja v zadnjih letih temeljito spremenila. Prostora in denarja za vrtičkarstvo ni več, zato je potrebno novo realnost sprejeti in se ji prilagoditi, ter na ta način graditi sodelovanje v več smereh, kot so redno sestajanje in ustrezen način izmenjave informacij, ne razkrivanje pomembnih informacij, jasna razmejitev pristojnosti na komplementaren način. URSIV v skladu z omenjeno nalogo izvaja redna usklajevanja na nivoju Koordinacijske skupine za kibernetsko varnost. Delovanje skupine se je izkazalo kot pomemben element dviga kibernetske varnosti. Samo delovanje skupine želimo z novim zakonom še nadgraditi, jo opolnomočiti, hkrati pa predvsem v tehničnem smislu, odpreti vrata sodelovanja ostalim zainteresiranim entitetam ekosistema kibernetske varnosti.

Pričakujete, da bo nacionalni kibernetski kompetenčni center uspel močneje združiti potrebne deležnike v dinamični ekosistem, potreben za hitrejši razvoj na tem zahtevnem področju?

Da. Nacionalni koordinacijski center za kibernetsko varnost, kot se uradno imenuje, je na URSIV umeščen v Sektor za dvig odpornosti, ki se je že doslej ukvarjal z izgradnjo zmogljivosti. Želimo si povezati deležnike s področja raziskav in razvoja, izobraževanja, industrije in javnega sektorja z namenom, da kar najbolje izkoristimo obstoječe potenciale na področju kibernetske varnosti ter jih še okrepimo. Pri tem bo izrednega pomena izgradnja skupnosti, katere člani se bodo lahko tesneje povezovali med seboj in s podobnimi skupnostmi v mreži NCC v ostalih državah. Vsekakor pa bomo med prvimi v skupnost povabili člane Sekcije za kibernetsko varnost pri ZIT, GZS in člane Slovenskega združenja za korporativno varnost.

Nov zakon ureja tudi odgovorno razkrivanje ranljivosti, ki naj bi jih koordiniral SI-CERT. Kakšna so pričakovanja glede omenjenega mehanizma?

Glede razkrivanja ranljivosti je treba povedati, da tu ne gre za novo vsebino, ampak gre le za njeno zakonsko ureditev. Nacionalni odzivni center za kibernetsko varnost SI-CERT je že do sedaj prostovoljno prevzemal vlogo koordinatorja odgovornega odkrivanja ranljivosti, kar pomeni, da je kot neodvisen subjekt koordiniral aktivnosti med stranjo, ki je ranljivost odkrila in stranjo, ki je ranljivost imela v svojih informacijskih sistemih. Pričakujemo, da bo mehanizem pozitivno sprejet, saj bodo vloge in postopki jasno opredeljeni, to pa bo pripomoglo k večji predvidljivosti in zanesljivosti.

Kakšne so izkušnje in vaši načrti na področju razvoja kvantnih komunikacij in predvsem kvantnega šifriranja komunikacij?

URSIV že od začetka leta 2023 sodeluje v konzorciju za vzpostavitev nacionalne kvantne komunikacijske infrastrukture za varno distribucijo kvantnih šifrirnih ključev. V konzorciju poleg URSIV sodelujejo še Fakulteta za matematiko in fiziko, Institut Jožefa Stefana, podjetje Beyond Semiconductor d.o.o. in UVTP. Projekt sestavlja zemeljski segment za vzpostavitev optičnih povezav, razvoj in namestitev komunikacijske opreme ter vesoljski segment za povezavo zemeljskih omrežij s konstelacijo satelitov. Trenutno se izvaja projekt SiQUID, ki pokriva zemeljski segment. Projekt je pomemben z vidika zagotavljanja nacionalne varnosti, saj obstoječe klasične rešitve za šifriranje, s prihodom kvantnih računalnikov, ne bodo več zagotavljale varnega prenosa podatkov. Prav zato je projekt namenjen končnim uporabnikom, ki delujejo na področju zagotavljanja nacionalne varnosti. Projekt, ki je pomemben tudi z vidika razvoja slovenske znanosti, se financira s sredstvi iz Načrta za okrevanje in odpornost (NOO), sredstvi EU razpisa iz programa Digitalna Evropa in sredstvi enega od partnerjev v konzorciju. URSIV je poleg aktivnosti na projektu zadolžen tudi za zagotovitev sredstev NOO za celoten projekt.

Slovensko združenje za korporativno varnost je v zadnjem obdobju organiziralo nekaj pomembnih javnih posvetovanj, ki so vključevala tudi izzive na področju kibernetske varnosti. Nameravate skupaj z omenjeno asociacijo tudi v prihodnje izvajati korake za čim hitrejšo implementacijo novega Zakona o informacijski varnosti?

S Slovenskim združenjem za korporativno varnost sodelujemo že vrsto let. To sodelovanje je nujno potrebno, tako z vidika ozaveščanja, izobraževanja različnih javnosti, strokovne razprave o raznovrstnih vprašanjih zagotavljanja kibernetske varnosti in njenega razvoja. Seveda si bomo tudi v prihodnje prizadevali za tesno sodelovanje, saj le s skupnimi močmi lahko dvignemo nivo zagotavljanja kibernetske varnosti v Sloveniji in širše. ■

Foto: arhiv URSIV

Z matričjem do varne omrežne arhitekture

Z vpeljavo omrežne tehnologije matričja t. i. Fabric povečajte odpornost na napredne kibernetske grožnje.

- Preprečite premikanje napadalca v notranjem omrežju
- Preprečite prehod skozi stranska vrata
- Zmanjšajte površino napada
- Omejite vidljivost omrežne infrastrukture
- Zagotovite popolno izolacijo kritičnih naprav
- Zagotovite učinkovito delovanje varnostnih mehanizmov



Naredite več z manj

SMART COM

UDEJANJAMO VAŠE VIZIJE

www.smart-com.si

Extreme networks

Tehnološki partner

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Janez Anžič, direktor Operativno-storitvenega centra Telekoma Slovenije*

BREZ PODPORE SODOBNEGA VARNOSTNO OPERATIVNEGA CENTRA SI TEŽKO ZAMIŠLJAMO USPEŠNO DELOVANJE ORGANIZACIJ

Varnostno okolje je postalo preveč zahtevno, tako da si brez podpore sodobnega varnostno operativnega centra težko predstavljamo učinkovit sistem zagotavljanja kibernetske varnosti. Telekom Slovenije na tem področju sledi začrtani strateški poti razvoja te pomembne storitve. Operativno-storitveni center združuje nadzorno-operativni center, v katerem Telekom Slovenije skrbi za nadzor omrežja, in Center kibernetske varnosti in odpornosti, ki ga Telekom Slovenije uporablja tako za lastne potrebe kot za zagotavljanje varnosti svojih uporabnikov, podjetij ter organizacij in dogodkov. Z direktorjem omenjenega centra smo se pogovarjali o izzivih, razvoju in načrtih na področju zagotavljanja kibernetske odpornosti.

Ob pospešenih korakih digitalizacije in informatizacije so kibernetska tveganja postala zelo izpostavljena stalnica poslovanja naših organizacij. Lahko ocenite, kako močno smo izpostavljeni tem varnostnim tveganjem?

Izpostavljenost varnostnim tveganjem postaja čedalje večja, samo zavedanje, da so organizacije in podjetja tem tveganjem izpostavljena, pa temu nujno ne sledi. Tudi v našem Centru kibernetske varnosti in odpornosti, ki smo ga vzpostavili pred šestimi leti, že od samega začetka delovanja beležimo konstanten porast različnih varnostnih dogodkov. Pričakujemo, da se bo z nadaljnjo digitalizacijo in informatizacijo poslovnih in drugih procesov ta trend le še nadaljeval.

Vodite Operativno-storitveni center Telekoma Slovenije, del katerega je tudi Center kibernetske varnosti in odpornosti, ki iz več zornih kotov predstavlja pomembno zmogljivost na področju obvladovanja kibernetskih tveganj. Nam lahko zaupate, zakaj ste se odlo-

V Centru kibernetske varnosti in odpornosti strokovnjaki Telekoma Slovenije ob pomoči sodobne tehnologije varnostne dogodke podrobno spremljajo, analizirajo in se nanje odzivajo 24 ur na dan. Lahko bi rekli, da upravljajo zaznavanje, odziv in odpornost.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



čili, da ob kibernetski varnosti posebej izpostavite tudi odpornost delovanja organizacij?

Pomembno je razumeti, da kibernetski napadi lahko povzročijo resno škodo, tako posameznikom kot organizacijam, vključno s krajo podatkov, izsiljevalskimi napadi, motnjami delovanja oz. poslovanja ter z drugimi oblikami zlonamernih aktivnosti. Pred tem nobeni sistemi in organizacije niso popolnoma varni, zato je treba zagotoviti zadosten nivo odpornosti delovanja predvsem za primere, ko se organizacija ne uspe ubraniti pred varnostnim incidentom. Odpornost delovanja postaja tako čedalje bolj pomembna, nanaša pa se predvsem na sposobnost organizacij, da oblikujejo ustrezne načrte za učinkovito omejevanje in obvladovanje potencialne škode ter načrte za zagotavljanje nadaljnjega delovanja kritičnih storitev in sistemov v primeru varnostnega incidenta. Ustrezna odpornost delovanja pomeni, da se organizacije v primeru napada hitro odzovejo, hitro prožijo ukrepe za okrevanje po napadu za obvladovanje škode ter hkrati ohranjajo svojo operativno sposobnost – to je pomembno predvsem v kritični infrastrukturi. Če uspe organizacija ohranjati visoko stopnjo odpornosti, se poveča tudi zaupanje deležnikov – za nas so to naročniki, stranke, poslovni partnerji, druge organizacije, s katerimi sodelujemo, ter tudi zaposleni in vodstvo.

Omenjeni center je po mnogih ocenah verjetno center z najvišjo stopnjo operativne zrelosti v Republiki Sloveniji. Nam lahko na kratko opišete razvojne stopnje, da ste uspeli center razviti do trenutne stopnje pripravljenosti za operativno delovanje?

Center kibernetske varnosti in odpornosti smo razvili iz že vgrajene informacijske varnosti in procesnega delovanja v Telekomu Slovenije. Pri tem smo želeli svoje znanje in izkušnje prenesti tudi na področje zagotavljanja kibernetske varnosti, ker pa je bil tovrsten center za vse v naši organizaciji nekaj novega, je pot do trenutnega stanja v veliki meri temeljila na vpeljavi najbolj učinkovitih praks s področja zagotavljanja informacijske varnosti. Sestavni del razvoja, da smo center razvili na tako visok nivo operativnosti, so bila strokovna izobraževanja in certificiranje tako zaposlenih strokovnjakov kot centra samega. Tako smo Center kibernetske varnosti in odpornosti certificirali po mednarodnih standardih ISO 27001 in ISO 22301. Ob širitvi obsega dela je k trenutni stopnji operativnosti seveda prispevalo tudi pridobivanje oziroma zagotavljanje zadostnega števila strokovnjakov za kibernetsko varnost, zaradi katerih lahko center deluje 24 ur na dan, vse dni v letu. Izjemno pomembno je, da center stalno razvijamo, pregledujemo in optimiziramo obstoječe postopke in procese. Razvoj je v veliki meri pogojen s stalnim prilagajanjem spremembam v okolju in izboljševanjem. V zadnjem obdobju razvojni cikel vključuje visoko stopnjo avtomatizacije, uporabo umetne inteligence, pregledovanje informacij (groženj) v različnih okoljih (temni splet, različni kanali, objave ukradenih podatkov,...), kar nam omogoča učinkovito zaznavo in odziv za dvig odpornosti na kibernetskem področju.

Katere so tiste zmogljivosti, na katere ste še posebej ponosni v Centru kibernetske varnosti in odpornosti?

Zadovoljni smo predvsem s tem, da smo uspeli vzpostaviti učinkovite sisteme zaznavanja in odzivanja na številne var-

nostne dogodke in potencialne kibernetske grožnje, pri čemer uporabljamo kombinacijo različnih tehnologij in sodobnih metod za prepoznavanje, odzivanje in analizo aktivnosti znotraj omrežij in sistemov. Posledično se lahko v našem centru zelo hitro odzovemo na varnostne dogodke ter sprejemamo hitre in učinkovite ukrepe za zamejitev potencialnih napadov. K temu prispevajo tudi dobro dodelani postopki in operativni načrti za obravnavo varnostnih dogodkov, ki jih glede na potrebe stalno posodabljamo, kar je ključno za učinkovit odziv.

Veliko pozornosti namenjamo pro aktivnosti in preventivnemu delovanju, kar pomeni, da stalno spremljamo in ocenjujemo potencialna varnostna tveganja. S tem lahko pravočasno identificiramo nove grožnje in varnostne ranljivosti ter sprejemamo ustrezne preventivne in korektivne ukrepe za celoviti izboljšanje stopnje kibernetske varnosti in odpornosti.

Pri vsem tem so seveda izjemno pomembni naši zaposleni, ki so ustrezno certificirani ter usposobljeni za hitro in učinkovito odzivanje. Naši strokovnjaki stalno nadgrajujejo svoje znanje in veščine, za kar skrbimo tako z internimi kot eksternimi izobraževanji, usposabljanji ter pridobivanjem izkušenj z aktivnim sodelovanjem v okviru mednarodnih vaj.

Vse navedeno prispeva k temu, da smo se uveljavili, kot trenutno verjetno najbolj zmogljiv center kibernetske varnosti in odpornosti na področju zagotavljanja kibernetske varnosti in odpornosti v Sloveniji.

Kadrovski potencial je izziv v vseh organizacijskih okoljih. Če govorimo o visoko specializiranem kadru na področju informacijske varnosti, pa je pomanjkanje še bolj izrazito. Kako uspete zagotoviti ustrezen kadrovski potencial za delovanje centra v obsegu 24/7/365?

Sodelavke in sodelavce pridobivamo tako z zunanjimi kot notranjimi razpisi, tesno sodelujemo s srednješolskimi in visokošolskimi izobraževalnimi programi, za mlade organiziramo lastne razvojno-izobraževalne programe, kakršen je bil naš TRIP 2023, prisotni smo na kariernih tržnicah, omogočamo štipendije, opravljanje prakse ter mentorstvo. Mladim omogočamo razvoj kariere in delo z najbolj naprednimi tehnologijami in sistemi za kibernetsko odpornost, pa sodelovanje z vrhunskimi strokovnjaki. Razvili smo tudi program vključevanja etičnega hackinga za dvig odpornosti na vseh segmentih omrežja in storitev.

Pri pridobivanju novih sodelavk in sodelavcev upoštevamo njihovo obstoječe znanje, strokovno izobrazbo ter izkušnje na področju informacijske in kibernetske varnosti in povezanih področjih. Kot je bilo že večkrat poudarjeno, za ustrezno usposobljenost zaposlenih skrbimo z neprestanim izobraževanjem in omogočanjem strokovnega razvoja. Brez tega si razvoja področja kibernetske in informacijske varnosti ni mogoče predstavljati. Pri pridobivanju strokovnjakov je delno izziv ta, da delo v našem centru poteka tudi v popoldanskem in nočnem času ter med vikendi in prazniki, vendar zaenkrat te izzive uspešno rešujemo.

K privabljanju potencialnih sodelavk in sodelavcev nenazadnje pripomore tudi to, da je Telekom Slovenije stabilno in ugledno podjetje ter da je naš Center kibernetske varnosti in odpornosti dobro prepoznan kot najbolj zmogljiv tovrstni center v Sloveniji.

Imate za nadaljnje razvojne korake centra ustrezno podporo strateškega vodstva organizacije?

Da, zagotavljanje varnosti je strateška prioriteta Telekoma Slovenije. Vodstvo podpira nadaljnji razvoj Centra za kibernetsko varnost in odpornost ter stalnemu nadgrajevanju naših zmogljivosti namenja veliko pozornosti. To se odraža na različnih ravneh - tako skozi močno podporo strokovnemu izobraževanju in ozaveščanju vseh zaposlenih, kot skozi vlaganja v dvig informacijske varnosti v omrežjih in storitvah.

Nadaljnji razvoj centra bo povezan s širitvijo obsega dela, s čimer se bo v prihodnosti verjetno povečevala tudi potreba po dodatnih strokovnjakih. Je pa na tej točki potrebno poudariti, da so nasploh na področju kibernetske varnosti kadrovske potrebe dejansko večje od razpoložljivih strokovnjakov; tudi globalno se organizacije srečujejo s tovrstnim izzivom.

Vaše storitve uporablja vedno več slovenskih organizacij, sploh večjih organizacijskih sistemov. Je cilj, da se v okviru enovite podpore Centra za kibernetsko varnost in odpornost v prihodnje združijo vse organizacije, ki v Sloveniji upravljajo s kritično infrastrukturo?

Odločitev o takšni organizaciji dela ostalih upravljalcev kritične infrastrukture ni v naši pristojnosti. Naše storitve so na voljo vsem zainteresiranim subjektom na trgu. Glede na

V letu 2023 so zaznali kar za 85 % več varnostnih incidentov kot v letu pred tem. Vse več je zlorab osebnih podatkov, vključno z gesli in podatki plačilnih kartic. Največ varnostnih incidentov je povezanih z aktivnostmi posameznikov na spletu. Uporabniki pogosto ignorirajo pravila varne rabe interneta ali podcenjujejo nevarnosti, strokovnjaki Telekoma Slovenije zaznavajo napačno vnašanje gesel, namestitve nedovoljene programske opreme, obiske zlonamernih spletnih strani, napade onemogočanja (DDoS). Zelo pogosto se dogaja, da se uporabniki na različnih digitalnih platformah, pa naj gre za profile na družbenih omrežjih ali spletne strani, trgovine, spletne banke in ostale platforme, prijavljajo z vedno istimi uporabniškimi podatki in gesli. Pri tem napadalci vse pogosteje aktivno iščejo tudi pomanjkljivosti sistemov in poslovnih procesov s poskusi skeniranja omrežja in s tem iskanja morebitnih ranljivosti.



omejitve v smislu razpoložljivosti strokovnjakov ter sistemov za najnaprednejše zagotavljanje kibernetske odpornost pa bi bilo vsekakor smiselno razmišljati o sinergijah na nivoju upravljalcev kritične infrastrukture. Tovrstno poslovno sodelovanje ima potencial za zagotavljanje koordiniranega in učinkovitega odzivanja na varnostne dogodke in kibernetske grožnje ter bi lahko posledično izboljšalo zaščito kritične infrastrukture, ki je ključna za delovanje države. Potencialno bi bilo odkrivanje, analiziranje in odzivanje na varnostne dogodke na nacionalni ravni lahko še hitrejše, organizacije bi med seboj lahko bolj enostavno delile informacije o grožnjah, ranljivostih in najboljših praksah, zagotovljeni bi bili enotni varnostni standardi in politike za usklajeno varovanje kritične infrastrukture pred kibernetskimi grožnjami. Hkrati bi takšen način dela lahko dodatno podprl razvoj in izvajanje celovitih strategij kibernetske varnosti za ključne sektorje in storitve. Ampak počakajmo, kaj bo na tem področju prinesel čas.

Ste pri svojem delovanju usmerjeni zgolj na slovensko tržišče ali se tudi s tem segmentom širite v širši regijski prostor?

Trenutno smo v določeni meri že prisotni v tujini in zagotavljamo učinkovito obravnavo varnostnih dogodkov tudi mednarodnim podjetjem in organizacijam. Tudi v prihodnje bo eden izmed naših ciljev še okrepiti svojo prisotnost, prepoznavnost in sodelovanje v mednarodnem prostoru.

Slovensko združenje za korporativno varnost predstavlja pomembno varnostno platformo. Menite, da je to tisti okvir, ki ga je potrebno še močneje izkoristiti za dvigovanje varnostnega zavedanja o pomenu podpore, ki jo na področju kibernetske varnosti lahko prinesejo zmogljivosti, kot jih predstavlja Center kibernetske varnosti in odpornosti?

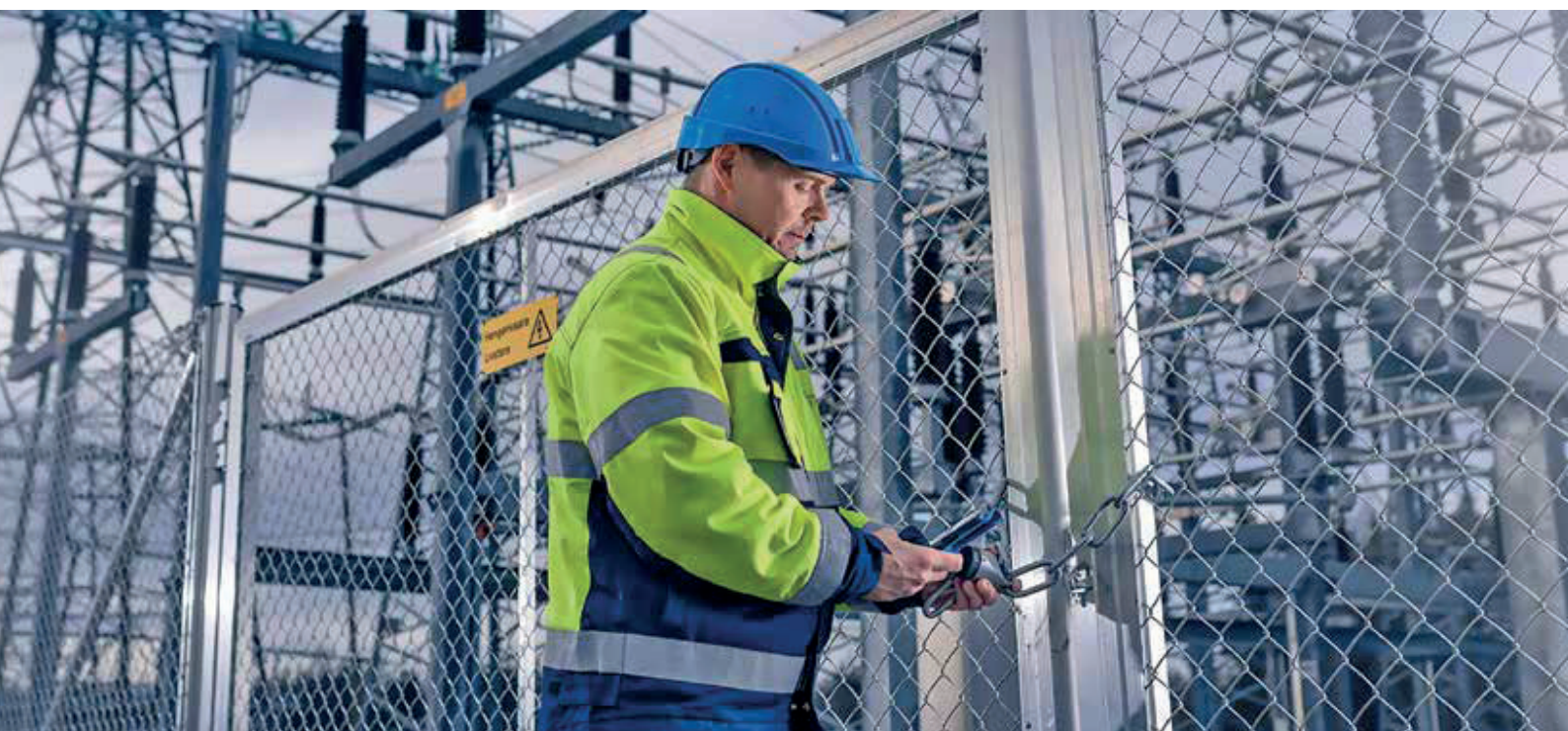
Slovensko združenje za korporativno varnost ima pomembno vlogo pri krepitvi varnostne kulture in zavedanja na področju korporativne, informacijske in kibernetske varnosti v Sloveniji. Delovanje takšnega združenja oziroma platforme je lahko pomembno predvsem za izmenjavo znanja, najboljših praks in izkušenj med strokovnjaki ter posledično za spodbujanje razvoja naprednih varnostnih rešitev. Seveda ima lahko takšna platforma pomembno aktivno vlogo pri promociji kibernetske varnosti in s tem povezanih centrov, kot je na primer tudi Telekomov Center kibernetske varnosti in odpornosti. Tudi v prihodnje bo pomembna skrb za dvig zavedanja o grožnjah, širjenje znanj in izkušenj preko izobraževalnih dogodkov, podporo pri implementaciji varnostnih standardov ter spodbujanje sodelovanja med različnimi deležniki. Ta pristop, ne le znatno prispeva k dvigu varnostnega zavedanja in odpornosti na kibernetske grožnje, ampak je ključen za gradnjo varnih digitalnih okolij v Sloveniji. ■

Foto: arhiv Telekom Slovenije, d.d.

DIGITALNI SISTEM ZAKLEPANJA ZA KRITIČNO INFRASTRUKTURO

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

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



BREZ BATERIJ IN KABLOV • BREZ STROŠKOV VZDRŽEVANJA • ZELENA REŠITEV

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

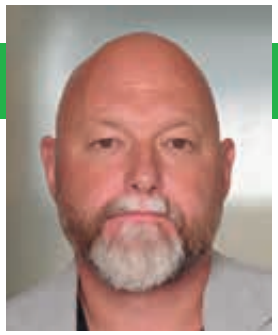


IDealni partner za identifikacijo in varnost

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

iLOQ

Avtor: pred. mag. Marko Potokar*



KOLUMNA

ZAČETEK KONCA ALI APOKALIPSA ZDAJ – RESNO?

Vojne, suša, lakota, povodnje, globalno segrevanje, pandemije, podnebne spremembe, kibernetski napadi, spletno nasilje, grožnje zasebnosti, popolni nadzor, razpad zdravstvenega sistema in vrednot, grožnja prevlade umetne inteligence in še in še. Smo res prišli do konca? Je to zaton civilizacije? Dvomim. Imam argument: jezdeci apokalipse so štirje, pa še ti, tako se govori, morajo zniževati stroške, dodatnega kadra pa ne smejo zaposlovati (morda študente in prekarce, kar pa ni dovolj). Torej je logična implikacija, da se bodo slej ko prej izčrpali – skratka ne bo jim uspelo. Gremo naprej!

Na enem izmed medijskih portalov je bila devetega aprila objavljena novica, da je evropsko sodišče za človekove pravice zavrglo tožbo šestih mladih proti dvaintridesetim državam, ker naj bi te nezadostno ukrepale proti podnebnim spremembam. Očitek je bil, da »s takim ravnanjem ne bodo dosegle cilja pariškega podnebnega sporazuma o omejitvi globalnega segrevanja na 1,5 stopinje Celzija«. Morda res nič posebnega, a je bila na seznamu držav navedena tudi Slovenija. Pa tudi to ni nič takega, saj je očitek preveč neotipljiv; kaj pa je poldruga stopinja v primeru s siceršnjimi nihanji temperature (pa ne samo fizikalne) v naših krajih. Nas je pa veliko bolj streslo prejšnji dan objavljeno obvestilo policije, prvotno naslovljeno na ravnatelje osnovnih šol, da naj bodo v teh dneh še posebej previdni, saj je bil na spletu objavljen komentar, da se bo desetega aprila tudi pri nas zgodilo nekaj podobnega, kot se je pred dnevi na Finskem. Tam je namreč dvanajstletnik v šoli izvedel strelski napad. Vendar to ni bil prvi tak dogodek na Finskem. Leta 2008 je v tej državi svoj smrtonosni pohod na zdravstveni šoli Kauhajoki pričel dvaindvajsetletni študent Matti Juhani Saari, a finska policija je odreagirala hitro: streljanje se je pričelo približno ob 10:40, intervencijske službe pa so prvi klic dobile ob 10:46. Nekaj minut zatem sta na kraj dogodka prišla policista in takoj pričela ukrepati. Storilec ju je pričakal s streli. Ko so kasneje v objekt vstopili dodatni policisti in naleteli na storilca, se je ta zaprl v sobo in storil samomor. Število žrtev: deset mrtvih, enajst ranjenih.

V policijskem žargonu AMOK situacija opisuje dejanje, ko eden ali več storilcev, na videz brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer je očitno, da s to aktivnostjo ne bo prenehal. Uporablja se tudi izraz aktivna strelska situacija, ki označuje množični umor, pri katerem storilec uporabi strelno orožje. Za množični umor gre, ko je v krajšem času na omejenem geografskem območju ubito večje število ljudi. Navedene situacije se pojmujejo pod skupnim izrazom aktivne življenju nevarne situacije.

Glede opozorila slovenske policije so bila, kot po navadi, mnenja v deželi kranjski deljena. Od »Ah, pretiravajo...« do »Končno varnostnika v vsako vas (no, šolo)«. A tovrstni opredeljenosti sta s koncev intervala mnenj – sta ekstrema, kot je naslednji večer v oddaji Odmevi odlično komentiral eden od povabljenih strokovnjakov. Prva diši po zanikanju;

*avtor je član Slovenskega združenja korporativne varnosti

druga je morda še bolj tvegana, saj je lahko povod uvedbe nesorazmernih ukrepov nadzora in kontrole družbe ter posameznikov.

School shooting je pojem, ki označuje strelske morilske pohode v šolah. Eden najbolj krvavih je znan kot katastrofa v bathskovski šoli (orig.: Bath School disaster). Andrew Philip Kehoe, znan po svoji varčnosti, je bil s strani sokrajanov izvoljen za skrbnika denarja na šoli v Bathu. Zagovarjal je znižanje prispevkov in bil zato večkrat v navzkrižju s preostalimi člani šolskega odbora. Kratek čas je bil tudi občinski uradnik, a ga sokrajani kasneje niso več izvolili. Masovni poboj s štiriinštiridesetimi smrtnimi žrtvami in oseminpetdesetimi ranjenimi (večina je bila otrok med sedmim in dvanajstim letom) je izvedel z detonacijo več sto kilogramov eksploziva, ki ga je več mesecev skrivoma nameščal v kleteh šole. Zgodilo se je 18. maja 1927.

V sedanjosti se je v zahodni družbi za tovrstna dejanja uveljavil izraz AMOK. Pa pojem sploh ni tako nov, niti nima svojega izvora v zahodni kulturi. Ko je kapitan James Cook v času poznega 18. stoletja objavil potopise s svojih obsežnih potovanj po svetu, se je zahodni svet prvič srečal s čudnim pojavom, ki naj bi obstajal med različnimi narodi malezijskega arhipelaga. Med prebivalci Malezije (Malay), ki so sicer sloveli po svoji miroljubnosti (Malay izhaja iz *malu = nežen, nežnost*), so se občasno dogajali primeri izbruha neobvladljivega nasilja brez vidnega razloga ali opozorilnih znakov. V svojih zapiskih je Cook pisal o posameznikih, ki se obnašajo brezumno in nasilno, pri čemer brez razloga ubijajo in pohabljajo ljudi in živali. O pojavu, poznanem pod različnimi imeni, kot so *mengamuk*, *pengamok* ali pa preprosto amok, so poročali tudi še potem, ko je Malezija že postala britansko ozemlje. Eden tipičnih je bil primer iz leta 1891, ko je malezijski kmet Imam Mamat med popravljanjem ograje na svojem posestvu nenadoma pričel pobijati družinske člane in sovaščane. Med morilskim pohodom je Imam z *golakom* (*golak* je mačeti podobno orodje za sekanje) in kopjem ubil šest ljudi, ranil pa štiri. Za posledicami ran, ki jih je med dejanjem prejel tudi sam, je naslednji dan umrl. Sovaščani so o njem vedeli povedati, da je bil do tega dejanja eden najprijaznejših prebivalcev. Na vprašanje, zakaj je postal nasilen, so priče izjavile, da Imam ni vedel, kaj počne ter da ga je obsedel hudič.

Zahodna družba »nerazvitemu« svetu seveda ne more ostati dolžna. V združenih državah je bil amok na podlagi številnih



poročil in študij primerov, ki so pokazali, da je bila večina posameznikov, ki so zagrešili *amok*, duševno bolnih, uvrščen med psihične motnje. Tako DSM-IV (Diagnostični in statistični priročnik duševnih motenj), ki ga je izdalo ameriško psihiatrično združenje, razvršča *amok* na dve uradni kategoriji: *amok* in *beramok*. *Amok* je redkejša oblika pojava in izvira iz besa, užaljenosti ali maščevanja proti posamezniku ali družbi in je tesneje povezan s psihozo, osebnostnimi motnjami, bipolarno motnjo in blodnjami. *Beramok*, ki je pogostejši, je povezan z depresijo in žalostjo, ki izhajata iz izgube, kot je smrt zakonca ali ljubljene osebe, ločitev, izguba delovnega mesta, denarja, moči itd. Povezan je z duševnimi težavami zaradi hude depresije ali druge motnje razpoloženja.

V klinični literaturi objavljene študije primerov *amoka*, ki zajemajo obdobje več kot sto let in posameznike od zgodnje odrasle dobe do srednjih let, nakazujejo, da pojav ni vezan na določeno življenjsko obdobje ali družbeni status. Medtem, ko so bili v večini *amok* primerov storilci nepismeni kmetje ali ribiči, so zabeleženi tudi primeri, ko so bili napadalci uspešni trgovci, vojaki, obrtniki in celo člani kraljeve družine Malezije. V vseh primerih, kjer je uspelo storilcem preživeti in se izogniti zaporu, so se le-ti brez posledic vrnili v prejšnji življenjski tok z malo ali brez ponavljanja nasilja.

Vprašanje, kaj povzroča *amok* vedenje, je desetletja begalo psihiatre in medicinske raziskovalce. Sprva so *amok* povezovali s psiho dinamskimi dejavniki, kot so izguba družbenega položaja, sovražnostjo in pripisovanjem krivde žrtvam, novejše raziskave pa pojav opisujejo kot vedenjski sindrom z različnimi možnimi vzroki, vključno z boleznimi, kot so malarija ali nevrosifilis. V nekaterih primerih je bila kot možen dejavnik predlagana tudi akutna zastrupitev. Ker je večina kliničnih amok primerov diagnosticiranih v zaporih in psihiatričnih bolnišnicah, ni presenetljivo, da so najbolj pogoste psihiatrične diagnoze za storilce shizofrenija in bipolarna motnja. Tako ostaja odprto vprašanje, ali se lahko te diagnoze uporabijo tudi za pojasnilo skrajnega nasilja v amok situacijah izven psihiatričnih in popravnih ustanov.

Poraja se tudi vprašanje, ali se je *amok* pojav sčasoma spremenil. Primeri v Maleziji in Indoneziji so bili pred angleško in nizozemsko zasedbo pogostejši, s pojavom psihiatričnega zdravljenja pa se je obravnava *amoka* in storilcev prenesla za zidove psihiatričnih bolnišnic in zaporov. Tudi uporaba izraza *amok* se je sčasoma spremenila. Čeprav še vedno prihaja do „klasičnih“ *amok* primerov, so Malezijci razširili uporabo izraza na kakršenkoli nenaden izbruh nasilja v Maleziji, povzročen s strani Malezijca ali tujca. Izraz *amok* se sicer drugje po svetu uporablja za označitev pojava množičnih umo-

Kot je razvidno iz obravnavanih primerov, se AMOK situacije bistveno razlikujejo od klasičnih nasilnih situacij in dejanj oziroma kršenj javnega reda in miru. V primeru AMOK situacije gre namreč za dejanja, ki so neposredno usmerjena proti življenju posameznikov, storilec pa se ne oziroma se ni pripravljen pogajati, ampak izvaja pomor.

rov (mass murders, spree killing), vendar ne smemo prezreti, da med njimi obstajajo pomembne razlike. Čeprav se izbruhi nenadnega nasilja dogajajo po vsem svetu, pojav *amok* v svoji osnovi neposredno izhaja iz tradicij lokalnih kultur.

V policijskem žargonu AMOK situacija opisuje dejanje, ko eden ali več storilcev, na videz brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer je očitno, da s to aktivnostjo ne bo prenehal. Uporablja se tudi izraz aktivna strelska situacija, ki označuje množični umor, pri katerem storilec uporabi strelno orožje. Za množični umor gre, ko je v krajšem času na omejenem geografskem območju ubito večje število ljudi. Navedene situacije se pojmujejo pod skupnim izrazom aktivne življenju nevarne situacije.

Seveda nas etimologija ne bo rešila v primeru pojava take situacije. Kako nas torej lahko varujejo varnostni organi?

Naloge in pristojnosti za delovanje policistov so opredeljene v Zakonu o policiji, v katerem so med drugimi opredeljene tudi naloge varovanja življenja in osebne varnosti. Vsakdo, čigar življenje oziroma osebna varnost ali premoženje so ogroženi ali kdor je žrtev kaznivega dejanja ali prekrška, sme zahtevati pomoč oziroma posredovanje policije. Na kraju posredovanja so policisti dolžni najprej vzpostaviti javni red in mir, če je ta ob njihovem prihodu še vedno kršen, in preprečiti morebitno nadaljnje ogrožanje varnosti oziroma izvajanje kakršnekoli oblike nasilja. Javni red in mir skušajo najprej zagotoviti s svojo navzočnostjo in z opozarjanjem oziroma ukazovanjem. Če to ne zadošča, morajo za vzpostavitev javnega reda in miru uporabiti prisilna sredstva. Policisti smejo uporabiti le tisto prisilno sredstvo, ki je sorazmerno načinu in moči upiranja ali napada. Pri uporabi prisilnih sredstev morajo spoštovati človekovo osebnost in njegovo dostojanstvo. Če smejo uporabiti več prisilnih sredstev hkrati, smejo hujše prisilno sredstvo uporabiti le, če je bila uporaba milejšega sredstva neuspešna ali če zaradi okoliščin in razlogov za varnost življenja, osebno varnost ali varnost premoženja ljudi ne bi bila mogoča. Za preprečevanje negativnih posledic takih protipravnih ravnanj je zelo pomembno, da so policisti ustrezno strokovno usposobljeni. Temu je namenjena redna vadba praktičnega postopka in samoobrambe, saj je treba prisilna sredstva uporabljati zakonito in strokovno, predpogoj za njihovo uporabo pa je, da se policisti znajo ubraniti napada nase in nato ustrezno ukrepati.

Kot je razvidno iz obravnavanih primerov, se AMOK situacije bistveno razlikujejo od klasičnih nasilnih situacij in dejanj oziroma kršenj javnega reda in miru. V primeru AMOK situacije gre namreč za dejanja, ki so neposredno usmerjena proti življenju posameznikov, storilec pa se ne oziroma se ni pripravljen pogajati, ampak izvaja pomor. Poraja se vprašanje, ali so policisti, ki prvi pridejo na kraj dogajanja, pripravljeni in ustrezno usposobljeni za ravnanje v tako kritični in življenjsko ogrožajoči situaciji. Imajo potrebno znanje in izkušnje, so dovolj izurjeni, vedo kako ukrepati in nenazadnje, je njihova oprema ustrezna?

Kaj pa varnostno osebje zasebnih varnostnih služb? Pravzaprav so varnostniki »prva bojna linija« za preprečevanje neprimernih in nezakonitih aktivnosti v organizacijah, kjer opravljajo svoje delo. Poleg vprašanja, ali so usposobljeni in primerno opremljeni tudi za ravnanje v izjemno nasilnih situacijah, obstaja tudi omejitev njihovih pooblastil. Podlaga za delovanje in ukrepanje varnostnika je namreč Zakon o zasebnem varovanju, ki ne vsebuje določil o ravnanju varnostnika v izrednih situacijah in ga k temu tudi ne zavezuje. Seveda mora varnostnik svojo službo opravljati vestno in pozorno spremljati okolico in dogajanje na varnostnem območju, preverjati prisotnost sumljivih predmetov in oseb ter ves svoj delovni čas preventivno delovati. Pa vendar je dovolj, da v primeru hujših oblik nasilja samo pokliče policijo ali pa intervencijsko službo, ki jo opravljajo njegovi kolegi? Tudi v tem primeru je na preizkušnji ustrezna usposobljenost, vključujoč znanje, izkušnje in izurjenost ter ustrezna opremljenost.

Kako pa je s pripravljenostjo organizacij v javnem in zasebnem sektorju? ZVZD-1 kot krovni predpis na področju varnosti in zdravja pri delu določa pravice in dolžnosti delodajalcev in delavcev v zvezi z varnim in zdravim delom ter ukrepi za zagotavljanje varnosti in zdravja pri delu. Določbe tega zakona se uporabljajo v vseh dejavnostih za vse osebe, ki so navzoče v delovnem procesu. Z vidika zagotavljanja osebne varnosti zaposlenih je pomembna določba, ki določa, da mora delodajalec načrtovati postopke za zmanjšanje nevarnosti za nasilje tretjih oseb. V prvem odstavku 23. člena ZVZD-1 je namreč opredeljeno, da mora delodajalec na delovnih mestih, kjer obstaja večja nevarnost za nasilje tretjih oseb, poskrbeti za tako ureditev delovnega mesta in opremo, ki tveganje za nasilje zmanjšata in ki omogočata dostop pomoči na ogroženo delovno mesto. Nadalje je v tem členu določeno tudi, da mora delodajalec načrtovati postopke za primere nasilja iz prvega odstavka tega člena in seznaniti z njimi delavce, ki na takih delovnih mestih delajo.

Smo zaradi določil zakonov državljani res varni?

Katerakoli razlaga pojava izbruha nekontroliranega nasilja je pravilna, je dejstvo, da imamo človeška bitja nasilje v sebi. Kdaj in na kakšen način nasilje izbruhne, je odvisno od vzgoje, situacije in samokontrole, zato bi se v družbi moralo poudariti širjenje znanja in zavedanja o varnostni kulturi ter vzgoji za nenasilje, ki je eden od mehanizmov, s katerim bi lahko povečali varnost. In ne glede na (ne)pripravljenost uradnih in neuradnih organov ter inštitucij, ne smemo pozabiti, da sta najboljša zaščita in obramba preprečevanje ter lastna ozaveščenost in skrb za varnost. Za lastno varnost smo namreč v prvi vrsti odgovorni sami.

Tokrat nas ni zadelo. Kaj pa jutri? Ne čakajmo, da se zgodi, ampak začnimo s sistematičnim izobraževanjem in usposabljanjem ter samozaščitnim ravnanjem vseh nas. Najprej moramo narediti miselni preskok (»To se lahko zgodi tudi pri nas.«), nato še čustveni (»Kar naležim se, ko pomislim, kaj se lahko zgodi.«). Kar pogumno, čaka nas veliko dela. ■

A1 Business

Razumemo
kibernetsko varnost.
Z mednarodnimi izkušnjami.



Matic Grobelšek
Direktor za poslovni trg
A1 Slovenija

"Prednost Skupine A1 je sodelovanje in usklajevanje obrambnih taktik ter odzivov na kibernetske grožnje na mednarodni ravni med več kot 200 izkušenimi varnostnimi inženirji iz različnih držav. Naš skupni cilj je dosledno uveljavljanje visokih standardov in nenehna krepitev kompetenc na področju kibernetske varnosti.

Zagotavljamo celovite varnostne preglede, izvajamo aktivnosti socialnega inženiringa, nudimo učinkovite varnostne in IT storitve ter vzpostavljamo in zagotavljamo najsodobnejše varnostne rešitve po meri.

Razumemo digitalno, da lahko vaš posel teče nemoteno."

Več

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Robert Bergles in **g. Vladimir Ban**, A1 Slovenija d.d.*

NOVI IZZIVI NA PODROČJU KIBERNETSKE VARNOSTI - MOČAN DEJAVNIK PRI RAZVOJU SEKTORJA TELEKOMUNIKACIJ

Kibernetski izzivi vedno bolj vplivajo na delovanje ključnih organizacij. Organizacije v sektorju telekomunikacij so temu še posebej izpostavljene. Učinkovita varnost, ki se zagotavlja pri delovanju tega pomembnega sektorja, ima neposreden in posreden vpliv tudi na vse ostale sektorje družbe. Zaradi navedenega je razvoj novih pristopov na področju kibernetske varnosti še toliko bolj pomemben. Z nami sta podelila nekaj strateških misli g. Robert Bergles, vodja informacijske varnosti (CISO) in g. Vladimir Ban, strokovnjak za kibernetsko varnost, oba iz A1 Slovenija.

Katere so glavne napake zaposlenih, ki jih opažate skozi svoje delovanje pri varnostnih pregledih v organizacijah? Kakšni so izzivi in kako premagati šibke točke?

Vladimir Ban: Zaposleni imajo seveda pomemben vpliv na nivo informacijske varnosti svoje organizacije. Zato moramo na nivoju nastavitev pravic in tehničnih rešitev poskrbeti, da se njihov vpliv na informacijsko varnost čimbolj omeji.

Zaposleni imajo seveda pomemben vpliv na nivo informacijske varnosti svoje organizacije. Zato moramo na nivoju nastavitev pravic in tehničnih rešitev poskrbeti, da se njihov vpliv na informacijsko varnost čimbolj omeji.

Najpogostejši napaki, ki ju srečujemo ob varnostnih pregledih, sta naslednji:

Zaposleni napačno odreagirajo na poizkus prevare (recimo na phishing e-mail sporočilo in podobno). Brez razmisleka izdajo svoje geslo napadalcem oz. zaženejo kodo, ki jim jo podtakne napadalec.

Zaposleni pogosto slabo skrbijo za svoja gesla. Bodisi so gesla preveč enostavna in predvidljiva, bodisi z geslom ne ravnajo tako, kot bi z gesli morali ravnati (ga posredujejo drugim sodelavcem, imajo v nekodirani obliki shranjenega v datoteki, dostopni ostalim uporabnikom, ipd.)

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Kako v A1 razumete matriko kibernetske varnosti, ki naj bi zagotavljala usmerjanje malih in srednjih podjetij ter korporacij k učinkovitim varnostnim strategijam?

Vladimir Ban: Matrika kibernetske varnosti je preprosto povedano seznam stvari, ki jih moramo imeti in narediti, da bi bila naša varnost takšna, kot si želimo.

Izziv pri tej matriki (posebej, ko govorimo o manjših in srednjih podjetjih) je, da v matriko ne moremo vstaviti vsega, kar bi bilo priporočljivo. Namreč manjša in srednja podjetja večinoma nimajo na voljo dovolj časa, človeških virov in denarja, da bi naredila vse, kar si morda želijo.

Pomembno je torej, da smo pri sestavi matrike kibernetske varnosti, kar se le da, najbolj optimalni. Vedno je smiselno z manj narediti več.

Kadrovski potencial je postal izziv vseh organizacijskih okolij. Kako se pri A1 s tem spoprijemate, predvsem na specifičnem področju informacijske varnosti?

Vladimir Ban: S pomanjkanjem specifičnega kadra se seveda spopadamo tudi v A1, zato aktivno delamo predvsem na dveh nivojih:

Ustvariti je potrebno dovolj trden »zgornji« sloj izkušenih kadrov, ki poskrbijo za trdno osnovo ekipe, ki se ukvarja s kibernetsko varnostjo. Ustvariti je potrebno kvaliteten sistem notranjega izobraževanja, prenosa znanja in izkušenj ter »mentorstva« pri uvajanju novih, manj izkušenih kadrov. Vedno bo sicer določen (morda celo večinski) del kadra imel manj izkušenj na tem področju.

Na splošno pa menim, da nam je v oddelku poslovne prodaje A1 Slovenija, v katerem deluje ekipa, ki skrbi za naše poslovne stranke na področju informacijske varnosti, to kar dobro uspelo. To se odraža tudi v velikem številu strank, s katerimi sodelujemo že več kot desetletje in se zanašajo na naše znanje in sposobnost prilagajanja ponudbe glede na razvoj, spremembe na področju informacijske varnosti in nenazadnje njihove potrebe.

Vaša dolgoletna strokovna pot vas je pripeljala v A1, kjer trenutno opravljate zahtevne naloge vodje informacijske varnosti (CISO). Kako vi ocenjujete, da se področje telekomunikacij razlikuje od ostalih področij s perspektive zagotavljanja kibernetske varnosti?

Robert Bergles: Ko govorimo o kibernetski varnosti je področje telekomunikacij zaradi svoje narave izjemno specifično. Telekomunikacijska omrežja so obsežna in sestavljena iz različnih tehnologij, ki se prepletajo. Če imamo na eni strani preprosto ožičenje, imamo na drugi strani velike količine prenosa in obdelave podatkov, zahtevne procese šifriranja in varovanje osebnih in drugih tajnih podatkov.

Naše telekomunikacijsko omrežje je del kritične infrastrukture, kar pomeni, da imajo lahko morebitni izpadi ali varnostni incidenti daljnosežne posledice, ne samo za posamezne uporabnike, ampak tudi za gospodarstvo in družbo kot celoto. Poleg tega smo zaradi pomembnosti in dostopnosti telekomunikacijskih omrežij pogosto tarča napadov. Zaradi

tega se soočamo s strogimi regulativnimi zahtevami, neprestano moramo slediti tehnološkim inovacijam, kot so 5G, IoT in oblačne storitve, te pa zahtevajo nenehno prilagajanje in izboljševanje naših varnostnih strategij.

Moja vloga je zagotoviti, da so naše strategije vedno usklajene s trenutnimi grožnjami in tehnološkim napredkom, ter da je naša ekipa ustrezno usposobljena in pripravljena na izzive, ki jih prinašajo te spremembe.

CISO ima v vsaki organizaciji izredno zahtevno vlogo, da na eni strani zagotavlja uveljavljanje ključnih varnostnih standardov na področju informacijske varnosti, na drugi strani pa je potrebno znati motivirati zaposlene, da razumejo potrebo po visokem varnostnem zavedanju. Kako vam uspeva združiti ta dva, včasih med seboj ne ravno najbolj usklajena procesa?

Robert Bergles: Nenehno moram slediti tehnično naprednim varnostnim rešitvam in biti aktiven na varnostnih forumih, saj mi to omogoča, da ostanem v koraku z najnovejšimi grožnjami in trendi, hkrati pa spodbuja izmenjavo znanja in izkušenj z drugimi strokovnjaki na področju kibernetske varnosti.

Vodja informacijske varnosti je ključni steber pri oblikovanju zavedanja in razumevanja realnih informacijskih tveganj znotraj organizacije. Pomembno je, da se vodstvo in zaposleni zavedajo, da informacijska tveganja niso več le občasni izzivi, temveč stalnica našega vsakdanjega operativnega okolja.

Zavedanje, da varovanje informacij zahteva določene omejitve in prepovedi v načinih dela, poudarja nujnost odlične komunikacije z zaposlenimi in izkazuje potrebo po neomajni podpori vodstva, ki se mora dosledno držati teh ukrepov.

Moja naloga je poskrbeti, da so varnostni standardi v naši organizaciji, ne le dosledno upoštevani, temveč tudi celovito integrirani in široko cenjeni, kar zagotavljam s kombinacijo jasnih komunikacijskih strategij, tehnološke podpore in vključevanja zaposlenih v procese oblikovanja varnostnih politik.

V proces oblikovanja varnostnih politik vključujemo vse zaposlene iz vseh oddelkov. To povečuje občutek pripadnosti in osebne odgovornosti za varnost podjetja, hkrati pa omogoča oblikovanje rešitev, ki so prilagojene specifičnim potrebam in izzivom posameznih oddelkov.

Pred nami so pomembne spremembe razumevanja delovanja informacijske družbe, kjer so informacijska tveganja postala stalnica našega operativnega okolja. Menite, da se v



organizacijah dovolj dobro zavedamo realnih izzivov pred katerimi se nahajamo?

Robert Bergles: Vodja informacijske varnosti je ključni steber pri oblikovanju zavedanja in razumevanja realnih informacijskih tveganj znotraj organizacije. Pomembno je, da se vodstvo in zaposleni zavedajo, da informacijska tveganja niso več le občasni izzivi, temveč stalnica našega vsakdanjega operativnega okolja. Sam aktivno delujem na tem, da to zavedanje prenesem na vse ravni organizacije, hkrati pa skrbim za implementacijo robustnih varnostnih strategij, ki so prilagojene dinamičnemu razvoju tehnologij in spreminjajočim se grožnjam.

Prav tako redno evalviram in prilagajam varnostne prakse, da so lahko naše obrambe vedno korak pred potencialnimi napadalci. Poleg tega spodbujam kulturo stalnega izobraževanja in osveščanja, kar je ključno za vzpostavitev in vzdrževanje visoke ravni varnostnega zavedanja v organizaciji.

Večkrat imamo občutek, da je razvoj tehnologije hitrejši, kot ga lahko dojame človeški potencial. Menite, da se bo ta razkorak v prihodnje še povečeval ali bomo uspeli z določenimi ukrepi zmanjšati to vrzel?

Robert Bergles: Priznavam, da je razvoj tehnologije pogosto hitrejši od človekovega potenciala dojemanja in prilagajanja tem spremembam. Vendar sem prepričan, da ta razkorak ne bo nujno vedno večji. Močna vloga vodij informacijske varnosti je ključna pri razvijanju strategij, ki ne samo naslavljajo trenutne tehnološke izzive, temveč tudi sistematično razvijajo človeški potencial in kreativnost znotraj organizacije.

Prav tako je pomembno, da sodelujem z vodstveno ekipo, da skupaj oblikujemo vizijo, kako lahko tehnologija služi kot orodje za povečanje zmogljivosti zaposlenih. Tako zmanjšamo vrzel med hitrostjo tehnološkega razvoja in človeškim potencialom, kar vodi k trajnostni rasti in inovacijam znotraj organizacije.

Kako se v A1, kot tehnološko napredni organizaciji srečujete z izzivi izobraževanja in usposabljanja zaposlenih?

Robert Bergles: Prepričan sem, da lahko kljub hitremu tehnološkemu razvoju zmanjšamo razkorak med tehnologijo in človeškim potencialom, s poudarkom na ciljno usmerjenem izobraževanju.

Aktivno sodelovanje v združenju za korporativno varnost ne izboljšuje samo mojega znanja in pripravljenosti na potencialne grožnje, ampak mi hkrati tudi omogoča, da lažje obrazložim potrebo po višjem varnostnem razumevanju pri strateških odločevalcih.

Izjemno pomembno je, da izobraževalne programe prilagodimo potrebam in sposobnostim zaposlenih, pri čemer je ključnega pomena osebni pristop.

V naši organizaciji dajemo prednost praktičnim primerom in interaktivnim delavnicam, ki zaposlenim omogočajo, da znanje takoj uporabijo v praksi, namesto da bi se omejili le na teoretično učenje preko spletnih portalov. Ta pristop ne samo, da spodbuja boljše razumevanje in zadrževanje informacij, temveč tudi povečuje motivacijo in angažiranost zaposlenih. Kot vodja aktivno sodelujem pri oblikovanju teh programov in skrbim, da so naša izobraževanja v koraku s tehnološkimi trendi, hkrati pa zagotavljajo, da tehnologija služi kot podpora zaposlenim, ne pa kot dodatno breme.

NIS direktiva in novo nastajajoči Zakon o informacijski varnosti pred organizacije postavlja veliko večji obseg zahtev, kot smo jih bili vajeni do sedaj. Menite, da bo aktiven pristop h kibernetski varnosti postal ključni element trajnostnega uspeha podjetja v digitalni dobi?

Robert Bergles: Aktiven pristop h kibernetski varnosti vključuje redno posodabljanje in prilagajanje standardov in je nujen za zagotavljanje, da podjetje ne le izpolnjuje zakonske zahteve, temveč tudi proaktivno ščiti svoje vire in informacije v nenehno spreminjajočem se digitalnem okolju. Poleg tega, da tak pristop podjetje aktivno ščiti pred trenutnimi grožnjami, postavlja tudi temelje za trajnostni uspeh v digitalni dobi, kjer je varnost postala kritični element poslovnega uspeha in zaupanja strank.

Vloga NIS2 direktive in novega Zakona o informacijski varnosti je, da postavi osnovne zahteve, ki jih morajo organizacije izpolnjevati za zagotovitev osnovne ravni kibernetske higiene. Te regulative predstavljajo temelj, na katerem morajo podjetja graditi, vendar je ključno, da se organizacije ne zadovoljijo zgolj z izpolnjevanjem minimalnih zahtev. Celovitejši standardi, kot so ISO 27001, ki se osredotoča na vzpostavitev in vzdrževanje informacijskega varnostnega sistema, ISO 22301, ki poudarja pomen obvladovanja neprekinjenosti poslovanja, ter NIST Cybersecurity Framework, ki omogoča celovit pristop k upravljanju kibernetskih tveganj, nudijo okvirje za bolj celostno zaščito.

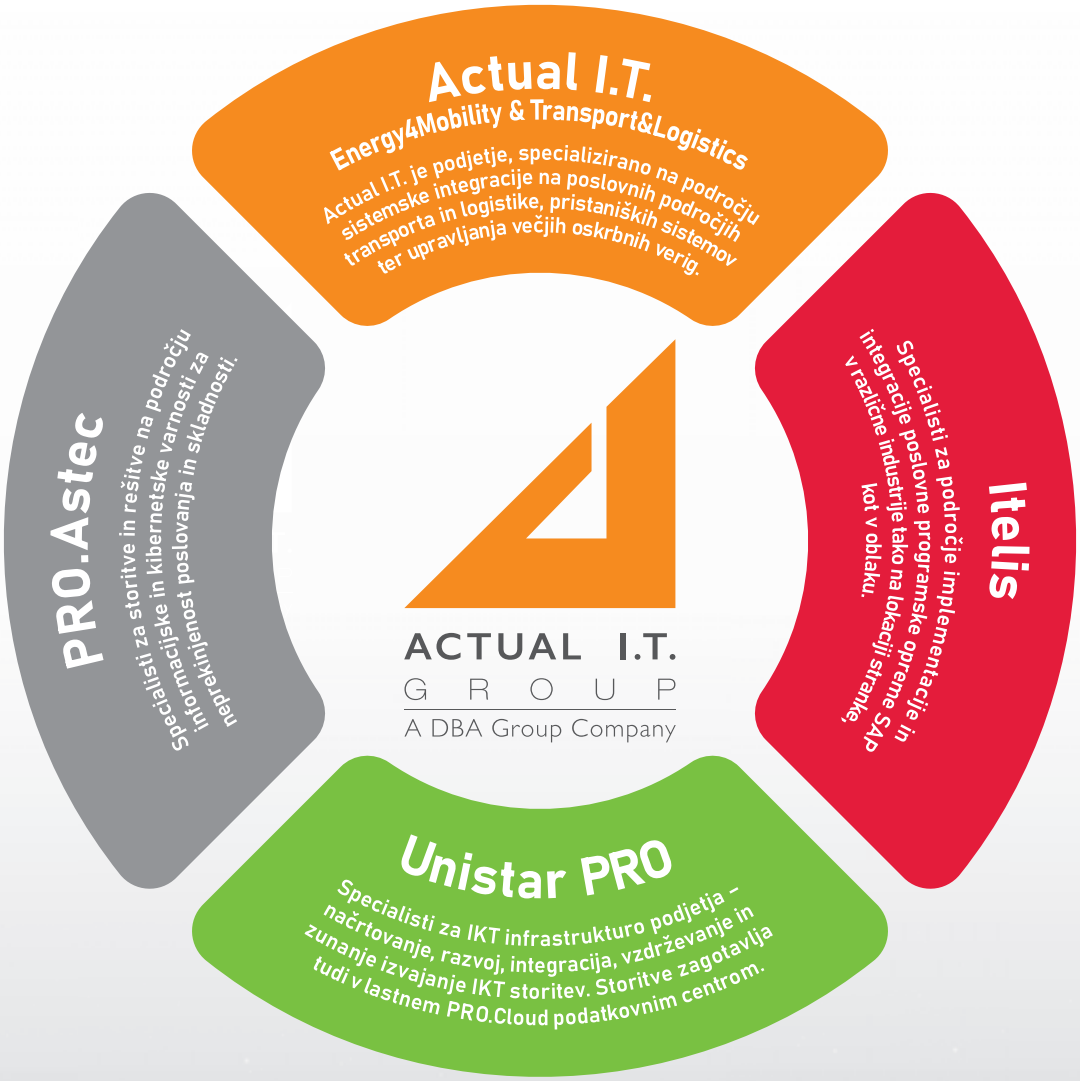
Menite, da lahko s pomočjo Slovenskega združenja za korporativno varnost zagotovite udejanjanje potrebe po višjem varnostnem razumevanju pri strateških odločevalcih, ki nenazadnje odobravajo potrebne investicije na področju informacijske in kibernetske varnosti?

Robert Bergles: Slovensko združenje, ki povezuje različne vrste podjetij, omogoča bogato izmenjavo izkušenj in najboljših praks, kar je izjemno pomembno v kontekstu kibernetske varnosti. Ta izmenjava znanja in izkušenj je neprecenljiva, saj omogoča strateškim odločevalcem, da razumemo kompleksnost in nujnost vlaganja v informacijsko varnost.

Aktivno sodelovanje v združenju za korporativno varnost ne izboljšuje samo mojega znanja in pripravljenosti na potencialne grožnje, ampak mi hkrati tudi omogoča, da lažje obrazložim potrebo po višjem varnostnem razumevanju pri strateških odločevalcih.

Prav tako nam sodelovanje v združenju omogoča, da strateškim odločevalcem predstavimo konkretne primere in scenarije, ki so jih doživela druga podjetja, ter kako so uspešna vlaganja v varnostne rešitve pomagala omiliti ali celo preprečiti te grožnje. ■

Foto: arhiv A1 Slovenija d.d.



ACTUAL I.T. astec ITELIS UNISTAR PRO

IT360°

www.actual-it.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
g. Božidar Dajčman, direktor Oddelka upravljanja fizične in informacijske varnosti v Novi kreditni banki Maribor*

KONSTANTNOST SPREMEMB JE STALNICA PRI DELOVANJU BANČNEGA SEKTORJA

Hitre spremembe, katerim so podvržene organizacije v bančnem sektorju, prinašajo določene izzive, ki so na področju obvladovanja še posebej zahtevne. Če v ta kontekst dodamo še zahtevno varnostno situacijo, lahko z gotovostjo trdimo, da je pred strokovnjaki s področja korporativne varnosti zahtevno obdobje. O teh dinamičnih spremembah in odprtih izzivih smo se pogovarjali z g. Božidarjem Dajčmanom.

Lahko bi ocenili, da ste zelo velik del vaše kariere preživeli v zahtevnem bančnem sektorju. Kateri so tisti varnostni izzivi, ki bodo v prihodnosti najbolj vplivali na razvoj tega sektorja?

Že pred koncem prejšnjega stoletja se je začel trend, ki traja še danes, in to je prehod strank od bančnih okenc na elektronske kanale. Sodeč po informacijah o varnostnih dogodkih v Sloveniji v tem obdobju ugotavljam, da so banke in njihove stranke na elektronsko poslovanje prešle hitreje, kot storilci kaznivih dejanj. Vdori v sisteme bank in naprave uporabnikov elektronskega bančništva niso povzročili visoke škode. Medtem, ko so ropi bančnih poslovalnic in napadi na bankomate še vedno aktualni.

Napadalci so ugotovili, da do računov neprevidnih strank najlažje pridejo s phishingom in da največ zaslužijo s spletnimi prevarami. Te so včasih tako preproste, da bi jih lahko izvajali brez računalnika, včasih pa zahtevajo nekaj tehničnih prijemov. V zadnjem času so najpogostejše prevare, pri katerih žrtve nakazujejo denar za izmišljene, navidezne investicije v kripto valute. Banke vlagajo veliko energije, da svoje stranke zaščitijo, ozaveščajo in izobražujejo, vendar kljub našemu prizadevanju del strank nasede prevarantom. Na področju preprečevanja prevar v prihodnjem obdobju pričakujem veliko dinamiko pri napadalcih in zaščitah. Obe strani bosta vedno bolj uporabljali umetno inteligenco.

Pri varovanju bančnih informacijskih sistemov bomo tudi v prihodnjih letih izpostavljeni podobnim tveganjem kot doslej. Novost je boljše zavedanje, da niso dovolj le ukrepi za preprečevanje napadov, ampak moramo imeti scenarije in rešitve tudi za primer, če zaščite odpovejo in je napad uspešen. Poudarek je torej na izboljševanju sposobnosti okrevanja po napadu.

Menite, da je danes sploh še možno uspešno upravljati organizacije brez upoštevanja varnostnih vplivov iz okolja, ki nas obdaja?

Sodeč po informacijah o varnostnih dogodkih v Sloveniji v tem obdobju ugotavljam, da so banke in njihove stranke na elektronsko poslovanje prešle hitreje, kot storilci kaznivih dejanj. Vdori v sisteme bank in naprave uporabnikov elektronskega bančništva niso povzročili visoke škode. Medtem ko, so ropi bančnih poslovalnic in napadi na bankomate še vedno aktualni.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Združevanje bank, vključevanje v druge bančne skupine in druge statusne spremembe vedno prinesejo začasno povečana varnostna tveganja. Tveganja so povečana z uvajanjem novih IT-rešitev, povečanjem števila neustrezno vzdrževanih »legacy« sistemov in nezadovoljstvom dela zaposlenih. Če ti procesi potekajo pod velikim časovnim pritiskom, je izvedba vseh potrebnih ukrepov še posebno velik izziv, na katerega moramo biti pripravljeni.

kateri še trajajo in lahko eskalirajo, kot npr. ruska agresija na Ukrajino. Drugi so se že ponovili, npr. blokirane pomorske poti. Tretji se lahko ponovijo v prihodnosti z manjšo ali večjo intenzivnostjo, npr. epidemija ali energetska kriza. Teroristični napadi so že dolgo stalnica. Lahko so državno sponzorirani in se dogajajo tudi v kibernetskem svetu.

Varnostne grožnje prinašajo tveganja, ki se jim lahko skušamo izogniti, jih zmanjšamo, prenesemo ali sprejmemo. V vsakem primeru jih moramo najprej analizirati in razumeti.

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



Metode za upravljanje tveganj so načeloma univerzalne in uporabne v različnih sektorjih, vendar so banke res nekoliko specifične zaradi regulatornih zahtev in posebnosti bančnega poslovanja. Pri poslovanju banke sprejemajo tveganja. Vsakič, ko banka odobri kredit, je tveganje, da posojeni znesek ne bo pravočasno vrnjen. Pomembno je, da tveganja ves čas ostajajo v vnaprej opredeljenem okviru (»risk appetite«) in da ima banka dovolj kapitala, da škodo prenese tudi ob nepričakovanih dogodkih in izrazito neugodnih ekonomskih razmerah. Banke morajo nadzornim inštitucijam in strankam nenehno dokazovati, da so vloge varčevalcev varne.

Različne vrste tveganj banka obravnava z različnimi koraki, vendar na koncu pridemo do skupne slike, profila tveganosti banke. O tem je možno veliko izvedeti tudi iz javno objavljenih finančnih poročil.

Za vse vrste tveganj, še posebno za varnostna, ves čas nadgrajujemo okvire upravljanja in rešitev. Pri tem sledimo evoluciji varnostnih groženj v okolju. Odgovore nanje moramo imeti pripravljene, preden to izrecno opredeli regulator. Regulativa nam samo pomaga, da so naše rešitve sistematske in konsistentne.

V zadnjem obdobju ste konstantno v zahtevni dinamiki združevanja v nove lastniške oblike in okvire delovanja. Posebej z varnostnega vidika je to verjetno pomemben izziv, ki prinaša tudi veliko novih izkušenj in dobrih praks. Lahko z nami podelite nekaj najpomembnejših?

Banke že dolgo optimirajo procese in se skupaj s strankami preusmerjajo na samopostrežne kanale. Te procese v zadnjem času imenujemo »digitalizacija«, čeprav izraz zveni precej neposrečeno. Zaradi zahtev poslovnega okolja in regulatorjev, večje banke lažje dosegajo pričakovane poslovne rezultate in hkrati zahtevano robustnost obvladovanja tveganj. Tako deluje ekonomija obsega. Banke se združujejo in zmanjšujejo stroške na enoto. Zaposlenih v bančništvu je vedno manj. Vzporedno se dogajajo premiki in konsolidacija posameznih bančnih skupin v regiji.
V praksi to za bančnike pomeni, da moramo včasih prevzemati varnostne standarde drugih bank, včasih pa svoje standarde uvajamo v druge članice skupine. Lahko celo oboje hkrati. To ni težko, če spremembe uvajamo z zrnom soli in uveljavljamo zahtevnejše varnostne standarde, kjer je mogoče. Pomembno je, da se ekipe ne delijo na prevzemnike in prevzete, vaše in naše. Potem vse steče, kot je treba.

Združevanje bank, vključevanje v druge bančne skupine in druge statusne spremembe vedno prinesejo začasno povečana varnostna tveganja. Tveganja so povečana z uvajanjem novih IT-rešitev, povečanjem števila neustrezno vzdrževanih »legacy« sistemov in nezadovoljstvom dela zaposlenih. Če ti procesi potekajo pod velikim časovnim pritiskom, je izvedba vseh potrebnih ukrepov še posebno velik izziv, na katerega moramo biti pripravljeni.

Kako pomemben je pri takem združevanju vidik organizacijske in varnostne kulture zaposlenih v različnih organizacijah, ki se integrirajo v enoten sistem? Kako nasloviti to različno mentaliteto, ki se je gojila v ločenih organizacijah in jo združujemo v enovito zgodbo?

Varnostna kultura je odvisna od tega, kakšni so odnosi v organizaciji. Eden nekdanjih nadrejenih mi je nekoč rekel, da je lažje zamenjati zaposlene, kot spremeniti organizacijsko kulturo. Na srečo to ni edini način. V Novi KBM je bil po moji, povsem subjektivni oceni narejen tektonski premik v organizacijski kulturi v letu ali dveh po privatizaciji banke. Transformacija se začne pri upravi, nadaljuje pri direktorjih področij in se konča pri ostalih zaposlenih. Vmes kdo tudi odide, ker ni pripravljen na spremembo. Bistveno je, da ne pustimo prostora za izogibanje odgovornosti in delovanje v ograjenih silosih. Ko so se nam pridruževali zaposleni iz drugih bank, so to kulturo sprejeli. Za varnostno kulturo velja enako.

Verjetno so poleg strokovnih kompetenc pomembne tudi komunikacijske veščine, da se slovensko znanje uspešno predstavi tudi v mednarodnem korporativnem okolju združenih organizacij?

Za vodenje varnosti v podjetju so nujne vodstvene veščine, vključno s komunikacijskimi. Če ne znamo upravi jasno in prepričljivo pojasniti, zakaj so potrebne naložbe v varnost, bomo dosegli malo. V okviru mednarodnih družb je to bolj kompleksno, ker je vključenih več deležnikov z različnimi izhodišči. Sodelavcem sem predlagal, naj v stikih z drugimi družbami nastopajo spoštljivo, samozavestno in optimistično. Tudi sam skušam ravnati tako.

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

Uprava banke se zaveda varnostnih tveganj in je pripravljena sorazmerno s tem tudi dodeljevati vire. Samoumevnosti in bianco čekov ni. Vsako naložbo ali dodatno delovno mesto je treba prepričljivo utemeljiti v jeziku strateškega managementa. Pri tem imamo managerji korporativne varnosti še veliko možnosti za izboljšave.

V organizaciji redno izvajate potrebne varnostne ukrepe, med katerimi so tudi varnostni pregledi fizičnih, tehničnih in informacijskih sistemov. Kakšne so vaše izkušnje? Je sploh še možno posamezne segmente varnostnega sistema pregledovati ločeno ali je zaradi soodvisnosti in povezanosti to postal enovit proces?

Tveganja želimo obvladovati celovito in čimbolj enotno. Iščemo skupne okvirje, metode in merila. Pri varnostnih tveganjih gre za neposredno soodvisnost. Slabosti v fizični in tehnični varnosti lahko omogočijo vdor v informacijski sistem in obratno. Naša izkušnja je, da je za celovit pogled na varnost potrebno kombinirati penetracijsko testiranje informacijske, fizične in tehnične varnosti.

Verjetno redno spremljate stanje na področju korporativne varnosti v slovenskem okolju. Kateri so tisti izzivi, ki bodo pomembno oblikovali razvoj te profesije v naslednjem obdobju 5 let?

Kot je povedal Yogi Berra, je napovedovanje težko, še posebno za prihodnost. Po navadi preprosto napovedujemo podaljšanje trendov iz preteklih let. Potem nas presenetijo dogodki, ki vse obrnejo na glavo. Pričakujem, da bo v prihodnjih letih varnost izpostavljena, kot ključen element operativne odpornosti organizacije v tesni povezavi s pojmi, kot so upravljanje neprekinjenega poslovanja, odzivanje na incidente in upravljanje tveganj zunanjega izvajanja. Pri vodenju korporativne varnosti potrebujemo več širine, in ne ozko specializacijo.

Po večletnem sodelovanju ni nobenega dvoma: združevanje na ta način je dragoceno. Če seštejemo znanje ter dobre in slabe izkušnje vseh posameznikov, ki sodelujejo v združenju, dobimo pravo enciklopedijo dobrih praks, ki jih lahko smiselno uporabimo vsak v svojem okolju.



Vaše podjetje je tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Kako ste zadovoljni z delovanjem te strokovne asociacije?

Po večletnem sodelovanju ni nobenega dvoma: združevanje na ta način je dragoceno. Če seštejemo znanje ter dobre in slabe izkušnje vseh posameznikov, ki sodelujejo v združenju, dobimo pravo enciklopedijo dobrih praks, ki jih lahko smiselno uporabimo vsak v svojem okolju. ■

Učinkovite rešitve za analize in obvladovanje kibernetskih tveganj v vsaki organizaciji

Temelj za zagotavljanje kibernetske varnosti je upravljanje tveganj, ki organizacijam omogoča sistematično prepoznavanje in ocenjevanje ter nato obvladovanje nevarnosti, ki ogrožajo njihova informacijska omrežja, sisteme, naprave, podatke in druge informacijske vire.

Težava in rešitev

Pri analizi kibernetskih tveganj večina organizacij uporablja pristop, ki temelji na popisih in ocenah sredstev (ang. Asset Based Approach).

Rezultati takšnih analiz so seznami stotin in več informacijskih sredstev s številčnimi ocenami tveganj, za katere v organizacijah porabijo ogromno časa, vendar nimajo skoraj nobene uporabne vrednosti.

Učinkovita rešitev je procesni pristop in finančne ocene tveganj, s katerim pridobimo dvojno korist.

Prva je uporaben seznam informacijskih sredstev, ki so najbolj izpostavljena različnim nevarnostim, na podlagi možnih finančnih posledic. Druga pa so ocene tveganj za informacijska sredstva v skladu z regulativnimi smernicami, kot je standard ISO/IEC 27005.

Kako vam lahko pomagamo?

Vsem, ki ste odgovorni za kibernetsko varnost, lahko pomagamo:

- s svetovanjem pri pripravi metodologije za analizo kibernetskih tveganj v skladu s procesnim pristopom (prepoznavanje, ocenjevanje, razvrščanje),
- z izvedbo delavnic za analizo kibernetskih tveganj,
- z informacijsko rešitvijo Silver Bullet Risk (SBR) za celovito obvladovanje kibernetskih tveganj z vsemi ključnimi procesi in podatki na enem mestu.



Za več informacij ali predstavitev rešitve SBR nam pišite na naslov **info@silverbulletrisk.com**.

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
dr. Janez Stergar, Agencija za energijo

SODELOVANJE IN SINERGIJE ZA KIBERNETSKO VARNOST V ENERGETIKI

V ospredju sedanjih razprav o energetski prihodnosti je vprašanje kibernetske varnosti, ki postaja vse pomembnejše za delovanje organizacij v energetskem sektorju. Za podroben vpogled v to tematiko smo se pogovarjali z dr. Janezom Stergarjem iz Agencije za energijo, ki nam je razkril ključne izzive, usmeritve in prizadevanja agencije na področju varnosti v energetiki.

Varnostno okolje postaja vedno bolj zahtevno, kar močno vpliva tudi na odpornost in neprekinjenost delovanja organizacij v energetskem sektorju. Kateri so tisti varnostni izzivi, ki bodo na podlagi vaše strokovne analize najbolj vplivali na delovanje tega sektorja?

Agencija kot najpomembnejše prepoznava strateške izzive. Z vidika ekonomske regulative, kot primarne dejavnosti regulatorja, smo jih podali v zadnjem Poročilu o stanju na področju energetike (2022), kjer smo skušali povzeti prepoznana področja, obravnavana v združenjih, v katerih agencija sodeluje v okviru sodelovanja z evropskimi regulatorji (CEER in ACER) in upoštevanjem ostalih pomembnejših izsledkov strokovnih združenj, ki naslavljajo energetski sektor, kot so ENISA, WEC, WEF, IEA, NREL in CISA. Gospodarske javne službe (GJS), ki skrbijo za oskrbo z energijo, se soočajo z vse večjimi izzivi obravnave naraščajočih tveganj v kibernetski varnosti, vključno s pomanjkanjem strateške osredotočenosti, splošno težnjo po omejevanju razkritja institucionalnih informacij, omejenim naborom kadrovskih virov, veščin in znanja ter zmanjšano izmenjavo informacij med deležniki. Navkljub dejstvu, da se bo preventiva osredotočala na omejevanje groženj, analiziranje ranljivosti in zmanjševanje vpliva kakršnih koli morebitnih napadov, bo glavni poudarek za GJS na prožnem digitalnem sloju, kjer lahko varno obratujejo. To pomeni zasnovati nov varnostni koncept z načrtovanjem in naknadnim opremljanjem/posodabljanjem sistemov z namenom odložitve vpliva kibernetskih groženj ali njihove absorpcije in prilagoditve robustnosti občutljivega, a nepogrešljivega digitalnega sloja. Izzivi, ki jih lahko prepoznamo kot pomembne za odločevalce v energetskem sektorju, so vlaganje v napredno infrastrukturo, potreba po večjem medsektorskem in medinstitucionalnem sodelovanju, hitro spreminjajoča se kibernetska krajina, ozaveščenost in kompetence, krepitev sodelovanja med/z varnostnimi strokovnjaki in izboljšave v notranji organiziranosti za doseganje večje sinergije na področju zagotavljanja integralne varnosti (vključno s kibernetsko varnostjo) z vidika kadrovskih in drugih razpoložljivih potencialov.

Agencija za energijo je zelo pomemben organ v energetskem ekosistemu, saj usmerja in nadzira izvajalce ener-

Strokovnjaki s področja informacijske in kibernetske varnosti so v okviru upravljanja tveganj, povezanih s pomanjkanjem kadra, sicer vse pogosteje obremenjeni tudi z drugimi nujnimi nalogami, ki so jih na podlagi svoje širše kompetence usposobljeni izvajati, zato uporabljamo prožno organiziranost področja ob uporabi agilnih metod.

*avtorica je članica Slovenskega združenja korporativne varnosti



getskih dejavnosti na področju elektrike in zemeljskega plina. Ali to pomeni, da ste tudi koordinativni in usmerjevalni organ na področju zagotavljanja kibernetske varnosti za ta sistem?

V kontekstu informacijske/kibernetske varnosti izvajalcev GJS v energetskem sektorju se agencija pri prepoznavanju nalog izvajalcev kritičnih oziroma bistvenih/pomembnih storitev primarno osredotoča na zakonodajni okvir, določen z Zakonom o oskrbi z električno energijo (v nadaljevanju ZOEE) in Zakonom o oskrbi s plini (v nadaljevanju ZOP). Ta v členih 45 in 69 izvajalcem GJS distribucije in prenosa električne energije (ZOEE) oziroma v členih 19 in 58 operaterju prenosnega sistema in operaterjem distribucijskega sistema zemeljskega plina (ZOP) nalagata zagotavljanje varnega, zanesljivega in učinkovitega obratovanja in vzdrževanja prenosnega oziroma distribucijskega sistema ter njun razvoj ob upoštevanju zahtev varnega in zanesljivega obratovanja sistemov. Stališče agencije je, da v okvir te opredelitve sodi izvajanje ustrezne informacijske varnosti oziroma kibernetske zaščite. Agencija se zaveda, da je verjetnost udejanjenja kibernetskih groženj sicer majhna, vendar lahko ima za sistem in končne uporabnike občutne, morda celo kolateralne posledice. Posledično agencija pričakuje, da so vse naložbe v kibernetsko oziroma informacijsko varnost načrtovane in koordinirane, usklajene s pristojnimi organi (Ministrstvo za infrastrukturo, Ministrstvo za obrambo, Pristojni nacionalni organ za informacijsko varnost, Nacionalni odzivni center za kibernetsko varnost), predvsem pa, da so stroškovno kratkoročno in dolgoročno učinkovite. Čeprav agencija naložbe v kibernetsko varnost zaenkrat metodološko ne izpostavlja, jih vrednoti posredno, v procesu usklajevanja/potrjevanja razvojnih in naložbenih načrtov, v prihodnosti pa načrtujemo spremljanje pripravljenosti na kibernetske grožnje z določenimi izbranimi ključnimi indikatorji. Nenazadnje nalagajo prihajajoča omrežna pravila za kibernetsko varnost (CS NC) regulatorju dodatne naloge tudi na področju primerjalnih analiz.

V zadnjem obdobju je tudi zaradi varnostnih izzivov, katerim je izpostavljen sektor energetike, dozorela ideja po enovitem Varnostno operativnem centru za celoten sektor energetike. Ali strokovno podpirate napore za vzpostavitev te skupne kibernetske zmogljivosti?

O stališču agencije je morda preuranjeno govoriti, saj s tozadevnimi strokovnimi podlagami nismo seznanjeni. Pozdravljamo pa aktivnosti za rešitev, ki je strokovno utemeljena in stroškovno ter operativno najbolj učinkovita. Izpostavljamo, da je pri načrtovanju pomembna strateška vizija, ki upošteva organizacijsko strukturo energetskega sektorja (strukturo financiranja, kot tudi pristojnosti različnih organov), predvsem izvajalcev GJS in je v tem kontekstu morda koristno razmisliti o hierarhičnem povezovanju/sodelovanju obstoječih varnostno operativnih centrov (VOC), tako vertikalno navzdol s povezovanjem z manjšimi operativnimi enotami (»Blue Teams«) pri elektrodistribucijskih podjetjih (EDP), kot tudi horizontalno, če gre za VOC ostalih deležnikov v energetskem sektorju (npr. VOC proizvajalcev, kot so opredeljeni v Direktivi (EU) 2019/944) oz. vertikalno navzgor, če gre za krovni VOC v prihodnosti. VOC je v okviru elektrodistribucijskih podjetij namreč že vzpostavljen, prav tako ima VOC kombinirani elektro operater. Tukaj izpostavljamo predvsem stališče regulatorja glede stroškovne in operativne učinkovitosti. Zaradi kritičnega pomanjkanja izvedencev je pričakovati, da bosta VOC-a, če to že ne počneta, v prihodnosti lahko angažirana tudi operativno pri podpori kibernetskim operativnim skupinam/enotam EDP, posebej v primeru stopnjevanja kibernetskih napadov (v sodelovanju s področno specializiranimi operativnimi enotami zunanjih ponudnikov storitev). Hierarhično reorganizacijo prepoznavamo kot pomembno ne samo pri odzivanju, ampak tudi pri vodenju. Seveda je kot pri vseh kritičnih protokolih oz. procesih vodenja smiselno razmišljati o arhitekturi VOC, ki bo zagotavljala operativno redundanco v primeru oviranih storitev oz. odpovedi in prioritete glede na pomembnost deležnikov. Hierarhična struktura sodelujočih VOC to omogoča. Ne gre zanemariti tudi vidika učinkovitega (optimalnega) poročanja o dogodkih/incidentih pristojnemu nacionalnemu uradu za kibernetsko varnost in regulatorju.

Kako na Agenciji svoje aktivnosti na področju dvigovanja robustnosti energetskih deležnikov na področju kibernetske varnosti usklajujete z URSIV in SI-CERT?

Agencija je začela ciljno spremljati dejavnosti reguliranih podjetij na področju informacijske/kibernetske varnosti pred dobrimi desetimi leti, ko smo vzpostavili letno poročanje o naložbah v informacijsko/kibernetsko varnost elektro distributerjev in elektrodistribucijskih podjetij. Spremljamo ekonomske vidike štirih primarnih področij: področja poslovne (IT) in procesne informatike (OT), področja naprednega merilnega sistema (NMS) in pametnih števcev ter področja drugih dejavnosti (npr. polnilna infrastruktura, obdelava osebnih podatkov ipd.). V tem obsegu podrobneje sledimo tudi varnostnim vidikom s spremljanjem dejavnosti izvajalcev GJS po ISO 27002/27019. Nedavno smo vpeljali tudi proces vzorčenja ključnih kazalnikov pripravljenosti na kibernetske grožnje – izvedeno je bilo prvo poskusno vzorčenje nekaterih ključnih operativnih in taktičnih kazalnikov. O nekaterih izsledkih neformalno poročamo pristojnemu nacionalnemu organu za kibernetsko varnost in ga občasno tudi seznanjamo z aktivnostmi, v okviru Slovenskega Energetskega Varnostnega Foruma (SEVF) pa smo se srečevali tudi s SI-CERT. Sicer se s predstavniki navedenih deležnikov sreču-

jemo tudi v okviru nacionalnih kibernetskih vaj (nedavno na LockedShields 2023).

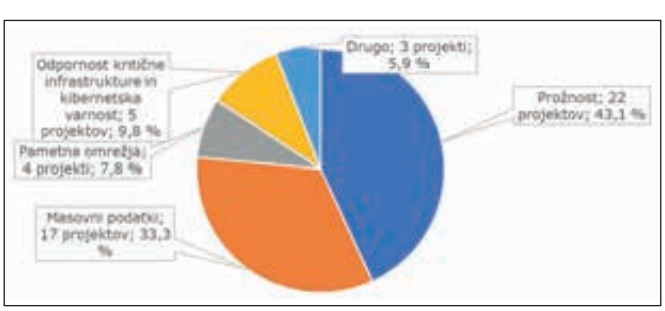
Se vam zdi sodelovanje organizacij energetskega sektorja v različnih EU projektih s področja kibernetske varnosti dodana vrednost za dvigovanje nivoja zrelosti teh organizacij?

Da. Zagotovo.

Največkrat s strani subjektov energetskega sektorja slišimo, da Agencija nima ravno posluha pri odmerjanju upravičenosti stroškov za razvoj in inovativne projekte, med drugim tudi na področju zagotavljanja kibernetske varnosti. Menite, da bi se tukaj dalo poiskati kakšne sinergije, kjer bi bilo tudi to področje močneje vključeno v odmero upravičenih stroškov zagotavljanja osnovne dejavnosti?

S temi navedbami se ne moremo strinjati. Področje zagotavljanja kibernetske varnosti je že v osnovi vključeno v upravičene stroške elektro operaterja v neposredni povezavi z razvojnimi načrti operaterjev. Ne poznamo primera, ko bi agencija posegla v področje upravičenih stroškov (CAPEX, OPEX) na področju zagotavljanja kibernetske varnosti ali iz razvojnih načrtov odstranila predlagane naložbe. Seveda pa agencija zahteva učinkovito izvajanje GJS in pričakuje od GJS, da bo zahteve po učinkovitosti tudi izpolnila.

Agencija je v zadnjih treh regulativnih obdobjih celo namensko vzpodbujala inovativne raziskave in inovacije v okviru kvalificiranih projektov iz sheme raziskav in inovacij (https://www.agen-rs.si/raziskave-in-inovacije/kvalificirani-projekti), kar vključuje tudi inovativne projekte na področju kibernetske varnosti. Shema spodbud je zastavljena po konceptu »peskovnika«, kjer imajo prijavitelji praktično proste roke pri izvajanju aktivnosti projektov. Iz tega segmenta je bilo v zadnjih obdobjih z naslavljanjem področja kibernetske varnosti kvalificiranih pet projektov (Defender, CyberSEAS, PHOENIX, PRECINCT, SUNRISE), kar pomeni skoraj 10 % skupnega števila prijav projektov (slika 1). Na strani reguliranih podjetij pa je, da vključijo obetajoče izsledke raziskav v naložbene načrte, če so se izkazali za smotrne in koristne. Agencija trenutno žal še ne prepoznava trenda prenosa obetajočih izsledkov iz RI projektov v naložbene načrte.



Slika 1: Delež zastopanosti področja kibernetske varnosti v shemi RI.

Agencija tudi dodatno spodbuja naložbene projekte v pametna omrežja, ki imajo naravo infrastrukturnih projektov (https://www.agen-rs.si/spodbujanje-uvajanja-pametnih-omrezij). Projekti rešitev pametnih omrežij morajo biti v skladu z definicijo pametnega omrežja oziroma pametne energetske infrastrukture iz splošnega akta, ki ureja metodologijo za določitev regulativnega okvira in skupaj s povezanimi podpornimi projekti zagotavljajo celovito izrabo funkcionalnosti pametnih omrežij. Podporni projekti vključujejo potrebno, v zasnovi kibernetsko varno IT podporo in IKT infrastrukturo, v obsegu, nujno potrebnem za uvajanje prej izpostavljenih projektov. Spodbuda za pametna omrežja se dodeli na podlagi kvalifikacije projekta in presoje o povezanih aktiviranih sredstvih, OPEX stroški na širšem segmentu naložb v pametna omrežja pa se priznajo v celoti in niso podvrženi splošnim zahtevam po učinkovitosti. Zelo verjetno gre pri določenih subjektih, ki izvajajo GJS, za ne najboljše poznavanje metodologije reguliranja in posledično ne izkoriščanje potenciala spodbud, ki jim ga zagotavlja agencija.

Kadri so večna nevralgična tema zadnjega obdobja. Kako se na Agenciji spoprijemate s pomanjkanjem visoko specializiranega kadra s področja informacijske in kibernetske varnosti?

Glede na splošen trend pomanjkanja kadrov s področja in finančnih omejitev v javnem sektorju, si agencija prizadeva slediti uveljavljenim strategijam, s poudarkom na izboljšanju notranje organiziranosti, ki med drugim obsegajo aktivnosti usposabljanja obstoječega osebja, aktivnosti pri vzpostavljanju partnerstev s strokovnjaki s tega področja v drugih organizacijah ali v akademskih institucijah, načrtovanju nadzorstev v informacijski/kibernetski varnosti z upoštevanjem uporabe naprednih »inteligentnih« avtomatiziranih sistemov za kibernetsko varnost, zunanjim izvajanjem določenih nalog ali projektov s specializiranimi zunanjimi ponudniki ter agilnim osredotočanjem na ključna področja v informacijski/kibernetski varnosti glede na krajino zaznanih tveganj. Strokovnjaki s področja informacijske in kibernetske varnosti so v okviru upravljanja tveganj, povezanih s pomanjkanjem kadra, sicer vse pogosteje obremenjeni tudi z drugimi nujnimi nalogami, ki so jih na podlagi svoje širše kompetence usposobljeni izvajati, zato uporabljamo prožno organiziranost področja ob uporabi agilnih metod.

Strokovna združenja so lahko pomembna dodana vrednost za dvigovanje kvalitete na določenih področjih. Na področju varnosti je to vsekakor Slovensko združenje za korporativno varnost, kamor so vključeni praktično vsi najpomembnejši deležniki energetskega sektorja, vključno s pomembnimi državnimi institucijami. Menite, da je čas, da se tej asociaciji priključi tudi Agencija in tako še utrdi napore na področju dvigovanja sistemskih ukrepov, tudi s področja kibernetske varnosti?

Agencija spremlja področje kibernetske varnosti s prisotnostjo/aktivnostjo v več združenjih: nacionalno v okviru SEVF, kjer smo tudi ustanovni član, zadnjo dekado v CEER CS WS (Cybersecurity Workstream) in ACER RISIG (REMIT Information Security Implementation Group) nedavno, zadnje triletje, pa še v CIGRE WG.54 (Regulatory approaches to enhance EPU's cybersecurity frameworks). V lanskem letu smo se pridružili tudi skupnosti deležnikov CyberSEAS (CyberSEAS Stakeholder Community), občasno pa smo prisotni še na srečanjih švicarskega IT-OT varnostnega foruma (Swiss OT-IT Cybersecurity Forum). Sodelovanju v novih združenjih/asociacijah smo sicer naklonjeni, vendar seveda le v obsegu, kot nam to omogočajo kadrovski viri in aktivne vloge v predhodno navedenih združenjih oz. skupnostih. ■

Foto: arhiv Agencije za energijo









ohranite neprekinjeno delovanje kritične infrastrukture

Zaščitite svojo kritično infrastrukturo s celovitimi varnostnimi rešitvami ALCEA. Sodelujte z nami za zaščito po meri: alceaglobal.com

ALCEA

ASSA ABLOY

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Sebastian Petek, direktor Službe korporativne varnosti in nadzora v Pošti Slovenije*

POŠTA SLOVENIJE V OBVLADOVANJU NOVIH VARNOSTNIH IZZIVOV PRIHODNOSTI

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

Obvladovanje varnostnih tveganj je zelo pomembna nit vaše strokovne kariere. Nam lahko poveste, katera so ključna področja pristojnosti, ki ste jih v svoji bogati karieri konkretno izvajali?

V svet korporativne varnosti sem vstopil relativno mlad, neizkušen in v času, ko so se v organizacijah šele kazali zametki razumevanja pomembnosti obvladovanja varnostnih tveganj, ki so jim podvrženi kompleksni poslovni sistemi. Iskreno povedano me je takrat, pred sedemnajstimi leti, v področje korporativne varnosti »zaneslo« po naključju, potem pa sem se z leti s področjem poistovetil in predvsem zaradi tega nato nadgrajeval znanje, kompetence in izkušnje. Zaradi dinamike oziroma nenehnih sprememb v okolju se mi zdi pomembno, da je kariero na področju korporativne varnosti potrebno graditi postopoma, kar se odraža recimo tudi pri pregledu področij in pristojnosti, ki sem jih izvajal na Pošti Slovenije. Konkretno lahko povem, da sem aktivno sodeloval pri vzpostavitvi sistema korporativne varnosti na strateškem nivoju Pošte Slovenije, kjer smo s kolegi večkrat orali ledino, še posebej pri vzpostavitvi lastnega nadzornega centra, implementaciji notranjih preiskav, testov integritete, nadzoru poslovanja itd. V zadnjih letih sem opravljal delo vodje oddelka korporativne varnosti in koordinatorja procesa varovanja ljudi in premoženja, s poudarkom na načrtovanju, organiziranju, koordiniranju, optimiziranju in nadziranju ter vodenju dela v organizacijski enoti. V zadnjem letu in pol na Pošti Slovenije opravljam delo vršilca dolžnosti direktorja korporativne varnosti in nadzora, dodatno opravljam še delo koordinatorja neprekinjenega poslovanja in zaupnika v sistemu »žvižgaštva.«

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

Vsekakor menim, da je razumevanje sprememb varnostnega okolja lahko konkurenčna prednost podjetij, vendar je nujna predpostavka, da se razumevanje nujno odrazi tudi na prilagajanju varnostnemu okolju, torej izvajanju določenih ukrepov. Predvsem veliki sistemi, ki so še posebej podvrženi spre-

> Vsekakor pa menim (in tudi delujem tako), da je pomembna moč strokovne argumentacije, tesno sodelovanje varnostnega managementa z vodstvom in nenazadnje velika stopnja zaupanja. Brez tega zadnjega, po mojem mnenju ne gre.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

> Z razmahom t.i. Dark neta in poznavanja zakonodaje s področja poštnega prometa ocenjujem, da se je velik del prometa s prepovedanimi drogami v zadnjih letih preselil v vsebino poštnih pošiljk oziroma v okvire poštnega prometa. Glede na izkušnje in informacije lahko potrdim, da promet s prepovedanimi drogami v poštnem prometu ni omejen zgolj na nacionalno raven.

membam, lahko denimo s pravočasnimi ukrepi preprečujejo finančne izgube, gradijo na poslovni etiki, ustrezno zaščitijo svojo kritično infrastrukturo itd.

Pošta Slovenije predstavlja podjetje, ki se ukvarja z zelo specifično dejavnostjo in je v določenih procesih vsekakor pomemben del infrastrukture Republike Slovenije. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Proces upravljanja tveganj je ena izmed pomembnih sestavin korporativnega upravljanja, ki ji na Pošti Slovenije, kot strateško pomembnemu državnemu podjetju, namenjamo veliko pozornosti. Razmerje med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov tako zagotavljamo s sistematičnim pristopom, z jasno definiranim procesom, odgovornostmi in predpisano metodologijo upravljanja tveganj. Korporativno varnost, kot del v celoti, pa determinirajo številni dejavniki, med katerimi lahko izpostavim razpršenost poslovalnic (približno 300 lastnih), izvajanje različnih dejavnosti (poštna, logistična, denarno poslovanje, podatkovni centri, ipd.), število zaposlenih (okvirno 5.900) ter zunanji deležniki. Navedeni dejavniki prav tako zahtevajo sistematičen in organiziran pristop pri obvladovanju varnostnih in z varnostjo povezanih tveganj.

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

Odkrito lahko povem, da se na Pošti Slovenije trenutno ni potrebno zatekati h kakšnim posebnim metodam prepričevanja vodstva glede organizacijskih in finančnih virov, ki jih potrebujemo za vzdrževanja oziroma nadgradnjo sistema korporativne varnosti. Vsekakor pa menim (in tudi delujem tako), da je pomembna moč strokovne argumentacije, tesno sodelovanje varnostnega managementa z vodstvom in nenazadnje velika stopnja zaupanja. Brez tega zadnjega, po mojem mnenju ne gre. Če se recimo postavim v vlogo vodstva, ki je med drugim odgovorno tudi za poslovne rezultate, se mi zdi nekako logično, da je v primeru ugodne varnostne situacije področje korporativne varnosti odmaknjeno nekoliko na stran in tu je mogoče potem tisti najpomembnejši moment



prepričevanja, argumentacije in zaupanja med varnostnim managementom in vodstvom podjetja.

V zadnjem obdobju se v javnosti pogosto pojavljajo informacije o zlorabi poštnih pošiljk za pošiljanje nedovoljenih substanc, kot so mamila, poživila in tudi orožje. Kakšne so vaše ocene tega varnostnega problema v mednarodnem merilu?

V principu informacije držijo. Pravzaprav se v zadnjih letih povečuje zloraba procesov poštnega prometa z namenom prometa s prepovedanimi drogami. Z razmahom t.i. Dark neta in poznavanja zakonodaje s področja poštnega prometa ocenjujem, da se je velik del prometa s prepovedanimi drogami v zadnjih letih preselil v vsebino poštnih pošiljk oziroma v okvire poštnega prometa. Glede na izkušnje in informacije lahko potrdim, da promet s prepovedanimi drogami v poštnem prometu ni omejen zgolj na nacionalno raven. Gre za globalno segajoč pojav. Nove tehnologije na eni strani in poštna zakonodaja na drugi, nudita storilcem anonimnost in manjše tveganje, da so lahko odkriti.

Kako se v Pošti Slovenije lotevate preprečevanja teh nelegalnih procesov?

Najprej naj poudarim, da je za vsebino poštnih pošiljk odgovoren pošiljatelj. Veljavna zakonodaja sicer prepoveduje pošiljanje določenih vsebin, hkrati pa Pošti onemogoča, da bi bila z vsebino, ki je pri opravljanju univerzalne poštne storitve ustavno varovana kategorija, v smislu tajnosti oziroma pravice do zasebnosti, vnaprej seznanjena in posledično preprečevala promet s tovrstno vsebino. Trenutno je edini način za odkrivanje prepovedane vsebine, ki ga imamo na voljo, pregled pošiljk z rentgenskimi napravami in napravo za identifikacijo prepovedanih drog in eksplozivnih snovi.

Ste pomemben del mednarodnega konzorcija evropskega projekta ARIEN, ki je usmerjen ravno v ukrepe odkrivanja nelegalne zlorabe poštnih pošiljk za tihotapljenje drog. Kaj za vas pomeni sodelovanje v takih projektih?

Pošta Slovenije je ne glede na dejavnost, ki jo opravlja v svojem bistvu družbeno odgovorno usmerjena, predvsem pa zasledujemo ničelno toleranco do vseh oblik kriminala oziroma v konkretnem primeru nelegalnih zlorab poštnega prometa. Projekt ARIEN je v osnovi namenjen prav temu, zato ga od vsega začetka podpiramo tudi v obliki aktivnega sodelovanja.

Kakšna so pričakovanja od končnih rezultatov projekta in ali te rezultate poskušate integrirati v izvajanje svojih varnostnih procesov pri nadzoru nad poštnimi pošiljkami?

Še posebej, ker govorimo o uporabi orodij umetne inteligence, se nadejamo, da bodo rezultati projekta skladni s pričakovanji. Torej, da bomo lahko v kombinaciji z že vzpostavljenimi tehničnimi in organizacijskimi ukrepi v prihodnje še učinkoviteje odkrivali prepovedane vsebine v poštnih pošiljkah. Vsekakor bomo rezultate integrirali tudi v procese, saj se zavedamo, da nove oblike sintetičnih drog in predvsem visoko koncentrirane sestavine za izdelavo drog niso zgolj prepovedane, ampak lahko tudi izjemno nevarne za zdravje naših zaposlenih, ki rokujejo s takšnimi pošiljkami. Ne gre torej zgolj za odkrivanje prepovedanega, ampak predvsem za obvladovanje tveganj v zvezi z zagotavljanjem zdravja naših zaposlenih.

Kako ocenjujete vaše sodelovanje s pristojnimi organi v Republiki Sloveniji na omenjenem področju?

Lahko rečem, da odlično. Pošta Slovenije s pristojnimi organi že vrsto let sodeluje na formalni pa tudi neformalni ravni. V tem času se je med Pošto Slovenije in organi pregona izgradil visok nivo zaupanja in vzpostavile so se vezi, ki nenazadnje koristijo tudi družbi.

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

Iz lastnih izkušenj lahko povem, da je izobraževanje in usposabljanje kadrov ter predvsem mentorstvo v smislu prenosa znanja iz izkušenega na neizoblikovanega najcenejši in najučinkovitejši način za obvladovanje varnostnih tveganj. Dejstvo je, da talentov s takšnimi lastnostmi in specifikami, ki jih zahteva področje korporativne varnosti ni veliko, zato jih je še toliko bolj potrebno znati prepoznati in usmeriti v področje, kjer bodo lahko dosegli izjemne rezultate. Nenazadnje govorimo o zagotavljanju varnosti ljudi, zdravja zaposlenih, varovanja informacij in premoženja, kar ob predpostavki, da smo pri tem učinkoviti, ločuje uspešne od neuspešnih ali povprečnih.

Dejstvo je, da talentov s takšnimi lastnostmi in specifikami, ki jih zahteva področje korporativne varnosti ni veliko, zato jih je še toliko bolj potrebno znati prepoznati in usmeriti v področje, kjer bodo lahko dosegli izjemne rezultate.

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

Absolutno. Lahko tudi rečem, da se je v preteklih letih nabralo že kar nekaj merljivih rezultatov. Pred leti smo na Pošti Slovenije z odobravanjem pospremili idejo o ustanovitvi Slovenskega združenja korporativne varnosti, od takrat pa v združenju tudi aktivno sodelujemo. Združenje zagotovo pomembno prispeva k prepoznavi pojmovanja korporativne varnosti in z njo povezanih tveganj, tako v Sloveniji kot tudi v tujini. Kot korporativni član združenja prepoznavamo dodano vrednost združenja v povezovanju različnih deležnikov na področju korporativne varnosti in gospodarstva kot celote, izmenjavi izkušenj in dobrih praks ter izobraževanju, pri čemer pozdravljamo usmeritev, da poudarek na izobraževanju ni podan samo na nosilcih in odgovornih osebah v podjetjih za korporativno varnost, ampak tudi na najvišjem managementu v podjetjih. Tudi v prihodnje ostajamo aktivni člani. ■

Foto: arhiv Pošta Slovenije d.o.o.

ZARJA ELEKTRONIKA

Varno v nov dan



• razvoj
• inženiring
• proizvodnja
• projektiranje
sistemov za tehnično varovanje

www.zarja.com

ZARJA ELEKTRONIKA d.o.o.
Kovinarska cesta 4, 1241 Kamnik, Slovenija • tel.: 01 831 74 88
• servis: 01 831 74 52 • info@zarja.com • prodaja@zarja.com

ISO 9001 Q-1210

Avtorica: dr. Jelena Virant Burnik / Urad Informacijskega pooblaščenca Republike Slovenije*



NA STIČIŠČU VARSTVA OSEBNIH PODATKOV IN UREDB DIGITALNE EU STRATEGIJE

EU je nedavno sprejela več aktov, ki urejajo digitalno okolje, digitalne storitve, stremijo k digitalnemu napredku, izrabi podatkov, ob hkratnem boljšem varovanju pravic uporabnikov digitalnih orodij, boljšemu varovanju pred zlorabami v digitalnem svetu. Sprejet je bil denimo Akt o upravljanju podatkov, pa Akt o digitalnih storitvah, Akt, ki določa nova pravila glede preglednosti in ciljanega političnega oglaševanja, tu je Akt o umetni inteligenci. Skupna točka večine aktov, ki pospešeno prihajajo iz EU in zavezujejo tudi organizacije in posameznike pri nas, pa je tudi, da večina v določenem delu specialno ureja tematiko varstva osebnih podatkov. Tu imamo že od leta 2018 v veljavi Splošno uredbo o varstvu podatkov, ki je postavila v EU visoke standarde varovanja osebnih podatkov, v Sloveniji pa nekatere specifike (npr. videonadzor, biometrijo itd.) ureja tudi Zakon o varstvu osebnih podatkov (ZVOP-2).

Prihod aktov digitalne EU strategije bo na marsikaterem področju zadeval varovanje osebnih podatkov, s tem pa se bodo ustvarila raznolika prepletanja z že obstoječimi pravili s področja varstva podatkov. Evropski odbor za varstvo podatkov tako v svoji izjavi[1] opozarja, da novi akti ne bi smeli pomeniti nižanja že zagotovljenih standardov varstva osebnih podatkov – npr. v primeru aktov, ki spodbujajo širšo rabo podatkov. Da se lahko ob velikem številu fragmentiranih aktov pojavijo nekonsistentnosti (npr. kaj pomeni anonimizacija podatkov) ter, da akti digitalne strategije prinašajo fragmentirano strukturo nadzora, kar lahko vpliva na učinkovitost. Evropske uredbe se v državah članicah uporabljajo neposredno, vendar pa morajo le-te običajno določiti nabor nadzornih organov, ki se med seboj lahko razlikujejo.

Za ilustracijo v nadaljevanju sledi oris prepleta področja varstva osebnih podatkov z Aktom o digitalnih storitvah (Digital Services Act), ki od februarja 2024 velja neposredno v vseh državah članicah EU, tudi v Sloveniji. Vzpostavlja sistemski nadzor nad spletnimi platformami in družbenimi omrežji in od upravljalcev digitalnih platform zahteva večjo odgovornost pri zaščiti uporabnikov in podjetij ter tudi, da okrepijo svoje mehanizme za odstranjevanje nezakonitih vsebin in preprečevanje širjenja sovražnega govora in dezinformacij. Cilj Akta o digitalnih storitvah je povečanje preglednosti ciljnega oglaševanja na družbenih omrežjih, zbiranja podatkov in delovanja algoritmov, ki jih omrežja

Akt o digitalnih storitvah naslavlja obveznosti štirih tipov ponudnikov storitev na spletu, (1) ponudnikov posredniških storitev, (2) ponudnikov gostovanja, (3) spletnih platform in spletnih iskalnikov ter (4) zelo velikih spletnih platform in spletnih iskalnikov (kriterij za slednje je več kot 45 milijonov mesečnih aktivnih uporabnikov).

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Spletne platforme bodo morale imeti vzpostavljene obvezne postopke za odstranjevanje nezakonitega blaga. Spletne tržnice bodo morale izslediti svoje trgovce, kar naj bi zagotavljalo varno, pregledno in zaupanja vredno okolje za potrošnike ter trgovce odvrnilo od prodaje nevarnega ali ponarejenega blaga. Spletne platforme bodo morale organizirati svoje spletne vmesnike, tako da bodo trgovcem omogočile izpolnjevanje njihovih obveznosti do potrošnikov.

uporabljajo pri ponujanju in predstavljanju vsebin končnim uporabnikom. Raziskovalcem bodo morali upravljalci največjih digitalnih platform za lažje razumevanje spletnih tveganj omogočiti dostop do svojih ključnih podatkov. Nadzor nad izvajanjem Akta o digitalnih storitvah si bodo delile Evropska komisija in države članice (te so morale določiti Koordinatorja digitalnih storitev, ter nacionalne nadzorne organe).

Akt o digitalnih storitvah naslavlja obveznosti štirih tipov ponudnikov storitev na spletu, (1) ponudnikov posredniških storitev, (2) ponudnikov gostovanja, (3) spletnih platform in spletnih iskalnikov ter (4) zelo velikih spletnih platform in spletnih iskalnikov (kriterij za slednje je več kot 45 milijonov mesečnih aktivnih uporabnikov). Mednje je Evropska komisija uvrstila nabor največjih multi-nacionalnih ponudnikov: Alibaba, AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Bing, Google Search[2]. Za tovrstne velike platforme je značilno, da je „osnovna storitev“ uporabniku pogosto na voljo brezplačno, medtem ko se monetizira z vedenjskim oglaševanjem, uporabo podatkov posameznikov/potrošnikov za profiliranje in prikazovanje prilagojenih vsebin in oglasov. Akt o digitalnih storitvah pa postavlja obveze tudi za druge spletne platforme, ne nujno čezmejnega značaja, torej platforme, ki omogočajo izmenjavo vsebin uporabnikov, hrambo njihovih podatkov (npr. spletne tržnice, iskalnike po različnih vsebinah), ponudnike hipnega komuniciranja, itd.

Akt o digitalnih storitvah prinaša pravila za boj proti nezakonitim vsebinam, določa ukrepe za umik ali spodbujanje umika nezakonitih vsebin, ob spoštovanju svobode izražanja, ščiti uporabnike pred nevarnim ali ponarejenim blagom. Spletne platforme bodo morale imeti vzpostavljene obvezne postopke za odstranjevanje nezakonitega blaga. Spletne tržnice bodo morale izslediti svoje trgovce, kar naj bi zagotavljalo varno, pregledno in zaupanja vredno okolje za potrošnike ter trgovce odvrnilo od prodaje nevarnega ali ponarejenega blaga. Spletne platforme bodo morale organizirati svoje spletne vmesnike, tako da bodo trgovcem omogočile izpolnjevanje njihovih obveznosti do potrošnikov.

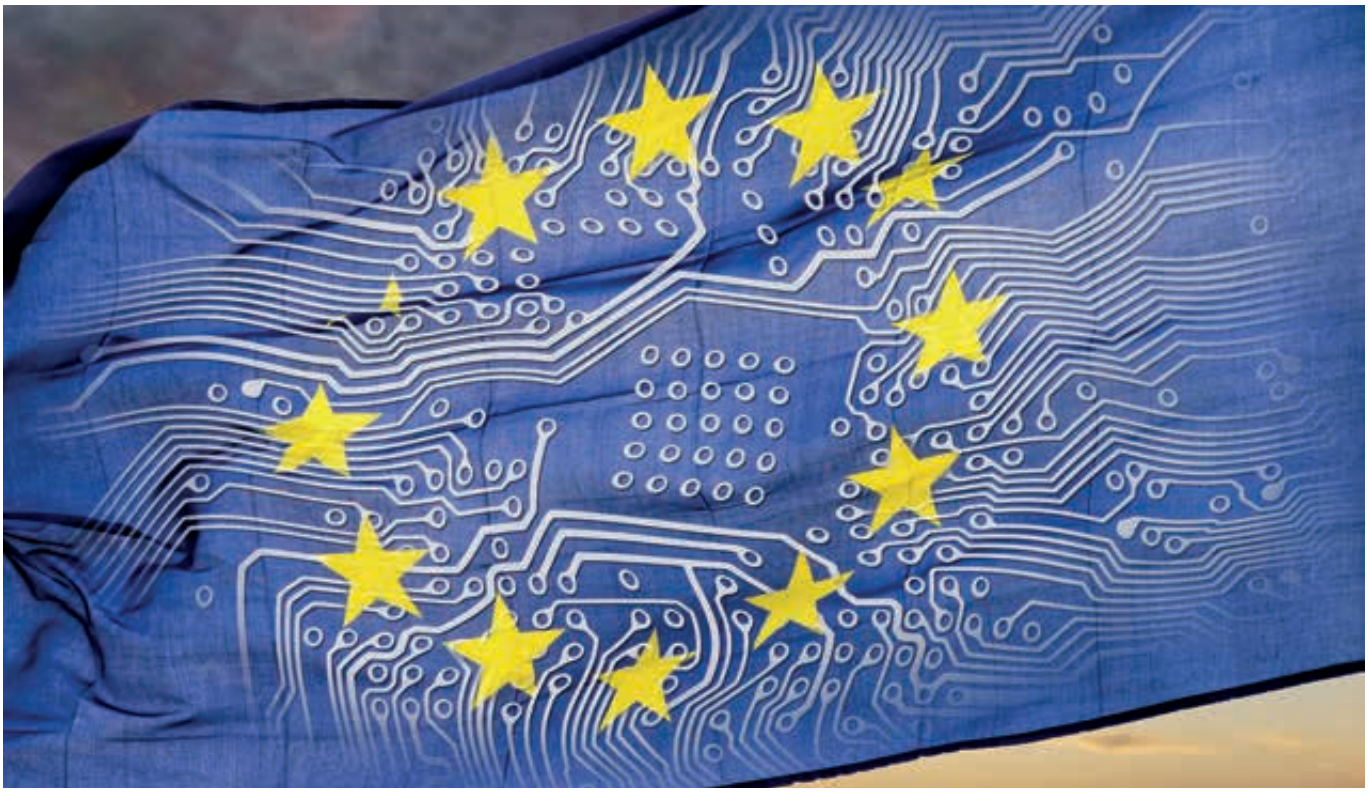


Tudi tržnice, kot je v Sloveniji denimo Bolha, si bodo morale prizadevati za naključno preverjanje, ali so bili proizvodi ali storitve opredeljeni kot nezakoniti, v kateri koli uradni podatkovni zbirki, in ali so bili sprejeti ustrezni ukrepi. Velike spletne platforme morajo uporabnikom ponuditi možnost, da izklopijo personalizirane vsebine. Nove so tudi obveznosti za oglase: poleg dodatne preglednosti in nadzora nad tem, zakaj v našem viru vidimo določen oglas, morajo spletne platforme oglase označiti.[3]

Nedavno sprejeti Zakon o izvajanju Uredbe (EU) o enotnem trgu digitalnih storitev (ZIUETDS) določa nadzorne organe, ki bodo materijo nadzorovali v Sloveniji. Vlogo koordinatorja digitalnih storitev bo izvajala Agencija za komunikacijska omrežja in storitve, ki bo hkrati izvajala tudi nadzor nad večino določb Akta o digitalnih storitvah. Drugi nadzorni organ je Informacijski pooblaščenec, in sicer v zvezi z določbami glede prepovedi vedenjskega oglaševanja na podlagi občutljivih osebnih podatkov in profiliranja otrok.

Kot pojasnjuje Informacijski pooblaščenec[4], se Akt o digitalnih storitvah in Splošna uredba o varstvu osebnih podatkov prepletata na več področjih, vendar pa Akt o digitalnih storitvah ne sme posegati v nabor druge EU zakonodaje, saj »Varstvo posameznikov v zvezi z obdelavo osebnih podatkov urejajo le pravila prava Unije z navedenega področja, zlasti Uredba (EU) 2016/679 in Direktiva 2002/58/ES.«[5] Akt o digitalnih storitvah ureja in uvaja obveznosti različnih ponudnikov digitalnih storitev, ti pa lahko nastopajo, glede na tip storitve, ki jo nudijo, tudi v vlogi upravljavca osebnih podatkov po Splošni uredbi oziroma v vlogi pogodbenega obdelovalca po Splošni uredbi, pri čemer morajo upoštevati tako določbe, kot jih določa Akt o digitalnih storitvah, kot tudi določbe glede varovanja osebnih podatkov po Splošni uredbi.

Platforme in ponudniki, ki jih ureja Akt o digitalnih storitvah, bodo imeli npr. široke obveze informiranja uporabnikov glede pogojev izvajanja storitev, glede algoritmov, ki so uporabljeni za priporočanje storitev, glede tega, kako so podatki uporabnikov uporabljeni za vedenjsko oglaševanje, glede vsebin vplivnežev, glede uporabe podatkov otrok. Obveznost informiranja pa se neposredno tiče informacij, ki jih morajo tovrstni ponudniki zagotoviti tudi glede na 13. člen Splošne uredbe. Tako Akt o digitalnih storitvah kot tudi Splošna uredba, predpisujeta mehanizme za odstranje-



vanje nezakonitih vsebin oziroma pravico do izbrisa osebnih podatkov, glede obdelave občutljivih podatkov (Splošna uredba) in prepovedi njihove uporabe za vedenjsko oglaševanje (člen 27 Akta o digitalnih storitvah), glede uporabe osebnih podatkov otrok (8. člen Splošne uredbe) in prepovedi vedenjskega oglaševanja na podlagi profiliranja otrok (člen 28 Akta o digitalnih storitvah). Pri tem Akt o digitalnih storitvah uvaja prepovedi, ki dopolnjujejo določbe Splošne uredbe, zlasti glede obdelave občutljivih osebnih podatkov, obdelave osebnih podatkov otrok ter informiranja uporabnikov/posameznikov o ozadju obdelave njihovih podatkov za namene priporočilnih sistemov in vedenjskega oglaševanja. Pri teh določbah se Akt o digitalnih storitvah sklicuje na Splošno uredbo in na definicije iz Splošne uredbe[6].

Glede na to povezanost aktov, ZIUETDS za nadzor nad določbama glede propovedi uporabe občutljivih osebnih podatkov za vedenjsko oglaševanje in glede oglaševanja otrokom, določa Informacijskega pooblaščenca. V zvezi s temi tematikami (profiliranje, obdelava občutljivih podatkov, obveščanje o obdelavi osebnih podatkov, itd. organi za varstvo osebnih podatkov v EU že izvajajo nadzore pri različnih zavezancih, izdajajo priporočila in smernice, usklajene tudi na ravni Evropskega odbora za varstvo podatkov. Slednji poudarja, da mora biti nadzor nad akti iz sklopa digitalnega paketa EU usklajen in da morajo biti ustvarjene obveze, da organi, ki jim bo v državah članicah zaupan nadzor nad temi akti, sodelujejo z organi za nadzor nad Splošno uredbo, saj akti digitalnega paketa posredno urejajo obdelavo osebnih podatkov posameznikov in ne smejo pomeniti nižjih ravni varstva, kot je zagotovljeno s Splošno uredbo.[7]

V tem duhu ZIUETDS uvaja tudi obvezo, da nadzorni organ (AKOS) pri nadzoru nad določbami, ki zadevajo varstvo osebnih podatkov upošteva prakso Informacijskega pooblaščenca in se z njim posvetuje. Tovrstno obveznost sodelovanja pristojnih organov je nedavno opredelilo tudi Sodišče EU v sodbi SEU št. C-252/21, kjer je pojasnilo, da lahko organ države članice, pristojen za konkurenco, s pridržkom spoštovanja svoje obveznosti lojalnega sodelovanja z nadzornimi organi, v okviru preizkusa zlorabe prevladujočega položaja s strani podjetja ugotovi, da splošni pogoji uporabe tega podjetja v zvezi z obdelavo osebnih podatkov niso v skladu s to uredbo, vendar pa organ, pristojen za konkurenco, pri tem ne sme odstopati od odločitve pristojnega nacionalnega nadzornega organa za varstvo podatkov oziroma se mora z njim posvetovati oz. zaprositi za sodelovanje.

Zgornji oris implementacije Akta o digitalnih storitvah in nadzora nad njim pokaže na kompleksnost prepletanja s pravili in nadzorom na področju varstva osebnih podatkov. Enaka usoda bo neobhodno doletela tudi ostale akte digitalne strategije, kjer bodo države članice EU morale pazljivo določiti nabor nadzornih organov, da se bodo izognile fragmentaciji ter prekrivanju pristojnosti nadzornih organov. Ključno je tudi, da že vzpostavljene pristojnosti organov za varstvo osebnih podatkov in nadzorni postopki ne bodo ohromljeni, in da se raven varstva osebnih podatkov ne niža. Kot kaže nedavna sodba SEU št. C-252/21 pa je rešitve potrebno iskati tudi v tesnejšem sodelovanju med pristojnimi organi za različna področja in v omogočanju pravnega okvira, ki bo take izmenjave praks med organi spodbujal.

1 https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf

2 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

3 https://www.mipi.si/teme/medijska-pismenost/kaj-se-je-po-evropi-spremenilo-od-uveljavitve-akta-o-digitalnih-storitvah

4 Mnenje IP 007-54/2023/2 z dne 18. 9. 2023

5 Uvodna izjava 10 Akta o digitalnih storitvah

6 Mnenje IP 007-54/2023/2 z dne 18. 9. 2023

7 https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf, https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf ■



Vodnik z vprašanji in odgovori

Spodbujanje kibernetske varnosti za MSP v Evropi

Global Digital Foundation
The Digital Policy Network

eit Digital

Co-funded by the European Union

HUAWEI

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
ga. Kristina Batistič, predsednica sekcije Women4Cyber

ŽENSKE NA PODROČJU KIBERNETSKE VARNOSTI PREDSTAVLJAJO POMEMBEN POTENCIAL

Na področju zagotavljanja kibernetske varnosti smo priča izredno velikemu pomanjkanju ustreznih kadrovskih virov. Ob dejstvu, da se ženske vedno bolj vključujejo na različna področja, ki do nedavnega niso bila najbolj izpostavljena pri njihovi izbiri profesije, lahko upravičeno pričakujemo, da bo v prihodnje to na področju kibernetske varnosti postala redna praksa. Za nekaj misli o priložnostih za hitrejše vključevanje ženske populacije na področje kibernetske varnosti smo prosili go. Kristino Batistič, predsednico sekcije Women4Cyber.

Najprej nam dovolite, da vam čestitamo ob ustanovitvi slovenskega poglavja mednarodne iniciative Women4Cyber. Nam lahko na kratko opišete glavno poslanstvo, ki ste si ga zadale z omenjeno pobudo?

Najlepša hvala! Namen pobude je povezati strokovnjakinje, ki delujemo na tem področju, nuditi medsebojno podporo, izmenjavo znanj in izkušenj, povečati vidnost ženskih strokovnjakinj na tem področju, vzpostavitev zgledov ter pritegnitev več deklet, da se odločijo za študij in delo na tem področju. Želeli bi, da bi s časom na področju delovalo večje število žensk. To, da je ženska strokovnjakinja na področju kibernetske varnosti, pa bi bilo tako samoumevno, da pobuda ne bi bila več potrebna.

Ob pomanjkanju visoko specializiranih strokovnjakov na področju informacijske varnosti se vsi sogovorniki na strateškem nivoju strinjajo, da je ravno ženski del populacije največji možni kadrovski bazen, kjer bi se dalo pridobiti večje število dodatnih strokovnjakinj. Kakšno je stališče vaše iniciative glede teh priložnosti?

Na področju kibernetske varnosti je globalno 25% žensk (WEF, 2021), v Evropi le 7% (ENISA, 2019). Pritegniti več žensk na to področje je nujno potreben korak. Spodbujamo in podpiramo programe, ki omogočajo izobraževanje, usposabljanje in mentorstvo žensk, da lahko razvijejo potrebne veščine in znanja za uspeh na tem področju. Naš cilj je tudi razbijanje stereotipov in spodbujanje večje vključenosti žensk, saj verjamemo, da raznolikost prinaša širšo perspektivo in boljše rešitve za izzive, s katerimi se sooča panoga.

Želeli bi, da bi s časom na področju delovalo večje število žensk. To, da je ženska strokovnjakinja na področju kibernetske varnosti, pa bi bilo tako samoumevno, da pobuda ne bi bila več potrebna.

*avtor je član Slovenskega združenja korporativne varnosti



Imate mogoče že kakšne konkretne rezultate raziskav slovenskega trga delovne sile in umeščenosti žensk na področju informacijske in še ožje kibernetske varnosti?

Po podatkih DESI indeksa je v Sloveniji v IKT panogi 17% žensk, žal natančnejših podatkov za področje kibernetske varnosti trenutno nimamo, bi pa bila to zagotovo zanimiva raziskava.

Katere se tiste psihološke, fiziološke in sociološke komponente, kjer bi ženske kolegice prinesle dodano vrednost na področje informacijske varnosti?

Verjamem, da sposobnost posameznika za določeno področje ni odvisna od spola. Vsak lahko razvije spretnosti za področje zanimanja z dovolj podpore, truda in vztrajnosti. Raziskave kažejo, da so raznolike ekipe bolj uspešne, saj združujejo različne veščine, izkušnje in perspektive, kar pripomore k večji kreativnosti, inovativnosti, bolj učinkovitemu reševanju problemov, večji prilagodljivosti in odpornosti organizacije. Imela sem izkušnjo, kjer sem se ekipi pridružila kot druga ženska, tekom moje zaposlitve pa se je odstotek žensk povečal na približno tretjino. Ob tem se je zelo povečalo sodelovanje, izboljšala komunikacija in povečal občutek pripadnosti ekipi.

Katere so tiste organizacije iz katerih prihajate glavne ustanoviteljice omenjene sekcije?

Ustanoviteljice smo zelo raznolike. Prihajamo iz privatnega sektorja, javnega sektorja ter akademskih institucij, naj omenim nekaj konkretnih institucij, kot so CREAPLUS, ACTUAL I.T., Huawei, NIL, Microsoft, CERT, URSIV, GeaCollege, Univerza v Mariboru, in še bi lahko naštevali. Mislim, da je zelo pomembno, da imamo tako široko sodelovanje, saj nam omogoča izmenjavo najboljših praks, skupno reševanje kompleksnih problemov in ustvarjanje močnejše skupnosti, ter krepi medsebojno zaupanje in podporo med organizacijami in posamezniki, kar je ključno za napredek in inovacije v našem sektorju.

Nam lahko zaupate katere aktivnosti pripravljate v naslednjem obdobju, da se bo glas o poslanstvu vaše iniciative hitreje razširil v strokovni javnosti?

Naslednji dogodek, ki ga pripravljamo, je konferenca »Kibernetska varnost – Priložnost za vse«, ki bo 28. 5. 2024 v Hiši EU v Ljubljani. Rdeča nit dogodka bo raznolikost področja kibernetske varnosti, raznolikost področij delovanja in profilov. Tematike bodo tako strokovne, povezane z aktualno regulativo NIS2, kot splošne o razvoju karierne poti na področju kibernetske varnosti. Vabljene so vse strokovnjakinje in strokovnjaki, študentke in študenti ter vsi, ki jih zanima kariera na področju kibernetske varnosti.

Slovensko združenje za korporativno varnost ima v svojem okviru veliko ženskih kolegic. Kako bi se po vaše lahko oblikovalo sodelovanje med posameznimi združenji, da bi se iskalo sinergije in ne vzpostavljalo prekomerne obremenitve članic s prevelikim številom dogodkov.

Vzpodbujati moramo raznolikost in vključenost na področju kibernetske varnosti in se več povezovati, več sodelovati. Kljub temu, da je to tradicionalno moško področje, v Sloveniji deluje kar nekaj strokovnjakinj na tem področju.



Menim, da bi bili dogodki v skupni organizaciji lahko idealna priložnost za sodelovanje in povezovanje članstva obeh organizacij.

Kaj bi še kot trenutna predsednica omenjene iniciative želela sporočiti našim bralkam?

Vzpodbujati moramo raznolikost in vključenost na področju kibernetske varnosti in se več povezovati, več sodelovati. Kljub temu, da je to tradicionalno moško področje, v Sloveniji deluje kar nekaj strokovnjakinj na tem področju. Smiselno je, da poskrbimo, da imamo na dogodkih tudi ženske govorke, da izpostavimo tudi njihove zgodbe ter da mladim damo tudi ženski zgled. Povabila bi tudi vse zainteresirane, da se nam pridružijo v iniciativi. ■

Foto: arhiv sekcije Women4Cyber





Analogno. Digitalno. Dva svetova. Ena rešitev.

REISSWOLF

Uničevanje dokumentacije:

Varen in sledljiv proces uničevanja.

Varnostni zabojniki z elektronskim sistemom zaklepanja (e.l.sy)-beleženje vseh dogodkov (revizijska sled).

Uničevanje skladno z evropskimi standardi in Uredbo GDPR.

Uničevanje vseh vrst podatkovnih nosilcev (papir, trdi diski, CD-ji, RTG slike, itd.).



Elektronski zajem in hramba podatkov:

Certificiran, varen in zanesljiv e-proces, skladen z Uredbo GDPR.

Skeniramo vse formate od A0, vključno s projektno in tehnično dokumentacijo.

Stroškovno učinkovita rešitev.

Neomejen 24/7 dostop do dokumentov.

Povečanje produktivnosti.

Fizična hramba:

Najvišji nivo varnosti in sledljivosti ter skladnosti z Uredbo GDPR.

Učinkovit in uporabniku prijazen spletni dostop do arhiva 24/7.

Najsodobnejša tehnologija upravljanja z dokumenti.

Stroškovno učinkovita rešitev fizičnega arhiviranja.

Reisswolf – varno, nadzorovano in sledljivo upravljanje z dokumentacijo:

Rešitve po meri uporabnika z mednarodnimi izkušnjami.

Optimizacija digitalnih in analognih potreb.

Primerno za majhna, srednja in velika podjetja.

Okolju in uporabniku prijazne storitve.

Upoštevanje varnostnih standardov.

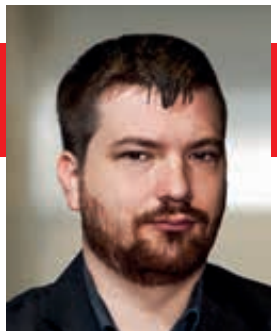
Ob oddaji povpraševanja do 31.05.2024 prejmite enkratno ekskluzivno ugodnost pri vseh storitvah REISSWOLF!

Pokličite nas na: **01 541 22 66**

Ali nam pišite na: **info@reisswolf.si**

simply. done.

Avtor: g. Matej Breznik, izkušeni analitik kibernetske varnosti,
Nacionalni odzivni center za kibernetsko varnost SI-CERT*



MEDSEBOJNA SOLIDARNOST PRI IZMENJAVI INFORMACIJ O KIBERNETSKIH GROŽNJAH V SLOVENSKEM PROSTORU

Naraščajoča potreba po hitri izmenjavi ključnih informacij za zaščito sistemov je prisotna v mednarodni ter posledično tudi slovenski kibernetski skupnosti. Hiter prenos informacij o kibernetskih grožnjah, njihova samodejna obdelava in učinkovitejša zaščita omrežij, so danes predpogoj za zagotavljanje kibernetske varnosti.

Veliko varnostnih strokovnjakov išče rešitve za pridobivanje informacij prek javnih in plačljivih virov, ki oskrbujejo ključne sisteme v omrežju z najnovejšimi tveganji v kibernetskem prostoru. Kot vedno pa obstajajo alternativne možnosti, ena izmed njih je razvita v okviru več kot desetletja starem projektu Malware Information Sharing Platform (v nadaljevanju MISP).

Stičišče MISP v Sloveniji upravlja Nacionalni odzivni center za kibernetsko varnost SI-CERT, ki širi zavedanje o pomembnosti izmenjave informacij med lokalnimi deležniki ravno prek platforme MISP. Zgodba uporabe platforme MISP je na SI-CERT stara skoraj deset let; posledično je v tujini izmenjava kibernetskih groženj prek platforme že dodobra razširjena in velja za nujnost v okoljih, kjer se ukvarjajo s preučevanjem ali omejevanjem kibernetskih groženj. Informacije o kibernetskih grožnjah, izmenjane s tujimi deležniki, so doprinesle k obogatitvi marsikatere preiskave, ki jo je vodil SI-CERT in prinesle tudi ključne informacije za ugotavljanje vzrokov in boljšo zaščito pred kibernetskimi grožnjami. Uporabnost platforme temelji ravno na široki skupnosti uporabnikov, ki redno nesebično delijo podatke o odkritih grožnjah v svojih omrežjih. Sodelujejo z zavedanjem, da je le na tak način mogoče ustvariti širšo zgodbo iz ugotovljenih analiz incidentov in dogodkov, saj je tudi v tem primeru zgolj vzpostavitev skupne obrambe najboljša rešitev za zaščito pred kibernetskimi napadi. SI-CERT spodbuja uporabo podatkov, ki so deljeni na platformi, kot tudi dodajanje informacij, zaznanih v omrežjih povezanih organizacij. Takšno solidarno delovanje bo prineslo lažje razumevanje o razširjenosti kibernetskih groženj in dodatno obogatilo vedenje o grožnjah samih.

Izmenjava podatkov z mednarodnimi partnerji poteka prek MISP povezav, ki obsegajo bogat nabor virov informacij: med njimi je sodelovalno okolje za izmenjavo groženj v okviru ENISA CSIRTs Network (mreža evropskih odzivnih centrov) ter evropska kontrola zračnega

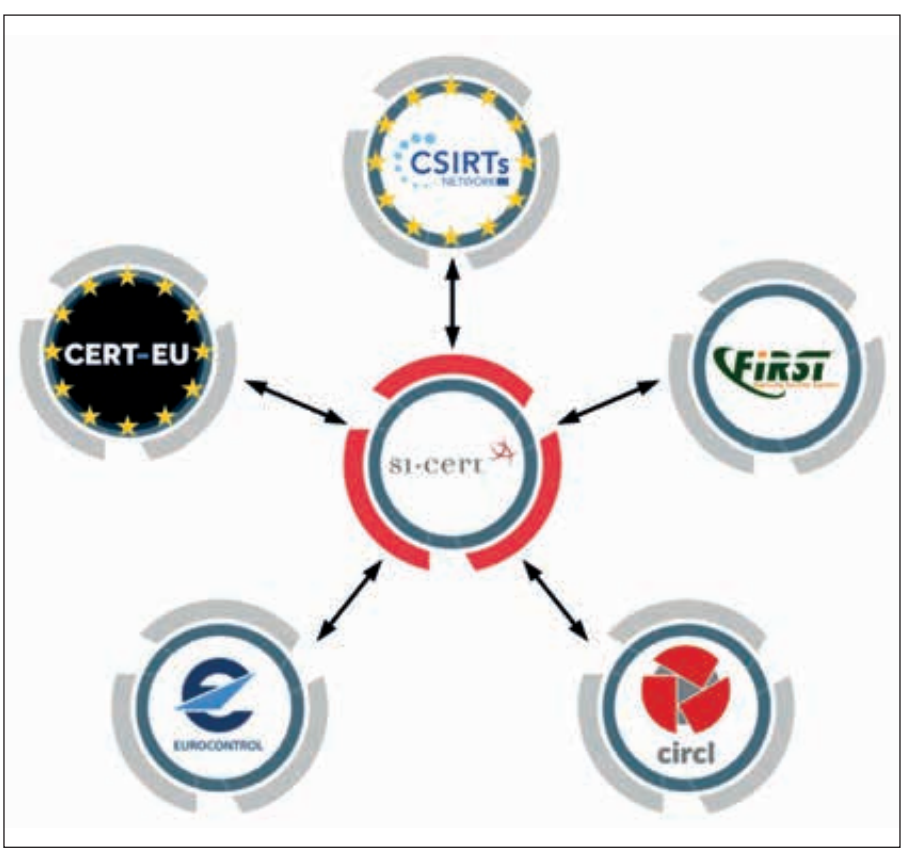
Stičišče MISP v Sloveniji upravlja Nacionalni odzivni center za kibernetsko varnost SI-CERT, ki širi zavedanje o pomembnosti izmenjave informacij med lokalnimi deležniki ravno prek platforme MISP. Zgodba uporabe platforme MISP je na SI-CERT stara skoraj deset let; posledično je v tujini izmenjava kibernetskih groženj prek platforme že dodobra razširjena in velja za nujnost v okoljih, kjer se ukvarjajo s preučevanjem ali omejevanjem kibernetskih groženj.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Deljenje informacij je ključnega pomena za boljšo zaščito posameznikov in izboljšanje stanja kibernetske odpornosti Slovenije. Zavedati se moramo, da kibernetska varnost ni naloga enega oddelka znotraj podjetja ali ene organizacije znotraj države, saj se kibernetske grožnje ne ustavijo na nacionalnih mejah. Kibernetska varnost zadeva vse – Cyber Security Is Everyone‘s Business, in najti učinkovit odziv na kibernetske grožnje je globalni izziv naše dobe.

prometa EATM-CERT, če izpostavimo le nekaj priznanih partnerjev. Potem so tu še neposredne izmenjave s priznanimi deležniki, med drugim CIRCL in CERT-EU. Na mednarodnem nivoju poteka izmenjava prek svetovnega združenja odzivnih skupin FIRST. Vsi ti viri informacij o kibernetskih grožnjah zagotavljajo Nacionalnemu odzivnemu centru SI-CERT širšo sliko svetovnih kibernetskih groženj.

V slovenskem prostoru že poteka izmenjava informacij s posameznimi deležniki prek platforme MISP. Ti z vključitvijo pridobijo dragocene podatke, ki jim, v povezavi s sistemom za pregled in zbiranje varnostnih informacij SIEM, omogočajo boljšo varnost nadzorovanih omrežij. Prednost tovrstne povezave je tudi hipna pridobitev podatkov o grožnjah, v primerih groženj, vnesenih s strani SI-CERT, celo hitreje kot prek drugih, morda plačljivih seznamov, saj pri predaji informacij ni vpletenih posrednikov in nepotrebnega preverjanja. Atributi, deljeni prek MISP, namreč lahko vsebujejo oznako, ki opredeljuje indikatorje okužbe oz. t.i. IoC podatke, kot primerne za omrežno pregledovanje in blokiranje. Tako lahko v primeru zaznanih korelacij s podatki, pridobljenimi s pomočjo MISP, ugotovijo sum na morebitne varnostne grožnje znotraj omrežja ali okužene delovne postaje. Če organizacija sama s preučitvijo varnostnega incidenta pridobi t.i. IoC podatke, lahko le-te vnese v MISP in jih tako deli z skupnostjo. Deljenje je lahko omejeno na posamezno skupino organizacij ali na priključene MISP platforme. MISP omogoča deljenje t.i. taktik, tehnik, postopkov oz. TTPs, ter tako omogoča poglobljen vpogled v deljen dogodek. Mogoče je izdelati časovnico pojavitve posameznih atributov, vzpostavitev relacij med atributi, povezovanje atributov v objekte, dodajanje besedilnega opisa dogodku, ... V okviru EU projekta CyberSEAS, kjer sodelujejo tudi partnerji iz Slovenije, bo razvit poseben MISP objekt, ki bo omogočal opis incidenta v skladu s slovenskim postopkom prijave. Tako bo v okviru projekta predstavljena tudi rešitev prijave incidentov prek MISP.



Slovenskim uporabnikom, ki želijo zgolj izboljšati varnost svojih omrežij na način, da obogatijo nabor indikatorjev zlorab, je na voljo izvoz MISP podatkov. Le-ta je na voljo širši javnosti, saj zanj ni potrebno vzpostaviti MISP povezave. Prek izvoza podatkov v MISP združljivi obliki, SI-CERT podaja zgolj svoje ugotovitve, denimo informacije o opaženih škodljivih priponkah, phishing straneh, opisne podatke o vzorcih škodljive kode ipd. Slabost predmetnega izvoza je izvzem informacij, pridobljenih od drugih MISP deležnikov, kot tudi odstranitev neposrednih vzorcev škodljive kode, ki omogočajo nadaljnjo analizo organizacijam, ki si tega želijo.

S promocijo platforme MISP, odzivni center SI-CERT tako aktivno sodeluje pri izmenjavi informacij o kibernetskih tveganjih in grožnjah. S platformo tudi aktivno postavlja nove mejnike varnosti v slovenskih omrežjih ter podaja informacije, ki lahko z ustrezno implementacijo pomagajo vsem državljanom. Deljenje informacij je ključnega pomena za boljšo zaščito posameznikov in izboljšanje stanja kibernetske odpornosti Slovenije. Zavedati se moramo, da kibernetska varnost ni naloga enega oddelka znotraj podjetja ali ene organizacije znotraj države, saj se kibernetske grožnje ne ustavijo na nacionalnih mejah. Kibernetska varnost zadeva vse – *Cyber Security Is Everyone‘s Business,* in najti učinkovit odziv na kibernetske grožnje je globalni izziv naše dobe. ■



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

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

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

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

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

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

CERTIFIED LPT (Master) CERTIFIED CHFI CERTIFIED CPENT CERTIFIED CEH MASTER CERTIFIED ECIH CERTIFIED OffSec OSCP

ISO 27001

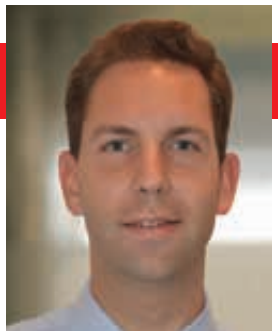
CERTIFIKAT O USPEŠNO OPRAVLJENEM IZPITU ZA VODILNEGA PRESOJEVALCA ZA PODROČJE PR320: ISMS ISO 27001:2013

BUREAU VERITAS

DPO

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

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



SODELOVALNI VIDIKI KIBERNETSKE VARNOSTI – DOBRE PRAKSE IN REŠITVE IZ PROJEKTA CYBERSEAS

Udejanjanje kibernetske varnosti v korporativnih okoljih postaja vse zahtevnejše, saj se v zadnjem času soočamo z naprednimi tehnikami napadov in porastom izpostavljenosti, kompleksnosti in povezljivosti teh okolij. Še zlasti so na udaru informacijski sistemi ter IT in OT integrirane infrastrukture, ki pomenijo ključ do uspešne digitalizacije. Prav tako v okoljih kritične infrastrukture in bistvenih storitev ne smemo prezreti posledic kaskadnih učinkov kibernetskih napadov, ki lahko ogrozijo povezane vire različnih deležnikov.

Uvod

Izzivi odpirajo potrebo po sodelovanju, ki jih dodatno poudarja dejstvo, da sta za učinkovito upravljanje kibernetskih tveganj in groženj ter za uspešno strateško in taktično odločanje bistvena dobra obveščenost ter souporaba znanja, postopkov in modelov za zaznavanje napadov in odzivanje nanje. V ospredje tako prihajajo proaktivni pristopi in sodelovalni vidiki kibernetske varnosti. Ti vidiki vključujejo izmenjavo obveščevalnih informacij za odločanje, standardizacijo in izmenjavo odzivnih procedur, vzpostavitev ekspertnih skupnosti z vpletenostjo varnostnih operativnih centrov in odzivnih ekip na korporativnem ali nacionalnem nivoju, uporabo pretočnih kanalov in platform za upravljanje s kibernetskimi dogodki ter številne druge mehanizme.

Implementacija mehanizmov sodelovanja na področju kibernetske varnosti prinaša več prednosti in priložnosti. S standardizacijo in izmenjavo odzivnih procedur ter mehanizmi za deljenje obveščevalnih informacij o kibernetskih grožnjah se vključujemo v nacionalne in mednarodne skupnosti, izboljšamo reaktivno odzivanje na kibernetske napade in proaktivno preprečevanje le-teh, podpremo odločanje na strateškem in taktičnem nivoju ter dvignemo splošno odpornost IT in OT infrastrukture.

Omenjene vidike posredno ali neposredno obravnava direktiva NIS2, ki jo je Evropska unija sprejela kot regulativni okvir za krepitev kibernetske odpornosti evropskega prostora, dvig varnosti dobavnih verig in standardizacijo postopkov obveznega poročanja o kibernetskih incidentih v državah članicah. Direktiva na ta način poudari pomen doslednega poročanja in izmenjave obveščevalnih informacij znotraj posameznih evropskih držav, kakor tudi med njimi, z namenom dviga splošne ravni kibernetske varnosti v Evropski uniji. V nadaljevanju članka opišemo nekatere ključne vidike, pristope in tehnološke rešitve za sodelovanje in koordinacijo med deležniki na področju kibernetske varnosti. Predstavljeni izsledki so rezultat razvojno-raziskovalnega projekta Horizon 2020 CyberSEAS, ki vpeljuje celovit nabor rešitev za zagotavljanje kibernetske varnosti kritične elektroenergetske infrastrukture.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Odzivanje in koordinacijo glede kibernetskih incidentov je potrebno standardizirati in avtomatizirati

Učinkovito in hitro odzivanje na incidente je ključnega pomena za kibernetsko varnost, saj omeji vplive kibernetskih incidentov, skrajša čas okrevanja ter zmanjša stroške, potrebne za odpravo posledic in obnovitev normalnega delovanja. Še posebej v okoljih kritične infrastrukture mora upoštevati vidike različnih deležnikov, ki se povezujejo v proizvodnih in dobavnih verigah, slediti nacionalni zakonodaji ter zagotoviti skladnost z direktivo NIS2 z namenom izboljšanja čezmejnega sodelovanja in poročanja nacionalnim odzivnim centrom v primerih resnejših incidentov. Kot je določeno v NIS2 in nacionalnih odzivnih načrtih (npr. v Sloveniji v načrtu NOKI), morajo organizacije slediti standardiziranim pravilom in postopkom poročanja v skladu z ocenjenim vplivom in posledicami incidentov.

Za dosledno zagotavljanje skladnosti z zakonodajnimi zahtevami ne zadošča, da organizacije vpeljejo izolirana pravila in mehanizme poročanja, temveč je priporočljivo, da jih integrirajo v standardizirane odzivne procedure (angl. playbooks). To omogoči, da v korporativnih okoljih in varnostnih operativnih centrih (VOC-ih) poročila o incidentih, ki jih posredujemo nacionalnim ali področnim odzivnim ekipam (CERT-om) avtomatiziramo, in jih tako prožimo samodejno v sklopu širšega nabora odzivnih aktivnosti. Sodelovalne aktivnosti med VOC-i in CERT-i, podprte z ustreznimi orodji, omogočijo koordiniran odziv na kibernetske incidente in tako znatno zmanjšajo potencialne negativne vplive le-teh na korporativne sisteme in kritične infrastrukture. Za potrebe koordinacije je najučinkoviteje poseči po platformah in orodjih, ki podpirajo izmenjavo obveščevalnih informacij (Cyber Threat Intelligence – CTI), ker lahko z njimi osnovne parametre napadov, kot so tipi napadov in IP naslovi napadalcev, ter ostale indikatorje kompromitiranja (Indicators of Compromise – IoC) neposredno delimo s širšo skupnostjo povezanih deležnikov na področju kibernetske varnosti. To omogoči drugim deležnikom takojšnje proaktivno ukrepanje za preprečevanje istih incidentov. Najbolj uveljavljeni tovrstni platformi sta STIX/TAXII in MISP (Malware Information Sharing Platform). Njuno uporabo velja priporočiti, saj poskrbita za varno izmenjavo informacij o kibernetskih dogodkih in ukrepih ter s tem zagotovita potreben nivo zaupanja med deležniki, ki se povezujejo v skupnosti z namenom izmenjave obveščevalnih informacij.

Pristop k oblikovanju in implementaciji odzivnih procedur

Doseganje skladnosti z direktivo NIS2 zahteva vzpostavitev formata za opis strojno berljivih, izvedljivih in izmenljivih odzivnih procedur ter oblikovanje več nivojskega procesa, ki lahko omogoči varnostnim analitikom, da specificirajo in uskladijo odzivne procedure na podlagi informacij in zahtev iz različnih korporativnih okolij in virov. Takšno procesno ogrodje mora zagotoviti opisovanje odzivnih procedur in znanja na več nivojih abstrakcije, in sicer v nestrukturiranem ali pol strukturiranem zapisu, v grafični modelirni notaciji, kakršna je BPMN (Business Process and Notation), ter v izvedljivi obliki, ki lahko sloni na standardu CACAO Security Playbooks, za katerim stoji organizacija OASIS. Med posameznimi nivoji morajo biti vzpostavljene ustrezne preslikovalne sheme.

Za izboljšavo postopkov poročanja in izmenjave CTI je torej ključen strukturiran pristop k oblikovanju odzivnih procedur. V začetnem koraku identificiramo scenarije napadov, ki zahtevajo poročanje in koordinacijo s CERT-i. V naslednjem koraku pripravimo za te scenarije splošne in delno strukturirane odzivne procedure, ki vključujejo vse faze odzivanja na incidente, kot jih določa NIST (National Institute of Standards and Technology), in sicer (1.) pripravo, (2.) zaznavanje in analizo, (3.) zamejitev, odpravo napak in okrevanje ter (4.) aktivnosti po incidentu. Te procedure morajo hkrati slediti tudi zahtevam nacionalnih CERT-ov. V tretjem koraku modeliramo odzivne procedure bolj natančno v grafični notaciji BPMN. Definirane aktivnosti in pravila opredelijo zahtevano koordinacijo s CERT-i, pri čemer določijo, kdaj in kako je potrebno poročati o incidentih glede na njihovo klasifikacijo, resnost, obseg ter vpliv s funkcionalnega in informacijskega vidika. V četrtem koraku lahko nato naslovimo izvedljive odzivne procedure. V ta namen posežemo po standardni notaciji CACAO, ki jo že podpirajo nekatera orodja za urejanje in izvajanje odzivnih procedur. Višje nivojsko notacijo BPMN pri tem z uporabo standardnega slovarja preslikamo v nižje nivojski zapis CACAO. Prva verzija zapisa v formatu CACAO praviloma še ni strojno izvedljiva, saj jo dobimo z neposredno preslikavo iz višje nivojske specifikacije. Zato jo v petem, zadnjem koraku dopolnimo z izvajalnimi, konfiguracijskimi in infrastrukturnimi parametri.

Koraka 3 in 4 vzpodbujata sodelovanje VOC-ov in CERT-ov ter izmenjavo modelov prek skupnega repozitorija. Priporočljivo je namreč identificirati obstoječe odzivne procedure za iste tipe incidentov ter jih ponovno uporabiti ali prilagoditi za specifično korporativno in informacijsko okolje. S tem oblikujemo skupno bazo odzivov na kibernetske incidente, ki standardizira odzivne procedure za posamezne tipe incidentov in jo lahko različne organizacije iz istega ali sorodnih sektorjev učinkovito ter hitro uporabijo. Moč takšnega pristopa je, da vpeljuje ter krepi sektorsko in meddržavno izmenjavo enotnih procedur za odzivanje, poročanje in koordinacijo.

Poenotenje evropskega kibernetskega prostora

Pri standardizaciji mehanizmov poročanja je potrebno upoštevati zakonodajne specifike posameznih držav članic Evropske unije. V skladu s prej opisanim procesom oblikovanja odzivnih procedur najprej le-te za različne tipe kibernetskih incidentov definiramo na nacionalnih nivojih. Nato lahko poiščemo stične točke in jih do neke mere poenotimo ter prikrojimo za enotni evropski kibernetski prostor. Da zagotovimo verodostojnost odzivnih procedur in pravil za koordinacijo z nacionalnimi CERT-i, moramo nasloviti več vidikov nacionalnih priporočil, praks in zakonodaje. Analiza, ki smo jo opravili v sklopu projekta CyberSEAS, izpostavi več podobnosti in skupnih mehanizmov, ki jih udejanjajo države članice Evropske unije:

- Zahtevana koordinacija s CERT-i: nosilci ključnih in digitalnih storitev so v vseh državah EU obvezani poročati nacionalnim CERT-om o kibernetskih incidentih z znatnimi posledicami.
- Odzivne procedure in pravila: v vseh državah temeljijo bodisi na modelu ISO 27001/27035 ali na NIST-ovem standardiziranem štiri faznem odzivnem procesu.
- Podatkovne strukture, formati in orodja za poročanje: najpogosteje so v uporabi standardni spletni obrazci za poročanje, poleg teh pa so bile uvedene tudi nekatere naprednejše tehnike,



kot so samodejna obdelava opozoril iz integriranih sistemov, namenska orodja za poročanje o incidentih (CSIRT Notification Format) ter protokoli STIX/TAXII in TLP (Traffic Light Protocol).
- Komunikacijska strategija in mehanizmi za deljenje informacij: slonijo na odzivanju v realnem času, izmenjavi informacij, tehnični podpori, koordinaciji z drugimi nacionalnimi in sektorskimi CERT-i ter javnem in situacijskem zavedanju.

Sodelovanje z uporabo platforme MISP

MISP (Malware Information Sharing Platform) je odprtokodna platforma za izmenjavo tehničnih in ne tehničnih informacij o zlonamerni programski opremi, kibernetskih napadih, incidentih in grožnjah ter drugih splošnih obveščevalnih informacij. Podatki so predstavljeni v standardizirani in strukturirani obliki, tako da je poleg osnovnih varnostnih podatkov, kot so indikatorji kompromitiranja in varnostni dogodki, možno shranjevati in deliti tudi kompleksnejše strukture, kakršne so odzivne procedure. Na ta način se lahko varnostne ekipe poenotijo glede obravnave varnostnih informacij, s čimer postanejo zmožne hitrejše razpoznave in premostitve varnostnih groženj. Sprotna izmenjava aktualnih podatkov o varnostnih dogodkih lahko pomaga organizacijam in njihovim varnostnim operativnim centrom pri učinkovitejšem preprečevanju kibernetskih napadov. Osnovni pogoj je, da se organizacije, sektorski VOC-i in nacionalni CERT-i povezujejo v skupnosti, tako da omogočijo pretok informacij med njihovimi lastnimi strežniki za platformo MISP.

Obstaja več scenarijev povezovanja deležnikov v skupnosti. Prva možnost je neposredno povezovanje varnostnih operativnih centrov. V primeru zaznanega varnostnega dogodka tako z objavo le-tega na platformi MISP posamezen VOC takoj obvesti vse ostale deležnike o potencialnem tveganju.

Še več koristi dosežemo z uporabo platforme MISP za povezovanje varnostnih operativnih centrov z nacionalnimi CERT-i. V tem scenariju postane MISP zmogljiva platforma za izmenjavo obveščevalnih informacij med sektorskimi in organizacijskimi VOC-i ter nacionalnimi CERT-i v skupnem evropskem kibernetskem prostoru. Nacionalni CERT lahko sledi več pretočnim kanalom, ki v obliki indikatorjev kompromitiranja izpostavijo na novo odkrite ranljivosti in vzorce neobičajnega prometa ali delovanja kot posledice kibernetskih incidentov. Čim je razpoznan relevanten indikator (npr. zlonameren naslov IP), posreduje CERT le-tega skozi povezano omrežje strežnikov MISP celotni skupnosti. Indikatorji so tako propagirani do sektorskih VOC, v okviru katerih se lahko samodejno sprožijo mehanizmi za zaščito infrastrukture varovanega ekosistema. V primeru zlonamernega naslova IP se lahko npr. na požarni pregradi vzpostavi pravilo za takojšnje blokiranje tega naslova. To znatno poveča odpornost IT in OT infrastruktur. Nekateri nacionalni odzivni centri, med njimi SI-CERT, vzpodbujajo ponudnike bistvenih storitev in ostale entitete, kot so vladne organizacije, k vključevanju v lokalna MISP omrežja, s čimer povečujejo učinkovitost in hitrost širjenja obveščevalnih informacij ter s tem odpornost infrastruktur in korporativnih ekosistemov.

MISP je tudi primerna platforma za poročanje nacionalnim CERT-om o kibernetskih incidentih. Ker se v praksi v Evropski uniji uporabljajo različni, ne poenoteni načini poročanja in ker še vedno prednjači ročno poročanje prek spletnih obrazcev, ki ne zagotavlja avtomatizacije, v sklopu priporočil projekta CyberSEAS predlagamo uporabo platforme MISP, kot standardnega medija za poročanje. To prinaša več prednosti. Poročanje lahko avtomatiziramo in ga izvedemo neposredno, kot del implementiranih odzivnih procedur. Nadalje lahko ob objavi novega zaznanega varnostnega dogodka, ki ga s preiskavo na višjih nivojih VOC potrdimo, kot dovolj resen incident na platformi MISP, hkrati v skupnem zapisu o dogodku vključimo tudi podatke, ki jih je potrebno poročati nacionalnemu odzivnemu centru in so namenjeni izključno zanj. Nazadnje tako predpišemo in zagotovimo standardno podatkovno strukturo za poročanje. Le-ta ima obliko objekta NOKI (Nacionalni načrt odzivanja na kibernetske incidente) in vsebuje vsa podatkovna polja, ki jih predpisuje NOKI, kar vključuje poročevalca, čas incidenta, stopnjo resnosti, klasifikacijo in opis incidenta idr.

Sklep

Implementacija mehanizmov sodelovanja na področju kibernetske varnosti prinaša več prednosti in priložnosti. S standardizacijo in izmenjavo odzivnih procedur ter mehanizmi za deljenje obveščevalnih informacij o kibernetskih grožnjah se vključujemo v nacionalne in mednarodne skupnosti, izboljšamo reaktivno odzivanje na kibernetske napade in proaktivno preprečevanje le-teh, podpremo odločanje na strateškem in taktičnem nivoju ter dvignemo splošno odpornost IT in OT infrastrukture. Tehnike in tehnologije za podporo sodelovanju in izmenjavi informacij lahko integriramo z drugimi temeljnimi tehnologijami za kibernetsko varnost, kot so požarne pregrade ali sistemi SIEM in SOAR, prav tako pa tudi z javnimi bazami in repozitoriji za izmenjavo informacij o ranljivostih in tehnikah napadov, kot so NVD, MITRE ATT&CK, CAPEC, CIS Security Controls idr. S tem še dodatno dvignemo nivo odpornosti. ■

BIOMETRIJA

Rešitev v skladu z ZVOP-2 (GDPR) zahtevami

- Pomoč pri pridobitvi **IP soglasja** in pri izdelavi **ocene učinka**
- Certifikat Grade4 za **najvišji nivo varnosti** po SIST EN 60839-11-1
- **Brezkontakten in sočasen zajem** slik obeh šarenic (za boljšo uporabniško izkušnjo)
- Možnost izvedbe verifikacije 1-1 ali identifikacije 1-N



HSI IRIS ID

www.hsi.si info@hsi.si 07 600 19 60

Odprite vrata od kjerkoli

doorcloud

www.doorcloud.com

Brez kartic, brez čitalcev



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

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



SPICA

Avtorica: ga. Urša Kragelj / koordinatorka projektov, CER Partnerstvo za trajnostno gospodarstvo*



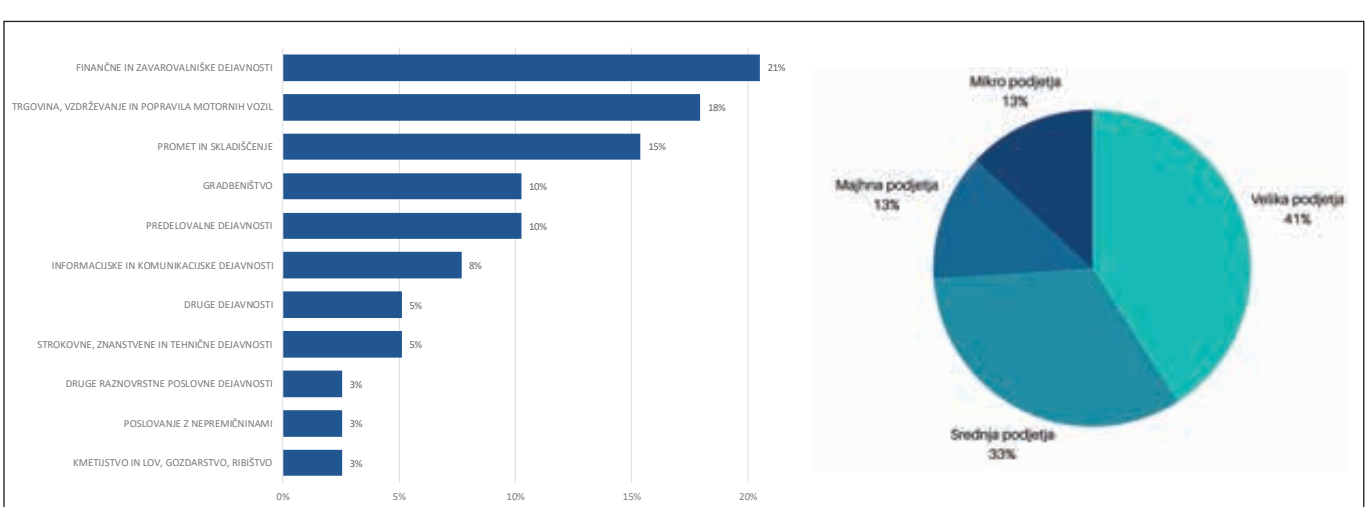
GREEN STAR – PRVA ANALIZA O ODNOSU SLOVENSKIH PODJETIJ DO TRAJNOSTNEGA POSLOVANJA

S pomočjo podatkov Green Star, certifikata za uvajanje trajnostnih ESG vidikov in podnebnega ukrepanja v podjetjih, ki ga je razvil CER Partnerstvo za trajnostno gospodarstvo, je bila marca letos narejena prva analiza v slovenskem prostoru o odnosu podjetij do trajnostnosti. Na eni strani je ugotovila, da so podjetja premalo ambiciozna, na drugi pa pokazala znaten napredek tistih, ki so v proces certificiranja stopila že drugič.

Enajst gospodarskih sektorjev

V analizo Green Star so bila zajeta mikro, majhna, srednja in velika podjetja iz enajstih različnih gospodarskih sektorjev.

Podjetja, ki so leta 2022 vstopila v certifikacijski proces Green Star, so z odgovori na 115 vprašanj prispevala k širšemu razumevanju trenutnega stanja in ciljev, ki si jih je slovensko gospodarstvo zadalo na področju trajnostnega upravljanja.



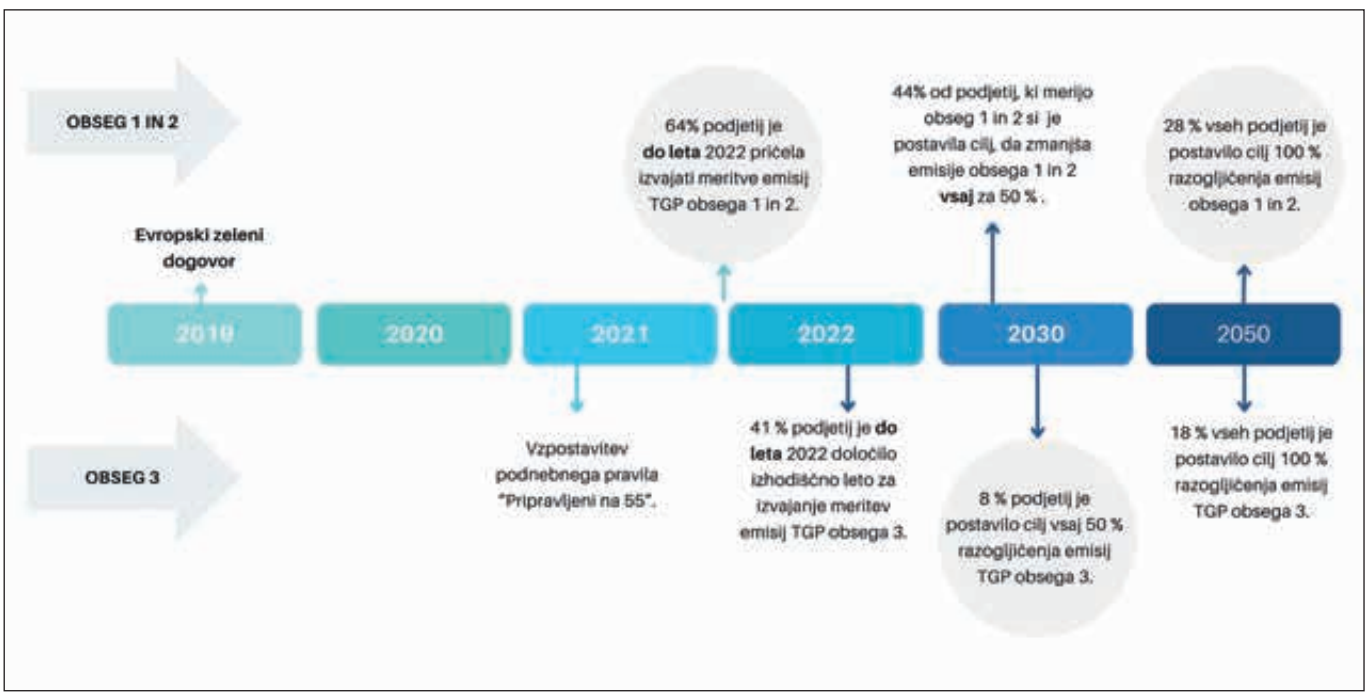
*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Podjetja so premalo ambiciozna

Izkazalo se je, da bi številna podjetja lahko bila bolj ambiciozna na področju razogljičenja in uvajanja trajnosti v poslovanje. **Ocena, ki je bila narejena s pomočjo 53 kriterijev ocenjevanja, je pokazala, da je večina podjetij premalo ali le delno ambicioznih. Sploh v luči evropskega zelenega dogovora, ki predvideva razogljičenje Evropske unije do leta 2050.** Pogled skozi prizmo omenjenega dogovora je razkril, da je pri zmanjševanju emisij v lastnem poslovanju dovolj ambiciozna le slaba tretjina podjetij, pri zmanjševanju emisij vzdolž verige vrednosti pa zgolj 18 % podjetij.

Pokazale so se številne vrzeli

Kljub temu, da 90 % podjetij pozna lastna podnebna tveganja, številna nimajo vzpostavljenih sistemskih pristopov za soočanje z njimi. Pod vprašaj je bila postavljena tudi verodostojnost podatkov. Visok odstotek podjetij sicer izračuna svoj ogljični odtis, a tega pri neodvisni organizaciji preveri le slaba petina, kar postavlja pod vprašaj njegovo točnost.



Ocena, ki je bila narejena s pomočjo 53 kriterijev ocenjevanja, je pokazala, da je večina podjetij premalo ali le delno ambicioznih. Sploh v luči evropskega zelenega dogovora, ki predvideva razogljičenje Evropske unije do leta 2050.

Manjša podjetja v trajnostnem poročanju vidijo priložnost

Kljub številnim pomanjkljivostim, je analiza ugotovila kar nekaj pozitivnih premikov. Poleg velikih, tudi manjša podjetja že pričenjajo s trajnostnim poročanjem, kar je spodbudno, saj nova Direktiva glede poročanja podjetij o trajnostnosti (CSRD) od njih tega še ne zahteva. Slednja so se trajnostnega poročanja lotila, ker so v tem videla priložnost.

Vidno postaja, da trajnost ni več domena posameznih oddelkov ali posameznikov. Trajnostno ravnanje se postopoma umešča v jedro poslovanja in odločitve, glede trajnostnega poslovanja in doseganja podnebne nevtralnosti pa se prenašajo na najvišjo vodstveno raven.

Največji premik je bil zaznan pri tistih podjetjih, ki so v certificiranje stopila dve leti zapored. Kar 50 % podjetij je namreč prejelo višjo Green Star oceno, kot leto pred tem, kar kaže na to, da spremljanje in merjenje podatkov podjetjem dokazano prinese napredek.

Vidno postaja, da trajnost ni več domena posameznih oddelkov ali posameznikov. Trajnostno ravnanje se postopoma umešča v jedro poslovanja in odločitve, glede trajnostnega poslovanja in doseganja podnebne nevtralnosti pa se prenašajo na najvišjo vodstveno raven.

»Green Star[1] je unikatno in prvo tovrstno orodje v Sloveniji, ki podjetjem pomaga na težki poti trajnostne preobrazbe, na sicer relativno enostaven način. Deluje kot navigator za podjetja – jih usmerja, pomaga meriti in zbirati podatke in nenazadnje opolnomoči vse zaposlene oziroma tiste, ki so vpleteni v proces certificiranja«.[2]

Green Star je pripomoček za sistematično spremljanje ESG podatkov

ESG podatki so postali ključno orodje za uspešno poslovanje in trajnostni razvoj podjetij v 21. stoletju. Kljub jasnim standardom za trajnostno poročanje pa se mnoga podjetja še vedno spopadajo z izzivom, saj premalo razumejo, kateri ESG podatki so ključni, in pogosto ne izvajajo ustreznih meritev, zajema in obdelave podatkov. Posledično ESG podatkov ne uporabljajo kot osnove za resne strateške poslovne odločitve.

Podjetja, ki so se podala na pot procesa Green Star, potrjujejo, da je Green Star orodje, ki ne le meri, ampak tudi svetuje, usmerja in opolnomoči. Proces je pripomogel k povezovanju različnih oddelkov v podjetjih ter spodbudil preobrat v dojemanju trajnostnih podatkov, ki jih mnogi prej sploh niso opazili. Letos na voljo izboljšana verzija Green Star 2.0

Podjetjem vseh velikosti in gospodarskih sektorjev je na voljo posodobljena verzija vprašalnika Green Star 2.0, ki je usklajena z ESRS standardi trajnostnega poročanja. Podjetja vodi preko vseh pomembnih ESG tematik trajnostnega upravljanja, omogoča vpogled v napredek in dosežke podjetja na trajnostnih ključnih kazalnikih uspešnosti, ponuja grafične prikaze stanja, tudi napredka, in na enem mestu združuje ključne podatke o delovanju, ciljih, ukrepih, porabi energentov in ogljičnem odtisu.

»Green Star[1] je unikatno in prvo tovrstno orodje v Sloveniji, ki podjetjem pomaga na težki poti trajnostne preobrazbe, na sicer relativno enostaven način. Deluje kot navigator za podjetja – jih usmerja, pomaga meriti in zbirati podatke in nenazadnje opolnomoči vse zaposlene oziroma tiste, ki so vpleteni v proces certificiranja«.[2]

1 Več na www.green-star.si

2 Ana Struna Bregar, izvršna direktorica CER Partnerstvo za trajnostno gospodarstvo ■



INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.

INFORMATIKA



Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

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

Vplivi kibernetskih napadov na različna področja v energetiki:

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

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

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

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

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

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

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

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

ČAS JE ZA ODLOČILEN KORAK

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

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

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

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

www.informatika.si



STOLETJU PRENOSA ZAVEZANI LJUDJE

Od pionirjev elektroprenosa Fala-Laško do skrbnikov nacionalnega elektroenergetskega sistema

Prvi 77-kilometrski 80 kV prenosni daljnovod v Sloveniji je bil postavljen leta 1924, in sicer med hidroelektrarno Fala in transformatorsko postajo v Laškem (RTP Laško) ter naprej do Termoelektrarne Trbovlje. V RTP Laško je za vzdrževalno-obratovalna dela skrbela skromna, a ambiciozna ekipa štirih zaposlenih, ki so jo sestavljali obratovodja, dva stikalca in ključavničar. Z razvojem in rastjo prenosnega omrežja sta se skozi desetletja povečevala tako število kot kadrovska struktura zaposlenih. Danes je v družbi ELES približno 550 zaposlenih, ki uresničuje poslanstvo zagotavljanja varnega, zanesljivega in kakovostnega prenosa električne energije.

4
zaposleni

1924 – RTP LAŠKO

604
zaposlenih

2024 – SKUPINA ELES