Korporativna varnost

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

Letnik 2024, oktober • št. 36

Slovensko združenje korporativne varnosti vključujoča platforma sodelovanja javno-zasebnega partnerstva

Tradicionalna 16. mednarodna konferenca Dnevi korporativne varnosti Brdo pri Kranju, 19.-20. maj 2025

VAŠA 360° VARNOST 365 DNI V LETU

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

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

CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

TelekomSlovenije
Vedno na boljše.

Telekom Slovenije, d.d., Ljubljana.

Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
tiskano v Sloveniji

Datum izida:
oktober 2024

Izvod revije je brezplačen

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

ISSN 2232-6170

Čeprav sta v mednarodnem okolju še vedno pomembno izpostavljeni varnostni krizi v Ukrajini in na Bližnjem Vzhodu, ki imata tudi posredne varnostne vplive na Evropo in s tem posledično tudi Slovenijo, se korporativno varnostno okolje sooča z drugimi varnostnimi izzivi. Vsekakor so ti pomembni izzivi povezani s kibernetskim okoljem, z negativnim vplivom na naravno okolje zaradi ekstremnih dogodkov, ki so postali stalnica in na koncu seveda izzivi, ki jih prinaša človeški faktor, kot vedno večji agregator varnostnih težav v organizacijah. Poleg stalnega iskanja ustreznega razmerja med nivojem varnostnega zavedanja in potrebe po ustrezni operativnosti delovanja, največji izziv verjetno predstavljajo omejene zmogljivosti absorpcije naglih tehnoloških sprememb v človeško dojemanje realnih tveganj, ki jih prinašajo nove tehnologije. To so neposredni izzivi, na katere je, poleg seveda vseh ostalih, potrebno najti ustrezne odgovore in ukrepe za njihovo ublažitev. Pred nami se nahaja obdobje, ko bo potrebno v operativno korporativno varnostno okolje naših organizacij integrirati zahteve in pričakovanja ključnih EU direktiv na pomembnih področjih kritične infrastrukture, kibernetske varnosti, uporabe umetne inteligence in na še nekaj ostalih pomembnih področjih. V upanju, da bodo potrebni koraki in napori, ki jih bomo izvajali skozi organizacijska okolja, prinesli tudi napredek v smeri odpornejših in prožnejših organizacij, katere bodo zagotavljale neprekinjeno delovanje in odzive na ponavljajoča krizna stanja. Seveda pa se pomanjkanju ustreznega izobraženega kadrovskega potenciala na področju korporativne varnosti nikakor ne moremo izogniti. To postaja vedno bolj izpostavljena težava, saj smo v operativnem okolju korporativne varnosti priča pogostim menjavam, ki se na teh funkcijah dogajajo ob menjavi strateškega vodstva v organizacijah. To poleg izraženih izzivov varnostnega okolja, na drugi strani organizacije pušča v nezavidljivem položaju za ustrezno sistemsko načrtovanje in izvajanje potrebnih ukrepov.

Pred nami je mesec oktober, ki je tradicionalno posvečen dvema pomembnima področjema in tematikama, kot sta kibernetska varnost in požarna varnost. Obema temama tudi v tokratni številki revije posvečamo pomembno pozornost. Poleg teh dveh težišč v reviji, ponovno skozi izbrane intervjuje, ponujamo možnost slišati tako strateški nivo odločevalcev, kakor tudi strokovnjake, kateri neposredno izvajajo aktivnosti v okviru svojih operativnih okolij. Poseben pomen posvečamo zaključnim korakom vzpostavljanja varnostno operativnega centra celotnega sektorja energetike, odpiramo pa tudi teme, kot so požarna tveganja, ki jih prinaša povečana uporaba sončnih elektrarn. Poleg navedenega smo želeli v tokratni številki revije vsebinsko osvetliti tudi dovolj širok spekter ostalih strokovnih vsebin, ki bodo strokovni javnosti v pomoč pri iskanju potrebnih rešitev in strateške modrosti za ustrezno upravljanje varnostnih tveganj, s katerimi smo dnevno soočeni. V uredništvu revije upamo, da bo tudi 36. številka revije v skladu z vašimi visokimi pričakovanji. Za vas se bomo skupaj trudili tudi v bodoče.

izr. prof. dr. Denis Čaleta
Glavni urednik

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

INTERVJU
dr. Jelena Virant Burnik, informacijska pooblaščenka*

PRIHODNJA TEŽIŠČA PRI VAROVANJU OSEBNIH PODATKOV

Dinamično družbeno okolje in uvajanje novih tehnologij postavlja proces varovanja osebnih podatkov pred nenehne izzive tehtanja dopustnosti posegov v le te. O prihodnjih težiščih dela institucije Informacijskega pooblaščenca smo se pogovarjali z novo informacijsko pooblaščenko dr. Jeleno Virant Burnik.

Najprej nam dovolite, da vam iskreno čestitamo ob nastopu te izredno zahtevne funkcije Informacijske pooblaščenke Republike Slovenije. Kateri so bili tisti vzgibi, motivi in predvsem cilji, ki so vas vodili, da ste se odločili za kandidaturo na to izredno zahtevno funkcijo?

Hvala za čestitke in lepe besede. Na IP in področju varstva osebnih podatkov delujem že več kot 15 let. Praktično celotno kariero se strokovno ukvarjam predvsem z izzivi, ki jih prinašajo digitalizacija, spletne storitve, tehnološki velikani, danes tudi umetna inteligenca, še posebej z vidika posegov v zasebnost. Zelo veliko sem se v teh letih ukvarjala tudi s pristopi ustrezne regulacije, ki ne duši inovativnosti, pa vendar ohranja visoko raven varstva naših temeljnih pravic.

Obdobje naslednjega desetletja – oziroma varstva podatkov 3.0, kot ga včasih poimenujem, bo nujno prežeto prav s temi tematikami – preliva nas digitalizacija, umetna inteligenca zelo hitro prehaja v naše procese, se uči na velikih količinah naših podatkov, po drugi strani pa še nimamo enovitega odziva, katere prakse omejiti, kako vse tehnologije uporabljati, da nam bodo v korist in s čim manj negativnih eksternalij za naše temeljne pravice. Iz EU prihaja plejada novih regulacij in aktov, ki bodo regulirali digitalne sfere in bodo morali loviti ravnotežje s Splošno uredbo o varstvu podatkov in ZVOP-2. Za IP kot nadzorni organ bo to obdobje novih izzivov in prilagoditev in verjamem, da bodo moje znanje in izkušnje lahko bistveno pripomogli, da bo IP tudi v naslednjem mandatu organ, ki strokovno in odločno spodbuja transparentnost in varuje osebne podatke ob tesnem sodelovanju s sorodnimi organi v EU.

Poleg tega želim okrepiti preventivno delovanje IP, in kolikor bodo dopuščale razmere in sredstva, nameniti pozornost ozaveščanju javnosti in zavezancev. Tudi na ta način lahko spodbujamo skladnost in prispevamo k temu, da podjetja in organizacije lažje spoštujejo pravila. Posebej bi želela več aktivnosti za ozaveščanje otrok in mladostnikov.

Dosedanji informacijski pooblaščenki sta postavili visoke standarde, tako na področju uveljavitve standardov zaščite osebnih podatkov, kakor tudi dostopa do informacij javnega značaja. Informacijski pooblaščenec je v družbi postal spoštovana institucija, brez katere si težko predstavljamo delovanje mnoštva ključnih družbenih procesov. Prevzemate institucijo v dobri kondiciji, vendar je verjetno še veliko možnosti za nadaljnji razvoj?

Kot sem že večkrat poudarila, z veliko hvaležnosti, sta predhodnici, vsaka v svojem obdobju in na svoj način oblikovali

> Kibernetska varnost je eden od najpomembnejših izzivov modernega varnostnega okolja. Vedno bodo na mizi dileme, kako zagotavljati ustrezno raven varovanja osebnih podatkov v informacijskem okolju.

*Informacijski pooblaščenec RS je korporacijski član Slovenskega združenja korporativne varnosti

velike čevlje, v katere sem stopila in s katerimi bom premagovala nove izzive v prihajajočih letih. IP je nedvomno institucija v dobri kondiciji, strokovno in z vidika ugleda, ki ga uživa v javnosti. Tu gre zahvala tudi odličnim sodelavcem, ki so izjemno strokovni in predani svojemu delu in dan za dnem skrbijo, da se uveljavljajo visoki standardi varovanja osebnih podatkov in dostopa do informacij javnega značaja. Seveda pa pridemo tudi do »ampak«: nove pristojnosti, ki jih bomo izvajali na IP v prihodnje, ko prihajajo vse nove EU regulacije bodo pomenile obremenitve, ki jih IP ne bo zmogel brez kadrovskih okrepitev. To je področje na katerem bo treba zelo aktivno začeti delovati že takoj. Tudi zato, ker že dosedanji porast nadzornih, pritožbenih in drugih postopkov, ki se je zgodil po uveljavitvi Splošne uredbe o varstvu podatkov pomeni, da smo na robu svojih zmogljivosti. Tudi Evropska komisija v svoji zadnji evalvaciji delovanja Splošne uredbe poudarja, kako pomembno je, da imamo nadzorni organi za varstvo podatkov dovoljšna sredstva, da izvajamo nadzor, in da smo generalno gledano organi podhranjeni.

IP bdi nad uresničevanjem dveh pravic – obe pa je treba razumeti tudi kot podstat za uresničevanje naših drugih temeljnih pravic. Pomembno je, da se zavedamo tega, da na IP ne varujemo le osebnih podatkov in razkrivamo informacij javnega značaja, pač pa s tem prispevamo k veliko širši problematiki upoštevanja temeljnih človekovih pravic, ki jih še posebej v digitaliziranem svetu moramo ohraniti, če želimo uživati vse dobre plati digitalizacije, in se izogniti slabim posledicam, diskriminaciji, posegom v svobodo gibanja, v demokratične procese, itd.

ZVOP-2 je v veljavi že dovolj časa, da lahko potegnete bistveno oceno o učinkovitosti in uspešnosti njegove integracije med zavezanci. Kateri so tisti izzivi, ki jih pri uveljavljanju tega zakona še vedno zaznavate skozi delo v vašem organu?

Področje varstva osebnih podatkov se zadnjih 10 let korenito spreminja, poleg tega pa ima zelo izrazito EU komponento, saj primarna regulacija področja prihaja s strani EU. Zakon o varstvu osebnih podatkov (ZVOP-2), je končno uredil manjkajoče podrobnosti za polno izvajanje pooblastil IP glede na Splošno uredbo. Predpisal je način sankcioniranja kršitev po Splošni uredbi. Se pa zaradi tega specifičnega sistema odpirajo nova vprašanja glede izvajanja teh pooblastil. ZVOP-2 je prinesel tudi nove postopkovne določbe, npr. novo urejen položaj posameznika s posebnim položajem, ki v nadzornem IP postopku nastopa kot stranka. Tudi to je novost v slovenskem administrativnem pravu in odpira vprašanja. V naslednjih letih bo zato potrebno aktivno povezovanje IP s prakso drugih sorodnih organov v EU, ki Splošno uredbo izvajajo že več let. Prav tako bomo s Ministrstvom za pravosodje pristopili k oceni delovanja zakona, na podlagi katere bodo, upam, tudi razjasnjene dileme, s katerimi se srečujemo.

Digitalizacija procesov močno vpliva tudi na varovanje osebnih podatkov in ukrepe, ki jih je potrebno zagotavljati v tej povezavi. Tukaj je še kar nekaj dilem in izzivov, ki jih je potrebno ocenjevati v vsakem konkretnem primeru. Menite, da imate s tega naslova kaj več vprašanj in dilem, ki prihajajo s strani različnih organizacijskih okolij?

Ko govorimo o raznih projektih digitalizacije sistemov v naši družbi, ali pa uvajanju novih sofisticiranih analiz in obdelav podatkov kot podporo nekim procesom, da bomo hitrejši, bolj učinkoviti, itd. se je treba zavedati, da lahko posegi v varstvo podatkov na koncu pomenijo zelo neželene posledice, ki zadevajo veliko več kot le zasebnost nekoga – lahko pomenijo diskriminacijo ranljivih, napačne odločitve, tudi vplivajo na demokratične procese, volitve. Na IP izdamo veliko mnenj na razne predloge oziroma projekte, ki uvajajo digitalizacijo na različnih področjih, kjer opozarjamo na te vidike. Želela bi si, da so naše intervencije sprejete konstruktivno, saj lahko upoštevanje izboljša sisteme digitalizacije, da bodo sistemi robustni, manj izpostavljeni tveganjem, da so podatki razkriti, napačno obdelani, da imajo posamezniki s tem težave, in da v rešitve ni zaupanja. Tu ne gre le za varovanje podatkov, pač pa za veliko več. Napake pri obdelavah podatkov v zdravstvu lahko pomenijo tveganje za življenje nekoga, nepremišljena obdelava podatkov z UI lahko pomeni, da nekdo ne bo prejel neke storitve ali sredstev, čeprav je do njih upravičen, dopuščanje obdelav podatkov za druge namene lahko pomenijo, da nas zasledujejo oglasi za dvomljiva zdravila in izkoriščajo naše ranljivosti. Še posebej je to pomembno, ko govorimo o mladostnikih, pa starejših, ki so bolj ranljivi za zlorabe.

V preteklem obdobju so bili sprejeti različni pomembni predpisi na nivoju EU in sicer Akt o upravljanju podatkov, pa Akt o digitalnih storitvah, Akt, ki določa nova pravila glede preglednosti in ciljanega političnega oglaševanja. Ste pri integraciji teh predpisov v nacionalni pravni red nosilna institucija ali podpirate druge organe pri njihovem uveljavljanju? Kateri so ključni izzivi, ki jih vidite na tem področju?

Da ima digitalizacija vsega tudi negativne posledice na družbo jasno kaže sprejem aktov digitalne strategije, ki prihajajo iz EU in nagovarjajo prav te negativne posledice profiliranja, priporočilnih sistemov, kršenja varstva podatkov na spletu, zavajajočih vzorcev, ki jih uporabljajo spletni velikani, vedenjskega oglaševanja, manipulacij. Večina aktov naslavlja digitalno ekonomijo in vsebuje kar nekaj novih omejitev.

Za IP bo zahtevno spoprijemanje z različnimi pravili in njihovim odnosom s Splošno uredbo o varstvu podatkov – nova pravila vendarle v delu urejajo prav obdelave podatkov. Tu lahko pričakujemo še več sodelovanja in usklajevanja v Evropskem odboru za varstvo podatkov, kjer že pripravljamo različne smernice glede Akta o digitalnih storitvah, pa Akta o umetni inteligenci, itd. Za integracijo teh aktov v nacionalni pravni red so odgovorna različna resorna ministrstva, ki pripravljajo predloge pravnih podlag. IP v tem procesu sodeluje s pripravo mnenj in odzivov glede ustreznih pooblastil in pristojnosti, ki se tičejo našega dela. Zelo pomembno je namreč, da se raven varstva, ki je dosežena s Splošno uredbo o varstvu podatkov ne zniža zaradi prepletanj z drugimi EU akti, da pride do čim manj pravnih nejasnosti – kdo je nadzorni organ za katero vrsto aktivnosti v digitalni sferi, kako organi med sabo sodelujejo.

Akt o umetni inteligenci je prvi pravni okvir o umetni inteligenci doslej, ki obravnava tveganja umetne inteligence in Evropi zagotavlja vodilno vlogo na svetovni ravni. Kje so po vašem največja tveganja povezana z umetno inteligenco in varstvom osebnih podatkov?

Akt o umetni inteligenci je vsekakor poseben dosežek EU, saj postavlja nekatere jasne omejitve glede sistemov, ki jih v našem okolju ne želimo, ker predstavljajo prevelik poseg v naše pravice – npr. sistem socialnega scoringa, prepoznave emocij in podobno. Postavlja tudi omejitve za veliko vsakdanjih rab UI, ki jim bomo kmalu priča, npr. v procesu šolstva, zaposlovanja, pri uporabi javnih storitev. Ker UI sistemi obdelujejo osebne podatke nas državljanov in smo s tem podvrženi mnogim tveganjem je prav, da imamo na tem področju jasne omejitve in tudi nadzor.

Z vidika varovanja osebnih podatkov gotovo lahko izpostavim, da so UI sistemi inherentno netransparentni, saj posameznik težko izve oziroma razume logike odločanja znotraj sistemov, mnogo takih sistemov nam je nevidnih, se ne zavedamo, da prihajamo v stik z njimi, težave so z izvajanjem pravic posameznika – vemo, da sistemi tipa Chat GPT halucinirajo, si pogosto »izmislijo« kak podatek. Hkrati pa sistem ne nudi možnosti popravka napačnih informacij. Problematika je široka in minilo bo še nekaj časa, preden bomo UI lahko uporabljali predvidljivo, ob upoštevanju vseh pravic, ki jih imamo uporabniki. Zato se je ob uvajanju UI treba zavedati, sploh, če gre za podatke posameznikov, da že zdaj obstajajo pravila v Splošni uredbi o varstvu podatkov, ki jih je treba upoštevati. Uporaba UI ne poteka v pravnem vakuumu, čeprav omejitve

iz Akta o UI še ne veljajo. Na spletni strani IP je že na voljo precej pojasnil na to temo. Želela bi si, da vsak, ki razmišlja o vpeljavi UI v svoje procese, to stori izjemno previdno in z upoštevanjem vidikov varstva osebnih podatkov.

Informacijski pooblaščenec je eden izmed pomembnih članov Slovenskega združenja za korporativno varnost. Menite, da se lahko odlično sodelovanje nadaljuje tudi v prihodnje? Skupnih izzivov verjetno ne bo zmanjkalo.

Kibernetska varnost je eden od najpomembnejših izzivov modernega varnostnega okolja. Vedno bodo na mizi dileme, kako zagotavljati ustrezno raven varovanja osebnih podatkov v informacijskem okolju. Še posebej, ker imajo te odločitve tudi konkreten poslovne in finančne posledice za upravljavce podatkov. Sodelovanje relevantnih institucij na tem področju je zelo pomembno, saj na ta način krepimo raven varnosti in zavarovanja, delimo dobre prakse s skupnim ciljem – to pa so varna digitalna okolja, robustni sistemi, ki so odporni na kibernetske napade, ki lahko škodujejo osebnim podatkov. Ozaveščanje in spodbujanje skladnosti na tem področju sta izziva, kjer naše sodelovanje gotovo prinaša rezultate. Skupnih izzivov pa na tem področju nedvomno ne bo zmanjkalo. ■

Foto: arhiv IP Republike Slovenije

Slovensko združenje korporativne varnosti

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

- združevanje znanja, izkušenj, interesov in razvojnih pogledov,
- 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.

Mestna občina Ljubljana

Onkološki inštitut Institute of Oncology Ljubljana

Gasilska zveza Ljubljana

Občina Slovenska Bistrica

Melamin

Mercator

CAA

SMART COM

URSIV

telemach

SIEMENS

NIJZ Nacionalni inštitut za javno zdravje

ELEKTRONČEK

Ministrstvo za infrastrukturo

GEN SKUPINA

Javni medobčinski stanovanjski sklad Maribor

Telekom Slovenije

Pošta Slovenije

DARS

PETROL Energija za življenje

AKRAPOVIČ

interblock Luxury Gaming Products

triglav

Informacijske storitve in inženiring, d.o.o. INFORMATIKA

SPICA

tenzor

nova kbm otp group

Elita i.b. d.o.o.

smartis Pametni informacijski sistemi

LON

ZARJA ELEKTRONIKA

UNISTAR PRO

CINKARNA

Slovenske železnice

energetika ljubljana

www.ics-institut.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
ga. Anita Veternik, okrožna državna tožilka

ISKANJE USTREZNIH KORAKOV ZA UČINKOVITO DELOVANJE PRAVOSODNIH ORGANOV V PRIMERU POJAVNIH OBLIK KIBERNETSKEGA KRIMINALA

V ospredju sedanjih razprav o kibernetski varnosti je vprašanje kako storilce na področju kibernetskega kriminala postaviti pred sodišče in tam za storjena kazniva dejanja doseči pravico. Za podroben vpogled v to tematiko smo se pogovarjali z gospo Anito Veternik, okrožno državno tožilko.

Najprej nam dovolite, da vam čestitamo za odličen nastop na Blejskem strateškem forumu, kjer ste se udeležili razprave o »Dešifriranju izsiljevalske programske opreme: izzivi pri preprečevanju izplačil v kripto valutah«. Glede na podatke, ki ji vsako leto posreduje SI-CERT vidimo, da je v Sloveniji zaznan trend upada kibernetskih napadov z izsiljevalskimi virusi in da se krepijo druge pojavne oblike kibernetskega kriminala. Kako resen je z vašega stališča ta problem v mednarodnem okolju?

Najlepša hvala za prijazne besede. V veliko čast mi je bilo sodelovati na tako pomembnem in odmevnem dogodku, kot je Blejski strateški forum. Prav tako se vam zahvaljujem za povabilo na ta intervju, ki sem se ga iskreno razveselila. Menim namreč, da je to izvrstna priložnost za predstavitev dela državnega tožilca, pa čeprav v zelo majhnem obsegu, ker je to ne le poklic ampak tudi poslanstvo, ki je resnično posebno in laični javnosti pogosto zapleteno in težko razumljivo. Mogoče je prav to razlog, da si včasih težje pridobimo zaupanje javnosti, ki pa je vendarle ključna tudi pri našem delu in za uspeh v kazenskih postopkih, kar bom poskušala obrazložiti skozi odgovore na vaša vprašanja.

Kibernetski kriminal je fenomen sodobnega časa. Razmišljam, ali ga sploh lahko tako poimenujem, glede na to, da so se prvi zametki kibernetskega kriminala pokazali že v 80-ih letih prejšnjega stoletja, ko so se računalniki in računalniški sistemi začeli širše uporabljati. Kljub vsemu se nenehno razvija in prilagaja, kar mu daje značilnosti fenomena v smislu hitro spreminjajočega se pojava, ki vpliva na družbo na različnih ravneh. Izsiljevalski virusi so samo en podtip kibernetskega kriminala in v pravkar opisanih trendih nobena izjema, saj naj bi bil prvi dokumentirani domnevni primer izsiljevalske programske opreme trojanski konj AIDS iz leta 1989, znan tudi kot PS Cyborg1, ki se je razširjal preko okuženih disket in za odkupnino zahteval 189 ameriških dolarjev. Če grem nazaj na vaše vprašanje, bom pri odgovoru zelo previdna. V vsakem primeru so izsiljevalske kode še vedno ena od najbolj razširjenih tipov, čeprav je mogoče opaziti rahel upad števila napadov. To potrjujejo različna poročila (npr. Europol IOCTA 2024[1], ENISA Threat Report 2024[2], veeam Insigthts Ransomware Trends 2024[3], Sophos The State of Ransomware 2024[4] ipd.). Kakorkoli, treba se je zavedati, da je pojavnost izsiljevalskih kod zelo odvisna od vrste različnih dejavnikov, med katerimi bi izpostavila predvsem stopnjo digitalizacije storitev v posamezni državi, finančno moč in stabilnost dr-

*avtorica je članica Slovenskega združenja korporativne varnosti

žave, kar predvideva potencialno višje odkupnine za storilce, geopolitično vlogo države, zakonodajo na področju kazenskega pregona pa tudi stopnjo ozaveščenosti, vlaganja v večjo kibernetsko varnost in okrepljeno ter uspešno mednarodno sodelovanje v tovrstnih zadevah. Napovedi, da se bo trend upadanja nadaljeval, so nehvaležne. Kljub temu, da si tega želimo, pa se bojim, da bi bilo lahko to samo zatišje pred nevihto, saj bi lahko bili napadi z uporabo nenehno razvijajoče se umetne inteligence, ki je že in bo zlorabljena tudi v prihodnje, spet bolj pogosti. Lahko pričakujemo, da bodo bolj sofisticirani in težji tako za detekcijo kot tudi za preiskovanje, za kriminalce pa posledično donosnejši, vsaj v obdobju, ko bodo policija, pravosodje in zakonodaja iskali ustrezne rešitve za soočanje s temi izzivi. Na podlagi vsega povedanega bi sklenila, da je na problem potrebno gledati širše; izven meja države, saj problem nedvomno o(b)staja, je skrajno resen tako z vidika finančnih posledic za gospodarstvo kot tudi vpliva na posameznika, in ga moramo še naprej skrbno spremljati.

Vaše jasno stališče, da v vsakem primeru, ki ga vodi državno tožilstvo, tudi na področju procesiranja kaznivih dejanj povezanih s kibernetskim kriminalom, pred sodišči želite doseči pravico. Glede na to, da gre v večini teh primerov za dobro organizirane mednarodne kriminalne združbe, je to zelo zahtevna naloga. Kateri so glavni izzivi s katerimi se tožilci soočate pri procesiranju teh primerov? Je to pomanjkanje specifičnih znanj, pomanjkljiva zakonodaja, težave Policije pri zbiranju dokazov ali kaj drugega?

Že pred leti sem zasledila izjavo tedanje evropske komisarke za pravosodje, potrošnike in enakost spolov, gospe Vere Jourove, ki je dejala: „Medtem, ko preiskovalci še vedno uporabljajo okorne metode, kriminalci za svoje delovanje uporabljajo hitro in najsodobnejšo tehnologijo. Organe preiskovanja in kazenskega pregona moramo opremiti z metodami 21. stoletja za boj proti kriminalu; prav tako kot kriminalci za izvrševanje kaznivih dejanj uporabljajo metode 21. stoletja.“ Ta izjava je mnogo povednejša, kot se zdi na prvi pogled. Ne samo, da moramo preiskovalcem dati na razpolago tehnična orodja, potrebno je zagotoviti tudi njihovo usposobljenost, razumevanje in znanje, ki se mora nujno nadaljevati tudi v tožilskih in sodniških vrstah. Seveda ne v enakem obsegu, potrebno pa je vsaj razumevanje osnov, da je mogoče dejansko stanje pravilno subsumirati pod abstraktno zakonsko normo, razumeti in pravilno ovrednotiti dokaze in izreči pravilno in zakonito sodbo. Seveda pa to velja le, če takšna norma obstaja in jo je zakonodajalec uspešno prilagodil sodobnim izzivom ter razširil njen domet preko meja fizičnega sveta, tudi digitalnega, v katerem se kibernetski kriminal dogaja. Tu pa je še mednarodno sodelovanje, kot ena najpomembnejših komponent, saj kibernetski kriminal ni omejen z državnimi mejami, posledično pa tudi ne z zakonodajo, ki velja le v posamezni državi. Vse omenjeno so kritične točke, ki se morajo v luči sprememb ves čas prilagajati tehnološkemu napredku in možnostim, ki jih kibernetski kriminal zlorablja.

V procesu izplačevanja odkupnin za pridobitev šifer za ponovno odklepanje podatkov se v zadnjem obdobju največkrat uporabljajo kripto valute, katere so bile že v osnovi ustanovljene zaradi manjšega nadzora nad njihovimi transakcijami in identifikacijo plačnika in prejemnika. Smo pa v razpravi slišali, da danes obstajajo ustrezni mehanizmi za spremljanje transakcij in identifikacijo plačnikov ter prejemnikov. Ima državno tožilstvo ustrezne strokovnjake za delovanje na teh kompleksnih primerih ali se tukaj naslanjate na pomoč Policije ali zunanjih ekspertov?

Državno tožilstvo je organ pregona, policija pa je organ preiskovanja. To v praksi pomeni, da je policija po zakonu pristojna za zbiranje obvestil, dokazov in izvedbo operativnih

preiskovalnih dejanj, ki vodijo do odkritja kaznivega dejanja in storilca. Državni tožilec na drugi strani prevzame zadevo v fazi, ko so zbrani dokazi in podatki že predloženi, in se na podlagi teh odloča, ali bo sprožil kazenski pregon ali ne. Posledično se tu v celoti zanašamo na usposobljenost policije. Ima pa državni tožilec v konkretni zadevi vedno na voljo možnost, ki jo predvideva določba 205. člena Zakona o državnem tožilstvu (ZDT-1), ko gre zagotavljanje strokovne pomoči s področja različnih strok, ki je potrebna za strokovno in učinkovito delovanje državnih tožilcev pri usmerjanju odkrivanja in pregonu storilcev kaznivih dejanj. Do sedaj se ta pomoč še nikoli ni zahtevala v zadevah z visokotehnološkimi elementi, prednjačijo namreč zadeve, kjer se potrebuje pomoč izvedencev ekonomske stroke. Osebno menim, da je samo vprašanje časa, kdaj bomo dobili prvo pobudo za postavitev strokovnjaka računalništva in informatike oziroma računalniške forenzike in informacijske varnosti.

Glede na vedno bolj zahtevne pojavne oblike kriminalnih aktivnosti, povezanih s kibernetskim področjem, bi verjetno v prihodnosti potrebovali tudi ustanovitev specializiranih državno tožilskih struktur, ki bi bile posebej usposobljene in opremljene za spopadanje s temi zahtevnimi pojavnimi oblikami. Trenutno je verjetno dodeljevanje primerov še vedno pogojeno po krajevni pristojnosti tožilstva? Ali to pomeni, da se državni tožilec ves čas srečuje z zelo različnimi in kompleksnimi oblikami kriminalitete?

Popolnoma prav imate. Državna tožilstva lahko skladno z ZDT-1 ustanovijo posebne oddelke, v katere razporedijo državne tožilce, ki se praviloma ukvarjajo z določenim področjem kriminalitete, ni pa to pravilo. Predvsem na manjših tožilstvih državni tožilci pogosto obravnavajo vse vrste kriminalitete in lahko si predstavljate kako zahtevno je danes biti strokovnjak za medicino, jutri za železniški promet in pojutrišnjem strokovnjak za kripto premoženje. Ponekod v svetu že obstajajo ureditve s t.i. »Cybercrime Unit«, kjer so v oddelke razporejeni preiskovalci in tožilci, ki poleg poznavanja domače in tuje zakonodaje, vključno z mednarodnim sodelovanjem z uporabo različnih pravnih podlag, razpolagajo tudi s poglobljenim znanjem o informacijski tehnologiji, omrežjih, kibernetski varnosti in najnovejših orodjih ter tehnikah, uporabljenih pri izvrševanju kaznivih dejanj s kibernetskimi elementi. Hkrati je takemu oddelku potrebno omogočiti dostop do naprednih orodij in tehnologije, ki omogočajo digitalno forenziko, zbiranje, ustrezno hrambo in analizo elektronskih dokazov, vključno z dešifriranjem podatkov in analizo transakcij kriptovalut. V Sloveniji trenutno še nismo na točki, ko bi se resno pogovarjali o ustanovitvi take enote, po vsej verjetnosti pa je to glede na predvidevanja o razvoju kibernetske kriminalitete v prihodnje edina prava pot.

Hitrost prijave takega kaznivega dejanje je lahko odločilna za uspešno odkrivanje storilcev, zbiranje dokazov in končno procesiranje na sodišču. Skozi prakso vidimo, da je tukaj kar nekaj izzivov, ki se rezultirajo skozi dejstva, da predvsem podjetja redkeje in nerada prijavljajo ta dejanja. Kaj je po vašem mnenju razlog in kako bi to zavedanje lahko izboljšali?

Drži, hitrost prijave je v takih primerih ključnega pomena. Elektronski dokazi so zelo volatilni – hitro se lahko izbrišejo ali spremenijo do mere, da niso več uporabni za preiskovanje in dokazovanje kaznivega dejanja. To se lahko zgodi namenoma ali pa nevede, saj do pomembnih sprememb lahko pride že s tako banalno aktivnostjo, kot je ponovni zagon elektronske naprave. Pravočasna prijava pa je le prva predpostavka uspešnega preiskovanja kaznivega dejanja, ki ji morajo slediti še učinkovita preiskava, skrbno in pravilno shranjevanje dokazov, pregled v skladu s standardi in pravili forenzičnih preiskav in pravilno vrednotenje dobljenih rezultatov. Kakorkoli, vse se začne s prijavo oškodovanca, ki pa lahko iz različnih vzrokov izostane. V sedmi izdaji Kibernetskega pravosodnega monitorja[5] je bilo prav to eno od področij raziskav, kjer je bilo ugotovljeno, da je glavni izziv sodelovanja med žrtvami in organi preiskovanja in kazenskega pregona v različnih interesih in pogosto tudi v pomanjkanju zaupanja. Žrtve napadov z izsiljevalsko programsko opremo, zlasti kadar govorimo o gospodarskih družbah in kritični infrastrukturi, verjetno dajejo prednost čim hitrejšemu ponovnemu vzpostavljanju sistemov in s tem obvladovanju škode. Brez ustreznega zavarovanja pa to v večini primerov vodi do spremembe ali izgube pomembnih dokazov, o čemer smo že govorili. Dalje je odločitev o prijavi lahko odvisna tudi od predvidenih posledic, ki bi jih razkritje napada lahko imelo v javnosti in bi potencialno lahko negativno vplivalo na njihov ugled in zaupanje strank. Tudi posamezniki kaznivih dejanj ne prijavijo – bodisi zaradi sramu ali ker preprosto ne verjamejo, da bo kaznivo dejanje uspešno preiskano in da bo storilec na koncu pravično kaznovan. Zato je treba okrepiti medsebojno zaupanje in delati v smeri učinkovitejšega dela organov preiskovanja in pregona s skupnim ciljem izpolnitve temeljnih načel kazenskega postopka.

Za učinkovito delovanje tožilstva pa tudi sodišča je izredno pomembna sodna praksa. Čeprav naš kontinentalni pravni sistem odstopa od klasičnega, na sodni praksi temelječega anglo-saksonskega sistema, je vendar tudi v Republiki Sloveniji sodna praksa zelo pomemben temelj. Ali nam lahko posredujete kakšne podatke ali statistiko vezano na uspešno realizirane primere specifičnih kaznivih dejanj povezanih z izsiljevalskimi virusi?

Novela KZ-1I[6] je v obe kaznivi dejanji, ki v naši zakonodaji predstavljata kibernetski kriminal v ožjem smislu, in sicer Napad na informacijski sistem (221. člen) in Zloraba informacijskega sistema (237. člen), vnesla novo izvršitveno obliko »oviranje dostopa do podatkov«. S tem naj bi novela izrecno inkriminirala uporabo izsiljevalske kode, ki jo storilec izrabi, da od žrtve zahteva plačilo za odklep zaklenjenih podatkov. V Sloveniji sodna praksa predstavlja sekundarni vir prava in je vsekakor je pomembna z vidika enotne uporabe prava. Žal pa je za to področje (zaenkrat) v Sloveniji ni, prav tako pa iz informacijskega sistema državnega tožilstva ne moremo pridobiti uporabnih statističnih podatkov za točno te primere. Dogodkov, vezanih na posamezno izvršitveno dejanje, namreč ne beležimo in bi tako lahko verodostojne podatke pridobili zgolj na podlagi ročnega pregleda in analize spisov.

Glede na to, da gre za mednarodne kriminalne združbe, je na vseh nivojih ključno tudi mednarodno sodelovanje in izmenjava podatkov. Smo v EU že dosegli ustrezno stopnjo sodelovanja v okviru Europola ali Eurojusta ali so tukaj še možne izboljšave in katere bi bile najbolj potrebne?

V vlogi pomočnice nacionalnega predstavnika za Slovenijo pri Eurojustu sem se prepričala, da je mednarodno sodelovanje neizbežno, če želimo zagotoviti učinkovit pregon kibernetskega kriminala s transnacionalnim elementom. Sodniki in državni tožilci se pogosto obračajo na nacionalno predstavništvo pri Eurojustu za pomoč, kar lahko izpostavim kot primer odlične prakse. Eurojust je vzpostavil obsežno mednarodno mrežo, ki tožilcem in sodnikom v EU omogoča dostop do več kot 50 jurisdikcij po svetu. Izmed orodij, ki jih ponuja, bi posebej izpostavila skupne preiskovalne skupine (JIT), ki zaradi svoje narave lahko znatno pohitrijo preiskave v zapletenih primerih in tudi močno poenostavijo zbiranje in izmenjavo dokazov. Tukaj tudi vidim prostor za izboljšave, saj bi z večjim številom skupnih preiskovalnih skupin združili tudi različna znanja in izkušnje, ki jih imajo mednarodni partnerji in so v tem kontekstu še kako pomembni. Dejstvo je, da se kibernetski kriminal dogaja v drugačnem svetu, za katerega zakonitosti fizičnega sveta pogosto ne veljajo, predvsem pa se nenehno spreminja, kar terja prilagajanja ne samo na ravni zakonodaje in mednarodnega sodelovanja, pač pa tudi nenehnega izobraževanja in usposabljanja. Po mojem mnenju je še nekaj manevrskega prostora na področju harmonizacije pravil na ravni EU (še vedno je pereče vprašanje o obvezni hrambi podatkov operaterjev in ponudnikov storitev informacijske družbe; t.i. Data Retention) in na področju enostavne, varne in hitre izmenjave elektronskih dokazov ter drugih podatkov (npr. eEDES).

Slovensko združenje za korporativno varnost je pomembno stičišče ključnih gospodarskih in tudi javnih organizacij. Menite, da je lahko to eden od pomembnih kanalov, kjer tudi s pomočjo izkušenj in dobrih praks, ki jih imate na državnem tožilstvu, zagotovimo višjo stopnjo zavedanja o pomembnosti hitre prijave za uspešnost nadaljnjega procesiranja?

Sem absolutna zagovornica povezovanja in sodelovanja med različnimi deležniki. Dejstvo je, da vsak od nas razpolaga z različnimi znanji in informacijami. Včasih ugotovimo, da se naši pogledi na določene stvari tudi razlikujejo, kar pa ni nič slabega. Izmenjava izkušenj in dobrih praks lahko pomaga k boljšemu razumevanju našega dela in izboljša sodelovanje med nami. Brez dvoma ima vsak od nas pomembno vlogo pri ozaveščanju javnosti, zato močno verjamem, da če se v prizadevanjih združimo, lahko s skupnimi močni bistveno zmanjšamo ranljivost posameznikov in podjetij ter prispevamo k varnejši družbi.

Oktober je med drugim tudi mesec kibernetske varnosti. Kakšno bi bilo vaše sporočilo za strateški management slovenskih podjetij in stroko, ki se v podjetjih ukvarja z zagotavljanjem korporativne varnosti?

To je zelo kompleksno in zahtevno vprašanje, odgovor pa bom podala na podlagi svojega znanja in izkušenj, ki sem jih pridobila kot državna tožilka in vodja Strokovno informacijskega centra pri Vrhovnem državnem tožilstvu RS. Med intervjujem smo govorili o številnih izzivih, ki jih strokovnjakom z različnih področij in družbi kot celoti, prinaša kibernetski kriminal. Dejstvo je, da je kibernetska varnost v današnjem času izrednega pomena zaradi palete različnih in nenehno razvijajočih se groženj, višje stopnje digitalizacije in globalne povezljivosti ter s tem tudi ranljivosti ter posledično potrebe po zagotavljanju gospodarske stabilnosti. Predpostavka za dobro načrtovanje in delo je vedno dobra strategija kibernetske varnosti, kjer ocenimo ključna tveganja in kritične podatke ter izdelamo načrt za odzivanje na incidente. Na državnem tožilstvu smo celovito prenovili tudi varnostne politike in močno okrepili naša prizadevanja v smeri izobraževanj in osveščanja zaposlenih na državnem tožilstvu, saj verjamemo, da bomo s tem pomembno zmanjšali možnosti kibernetskih napadov. Povsem jasno je , da človeškega faktorja nikoli ni mogoče v celoti izključiti, zato se je potrebno nasloniti tudi na varnostno tehnologijo, ki bo pravočasno prepoznala in preprečila vdore v sisteme. Nenazadnje pa se je pomembno zavedati, da kibernetska varnost ni enkratni projekt, pač pa nenehen proces proučevanja in prilagajanja, s ciljem ostati v koraku z razvojem tehnologije in novih groženj ter pravočasno prilagoditi aktivnosti, ki bodo omogočale varno in posledično nemoteno poslovanje.

1 https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

2 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

3 https://www.veeam.com/analyst-reports/2024-ransomware-trends-executive-summary-emea_wpp.pdf

4 https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

5 https://www.eurojust.europa.eu/publication/cybercrime-judicial-monitor-issue-7

6 Uradni list RS, št. 186-3697/2021 z dne 30.11.2021 ■

Informacijske storitve in inženiring, d.o.o.

INFORMATIKA

Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

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

Vplivi kibernetskih napadov na različna področja v energetiki:

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

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

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

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

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

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

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

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

ČAS JE ZA ODLOČILEN KORAK

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

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

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

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

www.informatika.si

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

KOLUMNA

BOMO ZMOGLI PRESTOPITI OMEJITVE PARCIALNIH INTERESOV ZA DOSEGO POMEMBNEGA NACIONALNEGA CILJA

V Sloveniji se nahajamo pred pomembnim izzivom, kako dokončati oblikovanje varnostno operativnega centra kibernetske varnosti v energetskem sektorju. Varnostni izzivi, katere prinaša kibernetsko okolje, so vedno bolj zahtevni in jih je nemogoče reševati s parcialnimi pristopi. To dejstvo še toliko bolj velja za energetski sektor, kjer je povezanost in soodvisnost delovanja med posameznimi energetskimi deležniki še toliko bolj pomembna. V pričujoči kolumni želimo dokončno osvetliti poti in stranpoti v razvoju te pomembne nacionalne kibernetske zmogljivosti v energetskem sektorju.

To, da energetski sektor potrebuje celovit pristop pri upravljanju kibernetskih tveganj, postaja jasno tudi največjim dvomljivcem. Kibernetski napadi, ki jih dnevno doživljajo energetske družbe, tudi v Sloveniji, niso več samo odmaknjena informacija, temveč realnost zelo zahtevnega varnostnega okolja. Tudi v Sloveniji imamo na žalost neposredne izkušnje s kibernetskimi napadi na najpomembnejše energetske deležnike. Učinkovito preprečevanje takih napadov in upravljanje kibernetske varnosti v tem pomembnem sektorju pa je možno samo z vzpostavitvijo celovitega centraliziranega sistema. Njegova vzpostavitev bo sicer terjala pomembno mero modrosti strateškega managementa v energetskih organizacijah, močno podporo države in državnih institucij ter dovolj strokovnega znanja pri neposrednih izvajalcih tega procesa v energetskih organizacijah, ko bodo končno dojeli nujnost tega koraka brez uveljavljanja svojih parcialnih pogledov. Čeprav nas je že prej navedeno varnostno okolje in varnostna situacija pripeljala do tega, da se načeloma vsi strinjamo s potrebo po vzpostavitvi take koordinativne zmogljivosti, pa nam vendarle pri končnem koraku to nekako ne steče.

Naj pojasnimo bližnjo zgodovino izvedenih korakov in vplivne dejavnike, ki so nujni za pravilno razumevanje trenutne situacije in jasnejšo sliko o potrebnih zaključnih odločitvah in operativnih korakih. Naj posebej poudarim, da so to majhni koraki za vsak posamezen energetski subjekt, vendar velik skok za celoten energetski sektor.

Na temo vzpostavitve Varnostno operativnega centra v energetskem sektorju je bilo pripravljenih nekaj nacionalnih in tudi ena mednarodna študija. Zadnja od njih je bila študija, ki jo je po naročilu ELES-a izvedel Institut za korporativne varnostne študije in je s svojim integrativnim pristopom podala glavne možne variantne rešitve za sprejem potrebne odločitve po kateri poti dokončati vzpostavitev te zmogljivosti. Dej-

*avtor je član Slovenskega združenja korporativne varnosti

Varnostni izzivi, katere prinaša kibernetsko okolje, so vedno bolj zahtevni in jih je nemogoče reševati s parcialnimi pristopi.

stvo je, da imamo v taki ali drugačni obliki dva delujoča Varnostno operativna centra (v nadaljevanju VOC) za zagotavljanje kibernetske varnosti znotraj elektro energetskega sistema in sicer sta to VOC-a v INFORMATIKI in ELES-u. Prvi upravlja in podpira zagotavljanje kibernetske varnosti pri vseh operaterjih distribucijskega omrežja, drugi pa je vzpostavljen za zagotavljanje interne kibernetske varnosti v ELES-u. Oba po javno dostopnih podatkih delujeta kombinirano, kar pomeni, da za svoje polno delovanje potrebujeta podporo zunanjih deležnikov. Drugi deli energetskega sektorja zagotavljajo to podporo s celovito naslonitvijo na zunanje partnerske organizacije. Torej iz napisanega je razvidno, da energetski sektor trenutno nima zadostnega strokovnega potenciala, ki bi lahko celovito podprl zagotavljanje te pomembne kibernetske operacije. Zaradi razpršenosti strokovnega kadra, pa to pričakovanje v danem trenutku predstavlja še toliko večji izziv. Vendar pa je zadeva vzpostavitve VOC energetskega sektorja izvedljiva, potrebuje samo močan potisk in določitev strateške smeri razvoja, ki bo centralizirala napore in vire, ki se trenutno vlagajo parcialno in s tem zgubljajo svojo učinkovitost.

V nadaljevanju želimo jasno predstaviti te nujne korake:

- Trenutno se na prvi pogled zdi, da je ELES s svojim direktorjem glavni promotor te vzpostavitve. ELES je sicer eden od najbolj pomembnih dejavnikov elektro energetskega sektorja in se zaradi svoje vpetosti v mednarodne prenosne energetske poti tudi zaveda izredno velike nevarnosti, ki jo za nemoteno delovanje energetskega sektorja predstavljajo kibernetska tveganja. Vendar ELES sam ne bo zmogel narediti vsega potrebnega za dosego tega cilja. Tukaj na žalost pogrešamo močnejšo vlogo države in ključnih državnih institucij od Vlade Republike Slovenije in njenega svetovalca za nacionalno varnost, Ministrstva za energetiko in naravne vire pa vse do Urada za informacijsko varnost, Agencije za energetiko in drugih pomembnih nacionalnih institucij.

Vzpostavitev takega koraka ni prepuščena samo deležnikom energetskega sektorja, da se ob svobodni gospodarski pobudi sami odločajo kako bodo oblikovali zagotavljanje kibernetske varnosti. Energetika je poseben sektor, kjer je država večinski lastnik, ta sektor pa centralni sektor od katerega so odvisni vsi ostali sektorji in družba kot celota. Torej je potrebno v tem sektorju zagotoviti, da bo že s strani države jasen signal in usmeritve, da se v danem trenutku preseka gordijski vozel parcialnih interesov posameznih delov tega sektorja. Zato ima poleg normativnih podlag tudi jasne upravljavske vzvode preko Slovenskega državnega holdinga. Torej pričakujemo, da ELES v tej bitki ne bo ostal osamljeni promotor te ključne nacionalne potrebe.

- Naslednji pomembni dejavnik sodi na področje nerazumevanja dejanske vloge VOC energetskega sektorja. Strateški managerji v energetskih organizacija se bojijo, da jim bo omenjena skupna zmogljivost vzela pristojnosti in tudi kadrovske vire za zagotavljanje kibernetske varnosti v njihovih organizacijah. To je neresnica, ki jo po navadi širijo tisti, ki ne želijo, da se ta zadeva sistemsko uredi. Strateški management bo s svojimi strokovnimi kadri še vedno pristojen zagotavljati kibernetsko varnost v svoji organizaciji. Vzpostavitev VOC energetskega sektorja bo samo dodana zmogljivost, ki bo centralno skrbela za usklajenost nadzora nad informacijskim sistemom in izvajanjem skupnih odzivov v primeru zaznanih kibernetskih tveganj. Vse primarne stvari zagotavljanja kibernetske varnosti ostajajo v rokah posameznih organizacij. Nerazumevanje je terminološke narave saj največkrat nastane pri nepoznavanju nivojev zagotavljanja delovanja VOC in nivoja delovanja, ki ga morajo zagotoviti v vsaki organizaciji posebej.

- Veliko je govora o višini stroškov. Vsak vložek v zagotavljanje varnosti je investicija in ne strošek, saj brez zagotavljanja neprekinjenosti delovanja energetskega sektorja ni učinkovitega in poslovno uspešnega delovanja energetskih družb. Seveda je dejstvo, da bo vzpostavitev take zmogljivosti prineslo dodatne stroške, ki pa bodo ob sistematičnih korakih in ustrezni usklajenosti tudi dosti nižji od trenutnih parcialnih in nesistemskih korakov, ki dokazano ne prinašajo ustrezne stopnje varnosti.

- Energetski sektor bi potreboval dolgo časovno obdobje, da bi sam oblikoval celovito in polno delujočo zmogljivost VOC. Zaradi navedenega je ključen sprejem odločitve o izbiri strateškega partnerja, ki bo podprl razvoj in delovanje VOC energetskega sektorja ter zagotovil polno delovanje te kombinirane zmogljivosti tudi v kasnejši razširitvi pristojnosti VOC v CSIRT energetskega sektorja. Seveda se tukaj, kot je v navadi, zaradi različnih vplivnih in lobističnih posredovanj, srečujemo s pomembnimi izzivi, ki omejujejo sprejem jasne razvojne poti. Deležnikov, ki bi se lahko strokovno pojavili kot strateški partner je zelo omejeno število, če pa vzamemo v obzir, da gre pri tako pomembnem sektorju, kot je energetika, za pomembne nacionalne interese mora vsak dober gospodar resno razmisliti kdo izven nacionalnega okolja lahko upravlja s ključnimi kibernetskimi podatki in se pojavi v vlogi tega strateškega partnerja. Lastniška struktura različnih ponudnikov teh storitev v Sloveniji celo presega meje držav EU. Si res želimo upravljanje tako ključnega sektorja postaviti v novo obliko tveganja? Temu v zadnjem obdobju tudi EU namenja resno pozornost, saj se je pomembno omejilo sodelovanje vseh deležnikov, ki imajo lastništvo izven držav EU na vseh pomembnih razpisih na kibernetskem področju. Torej izbira strateškega partnerja

mora biti takojšnja, jasna in dolgoročno zasnovana. Samo tako bodo lahko posamezni deli energetskega sektorja že danes začeli usmerjati svoje korake proti temu skupnemu cilju, ki bo kasneje močno olajšal integracijo v celovit sistem. Je pa res, da je potrebno VOC energetskega sektorja razviti do te ravni zmogljivosti, da se lahko v danem trenutku, ob spremenjenih okoliščinah, zamenja strateškega partnerja ali z dodatnimi ukrepi vzpostavi celovitost storitve znotraj VOC energetskega sektorja.

- Kadrovski izzivi so na tem področju pomemben dejavnik in mu bo potrebno nameniti ustrezno pozornost. Ponovno pa je pomembno ustrezno sprejemanje strategije, ki bo v daljšem časovnem obdobju omogočila usklajene prijeme, ki ne bodo predstavljali sistema kanibalizma oz. prevzemanja kadra iz ene organizacije v drugo. Zaradi navedenega je potrebno jasno načrtovano usmeriti izgradnjo kadrovskih zmogljivosti s pridobitvijo in usposobitvijo novih kadrovskih potencialov. Pomembno je omejiti nerealne poglede in se usmeriti po poti racionalnih zmožnosti ter jih vedno razumeti kot razvojno pot skupaj z izbranim strateškim partnerjem. Finančni vidik je sicer pomemben za zagotavljanje ustreznih kadrov, nikakor pa ne odločujoč. Drugi pogoji in ukrepi so ravno tako pomembni in na teh je potrebno narediti več, da bodo taka delovna mesta postala zanimiva za mlade in strokovne kadre.

- Razumevanje potrebe po modularnosti razvoja je zelo pomemben korak do uspeha. Nujno je potrebno začeti z ožjim delom elektro energetskega sektorja (ELES in distribucije), ki ima večji del teh zmogljivosti že izgrajenih in delujočih. V naslednjem koraku je potrebno poskrbeti, da se bosta sistemu priključila še oba proizvodna stebra električne energije v zadnjem koraku pa še celoten ostali del energetskega sektorja (plin, nafta). Kot zadnji korak pa lahko pomeni, da bi se tak delujoč VOC energetskega sektorja centralno uporabil tudi za ostale deležnike na področju kritične infrastrukture iz drugih sektorjev.

Naj za zaključek povzamemo, da je za dosego tega zelo pomembnega strateškega nacionalnega cilja potrebno pogledati izven okvirov svojih vsakdanjih omejitev, ki si jih, roko na srce, največkrat postavljamo sami. Razlogov za to je več, pomembno pa je, da v kritičnih trenutkih strateško vodstvo uveljavi svojo pristojnost po sprejemanju pravih odločitev in preseganju manjših parcialnih interesov. Veliki voditelji so tisti, ki se v trenutku odločitve upajo odločiti, čeprav se v danem trenutku vedno najdejo dvomljivci in nasprotniki. Zgodovina je tista sodnica o pravilnosti odločitev. V vsakem primeru smo dolžni zagotoviti kibernetsko varnost za neprekinjeno delovanje energetskega sektorja, ki v moderni družbi predstavlja njeno hrbtenico. Torej sploh ne sme biti vprašanje, ali bodo vzpostavili to kibernetsko koordinativno zmogljivost, temveč kdaj jo bomo ustanovili in kako bo učinkovita pri svojem delovanju. ■

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

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

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

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

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

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

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

ISO 27001

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

BUREAU VERITAS

DPO

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

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Matjaž Mravljak, direktor Inšpekcije za informacijsko varnost URSIV*

PRED NAMI SO POMEMBNE SPREMEMBE NA PODROČJU ZAGOTAVLJANJA INFORMACIJSKE VARNOSTI

Nahajamo se v fazi pomembnih korakov na področju uveljavljanja določil NIS-2 v nacionalni ekosistem operativnega delovanja za področje zagotavljanja informacijske varnosti. Inšpekcijski organi imajo v tem pogledu izredno pomembno vlogo in sicer tako na področju pravilnega razumevanja zakonsko predpisanih rešitev kot tudi za nadzor in oceno realnega stanja na tem pomembnem področju. Pogovarjali smo se z direktorjem Inšpekcije za informacijsko varnost URSIV.

Vsak inšpektorat ima pri upravljanju in izvajanju zakonsko predvidenih nalog s strani določenih subjektov izredno pomembno vlogo. Nam za začetek prosim zaupate bistvene naloge Inšpektorata za informacijsko varnost.

Inšpekcija za informacijsko varnost je notranje organizacijska enota Urada Vlade Republike Slovenije za informacijsko varnost. Cilj delovanja Urada Vlade Republike Slovenije za informacijsko varnost je zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah in zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti. Tako je primarna naloga inšpekcije preverjanje skladnosti zavezancev s predpisi s področja informacijske varnosti v inšpekcijskih postopkih, sekundarna pa pomoč in svetovanje zavezancem pri doseganju skladnosti s predpisi. Pomembna naloga naše inšpekcije je tudi stalno usposabljanje in strokovno izpopolnjevanje inšpektorjev. Smo pa inšpektorji vpeti tudi v izvajanje drugih strokovnih nalog urada.

Pred nami je sprejem novega zakona o informacijski varnosti, ki naj bi pomenil uveljavitev določil NIS-2, vendarle je potrebno poudariti, da imajo zavezanci že po trenutnem zakonu zelo pomembne naloge in odgovornosti. Nam lahko podate generalno oceno kako uspešni so bili trenutni zavezanci pri uveljavljanju določil povezanih z izdelavo potrebne varnostne dokumentacije in vzpostavitve sistema informacijske varnosti v svojih organizacijah?

Na podlagi ugotovitev iz inšpekcijskih nadzorov lahko stanje na področju informacijske varnosti delimo nekako na dva segmenta in sicer: stanje na področju informacijske varnosti pri izvajalcih bistvenih storitev in stanje na področju informacijske varnosti v organih državne uprave. Opažamo, da so bili izvajalci bistvenih storitev, pri uveljavljanju zakonskih zahtev, povezanih z izdelavo potrebne varnostne dokumentacije in vzpostavitve ustreznih varnostnih ukrepov, nekoliko bolj motivirani in uspešni kot organi državne uprave.

V zadnjem obdobju ste močno intenzivirali inšpekcije pri izvajalcih bistvenih storitev z namenom preverjanja stanja varnostne dokumentacije. Nam lahko zaupate kaj so osnovni cilji, ki ste si jih zastavili s to kampanjo?

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Inšpekcija izvaja inšpekcijske nadzore v skladu s sprejetimi Strateškimi usmeritvami in prioritetami inšpekcijskega nadzora Urada Vlade Republike Slovenije za informacijsko varnost za vsako posamezno leto. Na podlagi tega dokumenta inšpekcija za vsako leto pripravi načrt inšpekcijskih nadzorov, oba dokumenta odobri in podpiše direktor urada. Na primer, v 2022 je bil poudarek pri načrtovanju in izvajanju nadzorov na sektorju zdravstva, v 2023 je bil poudarek na sektorju energetike, v 2024 pa je na oskrbi s pitno vodo. Cilji so vedno enaki: ugotavljanje skladnosti zavezancev s predpisi s področja informacijske varnosti in posledično dvig odpornosti zavezancev ter tudi svetovanje in pomoč pri pripravi predpisane dokumentacije in implementacije varnostnih ukrepov. Pri načrtovanju inšpekcijskih nadzorov smo upoštevali tudi tveganja in kritičnost posameznih sektorjev.

Vsaka inšpekcija ima zelo pomemben vpliv, ki ni odmerjen samo na izvajanje kaznovalne politike, temveč predvsem na svetovanje, usmerjanje in preventivne korake udejanjanja dobrih praks v ključna okolja pri zavezancih. Je tudi vaša vizija delovanja Inšpekcije za informacijsko varnost tako usmerjena?

Z vašo podano tezo se popolnoma strinjam. Svetovanje, usmerjanje in preventivno dejavnost izvajamo tudi skozi inšpekcijske nadzore in s sodelovanjem na različnih konferencah ter dogodkih. Ugotovitve inšpektorja in roke za izvedbo ukrepov za odpravo nepravilnosti vselej usklajujemo z zavezanci. V bistvu v inšpekcijskih nadzorih uporabljamo bolj revizijski pristop, komunikacija z zavezanci pa je vedno dvosmerna. Vendar pa poleg podanih priporočil, za razliko od revizorjev, izrekamo tudi ukrepe za odpravo nepravilnosti. Pri ugotovljenih manjših nepravilnostih nikoli nismo izvajali prekrškovnih postopkov, medtem, ko se pri ugotovljenih hujših nepravilnostih temu ne moremo izogniti. Moramo spoštovati prekrškovno zakonodajo.

Izvajalci bistvenih storitev so medijsko zelo izpostavljeni kot eni od zavezancev na podlagi zakona o informacijski varnosti. V javnosti se dostikrat spregleda, da so zavezanci tudi organi državne uprave, ponudniki digitalnih storitev in državni organi, organi lokalnih skupnosti, javne agencije in nosilci javnih pooblastil ter drugi subjekti, ki niso organi državne uprave. Kako ste zadovolji s stanjem informacijske varnosti v ostalih segmentih zavezancev?

Trenutno imamo določenih 49 izvajalcev bistvenih storitev, 18 organov državne uprave in (samo) prepoznanega enega ponudnika digitalnih storitev. Z zadnjo spremembo Zakona o informacijski varnosti smo dobili še okoli 450 povezanih subjektov, ki pa so vsi subjekti, ki se povezujejo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom. Za slednje veljajo manj strožji pogoji glede izpolnjevanja zakonskih zahtev. V vsakem letnem načrtu nadzorov na področju informacijske varnosti načrtujemo tako nadzore pri izvajalcih bistvenih storitev kot pri organih državne uprave. Ugotovitve iz do sedaj izvedenih inšpekcijskih nadzorov zagotovo kažejo, da je stopnja zrelosti na področju informacijske oziroma kibernetske varnosti pri izvajalcih bistvenih storitev višja kot pri organih državne uprave.

Veliko se v zadnjem obdobju govori o tem, da bo uveljavitev določil NIS-2 skozi nov Zakon o informacijski varnosti prinesla velik obseg novih zavezancev. To bo tudi za vaš inšpektorat prineslo ogromno dodatno obremenitev. Načrtujete povečanje obsega sodelavcev v inšpektoratu ali imate kakšne druge načrte za spoprijemanje s temi zahtevnimi izzivi?

Prenos NIS 2 direktive v nov Zakon o informacijski varnosti bo zagotovo prinesel enormno povečanje števila zavezancev. To bo velik zalogaj za celoten Urad Vlade Republike Slovenije za informacijsko varnost. Za hitrejše in učinkovitejše izvajanje inšpekcijskih pregledov smo lani in letos uspešno testirali in uvedli dva namenska orodja. V naslednjem letu imamo v načrtu izvedbo testiranja orodja umetne inteligence, ki bo uporabno pri izvajanju inšpekcijskih nadzorov. Navedeno (on-premises) orodje razvijajo sodelavci v uradu in je še v fazi razvoja, obeti pa so dobri. V inšpekciji seveda načrtujemo povečanje števila inšpektorjev vendar imamo že sedaj velike težave pri pridobivanju novih sodelavcev, nimamo zasedenih vseh delovnih mest. Za strokovno in učinkovito delo inšpektorja je potrebno tako znanje s pravnega področja kot dobro poznavanje področja informacijsko – komunikacijskih tehnologij. Neustrezna plačna politika v javnem sektorju in veliko povpraševanje po ustreznih strokovnjakih na trgu dela bistveno zmanjšuje možnost zaposlitve kompetentnih uslužbencev. Lahko pa se v nekem trenutku zgodijo tudi težave pri zadržanju že zaposlenih uslužbencev. Močno upam, da bo prenova plačnega sistema v javnem sektorju, ki naj bi začela veljati drugo leto, prinesla pozitivne učinke tudi na tem področju.

Čeprav ste primarno zadolženi za izvajanje inšpekcijskih postopkov na podlagi nacionalnega Zakona o informacijski varnosti so verjetno skupni pristopi na nivoju pri izvajanju nadzora nad tem pomembnim področjem ravno tako pomembni. Imate vzpostavljeno kakšno sodelovanje med inšpekcijski organi drugih držav EU ali je to celo urejeno na EU nivoju?

Formalno nimamo vzpostavljenega sodelovanja med inšpekcijski organi drugih držav Evropske unije. Niti mi ni poznano, da bi takšne prakse v Evropski uniji obstajale. Sem pa na nivoju Evropske unije član delovne skupine Workstream Supervision, ki spada pod NIS Cooperation Group. Člani delovne skupine se redno sestajamo in se že nekaj časa ukvarjamo predvsem z implementacijo NIS 2 direktive na področju nadzora in čezmejnega sodelovanja.

URSIV je dolgoletni korporativni član Slovenskega združenja za korporativno varnost. Menite, da bi lahko to obliko sodelovanja še močneje izkoristili za posredovanje ustreznih sporočil, ki jih tudi vi preko Inšpektorata za informacijsko varnost želite posredovati v okolje izvajalcev bistvenih storitev?

Povezovanje, izmenjava informacij in sodelovanje vseh deležnikov na področju informacijske varnosti v Sloveniji, v vseh oblikah, je po mojem mnenju zelo pomembno za situacijsko zavedanje in zagotavljanje celovite slike ter posledično povečevanje odpornosti pred kibernetskimi grožnjami celotnega ekosistema. Pozdravljam vse oblike takšnega sodelovanja in povezovanja ter menim, da je vaše združenje na tem področju eden od pomembnih deležnikov. Inšpekcija se je vedno odzvala na prošnje za sodelovanje na različnih dogodkih in na prošnje zavezancev za strokovno (po)svetovanje. Preventivna dejavnost je ena od naših nalog. Naša želja je, da v inšpekcijskih nadzorih ne bi ugotavljali hujših kršitev predpisov.

Želite mogoče za konec posredovati še kakšno ključno sporočilo strokovni javnosti, ki bo pomembno vplivalo na nivo izvajanja informacijske varnosti v Republiki Sloveniji?

Kibernetski prostor je globalno informacijsko okolje, kjer ni državnih meja in kjer je informacijska oziroma kibernetska varnost ključnega pomena za zaščito naših podatkov, sistemov in infrastrukture, našega načina življenja. Republika Slovenija se tako kot drugi sooča z naraščajočimi in vedno bolj naprednimi kibernetskimi grožnjami, ki zahtevajo posebno pozornost vseh, ki so odvisni od omrežnih in informacijskih sistemov. Vsem tem organizacijam (še posebej tistim, ki niso zavezanci) zelo priporočam uporabo našega vprašalnika oziroma »orodja« za samooceno informacijske varnosti, ki je namenjeno organizacijam za pomoč in podporo pri njihovi začetni oceni kibernetske varnosti. Navedeni vprašalnik je dostopen na spletnih straneh Urada Vlade Republike Slovenije za informacijsko varnost in je popolnoma anonimen.

Naj si za zaključek izposodim znameniti citat: Kibernetska varnost je potovanje, ne cilj! (Calder, 2005). In vsako potovanje se prične s prvim korakom. ■

A1 Business

Razumemo
kibernetsko varnost.
Z mednarodnimi izkušnjami.

Matic Grobelšek
Direktor za poslovni trg
A1 Slovenija

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

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

Razumemo digitalno, da lahko vaš posel teče nemoteno."

Več

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Mitja Buda, izvršni direktor skupine ACTUAL I.T.

DINAMIČNO VARNOSTNO OKOLJE ZAHTEVA STALNE PRILAGODITVE NOVIM TEHNOLOŠKIM REŠITVAM

Neprekinjenost delovanja kritičnih sistemov in infrastrukture je ujeta med stalno prilagajanje med potrebo po povezljivosti in izmenjavi podatkov na eni strani ter na drugi strani po vedno večji potrebi po varnosti, saj se število groženj nenehno povečuje. Z nami je podelil nekaj strateških misli g. Mitja Buda iz podjetja ACTUAL I.T.

Pred časom ste nastopili to zahtevno funkcijo, ki ste jo prevzeli od g. Pavla Jazbeca. Predhodnik vam je postavil visoke kriterije, ki jih bo kar zahtevno preseči. Verjetno pa se vedno najdejo dodatne možnosti za izboljšave. Kje vidite težišča na katerih bodo temeljile vaše nadaljnje aktivnosti?

Prevzem te funkcije je zame velik izziv, ki ga jemljem zelo resno. Pavle Jazbec ostaja v naši skupini in s svojim znanjem ter izkušnjami prispeva k strateškem vodenju v okviru upravnega odbora, kar je za nas dragocenega pomena. Moje osrednje težišče dela je usmerjeno v krepitev sinergij znotraj skupine ACTUAL I.T. in zagotoviti optimalno poslovanje naših strank. Menim, da je ključno, da strankam kontinuirano nudimo prilagojene in optimalne rešitve, ki jim omogočajo dosego njihovih poslovnih ciljev. Na trgu bomo še naprej stremeli k nenehnemu izboljševanju naših storitev in rešitev, da ostanemo konkurenčni in ustrežemo spreminjajočim se potrebam.

Strateško varnostno okolje postaja vedno bolj zahtevno. Energetika in logistične dobavne verige so vedno bolj na udaru vplivov kriz s katerim smo soočeni. Kako iz vašega strateškega pogleda ocenjujete trenutno stanje in kakšen vpliv bo to imelo na vašo organizacijo?

Trenutno stanje je stabilno, a to ne pomeni, da se lahko sprostimo. Pomembno je, da nenehno spremljamo nove izzive in se proaktivno prilagajamo. To vključuje dodatne investicije v varnost naše infrastrukture in postopkov, ki jih uporabljamo pri zagotavljanju naših storitev. Poleg tega je nujno krepiti ekipo in spodbujati stalno izobraževanje, da bomo pripravljeni na vse morebitne spremembe in izzive, ki se lahko pojavijo.

Vedno bolj ste s svojimi rešitvami in znanjem prisotni v organizacijah, ki upravljajo s kritično infrastrukturo. Predvsem ste usmerjeni v področje energetike in logistike. Kje vidite posebej izpostavljene izzive v teh konkretnih področjih, ki jih bo potrebno začeti ustrezno naslavljati, če bomo želeli zagotavljati ustrezno neprekinjenost delovanja?

Vlaganje v inovacije, razvoj in umetno inteligenco je ključno za ohranjanje konkurenčnosti, tako na domačem kot tudi na mednarodnem trgu.

*avtor je član Slovenskega združenja korporativne varnosti

Srečujemo se z dvema nasprotujočima si izzivoma. Po eni strani imamo večjo potrebo po povezljivosti in izmenjavi podatkov, kar prinaša nove možnosti in izboljšave. Po drugi strani pa se moramo zavedati večje potrebe po varnosti, saj se število groženj nenehno povečuje. Z večino podjetij aktivno razvijamo rešitve, ki zagotavljajo pogoje za neprekinjeno poslovanje, kar je ključno za njihovo uspešnost in zanesljivost.

Digitalizacija je ena izmed osrednjih težišč, ki jo vse moderne organizacije poskušajo v čim večjem obsegu implementirati v svoje organizacijske in poslovne procese. Kje vidite vašo dodano vrednost, katero prinašate v ta segment s svojimi novimi informacijskimi rešitvami?

V skupini ACTUAL I.T. združujemo vrsto strokovnjakov z različnih področij - infrastrukture, varnostnih rešitev, informacijskih sistemov, poslovnih rešitev, idr., kar nam omogoča celostni pristop k procesu digitalizacije. Zavedamo se, da so izkušnje in znanje naših strokovnjakov ključni za napredno in uspešno izvedbo projektov, kot tudi da lahko zaradi tega »pokrijemo« več področij. Naše rešitve so zasnovane tako, da zagotavljajo celovitost in neprekinjeno poslovanje, kar je še posebej pomembno v današnjem hitro spreminjajočem se svetu.

Dokončna uveljavitev NIS-2 bo na področju kibernetske varnosti prinesla še dodaten pospešek. Kako se na tem področju pripravljate, da boste operativnemu okolju s svojim znanjem in tehnologijami priskočili na pomoč?

Za naše stranke smo organizirali že več izobraževalnih dogodkov, kjer smo predstavili, kaj NIS-2 prinaša in kako se lahko na direktivo pripravijo. Zavedamo se, da nekatera podjetja še oklevajo in ne razmišljajo o tem, zato je izjemno pomembno, da jih ves čas ozaveščamo in o tem izobražujemo. V skupini imamo strokovno usposobljeno ekipo ter interni SOC, kateri so usposobljeni za delovanje najbolj kritičnih sistemov.

Imate občutek, da v Sloveniji premalo pozornosti posvečamo sinergijskim učinkom, ki bi omogočali doseganje boljših rezultatov in višjo stopnjo zagotavljanja kibernetske varnosti?

Strinjam se, da v med podjetnem sodelovanju še vedno prevladuje „boj“ za stranke. Vendar pa znotraj naše skupine zelo dobro razumemo pomen sinergij in dobre prakse. To prenašamo na naše stranke, kar pripomore k večji varnosti in učinkovitosti.

Ste močno usmerjeni v mednarodno okolje in tudi prisotni v pomembnih infrastrukturnih sistemih. Katere so tiste izkušnje in dobre prakse, ki jih lahko prinesete v slovensko okolje?

Naše izkušnje in dobre prakse iz Slovenije prenašamo v mednarodno okolje, kar je pomembno za razvoj in rast. Sodelovanje z lokalnimi partnerji je ključno za zagotavljanje dobre uporabniške izkušnje in on-site podpore. Različni poslovni modeli, ki jih opazimo v mednarodnem okolju, nam omogočajo, da še bolje razumemo in naslavljamo potrebe, tudi tiste, ki jih »doma« še ne obravnavamo.

Področje raziskav in razvoja je posebej izraženo v vaši poslovni viziji. Zakaj se vam zdi pomembno, da temu področju namenjate toliko energije in pozornosti?

Vlaganje v inovacije, razvoj in umetno inteligenco je ključno za ohranjanje konkurenčnosti, tako na domačem kot tudi na mednarodnem trgu. V sodobnem poslovnem okolju se lahko zgodi, da se mnoga podjetja zadovoljijo s trenutnim stanjem in se umaknejo v tako imenovano „cono udobja“. Takšna stagnacija je zavirajoč element trajnostne strategije, saj lahko vodi v izgubo konkurenčne prednosti. Biti v coni udobja se morda zdi enostavno, a v resnici predstavlja resno nevarnost. Podjetja, ki ne vlagajo v inovacije, razvoj in umetno inteligenco, se pogosto znajdejo v položaju, kjer le podpirajo obstoječe stanje, brez pravega napredka. Nasprotno pa razvojno usmerjeni ponudniki aktivno iščejo nove priložnosti in izboljšave, kar jim omogoča, da svojim strankam nudijo konkurenčne prednosti. Zato je raziskava in razvoj za nas naša najpomembnejša prioriteta. Le z nenehnim vlaganjem v ta področja lahko ostanemo relevantni in uspešni, ter zagotavljamo dodano vrednost našim strankam v hitro spreminjajočem se tržnem okolju.

Umetna inteligenca bo tisti dejavnik, ki bo verjetno močno vplival tudi na razvoj vaših produktov in storitev. Je v tem trenutku kaj posebnega na tem področju, kateremu res posvečate veliko pozornosti?

Ustanovili smo kompetenčni center umetne inteligence, kjer deluje 20 strokovnjakov z različnih področij. Osredotočamo se na razvoj lastnih rešitev, ki izkoriščajo umetno inteligenco za zagotavljanje varnega in optimalnega delovanja naših storitev ter v rešitve za izboljšave interne učinkovitosti. ■

Foto: arhiv podjetja ACTUAL I.T.

ACTUAL I.T.
Member of DBA Group Company

KJER SE SREČAJO INOVACIJE IN TRADICIJA.

Največje IKT podjetje na Obali, ACTUAL I.T., ki je del mednarodne skupine, je prepoznano kot privlačen, zanimiv in družbeno odgovoren delodajalec, s katerim lahko ustvarjate prihodnost IT-ja.

Z vami že 30 let

www.actual-it.si

ACTUAL I.T. UNISTAR PRO astec ITELIS ACTUAL I.T. GROUP A DBA Group Company

Avtor: Matic Čaleta / Institut za korporativne varnostne študije

INTERVJU
g. Igor Mlakar, direktor operative v podjetju Smart Com d.o.o.*

UVAJANJE DIREKTIVE NIS 2 BO PRINESLO RESNE KONCEPTUALNE SPREMEMBE NA PODROČJU KIBERNETSKE VARNOSTI

Kibernetska varnost postaja za naša podjetja vedno večji izziv, ki od nas zahteva spremembo razumevanja in popolnoma nove konceptualne zasnove za ustroj našega kibernetskega ekosistema. Še posebej so tukaj izpostavljena industrijska informacijska okolja, kjer so kibernetska tveganja prinesla še dodatne izzive. O odprtih problemih in iskanju potrebnih rešitev smo se pogovarjali z g. Igorjem Mlakarjem.

V podjetju Smart Com opravljate pomembno vlogo direktorja operative, kar v vsaki organizaciji predstavlja njen bistven del. Nam lahko zaupate glavne izzive, s katerimi se trenutno soočate pri operativni izvedbi večjih IKT projektov?

Sodobni projekti na področju informacijsko-komunikacijskih tehnologij vključujejo širok spekter različnih tehnologij, platform in sistemov, ki jih je potrebno integrirati v enovito rešitev. Usklajevanje teh komponent ob sodelovanju več ekip in uporabi različnih virov pogosto vodi v zapletene procese, ki zahtevajo natančno načrtovanje, spremljanje in prilagajanje. Poseben izziv pri vodenju tovrstnih projektov je zagotavljanje skladnosti z izhodiščnimi zahtevami in projektnim načrtom ter pravočasno izvajanje nalog brez nepotrebnih zamud. Vse spremembe je potrebno sproti usklajevati z naročnikom. Dobra in pravočasna komunikacija med vsemi udeleženci na projektu je ključna, saj preprečuje nesporazume in nepotrebno dodatno delo.

Drug pomemben izziv predstavlja zagotavljanje ustreznih virov. Nagel tehnološki razvoj prinaša nove zahteve po vrhunskem znanju in kompetencah, ki pa niso vedno na voljo. Kadar je potrebno pri naročniku umestiti nove, napredne tehnologije, se pogosto pojavi potreba po dodatnem usposabljanju strokovnjakov, kar lahko upočasni izvedbo projekta. Podobne izzive imajo tudi proizvajalci, ki v želji po hitrem vstopu novih rešitev na trg pogosto kasnijo z zagotavljanjem ustreznih informacij in preverjanjem združljivosti novih rešitev z obstoječimi tehnologijami. Tudi sami se soočajo z izzivom usposabljanja strokovnjakov, ki morajo na različnih ravneh zagotavljati podporo za nove tehnologije. Dodatni izziv predstavlja združljivost novih rešitev z obstoječimi sistemi in migracijo podatkov ter funkcionalnosti s starih na nove sisteme. Prav zato je pomembno ohranjati ravnovesje med sledenjem najnovejšim tehnološkim dosežkom in zagotavljanjem stabilnega delovanja celotnega informacijskega okolja ob uvajanju preizkušenih tehnologij. Pri tem se močno zanašamo na dobre prakse in izkušnje sodelavcev, ki jih nenehno vgrajujemo v naše procese. Naša organizacijska vizija temelji na zaveda-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

nju, da z uvajanjem naprednih in varnih informacijsko-komunikacijskih tehnologij uspešno rešujemo sodobne izzive ter omogočamo učinkovito, zanesljivo in varno izvajanje poslovnih in tehnoloških procesov pri naših naročnikih.

Pomemben izziv predstavlja tudi zagotavljanje skladnosti s predpisi, še posebej na področju varovanja podatkov in kibernetske varnosti, kjer se organizacije soočamo z vse strožjo regulativo. Spremembe, kot je aktualna direktiva NIS 2, postavljajo visoke zahteve glede zaščite podatkov, poročanja o kibernetskih incidentih in splošne informacijske varnosti. Vsako odstopanje od skladnosti lahko vodi v resne posledice, kar zahteva nenehno preverjanje in prilagajanje načina delovanja. To vključuje ne le tehnične rešitve, temveč tudi redne presoje, usposabljanja zaposlenih in jasno opredeljene varnostne politike.

Pred nami je uveljavitev nove evropske direktive NIS 2, katere zahteve po višji ravni kibernetske varnosti se bodo prenesle skozi prihajajoči novi Zakon o informacijski varnosti. V Smart Comu ste se specializirali za kibernetsko varnost v okoljih kritične infrastrukture ter industrijskih okoljih. Ob napovedani vključitvi direktive v nacionalno zakonodajo organizacijam pomagate narediti prave korake do skladnosti. Kje vidite glavne izzive, ki jih je pričakovati pri integraciji teh določil v realna okolja?

Ne glede na celoten obseg zahtev, ki jih ni malo in so vsaka zase izjemno pomembne tako za skladnost kot za varnost poslovanja, bi ocenil, da je ozaveščenost deležnikov najpomembnejši element. Hkrati je to največji izziv pri uvajanju zahtev v vsakodnevno poslovanje. V prvi vrsti to velja za poslovodstva. V tistih organizacijah, kjer bodo najodgovornejši posamezniki ponotranjili potrebo po informacijski varnosti kot ključnemu dejavniku konkurenčnosti in uspešnosti poslovanja, bodo organizacije sposobne v celoti izkoristiti tehnološki potencial za zagotavljanje rasti in razvoja. To velja tako za gospodarske družbe kot za upravne organe in institucije, ki bodo z varnejšim poslovanjem in informacijsko ozaveščenim poslovodstvom hitreje uvajale potrebne spremembe za učinkovitejše izpolnjevanje svojega poslanstva. Velik izziv predstavlja tudi sprememba miselnosti strokovnjakov, ki se ne tako redko zapirajo v t.i. „slonokoščene stolpe" samozadostnosti in se težje soočajo z dodatnimi varnostnimi zahtevami in nadzorom. To je še posebej zahtevno pri prepotrebnem povezovanju strokovnjakov z različnih področij. Multidisciplinaren pristop postaja vse pomembnejši za sodobno varovanje informacijskih okolij. Nenazadnje pa takšen pristop uporabljajo tudi napadalci, ki skozi sofisticirane metode socialnega inženiringa, v povezavi z različnimi tehnološkimi orodji, poskušajo doseči svoje cilje.

Zelo močno ste prisotni pri krepitvi kibernetske odpornosti v industrijskih oz. procesnih (OT) okoljih. Z digitalizacijo industrije se je izpostavljenost kibernetskim grožnjam povečala tako zaradi povezovanja industrijske komunikacijske infrastrukture s poslovnim omrežjem na internetu kot tudi zaradi dodatnega števila zaposlenih. Se zaradi teh novih dejavnikov uveljavitev projektov implementacije varnih informacijskih rešitev pri vaših naročnikih podaljšuje ali je to nasploh postal nikoli dokončan razvojni cikel?

Pravilno ugotavljate, da se je izpostavljenost kibernetskim grožnjam v industrijskih oz. procesnih okoljih močno povečala. Procesna okolja, ki so bila pred leti razmeroma izolirana, se vse bolj odpirajo in danes praktično nobeno sodobno procesno okolje ne more delovati povsem ločeno od svetovnega spleta. Če nič drugega, je povezovanje s proizvajalci avtomatiziranih rešitev nujno za sprotno zagotavljanje ustreznih programskih dopolnitev in pomoč pri premagovanju obratovalnih težav. Strokovnjaki znotraj organizacij, ki upravljajo s tovrstno tehnologijo, pogosto nimajo zadostnega znanja s področja IKT niti nimajo potrebnih kompetenc s področja informacijske varnosti. Hkrati strokovnjaki za informacijsko varnost v teh organizacijah pogosto ne poznajo komunikacijskih protokolov, ki se uporabljajo v procesnih okoljih. Tako nastaja vrzel, ki jo lahko napadalci s pridom izkoristijo. Posodabljanje informacijskih rešitev je bilo vedno del razvojnih ciklov, vendar se ti cikli nenehno krajšajo. Še posebej, ko gre za zaščito pred kibernetskimi grožnjami, ne moremo več govoriti o tradicionalnih razvojnih ciklih. V ospredju so rešitve, ki imajo neprekinjeno izboljševanje vgrajeno tako tehnološko kot procesno.

Bi se strinjali s tezo, da nove tehnologije prinašajo tudi nove varnostne izzive in kako se pri tem hitrem tehnološkem razvoju lotevati področja kibernetske varnosti?

Zagotovo. Vsaka sprememba, naj si bo tehnološka, družbena ali okoljska, prinaša dodatne varnostne izzive. Zato je pomembno, da se kibernetske varnosti lotimo celovito, z uporabo konceptov rednega preverjanja in ocenjevanja tveganj, ugotavljanja poslovnih učinkov in preverjanja varnostne zrelosti organizacije na vseh za organizacijo pomembnih področjih uporabe. Na podlagi pridobljenih informacij in ustreznih ocen se lahko poslovodstvo po tehtnem premisleku odloči za uvedbo ukrepov na tistih področjih, kjer organizaciji preti največja grožnja oziroma tam, kjer bo učinek spremembe največji. Organizacija lahko oceno stanja in razmislek opravi sama, lahko pa poišče pomoč pri zunanjih

strokovnjakih za posamezno tehnološko področje ali za presojo in oblikovanje procesov.

Pomembno je, da postane tak način preverjanja stalnica v okviru procesa nenehnega izboljševanja. Vsako spremembo je treba po uvedbi ovrednotiti, da se ugotovi njen dejanski učinek, in po potrebi izvesti korektivne ukrepe za dosego načrtovanega stanja. Eden izmed načinov za spoprijemanje s to izjemno zahtevno nalogo je uporaba metode „13 področij uporabe“, ki smo jo razvili v podjetju Smart Com. Ta metoda načrtno modelira področja uporabe in z ustreznimi prilagoditvami pokriva vse organizacijske vidike katerekoli organizacije. Hkrati v preseku naslavlja vsa področja, ki so ključnega pomena za obvladovanje kibernetskih groženj.

Kateri so tisti ključni gradniki kibernetske varnosti, ki so nujno potrebni za zagotovitev primerne ravni kibernetske varnosti v industrijskih OT okoljih in bi jih skozi svoje bogate izkušnje posebej izpostavili?

Na to vprašanje je težko odgovoriti v nekaj stavkih. Kljub temu bi izpostavil dva ključna pogoja, brez katerih drugi ukrepi ne morejo doseči zadovoljivih rezultatov. Prvi je organizacijski. O tem smo že govorili – potrebno je vzpostaviti ustrezno raven sodelovanja med strokovnjaki za procesne tehnologije in strokovnjaki za IKT. Praviloma brez jasne usmeritve s strani poslovodstva tega cilja ni mogoče doseči. Drugi pogoj je tehnološki. Potrebno je zagotoviti preglednost celotnega procesnega okolja, kar pomeni vzpostaviti nadzor nad vsemi protokoli, ki se uporabljajo v procesnih okoljih in razumeti obnašanje prometnih tokov. Večina rešitev, namenjenih zagotavljanju kibernetske varnosti v okoljih IT, tega ne zmore in zato niso primerne za uporabo v procesnih okoljih. Ko sta ta dva pogoja izpolnjena, se lahko posvetimo ukrepom, kot so segmentacija omrežja, varnostno spremljanje in posodabljanje programske opreme, upravljanje z dostopi in identitetami...

Kako po vašem mnenju uskladiti razvojne dimenzije tako imenovanih »pametnih tovarn« in zagotavljanja in obvladovanja kibernetskih tveganj, ki se pri tem dodatno odražajo?

Takšna uskladitev zahteva celovit pristop, ki vključuje varnost že od same zasnove naprej. Ključno je, da so varnostni ukrepi vgrajeni v vsako fazo razvoja pametnih tovarn - od začetnega načrtovanja, implementacije in delovanja pa vse do končne razgradnje, kar se pogosto zanemarja. Pomembno je upoštevati medsebojno povezljivost naprav, saj pametne tovarne temeljijo na digitalizaciji in avtomatizaciji, to pa povečuje izpostavljenost kibernetskim grožnjam. Ob tem je potrebno poskrbeti za redno preverjanje varnostnih protokolov, šifriranje komunikacij, segmentacijo omrežij in strogo upravljanje z dostopi.

Poleg tehničnih ukrepov je izjemno pomembno izobraževanje zaposlenih ter sprotno spremljanje in ocenjevanje tveganj v realnem času. O potrebi po sodelovanju med oddelki za razvoj in varnost ter o pomenu jasnih usmeritev s strani poslovodstva smo že govorili. Le s takim pristopom lahko zagotovimo varno uvajanje novih tehnologij ter zmanjšanje ranljivosti. Na ta način podjetje ohranja svojo konkurenčnost, hkrati pa se učinkovito zavaruje pred kibernetskimi grožnjami.

Že dolgo časa v strokovni javnosti poudarjamo pomen celostnega pristopa k varnosti za večjo odpornost organizacij. Menite, da so začela strateška vodstva organizacij temu pristopu namenjati ustrezno pozornost?

Čeprav na tem področju ostaja še veliko prostora za izboljšave, bi rekel, da poslovodstva uspešnih organizacij zelo dobro razumejo pomen vlaganja v ustrezno raven informacijske varnosti in zaščite pred kibernetskimi grožnjami. Zavedajo se, da je celovit pristop ključen ne le za zaščito podatkov, temveč tudi za dolgoročno odpornost in stabilnost poslovanja. Predvsem pri poslovnih subjektih to predstavlja tudi konkurenčno prednost na trgu. Uvedba zahtev direktive NIS 2 bo organizacije še dodatno spodbudila k izgradnji robustnejših varnostnih sistemov ter prispevala k bolj strateškemu pristopu k obvladovanju kibernetskih tveganj. Varnost bo tako postala ena izmed prednostnih nalog v poslovnih strategijah. ■

Foto: Aleš Rosa

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

SMART COM

Zagotovite varno, zanesljivo in odgovorno digitalno prihodnost

https://bit.ly/skladnost-NIS2

- Smart Center upravljanih varnostnih in omrežnih storitev
- Kibernetska varnost v poslovnem in industrijskem okolju in okolju kritične infrastrukture
- Sodobna omrežja nove generacije za odlično uporabniško izkušnjo

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

KAKO BO DIREKTIVA NIS 2 VPLIVALA NA PRIHODNOST KIBERNETSKE VARNOSTI

Namen Direktive o varnosti omrežij in informacij 2 (NIS 2) je bistveno izboljšati kibernetsko varnost in odpornost organizacij v Evropski uniji. V primerjavi s prejšnjo direktivo, NIS 2 širi svoj obseg, zajema več sektorjev in poudarja potrebo po dosledni in usklajeni izvedbi v vseh državah članicah EU.

Namen izvirne direktive NIS iz leta 2016 je bila vzpostavitev celovitega regulativnega okvira za kibernetsko varnost v EU, a je neenotna izvedba na ravni držav članic v preteklih letih onemogočila, da bi direktiva zaživela v praksi. Kot odgovor na naraščajoče kibernetske grožnje, povezane z digitalno preobrazbo, ki jih je Agencija Evropske unije za kibernetsko varnost (ENISA) identificirala v svojem poročilu o grožnjah leta 2022 (grafika desno), je EU uvedla direktivo NIS 2 z namenom dviga standardov kibernetske varnosti in spodbude večje usklajenosti med državami članicami EU. NIS 2 tako kot NIS od držav članic zahteva, da pripravijo nacionalne strategije kibernetske varnosti in imenujejo pristojne organe za obvladovanje varnostnih incidentov. Obenem direktiva NIS 2, za razliko od svoje predhodnice, nalaga strožje varnostne obveznosti ter poročanje s strani podjetij in povečuje nadzor s strani nacionalnih organov.

Skica: 8 največjih groženj v letu 2022 po podatkih ENISE

Vloga NIS 2 pri izboljšanju nacionalne kibernetske varnosti

Za razliko od prvotne direktive NIS morajo direktivo NIS 2 v državno zakonodajo prenesti vse države članice EU. Čeprav lahko med postopkom sprejemanja nastanejo manjše razlike med državami članicami, ključne zahteve ostajajo dosledne in univerzalno uporabne. Obenem se pa pristopi uveljavljanja direktive v praksi v državah članicah bistveno razlikujejo. Nekatere države dajejo prednost obveznim revizijam, ki zajemajo vse elektronske informacijske sisteme (EIS), druge pa se osredotočajo le na sisteme, povezane z jedrnimi poslovnimi funkcijami ali specifičnimi sektorji. Obenem lahko države izberejo tudi poenostavljen pristop, ki zahteva samo splošno sprejete certifikate, kot je recimo ISO27001.

Primer: Madžarska je objavila podroben seznam tehničnih in organizacijskih ukrepov, ki jih je razvrstila po razredu varnostnega tveganja EIS. Seznam vključuje tudi neobvezne dopolnilne ukrepe.

Vse organizacije morajo v okviru NIS 2 obvezno poročati o incidentih svojemu nacionalnemu odzivnemu centru za kibernetsko varnost (CSIRT), ki mora nato informacije o incidentu posredovati EU CyCLONe, organu EU, ki je odgovoren za usklajevanje kibernetskih incidentov in kriznega upravljanja. Ta obveznost povečuje splošno odpornost z:

- izboljšanjem sodelovanja in poročanja m

ed državami članicami EU in organi za kibernetsko varnost;

- boljšimi vpogledi v trende incidentov z bolj natančnimi podatki ENISE;
- okrepljenimi mehanizmi za zaznavanje in odzivanje na čezmejne grožnje, kar omogoča hitrejše prepoznavanje in omilitev obsežnih kibernetskih napadov.

Pristop, ki temelji na tveganju: osredotočanje na kritične informacije

Temelj NIS 2 je upravljanje s tveganji. Direktiva ključnim sektorjem nalaga sprejem proaktivnega pristopa za obvladovanje kibernetskih tveganj s posebnim poudarkom na kritičnih sredstvih. Ključne zahteve glede upravljanja s tveganji so:

- Celovita strategija upravljanja s tveganji: Organizacije morajo uvesti zanesljivo strategijo upravljanja s tveganji, ki zajema identifikacijo, oceno in omilitev tveganj za njihove informacijske sisteme in omrežja. Strategija mora vključevati tudi zunanje dobavitelje, saj se lahko le tako zagotovi varnost dobavne verige. Sama strategija ni dovolj; podprta mora biti s konkretnim izvedbenim načrtom, ki strategijo prevaja v izvedljive korake.

- Specifične zahteve sektorja: Organizacije morajo upoštevati specifične grožnje in zahteve po skladnosti, ki so edinstvene za panogo, v kateri delujejo. (Primer: Storitve v finančnem sektorju morajo biti skladnje z Uredbo o digitalni operativni odpornosti, DORA).

- Prepoznavanje kritičnih informacijskih sredstev: Glede na omejene vire morajo organizacije prioritetno zaščititi svoje najbolj kritične sisteme. Za zagotovitev celovite zaščite pa je nujno uporabiti (vsaj) osnovno raven zaščite v vseh sistemih.

Krepitev dobavne verige

Glede na rezultate raziskave, ki jo je leta 2021 izvedla ENISA, kar 57 % malih in srednje velikih podjetij (MSP) verjame, da bi lahko zaradi kibernetskega napada bankrotirali. To poudarja velik vpliv, ki ga lahko imajo tovrstni incidenti na MSP. Poleg neposrednih posledic za prizadeta MSP, kibernetski napadi vplivajo tudi na zaupanje v poslovne operacije in motijo širši proces digitalne preobrazbe po Evropi. Učinek kibernetskih napadov na MSP lahko tako znatno škoduje gospodarstvu EU.

Kibernetska varnost MSP je posebej kritična za varnost nacionalnih in evropskih dobavnih verig. Kibernetska varnost dobavne verige se nanaša na odpornost vseh podjetij, izdelkov in storitev, vključenih v dobavo končnega izdelka ali rešitve končnemu uporabniku. Skrbi dejstvo, da se je število napadov na dobavne verige močno povečalo. ENISA v poročilu o grožnjah za leto 2022 razkriva, da so takšni napadi predstavljali 17 % vseh kibernetskih napadov v letu 2022. Gre za drastično povečanje, saj so tovrstni napadi v letu 2021 predstavljali zgolj 1 % kibernetskih napadov. Številne kršitve, ki ogrožajo omrežja ali podatke strank, so povezane z ranljivostmi v varnostnih sistemih dobaviteljev.

Izboljšanje kibernetske varnosti MSP bo pomembno okrepilo skupno odpornost EU na kibernetske napade. MSP so ključni za kritične sektorje evropskega gospodarstva, saj zagotavljajo ključne izdelke in storitve industrijam, kot so javne službe in IT. Kibernetski kriminal pogosto cilja prav na ta manjša in bolj ranljiva podjetja, saj jim odpirajo pot za vdor v večje in bolj varne sisteme. Reševanje vrzeli v kibernetski varnosti znotraj MSP je tako skupna odgovornost, kjer lahko NIS 2 zagotovi ključno podporo.

NIS 2 daje velik poudarek ocenam in upravljanju tveganj v dobavni verigi, pri čemer od vseh vključenih subjektov zahteva, da opravijo temeljit pregled svojih dobaviteljev. Ta podjetja morajo zagotoviti, da njihovi dobavitelji upoštevajo napredne ukrepe kibernetske varnosti – tako tehnične kot organizacijske. V nekaterih primerih lahko od vključenih subjektov zahtevajo, da uporabljajo certificirane izdelke ali storitve, ki ustrezajo priznanim certifikatom kibernetske varnosti, kar zagotavlja, da rešitve, ki jih sprejmejo, izpolnjujejo visok standard varnosti.

NIS 2 ureja tudi odgovornost za zagotavljanje varnosti dobavne verige. Dobavitelji, ki spadajo v obseg NIS 2 ali že vzdržujejo celovite sisteme upravljanja s kibernetsko varnostjo, so v izraziti prednosti. Te organizacije običajno lažje podpisujejo podrobne pogodbe o kibernetski varnosti in lahko dokažejo svojo zrelost z ustreznimi certifikati, kot so certifikati izdelkov ali skladnost z industrijskimi standardi, kar jim zagotavlja konkurenčno prednost.

Medtem ko NIS 2 vpliva predvsem na subjekte nad določeno velikostjo (na podlagi števila zaposlenih ali finančnega prometa), so lahko manjša podjetja izvzeta iz neposrednega nadzora. Vendar je za MSP prav tako ključnega pomena, da izvajajo stroge ukrepe na področju kibernetske varnosti. Pri tem jim lahko pomagajo smernice EU institucij, posvetujejo se lahko z mrežo EDIH (DIGI-SI) ali pa praktične nasvete poiščejo v **vodniku o kibernetski varnosti**, ki si ga lahko prenesejo s pomočjo QR kode:

Izzivi in priložnosti za organizacije

Pomanjkanje usposobljenih strokovnjakov za kibernetsko varnost je ena izmed največjih težav s katero se srečujejo organizacije. Povečana potreba po strokovnem znanju, ki jo narekujejo zahteve po skladnosti z NIS 2, pa je še povečala to težavo. Izboljšanje znanj zaposlenih v podjetju lahko predstavlja rešitev za podjetja, ki ne morejo najeti ekspertnih strokovnjakov ali ekip za kibernetsko varnost. Okvir veščin za kibernetsko varnost, ki ga je izdala ENISA, ponuja dragocene informacije, vključno s predhodno razvitimi opisi delovnih mest, učnimi materiali in priložnostmi za izobraževanje, ki pomagajo kadrovskim ekipam in organizacijam pri reševanju vrzeli v znanju.

Skladnost z NIS 2 zahteva tudi sodelovanje med različnimi poslovnimi funkcijami, vključno s pravnimi službami, strokovnjaki za skladnost in strokovnjaki za IT, močno podporo pa jim mora nuditi tudi vodstvo podjetja. Vodstvo mora biti ves čas seznanjeno z napredkom pri sprejemanju in uvajanju nacionalne zakonodaje, zlasti v zvezi z izvedbenimi akti in podrobnimi predpisi.

Poleg skladnosti pa NIS 2 organizacijam predstavlja priložnost za izboljšanje svojega položaja kibernetske varnosti med prizadevanji za digitalno preobrazbo. Novi digitalni sistemi in procesi morajo biti v skladu z zahtevami kibernetske varnosti NIS 2, kar lahko služi kot temelj za gradnjo bolj varne digitalne prihodnosti.

In zaključek?

Medtem ko mnoga podjetja NIS 2 dojemajo kot veliko breme skladnosti, pa nova direktiva prinaša tudi številne prednosti, saj predvideva krepitev nacionalne kibernetske varnosti in izboljšanje odpornosti dobavne verige, hkrati pa uveljavlja tudi sprejetje tehničnih in organizacijskih ukrepov ter spodbuja pristop h kibernetski varnosti, ki temelji na oceni tveganja. Čeprav je zahtevna in kompleksna, direktiva NIS 2 že prejema pomembno pozornost deležnikov.

V naslednjih petih letih večjih sprememb zakonodaje, razen manjših prilagoditev na nacionalni ravni, ni pričakovati. V tem času bodo EU in države članice spremljale izvajanje, vzdrževale stalen dialog s prizadetimi podjetji in ocenjevale učinek direktive.

Komu NIS 2 prinaša največ koristi? Navsezadnje bodo prebivalci EU tisti, ki bodo uživali v varnejših digitalnih izdelkih in storitvah, boljši zaščiti podatkov in povečanju zaupanja v digitalni ekosistem. ■

Vodnik z vprašanji in odgovori

Spodbujanje kibernetske varnosti za MSP v Evropi

Global Digital Foundation
The Digital Policy Network

eit Digital
Co-funded by the European Union

HUAWEI

Avtor: Matic Čaleta / Institut za korporativne varnostne študije*

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

KLJUČNO JE RAZUMEVANJE POMENA EVROPSKEGA TEHNOLOŠKEGA RAZVOJA

Celovito obvladovanje varnostnih tveganj ni več možno le s stališča posameznih domen ali sektorjev. Zaradi tega je ključno iskanje rešitev v smeri, katero zagotavljajo razvojna evropska podjetja skozi naslavljanje različnih povezanih izzivov. Dodatna pomembna točka pa so ukrepi pri zagotavljanju varnosti dobavne verige, ki jih podjetja, stacionirana v Evropi, mnogo lažje zagotavljajo za kritične subjekte naših družbenih okolij. O teh strateških pristopih smo se pogovarjali z g. Janom Veršnikom.

Letos v globalnem podjetju praznujete 30. obletnico delovanja, kar pomeni častitljiv jubilej. Ob tem vam iskreno čestitamo. Kako se je ta obletnica odrazila skozi aktivnosti letošnjega leta? Ste ta jubilej obeležili tudi v Sloveniji?

Hvala za vaše čestitke! Ob praznovanju 30. obletnice ASSA ABLOY so se v podjetju zvrstile različne prireditve, vključno s slovesnostmi, ki so potekale na različnih lokacijah po svetu. Te prireditve so bile namenjene tako zaposlenim kot strankam in partnerjem, da bi skupaj proslavili našo rast in dosežke.

V Sloveniji smo obletnico obeležili tako, da smo organizirali več manjši dogodkov, na katerih smo predstavili naše inovacije in rešitve ter se zahvalili našim strankam in partnerjem za njihovo zvestobo. Zaposleni v Sloveniji smo imeli priložnost sodelovati na različnih internih dogodkih, kjer so se spomnili dosežkov podjetja in se veselili prihodnosti.

Varnostno okolje in tveganja postajajo vedno bolj kompleksna, kar od ponudnikov tehnologij zahteva vedno hitrejši razvoj celovitih rešitev, ki so usmerjene v zagotavljanje varnosti na celotnem spektru varnostnih segmentov. Kako oblikujete svoj tehnološki portfelj, ki ga ponujate svojim uporabnikom v Sloveniji? Gre po principu zaznanih potreb strank ali analizirate specifična varnostna tveganja in se s produkti prilagajate tem analizam?

V ASSA ABLOY Slovenija se zavedamo, da postaja varnostno okolje vse bolj kompleksno in da se potrebe strank nenehno razvijajo. Zato pristopamo k oblikovanju našega tehnološkega portfelja na sistematičen in strateški način.

Redno spremljamo globalne tržne trende, nove tehnologije in spreminjajoče se regulative v različnih industrijah. Sodelovanje z mednarodnimi ekipami, deljenje znanja in inovacij ter dobre prakse iz drugih trgov pripomorejo k oblikovanju našega portfelja in implementaciji uspešnih rešitev v Sloveniji.

Pri razvoju naših rešitev je vedno tesno sodelovanje s strankami. To vključuje zbiranje povratnih informacij, sodelovanje z uporabniki in razumevanje njihovih konkretnih potreb in pričakovanj. Naš portfelj vključuje široko izbiro rešitev, ki jih nenehno prilagajamo in izboljšujemo.

Ta kompleksnost in soodvisnost varnostnega okolja in različnih sektorjev verjetno pomeni, da morate rešitve razvijati s smeri uporabnosti in integracije za celoten sklop različnih sektorjev brez ozkih omejitev na posamezne segmente?

*avtor je član Slovenskega združenja korporativne varnosti

Opažam, da se varnostno zavedanje v slovenskih podjetjih postopoma povečuje, vendar še vedno obstajajo področja, kjer je potrebna dodatna pozornost in usposabljanje.

Da, natančno tako. Varnostno okolje je danes izjemno kompleksno in soodvisno. Stremimo k temu, da so rešitve interoperabilne z obstoječimi sistemi drugih ponudnikov, kar omogoča, da jih lahko stranke enostavno integrirajo v svoj ekosistem brez potrebe po popolni zamenjavi sistemov. To zmanjša stroške in poveča učinkovitost.

Razvijamo rešitve, ki omogočajo enotno upravljanje različnih vidikov varnosti, kot so fizična zaščita, varnost in kontrola dostopa. Takšna integracija omogoča strankam, da na enostaven način upravljajo svojo varnost in odgovorijo na morebitna tveganja in grožnje.

Naše rešitve so zasnovane tako, da jih lahko enostavno prilagodimo specifičnim potrebam posameznih strank, ne glede na to, v katerem sektorju delujejo.

Kateri so tisti tehnološki segmenti, kjer ste s svojimi varnostnimi rešitvami še posebej prisotni v Republiki Sloveniji?

Korporacija je v Republiki Sloveniji prisotna v več tehnoloških segmentih, kjer nudi rešitve za kontrolo dostopa, ki vključujejo programsko opremo za upravljanje in strojno opremo, kot so elektronski cilindri, pametne kljuke, čitalci in električne ključavnice. Ti sistemi omogočajo podjetjem, da učinkovito upravljajo s tem kdo ima dostop do katerih območij in tako zmanjšajo varnostna tveganja.

Prav tako nudimo širok spekter avtomatskih, protipožarnih in varnostnih vrat, ki zagotavljajo fizično zaščito. K temu dodajamo tudi različne varnostne elemente, kot so protivlomni in protipožarni sistemi ter dodatki, ki izboljšajo splošno varnost.

Imate občutek, da je v slovenskih podjetjih dovolj visoko varnostno zavedanje, ki zagotavlja, da so koraki za obvladovanje ključnih varnostnih tveganj v teh organizacijah na ustreznem nivoju?

Opažam, da se varnostno zavedanje v slovenskih podjetjih postopoma povečuje, vendar še vedno obstajajo področja, kjer je potrebna dodatna pozornost in usposabljanje.

Kljub temu, da se varnostno zavedanje v slovenskih podjetjih izboljšuje, je potrebno še dalje dvigovati zavedanje o pomenih celovitih varnostnih strategij in nenehnega izobraževanja. V podjetju ASSA ABLOY Slovenija se trudimo prispevati k temu z izobraževalnimi iniciativami, delavnicami in svetovanjem, da bi pomagali podjetjem bolje razumeti in obvladovati varnostna tveganja v sodobnem poslovnem okolju.

Danes je eden od zelo izpostavljenih dejavnikov tudi varnost globalne dobavne verige. Glede na to, da vaša korporacija izvorno predstavlja Evropsko podjetje, pomeni tudi, da imate določene konkurenčne prednosti glede obvladovanja teh izzivov neprekinjene dobave kritičnih delov. Opažate, da je ta dejavnik pri vaših stran-

kah postal pomemben vidik na katerem se odločajo za implementacijo določenih varnostnih rešitev?

Da, varnost globalne dobavne verige je v zadnjih letih postala ključen dejavnik za številne organizacije, vključno z našimi strankami. S povečanjem kompleksnosti in ranljivosti dobavnih verig so stranke začele bolj pozorno spremljati, kako se podjetja, s katerimi sodelujejo, spopadajo z izzivi obvladovanja dobavne verige in zagotavljanjem neprekinjene dobave kritičnih delov.

Kot evropsko podjetje imamo razumevanje lokalnih tržnih razmer, regulativ in potreb, kar omogoča hitrejše in bolj prilagojene rešitve za stranke. S tem se povečuje zaupanje strank v sposobnost podjetja, da zagotovi dosledno in varno dobavo.

Zavezani smo k varnosti v vseh vidikih svojega poslovanja, vključno z dobavnimi verigami. Podjetje vlaga v rešitve in procese, ki zmanjšujejo tveganja, povezana z dobavnimi verigami, kar strankam omogoča, da se počutijo varne pri izbiri naših rešitev.

V EU smo v zadnjem obdobju dobili nekaj pomembnih pravnih predpisov, ki močno vplivajo tudi na razvoj in uporabo varnostnih produktov. Naj omenim samo nekatera področja kot so kritična infrastruktura, kibernetska varnost, varstvo osebnih podatkov, umetna inteligenca in še bi lahko naštevali. Kako močan dejavnik za oblikovanje razvoja tehnologij in tudi trga varnostnih rešitev predstavljajo ti pravni okviri? Ali uspete zagotavljati skladnost z vsemi zahtevami?

Pravni okviri, ki jih omenjate, so izjemno pomembni za razvoj in uporabo varnostnih produktov, ter igrajo ključno vlogo pri oblikovanju strategije našega podjetja. Ne le da te regulative postavljajo določene standarde, ampak tudi oblikujejo tržne pogoje in pričakovanja strank.

Naša zaveza zagotavljanju skladnosti z regulativami in standardi je ključen del naše strategije, saj želimo, da stranke zaupajo našim rešitvam in se lahko osredotočijo na svoje osnovne dejavnosti, medtem ko mi skrbimo za njihovo varnost in skladnost z zakonodajo. S tem pristopom ASSA ABLOY ne le da izpolnjuje zakonodajne obveznosti, ampak tudi dela na povečevanju zaščite in zaupanja v varnostne rešitve, ki jih ponujamo.

Dnevi korporativne varnosti so zelo izpostavljen strateško strokovni dogodek v Sloveniji in širši regiji. Kaj vam pomeni ta strokovni kanal za posredovanje vaših dobrih praks v ciljna okolja?

Dnevi korporativne varnosti nudijo platformo za povezovanje z drugimi strokovnjaki, podjetji in ključnimi odločevalci v industriji. To nam omogoča, da gradimo strateška partnerstva ter izmenjujemo ideje in prakse, kar prispeva k izboljšanju skupne ravni varnosti v Sloveniji in regiji. Prav tako nam dogodek omogoča, da predstavimo naše najnovejše inovacije in tehnološke rešitve podjetja na področju varnosti. ■

ohranite neprekinjeno delovanje kritične infrastrukture

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

ALCEA

ASSA ABLOY

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Dušan Podbelšek, inž. str., vodja projektive Zarja Elektronika, d.o.o.*

POŽARNA VARNOST SONČNIH ELEKTRARN

V zadnjem obdobju smo priča povečanemu številu požarov na sončnih elektrarnah, ki poleg škode na samem postrojenju sončnih elektrarn, povzročajo veliko škode tudi na objektih, na katerih so le te postavljene. Če vzamemo v obzir, da so omenjene elektrarne postavljene tudi na pomembnih infrastrukturnih objektih, nas lahko upravičeno skrbi, da smo pri načrtovanju obvladovanja tveganj spregledali pomembno varnostno tveganje, ki se kaže skozi povečano požarno ogroženost teh postrojenj. O problematiki smo se pogovarjali s strokovnjakom s tega področja g. Podbelškom.

V zadnjem obdobju smo lahko priča odmevnim primerom požarov na sistemih sončnih elektrarn. Naj omeniva primer požara na Osnovni šoli v Tržiču ali pa požar v Zavrhu pod Šmarno goro. Kaj je po vašem mnenju glavni razlog za te dogodke? Kateri so najpogostejši vzroki požara sončnih elektrarn?

O nameščanju sončnih elektrarn (v nadaljevanju »SE«) se bolj intenzivno govori v zadnjih letih in tudi spodbude na tem področju so vedno večje. Investicije v »SE« in vizija tako imenovane »samooskrbe« pa sega že krepko pred leto 2010. Kot ugotavljajo strokovnjaki na tem področju, fotovoltaični paneli (PV) predvsem s staranjem predstavljajo požarno tveganje. Nevarnost v sklopu »SE« predstavljajo poškodovani moduli, oksidirani spoji električnih instalacij, kabelske povezave in pregrevanje razsmernikov. Požar na »SE« je lahko posledica več dejavnikov, kot je slaba namestitev, okvarjeni deli, električni obloki, prenapetost, vremenski vplivi in tudi glodavci.

Požari na »SE«, ki smo jih v javnosti zasledili v zadnjem obdobju, so požari večjih razsežnosti. O manjših začetnih požarih in na manjših sistemih »SE« javnost niti ni obveščena. Na odmevnost požara v javnosti pa vpliva razsežnost požara, ki pa je odvisna tudi, kje je sama »SE« nameščena.

Kot navaja stroka na tem področju, analize požarov po svetu kažejo, da do požarov prihaja predvsem na starejših »SE«, po 10 letih in več uporabe. Najbolj pogost vzrok požara je električni oblok na visoko-napetostnih linijah enosmernega toka, do katerega lahko pride zaradi dotrajanosti sistema. S tem lahko govorimo o staranju »SE«, zato je ključnega pomena preventiva in ustrezno vzdrževanje. Poudariti je potrebno, da mora biti že sam začetek namestitve »SE« tehtno premišljen, kam in kako se namešča. Vrsta objekta je lahko ključnega pomena tudi pri samem vzdrževanju sistema. Ni moč enačiti »SE« postavljeno na stanovanjsko hišo, šolo ali hlev.

Kakšni so pogoji ob namestitvi sončnih elektrarn? Kaj pravi zakon o varstvu pred požarom in kakšne so smernice na tem področju?

Pogoje za namestitev sončne elektrarne opredeljuje Zakon o varstvu pred požarom, Pravilnik o požarni varnosti v stavbah, kjer med drugim 23. člen (graditev objektov) v 4 odstavku navaja *»Sončne elektrarne in druge naprave, ki proizvajajo električno energijo iz obnovljivih virov, se lahko v skladu s predpisi o energetski infrastrukturi montira in vgradi na objekte po predhodni strokovni presoji, s katero se dokaže, da se zaradi take energetske naprave požarna varnost objekta ne bo zmanjšala«.*

Pri načrtovanju postavitve »SE« je potrebno upoštevati tudi Tehnično smernico - TSG-1-001:2019 in pa smernico SZPV 512 – Smernica o požarni varnosti sončnih elektrarn, ki je namenjena investitorjem in projektantom kot vodilo pri prepoznavanju nevarnosti in kot pripomoček za izbiro ustreznih tehničnih rešitev.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Če se mogoče malo bolj dotakneva smernic na tem področju. Kakšne so osnove načrtovanja, posebne in dodatne zahteve s stališča požarne varnosti?

Vsi vpleteni v investicijski projekt (investitor, projektant, izvajalec) se morajo zavedati pomena požarne varnosti.

Pri načrtovanju sistema mora projektant upoštevati veljavno zakonodajo in standarde. Smernica SZPV 512 daje osnovne usmeritve za preprečevanja nastanka požara, preprečevanje širjenja požara po objektu in na sosednje objekte, omogočanje varnega gašenje, ki je v teh primerih še posebej oteženo. Smernica daje osnovne napotke ustreznega načrtovanja, izvedbe in vzdrževanja »SE« ter podaja minimalne zahteve posameznih elementov in konstrukcij kamor se lahko namesti »SE« s pripadajočo inštalacijo. Smernica sama eksplicitno ne zahteva namestitev naprav za samodejno odkrivanje in javljanje požara, lahko pa to zahteva načrt požarne varnosti, ki mora biti za tovrstne sisteme izdelan. Za samo varnost delovanja »SE« je pomemben del izvedbe tudi izbira ustrezno usposobljenega izvajalca. Odgovornost uporabnika sistema je skrb nad sistemom z rednimi vzdrževanji in preventivnimi pregledi. Uporabnikova redna kontrola povečuje možnost, da se napake ugotovijo že zelo zgodaj. Pri odkrivanju napak pa nam lahko bistveno pomagajo tudi posamezni tehnični sistemi, med drugim tudi sistem za zgodnje odkrivanje in javljanje požara.

Kdo potrjuje ustreznost izvedbe sončnih elektrarn s področja požarne varnosti?

Pomembno vlogo pri načrtovanju in nameščanju »SE« ima dejstvo, da so naprave, ki proizvajajo električno energijo s pomočjo sončne energije z nazivno močjo do vključno 1MW, uvrščene med enostavne naprave za proizvodnjo električne energije. V skladu s predpisi šteje njihova montaža za investicijsko-vzdrževalna dela. Pri predpostavki, da se investicija izvaja kot »investicijsko vzdrževalna dela« pa za postavitev »SE« zadostuje zgolj ustrezna presoja, ki jo predvideva Uredba o energetski infrastrukturi in ni potrebe po gradbenem dovoljenju. Hkrati po Zakonu o graditvi objektov ni potrebno izdelati zasnove požarne varnosti. V tem primeru je odgovornost postavitve »SE« v celoti prepuščena investitorju in izvajalcu, kakor tudi celotno področje požarne varnosti. Ker so postopki s tem bistveno enostavnejši, se to tudi s pridom izkorišča z izvedbami v več izvedbenih fazah oziroma več manjših ločenih izvedbah.

Pri postavitvi »SE« nazivne moči večje od 1MW je potrebno pridobiti gradbeno dovoljenje po Zakonu o graditvi objektov. Del tega je izdelava zasnove požarne varnosti oziroma študije požarne varnosti. Temu sledi celotno načrtovanje požarno varnostnih ukrepov in same izvedbe.

Če je potrebno pridobiti gradbeno dovoljenje, je potrebno po izvedbi pridobiti tudi uporabno dovoljenje. To pomeni, da mora biti izveden tehnični pregled, na katerem mora biti strokovnjakom organa, ki izdajajo uporabno dovoljenje, predložena predpisana dokazila o izpolnitvi načrtovanih ukrepov tudi s področja zahtevanih ukrepov požarne varnosti.

Ker pa je običajno, da pogosto razvoj prehiteva zakonodajo, je prav skrb vzbujajoče dejstvo, da se na trgu že pojavljajo mikro mobilni solarni sistemi z lastnim hranilnikom energije, ki ga lahko postavimo tudi na teraso ali balkon stanovanja, z ne zavedanjem rizika, ki ga taka investicija lahko prinese. V mislih imejmo samo požar električnega skiroja v stanovanju, ki se je nedavno zgodil v Srbiji ali pa požar električnega kolesa poštnega uslužbenca na poti.

Ali kakšna institucija skrbi za zagotavljanje in preverjanje varnosti delovanja že zgrajenih in delujočih sončnih elektrarn? Kakšne so vaše ugotovitve stanja požarne varnosti naših sončnih elektrarn?

Ko se za izvedeno »SE« pridobi dovoljenje za obratovanje, prevzame odgovornost za pravočasno in pravilno izvedbo vseh ukrepov, potrebnih za varno uporabo, lastnik. To velja tako za redno vzdrževanje kot investicijsko-vzdrževalna dela. Na napravi, ki ni redno vzdrževana se lahko poveča nevarnost za

nastanek in širjenje požara. Uporabnikova redna preventivna kontrola daje možnost ugotovitve napak že zgodaj. Servisna služba pa lahko napako na sistemu odpravi, če je o njej obveščena.

Ali obstajajo na trgu sistemi za javljanje požara in alarmiranje na, ki bi lahko v celoti preprečili tovrstne dogodke?

Na trgu obstajajo naprave in sistemi za uspešno zaznavanje požarov na sistemih »SE«, nikakor pa dogodkov ne morejo v celoti preprečiti. Za celovito preprečevanje tovrstnih dogodkov je potrebno nenehno skrbeti za preventivo in izboljšave. To pa lahko naredimo le skupaj z zakonodajo, proizvajalci, izvajalci, nadzornimi službami in uporabniki sistemov.

Do sedaj se v večini dogodki odkrijejo z vizualnim opažanjem ljudi v okolici, kar pa je običajno prepozno. Trenutno je v praksi zelo slabo razvita miselnost, da je preventiva ključna, predvsem pa se vse usmerja v miselnost stroškov preventivnih ukrepov in vgradnje zgolj tistega, kar je zakonsko obvezujoče. Na zakonodajnem področju, bi se lahko z jasnejšimi predpisi, strožjo zakonodajo in nadzorom, močno pripomoglo k večji požarni varnosti sistemov »SE«.

Ali so taki sistemi predpisani oziroma jih zajema kakšen standard na tem področju?

Če je vgradnja sistema aktivne požarne zaščite zahtevana skladno z načrtom požarne varnosti oziroma študijo požarne varnosti, potem so osnovna izhodišča projektanta na tem delu zahteve iz študije požarne varnosti. Oprema, po kateri se posega, pa mora biti skladna in certificirana po standardu EN-54, ki velja za to področje. Pri izbiri ključnih komponent sistema je predvsem ključno, da se zaupa stroki na področju aktivne požarne zaščite in projektantom, ki morajo prepoznati možne potencialne nevarnosti nastanka požara. Ni neke splošne definicije, kaj se uporabi in v kateri dotični točki. V večini je odločitev odvisna od samega koncepta postavitve »SE«, vrsta objekta, razporeditve modulov, potencialne nevarnosti, dostopi za montažo ter redno vzdrževanje in seveda varno ter brezhibno delovanje tudi v posebnih vremenskih pogojih.

Če se malo bolj poglobiva v sisteme za javljanje požara, jih lahko malo podrobneje opišete? Kateri so glavni sestavni sklopi?

Sistem javljanja požara delimo na komponente za zaznavanje požara, ki so lahko na osnovi detekcije dima, temperature, odprtih plamenov, IR sevanja. Sledijo elementi za alarmiranje in elementi za krmiljenje drugih sistemov ter naprav, ki lahko brez ustreznih krmiljenj in nadzora vplivajo na potek požara na posameznem objektu. Vse te naprave povezuje tako imenovana požarna centrala, ki skrbi za celovito delovanje in nadzor nad sistemom kot celota. Sistemi morajo biti ustrezno certificirani ter redno vzdrževani.
Pri skrbi za aktivno požarno varnost objekta je ključno, da se aktivna požarna zaščita obravnava kot celota, le tako se lahko objektu poveča varnost.

Katere produkte sistemov javljanja požarov na sončnih elektrarnah razvijate v vašem podjetju? Kakšne prednosti prinašajo?

Kot najboljše priporočilo je zaznavanje povišane temperature, ki lahko nastane kot posledica napak na sistemu. Najbolj izrazit in tudi pogost je prav električni oblok. V ta namen se uporablja tako imenovani linijski javljalnik temperature – Protectowire, ki zaznava toploto kjerkoli po svoji dolžini. Ima nespremenljivo mejno temperaturo in sproži alarm, ko je dosežena nazivna temperatura. Primeren je za nameščanje v težka območja, kar pa streha objekta vsekakor predstavlja.

Druga boljša napredna tehničnih rešitev je uporaba D-LIST sistema javljanja toplote, ki temelji na pridobivanju podatkov iz številnih temperaturnih senzorjev, ki so vgrajeni v sistemski senzorski kabel. Polprevodniški temperaturni senzorji so nameščeni znotraj senzorskega kabla na izbirnih intervalih. Temperaturna občutljivost posameznega senzorja je lahko do 0,1°C natančno, merilno območje je od -40°C do +120°C. Lokacija alarmnega dogodka je lahko določena zelo natančno in je odvisna od izbranih intervalno vgrajenih senzorjev. D-LIST kabel je odporen na ekstremna okolja in primeren za vgradnjo povsod, kjer običajna oprema za javljanje požara ni primerna in je potreba po natančnem zaznavanju toplotnih odstopanj.

Nadzore nad sistemi se izvaja tudi z HOTSPOT IR javljalniki toplote z infrardečo merilno tehnologijo in inteligentno analizo signala ali pa z naprednimi javljalniki odprtega plamena in tudi termovizijskimi nadzori.

Bistvo uspešnega sistema je, da je vgrajen na nivoju zaznavanja požara v najzgodnejši začetni fazi, kar lahko z ustreznim krmiljenjem in alarmiranjem preprečimo, da do razvitega požara ne pride.

Ne zadovoljimo se na nivoju, da zadostimo zakonodaji. Zakonodaja zahteva spodnjo mejo še sprejemljivega, nivo kvalitetne varnosti pa je lahko veliko višji in samo to nam lahko prinese varnost.

Ste že vrsto let člani Slovenskega združenja za korporativno varnost v katerem so včlanjene organizacije, ki obvladujejo kritično infrastrukturo. Kaj bi svetovali tem organizacijam pri postavitvi sončnih elektrarn na tako pomembne objekte? So kakšne zakonske omejitve? So kakšne dogovorjene tehnične rešitve?

Dogovorjenih rešitev ni. Podane so smernice za tovrstne sisteme, usmerjajo pa nas dobre in slabe prakse. Tako, kot se zakonodaja prilagaja potrebam trga, tudi mi projektanti in hkrati izvajalci nenehno stremimo k razvoju še boljših, varnejših in inovativnih rešitev.

Naše bogate izkušnje prav s področja aktivne požarne varnosti na kritični infrastrukturi, težki industriji ter kompleksnih tehničnih sistemih so tiste, ki nas postavljajo v sam vrh.

Ključno, kar lahko svetujem investitorjem pri postavitvi »SE« je, naj tehtno razmislijo kakšen riziko lahko prinese razvit požar na njihovi »SE«. Izguba objekta, ogrožanje življenj, propad poslovanja in drugo. Kakšne so lahko posledice?

Pravočasna investicija in realizacija izvedbe sistema za javljanje požara ter alarmiranja v najzgodnejši začetni fazi, ko je ukrepanje lahko še zelo hitro, je prava odločitev ter ključni korak k trajnostnemu in varnemu delovanju sistema »SE« ter predvsem same organizacije.

Škoda, ki nastane ob požaru ni zgolj materialna in finančna, je lahko tudi poslovno pogubna.
Naj ne bodo stroški glavno vodilo preventivnih ukrepov na področju požarne varnosti. ■

ZARJA ELEKTRONIKA

Varno v nov dan

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

www.zarja.com

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

ISO 9001 Q-1210

Avtor: Matjaž Kocjančič / Reisswolf d.o.o.*

DIGITALNA PREOBRAZBA IN IZZIVI VARNOSTI PODATKOV: PRILOŽNOSTI ZA PODJETJA V DOBI DIGITALIZACIJE

Digitalna transformacija je postala za mnoga podjetja ključen element poslovne uspešnosti. S prehodom na digitalno poslovanje se odpirajo priložnosti za hitrejše, učinkovitejše in transparentnejše delovanje, vendar pa ta proces prinaša tudi številne izzive, predvsem na področju varnosti in skladnosti z zakonodajo. Zakonodaja ter standardi s področja varnosti osebnih podatkov in poslovnih skrivnosti so postavili nova pravila in okvirje, ki jih morajo podjetja, pri upravljanju podatkov skozi celoten življenjski cikel – od njihovega ustvarjanja do varnega uničenja, upoštevati.

Podjetja danes niso zgolj odgovorna za to, kako zbirajo in obdelujejo podatke, ampak tudi za zagotavljanje varnosti teh podatkov, ne glede na njihovo obliko, fizično ali digitalno. To pomeni, da morajo zagotoviti popolno sledljivost, preglednost in integriteto obdelave podatkov na vseh ravneh. Digitalna transformacija tako ni zgolj tehnična nadgradnja, ampak zahteva celovito preoblikovanje poslovnih procesov, kar vključuje visoko raven strokovnosti in varnostnih ukrepov.

Zakonodajni okvir kot priložnost za izboljšanje poslovnih procesov

Zahteve GDPR in drugih zakonodajnih ter standardnih okvirjev prinašajo velik izziv za podjetja, saj so ta pogosto soočena z zapleteno in dinamično zakonodajo, ki se nenehno razvija. Po drugi strani pa lahko skladnost z zakonodajo prinese izboljšave v poslovnih procesih. Podjetja, ki v svoje poslovanje uspešno implementirajo zakonske in standardne zahteve, pridobijo prednosti na področju varnosti, transparentnosti in učinkovitosti delovanja. Digitalizacija procesov jim omogoča večjo hitrost obdelave podatkov, večjo preglednost in stalno sledljivost, kar olajša upravljanje in zmanjšuje tveganja.

Ključni izziv ostaja zagotavljanje varnosti podatkov pred vse bolj prefinjenimi grožnjami, kot so kibernetski napadi. Zaupnost podatkov je postala ena izmed najpomembnejših prednostnih nalog, saj lahko vsaka kršitev povzroči resne posledice, kot so visoke kazni, izguba zaupanja strank in dolgoročna škoda za ugled podjetja. Zato je vzpostavitev robustnih varnostnih ukrepov nujna za preprečevanje nepooblaščenih dostopov.

Strokovno svetovanje je ključnega pomena pri prehodu podjetij iz fizičnega v digitalno poslovanje. Digitalizacija ni le tehničen izziv, temveč zahteva tudi strateško načrtovanje in prenovo poslovnih procesov.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Skladnost kot poslovna priložnost

Na začetku so mnoga podjetja v zakonodajnih zahtevah videla zgolj dodatne stroške in birokracijo. Vendar pa se vedno več podjetij zaveda, da je skladnost z zakonodajo lahko tudi priložnost za optimizacijo poslovanja in krepitev ugleda. S pravilno implementacijo zakonskih zahtev lahko podjetja optimizirajo svoje procese, znižajo stroške in izboljšajo učinkovitost. Poleg tega skladnost krepi zaupanje strank, kar je v današnjem konkurenčnem okolju ključnega pomena.

Digitalizacija in arhiviranje podatkov: ključni izzivi

Prehod iz fizičnega v digitalno arhiviranje prinaša številne izzive, predvsem na področju varnosti in sledljivosti podatkov. Proces pretvorbe dokumentov iz fizične v digitalno obliko mora biti strogo nadzorovan in varen. Pomembno je, da podjetja zagotovijo popoln pregled nad tem, kdo ima dostop do podatkov in dokumentov, tako med procesom pretvorbe, kot po njem. Sledljivost je ključnega pomena, saj podjetjem omogoča nadzor nad tem, kdo dostopa do podatkov in kako jih obdeluje.

Digitalizacija ne zmanjšuje zgolj tveganj izgube ali poškodbe dokumentov, temveč tudi omogoča avtomatizirano upravljanje, kar zmanjšuje napake pri ročni obdelavi. Poleg tega digitalizacija omogoča varno in sledljivo arhiviranje podatkov, kar zagotavlja popolno skladnost z zakonodajo.

Pomembnost strokovnega svetovanja pri prehodu na digitalno poslovanje

Strokovno svetovanje je ključnega pomena pri prehodu podjetij iz fizičnega v digitalno poslovanje. Digitalizacija ni le tehničen izziv, temveč zahteva tudi strateško načrtovanje in prenovo poslovnih procesov. Podjetja morajo razumeti, kako bodo nove rešitve vplivale na njihovo poslovanje in kako lahko optimizirajo svoje procese, da povečajo učinkovitost in skladnost z zakonodajo.

Svetovanje vključuje vse od ocene trenutnega stanja do implementacije rešitev za digitalizacijo in zagotavljanje varnosti podatkov. Podjetja, ki se odločijo za prehod, morajo biti pozorna na vse faze procesa, od priprave dokumentov do varnega arhiviranja in morebitnega dokončnega uničenja podatkov. Celovit pristop zagotavlja, da prehod na digitalno poslovanje ne predstavlja zgolj tehnične nadgradnje, temveč prinaša tudi izboljšanje poslovnih procesov in povečanje konkurenčne prednosti.

Prihodnost digitalizacije in varnosti podatkov

Digitalizacija bo v prihodnje še bolj pridobivala na pomenu, saj podjetja vse bolj prepoznavajo njene prednosti. Z naraščajočo avtomatizacijo procesov se bo tudi področje upravljanja dokumentov in podatkov nenehno razvijalo. Skladnost med zakonodajo in standardi bo ostala ena ključnih prioritet, saj bodo podjetja vedno bolj osredotočena na varnost in sledljivost svojih poslovnih procesov.

Podjetjem, ki se pripravljajo na prehod iz fizičnega v digitalno poslovanje, svetujemo, naj ne odlašajo s to preobrazbo. Digitalna transformacija ne prinaša le večje učinkovitosti, temveč tudi skladnost z zakonodajo, kar je ključnega pomena za dolgoročni uspeh. Podjetja, ki bodo uspešno implementirala rešitve na področju digitalizacije in varnosti podatkov, bodo v prihodnosti bolj konkurenčna in zaupanja vredna na trgu. ■

Učinkovite rešitve za analize in obvladovanje kibernetskih tveganj v vsaki organizaciji

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

Težava in rešitev

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

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

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

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

Kako vam lahko pomagamo?

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

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

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

Avtor: mag. Marko Mihalič / Institut za korporativne varnostne študije*

INOVATIVNE TEHNOLOGIJE ZA HITRO ODKRIVANJE GHB

Projekt ARMADILLO bo policiji in forenzičnim inštitutom zagotovil revolucionarno prenosno orodje za hitro in natančno odkrivanje GHB v urinu, slini in pijači. Projekt temelji na napredni optični spektroskopiji in elektrokemijskih tehnikah.

GHB (gama-hidroksibutirat) je kemična spojina, ki se včasih uporablja kot zdravilo za zdravljenje motenj spanja[1] in kot anestetik. Poleg tega se GHB lahko zlorablja zaradi svojih učinkov, ki vključujejo zmanjšanje zavesti, sprostitev mišic in evforijo[2]. Zloraba GHB-ja je povezana s številnimi nevarnostmi, vključno z zasvojenostjo, predoziranjem in smrtnim izidom[3].

V praksi se uporaba tovrstnih drog drastično povečuje, kakor tudi kazniva dejanja, kjer so vzroki namerno podtikanje te droge osebam, ki so kasneje spolno ali kako drugače zlorabljene. Zaradi okoliščin uporabe, hitrosti razgradnje kemijskih spojin v telesu in izzivov pri uspešnosti odkrivanja ter dokazovanja je ključnega pomena nadaljevati že začeta raziskovanja, kako lahko novi tehnološki in metodološki pristopi to odkrivanje še intenzivirajo in naredijo bolj učinkovitega. Letos je Evropska unija s pomočjo raziskovalno-razvojnega mehanizma HORIZON Europe izbrala pomemben projekt ARMADILLO (**A**ccurate **R**eliable Portable and Rapid **M**ethods **A**nd Technologies for **D**etect**I**on of GHB Substances and Prevention Against Different Forms of Vio**L**ence and Assau**L**t Supp**O**rted by These Drugs) in ga bo tudi financirala. Projekt se osredotoča na ra-

*avtor je član Slovenskega združenja korporativne varnosti

zvoj natančnih, zanesljivih, prenosljivih in hitrih metod ter tehnologij za odkrivanje snovi GHB. Prav tako pa tudi za preprečevanje različnih oblik nasilja in napadov, povezanih z uporabo teh drog. Posebej smo ponosni, da je Institut za korporativne varnostne študije edina slovenska organizacija, ki je vključena v ta projekt. To nam omogoča, da še dodatno nadgradimo in povežemo rezultate našega dela tudi z ostalimi sorodnimi projekti, kjer smo kot partnerji prisotni. Posebej bi veljalo tukaj izpostaviti možnost sodelovanja s projektom ARIEN, o katerem smo že poročali v tej reviji.

Armadillo

Cilj programa ARMADILLO je opremiti organe kazenskega pregona, zlasti policijo in forenzične inštitute, z revolucionarnimi, enostavnimi in prenosnimi orodji za hitro zaznavanje GHB v urinu, slini in pijači. Projekt se osredotoča na razvoj naprednih sistemov za odkrivanje GHB na kraju samem, vključeval pa bo sodobne optične spektroskopske in elektrokemične tehnike za natančno identifikacijo GHB v različnih vzorcih.

Optične spektroskopske metode, kot sta Ramanova spektroskopija in fluorescenca, ter papirnati trakovi, bodo raziskani za zaznavanje GHB. Elektrokemične tehnike bodo združevale specializirane fluidne module in elektrode NAD/NADH. Poleg tega bodo razvita specifična protitelesa za GHB, kar bo povečalo selektivnost in natančnost zaznavanja.

Projekt bo izboljšal zbiranje in izmenjavo forenzičnih dokazov, zagotovil pa bo tudi interoperabilnost in usklajenost med različnimi sistemi. Povezovanje podatkov bo omogočilo zanesljive, varne in sodno sprejemljive forenzične dokaze, medtem ko bo umetna inteligenca prispevala k napredni analizi Ramanove spektroskopije.

ARMADILLO bo prav tako oblikoval celovito oceno tveganja za krepitev strategij preprečevanja nasilja in z drogami spodbujenih napadov, standardiziral uporabniške vmesnike ter uporabil napredne tehnike vizualizacije in poročanja. Da bi se izognil kliničnim preskušanjem in upošteval etične vidike, vključno z zasebnostjo in varnostjo udeležencev, bo ARMADILLO ocenil natančnost, občutljivost in specifičnost svojih tehnologij z uporabo sintetičnih vzorcev, ki simulirajo različne koncentracije GHB v urinu, slini ter v prisotnosti potencialnih motečih snovi.

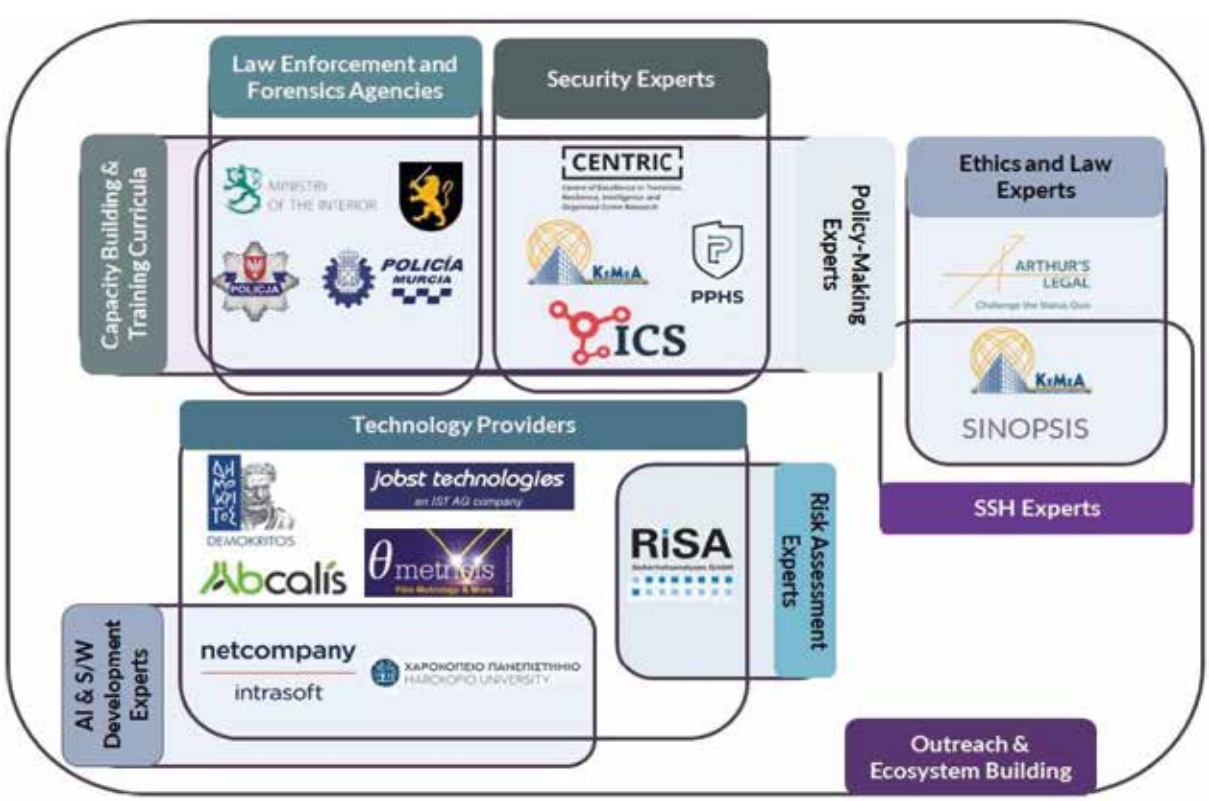
Glavni cilji projekta

Cilj 1: Razvil bo revolucionarna orodja za forenzično odkrivanje, enostavna za uporabo, ki varujejo zasebnost in jih je mogoče uporabiti na terenu in temeljijo na naprednih optičnih in elektrokemičnih metodah ter prenosnih čitalnikih. Ta orodja bodo omogočila natančno in hitro odkrivanje GHB ter zbiranje zanesljivih dokazov, sprejemljivih v sodnih postopkih.

Cilj 2: Opremil bo organe kazenskega pregona in forenzične strokovnjake z napredno tehnološko platformo, ki združuje kazalnike tveganja in podatkovno analitiko. Ta platforma bo omogočila izboljšano zbiranje in analizo podatkov, kar bo pripomoglo k bolj učinkovitemu preprečevanju in preiskovanju nasilja ter spolnih napadov, povezanih z uporabo teh drog.

Cilj 3: Potrdil bo učinkovitost predlaganega metodološkega okvira in platforme. Izvedena bo s štirimi potrditvenimi kampanjami, ki se osredotočajo na različne in dopolnjujoče primere uporabe. V teh kampanjah bodo aktivno sodelovali strokovnjaki s področja varnosti, kar bo omogočilo hitrejšo implementacijo inovativnih rešitev projekta.

Cilj 4: Zagotovil bo široko komunikacijo, znanstveno razširjanje in učinkovito uporabo rezultatov projekta za akademske in industrijske varnostne skupnosti. Povečal bo ozaveščenost in spodbudil sodelovanje med različnimi zainteresiranimi stranmi ter izmenjavo infor-



Slika 1: Komplementarnost konzorcija

macij na ravni EU. Tako bo omogočeno hitrejše in okolju zanesljivo prepoznavanje drog GHB ter preprečevanje različnih oblik nasilja in napadov, ki jih te droge lahko povzročijo.

Cilj 5: Rezultati projekta bodo posredovani ustreznim organizacijam ter strokovnjakom s področja varnosti z namenom spodbujanja političnih reform, podprtih z dokazi, v zvezi z odkrivanjem drog GHB v urinu, slini in pijači. Cilj dejavnosti je okrepiti socialno kohezijo in notranjo varnost držav članic EU.

Inštitut za korporativne varnostne študije bo v projektu vodil tri pomembne naloge. V prvem delu projekta bo pripravil GAP analizo za hitro, zanesljivo in natančno odkrivanje GHB. Vzporedno s to nalogo bo zbral vse potrebe in zahteve uporabnikov ter pripravil podroben opis scenarijev, ki bodo kasneje testirani v treh pilotih projekta. V drugem delu projekta bo pripravil učni načrt za krepitev zmogljivosti in usposabljanje varnostnega osebja.

Projekt ARMADILLO se je uradno začel že 1. oktobra 2024 in bo trajal 36 mesecev. Kot edini slovenski partnerji na projektu bomo skozi celoten razvojni cikel projekta zagotavljali vključenost ostalih strokovnih deležnikov iz Republike Slovenije, da bodo o pomembnih korakih ustrezno obveščeni. Zagotavljali bomo tudi okvir, kjer bo lahko strokovna skupnost podajala svoja mnenja in dobre prakse ter izkušnje, ki bodo za razvoj projekta ključnega pomena. O vseh nadaljnjih razvojnih korakih vas bomo pravočasno obveščali po različnih komunikacijskih kanalih. ■

"ARMADILLO project has received funding by the European Union's Horizon Europe, under grant agreement no 101168416."

Avtorji: Miran Novak / Melamin kemična tovarna d.d.*,
dr. Rok Rupnik /Fakulteti za računalništvo in informatiko, dr. Andrej Bregar / Informatika d.o.o.*

IZZIVI IN PASTI DIGITALIZACIJE

Svet okoli nas in življenje, ki ga na njem živimo, sta vsaj na ravni naše zaznave, zvezna in analogna. Vedno pa le ni tako. Če za primer opazujemo razvoj znanosti in tehnologije, hitro ugotovimo, da zadeve nekaj časa vztrajajo na doseženi ravni, dokler nekomu nekje ne uspe doseči novega mejnika in dvigniti letvico malo višje. Takrat se v zelo kratkem času celotna srenja zgane, osvoji novost in v pričakovanju naslednjega koraka nadaljuje na višji ravni.

Uvod

Premiki se torej dogajajo v diskretnih korakih. Vsake toliko pa se zgodi, da je premik tolikšen, da kar za nekaj časa zaznamuje dogajanje v panogi. V informacijski stroki se je tak tektonski premik zgodil s formiranjem svetovnega spleta. V obdobju kmalu po takšnem preskoku, se z nenavadno intenzivnostjo začne omenjati nova paradigma. Tudi tisti, ki o tem vedo malo, ali nič, si želijo svojega kosa pogače in na koncu izgleda, da prej ni bilo ničesar, zdaj pa je vsepovsod samo še zgolj to. Če vas povedano spominja na vseprisotno digitalizacijo, vas občutek verjetno ne vara.

1. Digitalizacija – nova nafta?

Vse od začetka Covid-19 izolacije, se beseda digitalizacija zelo pogosto pojavlja. Ta beseda v sebi implicitno vsebuje še najmanj pojma digitizacije in digitalne preobrazbe. Napačna je predstava, da se je digitalizacija začela s Covidom. Procesi so se digitalizirali že mnogo prej, a se je temu reklo informatizacija. Običajno se dogaja, da ko neka stvar postane popularna, mnogi skušajo okrog nje zgraditi tržno nišo in del te popularnosti pretvoriti v zaslužek. To seveda zaradi oglaševalskih in trženjskih mehanizmov popularnost le še poveča. Nekaj takega se zdaj dogaja z digitalizacijo.

Zakaj digitalizirati?

Vzrokov za skokovit porast digitalizacije ni težko najti. Okolje in razmere v njem, so za digitalizacijo namreč postale zelo ugodne. Poglejmo jih nekaj:

- Hitre in zmogljive optične komunikacije razpredene tako po mestih, kot tudi na podeželju. Kjer tega še ni, so na voljo hitre 5G radijske povezave. To omogoča neslutene možnosti prenašanja velikih količin digitalnih podatkov.
- Naprave za zajem in reprodukcijo slike in zvoka so skoraj v celoti digitalne. Vsak pametni telefon je opremljen z vso tehniko, za kreiranje digitalnih datotek, ki vsebujejo fotografije, video-zapise, zvoke in glasbo.
- Orodja in naprave za vsakdanjo rabo večinoma izgledajo tako, kot včasih, a so dejansko zgrajene okrog mikroračunalnika s komunikacijskim vmesnikom. Novejši avtomobili že omogočajo pošiljanje podatkov in komunikacijo z aplikacijami ter pošiljanje tehničnih parametrov vozila proizvajalcu. Klimatske naprave, toplotne črpalke in ogrevalni sistemi so povezani v svetovni splet in omogočajo daljinski nadzor in upravljanje.
- Obdelovalni stroji in orodja v proizvodnih tovarnah so tudi opremljeni s podobnimi funkcionalnostmi in možnostjo povezave v procesni informacijski sistem tovarne. Na podoben način so oskrbovalna in energetska omrežja (voda, elektrika, plin, nafta) opremljena s senzorji in aktuatorji, ki zajemajo stanje omrežja in omogočajo daljinsko krmiljenje njegovih vitalnih delov.

Neizbežno je, da se takšnemu okolju procesi dela in upravljanja prilagodijo in sicer tako, da začnejo zajemati numerične podatke, jih obdelovati, shranjevati in jih izmenjevati. Brez da bi se posebej trudili, zgolj z vsakodnevnim življenjem in uporabo naprav, ki jih imamo na voljo, smo se že digitalizirali.

Digitalne platforme

Poslovna digitalna platforma je programska oprema in tehnologija, ki se uporablja za poenotenje in racionalizacijo poslovnih procesov, operacij in sistemov. Digitalna platforma služi kot hrbtenica organizacije za poslovanje in sodelovanje s strankami in lahko standardizira poslovne procese, kar poveča učinkovitost ter preglednost poteka dela. Organizacija zato bolje upravlja notranje funkcije in zadovolji svoje stranke. Z uporabo digitalne platforme lahko učinkoviteje razvijajo in lansirajo

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

izdelke, servisirajo stranke in izvajajo poizvedbe za izboljšanje delovanja ter obveščanje o poslovni in produktni strategiji. Podatki na podlagi poizvedb služijo zaposlenim, za boljše sodelovanje s strankami in ustvarjanje prihodkov. Te platforme lahko gradimo sami, lahko njihovo izdelavo naročimo, ali pa uporabljamo obstoječe, ki so v uporabi. Podatki z digitalnih platform so večinoma v oblaku, lahko pa jih tudi lokaliziramo.

Procesi pred in po digitalizaciji

Do sedaj smo že ugotovili, da ne moremo digitalizirati samih sebe, k sreči smo še vedno analogna in oprijemljiva bitja, temveč digitaliziramo procese, ki jih opravljamo. Nekateri procesi se z digitalizacijo bistveno ne spremenijo, izvajamo jih zgolj z drugimi sredstvi. Sam proces se z digitalizacijo torej ni bistveno spremenil, le podatki nastali v procesu so lažje, hitreje in ceneje dostopni, kakor poprej.

Drugi procesi pa so se z digitalizacijo spremenili, vzemimo za primer oddajo davčne napovedi. Proces se je digitaliziral do te stopnje, da namesto mučnega izpolnjevanja obrazcev, zdaj zgolj še po pošti prejmemo odločbo. V tem primeru je razlika v procesu prej in potem velika. Nekatere javne storitve v razvitih državah so do tolikšne mere digitalizirane, da zlasti starejši in tehnološko nevešči ljudje, digitalnih storitev niso sposobni uporabljati in so brez pomoči veščih nebogljeni. Zato se formirajo državljanske iniciative, ki zahtevajo pravico do analognosti.

2. Ocena uspešnosti digitalizacije procesa

Procese digitaliziramo tako v javnem, kot tudi v poslovnem življenju. Že pri načrtovanju digitalizacije moramo imeti v mislih uspešnost svojega početja. Sodila za oceno uspešnosti si moramo opredeliti vnaprej in jih upoštevati pri načrtovanju. Pri tem moramo pogledati dovolj široko in upoštevati vsaj naslednja področja:

Učinkovitost

Digitaliziran proces mora biti vsaj tako učinkovit, kot proces pred digitalizacijo. Učinkovitost preverimo po dveh plateh. (1) Funkcijska učinkovitost kjer se vprašamo, ali proces po digitalizaciji funkcijsko omogoča vse, kar je omogočal proces pred digitalizacijo. Od tega lahko odstopimo zgolj, če proces oblikujemo tako, da zaradi zagotavljanja skladnosti z zakonodajo in predpisi, izboljšanjem varnosti, oziroma preprečitve škode ali nesreče, nekatera dejanja niso dovoljena. (2) Stroškovna učinkovitost, kjer bi se sredstva, vložena v digitalizacijo, praviloma morala v primernem časovnem obdobju povrniti skozi nižje stroške izvajanja digitaliziranega procesa. Tudi tu glede odstopanja od tega načela velja podoben razmislek, kot v prejšnjem odstavku.

Dostopnost

Digitaliziran proces mora biti uporabniku dostopen. Digitalizacijo lahko še tako skrbno načrtujemo in oblikujemo, a če si na koncu za izvajanje izberemo platformo, ki ne deluje stabilno, je proces neuspešen. Kot primer se lahko spomnimo sicer zgledno pripravljene spletne aplikacije za občane v postopkih javne uprave, ki pa je bila postavljena na strežnike z bistveno prenizko odzivnostjo. Po nekaj mesecih slabe volje so pomanjkljivost odpravili in od takrat storitev deluje zgledno.

Varnost

Ko proces iz fizičnega sveta prenesemo v računalniško okolje, ni več dovolj zagotavljati le fizične varnosti okrog procesa. Digitaliziran proces mora teči v okolju s

primerno ravnjo kibernetske varnosti. To področje je zahtevno in zelo široko ter presega namen in obseg tega prispevka, zato si oglejmo le nekaj priporočil za dvig ravni varnosti:

- Platforma mora biti umeščena na strojno in programsko opremo, ki se redno posodablja z varnostnimi popravki.
- V organizaciji morajo veljati varnostne politike za upravljanje z gesli, za upravljanje, vzdrževanje in varovanje krajevnega omrežja in aktivne omrežne opreme ter varnostnega kopiranja in arhiviranja,
- pravilno morajo biti nameščene in vzdrževane požarne pregrade in varnostna območja (DMZ cone),
- skrbeti je treba za redne varnostne preglede,
- uporabniki morajo biti ustrezno usposobljeni in redno osveščani glede kibernetskih groženj.

Zanesljivost

Zanesljivost delovanja digitaliziranega procesa mora biti premosorazmerna s pomembnostjo procesa. Ključni procesi, od katerih je odvisno izvajanje proizvodnje ali zagotavljanje procesne in osebne varnosti, morajo teči na platformah z zelo visoko razpoložljivostjo obratovanja (99,99 ali višjo, glede na pomembnost procesa). 99,99 razpoložljivost pomeni približno 1 uro nehotenega izpada delovanja na leto. Če se odločimo za platformo, ki teče v oblaku, moramo poskrbeti za zanesljiv dostop do spleta. Zanesljivost lahko povečamo z uvedbo vzporednega, redundantnega priključka z drugim operaterjem, ki dobavo zagotavlja po fizično drugih trasah. Prav tako zanesljivost povečamo z dvostranskim priključevanjem aktivne omrežne opreme na podvojeno, oziroma zazankano interno pokablitev.

3. Tveganja ob digitalizaciji

Vse prepogosto organizacije že ob načrtovanju digitalizacije pozabijo na ocene tveganj, ki se ob in po digitalizaciji procesa utegnejo udejanjiti in oceno uspešnosti omejijo zgolj na funkcijsko in stroškovno uspešnost, vsa ostala sodila iz prejšnjega razdelka pa spregledajo.

Ocena tveganj

Rast stopnje digitalizacije in pojavnosti kibernetskega kriminala sta vzporedni. S pospešeno digitalizacijo se polje delovanja malopridnežev pač širi in pričakovati je, da bo tudi njihova žetev rasla. Ocena tveganj je torej nujni korak, ki bi moral biti omenjen že v krovnem dokumentu, to je strategiji digitalizacije, ki bi jo naj družba pripravila in proučila pred začetkom digitalizacije.

Napeta in negotova politična situacija v svetu že povzroča, da se kibernetski napadi uporabljajo kot orožje v specialnih vojaških operacijah. Ni nemogoče, da bi strnjen in usmerjen DoS napad za nekaj ur, ali celo dni, onesposobil delovanje spleta v napadeni državi, ali celo regiji. Na takšna tveganja ne smemo pozabiti.

Če predpostavimo, da večina organizacij že ima izdelan načrt neprekinjenosti poslovanja, potem bi ob vsakem ključnem procesu, ki je podvržen digitalizaciji, nujno morali obnoviti oceno tveganja za ta proces in pripraviti ukrepe, v primeru, da proces preneha delovati. Ocenjevanje tveganj mora biti zvezen in stalen proces v organizaciji, ki v sovpregi s procesom upravljanja s spremembami, sproti pokaže nova, še neobvladana tveganja.

Obvladovanje tveganj

Tveganja, ki ga nismo zaznali, ne moremo obvladovati. Zaznana tveganja moramo obvladati. Dobre smernice pri tem nam ponuja standard ISO 31000. Ampak sprejemanje ukrepov, ki izhajajo iz prej omenjenih tveganj, s seboj prinaša dodatne stroške, kar predstavlja breme za organizacije, katerim bi se rade po osnovnih poslovnih logikah izognile. Organizacije in celotna družba se nahajamo v precej neenakopravnem položaju, glede na kibernetske kriminalce. Ti se namreč vse bolj organizirajo in svoje nečednosti počno že v kar korporativnih razsežnostih, ki že imajo negativne vpliva na narodna gospodarstva. Zato državni regulatorni organi pripravljajo in sprejemajo zakone, direktive in navodila, po katerih se morajo organizacije ravnati. Primer takšne zakonodaje sta EU NIS-2 direktiva, ki je že v veljavi in slovenski Zakon o informacijski varnosti, ki je še v javni obravnavi in bo kmalu sprejet. Obvladovanje kibernetskih tveganj, ki sledijo iz vse večje stopnje digitalizacije, je torej že podvrženo regulativi, da zagotovimo usklajen odziv na omenjene grožnje.

Upravljanje s kritično infrastrukturo je proces, od katerega smo odvisni ne zgolj na ravni posamezne države, ampak globalno. Zato se NIS-2 direktiva osredotoča predvsem na upravljalce kritične infrastrukture in širi krog zavezancev. Ti bodo vedno bolj izpostavljeni tveganjem organiziranih kriminalnih, vojaških in terorističnih napadov, zato je zelo pomembno, da se ne izogibamo odgovornostim, saj bomo posledice takšnega ravnanja na koncu čutili vsi. Tu ne gre zgolj za izpolnjevanje minimalnih regulatornih zahtev, temveč za moralno obvezo po stalnem povečevanju odpornosti sistemov, ker na koncu, kot je leta 1621 zapisal John Donne, nihče ni otok in ko bo zazvonilo, bo zvonilo nam vsem. ■

Avtorica: Katja Bitenc / Skrbnica ključnih kupcev, ID Shop d.o.o.

INTEGRACIJA NAPREDNIH VARNOSTNIH SISTEMOV V POSLOVNE, ZDRAVSTVENE IN TURISTIČNE PROSTORE

V današnjem hitro spreminjajočem se svetu je zagotavljanje varnosti postalo prednostna naloga v vseh sektorjih, od poslovanja do zdravstva in turizma.

Sodobni objekti, kot so poslovne stavbe, zdravstveni centri in turistične znamenitosti, zahtevajo celovite in napredne varnostne sisteme, ki ne le zagotavljajo zaščito, temveč tudi olajšajo upravljanje in izboljšajo uporabniško izkušnjo. Projekti, kot so DCB Montana, UKC Ljubljana, razgledni stolp v Rogaški Slatini, stadion Z'Dežele v Celju in avtobusna postaja v Radovljici, predstavljajo izjemne primere, kako lahko rešitve podjetja ID SHOP d.o.o. prinesejo dodano vrednost in visoko stopnjo prilagodljivosti v različna okolja.

Projekt DCB Montana: učinkovita integracija varnostnih sistemov v poslovni stavbi

DCB Montana v Ljubljani je poslovna stavba, kjer sta arhitektura in tehnologija skrbno prepleteni, da bi ustvarili vrhunsko delovno okolje. Zasnovali smo dvoplastni varnostni sistem, ki vključuje kombinacijo elektronske kontrole dostopa in mehanskega zaklepanja. Elektronski sistemi omogočajo prilagodljiv nadzor dostopa za različne uporabnike objekta, mehanski sistem pa zagotavlja dodatno varnost v izrednih situacijah.

Estetika in funkcionalnost sta bili ključnega pomena pri tem projektu. V sodelovanju z arhitekti smo poskrbeli, da varnostni elementi ne motijo sodobnega videza stavbe. Pametni čitalci, hitri prehodi povezani s sistemom dvigal in mehanski cilindri so bili skrbno izbrani tako, da se estetsko skladajo z arhitekturno zasnovo objekta, hkrati pa izpolnjujejo najvišje varnostne standarde. Ta celovita rešitev prinaša visoko raven varnosti in omogoča enostavno nadgradnjo sistema v prihodnosti, kar je izjemno pomembno v poslovnem svetu, kjer se zadeve hitro spreminjajo.

UKC Ljubljana: nadgradnja varnosti v zdravstvenem okolju

V projektu UKC Ljubljana smo nadgradili obstoječo baterijsko rešitev za shranjevanje osebnih predmetov zaposlenih z naprednim sistemom pametnih ključavnic. Implementacija je obsegala ožičen online sistem (ključavnice in krmilniki), kar omogoča centralizirano upravljanje in spremljanje dodeljenih omaric. S tem smo odpravili težave, ki so se pojavljale pri prejšnjem sistemu, kjer je prihajalo do težav z dostopom in sledljivostjo. Stari sistem je namreč pogosto povzročal težave, saj so zaposleni zaklepali svoje kartice v omarice, kar je oviralo dostop do drugih delov objekta. Z novim sistemom so te težave odpravljene.

Prenova je bila zahtevna, saj je bilo potrebno omarice predelati v več fazah, medtem ko so bile v uporabi in

zagotoviti napajanje. Implementacija je bila uspešna, rešitev pa zagotavlja višjo raven varnosti, sledljivost in optimizirano upravljanje.

Razgledni stolp v Rogaški Slatini: napredna tehnologija za turistično atrakcijo

Pri projektu turističnega razglednega stolpa v Rogaški Slatini smo vgradili celovito rešitev za nadzor dostopa, prilagojeno specifičnim potrebam turistične atrakcije. Vgradili smo hitri prehod in stopnične terminale za nadzor dostopa, ki vključuje dva prehoda ter števec obiskovalcev, integrirano z blagajniškim sistemom. Sistem omogoča učinkovito upravljanje prehodov obiskovalcev in prikaz števila prisotnih na stolpu preko elektronskega zaslona.

Poleg tega je bil vgrajen mehanski sistem zaklepanja, ki zagotavlja visoko raven zaščite vrat v objektu. S tem smo zagotovili optimalno varnost ter prilagodljivost sistema za prihodnje potrebe objekta.

Stadion Z'Dežele v Celju: varnostna prenova po UEFA standardih

Prenova stadiona Z'Dežele v Celju je zahtevala prilagojeno rešitev za nadzor dostopa, skladno s strogimi varnostnimi standardi UEFA. Rešitev vključuje nadzor prehodov na različnih tribunah, kar omogoča hiter in varen dostop za obiskovalce. Na vzhodni tribuni smo postavili tripode, visoka vrtljiva vrata na severni in južni tribuni ter hitri prehod na VIP vhodu.

Posebna pozornost je bila namenjena integraciji sistema z obstoječim sistemom za prodajo vstopnic, kar omogoča celovit nadzor nad obiskovalci in njihovo varnostjo med dogodki. Naša rešitev je zagotovila učinkovito upravljanje dostopa, hkrati pa upošteva vse zahteve po varnosti in prilagodljivosti za prihodnje nadgradnje.

Avtobusna postaja Radovljica: uvajanje plačljivih storitev in prilagojen dostop

V Radovljici smo v sklopu prenove toaletnih prostorov avtobusne postaje, uvedli rešitev za plačljiv dostop, pri čemer smo upoštevali tudi dostopnost za osebe s posebnimi potrebami in družine z vozički. Naša rešitev je omogočila enostaven dostop skozi hitri prehod, ki je bil prilagojen omejenemu prostoru, ter hkrati zagotovila varno in uporabniku prijazno izkušnjo.

Projekt je bil poseben tudi zaradi integracije z blagajniškim sistemom in terminalom za plačilo s kreditnimi in debetnimi karticami. Glavni cilj prenove je bil omogočiti povrnitev stroškov vzdrževanja sistema skozi plačljive storitve, kot so uporaba toaletnih prostorov, čistoča in zagotavljanje potrebščin (milo, papir, voda).

Zaključek: prilagojene rešitve za zahtevna okolja

Projekti, ki jih izvajamo v podjetju ID SHOP d.o.o., dokazujejo, kako pomembno je razumeti specifične potrebe naročnikov in jih integrirati v celovite varnostne rešitve. Naše rešitve združujejo mehanske in elektronske komponente, ki prinašajo visoko stopnjo zaščite, hkrati pa omogočajo prilagodljivost in enostavno upravljanje. Zanesljivost, estetika in funkcionalnost so ključni elementi, ki zagotavljajo dolgoročno zadovoljstvo uporabnikov in varnost na najvišji ravni. ■

VARNOSTNI PREHODI ZA KONTROLO DOSTOPA V NADZOROVANA OBMOČJA

Visoka in nizka vrtljiva vrata ter hitri avtomatizirani prehodi kot dodatna kontrola točka za vstop v omejena območja.

Primerno za zunanjo ali notranjo namestitev in za območja z velikim pretokom uporabnikov.
Možnost integracije z obstoječimi VNC sistemi in uporabo enega medija znotraj kompleksa.
Zvočni in svetlobni alarmi v primerih neavtoriziranega prehoda.
Možnost avtomatiziranih plačljivih prehodov ter dodatnih modulov po meri naročnika
(biometrija, ticketing – avtomatizirano preverjanje vstopnic, štetje obiskovalcev,...).

ID SHOP – ZANESLJIV PARTNER ZA ZAGOTAVLJANJE KONTROLE PRISTOPA V VAŠIH OBJEKTIH

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

- Nižji stroški fizičnega varovanja.
- Bolj kontroliran pretok ljudi.
- Večja izkoriščenost varnostno-nadzornega centra.
- Učinkovita integracija z obstoječo kontrolo pristopa v stavbi.
- Doseganje višjih varnostnih standardov.

ID Shop zagotavlja celovite rešitve za zagotavljanje kontrole pristopa:

Mehanski sistemi zaklepanja • Elektronski sistemi zaklepanja (pametne kljuke, digitalni cilindri, mehatronske komponente) • Varnostni prehodi (visoka, nizka vrtljiva vrata, hitri prehodi in zapore)

IDealni partner za identifikacijo in varnost

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

cominfo

Avtorja: Boštjan Oblak / iStor Swiss in Aleš Polajnko ORG. TEND d.o.o.

ZAKAJ KLJUB VARNOSTNIM KOPIJAM PODJETJA VSE POGOSTEJE IZGUBLJAJO PODATKE?

»Podatki so gonilna sila podjetja.« Trditev, ki je izpeta do onemoglosti, a je po vseh teh letih vendarle obrodila sadove. Podjetja so začela poslušati varnostne strokovnjake in vzpostavila sisteme za varnostno kopiranje in obnovo podatkov. Pojavila pa se je povsem drugačna, nepričakovana težava. Večina vzpostavljenih sistemov je neustreznih, v rokah neizkušenih izvajalcev, ki se povrhu še ne držijo dobrih, ustaljenih praks in glavnih zahtev varnostnega kopiranja podatkov.

Osveščenost o pomembnosti podatkov se dogaja na vsakem koraku. Zakaj pa se kljub vsemu podatki, še vedno in v vse večjem obsegu, izgubljajo?

Zelo pomembno je, da v primeru, ko zaupate hrambo vaših podatkov zunanjemu podjetju, da je ta izbira preverjena. Eden izmed pomembnih elementov pri tem je tudi, da takšno podjetje obstaja že več let in uspešno posluje. Podjetje iStor je eden najstarejših ponudnikov storitve varnostnega kopiranja v Evropi. Za podatke uspešno skrbijo že več kot 24 let, ker se držijo dobrih praks varnostnega kopiranja in ker so neodvisni od tretjih ponudnikov. So prva izbira organizacij z visokimi zahtevami. Njihova varnostna rešitev je v celoti plod lastnega razvoja.

Kaj pa so primeri dobre prakse varnostnega kopiranja? In kakšne so prednosti pri podjetju, ki ponuja takšno rešitev?

Omejen dostop z ustrezno sledljivostjo

Ali bi oseba, ki ima dostop do produkcijskih podatkov, morala imeti tudi dostop do varnostnih kopij? Odgovor je nedvoumno ne, kajti tako prepuščate usodo podjetja odločitvi ene osebe. Dostop mora biti striktno ločen, še posebej, če za vzdrževanje IT sistemov skrbi zunanji izvajalec. Dostop do varnostnih kopij je potrebno omogočiti le avtoriziranim osebam, v vsakem primeru pa vse posege in dostope do varnostnih kopij zabeležiti. V primeru sumljivih aktivnosti pa boste predčasno opozorjeni.

Kje hranite podatke? Lokalno, v oblaku ali kako drugače?

Zlato pravilo sistema varnostnega kopiranja je, da mora biti odporno na vse morebitne grožnje. To vključuje tudi naravne katastrofe, kot na primer požar, potres in poplave, čeprav si mislite, da je verjetnost njihovega nastanka skoraj nična. Lokalna kopija je vsekakor pomembna, a še bolj pomembno je, da imate varnostno kopijo shranjeno tudi na oddaljeni lokaciji. Pomembno je, da veste kje se vaši podatki nahajajo in da ta ponudnik podatke hrani na lastni infrastrukturi. Med njimi, naročnikom in varnostnimi kopijami ni tretjega posrednika. Sistemske kopije ločite od podatkovnih. Zakaj? Poenotene varnostne kopije terjajo časovni in finančni davek,

Veriga je močna, kolikor je močan njen najšibkejši člen, je pregovor, ki še kako velja v podatkovnem svetu.

zato se pogosto ne uvrščajo v primere dobre prakse. Seveda je pomembno, da izpad delovnih tokov ne traja predolgo, a na koncu bo vsakršna ponovna vzpostavitev sistemov nesmiselna, če ne boste uspeli rešiti podatkov. Tako dobro zasnovna rešitev zato prednostno obravnava podatkovne varnostne kopije, kajti podatki so nepogrešljivi, sistemi pa lažje obnovljivi.

Šifriranje podatkov na izvoru in več nivojska deduplikacija

Šifriranje podatkov je potrebno izvesti na samem izvoru, šifrirni ključ pa se ob generiranju samodejno preda lastniku podatkov. Marsikatero podjetje, ki upravlja z ogromnimi količinami podatkov, upravičeno skrbijo operativni stroški. Zalo pomembno je, da ima izbrana rešitev vgrajeno več nivojsko deduplikacijo, ki bistveno zmanjša čas varnostnega kopiranja, uporabo širokopasovne povezave in prostor, potreben za hrambo in zaščito podatkov.

Koliko časa je potrebno hraniti varnostne kopije?

Daljša kot je zgodovina hrambe varnostnih kopij, večja verjetnost je za obnovitev podatkov, ne samo v primeru vdora, naravne katastrofe, ampak tudi v primeru okvarjene podatkovne baze. Povprečna starost obnovljenih podatkov je 192 dni. iStor DataVault hrani varnostne kopije občutno dlje od povprečja, hkrati pa redno preverjajo stanje varnostnih kopij.

Veriga je močna, kolikor je močan njen najšibkejši člen, je pregovor, ki še kako velja v podatkovnem svetu. Smotrno je preveriti, kako vaši poslovni partnerji upravljajo s podatki. V primeru izgube podatkov v partnerskem podjetju se lahko sproži verižna reakcija, ki bo vplivala tudi na vaše podjetje.

Sodelovanje z lokalnimi razvijalci

Pomembno je, da takšna rešitev podpira vse največje aplikacije, platforme in podatkovne baze, hkrati pa podpirajo tudi bolj lokalizirane rešitve in rešitve specifične za določeno industrijo, kar jim omogoča tesna naveza z lokalnimi razvijalci s katerimi razvijajo rešitve za točno določeno aplikacijo oziroma namen.

Zaključek

Ključne zahteve za zanesljiv Backup so:

- Ločen skrbnik in sledljivost dostopa. *Osebe, ki imajo dostop do produkcijskih podatkov, ne smejo imeti dostopa do varnostnih kopij.*
- Oddaljena lokacija. *Številne nevarnosti, ki ogrožajo podatke, imajo lahko širše uničujoče posledice, na primer: požar, poplava, potres, razne druge nesreče, kriminal, človeške napake, terorizem,...*
- Šifriranje podatkov. *Varnostne kopije morajo biti ustrezno zaščitene tako fizično kot tudi tehnično. Šifriranje podatkov predstavlja enega ključnih varnostnih procesov*
- Ustrezno dolga zgodovina varnostnih kopij. *Povprečna starost podatkov, ki se obnavljajo iz varnostnih kopij je več kot tri mesece.*
- Redno preverjanje varnostnih kopij. *Edini način s katerim lahko 100% zagotovimo uporabnost podatkov v varnostni kopiji je preverjanje.*
- Ločena sistemska in podatkovna varnostna kopija. *Hitro okrevanje po okvari ali drugi katastrofi zahteva obe varnostni kopiji podatkov.*
- Ločen sistem uporabnikov. *Sistem pravic uporabnikov za varnostne kopije mora biti ločen od produkcijskega sistema.*
- Preverjanje poslovnih partnerjev. *Izguba podatkov enega podjetja lahko ogrozi tudi vse njihove partnerje.* ■

Avtor: Andrija Pušić / produktni direktor, Špica International d.o.o.*

12 NAČINOV ZA ODPIRANJE VRAT

V primeru, da so vaša vrata običajna, jih lahko odklenete le na en način – s ključem. Kaj pa, če za svoja vrata uporabite Door Cloud? Izkaže se, da obstaja najmanj 11 dodatnih načinov za odpiranje vrat! V nadaljevanju si bomo ogledali ves spekter teh možnosti.

Mobilna naprava

Filozofija Door Clouda je »najprej mobilna«, zato začnimo s tem. Najbolj očiten način je precej preprost. Prenesete aplikacijo, zaprosite za povabilo, pridobite svoje poverilnice in prejmete seznam vrat, ki jih lahko odprete. Ko odprete aplikacijo, tapnite vrata s seznama in *voilà*, vrata se odprejo!

Key link

Imeti mobilno aplikacijo za odpiranje vrat je povsem v redu za redne uporabnike, za enkratne obiskovalce ali goste pa je ta aplikacija morda nepotrebna. Zanje obstaja precej enostavnejša rešitev, imenovana Key Link. To je spletna povezava, ki jo gostitelj, redni uporabnik, za odpiranje vrat pošlje gostom. Gost prejme povezavo na svojo mobilno napravo, nato pa je preusmerjen na spletno stran za odpiranje vrat, kjer klikne gumb »ODPRI«.

Daljinsko odpiranje

Z uporabo mobilne aplikacije ali Key Linka ni nujno potrebno, da ste pri vratih, da jih odprete. Sodelavcu ali čistilcu lahko dovolite vstop, medtem ko ste na službeni poti. Glede na politiko vaše organizacije vam je morda dovoljeno odpiranje vrat od koderkoli ali samo z določenih lokacij.

Kartica

Najbolj priljubljen način za odpiranje elektronsko nadzorovanih vrat je zagotovo uporaba kartice ali obeska. Kartico prislonite na čitalnik in vrata se odprejo. Preprosto in hitro – brez mobilne naprave, brez aplikacij, računov ali gesel – a mora biti čitalnik kartic nameščen pri vratih. In seveda morate imeti s seboj kartico.

NFC

Ko uporabljate kartico, morate biti pri vratih. Včasih je to točno tisto, kar želimo. Pri uporabi mobilne naprave so vrata lahko označena z NFC oznakami, da zagotovimo strogo lokalno odpiranje. Mobilni telefon prislonite k oznaki, aplikacija jo v ozadju prebere in vrata se takoj odprejo. To deluje hitreje, saj ni treba uporabljati aplikacije.

Promocijski članek

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Notifikacija

Drugi način, kako se izogniti uporabi mobilne aplikacije, je nastavitev obvestila ob približevanju vratom. Namesto da odklenete telefon in odprete aplikacijo, preprosto tapnite na obvestilo in vrata se odprejo.

Biometrija

Če ne želite uporabljati mobilnega telefona ali kartic, imate lahko pri vratih biometrični čitalnik (na primer čitalnik obraza). Nekateri od teh čitalnikov vas lahko prepoznajo brez dodatnih informacij, samo z ujemanjem vašega obraza s predhodno izbranim vzorcem. Nekateri čitalniki morajo biti kombinirani s karticami ali PIN kodami. Nekateri bodo morda zahtevali kartico za prenos vašega vzorca. V vsakem primeru bi potrebovali biometrični čitalnik, ki posnema čitalnik kartic, in morda tudi nekaj upravljalne programske opreme.

Bluetooth

Pri odpiranju vrat mobilni telefon komunicira s kontrolorjem vrat prek interneta, zato morata biti obe napravi povezani. Če ena od njih ni povezana, lahko vrata še vedno odprete prek pomožne povezave Bluetooth. To lahko traja par sekund dlje kot spletno odpiranje, vendar je to še vedno sprejemljivo kot rezervna možnost.

Trajno zaklepanje in odklepanje

Kot skrbnik platforme Door Cloud vam je dovoljeno odpreti vrata brez posebnih dostopnih pravic. Pa ne le to – z zadostnimi upravljavskimi pravicami lahko vrata trajno zaklenete ali odklenete, dokler se ne odločite, da nadaljujete z običajnim delovanjem.

Načrtovano (od)klepanje

... In ni vam treba biti tam, ko se to zgodi. Lahko nastavite, da se vrata samodejno odklenejo (ali zaklenejo) ob vnaprej programiranih časih.

Preklop

Obstaja popolnoma drugačen način nadzora vrat, imenovan »Preklopni način«. Namesto da se vrata odprejo samo za par sekund, v preklopnem načinu ostanejo odprta. Naslednji dostop jih zapre nazaj in tako naprej. Preklopni način se običajno uporablja za učilnice ali sejne sobe, kjer ena oseba spusti skupino ljudi noter, nato pa zaklene vrata, ko odidejo.

Tako smo našteli 11 dodatnih načinov za odpiranje vrat s platformo Door Cloud. Ne pozabite, morda imate za vsak slučaj nekje varno shranjen dobri stari mehanski ključ. To bi bil dvanajsti način. Lahko izberete kateregakoli od teh načinov — ali celo vse. Prav tako lahko kadarkoli kombinirate vseh dvanajst metod za katerakoli vrata in uporabnika. ■

ELES 100 LET FALA LAŠKO

STOLETJU PRENOSA ZAVEZANI LJUDJE

Od pionirjev elektroprenosa Fala-Laško do skrbnikov nacionalnega elektroenergetskega sistema

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

4
zaposleni

1924 – RTP LAŠKO

604
zaposlenih

2024 – SKUPINA ELES

16. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 19. - 20. MAJ 2025

DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI