Korporativna varnost

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

Letnik 2026, maj • št. 41

Slovensko združenje za korporativno varnost vključujoča platforma sodelovanja

Svečana podelitev prestižnih nagrad “Slovenian Grand Security Award” Brdo pri Kranju, 18.-19. maj 2026

CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

KIBERNETSKA VARNOST 24/7/356

Podjetja se soočajo z vse pogostejšimi kibernetskimi napadi, zato ni več vprašanje, ali boste napadeni, temveč kdaj.

Sodoben pristop zahteva premik od pasivnega preprečevanja kibernetskih napadov k proaktivnemu odkrivanju in takojšnjemu odzivu. Vse to izvajajo naši visoko certificirani strokovnjaki iz **Centra kibernetske varnosti in odpornosti**, ki **vse dni v letu**, spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske grožnje, odkrivanju in takojšnjemu odzivu.

Telekom Slovenije, d.d., Ljubljana

TelekomSlovenije
Vedno na boljše.

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 2026

Izvod revije je brezplačen

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

ISSN 2232-6170

Pred nami so Dnevi korporativne varnosti, ki predstavljajo praznik, festival stroke in srečanje vseh, ki se v svojem profesionalnem okolju soočajo z zahtevnimi procesi obvladovanja varnostnih tveganj. Letošnje srečanje poteka v času zaostrenih geopolitičnih razmer, kjer aktualni konflikti, povezani z vojno v Iranu, resno vplivajo na globalne tokove energije in neposredno ogrožajo stabilnost energetske oskrbe Evrope. Posledice teh procesov bodo v prihodnjem obdobju močno zaznamovale tudi gospodarsko okolje, kar dodatno potrjuje, da varnost ni več zgolj podporna funkcija, temveč ključen dejavnik stabilnosti in razvoja.

Varnostno okolje je postalo tako zahtevno in kompleksno, da upravljanje tveganj ni več mogoče s parcialnimi pristopi. Celovitost pristopov in spoznanje, da lahko le z vključevanjem vseh deležnikov v procese zagotavljanja varnosti ter neprekinjenosti delovanja ključnih družbenih sistemov dosežemo ustrezne rezultate, postajata temelj sodobnega razumevanja odpornosti. V tem okviru je korporativna varnost kot proces postala neločljiv del celovitega sistema zagotavljanja stabilnosti družbe.

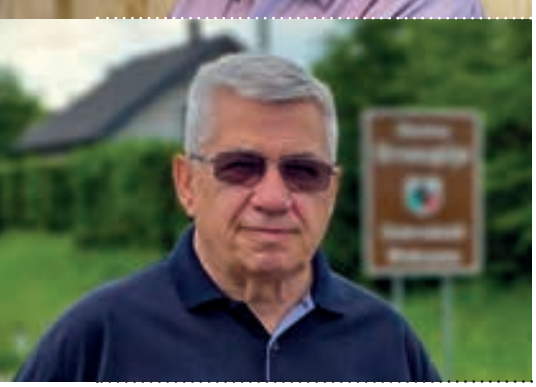
Na tem mestu velja izpostaviti misel, zapisano v prispevku predsednika Slovenskega združenja za korporativno varnost, da »prihodnost korporativne varnosti ni zgolj v njenem notranjem razvoju znotraj organizacij, temveč v njeni sposobnosti povezovanja, sodelovanja in soustvarjanja širšega varnostnega okolja. Le s takšnim pristopom bo mogoče preseči iluzijo nadzora in vzpostaviti dejansko odpornost, tako na ravni organizacij kot tudi celotne družbene skupnosti«.

Odpornost je v zadnjem obdobju postala ključna vrednota, ki ji na vseh ravneh namenjamo izredno veliko pozornosti. Prav zaradi naraščajoče nepredvidljivosti globalnega okolja, od energetskih pretresov do varnostnih kriz, je postala osrednja tema tudi tokratne konferenčne številke revije.

Z izborom intervjujev in prispevkov smo omogočili vpogled v strateške perspektive ključnih odločevalcev ter hkrati v konkretne izkušnje strokovnjakov, ki izvajajo varnostne procese na operativni ravni. Prav preplet strateškega razmišljanja in operativne izvedbe ostaja ključen za oblikovanje učinkovitih varnostnih sistemov, ki bodo sposobni odgovarjati na dinamične spremembe v varnostnem okolju. Predstavljene vsebine odražajo aktualna dogajanja na področju korporativne varnosti in so zasnovane tako, da bodo strokovni javnosti v podporo pri iskanju ustreznih rešitev, oblikovanju novih pristopov ter razvoju strateških usmeritev za doseganje večje odpornosti organizacij.

Prepričani smo, da bo predstavljena vsebina bralkam in bralcem nudila dodatno strokovno podporo ter jih spodbudila k nadaljnjemu razmisleku o pomenu usklajenega, sistematičnega in celostnega pristopa k obvladovanju varnostnih tveganj. S tem želimo prispevati k dvigu splošne varnostne kulture in krepitvi odpornosti organizacij ter družbe kot celote v sodobnem, vse bolj negotovem in izzivov polnem varnostnem okolju.

izr. prof. dr. Denis Čaleta
Glavni urednik



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

INTERVJU
mag. Aleksander Mervar, direktor ELES*

PRENOSNA OMREŽJA IN EVROPSKA INTEGRACIJA: KLJUČ DO ENERGETSKE ODPORNOSTI

Prenosna omrežja električne energije so temelj stabilnega in zanesljivega delovanja sodobnih družb ter ključni povezovalni element evropskega energetskega prostora. Njihova vloga presega nacionalne okvire, saj omogočajo učinkovito čezmejno izmenjavo energije in uravnoteženje sistemov v času vse večjih nihanj. V kontekstu energetske tranzicije in geopolitičnih izzivov postaja njihova odpornost strateškega pomena za celotno Evropo. Prav integrirana in tehnološko napredna prenosna omrežja predstavljajo enega ključnih vzvodov za zagotavljanje energetske varnosti ter trajnostne prihodnosti. O teh izzivih in prihodnjih usmeritvah smo se pogovarjali z direktorjem ELES, mag. Aleksandrom Mervarjem.

Energetska kriza je razkrila številne ranljivosti evropskih sistemov – kako ocenjujete odpornost slovenskega prenosnega omrežja danes in kje so njegove ključne strateške prednosti?

Slovensko prenosno omrežje je zaradi svoje geografske lege in močne čezmejne prepletenosti integralni del regionalnega ter širšega evropskega elektroenergetskega sistema. Prenosna infrastruktura, s katero upravlja ELES in na kateri temelji čezmejni prenos električne energije, je v preteklosti ob različnih vremenskih neprilikah, tudi denimo ob februarskem snegolomu ali marčevskem vetrolomu, dokazala svojo izjemno robustnost. To je v veliki meri posledica tako ustreznega vzdrževanja kot tudi nenehnih investicij v prenosno omrežje. Omenil bi prečni transformator v Divači, 400kV povezava Krško-Beričevo, nova 400kV povezava z Madžarsko Cirkovce - Pince. V zadnjih petnajstih letih je ELES v prenosno infrastrukturo vložil več kot milijardo evrov, kar je za državo naše velikosti izjemno veliko. Te naložbe se osredotočajo na tri področja: fizično krepitev omrežja, podporo prehodu na zeleno energijo z razpršenimi obnovljivimi viri in digitalizaciji ter kibernetski varnosti. Da bi naše omrežje pripravili na prihodnost, smo dali prednost sofisticiranim sistemom pred tradicionalno infrastrukturo. Projekti, kot je

Mediji v zadnjem času zelo radi uporabljajo izraze kot so denimo digitalizacija in pametna omrežja, toda dejstvo je, da se v Elesu s tem dejavno ukvarjamo že dve desetletji in rezultati so danes tukaj.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Torej, se spomnite električnega mrka v Španiji letos? Celotna Evropa je brez zavor vlagala v proizvodnjo iz obnovljivih virov energije, ni pa vlagala v distribucijsko omrežje. Ves čas sem zagovarjal stališče, da moramo najprej okrepiti omrežje.

TUNE – 400 milijonov evrov vredna pobuda s slovaškimi in madžarskimi partnerji – so osrednjega pomena za naša prizadevanja za omogočanje čezmejnih pretokov ter seveda ključno krepijo odpornost slovenskega elektroenergetskega sistema.

Tudi v operativnem smislu je obratovanje prenosnega omrežja podprto z dobro vzpostavljeno koordinacijo s sosednjimi operaterji prenosnih sistemov, tako na regionalni ravni kot tudi širše. To omogoča učinkovito predvidevanje kritičnih situacij in obvladovanje teh. Vse to prispeva k stabilnosti ne le slovenskega elektroenergetskega sistema, temveč tudi k stabilnosti v širši regiji.

Zavedamo se in v zadnjem obdobju nas o tem uči vse več nepredvidenih dogodkov, da so ekstremni vremenski pojavi vse pogostejši ter vse izrazitejši dejavnik tveganja tudi za elektroenergetsko infrastrukturo. Zato temu področju namenjamo pozornost tudi z vidika načrtovanja in razvoja omrežja: izvajamo kartiranja omrežja, prepoznavamo območja večje ranljivosti ter na tej podlagi načrtujemo in usmerjamo ustrezne tehnične, razvojne ter investicijske ukrepe, da zagotovimo pravočasne investicije v prenosno infrastrukturo. Prav to bo tudi v prihodnje, skupaj z digitalizacijo vodenja sistema in poglobljenim regionalnim sodelovanjem, ključno za nadaljnjo krepitev odpornosti prenosnega omrežja v razmerah naraščajočih obremenitev ter večje spremenljivosti pretokov zaradi vključevanja obnovljivih virov.

Mediji v zadnjem času zelo radi uporabljajo izraze kot so denimo digitalizacija in pametna omrežja, toda dejstvo je, da se v Elesu s tem dejavno ukvarjamo že dve desetletji in rezultati so danes tukaj. Mednarodne ocene, denimo s strani Svetovnega energetskega sveta (*World Energy Council – WEC*), ki ocenjuje slovensko energetiko, so v tem pogledu najbolj zgovorne: v tako imenovani analizi »trilema« WEC ocenjuje energetiko po treh ključnih dimenzijah, in sicer energetski varnosti, energetski enakopravnosti ter okoljski trajnosti. Slovenija je po zadnjem objavljenem indeksu sve-

tovne energetske »trileme«, ta je bil v letu 2024, zasedla odlično 11. mesto.

Pogosto slišimo, da je prenosno omrežje relativno robustno, medtem ko so največje ranljivosti na ravni distribucije – ali ta razkorak predstavlja sistemsko tveganje in kako ga nasloviti na nacionalni ravni?

Najprej moram povedati, da omejitve distribucijskega omrežja vsekakor obstajajo, a ne glede na to se strinjam s stališčem distributerjev, da moramo vendarle preudarno in racionalno pristopiti do nadgradenj omrežja ter novih investicij. Seveda investicije so potrebne, a pred očmi moramo imeti nacionalni interes, ne parcialne interese posameznikov. Če se na primer posameznik na nekem območju odloči, da bi rad zgradil sončno elektrarno, stanje v omrežju pa trenutno tega ne dopušča oziroma bi bila za priključitev v omrežje najprej potrebna velika investicija distributerja, ne moremo govoriti o racionalni porabi (tudi) javnih sredstev za uresničevanje interesov posameznikov.

Torej, se spomnite električnega mrka v Španiji letos? Celotna Evropa je brez zavor vlagala v proizvodnjo iz obnovljivih virov energije, ni pa vlagala v distribucijsko omrežje. Ves čas sem zagovarjal stališče, da moramo najprej okrepiti omrežje. Tudi zato v družbi ELES izvajamo evropske projekte pametnih omrežij, denimo Green Switch, SinCroGrid, ki pripomorejo k temu, da omrežje prenese veliko razpršenih virov. Toda poudariti moram, da te zagonetke z obnovljivimi viri ni še nihče dokončno rešil.

Kot direktor družbe ELES vidim možne izboljšave predvsem v boljšem usklajevanju postopkov med prenosnim in distribucijskim omrežjem ter vlaganjih v odpornost distribucijske infrastrukture. Tako družba ELES kot distribucijska podjetja so sicer trenutno sredi rekordnega razvojnega investicijskega cikla. Medtem ko je družba ELES v minulih letih opravila domačo nalogo in v omrežje neprestano vlagala, zato v naslednjem desetletju načrtuje »le« za 1,2 milijardi evrov vlaganj, pa na drugi strani elektrodistribucijska podjetja načrtujejo investicije v višini 3,94 milijarde evrov. Želim si, da bi jih izvedla in s tem ta razkorak, kot ste vprašali, premostila, žal pa ugotavljam, da v tem trenutku za načrtovane investicije še nimajo zagotovljenih 2,1 milijarde evrov finančnih virov. Največji potencialni viri za obdobje po letu 2028 so Podnebni sklad in kohezijski sklad, ki lahko pomembno

Kot direktor družbe ELES vidim možne izboljšave predvsem v boljšem usklajevanju postopkov med prenosnim in distribucijskim omrežjem ter vlaganjih v odpornost distribucijske infrastrukture. Tako družba ELES kot distribucijska podjetja so sicer trenutno sredi rekordnega razvojnega investicijskega cikla.

pripomoreta k financiranju investicij. Tako lahko kot direktor sistemskega operaterja kombiniranega prenosnega in distribucijskega omrežja ugotovim le, da bi bilo v tem trenutku mogoče zagotoviti dodatna finančna sredstva za financiranje investicije ter s tem premostitev razkoraka z dvigom tarif za distribucijsko omrežje od leta 2027 naprej, kar pa bi gotovo predstavljalo velik izziv za končne porabnike.

Dodatno je treba izboljšati procedure rednega vzdrževanja, ki bodo pripomogle k višji fizični odpornosti omrežja. Za hitre akcije obnove morebitnega porušenega in poškodovanega omrežja v vremenskih ujmah, tako prenosnega kakor tudi distribucijskega, je treba še povečati usposobljenosti ekip, zagotoviti zadovoljivo opremo in zadostno havarijsko rezervo ključne visokonapetostne opreme in materialov. Zagotoviti je treba tudi aktivna pogodbena razmerja za primere večjih posegov z zato usposobljenimi izvajalci in dobavitelji, predvsem v smislu predčasnega priznanja sposobnosti in sklenitve okvirnih sporazumov. Za samo posodobitev infrastrukture pa mora država zagotoviti ustrezno hitre postopke umeščanja v prostor, predvsem za potrebne novogradnje in možnost obnove obstoječih prenosnih ter distribucijskih poti brez ponovnega umeščanja v prostor.

Kakšne investicije so danes ključne za dolgoročno odpornost elektroenergetskega sistema – gre predvsem za krepitev infrastrukture, digitalizacijo ali spremembo upravljanja sistema?

Predvsem pametne investicije, napredne energetske rešitve, ki prispevajo k celostni digitalizaciji oziroma digitalni preobrazbi našega elektroenergetskega sektorja. Zeleni prehod – ne glede na to, ali govorimo o Sloveniji, Španiji ali ZDA – bo obstal ali padel na vzdržnosti omrežja in vseh njegovih sestavnih delov. Ko namreč govorimo o zelenem prehodu, v splošnem ljudskem dojemanju to pomeni predvsem celo množico obnovljivih virov energije, ob besedni zvezi instinktivno pomislimo na sončne elektrarne na strehah hiš ali na vetrna pola. Ampak za uspešen zeleni prehod je veliko pomembnejše primerno digitalizirano

Zeleni prehod – ne glede na to, ali govorimo o Sloveniji, Španiji ali ZDA – bo obstal ali padel na vzdržnosti omrežja in vseh njegovih sestavnih delov.

elektroenergetsko omrežje, česar pa se javnost bistveno premalo zaveda. Nove digitalne rešitve bodo namreč omogočile boljše povezovanje različnih sistemov, pametnejše upravljanje napetosti v omrežju in učinkovitejšo ter preglednejšo izmenjavo podatkov. V tem kontekstu velja omeniti, da sta družbi ELES in Hitachi Energy s podpisom pogodbe o strateškem sodelovanju začeli projekt »Sistem vodenja naslednje generacije«. Razvijali bosta napredne digitalne rešitve za centre vodenja prenosnega elektroenergetskega omrežja. Gre za tehnološko napreden projekt, ki bo pomembno prispeval k varnejšemu, učinkovitejšemu in bolj trajnostnemu delovanju slovenskega elektroenergetskega sistema. Je pomemben korak v slovenskem zelenem prehodu. Napredne naprave ali koncepti – vse to so gradniki pametnega omrežja – namreč omogočajo, da po isti žici prenašamo večje količine električne energije.

V Elesu ogromno delamo na t.i. Smart grid projektih. Smart grid je skupek tehnologij, storitev in konceptov. Elesova projekta Nedo in FutureFlow sta leta 2020 prejela prvo in drugo nagrado za dva najboljša Smart grid projekta na svetu. Prvo mesto je zasedel projekt Nedo za prilagajanje odjema, ki smo ga razvili ob našem prvem skupnem sodelovanju skupaj s Hitachijem. Drugi projekt s 100-odstotnim financiranjem Evropske komisije je bil FutureFlow. Gre za mednarodni raziskovalni projekt virtualnih sistemskih storitev.

Kako v praksi poteka vzpostavljanje bolj integriranega in celostnega (integralnega) vodenja operativnega centra (VOC) v energetskem sektorju – in kje so največji izzivi pri povezovanju različnih deležnikov?

Delno sem vam že odgovoril v prejšnjem vprašanju, vam bom pa konkretno pojasnil, za kaj točno pri tem projektu s Hitachijem gre. V okviru projekta bosta ELES in Hitachi Energy razvijala tri ključne funkcionalnosti nove generacije: prva je Enterprise Service Bus, to je programska rešitev, ki povezuje različne aplikacije, da lahko med seboj komunicirajo in izmenjujejo podatke — tudi če uporabljajo različne jezike, protokole ali formate. Različne deležnike torej, kot me sprašujete. V praksi bo ta rešitev implementirana na primeru sistema za ugotavljanje meja obratovanja. Druga je Voltage Var Control, ki predstavlja nadgradnjo obstoječega sistema uravnavanja napetosti z uvedbo kompleksnih funkcij in naprednih načinov regulacije. Tretja pa Common Information Model, ki izboljšuje učinkovitost podatkov omrežnih modelov, ki si jih izmenjujejo različni sistemi in organizacije, predvsem pa različni operaterji prenosnih sistemov. Projekt »Sistem vodenja naslednje generacije« je usmerjen prav v naš center vodenja in bo predvidoma trajal dve leti. Družba ELES bo v izboljšave vložila lastna sredstva, v družbi Hitachi Energy pa bodo razvili dogovorjene funkcionalnosti in jih skupaj z Elesom verificirali. Družba Hitachi Energy bo nove funkcionalnosti kasneje vključila v svojo standardno (Network Manager EMS) ponudbo.

Kako pomembno vlogo imajo čezmejne prenosne povezave pri stabilnosti ne le slovenskega, temveč tudi evropskega elektroenergetskega sistema – so danes bolj prednost ali tudi potencialna ranljivost?

Čeprav je Slovenija petnajstkrat manjša od denimo Španije, ima dvakrat večje čezmejne prenosne zmogljivosti in petkrat večje toplotne zmogljivosti kot Španija. Slovenski prenosni elektroenergetski sistem, s katerim upravlja družba ELES, je praktično najbolj vpet sistem v Evropi in povezanost s sosednjimi sistemi je ključna.

Oboje. Naša strateška lega v Evropi nam je omogočila razvoj močnih čezmejnih povezav in tako ima Slovenija danes relativno največje prenosne čezmejne kapacitete v Evropi. Konec leta 2022 smo se povezali še z zadnjo sosednjo državo, s katero nismo imeli čezmejnih prenosnih daljnovodov, Madžarsko. Čeprav je Slovenija petnajstkrat manjša od denimo Španije, ima dvakrat večje čezmejne prenosne zmogljivosti in petkrat večje toplotne zmogljivosti kot Španija. Slovenski prenosni elektroenergetski sistem, s katerim upravlja družba ELES, je praktično najbolj vpet sistem v Evropi in povezanost s sosednjimi sistemi je ključna. Naša konična moč znaša 2,3 gigavata (GW), imamo pa okoli 13 GW moči termičnih kapacitet čezmejnih prenosnih zmogljivosti. Medtem ko lahko Španija iz uvoza ENTSO-e prek Francije pokrije le okoli 15 odstotkov svoje konične porabe, lahko Slovenija pokrije šestkratnik svoje konične porabe. Evropsko omrežje operaterjev prenosnih sistemov za električno energijo (ENTSO-E) uvršča naše omrežje med tri najnaprednejša v Evropi in menim, da je ravno elektroenergetika ključna konkurenčna prednost naše države.

S tega vidika smo torej kot država na (razmeroma) varni strani, recimo, ko govorimo o verjetnosti mrka v Sloveniji – četudi je nikoli ne moremo povsem izključiti. Še toliko manjša pa je verjetnost, da bi se ta začel v Sloveniji. Toda naša povezanost je hkrati tudi slabost, kajti, če bomo v Sloveniji doživeli električni mrk, bo to mrk, ki bo zajel širšo regijo in se kaskadno širil čez več sosednjih držav, tudi našo. Kajti bolj kot smo povezani z okoliškimi sistemi, večje je tudi tovrstno tveganje, da nas katastrofe v soseščini potegnejo zraven.

S katerimi ključnimi projekti ali iniciativami na področju odpornosti, modernizacije omrežij in digitalizacije bi se ELES lahko posebej pohvalil v zadnjem obdobju?

Več projektov sem že naštel, v zadnjem času pa smo v Elesu še zlati pozorni na kibernetsko varnost. Eden najtršjih orehov v letošnjem letu je prav vzpostavitev tako imenovanega skupnega elektroenergetskega varnostnega operativnega centra (e-VOC). Eles je v zadnjih letih v svoje omrežje vgradil cel kup sofisticiranih pametnih naprav in sodeloval v mednarodnih projektih. Šlo je za priprave prenosnih omrežij na vse izzive, ki jih prinaša zeleni prehod. ■

Foto: arhiv ELES d.o.o.

Čeprav je Slovenija petnajstkrat manjša od denimo Španije, ima dvakrat večje čezmejne prenosne zmogljivosti in petkrat večje toplotne zmogljivosti kot Španija. Slovenski prenosni elektroenergetski sistem, s katerim upravlja družba ELES, je praktično najbolj vpet sistem v Evropi in povezanost s sosednjimi sistemi je ključna.

PODELITEV NAGRAD

SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 19. MAJ 2026

17. mednarodna konferenca Dnevi korporativne varnosti

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

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

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

Avtor: Eva Čaleta / Institut za korporativne varnostne študije

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

TELEKOMUNIKACIJSKA OMREŽJA HRBTENICA SODOBNE DRUŽBE

Telekomunikacijska omrežja danes predstavljajo temeljno infrastrukturo, brez katere sodobna družba preprosto ne more delovati. Njihova zanesljivost in odpornost neposredno vplivata na delovanje gospodarstva, javnih storitev ter vsakdanjega življenja posameznikov. V času vse pogostejših kriz in digitalne odvisnosti postaja vprašanje njihove varnosti ter neprekinjenega delovanja strateško vprašanje države. O teh izzivih in prihodnjih usmeritvah smo se pogovarjali z mag. Vesno Prodnik, članico uprave Telekom Slovenije.

Telekomunikacijska omrežja predstavljajo informacijsko hrbtenico sodobne družbe – kako v Telekomu Slovenije sistemsko krepite kibernetsko odpornost v luči vse bolj kompleksnih groženj?

V Telekomu Slovenije gradimo kibernetsko odpornost sistemsko, kot kombinacijo upravljanja tveganj, skladnosti, identifikacije groženj, odpravljanja ranljivosti, tehnične večplastne zaščite, preprečevanja in detekcije, operativne pripravljenosti ter možnosti hitrega okrevanja. Pomembno je, da varnosti ne obravnavamo kot ločen »IT projekt«, temveč kot neločljiv del življenjskega cikla storitev in omrežja. Od načrtovanja, nabave in konfiguracije do obratovanja, nadzora ter vzdrževanja. Ključna pa je celovita podpora in razumevanje vodstva. Kibernetska odpornost je v Telekomu Slovenije ena od ključnih prioritet. Strategija in jasno zastavljeni cilji na tem področju so pomembni, a bistvena je varnostna kultura vseh zaposlenih v podjetju. Ta se gradi na kombinaciji izkušenj in nenehnega pridobivanja novih znanj.

> Danes CKVO vidimo kot operativno jedro odpornosti, ne le za zaščito lastne infrastrukture, temveč tudi kot ključnega partnerja v širšem ekosistemu, katerega krepitev neposredno pripomore k boljši skupni situacijski sliki v državi.

Danes se tehnologije hitro razvijajo in s tem tudi grožnje postajajo vse kompleksnejše. V Telekomu Slovenije na to odgovarjamo z višjo stalno pripravljenostjo, večplastno zaščito in okrepljeno odpornostjo. To nam omogoča, da zagotavljamo najvišjo raven zaupnosti, celovitosti, avtentičnosti in razpoložljivosti. Tako za naše telekomunikacijske storitve kot za IKT okolja, ki nam jih v varovanje zaupa vse več organizacij.

Katere so danes največje kibernetske grožnje za telekomunikacijski sektor in kako se nanje pripravljate na operativni ravni?

Danes so največje grožnje za telekomunikacijski sektor kombinacija napadov na razpoložljivost, kompromitacije upravljavskih okolij, izkoriščanja ranljivosti v dobavni verigi in ciljanih kampanj, kjer napadalci iščejo dolgoročen dostop (t.i.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

persistent access). Telekomunikacijsko okolje je specifično, ker je velik del funkcionalnosti omrežja programsko definiran, močno avtomatiziran in povezan s številnimi dobavitelji, zato se grožnje pogosto selijo iz klasičnega IT-ja v omrežne domene (upravljavski sistemi, orkestracija, virtualizacija, APIji, nadzorna raven itd.). Pomembno je, da smo v Telekomu Slovenije trend zlivanja IT-ja in omrežnega sveta zaznali pravočasno. S celovitim in enotnim ciklom načrtovanja uspešno obvladujemo tveganja, ki izhajajo iz teh groženj. Ob tem ne smemo spregledati morda največje in pogosto zanemarjene krovne grožnje: brezglave cenovne vojne in nenehnega nižanja stroškov, ki slej ko prej vodita v spiralo neobvladljivih tveganj. Naš odgovor je jasen: zagotavljanje in krepitev odpornosti je ena od ključnih prioritet Telekoma Slovenije. A odpornost gradimo premišljeno in ekonomsko utemeljeno: kot delniška družba jo razumemo kot naložbo v stabilnost in zanesljivost za vse deležnike ter kot del trajnostnega razvoja.

Na operativni ravni se pripravljamo z večplastnim modelom, ki vključuje zaščito pred izpadi (DDoS, izčrpavanje virov), zaščito upravljavskih sistemov, zaščito pred kompromitacijo končnih točk in strežnikov, poudarek je na obvladovanju ranljivosti v kontroli dobavne verige. Socialni in identitetni napadi ostajajo krovni izziv, zato so nujni obnovitveni programi ozaveščanja ter seveda tehnični ukrepi. Ob vsem moramo stalno skrbeti za odlično uporabniško izkušnjo, da se prednosti digitalizacije ne sprevržejo v njihovo nasprotje.

Pri tem se kot eden ključnih vektorjev vse bolj izpostavljajo identitetni napadi, zato je ob tehničnih ukrepih odločilno tudi učinkovito upravljanje identitet in dostopov. Sodobni napadi niso več omejeni le na hibe v sistemih, temveč vse bolj ciljajo na same identitete, na naše račune, pravice in privilegirane dostope. V boju proti njim je hitrost vse, odločata namreč čas zaznave in čas omejitve incidenta. Temelj za uspešen odziv ostaja nepopustljiva operativna disciplina prek standardiziranih konfiguracij, strogega upravljanja sprememb in revizijskih sledi. Ob tem pa vsi vemo, kaj se dogaja ob razvoju umetne inteligence (UI). V luči hitrega napredka UI je Anthropic nedavno predstavil projekt Glasswing, ki je skupna pobuda tehnoloških velikanov (Amazon, Microsoft, Google, Apple idr.) za zaščito kritične programske opreme. Napredni UI modeli namreč že lahko avtonomno odkrivajo ranljivosti in razvijajo t. i. exploite hitreje ter bolje od strokovnjakov. Ker to močno znižuje vstopni prag za kibernetske napade, je glavni cilj projekta jasen: zmogljiva UI mora biti najprej in najmočneje uporabljena za obrambo, ne za napad. Jedro pobude je javnosti nedostopen model Claude Mythos Preview, ki deluje povsem avtonomno in presega dosedanje modele. Odkril je že tisoče »zero-day« ranljivosti (med njimi 27 let staro luknjo v OpenBSD in 16 let star hrošč v FFmpeg), ki so bile že odgovorno prijavljene ter odpravljene. Orodja že uporablja več kot 40 organizacij. V prihodnje želi Glasswing vzpostaviti nove varnostne standarde za dobo UI (npr. avtomatizirano krpanje in »*secure-by-design*« razvoj) ter v sodelovanju z vladami morda prerasti v neodvisno telo. Gre za nujen korak, da najnevarnejše zmožnosti UI uporabimo za zaščito sveta, preden pristanejo v rokah napadalcev.

Kako vaš Center kibernetske varnosti in odpornosti prispeva k zaščiti ne le lastne infrastrukture, temveč tudi širšega ekosistema kritične infrastrukture v Sloveniji?

V Telekomu Slovenije smo operativni center kibernetske varnosti vzpostavili leta 2018, kar je predstavljalo prvo obdobje sistematičnega upravljanja kibernetske varnosti, tako za Skupino Telekom Slovenije kot za trg. Z letom 2023 smo vstopili v novo obdobje, v katerem dajemo še večji poudarek celoviti odpornosti, zato smo center preimenovali v Center kibernetske varnosti in odpornosti (CKVO). V CKVO deluje več kot 100 strokovnjakov, ki 24 ur na dan spremljajo dogajanje in skrbijo za varnost sistemov ter uporabnikov.

Danes CKVO vidimo kot operativno jedro odpornosti, ne le za zaščito lastne infrastrukture, temveč tudi kot ključnega partnerja v širšem ekosistemu, katerega krepitev neposredno pripomore k boljši skupni situacijski sliki v državi. Pri našem delu je pomembno, da dogodke hitro zaznamo in razumemo, saj se kibernetski incidenti prepogosto najprej pokažejo zgolj kot anomalije v omrežnem prometu, signalizaciji, na dostopih ali upravljavskih ravninah. CKVO deluje kot napreden senzorski in analitični sloj, ki v smiselno celoto povezuje telemetrijo omrežja, sistemov, platform, aplikacij, identitet in storitev. Njegov prispevek k širši varnosti se odraža predvsem v zakoniti izmenjavi indikatorjev kompromitacije in vzorcev napadov ter v strokovni koordinaciji ob incidentih, ki vključujejo več deležnikov, kot so dobavitelji, druge kritične organizacije in nacionalni mehanizmi. Prav tako redno izvajamo skupne vaje za izboljšanje interoperabilnosti in nenehno krepimo varnostne standarde pri storitvah, ki jih nudimo trgu, kot so zaščita pred napadi DDoS, upravljanje identitet ter varne povezave. CKVO je zmogljiv procesni mehanizem, ki vsak varnostni dogodek strukturirano vodi skozi faze triaže, poglobljene analize, zajezitve napada, odstranitve grožnje in končnega vrednotenja naučenih lekcij.

Telekomunikacijski sektor je močno odvisen od drugih sistemov, predvsem energetike. Kako naslavljate te

medsektorske odvisnosti z vidika odpornosti in neprekinjenega delovanja?

Telekomunikacijski sektor, vse bolj imenovan kot digitalna infrastruktura, in energetika sta medsebojno odvisna sistema. Zato odpornost gradimo na tehnični odpornosti infrastrukture in organizacijsko-operativni usklajenosti. Tehnično to pomeni kombinacijo redundanc (več poti, več lokacij, raznoliki viri), rezervnega napajanja, nadzora nad porabo in načrtovanja prioritet delovanja v razmerah omejitev. Organizacijsko pa pomeni dogovorjene protokole sodelovanja, kontaktne točke, scenarije in redne vaje. Praksa kaže, da moramo v zelo kritičnih situacijah, ko recimo nekje odpove delovanje javnega energetskega sistema, sami poskrbeti za rezervna (baterijska, agregatna) napajanja, zato da lahko ohranimo temeljno delovanje javnega komunikacijskega omrežja. Pri zagotavljanju neprekinjenega delovanja je ključno, da se ne zanašamo zgolj na idealne pogoje. Načrtno se moramo pripravljati na najzahtevnejše scenarije, kot so dolgotrajni izpadi električne energije, motnje v oskrbi z gorivom, sočasni izpadi na več lokacijah, ekstremni vremenski dogodki in kompleksni kombinirani incidenti, na primer kibernetski napad, ki se zgodi hkrati z motnjami v dostopnosti energije. Prav zato je sistematično načrtovanje neprekinjenega poslovanja za telekomunikacijske storitve neobhodno. Določiti moramo jasne prioritete in minimalne nivoje delovanja ter jih redno preverjati v praksi. Zgolj obstoj dokumentacije ni dovolj; ključni so redni praktični preizkusi in nenehne izboljšave procesov. Hkrati moramo proaktivno obvladovati odvisnosti od zunanjih dobaviteljev in vzdrževalcev, kar pomeni vnaprejšnjo zagotovitev servisnih poti, dostopnosti rezervnih delov in zanesljive logistike v kriznih razmerah. Prava odpornost namreč ne pomeni zgolj tega, da imamo na voljo agregate. Pomeni, da natančno vemo, kako dolgo in pod katerimi pogoji lahko delujejo ter kako je ukrepanje koordinirano. V kriznih situacijah je za uspešen odziv odločilna nemotena komunikacija med vsemi sektorji z jasnimi operativnimi in eskalacijskimi kanali. Ta komunikacija je izjemno odvisna prav od stabilne in kar se da zanesljive digitalne infrastrukture Telekoma Slovenije.

S katerimi ključnimi projekti ali iniciativami na področju kibernetske varnosti in odpornosti kritične infrastrukture ste se v zadnjem letu najbolj izkazali?

Nenehno krepimo celotni cikel zagotavljanja kibernetske varnosti in odpornosti. Popolnoma smo prenovili strategijo na tem področju za naslednje obdobje, praktično smo v dobi kibernetske varnosti Telekoma Slovenije 2.0. To zaznamuje tudi nadgradnja zaznavanja in odzivanja, izboljšanje korelacije dogodkov, avtomatizacija odzivov, izboljšano obvladovanje incidentov ter analiz po incidentih. Skrbimo, da incidenti ne prerastejo meja, ko bi ogrožali ZCRA – slednji izhaja tudi iz novega ZINF, skladnost s katerim je naša primarna prioriteta.

V Telekomu Slovenije sistematično krepimo varnost omrežnih in upravljavskih domen z dosledno segmentacijo, utrjevanjem konfiguracij, nadzorom privilegijev in proaktivnim upravljanjem ranljivosti. Uspešno širimo tudi naše CSIRT kapacitete, s katerimi prek storitev upravljane varnosti in sodelovanja v evropskih projektih pomagamo vse večjemu številu organizacij v širši regiji.

Ker se zavedamo pomena celovite zaščite, strogo obvladujemo varnost in skladnost v dobavni verigi ter z rednimi usposabljanji, izobraževanji in simulacijami napadov gradimo močno varnostno kulturo vseh zaposlenih na vseh nivojih. Naša največja prednost namreč ni zgolj napredna tehnologija, temveč visoka zrelost procesov, ki nam ob varnostnem incidentu zagotavlja hiter, usklajen in ponovljiv odziv.

Najvišje standarde upravljanja kibernetske odpornosti Telekoma Slovenije potrjujejo zlata medalja CyberVadis 2025 in številni certifikati, saj je naše poslovanje skladno z evropsko direktivo NIS2 ter najstrožjimi mednarodnimi standardi, kot so ISO 27001, ISO 22301 in ISO 27017/18. Z bogatimi izkušnjami, lastno infrastrukturo in jasno vizijo v Telekomu Slovenije tako utrjujemo svoj položaj kot osrednji varuh digitalnega življenja v Sloveniji.

Kako vidite vlogo telekomunikacijskih podjetij pri obvladovanju informacijskega prostora v kriznih razmerah, zlasti pri omejevanju širjenja dezinformacij?

Telekomunikacijska podjetja imamo v kriznih razmerah predvsem vlogo zagotavljanja zanesljivega delovanja komunikacijskih poti. Ko je infrastruktura stabilna, lahko državni organi, zaščita in reševanje, mediji ter druge službe prebivalstvu posredujejo pravočasne in preverjene informacije. Naša primarna odgovornost je torej razpoložljivost, integriteta in odpornost storitev, še posebej v trenutkih povečanih obremenitev ali poskusov motenja. Na vsebino komunikacij v nobenem primeru nimamo vpliva. Pri dezinformacijah je pomembno ločiti vlogo telekomunikacijskih podjetij od vlog uredniških in regulatornih akterjev. Telekomunikacijska podjetja nismo in ne moremo biti »arbitri resnice«. ■

Foto: arhiv Telekom Slovenije d.d.

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

KOLUMNA

KORPORATIVNA VARNOST DANES: MED TVEGANJI IN ILUZIJO NADZORA

Korporativna varnost danes ni več reaktivna funkcija, temveč preventivni mehanizem strateškega upravljanja tveganj. Kljub njeni vse večji vlogi v organizacijah razdrobljeni modeli umeščenosti še vedno ustvarjajo neenotne in pogosto neučinkovite rezultate. Pomanjkanje specializiranih kadrov in neustrezne kadrovske prakse dodatno poglabljajo razkorak med zaznano ter dejansko ravnjo varnosti. Le celovit pristop, podprt z javno-zasebnim partnerstvom in aktivno strokovno skupnostjo, lahko zagotovi resnično odpornost sodobne družbe.

V zadnjem desetletju se je področje korporativne varnosti iz relativno podporne funkcije razvilo v enega ključnih stebrov stabilnega in trajnostnega poslovanja organizacij. Globalizacija, digitalizacija, geopolitične napetosti in vse bolj kompleksna regulatorna okolja so bistveno preoblikovali razumevanje tveganj. V tem kontekstu korporativna varnost ni več zgolj operativna dejavnost, temveč strateška funkcija, ki neposredno vpliva na odpornost organizacij. Ob tem pa postaja vse bolj jasno, da je njena vloga predvsem preventivna, usmerjena v pravočasno prepoznavanje, zmanjševanje in obvladovanje tveganj, in ne v zagotavljanje reaktivnih odzivov, ki ustvarjajo zgolj iluzijo nadzora med zaposlenimi. Kljub temu se v praksi še vedno pogosto pojavlja pričakovanje, da bo varnost delovala kot zadnja obrambna linija, kar dodatno utrjuje napačne predstave o njeni dejanski funkciji.

Krepitev profesije korporativne varnosti se nedvomno odraža v njeni vedno bolj izpostavljeni vlogi znotraj organizacij. Vse več podjetij vključuje varnostne strokovnjake v najvišje ravni odločanja, kar je jasen signal zavedanja, da so varnostna tveganja poslovna tveganja. Vloga vodij korporativne varnosti se širi, od klasičnega fizičnega varovanja in zaščite informacij do upravljanja kriz, skladnosti, kibernetske varnosti in celo strateškega obvladovanja ugleda. Vendar pa ta napredek ni enakomeren in pogosto ostaja zgolj deklarativen.

Eden ključnih izzivov ostaja dejstvo, da različni modeli umeščenosti procesa korporativne varnosti v organizacijah prinašajo zelo različne rezultate uspešnosti. V nekaterih organizacijah je varnost integrirana kot samostojna, neodvisna funkcija, ki neposredno poroča upravi. Drugod je razpršena med različne oddelke, pravno službo, IT, kadrovsko funkcijo ali operativno vodstvo. Takšna razdrobljenost pogosto vodi v pomanjkanje jasne odgovornosti, podvajanje nalog ali celo v kritične vrzeli v nadzoru. Posledično organizacije ustvarjajo občutek nadzora, ki pa v resnici temelji na nepovezanih in neučinkovitih procesih.

Dinamično in vedno bolj zahtevno varnostno okolje dodatno poudarja potrebo po sistematični in celostni organizaciji korporativne varnosti. Hibridne grožnje, kibernetski napadi, notranje zlorabe, dobavne verige z več plastmi tveganj in nepredvidljivi globalni dogodki zahtevajo prilagodljivost ter in-

*avtor je član Slovenskega združenja korporativne varnosti

terdisciplinarno znanje. Organizacije, ki še vedno obravnavajo varnost kot strošek in ne kot investicijo, vse težje sledijo tempu sprememb. V takšnih okoljih se pogosto ustvarja lažen občutek stabilnosti, dokler ne pride do incidenta, ki razkrije sistemske slabosti.

Vedno močneje pa se izražajo tudi kadrovski izzivi, ki postajajo ena največjih ovir za razvoj področja. Potreba po specializiranih kadrovskih potencialih je v izrazitem porastu, vendar trg dela tej potrebi ne sledi. Kompetenčne zahteve za strokovnjake s področja korporativne varnosti so izjemno široke: razumevanje tehnologije, pravnih okvirov, psihologije, kriznega upravljanja, analitike tveganj in organizacijskega vedenja. Takšnega profila pa ni mogoče enostavno oblikovati skozi obstoječe izobraževalne programe.

Prav tu se pokaže ena izmed ključnih sistemskih slabosti: izobraževalni programi na področju korporativne varnosti obstajajo v zelo omejenih okvirih in pogosto ne sledijo dejanskim potrebam prakse. Posledično organizacije zapolnjujejo kadrovske vrzeli z ljudmi, ki sicer imajo določene izkušnje, vendar ne razpolagajo s celostnim znanjem. To vodi v fragmentirano razumevanje varnosti in v odločitve, ki niso optimalne ali so celo tvegane.

Posebej problematičen pojav pa je vključevanje nestrokovnih oseb v vodenje procesov korporativne varnosti, ki so izbrane na podlagi neformalnih ali »političnih« kriterijev, namesto na podlagi referenc in kompetenc. Takšne prakse ne le znižujejo strokovni nivo upravljanja varnosti, temveč ustvarjajo tudi nevarno kulturo podcenjevanja tveganj. Vodenje varnosti zahteva avtoriteto, znanje in integriteto. Brez tega se funkcija hitro spremeni v formalnost brez dejanskega vpliva.

V zadnjih štirih letih smo bili priča posebej intenzivnim negativnim procesom, ki stanje na področju korporativne varnosti postavljajo v alarmantno stanje. Pandemija, geopolitične krize, pospešena digitalizacija in porast kibernetskih incidentov so razgalili številne sistemske pomanjkljivosti. Organizacije so bile prisiljene v hitre prilagoditve, pogosto brez ustreznih strategij in kadrovskih virov. V takšnih razmerah so se razlike med zrelimi in manj razvitimi varnostnimi sistemi še dodatno poglobile.

Ob tem ne gre prezreti tudi dejstva, da regulativa sicer postaja strožja, vendar sama po sebi ne zagotavlja višje ravni varnosti. Prevečkrat se organizacije osredotočajo na formalno skladnost, namesto na dejansko obvladovanje tveganj. S tem se krepi iluzija nadzora, občutek, da so sistemi učinkoviti, ker ustrezajo predpisom, čeprav v praksi ne zagotavljajo ustrezne zaščite.

Kljub vsem izzivom pa obstajajo tudi pozitivni premiki. Vse več organizacij prepoznava potrebo po profesionalizaciji korporativne varnosti, vlaganju v razvoj kadrov in vzpostavljanju integriranih sistemov upravljanja tveganj. Pojavljajo se pobude za standardizacijo kompetenc, razvoj specializiranih izobraževalnih programov in krepitev sodelovanja med akademsko sfero ter gospodarstvom. To so pomembni koraki, ki pa zahtevajo čas, vztrajnost in predvsem jasno strateško usmeritev.

Če želimo preseči trenutne slabosti, bo treba narediti odločen premik od deklarativnega k dejanskemu razumevanju pomena korporativne varnosti. To pomeni jasno opredelitev vloge znotraj organizacij, vlaganje v strokovni kader, odpravo neustreznih kadrovskih praks in razvoj celostnih pristopov k upravljanju tveganj. Le tako bomo lahko zmanjšali razkorak med zaznanim in dejanskim stanjem varnosti.

Korporativna varnost danes tako stoji na razpotju. Na eni strani se krepi njena vloga in pomen, na drugi pa jo omejujejo strukturne, kadrovske ter sistemske pomanjkljivosti. Ključno vprašanje ni več, ali je varnost pomembna, temveč kako jo učinkovito organizirati in upravljati. Dokler bomo vztrajali pri parcialnih rešitvah in iluziji nadzora, bodo tveganja prehitevala našo sposobnost odzivanja. Pravi preboj bo mogoč šele tak-

rat, ko bo korporativna varnost prepoznana kot to, kar v resnici je, temeljna funkcija sodobnega poslovanja.

V tem kontekstu pa ima posebno, skorajda nepogrešljivo vlogo tudi stanovsko povezovanje in strokovna samoorganizacija profesije. Slovensko združenje za korporativno varnost s svojo varnostno platformo predstavlja enega ključnih nosilcev razvoja, standardizacije in promocije stroke v slovenskem prostoru. Takšna združenja niso zgolj formalni okvir sodelovanja, temveč prostor izmenjave znanj, dobrih praks in oblikovanja strokovnih standardov, brez katerih profesija ne more dozoreti.

Poseben pomen v tem okviru imajo tudi Dnevi korporativne varnosti, ki vse bolj upravičeno dobivajo oznako festivala profesije korporativne varnosti. Ne gre zgolj za konferenco, temveč za osrednji letni dogodek, kjer se srečujejo ključni deležniki, strokovnjaki, odločevalci, akademiki in ponudniki rešitev. To je prostor, kjer se preverja utrip stroke, soočajo različni pogledi in postavljajo smernice prihodnjega razvoja.

Za vse, ki svojo strokovno integriteto gradijo na znanju, izkušnjah in odgovornosti, je prisotnost na takšnem dogodku več kot le priporočljiva – je del profesionalne dolžnosti. Aktivno sodelovanje v strokovni skupnosti namreč ni dodatna vrednost, temveč temelj resnega in odgovornega delovanja na področju korporativne varnosti. Tisti, ki v tem ne prepoznajo pomena in iščejo izgovore za neudeležbo, se morda soočajo z vprašanjem, ki presega zgolj organizacijske omejitve, ali so res izbrali pravo profesijo.

Dodatno razsežnost pomena korporativne varnosti pa predstavlja njena vloga pri zaščiti kritične infrastrukture, ki je temelj delovanja sodobne družbe. Energetski sistemi, telekomunikacije, promet, finančni sistemi, zdravstvo in oskrbne verige so vse bolj odvisni od stabilnega ter varnega delovanja zasebnih in javnih organizacij. V praksi to pomeni, da korporativna varnost že zdavnaj presega meje posamezne organizacije in postaja ključen dejavnik nacionalne odpornosti.

V tem okviru se korporativna varnost vse bolj uveljavlja kot relevanten in nepogrešljiv sogovornik institucij nacionalno-varnostnega sistema. Brez aktivnega vključevanja gospodarskih subjektov in njihovih varnostnih struktur ni mogoče vzpostaviti učinkovitega sistema zgodnjega zaznavanja tveganj, preprečevanja incidentov ter kriznega odzivanja. Prav korporativna okolja so pogosto prva, ki zaznajo anomalije, spremembe v tveganjih ali konkretne grožnje, zato je njihova vloga v širšem varnostnem ekosistemu izjemnega pomena.

Ključno spoznanje sodobnega časa je, da varnosti ni več mogoče zagotavljati v izoliranih sistemih. Samo celovit pristop, ki vključuje vse deležnike, javni sektor, zasebne organizacije, regulatorje, raziskovalne institucije in strokovna združenja, lahko zagotovi učinkovito obvladovanje kompleksnih tveganj. Sinhronizirano delovanje teh akterjev je temelj za vzpostavitev resničnega javno-zasebnega partnerstva, ki ni zgolj formalni koncept, temveč operativni mehanizem odzivanja.

Prav to partnerstvo pa postaja ključen segment odzivanja na vse pogostejše krizne situacije, s katerimi se sooča sodobna družba. Naravne nesreče, kibernetski napadi, geopolitični pretresi in sistemske motnje zahtevajo hitro, usklajeno ter strokovno podprto ukrepanje. Brez vključene in kompetentne korporativne varnosti bi bili ti odzivi bistveno počasnejši, manj učinkoviti ter bolj tvegani.

Zato prihodnost korporativne varnosti ni zgolj v njenem notranjem razvoju znotraj organizacij, temveč v njeni sposobnosti povezovanja, sodelovanja in soustvarjanja širšega varnostnega okolja. Le s takšnim pristopom bo mogoče preseči iluzijo nadzora in vzpostaviti dejansko odpornost, tako na ravni organizacij kot tudi celotne družbene skupnosti. ■

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.

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Boštjan Kolar, pooblaščenec za varnost in skladnost, Cetis d.d.*

VARNOST JE PRI NAS NELOČLJIVO POVEZANA Z ENO OD TEMELJNIH VREDNOT PODJETJA – ZAUPANJEM

V zahtevnem globalnem okolju, kjer so tveganja vse bolj kompleksna, postaja varnost temelj zaupanja in dolgoročne poslovne uspešnosti. Boštjan Kolar, letošnji korporativni manager leta, s svojim vodenjem potrjuje, da je prav strateško upravljanje varnosti ključno za stabilen razvoj podjetja. V CETIS to razumevanje uspešno prepletajo z inovativnostjo in globalno prisotnostjo.

Ob prejemu nagrade *Slovenian Grand Security Award* za korporativno varnostnega managerja leta – kaj to priznanje pomeni za vas osebno in za organizacijo CETIS?

Prejem nagrade *Slovenian Grand Security Award* ima zame osebno posebno težo, saj sem v družbi CETIS zaposlen že več kot dvajset let in sem v tem času opravljal zelo različne vloge – od projektnega vodenja, vodenja IT-ja do današnje odgovornosti za celovito korporativno varnost. Moja karierna pot se je v veliki meri razvijala vzporedno z razvojem področja varnosti: od začetnih, bolj tehničnih in parcialnih pristopov, do celostnega, sistemskega upravljanja varnostnih tveganj. Tako kot se je v tem obdobju spreminjalo varnostno okolje, se je postopoma, korak za korakom, dvigovala tudi raven varnosti v družbi CETIS.

Prejem nagrade *Slovenian Grand Security Award* ima zame osebno posebno težo, saj sem v družbi CETIS zaposlen že več kot dvajset let in sem v tem času opravljal zelo različne vloge – od projektnega vodenja, vodenja IT-ja do današnje odgovornosti za celovito korporativno varnost.

Že zelo zgodaj smo se v podjetju začeli zavedati, da varnost ne more biti več le dodatna naloga posameznikov, temveč mora postati profesionalna, jasno opredeljena odgovornost. K temu so nas močno spodbudili tudi zahtevni mednarodni varnostni standardi, ki smo jih morali uvesti in dolgoročno vzdrževati zaradi zahtev naše panoge – varnostnih dokumentov ter rešitev za upravljanje identitete in izdajo dokumentov. Ker dobro poznam strokovno skupnost in ljudi, ki stojijo za podelitvijo te nagrade, ter vem, kdo vse jo je že prejel, mi priznanje pomeni iskreno potrditev, da so bili naši pristopi in odločitve prepoznani tudi širše. To mi predstavlja predvsem osebno čast in strokovno zaupanje.

Za CETIS pa ima nagrada še širši pomen. Varnost je pri nas neločljivo povezana z eno temeljnih vrednot podjetja – zaupanjem. Ustvarjamo rešitve in storitve za vlade ter podjetja po vsem svetu, kjer

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

brez zaupanja dolgoročnega sodelovanja preprosto ni mogoče. Zato te nagrade ne dojemam kot individualne, temveč kot priznanje vsem sodelavcem, ki vsakodnevno prispevajo k višji ravni varnosti, in vodstvu podjetja, ki razume kompleksnost tega področja ter ga podpira in se zaveda, da varnost zahteva tako znanje kot tudi stalne, premišljene investicije.

Kako danes razumete vlogo korporativne varnosti v podjetju, kot je CETIS, ki deluje na področju visoko občutljivih in varnostno kritičnih storitev?

Vlogo korporativne varnosti danes razumem predvsem kot strateško funkcijo, ki mora biti urejena na najvišji, konceptualni ravni, z jasno opredeljenimi odgovornostmi in pristojnostmi. Če so tveganja pravilno prepoznana in realno ocenjena, jih je mogoče s pravimi organizacijskimi, tehničnimi in procesnimi ukrepi učinkovito zmanjšati. Cilj takšnega pristopa je, da se organizacija v vsakdanjem delovanju ne ukvarja z znanimi in predvidljivimi težavami, temveč je pripravljena na nove, nepričakovane izzive, ki jih prinaša hitro spreminjajoče se varnostno okolje.

V družbi CETIS imamo zavestno vzpostavljeno združeno funkcijo, ki celostno pokriva tehnično, fizično in informacijsko varnost. To omogoča enoten pogled na varnostna tveganja in preprečuje razdrobljenost odgovornosti. Naša naloga je vzdrževati takšen nivo varnosti, da lahko obvladujemo tveganja na vseh ključnih področjih – od varnosti posameznih varnostno občutljivih komponent izdelkov, varnosti proizvodnih procesov, fizičnega in tehničnega varovanja objektov (vključno z vlomno zaščito ter videonadzorom) do stalnega spremljanja in izboljševanja informacijske varnosti. V okolju, kjer podjetje deluje na področju visoko občutljivih in varnostno kritičnih storitev, korporativna varnost ni več podporna funkcija, temveč eden od temeljnih pogojev za nemoteno poslovanje ter dolgoročno zanesljivost. Njena vloga je ustvariti stabilno in zaupanja vredno okolje, v katerem lahko ostali poslovni procesi delujejo učinkovito, varno ter skladno z najvišjimi zahtevami naših kupcev in regulatorjev.

Podjetje je tik pred zaključkom pomembne infrastrukturne investicije, novega objekta na matični lokaciji v Celju. Kakšne izzive je ta projekt predstavljal z vidika načrtovanja in implementacije celovite korporativne varnosti?

Projekt izgradnje novih proizvodno-poslovnih prostorov v Celju je z vidika korporativne varnosti predstavljal izjemno velik, a hkrati redek in dragocen izziv. CETIS, kot ga Celjani poznajo, na tej lokaciji deluje že od začetka osemdesetih let prejšnjega stoletja. Obstoječa stavba se je sicer skozi desetletja dograjevala in prilagajala, vendar so rast obsega poslovanja, visoka stopnja avtomatizacije proizvodnje, novi tehnološko zahtevni stroji in sodobni standardi delovnih pogojev jasno pokazali, da je potrebna celovita prostorska ter infrastrukturna prenova, kar je bilo najbolj smiselno izvesti z gradnjo nove stavbe. Pri tem ne gre zanemariti niti pričakovanj zaposlenih, ki so si lepše, sodobnejše in bolj funkcionalne delovne prostore želeli že dalj časa.

Z vidika varnosti je bil ključen predvsem zgodnji začetek. V projekt smo bili vključeni že povsem na začetku, ko smo na podlagi mednarodnih varnostnih standardov za področje varnostnega tiska pomagali načrtovati razporeditev proizvodnje, opredeliti varnostne ukrepe in določiti zahteve glede opreme, gradbenih materialov ter tehničnih rešitev. Na določenih področjih so te zahteve zelo natančno in strogo predpisane, kar projekt dodatno zaplete. Vsaka gradnja proizvodnega objekta je sama po sebi kompleksen proces, v našem primeru pa so bile zaradi izjemno visokih varnostnih zahtev toleranca za napake in improvizacijo še bistveno manjše.

Seveda tudi pri tako skrbno načrtovanem projektu ni šlo brez izzivov. Pri nekaterih rešitvah se je izkazalo, da bi jih

lahko v fazi projektiranja zastavili drugače, ponekod se je v komunikaciji med številnimi deležniki izgubila kakšna pomembna podrobnost. Ključno je bilo, da smo gradnjo ves čas aktivno spremljali in odstopanja sproti odpravljali. Ob pisanju tega odgovora se zaključujejo še zadnje aktivnosti na področju varnosti. Ponosni smo na novo stavbo in na pomembno pridobitev, ki bo družbi CETIS dolgoročno omogočala varno, stabilno ter razvojno naravnano poslovanje. Z novo stavbo bomo pridobili dodatne, nujno potrebne prostore z najsodobnejšo strojno in programsko opremo za izdelavo in izdajo elektronskih potovalnih dokumentov. S tem bomo bistveno povečali zmogljivost, kakovost, produktivnost in stopnjo avtomatizacije ter dodatno optimizirali poslovne procese. Hkrati bomo zaposlenim zagotovili prijetnejše delovno okolje in ustvarili ustreznejše pogoje za sodelovanje s poslovnimi partnerji. Posebno pozornost smo namenili funkcionalnosti, energetski učinkovitosti in zmanjševanju okoljskih vplivov.

S katerimi ključnimi varnostnimi izzivi se trenutno soočate? Ali so v ospredju bolj fizična, kibernetska ali hibridna tveganja?

Danes se varnostni izzivi vse manj delijo na strogo ločena področja, saj gre v praksi skoraj vedno za preplet fizičnih, tehničnih in kibernetskih tveganj. Tehnologija na področju tehničnega in fizičnega varovanja hitro napreduje ter nam omogoča rešitve, ki so bile še pred leti skoraj nepredstavljive. To nam bistveno olajša delo in povečuje učinkovitost varnostnih mehanizmov, hkrati pa odpira dodatne priložnosti za nadaljnjo digitalizacijo ter avtomatizacijo postopkov, kjer še vidimo precej prostora za razvoj.

Bistveno večje izzive trenutno prepoznavamo na področju kibernetske varnosti. Grožnje postajajo vse bolj kompleksne, ciljno usmerjene in prilagodljive, pri čemer je poudarek vse pogosteje na izkoriščanju človeškega faktorja. Zaposleni so najpomembnejši del podjetja, a hkrati tudi najbolj izpostavljen člen, predvsem zaradi vedno bolj dovršenih oblik socialnega inženiringa. Zato poleg tehničnih ukrepov veliko pozornosti namenjamo ozaveščanju, usposabljanju in gradnji takšne varnostne kulture, kjer posameznik razume svojo vlogo in odgovornost v celotnem sistemu.

Da gre za širši, sistemski izziv, se kaže tudi na ravni zakonodaje in regulative. Kibernetska varnost je postala prednostna tema tudi na državni in evropski ravni, kar se odraža v vse strožjih zahtevah na področju skladnosti, kot sta uredbi NIS2 in CRA. Za podjetje, kot je CETIS, to pomeni dodatno odgovornost, hkrati pa tudi jasen okvir, znotraj katerega lahko dolgoročno in strukturirano gradimo odpornost na hibridna tveganja prihodnosti.

Kako v praksi povezujete različne vidike varnosti (fizično, informacijsko, organizacijsko) v enoten sistem upravljanja tveganj in odpornosti?

V praksi na varnost gledamo zelo življenjsko in celostno. Ne ločujemo strogo med fizično, informacijsko ali organizacijsko varnostjo, temveč jih razumemo kot dele iste zgodbe. Pomembno nam je, da vemo, kaj v podjetju varujemo, kje so resnična tveganja in kdo je za kaj odgovoren. Ker so te funkcije v družbi CETIS združene, lahko težave obravnavamo povezano – od dostopov in proizvodnje do informacijskih sistemov ter ravnanja zaposlenih. Tako je varnost del vsakdanjega dela, ne nekaj, s čimer se ukvarjamo šele takrat, ko gre kaj narobe.

Kako pomembna je vloga zaposlenih pri zagotavljanju varnosti in kako v podjetju gradite varnostno kulturo ter zavedanje?

Vloga zaposlenih je pri zagotavljanju varnosti ključna, saj noben tehnični ali organizacijski ukrep ne more nadomestiti odgovornega ravnanja posameznika. V družbi CETIS varnostno kulturo gradimo postopno in skozi vsakdanje delo – z jasnimi pravili, rednim ozaveščanjem, izobraževanji ter odprto komunikacijo. Zaposlenim želimo približati razumevanje, zakaj so določeni ukrepi potrebni, in jih spodbuditi, da varnosti ne dojemajo kot omejitev, temveč kot skupno odgovornost, ki ščiti njih, podjetje ter naše partnerje.

Skozi svoje storitve ste izredno mednarodno vpeti, tudi na območje držav tretjega sveta. Kako zahtevna je varnostna podpora tem projektom zaradi oddaljenosti, slabših infrastrukturnih zmogljivosti in tudi pomembnih kulturnih razlik?

Mednarodni projekti, še posebej v okoljih z manj razvito infrastrukturo in drugačnimi kulturnimi vzorci, predstavljajo specifičen varnostni izziv. Ključno je dobro razumevanje lokalnega okolja, realna ocena tveganj in prilagoditev varnostnih rešitev dejanskim razmeram, ne idealnim pogojem. Pri tem se ne moremo zanašati le na tehnologijo, temveč veliko vlagamo v jasne postopke, dobro pripravo sodelavcev in sodelovanje z zaupanja vrednimi lokalnimi partnerji. Prav kombinacija strokovnega znanja, prilagodljivosti in razumevanja kulturnih razlik nam omogoča, da tudi v bolj zahtevnih okoljih zagotavljamo ustrezen varnostni nivo.

Kako vidite razvoj področja korporativne varnosti v prihodnje, katere kompetence in pristopi bodo ključni za uspešno upravljanje tveganj v vse bolj kompleksnem okolju?

Področje korporativne varnosti je in bo ostalo dinamično in vedno bolj prepleteno z vsakdanjim poslovanjem. Ne bo več dovolj, da imamo dobre tehnične rešitve – pomembno bo, da znamo povezovati ljudi, procese in tehnologijo ter varnost prilagajati realnim potrebam okolja. Vse večjo težo bodo imele dobra komunikacija in zdrava organizacijska kultura, kjer varnost ni nekaj vsiljenega, temveč je razumljena kot naravni del dela.

Ob tem se moramo zavedati, da se svet zelo hitro spreminja in da bomo v prihodnje soočeni s povsem novimi izzivi. Prav zato bo ključna prilagodljivost, odprtost za učenje in pripravljenost na spremembe. Varnost nikoli ni končno stanje, temveč stalen proces prilagajanja novim okoliščinam. ■

Foto: arhiv Cetis d.d.

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

INTERVJU
g. Jože Grozde, letošnji nagrajenec za življenjsko delo*

VARNOST JE UMETNOST POVEZOVANJA SISTEMOV IN LJUDI

Celovit pristop k varnosti danes zahteva preseganje tradicionalnih meja med civilnim in vojaškim okoljem. Izkušnje kažejo, da so prav povezovanje, izmenjava informacij in skupna uporaba zmogljivosti ključ do učinkovitega odzivanja na sodobne krize. Jože Grozde skozi svojo bogato kariero dokazuje, da je integracija različnih varnostnih sistemov temelj odpornosti družbe. Njegovo delo in razmišljanje ostajata pomemben navdih za razvoj prihodnjih generacij strokovnjakov na področju varnosti.

Vaša skoraj 40-letna karierna pot je prepletala gospodarstvo in sistem nacionalne varnosti. Kateri ključni trenutki so najbolj zaznamovali vaš strokovni razvoj?

Spremljanje tehnološkega razvoja in uvajanje novih tehnologij, procesov ter standardov me spremlja že od srednješolskih let. Moj osnovni poklic je elektrotehnik, kjer sem se že v času šolanja soočil z velikim tehnološkim napredkom – to, kar sem se učil na začetku šolanja, je bilo ob njegovem koncu že zastarelo (od elektronk do tranzistorjev, integriranih vezij in računalnikov). Delo v Iskrinem razvoju me je naučilo analitičnega in kritičnega razmišljanja ter zavedanja, da bo nenehno izobraževanje sestavni del moje delovne kariere.

Po končanem šolanju za rezervne častnike sem kot rezervist v nekdanji TO uspešno povezoval civilna in vojaška znanja ter veščine. Nadaljnja karierna pot je bila prepletena med civilnim in vojaškim področjem, ki je po osamosvojitvi postalo moja poklicna pot. Pridobljena znanja in izkušnje so mi omogočila uspešno zaključiti študij obramboslovja. Sodeloval sem v procesih preoblikovanja Slovenske vojske iz naborniške v poklicno vojsko, sposobno delovanja skupaj z zavezniki v operacijah kriznega odzivanja.

Za razvoj Slovenske vojske je značilno stalno preoblikovanje strukture in prilagajanje varnostnim razmeram v nacionalnem ter mednarodnem okolju. Nove naloge, ki so izhajale iz spremenjenih virov ogrožanja, so zahtevale nova znanja in veščine, ki niso bila omejena zgolj na vojaško področje. Karierno pot so spremljali stalno usposabljanje, izobraževanje in objavljanje strokovnih člankov. Zlasti bi izpostavil delo v obveščevalni analitiki, kjer sem sodeloval v procesih podpore strateškemu odločanju in vodenje vojaške zdravstvene enote.

Za razvoj Slovenske vojske je značilno stalno preoblikovanje strukture in prilagajanje varnostnim razmeram v nacionalnem ter mednarodnem okolju. Nove naloge, ki so izhajale iz spremenjenih virov ogrožanja, so zahtevale nova znanja in veščine, ki niso bila omejena zgolj na vojaško področje.

Kako se je skozi vašo kariero spreminjalo razumevanje varnosti, zlasti v

*nagrajenec je član Slovenskega združenja korporativne varnosti

kontekstu vedno bolj kompleksnega in povezanega varnostnega okolja?

V bipolarnem svetu je bila varnost razumljena predvsem kot zaščita države pred zunanjim vojaškim napadom. Nasprotnik je bil znan, poznane so bile gospodarske in vojaške zmogljivosti ter načela vojaškega delovanja. Po koncu hladne vojne pa je svet postal globalen in povezan, zato varnost ni več omejena zgolj na vojaško obrambo. Pojavile so se nove grožnje: terorizem, migracijske krize, organizirani kriminal, kibernetski napadi, pandemije, energetska odvisnost in naravne nesreče, povezane s podnebnimi spremembami.

Sodobno varnostno okolje je kompleksno, grožnje pa medsebojno povezane. Zato je potreben celovit pristop in povezovanje civilnih, varnostnih ter vojaških zmogljivosti. Zlasti izstopa pomen informacijskega prostora, ki je poleg fizičnega prostora ključen za nacionalno varnost. Učinkovito upravljanje kibernetskega prostora neposredno vpliva na varnost posameznika, družbe in države.

Korporativna varnost ima ključno, operativno in povezovalno vlogo pri zaščiti kritične infrastrukture. V zadnjem desetletju se je razvila iz fizičnega varovanja v širše področje, ki vključuje informacijsko varnost, krizno upravljanje in zagotavljanje neprekinjenega poslovanja.

Posebej ste izpostavljali pomen povezovanja civilnega in vojaškega okolja. Kje vidite največje prednosti takšnega sodelovanja v praksi?

Prednosti se kažejo v racionalni uporabi virov in hitrem ter usklajenem odzivu ob naravnih nesrečah. Vojska prispeva logistiko, transport, opremo in kadre, civilni deležniki pa lokalno znanje in specializirane storitve.

Primeri dobre prakse so sodelovanje Civilne zaščite, Slovenske vojske, gasilcev, policije in lokalnih skupnosti ob poplavah, žledolomu ter požarih in v času pandemije še z zdravstvom. Pomemben je tudi prispevek vojske pri reševanju v gorah, medicinski pomoči ali evakuaciji iz tujine. Izzivi ostajajo na področju zaščite kritične infrastrukture in kibernetske varnosti, kjer medsebojno sodelovanje potrebno tudi zaradi omejenih kadrovskih virov.

Kako ocenjujete pripravljenost sodobnih sistemov na obvladovanje kriz, zlasti tistih, ki izhajajo iz naravnega okolja ali hibridnih groženj?

Pripravljenost v Sloveniji na naravne nesreče je zelo dobra, kar se kaže v hitrem odzivu in dobri organiziranosti ob vsakokratnem izrednem dogodku. Pri hibridnih grožnjah pa ostajajo izzivi, predvsem na področju preventive, digitalne varnosti, odpornosti in sistemskega povezovanja vseh deležnikov.

Strnjeno: dobri smo pri odzivanju na pričakovane krize, slabši pa pri upravljanju nepričakovanih.

Kakšno vlogo ima po vašem mnenju korporativna varnost pri zaščiti kritične infrastrukture in njenem vključevanju v širši sistem nacionalne varnosti?

Korporativna varnost ima ključno, operativno in povezovalno vlogo pri zaščiti kritične infrastrukture. V zadnjem desetletju se je razvila iz fizičnega varovanja v širše področje, ki vključuje informacijsko varnost, krizno upravljanje in zagotavljanje neprekinjenega poslovanja. Pomembno vlogo ima tudi uvajanje standardov in normativna podpora. Poleg tega korporativna varnost deluje kot most med zasebnim sektorjem in institucijami nacionalne varnosti, saj

omogoča pravočasno izmenjavo ključnih informacij ter usklajeno odzivanje na grožnje. Njena vloga je zlasti izrazita pri preprečevanju incidentov, kjer z zgodnjim zaznavanjem tveganj bistveno zmanjšuje potencialne posledice. S sodobnimi analitičnimi pristopi in vključevanjem naprednih tehnologij postaja tudi pomemben dejavnik pri krepitvi situacijskega zavedanja. Na dolgi rok pa prispeva k večji odpornosti celotne družbe, saj povezuje različne deležnike v enoten in učinkovito delujoč varnostni ekosistem.

V svoji karieri ste veliko prispevali tudi k izobraževanju. Katere ključne kompetence bi morali danes razvijati mladi strokovnjaki na področju varnosti?

Mladi strokovnjaki na področju varnosti bi morali danes razvijati kombinacijo strokovnih, tehnoloških in osebnih kompetenc, saj je sodobno varnostno okolje zelo dinamično ter kompleksno. Ključne so: analitično in kritično razmišljanje, prilagodljivost, vseživljenjsko učenje, digitalna varnostna znanja, poznavanje predpisov ter sposobnost delovanja v stresnih razmerah.

Sodobni varnostni strokovnjak je povezovalec med tehnologijo, ljudmi in organizacijo tako v fizičnem kot kibernetskem prostoru. Pomembna lastnost uspešnega varnostnega strokovnjaka je tudi kombinacija vztrajnosti (ne odneham) in strateškega prilagajanja realnim razmeram (učim se, prilagajam in grem naprej).

Kako vidite razvoj sodelovanja med institucijami, kot je Slovenska vojska in civilnimi ter gospodarskimi subjekti v prihodnje?

V prihodnje pričakujem, da se bo sodelovanje med institucijami, kot je Slovenska vojska, civilnimi in gospodarskimi subjekti še okrepilo, predvsem zaradi vse bolj prepletenih varnostnih, tehnoloških, okoljskih ter kriznih tveganj. Sodelovanje se bo še okrepilo zaradi vse bolj prepletenih tveganj. Premika se od občasne koordinacije k stalnemu, sistemsko urejenemu modelu. Cilj ni le odzivanje na krize, temveč celovito upravljanje odpornosti države.

V tem kontekstu bo ključnega pomena vzpostavljanje skupnih platform za izmenjavo informacij in razvoj skupnih zmogljivosti za odzivanje. Povečala se bo tudi potreba po skupnih vajah in usposabljanjih, ki bodo omogočala boljšo pripravljenost vseh deležnikov. Gospodarski subjekti bodo vse bolj prepoznani kot enakovredni partnerji v sistemu nacionalne varnosti, zlasti na področju zaščite kritične infrastrukture. Takšen razvoj bo prispeval k večji usklajenosti delovanja, hitrejšemu odzivanju in dolgoročni krepitvi odpornosti celotne družbe.

V prihodnje pričakujem, da se bo sodelovanje med institucijami, kot je Slovenska vojska, civilnimi in gospodarskimi subjekti še okrepilo, predvsem zaradi vse bolj prepletenih varnostnih, tehnoloških, okoljskih ter kriznih tveganj. Sodelovanje se bo še okrepilo zaradi vse bolj prepletenih tveganj. Premika se od občasne koordinacije k stalnemu, sistemsko urejenemu modelu. Cilj ni le odzivanje na krize, temveč celovito upravljanje odpornosti države.

V Slovenskem združenju za korporativno varnost ostajate aktivni tudi po upokojitvi. Kaj vas še danes najbolj motivira pri prenosu znanja in izkušenj na mlajše generacije?

Navdušen sem nad znanjem, zagnanostjo in motivacijo mlajše generacije, predvsem pa pripadnosti stroki. Z veseljem sodelujem na dogodkih združenja. Kot upokojenec lahko z več distance spremljam razvoj področja. Prenos znanja se nanaša predvsem na delo z ljudmi, ki kljub moderni tehnologiji ostajajo najšibkejši člen.

Kako skozi svojo prizmo vidite razvoj omenjenega združenja?

Na svoji članski izkaznici imam številko 8 (leto 2012). Združenje je doživelo izjemen razvoj – od spremljanja klasične fizične varnosti do celovitega upravljanja tveganj v hibridnem okolju. Ključna je povezava strokovne javnosti in izmenjava znanja ter izkušenj med javnim in zasebnim sektorjem, pri tem bi izpostavil tudi Slovensko vojsko ter policijo.

Združenje aktivno sodeluje pri razvoju standardov, zakonodaje in javno-zasebnega partnerstva. Vesel sem, da sem del te skupnosti. ■

ENDURANCE

Strategies and Services for Enhanced Disruption Resilience and Cooperation

3 Year Project Duration

23 Partners across Europe

€5m EU Horizon Funding

@ENDURANCE_EU

ENDURANCE_EU

ENDURANCE Project

The ENDURANCE project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement no.101168007.

Avtor: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Jure Remškar, direktor podjetja Smart Com, d.o.o.*

SMART COM SE UVELJAVLJA KOT SISTEMSKI INTEGRATOR DIGITALNE ODPORNOSTI

Digitalna odpornost postaja ključen dejavnik stabilnega delovanja sodobnih organizacij in kritične infrastrukture. Smart Com se kot sistemski integrator vse bolj uveljavlja z naprednimi rešitvami, ki povezujejo kibernetsko varnost, omrežja in upravljanje tveganj v celovit okvir. O vlogi podjetja in prihodnjih izzivih smo se pogovarjali z direktorjem Juretom Remškarjem.

Kako v Smart Comu naslavljate vse večje zahteve po kibernetski odpornosti kritične infrastrukture, zlasti v okolju, kjer se prepletajo poslovni (IT) in procesni (OT) sistemi?

V Smart Com kibernetsko odpornost kritične infrastrukture obravnavamo kot sposobnost organizacije, da prepreči, zazna, se odzove in hitro okreva, seveda brez ali ob minimalnem vplivu na ključne storitve. Zato k odpornosti pristopamo integrirano: z vidika regulatornih zahtev, arhitekture omrežij, varnostnih kontrol, procesov in ljudi, ne zgolj prek tehnologij ter tehničnih orodij. V okoljih, kjer se IT in OT prepletata, je odločilno, da varnost vgrajujemo že v fazi načrtovanja ter nabave, ne šele naknadno. To pomeni jasne varnostne zahteve v specifikacijah, segmentacija omrežja, nadzor nad oddaljenimi dostopi, stalno spremljanje in vaje za simulacijo kibernetskih napadov, odzivanje na njih ter obnove po incidentu. Pri tem organizacijam pomagamo tudi operativno, z upravljanjem storitve zaznave in odziva (8/5 ali 24/7), kjer ukrepamo po vnaprej z naročnikom usklajenimi protokoli.

OT okolja ostajajo ena od kritičnih vstopnih točk za napade – kako pristopate k njihovemu varovanju in kako pomembno je razumevanje njihove integracije v celovit okvir kibernetske varnosti?

OT okolja so specifična, saj je za njih ključno, da neprekinjeno delujejo, posodobitve sistemov so pogosto omejene, protokoli pa pogosto niso bili zasnovani z varnostjo v mislih. Zato je prvi korak v teh okoljih zagotoviti vidljivost: natančen popis OT sredstev, razumevanje komunikacijskih tokov in odkrivanje anomalij v realnem času. Drugi ključni element je segmentacija omrežja in strogo upravljanje prehodov med IT ter OT okoljem, s čimer omejimo širjenje kibernetskega napada in zaščitimo najbolj kritične sisteme ali infrastrukturo. Tretji element, ki bi ga izpostavil, pa je zagotovitev varnega oddaljenega dostopa z uvedbo principa najmanjših pravic in strogi nadzor, saj se ravno oddaljeni dostopi v praksi najpogosteje izrabljajo za izvedbo napada. Pri tem pa je nujno razumevanje integracije IT in OT okolja, saj velik del groženj v OT vstopi iz IT sveta, zato mora biti OT varovanje del enotnega okvira upravljanja tveganj, nadzora, odzivanja ter poročanja in ne ločen »otok«.

Kakšne učinke opažate ob implementaciji zakonodaje, kot je ZInfV-1, na dvigovanje zavedanja in dejanske kibernetske odpornosti organizacij v Sloveniji?

ZInfV-1 je v slovenski prostor prinesel pomemben premik, saj ocenjujem, da kibernetske varnosti ne razumemo več kot zgolj tehnično področje, temveč kot sistemsko upravljanje tveganj, za katero smo odgovorni poslovodje, z jasnimi pričakovanji glede ukrepov in poročanja o izpolnjevanju zahtev. V praksi opažam dva učinka zakona. Prvi je dvig zavedanja o pomembnosti kibernetske varnosti, saj se organizacije bolj strukturirano lotevajo vprašanj, kot so popis oz. register sredstev, upravljanje varnostnih ranljivosti, postopki odzivanja na zaznane anoma-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

lije, obvladovanje dobavne verige in formalizacija poročanja o incidentih. Drugi učinek zakona, ki je še bolj pomemben, pa je spodbuditev spremembe kulture, kjer varnost postaja del odločanja, prioritet in virov ter ne le »kljukica« v dokumentaciji. Pri tem pa je ključno, da se skladnost ne konča pri dokumentih, temveč se prevede v operativno prakso: redno preverjanje, izboljšave, vaje odzivanja in jasno razmejene odgovornosti za zagotavljanje visokega nivoja kibernetske varnosti.

V čem se vaši pristopi in rešitve razlikujejo od drugih ponudnikov kibernetske varnosti na trgu, zlasti pri obravnavi kompleksnih IT/OT okolij?

Naša ključna razlika je, da nastopamo kot sistemski integrator digitalne odpornosti: povezujemo omrežno arhitekturo, varnostne tehnologije in operativne procese v celoto. Pri kompleksnih IT/OT okoljih je to odločilno, ker varnost in razpoložljivost izhajata iz iste arhitekture od segmentacije ter nadzora dostopov do zaznavanja in odzivanja. Druga razlika je operativna izvedba: poleg zasnove in implementacije zagotavljamo tudi upravljanje ter nadzor sistemov z vnaprej dogovorjenimi protokoli in ločenimi pristopi za IT ter OT okolja, saj smo se specializirali tako za poslovna kot operativna/kritična okolja, ki imajo posebne značilnosti. Tretjo razliko pa vidim v naši zrelosti pri delovanju v kritičnih okoljih: delujemo skladno z zahtevami za varovanje informacij in imamo ustrezna dovoljenja za delo s tajnimi podatki (nacionalno, EU, NATO), kar je za določene segmente kritične infrastrukture ter nacionalno-obrambnega sistema pomembna prednost.

Kako s svojimi pristopi, inovacijami in rešitvami prispevate k razvoju slovenskega trga na področju kibernetske varnosti ter odpornosti kritične infrastrukture?

Na slovenski trg vplivamo na tri načine: z dvigom kompetenc, operativnih zmogljivosti in z inovacijami, ki zmanjšujejo odvisnost ter povečujejo suverenost. Vlagamo v lastno znanje, izobraževanje in ozaveščanje, tako pri strankah kot v širši strokovni skupnosti, saj proaktivno sodelujemo tudi v mednarodnem študijskem komiteju za naslavljanje izzivov kibernetske varnosti, informacijske tehnologije ter telekomunikacij v elektroenergetik - D2 Pariške organizacije CIGRE, Sekciji za kibernetsko varnost pri GZS in sooblikujemo slovenski trg na področju kibernetske varnosti. Poleg tega gradimo in širimo zmogljivosti našega operativnega centra, s katerim organizacijam omogočamo, da tudi ob morebitnemu pomanjkanju kadrov dosežejo visok nivo nadzora, odzivanja, poročanja ter skladnosti z zakonodajnimi zahtevami. Nadalje razvijamo storitve in rešitve z uporabo odprtokodnih komponent z lastnim znanjem ter skladno z usmeritvami EU glede tehnološke suverenosti.

Kako spoznanja iz projektov (tudi EU projektov) uspešno prenašate v praktične procese in rešitve, ki organizacijam omogočajo bolj učinkovito upravljanje kibernetskih tveganj?

Spoznanja iz razvojnih in EU projektov prenašamo v razvoj orodij ter v operativne prakse. Na ravni evropskih projektov sodelujemo v konzorcijih, kjer razvijamo ali preizkušamo pristope, ki krepijo kibernetsko varnost skozi življenjski cikel, in sicer od zahtev ter načrtovanja do DevSecOps praks in pilotnih postavitev. Pridobljeno znanje nato standardiziramo v interne metodologije in storitve za izboljševanje kakovosti ter naše dodane vrednosti za naše stranke. ■

Foto: arhiv Smart Com, d.o.o.

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

SMART COM

Zagotovite varno, zanesljivo in odgovorno digitalno prihodnost

Skladnost z regulatornimi zahtevami in mednarodnimi standardi za zagotavljanje informacijske varnosti.

Kibernetska varnost v poslovnem in industrijskem okolju in okolju kritične infrastrukture

Sodobna omrežja nove generacije za odlično uporabniško izkušnjo

Smart operativni center upravljanih varnostnih in omrežnih storitev

https://bit.ly/smart-resitve

SPICA
doorcloud

Napredna oblačna rešitev za kontrolo dostopa

Door Cloud omogoča upravljanje in nadzor dostopa do prostorov v realnem času, od kjerkoli. Deluje z obstoječimi električnimi ključavnicami ter v enoten sistem povezuje vrata, zapornice, rampe, domofone in brezžične ključavnice Aperio (Assa Abloy).

Dostop je mogoč tudi prek pametnega telefona ali Apple Watch, **sistem pa omogoča kombinacijo mobilnega in klasičnega dostopa** brez menjave infrastrukture.

Rešitev izpolnjuje **najvišje varnostne standarde ISO 27017, ISO 27018, ISO 9001 in IEC 60839** za varnostne in alarmne sisteme.

Špica International d.o.o., Pot k sejmišču 33, SI-1231 Ljubljana, Slovenija
www.spica.si | www.doorcloud.com | T: +386 1 568 08 16 | info@spica.si

Avtor: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
g. Gašper Pintarič, vodja izvedbe, Špica International d.o.o.*

OPTIMIZACIJA IN VARNOST NISTA V NASPROTJU – V RESNICI SE DOPOLNJUJETA

Optimizacija poslovnih procesov in zagotavljanje varnosti sta danes neločljivo povezana dejavnika uspešnega delovanja organizacij. Špica International s svojimi rešitvami dokazuje, da je mogoče učinkovitost in varnost razvijati sočasno in sinergijsko. O tem, kako se ti dve področji v praksi dopolnjujeta, smo se pogovarjali z vodjo izvedbe Gašperjem Pintaričem.

V Špica International poudarjate obvladovanje časa in prostora v organizacijah, kako te rešitve prispevajo k večji varnosti in odpornosti podjetij v sodobnem poslovnem okolju?

V Špica že vrsto let izhajamo iz prepričanja, da sta čas in prostor ključna strateška vira, ki vplivata ne le na učinkovitost, temveč tudi na varnost, odpornost ter neprekinjeno poslovanje organizacij. Upravljanje časa in prostora razumemo širše od klasične evidence delovnega časa ali fizične kontrole dostopa – kot integriran poslovnovarnostni mehanizem, ki zagotavlja pregled nad tem, kdo, kdaj ter kje izvaja določene aktivnosti.

Naši sistemi omogočajo delovanje v realnem času in realnem prostoru, kar je ključno v okoljih z visokimi varnostnimi zahtevami (kritična infrastruktura, industrija, logistika, finance). Organizacijam omogočajo natančno razumevanje dejanskih tokov ljudi, dela in procesov, hitro zaznavanje odstopanj ter odzivnost v primeru incidentov, motenj ali kriznih razmer.

Takšen pristop neposredno prispeva k operativni odpornosti, saj organizacije ne reagirajo zgolj naknadno, temveč proaktivno preprečujejo tveganja in imajo ves čas na voljo zanesljive podatke za odločitve.

Kako digitalna evidenca delovnega časa in kontrola pristopa vplivata na boljšo preglednost, nadzor ter upravljanje tveganj v organizacijah?

Digitalna evidenca delovnega časa in sistemi kontrole pristopa danes predstavljajo hrbtenico notranje preglednosti organizacije. Njihova vrednost presega administrativno skladnost in se neposredno dotika področij korporativne varnosti, revizije ter upravljanja tveganj.

Sodobna korporativna varnost ne temelji več zgolj na fizični zaščiti ali pravilnikih, temveč na podatkih in preglednosti. Digitalna evidenca delovnega časa in kontrola dostopa omogočata natančno, časovno ter prostorsko vezano sledljivost – kdo je bil prisoten, kje se je gibal in pod kakšnimi pravili. V okviru Špice 360 so ti podatki zbrani in usklajeni v eni platformi: registracije preko mobilnih naprav ali terminalov, pametni krmilniki, revizijske sledi, alarmni dogodki ter potrjevalni tokovi. To bistveno poenostavi notranje in zunanje revizije, hkrati pa omogoča boljše upravljanje notranjih tveganj, zlorab ter operativnih incidentov. Ko so podatki razdrobljeni, tveganj ne vidimo pravočasno – ko so povezani, jih lahko aktivno obvladujemo.

V praksi to pomeni nižjo izpostavljenost notranjim zlorabam, napakam in nepooblaščenim dostopom, hkrati pa večjo transparentnost za vodstvo ter vse zaposlene.

Kakšno vlogo ima digitalizacija oskrbovalne verige pri zagotavljanju stabilnosti in odpornosti poslovanja, zlasti v času motenj ter kriz?

Oskrbovalna veriga je danes ena najbolj izpostavljenih točk tveganj, kar so pokazale tako geopolitične kot operativne krize. Digitalizacija oskrbovalne verige je ključna za stabilnost in odpornost po-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

slovanja, saj organizacijam omogoča neposredno povezavo med realnim dogajanjem na terenu ter sistemi odločanja. Špica oskrbovalno verigo razume celovito – kot preplet materialnih tokov, ljudi, sredstev in informacij, kjer preglednost in sledljivost igrata osrednjo vlogo.

Špica digitalizacijo oskrbovalne verige obravnava kot razširitev upravljanja časa in prostora tudi na zunanje deležnike – dobavitelje, prevoznike, podizvajalce ter obiskovalce. Z rešitvami za sledljivost blaga in sredstev, digitalno skladiščno poslovanje, označevanje izdelkov ter popis osnovnih sredstev organizacije pridobijo zanesljiv vpogled v stanje in gibanje znotraj verige. To omogoča hitrejše in bolj utemeljene odločitve, zlasti v času motenj, ko so ročni postopki ter nepovezani sistemi najbolj izpostavljeni tveganjem.

Z vidika korporativne varnosti digitalizacija zmanjšuje odvisnost od posameznikov in improviziranih postopkov ter zagotavlja neprekinjeno sledljivost in nadzor nad dogajanjem. Organizacije se lahko hitreje odzovejo na izpade dobav, kadrov ali infrastrukture in lažje izvajajo alternativne scenarije. Digitalizirana oskrbovalna veriga tako postane pomemben steber poslovne kontinuitete in odpornosti, ne zgolj podporna logistična funkcija.

V čem vidite svojo ključno konkurenčno prednost v primerjavi z drugimi ponudniki rešitev za upravljanje časa, dostopa in procesov, kaj je tisto, kar vas na trgu resnično razlikuje?

Naša ključna konkurenčna prednost ni ena sama funkcionalnost, temveč celovit, dolgoročno vzdržen pristop, ki združuje tehnologijo, varnost in lokalni kontekst.

Špico na trgu razlikujejo predvsem lastni razvoj programske in strojne opreme, kar zagotavlja nadzor nad kakovostjo, varnostjo ter dolgoročno podporo. Gostovanje z oblačno infrastrukturo na Microsoft Azure v EU in certificirano informacijsko varnostjo (ISO 27001, 27017, 27018, IEC 60839). S 40 leti izkušenj smo razvili globoko razumevanje realnih okolij (industrija, logistika, kritična infrastruktura), integrirali upravljanje časa, prostora, dostopa in procesov na eni platformi ter dokazali delovanje v velikih in varnostno zahtevnih sistemih v regiji ter širše. Z lastnimi podjetji po Balkanu lahko z eno rešitvijo podpremo uporabnike, ki so prisotni v celotni Adriatic regiji.

Naše rešitve so preverjeni sistemi, ki delujejo tudi takrat, ko razmere niso idealne. Zato nas organizacije ne izbirajo zgolj kot dobavitelja, temveč kot dolgoročnega partnerja za korporativno varnost.

Kako vaše rešitve konkretno pomagajo organizacijam pri optimizaciji procesov, hkrati pa povečujejo varnost in pripravljenost na nepredvidljive dogodke?

Optimizacija in varnost nista v nasprotju – v resnici se dopolnjujeta. Jasni, avtomatizirani in podatkovno podprti procesi so manj ranljivi za napake ter zlorabe. Špica platforma zmanjšuje ročno delo, podvajanje podatkov in nejasnosti ter vse ključne informacije povezuje v enotno sliko. V kriznih situacijah se pokaže prava vrednost takšnega pristopa. Organizacija ima že vzpostavljeno preglednost, revizijske sledi, jasne vloge in podatke v realnem času. To omogoča hiter in nadzorovan odziv. Ne gre za vprašanje *če* se nepredvideni dogodki zgodijo, temveč *kdaj*. Naš cilj je, da so organizacije takrat pripravljene – z vidika poslovanja, varnosti in odgovornosti. ■

Foto: arhiv Špica International d.o.o.

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

INTERVJU
mag. Jože Knavs, direktor, Informatika d.o.o.*

INFORMATIKA POSTAJA KLJUČEN INTEGRATOR PODPORNIH SISTEMOV ZA ELEKTRODISTRIBUCIJSKA PODJETJA

Digitalna transformacija elektrodistribucijskega sistema zahteva zanesljive, povezane in varne podporne sisteme. Informatika se uveljavlja kot ključni integrator rešitev, ki povezujejo operativne, poslovne, varnostne in analitične funkcije v enoten ekosistem. O vlogi Informatike pri razvoju distribucijskih podjetij smo se pogovarjali z direktorjem mag. Jožetom Knavsom.

Distribucijska elektroenergetska omrežja so v zadnjem obdobju pod vse večjim pritiskom – kateri so ključni izzivi, s katerimi se danes soočate, zlasti z vidika odpornosti, digitalizacije in kibernetske varnosti?

Elektrodistribucijska omrežja se danes soočajo z izrazitim povečanjem kompleksnosti, predvsem zaradi pospešene digitalizacije in uvajanja naprednih tehnologij, kot so pametni merilni sistemi, daljinsko vodenje ter vključevanje razpršenih virov energije. Ti procesi prinašajo večjo učinkovitost in fleksibilnost, hkrati pa povečujejo ter odpirajo nove vektorske točke napadov.

Eden ključnih izzivov je konvergenca IT in OT okolij. Operativni sistemi, kot so SCADA in DMS, pogosto niso bili zasnovani z upoštevanjem sodobnih varnostnih zahtev, poleg tega pa zaradi potrebe po neprekinjenem delovanju dopuščajo le omejene posege in posodobitve. To ustvarja dodatna tveganja, saj lahko napadalci izkoristijo vrzeli med IT in OT segmenti ter ogrozijo kritične procese.

Dodatno kompleksnost prinašajo še regulatorne zahteve (direktiva NIS 2, ZInfV-1), ki uvajajo strožje obveznosti na področju upravljanja tveganj, zaznavanja in poročanja o incidentih. V kombinaciji z razpršeno infrastrukturo distribucijskih omrežij to pomeni, da kibernetska varnost postaja sistemska naloga. Ključni poudarki so zato vidljivost dogajanja, pravočasna detekcija in usklajen ter učinkovit odziv na incidente.

Kako v Informatika d.o.o. potekajo aktivnosti na področju vzpostavljanja bolj integriranih procesov skupnega energetskega VOC (operativnega centra) kibernetske varnosti in kakšne koristi to prinaša za distribucijski sektor?

V podjetju Informatika d.o.o. aktivnosti na področju vzpostavljanja integriranih procesov skupnega distribucijskega varnostno operativnega centra (VOC) temeljijo na povezovanju zaznavanja, analize in odziva v enoten operativni model. Ključni cilj je vzpostaviti centralizirano točko nadzora nad varnostnimi dogodki v IT in tudi v OT okoljih elektrodistribucijskih podjetij. Pri tem se uporabljajo napredne platforme za zbiranje, korelacijo dogodkov in avtomatizacijo odzivanja (*Security Information and Event Management -SIEM* in *Security Orchestration, Automation and Response - SOAR*), ki se nadgrajujejo s kibernetsko obveščevalno dejavnostjo (*Cyber Threat Intelligence – CTI*) ter izmenjavo indikatorjev ogroženosti prek platform, kot je MISP (*Malware Information Sharing Platform*).

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Med najpomembnejšimi koristmi, ki jih takšen VOC prinaša elektrodistribucijskim podjetjem, so izboljšana vidljivost nad varnostnim stanjem, hitrejše zaznavanje in odzivanje na incidente ter boljše upravljanje tveganj. Centraliziran pristop omogoča tudi učinkovitejšo izmenjavo informacij o grožnjah med deležniki in racionalizacijo virov, saj posamezna podjetja ne potrebujejo lastnih, popolnoma ločenih zmogljivosti 24/7 nadzora.

Kako spoznanja in izkušnje iz EU projektov vključujete v razvoj novih pristopov, zlasti na področju zagotavljanja kibernetske varnosti za distribucijska omrežja v Sloveniji?

Raziskovalno, razvojno in inovacijsko delo, ki ga podjetje Informatika d.o.o. izvaja v sklopu EU projektov, je sestavni del celovite strategije kibernetske varnosti. Kibernetska varnost ni izolirana aktivnost, temveč jo obravnavamo kot krožni proces, v katerem spoznanja in izkušnje, pridobljene iz EU projektov, kontinuirano izboljšujejo vpogled v aktualne trende ter izzive. Zlasti pilotni scenariji izpostavijo realne potrebe in ranljivosti informacijske ter elektroenergetske infrastrukture. Informatika d.o.o. zato pristopa k EU projektom ne samo kot razvojni, temveč predvsem kot pilotni partner. Na ta način v našem okolju potrdimo učinkovitost inovativnih rešitev za kibernetsko varnost in jih nato ustrezno vpeljujemo v varnostne procese, tako znotraj podjetja kot tudi v varnostnem operativnem centru za širši elektrodistribucijski sistem v Sloveniji.

Rešitve in spoznanja iz EU projektov vključujemo v tiste pristope h kibernetski varnosti, ki so ključni za okolje elektroenergetske infrastrukture. Ti pristopi so vselej preplet procesov, tehnologije, standardov in regulativ. Tako smo na podlagi spoznanj projekta CyberSEAS npr. vpeljali mehanizme izmenjave obveščevalnih informacij (CTI), ki združujejo tehnologijo MISP, požarne pregrade naslednje generacije, standardne formate in procedure za izmenjavo indikatorjev zlorab (*Indicators of Compromise – IoCs*) ter mehanizme sodelovanja in poročanja v skladu z nacionalnim odzivnim načrtom (NOKI) ter direktivo NIS 2. Inovativni pristopi, ki črpajo iz spoznanj in rezultatov EU projektov, vključujejo tudi na umetni inteligenci temelječe sisteme za zaznavanje anomalij, upravljanje kibernetskih ranljivosti ter odprte platforme za modeliranje, izvajanje, standardizacijo in izmenjavo odzivnih procedur.

Kako lahko vaše rešitve in storitve konkretno prispevajo k večji odpornosti distribucijskih sistemov, ki veljajo za enega bolj ranljivih delov elektroenergetskega sistema?

Rešitve in storitve podjetja Informatika d.o.o. krepijo odpornost distribucijskih sistemov predvsem z vzpostavitvijo stalnega nadzora, pravočasne detekcije ter usklajenega odziva na varnostne incidente. Ključno vlogo pri tem ima varnostno operativni center, ki omogoča 24/7 spremljanje dogodkov iz različnih virov, od klasičnih IT sistemov do elementov OT okolja. S centralizacijo podatkov v SIEM platformi in uporabo naprednih korelacijskih pravil se bistveno poveča vidljivost nad dogajanjem ter zmanjša čas zaznave potencialnih groženj.

Dodatno se uvajajo elementi avtomatizacije (SOAR), predvsem za obvladovanje ponavljajočih se nalog, kot so obogatitev dogodkov, inicialna analiza in sprožanje osnovnih odzivnih ukrepov, s čimer se razbremenjujejo analitiki ter skrajšuje odzivni čas.

S katerimi ključnimi projekti, inovacijami ali dosežki iz zadnjega obdobja bi se Informatika d.o.o. lahko posebej pohvalila na področju kibernetske varnosti in odpornosti?

Informatika d.o.o. je imela ključno vlogo pri razvoju odločitvenega sistema za oblikovanje in ocenjevanje proaktivnih strategij proti kibernetskim grožnjam, napadom ter ranljivostim. Ta sistem integrira napredne tehnike skupinskega odločanja in standardna ogrodja, kot so MITRE ATT&CK, CIS CSC (*Cyber Security Controls*) in NVD (*National Vulnerability Database*). Sistem nadgrajujemo in avtomatiziramo s sodelovalnimi agenti ter generativno umetno inteligenco.

Informatika d.o.o. kontinuirano vpeljuje in izboljšuje rešitve za izmenjavo obveščevalnih informacij (CTI) ter standardizacijo odzivnih procedur (*playbooks*). Osnova za CTI je platforma MISP, s katero se na nacionalnem in meddržavnem nivoju povezujemo v skupnosti z deležniki v elektroenergetskem sektorju ter širše. MISP smo integrirali z drugimi varnostnimi tehnologijami, kot je požarni zid naslednje generacije, s čimer lahko proaktivno preprečujemo grožnje, še preden se te udejanjijo v obliki kibernetskih napadov.

Nadgradnji teh pristopov sta integrirani platformi NG-SOC in ALiEnS-SOC za varnostne operativne centre naslednje generacije. Ti platformi vključujeta napredne sisteme za zaznavanje incidentov (SIEM) in orkestrirano odzivanje nanje (SOAR), modele umetne inteligence za razpoznavanje anomalij v omrežnih tokovih IT ter OT infrastruktur, orodja za ocenjevanje kibernetskih tveganj in ranljivosti storitev ter virov, mehanizme za izmenjavo obveščevalnih informacij, osrednji sistem za upravljanje postopkov odzivov na incidente in platformo za kibernetsko ozaveščanje ter izobraževanje.

Bi želeli še kaj sporočiti bralcem revije?

Omenjene sodobne tehnologije za zagotavljanje kibernetske varnosti same po sebi niso dovolj za učinkovito zaščito pred kibernetskimi napadi. Najpomembnejši dejavnik ostajajo ljudje, saj prav njihove odločitve in odzivi pogosto odločajo o tem, ali bo napad uspešen ali pravočasno zaustavljen. Zato veliko pozornosti namenjamo ozaveščanju naših zaposlenih in njihovemu rednemu izobraževanju, kot tudi deljenju znanja z uporabniki našega VOC, saj lahko le dobro informirani ter pripravljeni posamezniki učinkovito prispevajo k varnemu digitalnemu okolju. ■

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

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

INTERVJU
g. Jan Veršnik, vodja poslovnega razvoja, ASSA ABLOY Slovenija d.o.o.

ASSA ABLOY PROMOTOR TEHNOLOŠKE PODPORE ZA ODPORNOST V KRITIČNI INFRASTRUKTURI

Tehnološke rešitve za nadzor dostopa in fizično varnost postajajo ključni element odpornosti kritične infrastrukture. ASSA ABLOY s svojimi naprednimi sistemi aktivno prispeva k varnejšemu in bolj nadzorovanemu delovanju organizacij. O vlogi tehnologije pri krepitvi odpornosti smo se pogovarjali z vodjo poslovnega razvoja g. Janom Veršnikom.

Kako lahko sodobna tehnična sredstva za zagotavljanje varnosti prispevajo k večji odpornosti kritične infrastrukture v vse bolj kompleksnem varnostnem okolju?

Sodobna tehnična sredstva za zagotavljanje varnosti danes ne služijo več zgolj preprečevanju nepooblaščenega dostopa. Njihova vloga je predvsem v tem, da organizacijam omogočajo boljše razumevanje tveganj, hitrejše odločanje in učinkovitejši odziv, s čimer prispevajo k stabilnemu ter neprekinjenemu delovanju tudi v zahtevnih razmerah.

Z uporabo sodobnih, povezanih varnostnih rešitev lahko organizacije vzpostavijo večjo preglednost nad dogajanjem in omejijo vpliv morebitnih varnostnih incidentov. Pomemben del teh rešitev so tudi podatki, ki omogočajo analizo dogodkov, prepoznavanje vzorcev in boljše upravljanje tveganj. Na ta način varnost ni več zgolj zaščitni ukrep, temveč postane aktiven element odpornosti infrastrukture in podpore ključnim poslovnim procesom.

Prisotni ste v številnih vertikalah – katere ključne spremembe opažate pri naročnikih zaradi zaostrovanja varnostnih razmer in kako se te odražajo v njihovih zahtevah po varnostnih rešitvah?

Pri naročnikih opažamo vse večje zavedanje, da je varnost dolgoročen proces in ne enkratna naložba. Ne glede na panogo pričakujejo zanesljive rešitve, ki jih je mogoče enostavno upravljati in prilagajati spreminjajočim se zahtevam ter razmeram.

Opazne so zahteve po bolj naprednih tehnologijah in sistemih. Naročniki se vse pogosteje odločajo za prehod iz mehanskih na elektromehanske rešitve, saj te omogočajo večjo prilagodljivost, boljši nadzor in podporo sodobnim načinom upravljanja dostopov.

Naročniki pričakujejo celostne rešitve, ki omogočajo enotno upravljanje in jih je mogoče učinkovito povezati z obstoječimi sistemi. Zato postajajo integracije vse pomembnejše, saj omogočajo boljši pregled, enostavnejše upravljanje in večjo zanesljivost celotnega varnostnega okolja.

Katere so danes največje ranljivosti na področju fizične varnosti in kako jih lahko organizacije učinkovito naslovijo z naprednimi rešitvami?

Ena največjih ranljivosti danes izhaja iz dejstva, da se meje med fizičnim in digitalnim svetom brišejo, številne organizacije pa še vedno uporabljajo zastarele ter med seboj nepovezane varnostne sisteme. Klasične mehanske rešitve in zaprti elektronski sistemi ne omogočajo nadzora v realnem času, niti ustrezne povezave z IT okoljem, kar povečuje tveganja in zmanjšuje odpornost.

V skladu z usmeritvami NIS2 je učinkovit odgovor na te izzive integracija fizične varnosti v informacijsko okolje organizacije. To pomeni uporabo povezanih sistemov, ki temeljijo na načelih ničelnega zaupanja, kjer je vsak dostop preverjen in nadzorovan. Pomembno vlogo ima tudi uvedba šifrirane komunikacije, mobilnih poverilnic in večfaktorske avtentikacije, saj te omogočajo sprotno preverjanje identitete ter bistveno zmanjšujejo varnostna tveganja. S takšnim pristopom fizična varnost postane sestavni del celostnega upravljanja tveganj in odpornosti organizacij.

V čem se ASSA ABLOY s svojimi pristopi in produkti razlikuje od drugih ponudnikov na trgu – kaj je vaša ključna konkurenčna prednost?

ASSA ABLOY ima vodilno pozicijo na področju rešitev za fizično varnost, ki temelji na globalni prisotnosti, bogatih izkušnjah in poglobljenem strokovnem znanju. Prisotnost na različnih trgih nam omogoča dober vpogled v raznolike varnostne zahteve in prenos preverjenih rešitev ter dobrih praks v lokalna okolja.

Pomemben del naše konkurenčne prednosti so inovacije. Stalno vlagamo v razvoj novih tehnologij in rešitev, ki sledijo dejanskim potrebam uporabnikov ter razvoju varnostnih zahtev in regulative. Pri tem se ne osredotočamo zgolj na tehnologijo, temveč tudi na njeno praktično uporabo, dolgoročno zanesljivost in upoštevanje okoljskih vidikov.

Naš produktni portfelj združuje mehanske, elektromehanske in digitalne tehnologije, kar naročnikom omogoča celovite, prilagodljive ter razvojno odprte rešitve. Prav ta kombinacija širine ponudbe, strokovnega znanja in inovacij nam omogoča, da naročnikom dolgoročno ostajamo zanesljiv partner.

Vaša močna mednarodna prisotnost omogoča prenos izkušenj in dobrih praks – kako te globalne vpoglede prenašate v lokalno okolje ter jih uporabljate za dvig varnosti in odpornosti organizacij?

Mednarodna prisotnost nam omogoča neposreden vpogled v različne varnostne scenarije, regulativne okvire in dobre prakse na globalni ravni. Te izkušnje sistematično prenašamo v lokalno okolje skozi tesno sodelovanje z lokalnimi enotami, projektanti, partnerji in naročniki.

Pri tem je ključno, da globalne pristope vedno prilagodimo lokalnim specifikam, tako zakonodajnim kot operativnim. Na ta način lahko naročnikom ponudimo preverjene rešitve, ki temeljijo na mednarodnih izkušnjah, hkrati pa so skladne z lokalnimi zahtevami in realnimi izzivi okolja, v katerem delujejo.

Kot globalno vodilno podjetje na svojem področju vidimo svojo vlogo tudi v prenosu znanja in inovacij v lokalno okolje. To izvajamo preko strokovnih dogodkov, izobraževanj in neposrednega sodelovanja, s ciljem dviga varnosti ter odpornosti organizacij.

Bi še kaj sporočili našim bralcem?

Fizična varnost danes ni več nekaj samoumevnega, temveč pomemben del uspešnega in varnega poslovanja. Ker se tveganja hitro spreminjajo, je vse bolj pomembno, da organizacije pravočasno vlagajo v sodobne varnostne rešitve. Te pomagajo zaščititi ljudi, premoženje in zagotoviti, da delo poteka nemoteno. Pri tem veliko šteje tudi izbira zaupanja vrednih partnerjev.

Pri ASSA ABLOY verjamemo, da je prihodnost varnosti v povezanih, inteligentnih in uporabniku prijaznih rešitvah, ki predstavljajo dolgoročno naložbo v zaupanje, učinkovitost ter zaščito. Naš cilj je v sodelovanju z naročniki soustvarjati varnostno okolje, ki krepi odpornost organizacij, podpira nemoteno delovanje in prispeva k višji ravni zaščite ljudi ter sredstev. To strokovno usmeritev in odgovornost do varnosti želimo dosledno deliti tudi s širšo strokovno javnostjo. ■

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

INTERVJU
g. Igor Zgonc, direktor, Silver Bullet Risk*

CELOVITOST IDENTIFIKACIJE IN UPRAVLJANJA TVEGANJ KLJUČNA ZA PREŽIVETJE ORGANIZACIJ

Celovito razumevanje tveganj postaja temelj dolgoročne stabilnosti in odpornosti organizacij. Silver Bullet Risk razvija pristope, ki združujejo identifikacijo, analizo in upravljanje tveganj v enoten strateški okvir. O ključnih izzivih in rešitvah na tem področju smo se pogovarjali z direktorjem Igorjem Zgoncem.

Vse bolj kompleksno varnostno okolje zahteva sistematičen pristop k tveganjem. Kako ocenjujete zrelost upravljanja tveganj v organizacijah danes?

Če sem popolnoma direkten – večina organizacij danes nima upravljanja tveganj. Imajo iluzijo upravljanja tveganj. Ta iluzija temelji na tem, da obstaja nek dokument, neka Excel tabela, nek letni proces. Ampak to ni upravljanje, to je dokumentiranje. In to je ključna razlika, ki jo moramo jasno komunicirati.

Vidimo tipičen vzorec: enkrat letno ocena, nekaj ukrepov, podpis in arhiv. Medtem pa se poslovanje spreminja vsak dan. Tveganja živijo vsak dan. Sistem pa ostaja statičen.

Če pogledamo čisto poslovno logiko: nihče si ne bi dovolil, da bi finančne podatke posodabljal enkrat letno, pri tveganjih pa to še vedno počnemo.

Če tveganj ne upravljaš sproti, jih ne upravljaš. In večina organizacij je danes še vedno v fazi, kjer imajo občutek nadzora – brez dejanskega nadzora.

Ali vodstva res razumejo tveganja kot poslovno vprašanje?

Razumejo jih, dokler je vse v redu. Ko pride do težave, pa pride tudi vprašanje: »Kako je to mogoče?« In to je zelo zanimiv moment, ker se pogosto izkaže, da je bilo tveganje že prepoznano, vendar ni bilo upoštevano pri odločanju. Ključni problem v večini primerov torej ni pomanjkanje znanja, temveč njegova uporaba, ker se tega znanja ne uporablja pri odločanju.

Upravljanje tveganj brez vpliva na odločitve je samo administracija.

Dokler vodstvo tveganj ne začne uporabljati za konkretna vprašanja – kam investirati, kaj ustaviti, kje smo najbolj izpostavljeni – bo vse skupaj ostalo na nivoju poročila. In tukaj je ključ: Vodstvo določa, ali bo »risk management« živ ali mrtev.

In smo spet pri iluziji nadzora. Občutek, da imamo stvari pod kontrolo, ker imamo dokument.

Kako se vaša rešitev Silver Bullet Risk umešča v primerjavi s tradicionalnimi pristopi, kot je Excel?

Excel ni problem. Problem je, da ga uporabljamo za stvari, za katere nikoli ni bil namenjen. Gre za orodje, ki je pasivno, nepovezano in brez časovne dimenzije. Z Excelom odgovarjaš na vprašanje – »Kaj smo zapisali?«

S sodobnimi sistemi pa lahko odgovorimo, kaj se dogaja, kaj se bo zgodilo in kaj moramo storiti danes. To ni majhna razlika! To je razlika med evidenco in upravljanjem. In tukaj pridemo do ključne zmote na trgu –

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

percepcije stroška. Cena Excela je praktično brezplačna, ampak cena napačne odločitve pa nas lahko stane podjetja. Tukaj je prisoten tudi večni slovenski problem, prevzemanje odgovornosti. Dokler organizacije gledajo na orodje kot strošek, so na napačni strani enačbe. Ne kupujemo orodja. Kupujemo sposobnost boljšega odločanja.

Kako izkušnje iz EU projektov vplivajo na razvoj vaših rešitev?

EU projekti jasno pokažejo, da organizacije praviloma vedo, kaj morajo narediti, standardi so jasni. Težave nastanejo pri implementaciji. Kompleksnost zahtev, ročni procesi in nepovezani sistemi povzročijo, da upravljanje tveganj ostane na papirju. Naš fokus je zato pretvoriti kompleksne zahteve v rešitve, ki so dovolj enostavne, da jih uporabniki dejansko uporabljajo.

Realno je, da če rešitev ni enostavna, se ne bo uporabljala.

Kako lahko s svojimi rešitvami konkretno prispevate k večji odpornosti organizacij?

Ko govorimo o odpornosti, to pogosto zveni abstraktno. Ampak v resnici gre za zelo konkretno vprašanje – »Ali bo organizacija preživela naslednji šok ali ne?«

Mi pomagamo organizacijam narediti premik iz odločanja na podlagi občutka v odločanje na podlagi podatkov. Namesto »mislim, da je to tveganje veliko«, imamo kazalnike, trende in realno sliko.

Drugi premik je iz reakcije v predvidevanje. Večina organizacij reagira, ko se incident zgodi. Mi želimo, da zaznajo signal prej.

In tretji premik je iz kaosa v prioritete. Vsi imajo preveč tveganj. Ključno vprašanje je: katera so tista, ki jih moramo obvladovati danes.

Odpornost ni v tem, da nimaš problemov. Odpornost je v tem, kako hitro jih zaznaš in kako dobro se odzoveš, kako jih obvladuješ.

Proces upravljanja tveganj pogosto ostaja statičen. Kako ga preoblikovati v dinamičen sistem?

Največja napaka, ki jo vidimo, je, da je upravljanje tveganj vezano na koledar. Enkrat letno, enkrat kvartalno, kot da tveganja čakajo na termin. Ampak tveganja ne delujejo po koledarju. Dogajajo se ves čas. Če želimo narediti preboj, moramo spremeniti logiko.

Tveganja morajo biti povezana z realnimi dogodki – z incidenti, spremembami v procesih, z dejanskim poslovanjem. Če te povezave ni, govorimo o teoriji.

Naslednja ključna stvar je merjenje. Če tveganja ne meriš, ga ne upravljaš. Spremljati moramo kazalnike, trende in postavljati pragove. Brez vsega tega je vse skupaj samo mnenje.

In ne nazadnje sistem. Procesi, ki temeljijo na ročnem delu, ne morejo slediti dinamiki okolja. Ročni sistem upravljanja tveganj je že v osnovi zastarel.

Ko to vse povežemo, dobimo živ sistem. In takrat se zgodi ključni preobrat. Upravljanje tveganj postane nekaj, kar dejansko pomaga voditi podjetje.

Kaj je danes ključno sporočilo za vodstva organizacij?

Organizacije praviloma ne propadejo zato, ker tveganj ne bi poznale, temveč zato, ker jih ne obravnavajo pravočasno. Upravljanje tveganj ni več zgolj formalna zahteva, temveč ključna disciplina za stabilnost in rast. Tudi ni Excel ali samo poročilo. Upravljanje tveganj je disciplina preživetja in rasti.

Pravo vprašanje danes ni več, ali ga potrebujemo, ampak ali si lahko privoščimo, da ga nimamo. ■

Foto: arhiv Silver Bullet Risk

UČINKOVITO OBVLADOVANJE TVEGANJ ZA ZAŠČITO KRITIČNE INFRASTRUKTURE IN INFORMACIJSKIH SISTEMOV

Motnje v delovanju kritične infrastrukture in kibernetski napadi so danes ena največjih groženj za podjetja in organizacije ter družbo nasploh.

Upravljanje teh tveganj zahteva sistematičen pristop, skladnost s predpisi in podporo naprednih rešitev.

Ekipa Silver Bullet Risk (SBR) vam nudi:

- svetovanje pri identifikaciji, oceni in obvladovanju tveganj,
- podporo pri doseganju skladnosti (NIS2/ZInfV-1, CER/ZKI-1, ISO/IEC 27001, ISO 22301),
- programsko rešitev za digitalizacijo procesov upravljanja tveganj,
- orodja za spremljanje, poročanje (upravi, nadzornim organom, regulatorjem) in odločanje.

Kritična infrastruktura potrebuje sistematično obvladovanje tveganj. Pišite nam in pokazali vam bomo, kako.

info@silverbulletrisk.com - www.silverbulletrisk.com

KRIK aksum

Zavarovalno posredniška družba d.o.o.

ZAVAROVANJE KIBERNETSKIH TVEGANJ

Strokovna pomoč pri pridobivanju zavarovanja kibernetskih tveganj tako doma kot v tujini

Zavarovanje krije predvsem:

- kritje lastne škode
- kritje odškodninskih zahtevkov tretjih oseb (odgovornost iz omrežja)
- kritje za obratovalni zastoj
- kritje kibernetskega izsiljevanja in kriminala

Več info na cyber@krikaksum.si

www.krikaksum.si

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

INTERVJU
g. Miha Abrahamsberg, prokurist, KRIK AKSUM
Zavarovalno posredniška družba d.o.o.

ZAVAROVALNIŠTVO V DOBI KRIZ: GRADNIK SISTEMSKE ODPORNOSTI

Zavarovalništvo v času naraščajočih tveganj postaja ključni mehanizem za zagotavljanje finančne in operativne odpornosti organizacij. KRIK AKSUM d.o.o. s celovitimi pristopi k upravljanju tveganj pomembno prispeva k stabilnosti poslovnega okolja. O vlogi zavarovalništva pri krepitvi sistemske odpornosti smo se pogovarjali s prokuristom Miho Abrahamsbergom.

Kibernetska tveganja postajajo ena ključnih poslovnih groženj – kako v Krik Aksum pristopate k oblikovanju zavarovalnih programov, ki ustrezno pokrivajo ta hitro razvijajoča se tveganja?

Drži, kibernetska tveganja danes niso več le tehničen izziv, temveč ena ključnih poslovnih groženj, ki lahko neposredno ogrozi obstoj podjetja. V družbi KRIK AKSUM d.o.o. k oblikovanju zavarovalnih programov pristopamo sistematično in individualno, saj se zavedamo, da so digitalni procesi ter delo na daljavo postali neločljiv del vsakega sodobnega poslovanja.

Naš proces temelji na treh ključnih fazah:

- ***Identifikacija in analiza tveganj:*** Kot neodvisni zavarovalni posrednik najprej s stranko identificiramo kritične točke poslovanja. Pri tem si pogosto pomagamo z našimi strokovnimi orodji (kot je npr. SimpRisk), ki omogočajo pregledno oceno in vrednotenje tveganj. To je najpomembnejša faza, kjer določimo, katera tveganja so za stranko ključnega pomena.

- ***Strukturiranje zavarovalnega programa:*** Na podlagi analize pripravimo nabor zavarovalnih kritij. Kibernetska zavarovanja strankam praviloma predlagamo že v prvi fazi kot eno od ključnih zaščit.

- ***Prilagoditev in potrditev:*** V zadnji fazi upoštevamo specifične zahteve in želje stranke. Končni zavarovalni program je tako povsem prilagojen potrebam pooblastitelja, ki mu na podlagi neodvisne analize trga zagotovimo optimalno razmerje med obsegom kritij in višino premije.

Čeprav kibernetska tveganja vključujemo v osnovne predloge praktično vsem strankam, pa program vedno prilagodimo njihovi specifični dejavnosti. Naš cilj je, da stranka sprejme odločitev o poslovnih zavarovanjih na podlagi celovitih informacij, s čimer zagotovimo dolgoročno varnost njenega poslovanja.

Kako ocenjujete zrelost slovenskih organizacij pri razumevanju kibernetskih tveganj – ali zavarovanje še vedno dojemajo kot formalnost ali kot pomemben del celovite odpornosti?

Zavedanje v Sloveniji glede zavarovanja kibernetskih tveganj se hitro izboljšuje. Če so podjetja še donedavno to zavarovanje dojemala kot nepotreben strošek ali zgolj formalnost, danes v njem vse bolj vidijo ključni steber odpornosti. K temu so prispevali odmevni incidenti, pa tudi spoznanje, da zavarovanje ne krije le finančne škode, temveč zagotavlja takojšnjo krizno asistenco v organizaciji z zavarovalnico. Čeprav imamo v primerjavi z EU (in predvsem UK ter ZDA) še precej prostora za napredek, se trend jasno odmika od podcenjevanja tveganj k

njihovemu aktivnemu upravljanju; to je v kontekstu zavarovanja.

Kot neodvisni posrednik imate vpogled v različne ponudbe na trgu – kako pomagate strankam izbrati optimalno kibernetsko zavarovanje glede na njihove dejanske potrebe in tveganja?

Kot neodvisni posrednik strankam zagotavljamo objektivno analizo trga in rešitve po meri. Naš proces se vedno začne pri domačih zavarovalnicah, kjer preverimo razpoložljive možnosti in pogoje. Vendar pa so kibernetska tveganja specifična, zato v primerih, ko slovenski trg ne nudi zadostnih kritij, ko so premije nekonkurenčne, ali pa gre za kompleksna tveganja, posežemo tudi po mednarodnih rešitvah.

Družba KRIK AKSUM ima neposreden dostop do tujih trgov, predvsem do vsem dobro poznanega londonskega Lloyd'sa. To nam omogoča, da strankam zagotovimo najsodobnejše produkte z najširšimi kritji. Naš cilj je vedno enak: poiskati optimalno razmerje med varnostjo in stroškom.

Kako pomembna je vaša vloga v primeru kibernetskega incidenta – kako konkretno podpirate stranke pri uveljavljanju zavarovalnin in komunikaciji z zavarovalnicami?

Stranko najprej opozorimo na možne nevarnosti, da se jim izogne in do škodnega primera sploh ne pride, saj delujemo tako preventivno kot kurativno. V primeru kibernetskega incidenta nas stranka o tem takoj obvesti, mi pa jo usmerjamo pri prijavi škode. Pri tem je ključno, da se čim prej vključi zavarovalnico in skupaj z njo specializirane strokovnjake oziroma forenzike, ki poskrbijo za čim hitrejšo odpravo posledic napada.

V celotnem postopku stranki svetujemo z našim strokovnim znanjem in bogatimi izkušnjami. Če zavarovalnica neustrezno zavrne kritje, za stranko pripravimo ugovor ali pritožbo. Poleg tega izvajamo redne sestanke, kjer preverjamo ustreznost kritij glede na spreminjajoče se okoliščine in zakonodajo, saj se potrebe po zavarovalni zaščiti nenehno razvijajo.

V čem vidite svojo ključno konkurenčno prednost pri obravnavi varnostnih in kibernetskih tveganj – kaj je tista dodana vrednost, ki jo prinašate svojim strankam v primerjavi z drugimi ponudniki na trgu?

Naša ključna konkurenčna prednost temelji na treh stebrih: tradiciji, mednarodnem dosegu in nenehnem razvoju. Kot ena največjih zavarovalno-posredniških družb in z enim najdaljših staležev na slovenskem trgu razpolagamo z neprecenljivimi izkušnjami, ki nam omogočajo, da predvidimo izzive, ki jih drugi morda spregledajo.

Dodana vrednost, ki jo prinašamo, pa se kaže predvsem v naslednjem:

- ***Odlično poslovno sodelovanje*** z vsemi največjimi domačimi zavarovalnicami in dostop do globalnih zavarovalnih trgov. To nam omogoča, da svojim strankam ponudimo napredna zavarovalna kritja, ki na slovenskem trgu lahko še niso na voljo, ali pa jih sami pomagamo oblikovati.

- ***Neodvisnost in strokovnost:*** Strank ne obravnavamo le kot kupce polic, temveč kot partnerje. Z uporabo lastnih metodologij za oceno tveganj zagotavljamo, da je vsak zavarovalni program ukrojen po meri dejanskih potreb podjetja.

- ***Proaktivna vizija:*** Kljub vodilnemu položaju ne »spimo na lovorikah«. Zavarovaljiva tveganja se spreminjajo dnevno, zato nenehno vlagamo v izobraževanje in nove tehnologije. Naša dolgoročna vizija je biti korak pred nevarnostmi, s čimer strankam zagotavljamo brezskrbno poslovanje v moderni, digitalni dobi. ■

Foto: arhiv KRIK AKSUM

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

INTERVJU
g. Boštjan Primec, direktor, Simtech d.o.o.*

INTEGRACIJA BREZ KOMPROMISOV: POT DO PAMETNIH IN VARNIH SISTEMOV

Celovita integracija tehničnih sistemov je temelj za učinkovito, varno in pametno upravljanje sodobnih objektov in procesov. Simtech razvija rešitve, ki brez kompromisov povezujejo različne sisteme v enoten in zanesljiv ekosistem. O izzivih in priložnostih integracije smo se pogovarjali z direktorjem Boštjanom Primcem.

Kot ambiciozno podjetje in zastopnik vodilnih znamk na področju kontrole pristopa ter AI video nadzora – kako vidite razvoj varnostnih tehnologij v kontekstu vedno večjih zahtev po odpornosti organizacij?

V Simtechu prihajamo iz sveta informacijske tehnologije in varnosti, zato prihodnost vidimo v popolni avtomatizaciji ter integraciji v enovit, pameten EKO sistem. Organizacije so odporne le, ko tehnični segmenti delujejo usklajeno. Inteligentni videonadzor takoj zazna incident in obvesti službe, prava moč pa se pokaže ob povezavi s kontrolo pristopa. V primeru požara sistem sprosti evakuacijske poti, ob napadu pa brez človeškega posredovanja izvede »Lock down« in zapre dostope, reševalcem pa natančno sporoči število ljudi v stavbi. V ta ekosistem se logično vključujejo tudi alarmni in požarni sistemi ter napredna robotika in droni. Naša filozofija je preprosta: ljudje smo zmotljivi, le napredna tehnologija lahko 365 dni v letu z 99,9-odstotno zanesljivostjo zagotavlja dokumentirano varovanje brez napak.

Kako lahko napredne rešitve prispevajo k višji ravni varnosti tako v podjetjih kot v širšem kontekstu kritične infrastrukture?

Ključna je povezanost. Na trgu je veliko zaprtih sistemov, mi pa z IT pristopom načrtujemo arhitekturo, ki zagotavlja visoko zanesljivost, avtomatsko arhiviranje podatkov in takojšen preklop na rezervni strežnik, kar je pri varovanju kritične infrastrukture nujno. Da bi pri uporabniku vzpostavili pameten sistem, obstoječe opreme ne zavržemo na silo. Z našim »Retrofit« konceptom večinoma ohranimo obstoječe kamere in zamenjamo le strežnik, ki sistemu vdahne umetno inteligenco. Prav tako rešitve kontrole pristopa vgrajujemo brez kabliranja – baterijsko napajanje zdrži več kot 150.000 vstopov, enote pa zanesljivo delujejo v ekstremnih vremenskih razmerah. Ključno je, da ima uporabnik nadzor nad vsem vedno pri sebi na telefonu, od koder na daljavo upravlja vhode in takoj prejema obvestila o incidentih.

V čem vidite ključno dodano vrednost sodelovanja z vodilnimi proizvajalci – kako to partnerstvo prenašate v konkretne koristi za naročnike?

Zastopamo globalne gigante, ki ne le sledijo trendom, temveč soustvarjajo standarde prihodnosti. Naš glavni partner za videonadzor je Motorola Solutions, pod okriljem katere so danes združene vrhunske znamke, kot so Avigilon, Pelco in pametni senzorji HALO. Ponosni smo, da imamo najvišji partnerski in distribucijski status za balkanski trg. Pri kontroli pristopa pa ekskluzivno stavimo na španskega inovatorja Salto Systems. Trg je preplavljen s cenenimi rešitvami z Daljnega vzhoda, ki jih hekerji hitro lahko razbijejo. Ker z elektronskimi ključavnicami varujemo življenja, informacije in premoženje, se držimo načela: »Nisem tako bogat, da bi

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

poceni kupoval.« Največja korist za naročnike pa je naša izjemna tehnična ekipa, ki v Sloveniji pri največjih korporacijah že vzdržuje nekaj tisoč pristopnih točk in na stotine alarmnih sistemov proizvajalca Ajax.

Katere ključne izzive opažate pri organizacijah pri uvajanju sodobnih varnostnih rešitev in kako jim pomagate pri prehodu na bolj napredne sisteme?

To je zelo pogosto in hkrati eno najtežjih vprašanj v naši industriji. Če smo povsem iskreni, so na prvem mestu pri naših korporativnih uporabnikih skoraj vedno razpoložljiva finančna sredstva za investicije. Nabavni procesi v korporativnih okoljih so dolgi, kompleksni in močno odvisni od tega, kako vodstvo razume vlogo ter dodano vrednost tehničnega varovanja. Pogosto se nanj še vedno gleda zgolj kot na strošek.

Drugi velik izziv je pomanjkanje zavedanja o tehnološkem napredku in strah pred spremembami. Uporabniki niso vedno seznanjeni z najnovejšimi zmožnostmi tehnologije, hkrati pa se bojijo, da prehod na napreden sistem pomeni, da bodo morali celotno obstoječo opremo zavreči in vse graditi na novo.

V podjetju Simtech k tem izzivom pristopamo zelo pragmatično in s tremi ključnimi rešitvami:

- **Kvantificirani finančni prihranki (ROI):** Uporabniku ponudimo rešitve, pri katerih lahko jasno, v številkah, izmerimo finančni prihranek. Naj si bo to z optimizacijo stroškov, preprečevanjem izpadov ali avtomatizacijo procesov.
- **»Retrofit« namesto revolucije:** Obstoječih sistemov ne mečemo stran. Zamenjamo zgolj ključna vozlišča in obstoječi opremi vdahnemo pamet. Ko naročniki vidijo, kako enostavno in učinkovito je mogoče implementirati naše rešitve, so vedno izjemno pozitivno presenečeni.
- **Varnost kot storitev (*Solution as a Service*):** Na trgu ne ponujamo le klasičnega modela, temveč naročnikom omogočamo najem rešitve. V tem modelu mi investiramo v opremo in implementacijo, naročnik pa uporabo sistema plačuje kot fiksni mesečni strošek. S tem investicijo premaknemo iz t. i. *CAPEX-a* v *OPEX*, kar vodstvom bistveno olajša odobritev.

Ta model storitve in naš celoten pristop pa izhajata iz naše osnovne filozofije, ki bi jo tu rad posebej izpostavil: **naših poslovnih kupcev ne obravnavamo zgolj kot strank, temveč kot naše dolgoročne partnerje**. Za nas nista ključna zgolj prodaja in gola implementacija, temveč tisto, kar sledi – absolutno najpomembnejša sta nam dolgoročno, brezhibno delovanje naših rešitev ter popolno zadovoljstvo uporabnikov. Le na takšen način lahko zgradimo trden EKO sistem in medsebojno zaupanje, ki je pri varnosti neprecenljivo.

Kako lahko s svojimi inovativnimi rešitvami in pristopi prispevate k večji varnosti ter odpornosti ne le posameznih organizacij, temveč tudi širšega družbenega okolja?

Življenje v Sloveniji je bilo doslej relativno varno, a to prinaša nevarnost lažnega občutka nedotakljivosti. Kriminal je v porastu. Na eni strani imamo ulično kriminaliteto, na drugi pa se v korporativnem svetu bijejo tihe bitke – kraje podatkov in industrijsko vohunstvo, o katerih podjetja javno molčijo. Naša tehnologija in strokovnost predstavljata neprebojen ščit, ki varuje gospodarstvo in delovna mesta. Vendar pa vrhunska tehnika ni vse. Naša širša vizija je dvig varnostne kulture vsakega posameznika. Zbuditi se moramo in biti pozorni na nevarnosti v svoji okolici. Tehnologija, ki jo uvajamo, nikoli ne zaspi, a za resnično odporno in varno družbo mora biti buden predvsem človek. ■

Foto: arhiv Simtech d.o.o.

SIMTECH

OPTIMIZACIJA VAROVANJA VAŠEGA OBJEKTA
Z UČINKOVITO IN UGODNO REŠITVIJO

info@simtech.si www.simtech.si

AVIGILON
MOTOROLA SOLUTIONS
salto INSPIRED ACCESS
AJAX

Integrirane rešitve
INTELIGENTNEGA VIDEONADZORA
in kontrole pristopa.

NADZORNE KAMERE

PAMETNI SENZORJI

KOMUNIKACIJE KI VARUJEJO

Vodilne rešitve za **VARNOST** in **ZANESLJIVO KOMUNIKACIJO** tam kjer šteje vsaka sekunda.

PAMETNI NADZOR DOSTOPA, KJERKOLI IN KADARKOLI

Inovativne rešitve za **ELEKTRONSKI NADZOR PRISTOPA** - varno, prilagodljivo brez kompromisov.

PAMETNA VARNOST BREZ KOMPROMISOV

Celovita varnostna rešitev z **UMETNO INTELIGENCO** za popolen nadzor - kjerkoli in kadarkoli.

CELOVITE REŠITVE ZA OKOLJA Z NAJVIŠJIMI VARNOSTNIMI ZAHTEVAMI

V okoljih, kjer se upravlja kritična infrastruktura, občutljivi podatki ali procesi, je ključna kombinacija popolne sledljivosti, fizične zaščite in centralnega nadzora.

Digitalno zaklepanje ni več nadgradnja, temveč nujen korak k skladnosti, varnosti in obvladovanju tveganj v sodobnih podatkovnih centrih.

iLOQ S50 digitalni sistem zaklepanja

omogoča upravljanje dostopa do rack omar in tehničnih prostorov prek pametnega telefona.

iLOQ S50 podpira cilje NIS2, saj omogoča:

- jasno identifikacijo vsakega uporabnika,
- sledljivost in revizijsko evidenco dostopov,
- takojšen preklic pravic ob varnostnem incidentu,
- zmanjšanje tveganja zaradi izgubljenih ali kopiranih ključev.

Tubularna varnostna vrata za kontroliran prehod v varovani perimeter

Povsod, kjer je varnost proces, ne zgolj oprema, je nadzor prehoda ključen del zaščite.

- Učinkovito preprečevanje tailgatinga (prehoda dveh oseb).
- Napredno senzorsko zaznavanje nepravilnosti.
- Robustna jeklena konstrukcija in varnostno steklo za industrijsko uporabo.
- Integracija s kontrolo pristopa in evidenco delovnega časa.

ID Shop – povezujemo tradicionalno varnost in pametne tehnologije.

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

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

INTERVJU
g. Predrag Petrović, direktor, ID Shop d.o.o.

ID SHOP KLJUČNI DELEŽNIK NA PODROČJU NAPREDNIH SISTEMOV KONTROLE DOSTOPA

Napredni sistemi kontrole dostopa postajajo ključni element celovite varnosti organizacij. ID Shop se uveljavlja kot pomemben deležnik pri razvoju zanesljivih in tehnološko naprednih rešitev za nadzor dostopa. O trendih in prihodnjih izzivih smo se pogovarjali z direktorjem Predragom Petrovičem.

Fizična varnost ostaja temelj odpornosti organizacij – kako iLOQ sistemi za zaklepanje prispevajo k višji ravni zaščite in odpornosti ključnih organizacij ter kritične infrastrukture?

Če izhajam iz prakse in večletnih izkušenj z rešitvami iLOQ, se je kot ena večjih pomanjkljivosti pokazalo dejstvo, da številne organizacije določenih lokacij sploh niso mogle vključiti v sistem kontrole dostopa. Govorim predvsem o oddaljenih tehničnih objektih, kjer ni elektrike, ni signala, vremenski pogoji pa so pogosto zelo zahtevni.

Z iLOQ smo to dejansko spremenili. Gre za rešitev, ki ne potrebuje baterij ali ožičenja, pa vseeno omogoča vse funkcionalnosti, ki jih od sodobne kontrole dostopa pričakujemo – centralno upravljanje, revizijsko sled, dodeljevanje pravic na daljavo. To pomeni, da lahko danes tudi takšne lokacije obravnavamo enakovredno kot objekte v urbanem okolju.

Meni osebno se zdi ključna ta kombinacija: na eni strani robustnost mehanskega sistema, na drugi strani fleksibilnost elektronike. Organizacije se tako izognejo pomanjkljivostim fizičnih ključev; zmanjšajo tveganje izgube ali zlorabe, hkrati pa imajo natančen vpogled v to, kdo je dostopal do objekta in kdaj. To je še posebej pomembno pri kritični infrastrukturi, kjer so takšni podatki pogosto odločilni.

Kako se potrebe trga na področju varnostnih rešitev spreminjajo v zadnjih letih – ali organizacije danes bolj razumejo pomen celostne odpornosti, tudi na ravni fizičnega dostopa?

Zavedanje o pomenu fizične varnosti se nedvomno izboljšuje, vendar v praksi še vedno opažam precejšen razkorak. Organizacije danes veliko vlagajo v videonadzor in kibernetsko varnost, pogosto pa kontrolo dostopa omejijo zgolj na vhodne točke – velikokrat tudi z namenom beleženja delovnega časa.

Čeprav so takšni ukrepi smiselni, se pri tem pogosto pozablja na osnovno dejstvo: do kritičnih prostorov, podatkov ali opreme je še vedno mogoče dostopati fizično – skozi vrata. Prav zato v našem podjetju vedno izhajamo iz temeljev. Prvi korak je urejen mehanski sistem zaklepanja, kar pomeni nadzorovano število ključev, jasno definirane pravice dostopa in zaščiten sistem, ki preprečuje nepooblaščeno kopiranje. Šele potem ima smisel nadgrajevati z elektronskimi sistemi.

Pogosto se srečujemo z napačnim razumevanjem kontrole dostopa – prisotnost kartičnega sistema še ne pomeni, da so vrata dejansko varna. Če vrata niso ustrezno zaklenjena, je mogoče sistem razmeroma enostavno obiti, brez da bi kontrola dostopa kjerkoli zabeležila ta prehod. Zato vedno poudarjam: kontrola dostopa ne nadomešča zaklepanja, temveč ga mora nadgraditi.

Pomemben vpliv na dvig zavedanja ima tudi direktiva NIS2, ki jasno poudarja, da brez ustrezne fizične varnosti ni celovite zaščite. Zahteve po sledljivosti dostopov in nadzoru nad vstopi danes niso več priporočilo, temveč standard – in to je korak v pravo smer.

Katere ključne projekte ali implementacije iz zadnjega obdobja bi izpostavili kot primere dobrih praks pri krepitvi varnosti in odpornosti?

En projekt, ki ga rad izpostavim, je implementacija v podatkovnem centru, kjer smo zaklenili posamezne strežniške omare. Prej so uporabljali klasične ključe, kar pomeni, da niso imeli realnega vpogleda v to, kdo dostopa do katere opreme. Danes imajo za vsako omaro natančno revizijsko sled. To je konkreten primer, kako fizična varnost neposredno podpira tudi kibernetsko – in tudi zahteve, ki jih prinaša NIS2.

Drug primer so projekti v energetiki, kjer pride do izraza ATEX certification. To pomeni, da lahko naše rešitve uporabljamo tudi v eksplozijsko nevarnih okoljih, ker ne povzročajo iskrenja ali drugih virov vžiga. Takšnih objektov je veliko in pogosto so razpršeni, brez nadzora nad dostopi. Z uvedbo sistema smo omogočili centralno upravljanje in pregled nad dogajanjem, kar prej ni bilo mogoče.

Zelo zanimiv segment je tudi transport – recimo železnice. Tam se je kot ključna prednost pokazala fleksibilnost. Če pride do okvare, lahko dostop v nekaj sekundah dodelimo serviserju, ki je najbližje. Ni več logistike s ključi, ni čakanja. To se v praksi zelo pozna – tako z vidika varnosti kot učinkovitosti.

Kako lahko napredni sistemi upravljanja dostopa, kot jih razvijate v ID Shop-u, prispevajo k večji odpornosti organizacij v kriznih situacijah (npr. omejevanje dostopa, hitro prilagajanje režimov varovanja)?

V kriznih situacijah se po mojem mnenju najbolj pokaže prava vrednost takšnih sistemov. Ključno je, da lahko reagiraš hitro in brez zapletov.

Z mobilnimi ključi lahko v realnem času omogočimo dostop tistemu, ki je najbližje lokaciji. Ni potrebe po fizični predaji ključev, ni izgube časa. To je v določenih situacijah lahko odločilno.

Hkrati imaš ves čas pregled nad tem, kaj se dogaja – kdo je vstopil, kdaj in koliko časa se je zadrževal. To ni samo varnostni vidik, temveč tudi operativni – lažje se odločaš, ker imaš konkretne podatke.

Osebno se mi zdi pomembno tudi to, da s tem zmanjšujemo kompleksnost. Manj logistike, manj fizičnih ključev, manj možnosti za napake. V kriznih situacijah je ravno to tisto, kar organizacije potrebujejo – enostavne in zanesljive rešitve.

Kakšno vlogo vidite za podjetja, kot je ID Shop, pri krepitvi širše družbene odpornosti – kje lahko zasebni sektor najbolj prispeva k varnosti in stabilnosti kritične infrastrukture?

Našo vlogo vidim predvsem v tem, da organizacijam pomagamo razumeti njihova dejanska tveganja. Tehnologija sama po sebi danes ni več omejujoč dejavnik – ključna je pravilna zasnova sistema.

Zelo pomemben del našega dela je tudi izobraževanje strank. V poplavi informacij, regulative in različnih rešitev pogosto opažamo, da prave informacije težko dosežejo prave odločevalce. Zato smo veliko prisotni na terenu, kjer obstoječim in novim strankam predstavljamo novosti, razlagamo, katere probleme posamezne rešitve dejansko rešujejo, ter jih povezujemo z njihovimi konkretnimi izzivi.

V podjetju ID Shop se ne vidimo zgolj kot dobavitelj, temveč kot dolgoročni partner. Velik poudarek namenjamo svetovanju – od postavitve ustreznega sistema do integracije mehanske in elektronske varnosti ter priprave na regulatorne zahteve, kot jih prinaša NIS2.

Menim, da lahko zasebni sektor največ prispeva prav s prenosom znanja in dobrih praks. Delo v različnih industrijah nam omogoča vpogled v učinkovite rešitve, in če to znanje uspešno prenesemo naprej, lahko pomembno prispevamo k dvigu splošne ravni varnosti.

Zaključno sporočilo

Če bi moral izpostaviti eno stvar, bi rekel: začnite pri osnovah. Urejen sistem mehanskega zaklepanja je temelj – brez tega tudi najbolj napredne rešitve ne bodo delovale, kot bi morale.

Druga stvar pa je razumevanje, da kontrola dostopa ni sama sebi namen. Ni namenjena samo vstopni točki za beleženje delovnega časa, temveč predvsem preprečevanju incidentov.

Velikokrat se z varnostjo začnemo ukvarjati šele, ko gre nekaj narobe. Moja izkušnja pa je, da so stroški preventive vedno nižji kot stroški posledic. Če imaš sistem postavljen pravilno, lahko marsikaj preprečiš – če pa se incident vseeno zgodi, ga vsaj bistveno hitreje razrešiš, ker imaš podatke in nadzor. ■

Foto: arhiv ID Shop d.o.o.

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

INTERVJU
mag. Igor Hostnik, izvršni direktor, skupina ACTUAL I.T.

ACTUAL I.T. POMEMBEN DELEŽNIK KIBERNETSKEGA EKO SISTEMA

Kibernetska varnost postaja temelj digitalne stabilnosti in odpornosti organizacij. Actual I.T. se kot pomemben deležnik aktivno vključuje v razvoj celovitega kibernetskega ekosistema in naprednih varnostnih rešitev. O vlogi podjetja in ključnih izzivih na tem področju smo se pogovarjali z izvršnim direktorjem Igorjem Hostnikom.

Kako v skupini ACTUAL I.T. naslavljate vse večje zahteve po kibernetski varnosti in odpornosti v okolju, kjer se grožnje hitro razvijajo in postajajo vse bolj kompleksne?

V skupini smo navajeni hitrih sprememb v okoljih, v katerih delujemo. Zavedamo se, da naše rešitve za trg, kot tudi interne, predstavljajo osnovo, na kateri z ostalimi ukrepi zagotavljamo odpornost. Ti ukrepi so tako organizacijske narave kot predvsem znanje in veščine ljudi, ki uporabljamo tehnologijo. Vse večje zahteve po varnosti zahtevajo stalne aktivnosti v načinu uporabe kot tudi stalno preverjanje sistemov in obnašanja uporabnikov. Naša vizija optimalnega poslovanja nas sili k stalnemu spremljanju zakonodaje, priporočil in iskanju takšnih rešitev, kjer sodelujejo tako izkušeni strokovnjaki, kot mlajši specialisti, ki imajo še bolj odprt pogled na izzive sedanjega časa.

Imate bogate izkušnje iz različnih sektorjev kritične infrastrukture – katere ključne skupne ranljivosti opažate in kje se sektorji med seboj najbolj razlikujejo?

Izkušnje različnih sektorjev, v katerih delujemo, so zagotovo naša prednost. To nam priznavajo stranke, ki sodelujejo z več partnerji, in tudi naši strokovnjaki, ki imajo možnost primerjanja delovanja določenih rešitev v različnih okoljih. Velik izziv so obstoječi sistemi oz. tehnologije, kjer ni več aktivne podpore proizvajalcev, so pa implementirane v tistih delih poslovanja, ki so ključni za osnovno delovanje. Prav tako je izziv ločevanja in hkrati povezovanja različnih okolij, kot npr. IT in industrijskih ali OT okolij. Zavedamo se, da je vsaka implementirana rešitev odraz časa in na nek način časovna kapsula in ne moremo pričakovati, da bo enako učinkovita ob novonastalih razmerah. Zato je treba stalno prilagajati poslovne potrebe in potrebe po informatizaciji na način, da ostanejo storitve dovolj varne ter omogočajo večjo dodano vrednost. Pri tem opažamo naslednji izziv, in to je kontrola dostopa oz. upravljanje identitet, saj s kompleksnostjo uporabe dostopa vse več različnih uporabnikov, ki so lahko sistemski ali človeški. S tem smo pri naslednjem izzivu, ki je človeški, saj imamo različno usposobljenost za uporabo sodobnih rešitev, ki so tako v IT kot OT okoljih. Pri tem hitro pridemo do odvisnosti od ključnih posameznikov, ki je naslednji izziv. Tudi nezadostno upravljanje dobavne verige je velik izziv, saj kompleksne rešitve zahtevajo upravljanje različnih vzdrževalcev, integratorjev, proizvajalcev in vsebinskih nosilcev. Največji izziv pa vidimo v pomanjkanju znanja in virov zaznavanja ter odzivanja na dogodke, kar je povezano z regulativo in dokumentacijo.

Sektorji se najbolj razlikujejo po vzpostavljenem internem sistemu kakovosti, katerega del je obvladovanje tveganj, saj so posamezni sektorji podvrženi različnim regulativam ne glede na to, da vsi sodijo v sklop kritične infrastrukture.

Kako vaše rešitve konkretno prispevajo k večji odpornosti organizacij – ne le na ravni zaščite, temveč tudi pri zagotavljanju neprekinjenega delovanja in hitrega okrevanja po incidentih?

Vedno skušamo delovati preventivno, saj je najboljša zaščita preventiva. Ne le z usposabljanji in iskanjem tveganj, temveč z ocenjevanjem groženj ter izpostavljenosti naročnikov. Trenutno se naše storitve naprednega iskanja kibernetskih groženj (angl. *CTI - Cyber Threat Intelligence*) izkazujejo kot najbolj učinkovita preventiva, saj s temi storitvami navadno preprečimo morebiten izpad in zagotavljamo neprekinjenost poslovanja. Potrebno pa je zavedanje, da ni ene same rešitve, ki zagotavlja neprekinjenost delovanja, temveč skupek rešitev. Podobno kot pri odpornosti zdravja ljudi, je potrebna kombinacija aktivnosti, ki zmanjša vpliv nepredvidenih izpadov.

V primerih incidentov pa so potrebne druge aktivnosti, ki morajo privesti organizacije do ponovne vzpostavitve delovanja osnovne dejavnosti, kjer pa sodeluje več dejavnikov. Z našimi storitvami, ki jih lahko štejemo v skupino nudenja celovitega zagotavljanja varnostnih storitev (angl. *SOC – Security Operation Center*), najprej omejimo škodo, zavarujemo dokaze in po vnaprej dogovorjenih korakih vzpostavimo ponovno delovanje. Pri tem je ključno sodelovanje z naročnikom, ostalimi partnerji naročnika, državnimi organi in dobro vnaprejšnje načrtovanje korakov ob takšnih incidentih.

Kako spoznanja in izkušnje iz EU projektov prenašate v razvoj svojih rešitev in kako se to odraža v konkretni dodani vrednosti za vaše stranke?

Neposredno delujemo v regiji od Črnega morja do Malte. Projektno tudi globalno. Zagotovo je domači trg tisti, ki je najbolj zahteven in nam omogoča mednarodno delovanje. EU projekti in projekti izven EU prinašajo izkušnje delovanja v okoljih, ki imajo druge poslovne cilje, saj gre praviloma za projekte, kjer je udeleženih več partnerjev iz različnih držav. Ravno projektno delo je tisto, ki pokaže moč posamezne rešitve in s tem, kako dobro je rešitev načrtovana ter izpeljana. Neposredna dodana vrednost za naše stranke je porazdelitev razvoja na več strank in izkušnje delovanja implementirane rešitve. Smo namreč skupina, ki rešitve tudi razvija in zato imamo na ta način v upravljanju celoten razvojni ter življenjski cikel rešitve.

Kako pomembno vlogo imajo integrirane in celostne rešitve (npr. povezovanje IT, OT in varnostnih sistemov) pri gradnji odpornosti organizacij v praksi?

Celostne rešitve imajo čedalje pomembnejšo vlogo, saj je povezovanje sistemov danes nujno. Ni nujno, da isti izvajalec obvladuje tako IT kot OT del. Pomembno pa je dobro sodelovanje med partnerji, učinkovito projektno vodenje in upravljanje rešitve. Samostojne, samozadostne rešitve, ki obljubljajo preveč ambiciozne rezultate navadno niso prilagodljive in jih težje vključimo v integrirani sistem. S tem lahko ogrozimo odpornost organizacij ne glede na robustnost posamezne rešitve. Zato v več primerih izvajamo bodisi svetovanje pred izvedbo projektov ali le vodenje izvedbenih projektov. Torej nismo vedno le izvajalec projekta, temveč že v pripravljalni fazi zaupanja vreden partner. Prav tako nastopamo kot IT revizor izvedenih projektov, kjer izvajamo različne preglede za oceno tveganj po izvedbi.

Kateri projekti ali implementacije iz zadnjega obdobja najbolje ponazarjajo vaš prispevek h krepitvi kibernetske varnosti in odpornosti v kritičnih sektorjih?

Zadnje čase uspešno implementiramo rešitve zagotavljanja odpornosti, ki so ponujene po poslovnem modelu storitev. S tem naročniki pridejo hitreje do rešitev, ki manj bremenijo njihovo poslovanje, so pa nujne pri zagotavljanju odpornosti. Še posebej uspešni smo pri nudenju kombiniranih storitev iz področja infrastrukture in varnosti, kjer strankam implementiramo tiste, ki so jih v danih razmerah sposobne upravljati same ali pa tudi upravljanje vsaj deloma prepuščajo našim strokovnjakom. Ena takšnih storitev, ki je prispevala največji delež h krepitvi kibernetske varnosti, je iskanje kibernetskih groženj na način, kot ga vidijo »napadalci«, in ne kot ga vidijo upravljalci sistemov. ■

Foto: arhiv skupina ACTUAL I.T.

Vsak IT izziv ima rešitev.
Tudi vaš.

ACTUAL I.T.
A DBA Group Company

ACTUAL PRO
A DBA Group Company

www.actual-it.si

ZARJA ELEKTRONIKA

Z NAMI VARNI IN POLNI ZAUPANJA ŽE VEČ KOT 64 LET.

Zarja Elektronika je vodilni ponudnik tehničnega varovanja v Sloveniji in širši balkanski regiji. Pri najzahtevnejših projektih zagotavljamo celovito podporo od prve ideje in implementacije varnostnih rešitev do dolgoročnega vzdrževanja industrijskih, poslovnih ter zasebnih objektov. Poleg lastnih inovacij po najvišjih standardih zastopamo vrhunske svetovne proizvajalce sistemov za javljanje požara, protivlomno varovanje, video nadzor, detekcijo iskre in kontrolo pristopa.

VRHUNSKA KAKOVOST IN INOVACIJE

Lasten razvoj in proizvodnja zagotavljata popoln nadzor nad kakovostjo ter visoko prilagodljivost pri razvoju tehnološko najnaprednejših sistemov.

ENOSTAVNO UPRAVLJANJE

S centralnimi nadzornimi sistemi (CNS) omogočamo pregleden nadzor in varno upravljanje vseh varnostnih parametrov objekta.

24/7 PODPORA IN VZDRŽEVANJE

Regionalna servisna mreža zagotavlja hitro odzivnost, zakonsko skladnost in redno vzdrževanje, kar podaljšuje življenjsko dobo vaše opreme.

CELOVITA PONUDBA NA ENEM MESTU

Združujemo lastne inovacije z zastopstvi vrhunskih svetovnih proizvajalcev za sisteme javljanja požara, gašenja, video nadzora in protivlomnega varovanja.

REŠITVE PO MERI

Specializirani smo za kompleksne industrijske objekte in kritično infrastrukturo, kjer zagotavljamo modularne sisteme, prilagojene vašemu okolju.

ZAUPAJTE VARNOST SVOJEGA OBJEKTA STROKOVNJAKOM Z IZKUŠNJAMI.

www.zarja.com

info@zarja.com

01 831 74 52

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

INTERVJU
g. Thomas Tomsich, direktor, Zarja Elektronika d.o.o.*

ZARJA ELEKTRONIKA Z INOVACIJAMI NA PODROČJU POŽARNE VARNOSTI

Požarna varnost ostaja eden ključnih stebrov zaščite ljudi, premoženja in infrastrukture v sodobnem okolju. Zarja Elektronika z inovativnimi rešitvami pomembno prispeva k razvoju naprednih sistemov za zgodnje odkrivanje in obvladovanje požarnih tveganj. O vlogi inovacij in prihodnjih usmeritvah smo se pogovarjali z direktorjem Thomasom Tomsichom.

Požarna varnost ostaja eden ključnih stebrov celovite odpornosti organizacij – kako v Zarja Elektronika z inovacijami na področju požarnih sistemov naslavljate nove, vse bolj kompleksne varnostne izzive?

V podjetju vstopamo v eno najbolj vznemirljivih obdobij doslej. Naša filozofija ostaja neomajna: verjamemo v celostno obvladovanje procesov, zato razvoj, proizvodnjo in prodajne poti ohranjamo pod lastno streho. Takšen pristop nam omogoča hitro prilagajanje trgu in zagotavljanje brezkompromisne kakovosti. Vse skupaj kronamo s stalnim razvojem novih produktov, ki združujejo dolgoletne izkušnje z najsodobnejšimi tehnološkimi trendi. Nenehno optimiziramo vse procese, od proizvodnje do digitalnih orodij v prodaji in servisu. Ob tem se zavedamo, da tehnologija brez strokovne ekipe ne pomeni nič, zato vlagamo v znanje zaposlenih, ki so srce naših inovacij. Ostajamo zvesti domačemu okolju, a z novimi rešitvami samozavestno stopamo ob bok svetovni konkurenci.

Prisotni ste v številnih ključnih sistemih in sektorjih – katere glavne izkušnje ste pridobili pri zagotavljanju požarne varnosti v okoljih kritične infrastrukture?

Naše izkušnje v sektorju kritične infrastrukture temeljijo na tehnično najzahtevnejših projektih v Sloveniji. Zagotavljanje požarne varnosti v objektih, kot so jedrski objekti, rudniki, termoelektrarne, skladišča vnetljivih snovi in bolnišnice, zahteva stopnjo odgovornosti ter specifičnega znanja, ki presega standardne strokovne okvire. Ker verjamemo v koncept celovite skrbi, sistemov v kritični infrastrukturi ne le načrtujemo in opremljamo, temveč jih tudi aktivno vzdržujemo. Lastni razvoj opreme nam omogoča unikaten vpogled v njeno delovanje skozi celotno življenjsko dobo, kar zagotavlja 100-odstotno pripravljenost tudi v najbolj ekstremnih pogojih. Standarde zanesljivosti iz okolij z najvišjimi tveganji dosledno prenašamo v vse naše procese. Ker obvladujemo celotno verigo – od lastnega razvoja do proizvodnje – zagotavljamo prilagojen inženiring in rešitve po meri najzahtevnejših naročnikov.

Katere tehnološke in razvojne inovacije na področju požarne varnosti v zadnjem obdobju najbolj izstopajo ter kako prispevajo k večji odpornosti organizacij?

V zadnjem obdobju na področju požarne varnosti izstopa predvsem prehod od klasičnih sistemov k inteligentnim, povezanim in napovednim rešitvam. Napredna analitika omogoča precej zgodnejše in zanesljivejše odkrivanje požarov, saj sistemi ne temeljijo več zgolj na zaznavi dima ali temperature, temveč razumejo širši kontekst dogajanja v prostoru. Ključno postaja prepoznavanje tveganj še pred nastankom požara, na primer pregrevanja opreme ali nenavadnih odstopanj v delovanju, tudi v zahtevnih tehnoloških procesih in postrojenjih. Razvoj tehnologij omogoča povezovanje posameznih elementov požarne varnosti v pametne sisteme, ki zagotavljajo nadzor v realnem času in integracijo z drugimi sistemi tehnične varnosti ter industrijskih procesov.

Napredne rešitve omogočajo tudi učinkovit nadzor težko dostopnih ali nevarnih območij in povečujejo varnost interven-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

cijskih ekip. Razvoj dopolnjujejo nove metode gašenja in napredni materiali, ki omogočajo bolj ciljno ter učinkovito posredovanje ob zmanjševanju škode. Skupni učinek teh pristopov je precej večja odpornost organizacij, saj omogočajo zgodnejše zaznavanje, hitrejši odziv, boljše upravljanje tveganj in prehod iz reaktivnega v proaktivno oziroma preventivno delovanje.

Kako lahko s svojim znanjem, izkušnjami in rešitvami v Zarja Elektronika konkretno prispevate k dvigu ravni požarne varnosti v organizacijah ter širši družbi?

V podjetju Zarja Elektronika požarno varnost razumemo kot celovito disciplino, h kateri prispevamo s povezovanjem naprednih tehnoloških rešitev, strateškega svetovanja in družbene odgovornosti. Naše sodelovanje z naročniki presega zgolj implementacijo sistemov, saj v proces integriramo kontinuirano izobraževanje in optimizacijo varnostnih protokolov, kar zagotavlja visoko stopnjo varnosti objektov. Svojo vlogo strokovne avtoritete udejanjamo s prenosom znanja na vseh ravneh. Aktivno sodelujemo pri izdelavi strokovnih podlag in literature, npr. pri pripravi učbenika za nacionalno poklicno kvalifikacijo varnostnikov, ter izvajamo specializirana usposabljanja za poklicne gasilske enote. Z vključevanjem v pedagoški proces kot gostujoči predavatelji na univerzah in z nudenjem štipendij ter praktičnega mentorstva v lastnem izobraževalnem centru sistemsko pripravljamo nove generacije strokovnjakov. S takšnim holističnim pristopom ne le dvigujemo standarde poslovanja, temveč aktivno soustvarjamo varno in odporno družbeno okolje.

Kakšne so vaše strateške usmeritve in aktivnosti v širšem regijskem prostoru ter kakšna so vaša pričakovanja za prihodnost, glede na to, da postaja varnostno okolje vse bolj zahtevno, tveganja pa vse bolj kompleksna?

Naša strategija temelji na utrjevanju vodilnega položaja v Sloveniji in načrtni rasti tržnega deleža v regiji Adria, hkrati pa se intenzivno pripravljamo na prodor z lastnimi produkti na ostale evropske trge. Pri tem se opiramo na več desetletij tesnega sodelovanja z vodilnimi svetovnimi znamkami na področju požarne zaščite, s katerimi nenehno izmenjujemo znanje, s ključnimi partnerji pa smo skupaj stopili tudi v razvoj novega produkta. Glede na aktualne svetovne razmere varnost kot temeljna pravica pridobiva vse večjo pozornost, zaradi česar bo naša dejavnost v prihodnje pridobila še večji pomen in težo. Pri vsem tem nam je ključno zaupanje uporabnikov, saj jim z našimi rešitvami zagotavljamo občutek varnosti in tisti dragocen notranji mir, ki je v današnjem času neprecenljiv.

Bi še kaj posebnega sporočili bralcem revije?

Varnostne politike v organizacijah ne bi smele temeljiti zgolj na doseganju minimalnih zakonsko zahtevanih standardov. Ti namreč predstavljajo le nujno izhodišče, ne pa tudi zadostne zaščite v nepredvidljivih in kompleksnih okoljih. Požarna varnost je temeljni steber varovanja človeških življenj, kjer so posledice podcenjevanja tveganj lahko nepopravljive. Tragični dogodki, kot so požar v stolpnici Grenfell Tower v Londonu, katastrofa v švicarskem klubu Le Constellation ali požar v nočnem klubu Pulse v Kočanih, služijo kot kritičen opomin, da sistemske pomanjkljivosti in zanašanje na najnižje tehnične pragove vodijo v smrtonosne tragedije. Ključno je razumevanje, da požarna varnost ni zgolj strošek, temveč strateška naložba v varno prihodnost. ■

Foto: arhiv Zarja Elektronika d.o.o.

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

INTERVJU
g. Matej Matija Grobelšek, direktor za poslovni trg, A1 Slovenija d. d.*

ALI PODJETJA DOHAJAJO NOVO REALNOST KIBERNETSKIH GROŽENJ?

Kibernetske grožnje se razvijajo hitreje kot kadarkoli prej, podjetja pa se soočajo z vse večjim pritiskom po zagotavljanju digitalne odpornosti. A1 Slovenija d. d. kot pomemben ponudnik naprednih digitalnih rešitev aktivno podpira organizacije pri soočanju z novimi tveganji. O tem, ali podjetja dohajajo novo realnost kibernetskih groženj, smo se pogovarjali z direktorjem za poslovni trg Matejem Matijo Grobelškom.

Kibernetski napadi se doma in po svetu stopnjujejo. Kako varna so slovenska podjetja v primerjavi z drugimi v EU?

Resnična odpornost se pokaže šele ob napadu – ne v skladnosti, temveč v hitrosti odziva.

Slovenska podjetja v povprečju niso bolj izpostavljena napadom kot podjetja drugod po Evropi, razlike pa se pokažejo pri pripravljenosti in odzivnosti. Večja podjetja imajo sicer pogosto vzpostavljene osnovne varnostne mehanizme, vendar obstaja opazen razkorak med formalno skladnostjo in dejansko odpornostjo v praksi. Pri malih in srednje velikih podjetjih so pomanjkljivosti še izrazitejše – predvsem pri zaznavanju incidentov, upravljanju dostopov ter kriznem odzivanju.

Resnična odpornost se pokaže šele ob napadu: kako hitro ga zaznamo, kako jasno odločamo in kako učinkovito omejimo škodo. Prav na teh področjih podjetja pogosto zaostajajo, ne zaradi pomanjkanja tehnologije, temveč zaradi nesistematičnega pristopa k upravljanju tveganj. Zato priporočamo redne celovite varnostne preglede – vsaj enkrat letno oziroma na dve leti za manjša podjetja.

Ljudje ostajajo najšibkejši člen. Kako umetna inteligenca danes napadalcem omogoča še učinkovitejše napade?

Z uporabo umetne inteligence se je uspešnost phishing napadov povečala tudi za desetkrat ali več. Napadalci lahko hitro pripravijo jezikovno dovršena sporočila brez očitnih napak, kar poveča verjetnost, da jim uporabniki nasedejo. Poleg tega UI omogoča množično personalizacijo – sporočila so lahko prilagojena posamezniku, tudi v slovenščini, kar jih naredi še bolj prepričljiva.

Pomemben vidik je tudi avtomatizacija: od zbiranja podatkov do pošiljanja napadov. To napadalcem omogoča izvajanje obsežnih kampanj na več trgih hkrati. V takšnem okolju sta ozaveščenost zaposlenih in ustrezna tehnična zaščita ključna stebra varnosti.

Katere nove vrste napadov trenutno najbolj izstopajo?

Napadi se nenehno razvijajo, njihove »življenjske dobe« pa so vse krajše. Trenutno so v ospredju napadi na oblačna okolja, ki postajajo osrednji del poslovanja podjetij. Ta okolja zahtevajo drugačne pristope k zaščiti, saj tradicionalni načini obrambe pogosto niso več zadostni. Tipičen primer so platforme, kot je M365, kjer lahko nepravilne nastavitve ali slabo upravljanje dostopov predstavljajo veliko tveganje.

Predvidevamo pa lahko, da bo v bližnji prihodnosti zaradi povečane uporabe izboljšanih orodij UI lahko tudi več t. i. »zero-day« napadov, saj bodo napadalci s temi orodji pospešeno iskali luknje v programski opremi, ki jo uporabljamo.

Kako lahko telekomunikacijski operaterji prispevajo k večji varnosti podjetij?

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Operaterji imajo pomembno vlogo, saj predstavljajo vstopno točko v digitalni svet. Določene zaščitne mehanizme lahko zagotovimo že na ravni omrežja. Tako imajo na primer pri A1 podjetja že v osnovnih paketih vključeno zaščito pred DDoS napadi in dostopom do zlonamernih spletnih strani.

Za celovitejšo zaščito pa so ključni dodatni ukrepi, kot so redni varnostni pregledi in storitve varnostno operativnega centra (SOC). Prednost takšnih centrov je kombinacija naprednih orodij in dostopa do širšega nabora znanja ter informacij, tudi na mednarodni ravni.

Kakšen je pomen varnostno operativnih centrov danes?

Danes si učinkovite kibernetske zaščite brez SOC-a praktično ne moremo več predstavljati. Podjetje potrebuje vsaj tri stvari: urejeno in varno IT-okolje, tehnologijo za zaznavanje napadov ter jasno definirane procese odzivanja. Prav slednje je najtežje vzpostaviti brez specializirane podpore. SOC omogoča stalni nadzor, hitro zaznavo anomalij in ustrezno ukrepanje, kar bistveno zmanjša posledice napadov.

Kako blizu smo točki, ko bo umetna inteligenca sama zaznala in zaustavila napad?

Na nekaterih področjih smo že zelo blizu. Sodobna orodja lahko analizirajo ogromne količine podatkov in skoraj v realnem času zaznajo anomalije. To je danes standard.

Težava pa nastane pri interpretaciji – napadi niso vedno enoznačni. Sistem lahko zazna nenavadno dejavnost, ne more pa vedno zanesljivo presoditi, ali gre za napad ali legitimno dejanje. Za to je potrebno razumevanje konteksta poslovanja, kar ostaja domena izkušenih strokovnjakov.

V prihodnje pričakujemo razvoj naprednejših UI agentov, ki bodo bolje razumeli okolje in omogočali še hitrejše ter natančnejše odločitve.

Ali lahko umetna inteligenca napade tudi predvideva?

UI sistemi analizirajo vzorce vedenja in odstopanja v prometu ter tako zaznajo potencialne grožnje, ki bi jih človek težko opazil.

Vendar pa ima obrambna uporaba UI dodatne omejitve, predvsem zaradi varovanja občutljivih podatkov. Zato se razvijajo zaprta okolja, kjer je mogoče varno obdelovati podatke in izboljševati zaščito. Kljub temu ostajajo ključni strokovnjaki, ki razumejo poslovni kontekst in znajo pravilno interpretirati dogodke.

Katere tehnologije bodo zaznamovale prihodnost kibernetske varnosti?

Na strani napadalcev bodo ključne tehnologije za avtomatizacijo in optimizacijo napadov – torej orodja, ki omogočajo hitrejše, bolj ciljno usmerjene ter učinkovite napade.

Na strani obrambe pa pričakujemo razvoj naprednih sistemov za zaznavanje in odzivanje ter večjo integracijo umetne inteligence v varnostne procese. Pomembno je tudi, da so trenutno najzmogljivejši UI sistemi še relativno nadzorovani, saj zlonamerna uporaba pogosto naleti na omejitve. A to se lahko hitro spremeni.

Kako ocenjujete pripravljenost slovenskih podjetij v širšem evropskem kontekstu?

Tehnološko slovenska podjetja večinoma ne zaostajajo, težava pa je v zrelosti varnostnih praks. Manj je uporabe večfaktorske avtentikacije, manj stalnega nadzora in manj sistematičnega izobraževanja zaposlenih.

Razlike se pokažejo predvsem ob incidentih – naprednejša podjetja imajo vzpostavljene in preizkušene procese odzivanja, kar bistveno zmanjša škodo ter čas motenj poslovanja.

Kako gledate na regulativo, kot je direktiva NIS2?

NIS2 prinaša pomembne izboljšave in spodbuja uvedbo dobrih praks, ki so že del standardov, kot sta ISO 27001 ter ISO 22301. Vendar sama skladnost še ne pomeni dejanske odpornosti.

Pogosta napaka je, da podjetja dosežejo skladnost zgolj formalno, brez resničnega uvajanja sprememb v praksi. Varnostne vrzeli se najbolje odkrijejo s poglobljenimi pregledi – in teh je na trgu še vedno veliko.

Kaj je minimalni standard, ki ga mora podjetje doseči za osnovno zaščito?

Minimalni standard vključuje tri ključne elemente: varno in urejeno IT-okolje, učinkovita orodja za zaznavanje napadov ter jasno definirane procese odzivanja.

V praksi vse to najlažje zagotavlja dobro vzpostavljen varnostno operativni center, ki povezuje tehnologijo, procese in strokovno znanje. ■

Foto: arhiv A1 Slovenija d. d.

A1 Business

Zanesljiv partner pri gradnji kibernetske odpornosti

“Kibernetska varnost zahteva več kot zgolj izpolnjevanje predpisov. Skladnost je le izhodišče – cilj je odpornost. Podjetja moramo preiti iz reaktivnega v proaktivni pristop ter graditi kulturo, procese in zmogljivosti, ki nas varujejo pred sodobnimi grožnjami.

V Skupini A1 več kot 400 varnostnih inženirjev združuje znanje in izkušnje ter nam omogoča vpogled v najnovejše trende in učinkovite obrambne pristope.

Prek A1 Varnostno operativnega centra vsak dan spremljamo IT-okolja številnih slovenskih podjetij, kar nam daje neposreden stik z realnimi incidenti – zlasti pri malih in srednje velikih podjetjih.

Zato lahko podjetjem pomagamo ne le pri izpolnjevanju regulative, temveč predvsem pri gradnji prave kibernetske odpornosti.«

Dejan Turk,
predsednik uprave A1 Slovenija in A1 Hrvaška

Več

A1 Slovenija, d. d., Ameriška ulica 4, SI-1000 Ljubljana

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 31.05.2026 prejmite enkratno ekskluzivno ugodnost pri vseh storitvah REISSWOLF!

Pokličite nas na: **01 541 22 66**

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

simply. done.

VARNA POVEZAVA MED ALARMNIM SISTEMOM IN VNC-JEM

- **Komunikacijski vmesnik se ne programira pri naročniku**
- **Razširljiva in fleksibilna infrastruktura**
- **Kompatibilnost za vse proti-vlomne in proti-požarne naprave**
- **Centralni nadzor in programiranje**
- **Enostavna montaža** (samo 4 žice)
- **Komunikacijska pot kot storitev**
- **Varno in zanesljivo**
- **EN50136 in EN54**

HSI hsi.si

ealarm.io info@ealarm.io 07 600 19 60

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 | CHFI CERTIFIED | CPENT CERTIFIED | CEH MASTER CERTIFIED | ECIH CERTIFIED | 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


ELES
GRADIMO
ENERGETIKO PRIHODNOSTI
Elektroenergetika je na pragu tektonskih podnebnih in družbenih sprememb. Naša skupna odgovornost je, da se nanje prilagodimo in si hkrati prizadevamo za ogljično nevtralnost. Pred nami je novo, drugačno obdobje prenosa in distribucije električne energije.
ELES je in bo ostal hrbtenica zelenega prehoda v Sloveniji. Z zanesljivo, varno in trajnostno oskrbo z električno energijo skrbi za to, da bo elektroenergetska infrastruktura bolj prilagojena potrebam jutrišnjega dne. Predvsem pa bo še naprej oral ledino pri postavljanju novih standardov družbenega napredka. ELES bo Slovenijo popeljal v boljšo, zeleno prihodnost.
www.eles.si