Korporativna varnost

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

Letnik 2020, november • št. 24



Požarna varnost mora postati del naše varnostne zavesti

mag. Janko Cerkvenik, predsednik Gasilske zveze Slovenije

V pripravi nova Strategija o kibernetski varnosti RS

TelekomSlovenije

STE ZAŠČITENI PRED **KIBERNETSKIMI NAPADI?**

Vsak dan po omrežju potuje ogromna količina različnih podatkov, ti pa imajo danes veliko tržno vrednost. Zato so podjetja **izpostavljena vdorom ter krajam in zlorabam podatkov**. Poskrbite za ustrezno zaščito in **nadzorujte vsa tveganja kibernetskih napadov** s pomočjo Operativnega centra kibernetske varnosti Telekoma Slovenije.

OPERATIVNI CENTER KIBERNETSKE VARNOSTI TELEKOMA SLOVENIJE ZAGOTAVLJA:

ZNIŽEVANJE OPERATIVNIH TVEGANJ POVEZANIH S KIBERNETSKO VARNOSTJO

+ DOSEGANJE IN OHRANJANJE SKLADNOSTI S STANDARDI IN REGULATIVO

+ ZAZNAVANJE VARNOSTNIH DOGODKOV, ODZIVANJE, OMEJITEV IN POVRNITEV PODATKOV IN STORITEV



OPERATIVNI CENTER KIBERNETSKE VARNOSTI TELEKOMA SLOVENIJE OMOGOČA VIŠJO RAVEN VARNOSTI OB NIŽJIH STROŠKIH.

www.telekom.si/poslovni



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
NOVEMBER 2020

Izvod revije je brezplačen

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

ISSN 2232-6170

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

Situacija z epidemijo COVID-19 se ne umirja. Še več, prišel je drugi val, ki pa je presegel napovedi oziroma pričakovanja o možnem obsegu. Posamezniki, organizacije in družba kot celota, se ponovno sooča z resno krizno situacijo, ki je že zdavnaj presegla ne samo zdravstveni vidik, temveč lahko govorimo o multiplikativni krizi, ki se je zajedla v vse pore družbe. Seveda je v tem kontekstu zagotavljanje varnosti izredno pomembno. Ni pa korona kriza edini dejavnik, ki v mednarodnem varnostnem okolju predstavlja pomembne izzive. Ob tem se z nezmanjšanim obsegom pojavlja cela vrsta že poznanih varnostno izpostavljenih dejavnikov, kot so kibernetski napadi in kibernetski kriminal, terorizem in radikalizacija, geopolitične napetosti, odtujevanje ključnih podatkov v organizacijah in še bi lahko naštevali. Vsi ti varnostniki dejavniki so bili v zadnjem obdobju, pod plaščem medijskega fokusa, usmerjenega v epidemijo koronavirusa, nekoliko potisnjeni v ozadje. Preusmerjanje fokusa pa je lahko za učinkovito obvladovanje tveganj v naših organizacijah zelo nevarno. Tega se morajo predvsem zavedati strokovnjaki s področja korporativne varnosti. Z gotovostjo lahko trdimo, da vsaka kriza prinaša možnosti za nove koncepte. Popolna reorganizacija delovanja naših organizacij nas je prisilila v iskanje ustreznih učinkovitih poti, ki v danih razmerah omogočajo neprekinjenost delovanja osnovnih poslovnih procesov. Ravno v tem času je korporativna varnost s svojimi aktivnostmi in odzivnostjo pomembno prispevala k udejanjanju te nove realnosti. To na drugi strani pomeni, da je prepoznavnost tega procesa pri strateških voditeljih organizacij postala dejstvo, ki ima lahko v prihodnosti pomembne vplive na hitrost nadaljnjega razvoja korporativne varnosti, kot profesije in ključnega organizacijskega procesa.

Tokratno številko revije Korporativna varnost ne uokvirjamo samo v stanje epidemije in izkušnje ter odzive na to tveganje. Vsebino smo želeli postaviti dovolj široko, da v tem okviru prenesemo določene nove vidike in izkušnje tudi na področjih, kot so uvajanje novih tehnologij. Področju kibernetske varnosti tudi tokrat namenjamo pomemben spekter prispevkov v sami reviji, prostor pa dajemo tudi ostalim varnostnim vsebinam. Posebej bi želel izpostaviti strateško geopolitično oceno, ki jo prinaša tokratna kolumna. Izkoristili smo priložnost in se pogovorili s pomembnimi strateškimi voditelji in strokovnjaki z različnih področij, ki z nami delijo svoje izkušnje in strateške poglede. Del prostora namenjamo tudi reportaži iz nedavno končanih Dnevov korporativne varnosti 2020. Revija pa prinaša tudi druge odlične in strokovno informativne teme, ki bodo strokovnjakom različnih profilov pomagale pri širitvi njihovega strokovnega razumevanja varnostnega okolja in procesov, ki stojijo pred njimi.

V uredništvu revije upamo, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji. Za vas se bomo skupaj trudili tudi v bodoče. Za konec nam dovolite, da vam ob dejstvu, da je to zadnja letošnja številka, zaželimo vse dobro, predvsem obilo zdravja in osebne sreče, ki bo dobra podlaga za uspešno delo v prihodnjem letu.

izr. prof. dr. Denis Čaleta
Glavni urednik



KOLUMNA
Vojko Volk, veleposlanik

ONSTRAN KITAJSKEGA ZIDU

9



INTERVJU
Matjaž Tavčar, direktor Službe za korporativno varnost v UKC Ljubljana

V ČASU KRIZE SMO USPELI ZAGOTOVITI NEPREKINJENO DELOVANJE KRITIČNE INFRASTRUKTURE

17



AVTOMATIČNO MERJENJE TELESNE TEMPERATURE – IZZIVI UPORABE V PRAKSI

Novi koronavirus (COVID-19), ki se je pojavil praktično čez noč, je hipoma spremenil naša življenja in zaradi uvajanja ukrepov za zajezitev njegovega širjenja dodobra ohromil ali celo zaustavil delovanje celotnih panog in posledično upočasnil dobršen del gospodarstva.

22



KIBERNETSKA VARNOST JE NEPOGREŠLJIV DEL SODOBNEGA POSLOVANJA

Ne glede na to, v kateri gospodarski panogi posluje vaše podjetje, mora skrb za kibernetsko varnost postati temeljni gradnik strategije poslovanja. Kraje podatkov in/ali denarja, izklopa sistemov ter izgube ugleda si danes zares nihče ne more privoščiti, še toliko manj industrijska okolja in podjetja, ki upravljajo kritično infrastrukturo države.

33



SODELOVANJE NOTRANJE REVIZIJE IN INFORMACIJSKE VARNOSTI PRI OBVLADOVANJU TVEGANJ KIBERNETSKE VARNOSTI

Tveganja postajajo v sodobnem poslovnem okolju čedalje bolj prepletena, kar pomeni, da je obvladovanje vseh tveganj postalo prioriteta vseh organizacij, če želijo preživeti.

37

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Janko Cerkvenik,
predsednik Gasilske zveze Slovenije*

POŽARNA VARNOST MORA POSTATI DEL NAŠE VARNOSTNE ZAVESTI

Mesec oktober je med drugim tudi mesec požarne varnosti. To je bila odlična priložnost, da se o izzivih in bodočih načrtih na področju požarne varnosti pogovorimo s predsednikom Gasilske zveze Slovenije mag. Jankom Cerkvenikom.

Kako kot predsednik vidite nadaljnji razvoj GZS v teh zahtevnih gospodarskih in družbenih okoliščinah?

Razvoj gasilske organizacije na Slovenskem je bil, in ostaja, velik izziv vseh funkcionarjev, saj se zavedamo našega pomena in ugleda v javnosti. Moji najpomembnejši nalogi sta zagotavljanje človeških in finančnih virov, primerna komunikacija na vseh nivojih in predstavnost. Pri tem se zavedam, da moram z organi upravljanja in vodenja dajati primeren vzgled ter ustvarjati vse potrebne pogoje za razvoj avtentičnega in agilnega vodenja. Pri zagotavljanju človeških virov se opiram na našo tradicijo in organiziranost, z doslednim upoštevanjem pomembnosti vrednot, ki jih neguje naša organizacija. Pri zagotavljanju finančnih virov, glede na sedanje gospodarske okoliščine, ko razmere niso najboljše, se jim pa moramo prilagajati. Lahko pohvalim, da država in občine, razumejo naše potrebe in poskrbijo za primerno finančno podporo za naše redno delovanje. Žal gasilci prevzemamo vedno več novih nalog pri odpravljanju podnebnih in drugih sprememb, ki zahtevajo dodatna znanja in novo primerno opremo, za zagotavljanje osebne in v nadaljevanju kolektivne varnosti. Veseli me, da država, lokalne skupnosti in gospodarstvo razumejo naše potrebe in pripravljenost, da jih dogovorno tudi rešujemo in postopoma realiziramo.

> Veseli me, da država, lokalne skupnosti in gospodarstvo razumejo naše potrebe in pripravljenost, da jih dogovorno tudi rešujemo in postopoma realiziramo.

Mesec oktober je mesec požarne varnosti. Kako ocenjujete stanje na področju zavedanja o pomenu požarne varnosti v obdobju, ko so vse oči in viri usmerjeni v obvladovanje zdravstvene krize pogojene s korona virusom?

Vsako leto v mesecu oktobru preverjamo naše znanje in praktične izkušnje ter jih poskušamo deliti z okoljem v katerem delujemo. V spomladanskem in jesenskem času so bila usposabljanja okrnjena, za vzdrževanje praktične usposobljenosti in izvajanja veščin, smo opravili tudi manj vaj. Kljub temu skrbimo, da teoretične in praktične vsebine vzdržujemo, saj se zavedamo, da moramo poleg zagotavljanja požarne varnosti, v času krize pomagati tudi pri drugih aktivnostih. Tako se povezujemo z enotami ZiR, opravljamo operativne naloge z ustrezno logistiko tako organizacijam in oskrbi občanov, dekontaminacijo skupnih prostorov in vključujemo se v vse naloge, ki jih narekujejo ukrepi Civilne zaščite. Pri zasledovanju mesečnih statističnih podatkov, zaradi ukrepov korona krize, ne beležimo poslabšanja stanja na področju požarne varnosti. Iz navedenega lahko sklepamo, da se, posamezniki in družba, zavedajo pomena lastne in kolektivne varnosti in da še poznamo samozaščitne ukrepe.

Kljub omenjeni zdravstveni krizi se člani vaše organizacije pojavljajo v prvi vrsti intervencijskih služb ob na-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Pri zasledovanju mesečnih statističnih podatkov, zaradi ukrepov korona krize, ne beležimo poslabšanja stanja na področju požarne varnosti. Iz navedenega lahko sklepamo, da se, posamezniki in družba, zavedajo pomena lastne in kolektivne varnosti in da še poznamo samozaščitne ukrepe.

ravnih in drugih nesrečah, ki niso v tem obdobju nič manjše. Kako zagotavljate ustrezno delovanje gasilske organizacije, kljub nevarnostim, ki jih za vaše pripadnike prinaša tveganje korona virusa?

Tudi gasilci smo se morali prilagoditi novim razmeram, še naprej vse intervencije opravljamo nemoteno vendar ob upoštevanju varnostnih ukrepov. Skupaj z URSZR smo pripravili jasna navodila, da je možnost okužbe čim manjša. Smo se pa dogovorili, da se gasilci ne vključujemo v ostale prostovoljne aktivnosti, ki jih je potrebno postoriti v posamezni občini. Želimo ohraniti zdravo operativno jedro, prostovoljca lahko lažje nadomestiš, kot pa gasilca z ustreznim znanjem.

Kakšen je vaš pogled na odprta vprašanja, ki jih prinašajo procesi prostovoljnosti, profesionalnosti in poklicnosti v gasilski organizaciji?

Pogled je zelo jasen, želimo, da je še naprej lokalna skupnost odgovorna, tako za prostovoljce, kot za poklicne gasilce. V Sloveniji imamo gasilstvo tako organizirano, da temelji na prostovoljcih (okrog 50.000 operativnih gasilcev in okrog 700 poklicnih gasilcev, ki opravljajo javno gasilsko službo). Poklicne gasilske enote imamo samo v večjih mestih. Kombinacija, ki jo imamo je zelo dobra in v praksi odlično deluje, skupaj se dopolnjujemo. Tudi odnosi so se v zadnjem obdobju zelo izboljšali, na terenu ni več nesoglasij, kdo kaj in kdo je bolj pomemben. Oboji imamo dobre in slabe lastnosti, skupaj pa smo močni. Samo s poklicnimi gasilci ne moremo doseči takšne kvalitete pomoči, kot jo imamo danes, sploh pri večjih naravnih nesrečah, kjer poklicnih gasilcev skoraj ni na terenu.

Izobraževanje in usposabljanje verjetno tudi naprej ostaja ključna komponenta vložkov v kadrovski potencial gasilske organizacije. Kakšni so vaši načrti na tem področju?

Na tem področju se nam je v prvem in sedaj v drugem valu skoraj vse ustavilo. Tukaj imamo največ težav, pa ne samo pri vajah in usposabljanjih, tudi pri drugih aktivnostih je delo zastalo ali se v celoti ustavilo. To se zelo pozna pri delu z mladimi, bojimo se, da bo proces vračanja v normalno stanje zelo težak. Se pa prilagajamo novim razmeram, kar nekaj aktivnosti že poteka na daljavo, tudi usposabljanja prilagajamo, oziroma ustvarjamo pogoje za izvajanje na daljavo, vsaj teoretičnega dela, praktičen žal ne gre.

So po vašem mnenju procesi centralizacije državne uprave in s tem tudi dejavnosti kriznega upravljanja, ki jih združuje Uprava RS za zaščito in reševanje pravi korak v smeri zagotavljanja hitrega odzivanja na naravne in druge nesreče?

Do neke mere da, vendar se nobena državna enota ne more odzvati takoj, sistem ni tako zastavljen. Vključevanje države je bolj v vlogi podpore ob večjih intervencijah, sodeluje pa z enotami, ki so specializirane za posebne dogodke. V Sloveniji se te enote redko uporabljajo, so pa uspešno sodelovale v tujini. Centralizacija državne uprave in s tem tudi dejavnost kriznega upravljanja, je pomembna takrat, ko so razmere zares kritične (žled) in je v to vključenih več sil sistema zaščite in reše

vanja. Pri nas imamo sistem tako zastavljen, da se z njim ni potrebo ukvarjati na nivoju države. Ob klicu na številko 112, se stvari začnejo odvijati same po sebi in so jasno določene tudi do najbolj zahtevnih intervencij.

Opremljenost gasilcev ne sledi potrebam realnega okolja in tempu, ki bi si ga verjetno vsi želeli. Kaj lahko naredimo na področju opremljanja in s tem dvigovanja učinkovitosti dela profesionalnih gasilskih enot?

Ne moremo ravno reči, da smo slabo opremljeni, kvalitetne intervencije ni brez ustreznega znanja in ustrezne zaščitne in ostale opreme. Ravno na teh dveh področjih smo v zadnjih 20 -25 letih naredili največ, naloge opravljamo zelo profesionalno tako poklicni kot prostovoljni, na terenu so te razlike vedno manjše. Nove tehnologije in številne nevarnosti povezane z njimi pa nas silijo, da se moramo prilagajati novim razmeram, z znanjem in tehniko, ki pa je običajno zelo draga. Primanjkuje nam predvsem specialne tehnike, zato smo veseli, da bomo lahko v naslednji evropski perspektivi 2021 – 2027 tudi gasilci sodelovali pri črpanju EU sredstev, načrti so zelo spodbudni ravno na področju nabave ustrezne specialne tehnike.

Prostovoljna gasilska društva so v tem okviru verjetno še bolj problematična in močno odvisna od finančne moči lokalne skupnosti?

Financiranje gasilske organizacije na lokalni ravni je urejeno z Zakonom o gasilstvu in je v pristojnosti občin, katerim država priporoča, da v svojih proračunih namenijo za opravljanje javne gasilske službe 2,5% od primerne porabe občine. Zavedamo se, da povsod ni mogoče zagotavljati višino teh sredstev, vendar se krovna organizacija trudi, da bi v razgovorih z zakonodajalcem dosegla razbremenitev občin, na način, da bi določene njihove obveznosti pokrila država. Tako so v zaključni fazi usklajevanja, da država prevzame breme zavarovanja prostovoljnih in poklicnih gasilcev.
Večja težava je zagotavljanje lastnih virov gasilskih društev, ki so zaradi korona krize povsem upadli, saj so zaradi ukrepov, ki prepovedujejo druženja in družabne dogodke, društva ostala brez nekaterih virov dohodka.

Nam lahko zaupate vizijo nadaljnjega razvoja gasilstva na področju večjih industrijskih obratov?

S preoblikovanjem gospodarskih družb koncem 20. stoletja, je na področju zagotavljanja požarne varnosti nastala vrzel, saj je razmišljanje takratnih poslovodnih struktur temeljilo le na oceni zmanjšanja stroškov dela, za vsako ceno. Pri tem se odgovorni niso ozirali na pomembnost zagotavljanja človeških virov in vzdrževanja sistemov za požarno varnost. V tem času so ukinili 80 odstotkov Prosto-



voljnih industrijskih gasilskih društev. To je bil tudi začetek razkoraka med nekdaj odličnim povezovanjem odločevalcev in projektantov, nadzorom in inšpekcijskimi službami. Za obnovo obstoječih ali gradnjo novih industrijskih objektov, se niso upoštevali tehnični predpisi na tem področju. Zaradi zmanjševanja stroškov investiranja, se sistemi fizičnega in tehničnega varovanja niso vgrajevali, obstoječi pa niso bili vzdrževani. Pri tem želim izpostaviti izjemo, da pa so v okoljih kritične infrastrukture, ne glede na gospodarske razmere, vedno zagotavljali ustrezne pogoje za ustrezno požarno varnost.

Po nekaterih katastrofalnih požarih v industriji oz. gospodarskih družbah v preteklih letih, je zavedanje pomena zagotavljanja požarne varnosti dobilo nov zagon. Vsi prej omenjeni deležniki, smo z različnimi oblikami sodelovanja in usposabljanja, naredili prvi korak, da se to stanje čim prej uredi. Kot zanimivost naj omenim, da tuji vlagatelji pri razumevanju zagotavljanja sistemov varnosti, v večini primerov nimajo težav, še več, nekateri si želijo povezovanja z nami ali pridobiti potrebne informacije ali izkušnje.

Menite, da je lahko Slovensko združenje za korporativno varnost ustrezen partner Gasilski zvezi Slovenije pri zagotavljanju njenega osnovnega poslanstva, predvsem v industrijskih okoljih in okoljih delovanja kritične infrastrukture?

Slovensko združenje za korporativno varnost je že od vsega začetka odličen partner pri zagotavljanju njenega osnovnega poslanstva ter zelo dober svetovalec in kompetenten sogovornik, tako med gospodarstvom in našo stroko. Ravno na tem področju vidim priložnost za oba partnerja, da s potrebnim tehničnim znanjem in širokim krogom vrhunskih strokovnjakov, izpostavimo v na novo oblikovanih okoljih, zavedanje o vlogi osebne ali kolektivne varnosti na primerno mesto. Prepričan sem, da združenje z izmenjavo znanj, ob številnih srečanjih članov, kot tudi pri širitvi v mednarodnem okolju na dosedanjih konferencah, izpolnjuje osnovno poslanstvo, da lahko samo s potrebnim znanjem in izkušnjami, vplivamo na potrebne spremembe na področju urejanja zakonodajnih in tehničnih predpisov. ■



Slovensko združenje za korporativno varnost je že od vsega začetka odličen partner pri zagotavljanju njenega osnovnega poslanstva ter zelo dober svetovalec in kompetenten sogovornik, tako med gospodarstvom in našo stroko.

Avtor: Vojko Volk / veleposlanik



KOLUMNA

ONSTRAN KITAJSKEGA ZIDU

„Kitajce dobro poznam. S Kitajci sem zaslužil veliko denarja. Vem, kako razmišljajo Kitajci.“

/Donald J. Trump, The art of the deal/

V teh čudnih in težkih časih, ko se ves svet bojuje z virusom Covid-19, je Kitajska največja oaza sveta, kjer virusa ni več. Finančni trgi predvidevajo, da bo ob koncu leta Kitajska edina od večjih gospodarstev sveta, ki bo beležila pozitivno rast. Kitajci živijo skorajda povsem normalno, delajo in se zabavajo, le da nekoliko previdneje kot prej. Na dan ob koncu oktobra, ko tole pišem, ima 22 milijonski Peking 19 primerov okuženih s Covid-19, občina Žalec pa na isti dan 26 okuženih ... Vseh 19 okuženih je v Peking prišlo iz tujine in vsak od njih je moral v obvezno 14-dnevno karanteno v precej drag hotel in vsak je dobil policista pred vrata, ki je skrbel, da bo osama v celoti spoštovana. Ob koncu karantene še dva negativna testa in šele potem prostost. Pri vsem je seveda treba upoštevati, da je Kitajska „normalnost“ življenja vselej močno drugačna od naše, zahodne normalnosti. In je treba upoštevati tudi to, da Kitajska in zahod nikoli nista imela veliko skupnih točk v pogledih na svobodo posameznika, na družbo, pravo in državo. Na Kitajskem človek šteje toliko, kolikor je pomemben za skupnost, pri nas pa je skupnost vredna toliko, kolikor je pomembna za človeka. Pri Kitajcih so voditelji nedotakljivi, pri nas so zamenljivi. Ali še bolj preprosto in povsem naravnost; enakopravnost in demokracija sta model, ki je kitajski družbi popolnoma tuj in morda ne bo sprejet nikoli.

Zato ni čudno, da se je Kitajska najbolj približala zahodu šele v zadnjih treh desetletjih, ko je kitajska komunistična partija odpravila maoistični komunizem in si namesto družbene enakosti zadala cilj pospešenega ekonomskega razvoja. Vse odtlej se na Kitajskem vse odločitve komunistične partije sprejemajo skozi ‚cost-benefit‘ izračun, preveden najprej na cilje in koristi partijskega vodstva in šele potem na vse ostalo, nazadnje tudi na ljudi. Vodilna deseterica kitajskih komunistov sodi v sam vrh najbogatejših ljudi sveta. In tako smo dosegli točko v zgodovini, ko je dobiček združil trgovski duh Donalda Trumpa s kapitalističnim komunizmom kitajske partije. „Egoistični trgovski duh ne pozna meja in ne pozna usmiljenja do načel, razen do dobička“ je svoje strahove za prihodnost Amerike izrazil že Thomas Jefferson, ustanovni oče in tretji predsednik ZDA. Po Marxu bi lahko rekli, da je kitajski komunizem zadnja faza v razvoju kapitalizma.

Od takrat je minilo 200 let in na zahodu so bile pravice človeka počasi in po mnogih bitkah vgrajene v sistem liberalne demokracije, ki temelji na enakopravnosti vseh ljudi, ne glede na pripadnost veri ali komunistični partiji. V Evropi pa so socialistična gibanja po drugi svetovni vojni ob političnih izsilila še socialne pravice človeka, v prvi vrsti javno in vsem dostopno zdravstvo, solidarnostni pokojninski sistem, brezplačno šolstvo, plačani dopust, porodniške in bolniške... Vse tisto, česar izven Evrope ne najdemo skoraj nikjer. In ker si tovrstne, „evropske“ in za kapital škodljive blaginje želi vse več ljudi, tudi Američanov, je bil prav v času Trumpa „socializem“ izenačen s komunizmom, kar je podobno, kot če bi enačili socializem in nacizem. Ključna Trumpova zmerljivka za Joe Bidena je, da je socialist, ki bo v Ameriki uvedel komunizem. Pod komunizem pa Trump pomete vse tisto, kar Amerika kot ena najbogatejših družb sveta svojim ljudem ni sposobna nuditi; blaginjo za vse, tudi za tiste, ki ne zmorejo tekmovati ali pa tega enostavno niso sposobni. Amerika vztraja v darwinističnem dojemanju družbe, ki temelji na tekmi in zanemarja naravno okolje. S tem postaja naravni paradoks; če bi se vsa moč

Na Kitajskem človek šteje toliko, kolikor je pomemben za skupnost, pri nas pa je skupnost vredna toliko, kolikor je pomembna za človeka. Pri Kitajcih so voditelji nedotakljivi, pri nas so zamenljivi.

Nihče si ne dela več utvar, da lahko ZDA in Kitajska tekmujeta za prevlado kjerkoli drugje kot v Evropi, ki je največji trg sveta in edini lahko kupuje njihove najnaprednejše tehnološke izdelke.

nakopičila samo pri eni vrsti, bi narava posegla in vzpostavila ravnovesje. To se je primerilo dinozavrom, ki so potacali podrast in pojedli vse okrog sebe, na koncu pa ostali brez možnosti za preživetje.

Ko je leta 2016 v ZDA presenetljivo zmagal Donald Trump, je analiza razlogov za njegovo zmago pokazala predvsem dvoje. Prvič, da so se ameriški volivci naveličali neuresničenih obljub o sociali in solidarnosti v ameriški družbi, in drugič, da so imeli dovolj predsednikov, ki so se veliko ukvarjali z zunanjim svetom in premalo z Ameriko samo. Glede prvega je sledilo razočaranje, glede drugega pa zadovoljstvo; Trump se je res držal pravila ‚Najprej Amerika'. A čeprav ni nikjer sprožil nove vojne je že kmalu postalo jasno, da svet, v katerem Amerika ne igra vloge šerifa, ni nič varnejši od prejšnjega. Še več, število beguncev in razseljenih oseb je v zadnjih letih doseglo rekordne razmere, enake rekorde dosega revščina in število lačnih ljudi na svetu. Trump si je zadal nekaj jasnih ciljev, prvi med vsemi pa je bil utrditi gospodarsko in vojaško prevlado ZDA v svetu. Za ta cilj je bil pripravljen skleniti zavezništvo s Putinovo Rusijo, s trgovinskimi sankcijami pa omejiti vpliv Kitajske v svetovni trgovini in si nazadnje, kot češnjo na torti, z revidiranimi trgovinskimi sporazumi podrediti EU. Trump si je želel, da bi se o trgovinskih sporazumih pogajal z vsako državo posebej, ne pa z Evropsko komisijo, ki se trdo pogaja za celo EU. Edino tako bi lahko strl Nemčijo, česar si je želel še posebej. Vzvod podrejanja EU je bila energetika oziroma ponujanje ameriškega zemeljskega plina v zameno za neodvisnost od ruskega plina ter povečevanje stroškov za varnost in obrambo. Pri plinu se ni izšlo, ker je ruski plin zlahka najcenejši in ker v Evropi že skoraj desetletje obstajajo presežki plina, ponudba pa narašča. Pri varnosti in obrambi je bilo uspeha še manj, ker sta se Francija in Nemčija uprli in poslej odkrito stavita na lastne in evropske vire, tako pri proizvodnji orožij in obrambnih sistemov kot tudi pri zamislih za evropsko vojsko, ki bi delovala pod okriljem EU. EU postaja ambiciozna tudi v vesolju, kar je zadnji mejnik evroatlantskega zavezništva.

Po štirih letih mandata vse kaže, da je Trumpu od vseh namer še najbolj uspelo utrditi ameriško gospodarstvo in omejiti vpliv Kitajske, ki se ji je po ameriških trgovinskih sankcijah močno znižala gospodarska rast. Podobno, kot je Rusija strahovito klecnila po uvedbi zahodnih sankcij po aneksiji Krima, so ameriške sankcije močno prizadele Kitajsko. Ostre reakcije Kitajske na ameriške sankcije pa so odprle oči tudi Evropi, ki je končno zaslutila, da bo tudi evropski trg potreben dodatne zaščite. Ob krizi z virusom Covid-19 je odvisnost Evrope od zaščitnih izdelkov in opreme iz Kitajske na plan udarila tako močno, da je bila streznitev hipna. Drugi strateški cilj Trumpa, zavezništvo s Putinom, pa se zaradi domačih afer o razkritju podatkov o vplivu Rusije na ameriške volitve ni obnesel. Ko gre za Evropo je kot Trumpov „dosežek" še najbolj opazen močno omajan vpliv evroatlantskega zavezništva, celo tako močno, da je Macron govoril, da je „NATO klinično mrtev" in da se posledično med evropskimi zavezniki vse bolj utrjuje spoznanje o nuji ustanovitve evropske vojske. Macron je bil sicer prvi, ki je v začetku mandata s Trumpom stkal močne vezi, a si hitro premislil in se od Trumpa distanciral, podobno kot kanclerka Merklova. Vse bolj zaznavna želja evropskih voditeljev je evropska varnost, ki ne bi bila več odvisna od zunanjepolitičnih muh vsakokratnega ameriškega predsednika. Pri tem ne gre samo za fizično varnost in obrambo ampak za varnost na področju modernih tehnologij, vesoljske tehnolo-





gije, razvoja umetne inteligence in vsega, kar lahko Evropo zaščiti pred vplivi tako ameriških kot kitajskih interesov. Varnost zato postaja stvar preživetja EU.

Nihče si ne dela več utvar, da lahko ZDA in Kitajska tekmujeta za prevlado kjerkoli drugje kot v Evropi, ki je največji trg sveta in edini lahko kupuje njihove najnaprednejše tehnološke izdelke. Kitajska skoraj polovico svojega izvoza opravi v Evropo (600 mrd eur) iz EU pa uvozi skoraj 3 krat manj, zato je njen trgovinski položaj usodno odvisen od odprtosti evropskega trga (v Indijo Kitajska izvozi 80 mrd evrov letno, op.a) v ZDA pa za 450 mrd. ZDA izvozijo v Evropo za 560 mrd eur, a za razliko od Kitajske ima Evropa močan presežek (150 mrd). Iz teh razmerij izhaja, da tri gospodarske velesile obvladujejo trgovino sveta, pri čemer so vloge Japonske, Rusije ali Indije v teh razmerjih bolj epizodne kot strateške. Evropa si zato ne more privoščiti, da bi kot prva gospodarska sila sveta ostala potisnjena na rob v strateških političnih odločitvah, ki zadevajo mir in stabilnost sveta in kjer ima ob Rusiji in Indiji vse več vloge tudi izzivalna in vse bolj agresivna Turčija.

Zaradi Trumpovih pritiskov na Nemčijo si je ta znotraj EU utrdila položaj sile, brez katere ne zmore praktično nobeno evropsko gospodarstvo več. Prav tako niso bile uspešne ambicije Kitajske, da bi v Evropi prevladala s svojimi gradbenimi in logističnimi podjetji. Nemčija in Francija sta dosegli, da EU trdno vztraja, da morajo kitajska podjetja sodelovati na razpisih, tam pa imajo problem dumpinga. Nobeno evropsko podjetje namreč ne more konkurirati kitajskim pri nizkih plačilih delavcev in strokovnjakov, zaradi česar so kitajska podjetja vselej najcenejša. To se je primerilo v pristanišču Trst, ki se je odpovedalo sodelovanju s Kitajci in septembra letos sprejelo nemškega partnerja (HHLA Hamburg). Podobno je bilo z razpisom za gradnjo drugega tira Koper-Divača v Sloveniji. Da o usodi kitajske tehnologije 5G v EU niti ne govorimo, saj tudi Kitajci ne dovolijo nikomur, da na njihov trg vstopi s svojimi tehnologijami.

> Gre za to, da dobro poznamo predvsem sami sebe in da varujemo naše dosežke na področju pravic človeka, varovanja okolja in zdravja ljudi in da s Kitajsko vzpostavimo uravnotežene odnose.

Naj sklenem. Še nedavno je veljalo, da brez kitajskih proizvodov srednji razred zahoda ne bi mogel napredovati, nižji sloji pa ne preživeti. V 80-ih je bila na tem zasnovana filozofija Wal-Mart trgovin v ZDA. Ko je v 90-ih vse skupaj pljusknilo v Evropo je bilo drugače. Ceneni kitajski izdelki in hrana so se prijeli v revnejših delih Evrope, drugod pa manj. Danes je evropski potrošnik močno ozaveščen o zdravi hrani in okolju, obleki, javnem prevozu, izrabi energije, vode, zraka, zdravem življenju. To so načela, ki jih v Evropi vnašamo v naše predpise in zakone. V ospredju ni več samo dobiček ampak počutje in zdravje ljudi. Vse to pa so stvari, ki so tesno povezane z demokracijo, torej s tistim, česar Kitajska nima. Zato je ugotovitev Donalda Trumpa iz uvodnega citata danes že krepko presežena. Ne gre več za to, da je treba Kitajsko dobro poznati, da bi z njo bolje služili denar. Gre za to, da dobro poznamo predvsem sami sebe in da varujemo naše dosežke na področju pravic človeka, varovanja okolja in zdravja ljudi in da s Kitajsko vzpostavimo uravnotežene odnose. Če se s Kitajsko spustimo v divjo tekmo dobičkov in presežkov, smo bitko izgubili že vnaprej. Spoznanje je preprosto; onstran Kitajskega zidu je Kitajska, tostran pa je ves ostali svet. ■

Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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.

telemach
Mestna občina Ljubljana
tus
Občina Slovenska Bistrica
NIJZ Nacionalni inštitut za javno zdravje
Pošta Slovenije
as
Ministrstvo za infrastrukturo
Javni medobčinski stanovanjski sklad Maribor
SmartIS Pametni informacijski sistemi
Informacijske storitve in inženiring, d.o.o. INFORMATIKA
triglav
PETROL Energija za življenje
Telekom Slovenije
AKRAPOVIČ
interblock Luxury Gaming Products
spica
Ford SUMMIT AVTO
Elektro Ljubljana
Elita i.b. d.o.o.
SIEMENS
DARS
ZARJA ELEKTRONIKA
UNISTAR PRO
Nova KBM Pripravljeni na jutri
LON
CINKARNA
Slovenske železnice
energetika Ljubljana

www.ics-institut.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
izr. prof. dr. Denis Čaleta,
predsednik Slovenskega združenja korporativne varnosti

ČAS KRIZE LAHKO PRINESE TUDI NOVE PRILOŽNOSTI

O letu, ki se zaključuje in izzivih, ki stojijo pred Slovenskim združenjem korporativne varnosti, smo se pogovarjali z njenim predsednikom dr. Denisom Čaleto. V odkritem pogovoru nam je podrobneje predstavil delo združenja v tem zahtevnem času in načrte razvoja za naslednje obdobje.

Počasi se zaključuje nenavadno in izzivov polno leto 2020. Kako bi ga ocenili?

Res je, zaključuje se leto, ki je pred nas postavilo resne izzive za normalno delovanje širše družbene skupnosti. Tako obsežnega vpliva pandemije koronavirusa ni uspel predvideti praktično nihče, kar je za seboj potegnilo resne motnje v delovanju družbe, gospodarstva, meddržavnih in tudi neposredno medosebnih odnosov. Vse to pa je prineslo tudi pomembne izzive na področju zagotavljanja varnosti na vseh možnih nivojih v družbi in poslovnih organizacijah. Zavedati se je potrebno, da grožnje in tveganja, ki smo jih poznali do sedaj niso bili nič manjši, temveč so se v tem obdobju koronakrize samo modificirali. Še vedno so, poleg obvladovanja koronakrize, pred nami pomembni izzivi obvladovanja kibernetskih tveganj, upoštevanja človeškega potenciala, kot pomembnega agregatorja tveganj, terorizma, organiziranega kriminala in korupcije ter grobega uveljavljanja strateških interesov med pomembnimi geostrateškimi igralci V globalnem okolju. Predvsem pa so bili izpostavljeni izzivi, kako v danih razmerah zagotoviti varno in neprekinjeno delovanje organizacij, še posebno tistih, ki upravljajo s kritično infrastrukturo in izvajajo bistvene storitve.

Slovensko združenje za korporativno varnost je tudi v letošnjem letu z nezmanjšano hitrostjo izvajal aktivnosti, ki jih predvideva njegovo poslanstvo. Posebno me veseli, da so vrednost te referenčne asociacije prepoznali tako ključni strateški odločevalci na državni ravni, kakor tudi strateški management v poslovnih organizacijah.

Seveda pa bi želel jasno poudariti, da vsaka kriza prinaša tudi priložnosti za novo oceno situacije, učinkovitosti dosedanjih procesov in organizacijskih pristopov ter porabe virov. Korporativna varnost je, kot proces in dejavnost v letošnjem letu, zaradi izpostavljenosti pri izvajanju procesov obvladovanja koronakrize, močno pridobila na pomembnosti in prepoznavnosti v različnih organizacijskih okoljih. S strokovnega stališča je to vsekakor močan pozitivni vidik krize, ki smo ji priča v letošnjem letu.

Slovensko združenje za korporativno varnost uspešno nadaljuje svoje poslanstvo. Kako bi ocenili letošnje delovanje združenja?

Slovensko združenje za korporativno varnost je tudi v letošnjem letu z nezmanjšano hitrostjo izvajal aktivnosti, ki jih predvideva njegovo poslanstvo. Posebno me veseli, da so vrednost te referenčne asociacije prepoznali tako ključni strateški odločevalci na državni ravni, kakor tudi strateški management v poslovnih organizacijah. V združenje so že vključene ključne državne institucije s področja kibernetske varnosti in kritične infrastrukture, kot so Ministrstvo za infrastrukturo, AKOS, SI-CERT, Informacijski pooblaščenec Republike Slovenije, Nacionalni inštitut za javno zdravje, pomembne lokalne skupnosti, še posebej Mestna občina Ljubljana, večina najpomembnejših upravljalcev kritične infra-

*avtor je član Slovenskega združenja korporativne varnosti



strukture in izvajalcev bistvenih storitev ter druge organizacije in institucije ter nacionalne zveze, kot na primer Gasilska zveza Slovenije in Nogometna zveza Slovenije, kot ene najpomembnejših športnih zvez. Vse to kaže, da ravno ta raznolikost članov pomeni največjo sinergijo in strokovno moč ter avtoriteto združenja. Vsak izziv je možno analizirati in obravnavati z različnih zornih kotov ter tako dobiti zelo kvalitetna izhodišča in dobro prakso, ki jo s pridom uporabljamo znotraj združenja, kakor tudi v razmerju do strateških odločevalcev. Letos smo poleg spopadanja z epidemijo COVID-19 poseben fokus namenili kibernetski varnosti in kritični infrastrukturi, posebej v smeri iskanja odgovorov, kako uskladiti zakonske okvire, da bodo usmerjeni v čim bolj jasne zahteve za zagotavljanje neprekinjenosti delovanja te ključne infrastrukture in storitev ter zmanjšali nepotrebno podvajanje uporabe virov. Posebno energijo bomo ob koncu leta namenili pripravi nove Strategije kibernetske varnosti republike Slovenije, kjer želimo pomagati z znanji in izkušnjami, predvsem s stališča upravljalcev kritične infrastrukture. Na tem delu zelo tesno sodelujemo z Upravo za informacijsko varnost Republike Slovenije, ki se nam bo, po njihovih besedah, priključila v združenju v čim krajšem času. Vse to me navdaja s posebnim ponosom, da združenje eksponentno raste z novimi pomembnimi deležniki, ki bodo še okrepili vsebinsko kvaliteto združenja.

Kako je stanje korona krize vplivalo na delovanje združenja?

Zelo hitro smo se prilagodili nastali situaciji in s pomočjo različnih spletnih orodij zagotavljali nemoteno okolje in okvir za izmenjavo dobrih praks, najnovejših spoznanj in izkušenj med člani združenja. Posebno pozornost smo namenjali tudi predstavitvam določenih tehnoloških in metodoloških pristopov, ki so jih člani zaradi uveljavljanja ukrepov vlade pri obvladovanju širjenja virusa COVID-19 tudi najbolj potrebovali. Zaradi pomankanja fizičnih srečanj, ki jih vsi člani zelo pogrešamo, smo se odločili, da smo dodali še eno dodatno virtualno srečanje na mesec in tako poskušali zapolniti te vrzeli, ki so nastale zaradi onemogočanja večine fizičnih srečanj v letošnjem letu. Najbolj ponosen sem bil na naše člane, ko sem videl, kako so si v času najtežjih preizkušenj za naše organizacije, bili pripravljeni priskočiti na pomoč, z idejami, izkušnjami, tudi zaščitno opremo, če je bilo to potrebno. V takih situacijah se pokaže, kako osnovna postulata združenja »Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha« in »A buno disce omnes (po enem spoznaj vse)«, zares živita. Močno smo se trudili predvsem povezati vse niti in komunikacijo tam, kjer je bila potrebna. SKUPAJ SMO RES MOČNEJŠI!

Stanje na področju varnostnih tveganj postaja vedno bolj kompleksno. Kje vidite v prihodnje največje izzive s katerimi se bodo srečevali člani združenja?

Na žalost moramo ugotoviti, da nas bo neposredni in posredni vpliv COVID-19 spremljal še naprej v naslednjem obdobju. Seveda to ne pomeni, da bodo ostala tveganja zaradi tega potisnjena kaj bolj na obrobje. Podatki kažejo na dejstvo, da se zaradi epidemije ni nič zmanjšalo število kibernetskih napadov na informacijske sisteme organizacij. Še več, kibernetski napadi so se izvajali tudi na ključne zdravstvene organizacije, ki so bile posebej obremenjene in usmerjene v obvladovanje te zdravstvene krize. Zaradi ukrepov omejevanja druženja bodo v prihodnosti še posebej izpostavljeni vsi dejavniki povezani s človeškim faktorjem in napetostmi, ki

Naša pomembna usmeritev in želja je, da se pri pripravi določenih novih zakonskih rešitev in pristopov na področjih korporativne varnosti, še posebej kritične infrastrukture in kibernetske varnosti, združenje pojavi, kot pomemben deležnik v razpravi priprave teh predlogov. S svojim znanjem in izkušnjami lahko pomembno prispevamo h kvaliteti oblikovanih rešitev, ki bodo dosegla svoj namen višje ravni varnosti v naši družbi in naših organizacijah.

jih bodo prinašali različni psihološki vidiki oz. posledice trenutne epidemije. Tukaj nikakor ne smemo zanemariti procesov radikalizacije, ki so povezani z različnimi dejavniki in se rezultirajo skozi možna teroristična dejanja, AMOK situacije, namernemu odtujevanju ključnih informacij organizacije in podobno.

Čemu nameravate v prihodnjem letu v Slovenskem združenju za korporativno varnost posvetiti posebne poudarke?

Kot sem poudaril že v zgornjih odgovorih bomo poskušali biti posebej aktivni pri naši strokovni podpori na področju priprave nove Strategije kibernetske varnosti, da bo le ta realna in podkrepljena z ustreznimi viri in jasnimi odgovornimi subjekti za njeno implementacijo. Pomembno področje, ki ga imamo v naših načrtih, je tudi doseči določene vsebinske popravke in uskladitev zakonodaje s področja kritične infrastrukture s področjem zagotavljanja informacijske varnosti. V splošnem pa bodo naša glavna usmeritev še naprej procesi zagotavljanja neprekinjenega delovanja kritične infrastrukture, obravnave in analize varnostnega okolja, kibernetske varnosti in izzivov, ki jih prinaša človeški potencial v naših organizacijah.

Kako lahko Slovensko združenje vpliva na pomembne procese, ki se bodo v prihodnje odvijali na področju kritične infrastrukture?

Naša pomembna usmeritev in želja je, da se pri pripravi določenih novih zakonskih rešitev in pristopov na področjih korporativne varnosti, še posebej kritične infrastrukture in kibernetske varnosti, združenje pojavi, kot pomemben deležnik v razpravi priprave teh predlogov. S svojim znanjem in izkušnjami lahko pomembno prispevamo h kvaliteti oblikovanih rešitev, ki bodo dosegla svoj namen višje ravni varnosti v naši družbi in naših organizacijah. Pomembo pozornost posvečamo tudi splošnemu dvigovanju varnostnega zavedanja v različnih organizacijskih okoljih. V to usmerjamo ogromno energije, ki se odraža skozi pomembne rezultate. Posebno želimo izpostaviti kanale, kot so revija Korporativna varnost ter določeni usmerjeni posveti in okrogle mize, kjer širši javnosti posredujemo in odpiramo aktualne vsebine s področja korporativne varnosti v najširšem pomenu besede.

Kako bi lahko ocenili sodelovanje z državo, kot zakonodajalcem na pomembnih področjih povezanih z neprekinjenim delovanjem kritične infrastrukture in zagotavljanjem kibernetske varnosti?

Sodelovanje bi ocenil, kot zelo dobro. Seveda so vedno priložnosti za nadgradnjo in poglobitev sodelovanja. Pomembno je, da strateški voditelji teh državnih organov združenje prepoznavajo, kot učinkovito platformo za izmenjavo dobrih praks in izmenjavo strokovnih informacij. Že to, da naše združenje sestavljajo organizacije z različnih strateških okolij, nam daje tudi v prihodnosti priložnost, da skrajšamo in vsebinsko okrepimo potreben pretok podatkov med vsemi deležniki, ki so pomembni pri vzpostavitvi močnega in prožnega varnostnega sistema v Republiki Sloveniji in posredno tudi varnostnih sistemov v posameznih organizacijah.

Kje vidite še določene priložnosti za hitrejši razvoj področja korporativne varnosti v Republiki Sloveniji?

Globalno varnostno okolje nas sili v smeri vedno večjega pomena in vpetosti korporativne varnosti v naše ključne poslovne procese v organizacijah. Kriza, kot smo ji priča trenutno, te procese še pospešuje. So pa po naših ugotovitvah zelo velike razlike med posameznimi organizacijskimi okolji. Čimprej moramo doseči minimalne varnostne standarde v vseh organizacijskih sredinah. Zelo pomembno vlogo v tem okviru bo imelo tudi izobraževanje, in to ne samo strokovnjakov s področja korporativne varnosti, temveč tudi strateških voditeljev, da bodo imeli boljše razumevanje za orodja in zmogljivosti, katere jim omogoča proces korporativne varnosti.

Kako bo v prihodnjem letu na delovanje naših organizacij vplivalo globalno varnostno okolje?

Ta vpliv je bil že do sedaj zelo močan, saj je Slovenija s svojim majhnim in odrtim gospodarstvom močno vpeta v mednarodno okolje. Poleg že navedenih varnostnih tveganj, ki sem jih omenil v prejšnji razpravi, bi želel posebej poudariti tveganja, ki jih bo v globalnem varnostnem okolju prineslo globalno tekmovanje med strateškimi mednarodnimi igralci. Nedavni rezultati predsedniških volitev v ZDA lahko te napetosti nekoliko zmanjšajo, nikakor pa jih ne bodo odpravili. Ti izzivi, ki so posledično povezani tudi z varnostnimi tveganji, bodo še posebej pomembni za organizacije, ki so močno izvozno usmerjene in bodo v prihodnosti morale znati skozi ustrezne analize zagotavljati tudi razumevanje vseh varnostnih implikacij za njihovo nemoteno poslovanje. Samo ustrezno razumevanje varnostnega okolja, v katerem poslujejo, jim bo skozi ustrezno obvladovanje varnostnih tveganj, lahko v določenih primerih to predstavljalo pomembno konkurenčno prednost.

Kaj želite za konec sporočiti članom Slovenskega združenja za korporativno varnost.

Za konec mi dovolite, da se vsem članom Slovenskega združenja korporativne varnosti zahvalim za njihovo požrtvovalnost in odrekanje, ki so ga letos vlagali v obvladovanje te pomembne zdravstvene krize. Želim jim veliko osebne sreče, zdravja in predvsem pozitivne energije, ki jo bomo v Slovenskem združenju za korporativno varnost v naslednjem obdobju zelo veseli. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Matjaž Tavčar,
direktor Službe za korporativno varnost v UKC Ljubljana*

V ČASU KRIZE SMO USPELI ZAGOTOVITI NEPREKINJENO DELOVANJE KRITIČNE INFRASTRUKTURE

Gospod Matjaž Tavčar, direktor Službe za korporativno varnost v UKC-Ljubljana je v pogovoru z nami predstavil varnostne izzive, ki jih je čas epidemije prinesel pred najpomembnejšo organizacijo zdravstvenega sektorja.

UKC Ljubljana predstavlja glavno zdravstveno institucijo v Republiki Sloveniji. Kako bi ocenili to kratko obdobje po vzpostavitvi Službe za korporativno varnost v UKC? Kateri so tisti glavni dosežki, ki bi jih bilo potrebno izpostaviti?

Glede na to, da smo službo vzpostavili 1.1.2019 z željo, da celovito poveže obvladovanje tveganj s področja varnosti, zaščite in reševanja, smo lahko izjemno zadovoljni z vlogo, ki jo je služba izvajala in jo še izvaja na področju varovanja, zaščite in reševanja. Tudi dobro sodelovanje s Policijo, Slovensko vojsko in Civilno zaščito tako na nivoju mesta Ljubljana, kot države, je prispevalo k uspešnemu načrtovanju in izvajanju potrebnih ukrepov.

Epidemija SARS-CoV-2 v začetku leta 2020 je predstavljala dodaten izziv. Potrdilo se je, da so bile vse aktivnosti v letu 2019, kjer mislim predvsem na zagotavljanje zalog zaščitne opreme ter izdelavo načrtov delovanja UKCL, nujne in v celoti potrebne.

Trenutna kriza korona virusa in že druga razglašena epidemija je pred vas postavila pomembne zahteve za zagotavljanje varnosti v vseh objektih UKC-Ljubljana. Kakšni so bili glavni organizacijski pristopi, da ste zagotovili ustrezen nivo varnosti v teh razmerah povišane nevarnosti za vnos okužb v to pomembno zdravstveno institucijo?

Že pred epidemijo, leta 2019, smo pripravili Strategijo varovanja UKCL, katere cilj je bil evidentirati vstopne točke, ki jih lahko nadzorujemo tehnično, s kontrolo pristopa, in so namenjene zgolj zaposlenim. Vzporedno smo naredili načrt videonadzora ter tako omejili fizično varovanje objektov. Vzpostavitev tehničnega varovanja zahteva poleg samega načrtovanja tudi pripravo pravilnikov, sklepov in drugih administrativnih ukrepov za zagotavljanje varovanja podatkov. Veseli smo, da je bil odziv zaposlenih nad takimi rešitvami pozitiven in, da se tako počutijo varneje.

Večino operativnega kadra, sploh na področju fizične varnosti, zagotavljate z angažiranjem zunanjih izvajalcev. Kako vam uspe v tem obdobju povišane nevarnosti okužb zaradi epidemije zagotavljati ustrezno koordinacijo z zunanjimi izvajalci, sploh ob dejstvu, da je od njihovega učinkovitega delovanja velikokrat odvisno preprečevanje vnosov dodatnih okužb v prostore UKC-Ljubljana?

Področja korporativne varnosti se iz tehničnega in fizičnega varovanja širijo tudi na druge funkcije nadzora.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Z odredbo Vlade Republike Slovenije smo zavezani k varovanju, ki ga mora zagotavljati zasebna varnostna služba. Trenutno to varovanje izvaja podjetje Sintal, s katerim imamo neprekinjeno komunikacijo. Naši nadzorniki preverjajo izvajanje načrta varovanja in navodil na varnostnih točkah. Vsi odkloni so elektronsko beleženi v sistemu odklonov in obravnavani, kakor sledi iz akreditacije za zdravstveno dejavnost. Posledično sledijo varnostni razgovori in korektivni ukrepi. Prav z izrednimi nadzori nad uporabo zaščitne opreme smo dosegli, da so bili vdori virusa SARS-CoV-2 v naše objekte majhni in zapozneli. K temu je pripomogla tudi prepoved obiskov in omejitev nenujnih napotitev bolnikov.

Je v okviru t.i. Covid oddelkov oz. oddelkov za intenzivno nego vzpostavljen še kakšen dodaten sistem varnosti vezano na vstope in samo gibanje po teh prostorih? Ali te ukrepe nadzoruje samo medicinsko osebje ali jim tukaj Služba za korporativno varnost nudi kakšno dodatno pomoč?

Poleg vstopnih točk v te objekte smo morali zaradi pomanjkanja zdravstvenega kadra in hitrega širjenja COVID-19 oddelkov zagotoviti nadzor bolnikov preko videonadzora – »podaljšano oko«, kar nam je omogočilo, da lahko zdravstveni delavci nadzirajo vitalne funkcije več bolnikov hkrati.

Gibanje na oddelkih je nadzorovano ločeno, z najavo premikov in na nekaterih oddelkih tudi s sireno, ki opozarja, da gre za premik SARS-CoV-2 pozitivnega bolnika. Tako se morebitni mimoidoči ta čas umaknejo. Vse te tehnične rešitve usklajuje Služba za korporativno varnost. Pri tem smo morali poskrbeti tudi za vse pravne podlage, skladne z zahtevami Informacijske pooblaščenke.

Korporativna varnost že dolgo časa ni omejena samo na zagotavljanje fizičnega in tehničnega varovanja, temveč vedno bolj tudi na področje informacijske varnosti. Kakšne organizacijske in procesne spremembe se dogajajo na tem področju?

Področja korporativne varnosti se iz tehničnega in fizičnega varovanja širijo tudi na druge funkcije nadzora. Tako na nadzor poslovanja, goljufij pri izjavah za prevoz na delo, kot tudi kibernetske varnosti. Zaenkrat organizacijskih sprememb, ki bi omogočale ustrezno informacijsko varnost v okviru Službe za korporativno varnost, ni. Je pa dobrodošlo, da je komunikacija med službami odlična in dobra podlaga za rešitve, ki bodo za to potrebne.

UKC-Ljubljana je ena izmed ključnih organizacij tudi na področju zagotavljanja neprekinjenega delovanja kritične infrastrukture in izvajanja bistvenih storitev. Ima v teh procesih Služba korporativne varnosti v UKC-Ljubljana pomembno mesto? Kje je to najbolj izraženo?

UKC Ljubljana je vsekakor pomembna ustanova za obrambo in delovanje države. V okviru Službe za korporativno varnost deluje tudi enota za obrambo in zaščito, ki v izrednih razmerah organizira delovanje Štaba civilne zaščite UKCL. V tem Štabu pa so vsi predstavniki služb, ki morajo zagotavljati ne-

prekinjeno in nemoteno delovanje ustanove. Problem s katerim se srečujemo je, da vse aktivnosti, ki jih mora zagotavljati UKCL za neprekinjeno delovanje in varnost niso posebej financirane.

Glede na izdelane načrte se v prvi fazi krize oblikuje ožji Štab Civilne zaščite UKCL, ki ga sestavljajo vodja Službe za korporativno varnost, koordinator Enote za obrambo in zaščito naše službe, ki je hkrati poveljnik Civilne zaščite UKCL in njegov namestnik. V naslednji fazi pa se delovanje usklajuje preko Štaba Civilne zaščite.

Glede na dejstvo, da je UKC-Ljubljana pomemben segment v zdravstvenem sektorju ima verjetno pomembno mesto tudi pri usklajevanju z ostalimi deležniki. Nam lahko osvetlite kvaliteto in obseg sodelovanja z Ministrstvom za zdravje, NIJZ in ostalimi bolnicami na področju zagotavljanja neprekinjenosti delovanja tega sistema?

Težava, s katero smo se soočili ob epidemiji marca 2020 je da je bil UKCL ne samo vodilna ampak tudi edina ustanova v Republiki Sloveniji, ki je usmerjala delovanje zdravstvenega sistema. Žal je bilo pristojno ministrstvo na tem delu povsem obnemoglo. NIJZ, kot nosilec delovanja v primeru epidemije pa je podlegel političnim igračkanjem. Ob vsem tem smo morali ustvarjati pogoje za delo in izvajanje storitev, ne samo za COVID-19 bolnike, ampak tudi za vse ostale.

Na vse pomanjkljivosti, na katere smo opozarjali ob vsakoletnem izbruhu gripe, ni bilo odzivov. Še posebej na pomanjkanje kadra in opreme. To se je v primeru epidemije COVID-19 izkazalo, kot zamujena priložnost, ki smo jo po prvem valu vsaj z nabavo opreme delno nadomestili. Na področju kadrovskega primanjkljaja pa je to seveda v šestih mesecih nemogoče.

Ste med samo krizo povezano z obdobjem korona epidemije zaznavali kakšne pomembne anomalije in zunanje grožnje za neprekinjeno delovanje vaših organizacijskih in informacijskih sistemov?

Ob prvi, in tudi drugi epidemiji, nismo imeli groženj od zunaj. Prvo epidemijo smo obvladali z izjemnimi napori zaposlenih. Drugo epidemijo pa so zaznamovali »kolesarski protesti«, ki so dajali znake, da je ves trud naših zaposlenih zaman. To pa je povzročilo izjemne psihološke pritiske in travme zaposlenih. Tako je bilo poletno obdobje zaznamovano s prepričevanjem, da gre za resno bolezen, namesto, da bi se na jesenski val pripravljali vsi, kot družba.

Težava, s katero smo se soočili ob epidemiji marca 2020 je da je bil UKCL ne samo vodilna ampak tudi edina ustanova v Republiki Sloveniji, ki je usmerjala delovanje zdravstvenega sistema. Žal je bilo pristojno ministrstvo na tem delu povsem obnemoglo.





Za učinkovit razvoj Službe za korporativno varnost je nujno potreben ustrezen strokovno usposobljen kadrovski potencial z različnimi kompetencami znanj. Je kadrovska politika na tem področju ustrezno načrtovana in ali imate s strani strateškega vodstva UKC-Ljubljana ustrezno podporo?

Služba za korporativno varnost je nastala, kot nadgradnja Službe za obrambo in zaščito. Le-ta je bila brez kadrovskih potencialov za oblikovanje tega, kar zahteva korporativna varnost. Naslonili smo se na sodelovanje s Policijo, ki nam je na vseh področjih delovanja neizmerno pomagala. Tako so nastale tudi ustrezne podlage za oblikovanje kadrovske strukture službe, ki jo izvajamo. Služba, kot je naša brez podpore vodstva ne more biti učinkovita. In veseli smo, da so do sedaj vse uprave prepoznale pomen naše službe in jo v celoti in povsem podpirajo. Tako vsakodnevno, kot razvojno.

Kakšno stališče imate v UKC-Ljubljana vezano na sodelovanje v različnih evropskih projektih s področja obvladovanja tveganj in zagotavljanja neprekinjenosti delovanja? Menite, da lahko skozi take projekte pridete do nujno potrebnih novih znanj, ki bodo pripravljenost v vaši organizaciji postavila na višji novo?

Predvsem je pomembna povezava med sektorji kritične infrastrukture. Samo predstavljate si lahko, kaj pomeni sodelovanje med energetskimi družbami in zdravstvom v kriznih razmerah. Ravno Slovensko združenje korporativne varnosti predstavlja ta pomembni vezni člen.

V UKCL se povsem zavedamo pomena sodelovanja v projektih EU. Na različnih področjih smo vanje vpeti in ponosni smo, da imamo na področju medicine zavidljive rezultate. Ker so podporne službe navadno v tako imenovanem »drugem planu«, se šele v zadnjem obdobju tudi te službe prijavljajo oziroma sodelujejo v takih projektih. Vsekakor pa so ti projekti izjemnega pomena za izmenjavo izkušenj, dobrih praks in znanj.

Večina upravljalcev pomembne infrastrukture je združena v Slovenskem združenju korporativne varnosti. Vključeno je tudi nekaj pomembnih organizacij s področja zdravstvenega sektorja. Vam te povezave znotraj združenja olajšujejo operativno komunikacijo v realnem okolju?

V veliko veselje in ponos nam je, da smo del družine »korporativne varnosti« v Sloveniji. Ne gre samo za zdravstveni sektor, kjer imamo tudi druge oblike sodelovanja. Predvsem je pomembna povezava med sektorji kritične infrastrukture. Samo predstavljate si lahko, kaj pomeni sodelovanje med energetskimi družbami in zdravstvom v kriznih razmerah. Ravno Slovensko združenje korporativne varnosti predstavlja ta pomembni vezni člen. Zadnje krize so nam potrdile, da so rešitve na podlagi osebnih odnosov in ne sistemskih rešitev.

Ali bi lahko na tej točki potegnili nekatere splošne zaključke glede učinkovitosti spopadanja zdravstva z epidemijo, predvsem pa kaj smo se iz tega naučili za ravnanje v podobnih izrednih razmerah?

Ponovno se je potrdilo, da smo v Sloveniji mojstri improvizacije. Odlično smo in še obvladujemo krizne razmere, vendar mimo načrtov, ki so za to pripravljeni. To potrjuje, da so bili načrti pisani sami zaradi sebe ne pa za uporabo. V zadnjih mesecih nastajajo načrti, ki so uporabni. Potrdili smo tudi, da se vse rešitve zgodijo na podlagi osebnih poznanstev in »uslug« med prijatelji. In ta »sistem« deluje. Želimo pa si da vzpostavimo sistem, ki bo od tega neodvisen in bo temeljil na znanju in izkušnjah vseh v stroki. ■



Z aktivnim pristopom identificirajte in zmanjšajte tveganja ter ustvarite varno in finančno uspešno poslovno okolje

Silver Bullet Risk je edino specializirano in vodilno podjetje na področju celovitega upravljanja in obvladovanja tveganj v Sloveniji. Izkoriščamo moč znanja, izkušenj in tehnologije, da vam ponudimo širok in celovit nabor rešitev, ki vam pomagajo oceniti in obvladati tveganja in s tem v celoti izkoriščati poslovne priložnosti.

SVETOVANJE

IZOBRAŽEVANJE

PROGRAMSKA OPREMA

www.silverbulletrisk.com

Avtorji: mag. Andrej Maslo, mag. Miran Vršec in Vito Murgel*





AVTOMATIČNO MERJENJE TELESNE TEMPERATURE – IZZIVI UPORABE V PRAKSI

Novi koronavirus (COVID-19), ki se je pojavil praktično čez noč, je hipoma spremenil naša življenja in zaradi uvajanja ukrepov za zajezitev njegovega širjenja dodobra ohromil ali celo zaustavil delovanje celotnih panog in posledično upočasnil dobršen del gospodarstva. Ključni problem je v hitri prenosljivosti okužb, zato je pravočasna zaznava simptomov okužbe bistvenega pomena za zajezitev ali vsaj omejitev širjenja okužbe. Z merjenjem zvišane telesne temperature na dokaj enostaven način odkrivamo enega od pomembnih simptomov okužbe. A pri tem so se pojavile dileme o zakonitosti, sorazmernosti, zanesljivosti, smiselnosti in dejanski dodani vrednosti meritev telesne temperature v poslovnih okoljih.

Naj v uvodnem delu izpostavimo opozorila strokovnjakov, da termometri za merjenje telesne temperature niso merila, za katera se uporabljajo določbe Zakona o meroslovju, ampak sodijo k medicinskim pripomočkom. Področje medicinskih pripomočkov pa ureja Zakon o medicinskih pripomočkih. Za merila je potrebno izvajati kalibracijo, v primeru termometrov kot meril, pa to kalibracijo izvajajo v za to akreditiranih laboratorijih po Sloveniji. Ob izvajanju meritve se vselej postavlja vprašanje kakovosti meritev. Pri merjenju temperature je kakovost meritve odvisna od različnih dejavnikov, ki lahko bistveno vplivajo na izmerjeno vrednost. Zaradi tega so v Laboratoriju za metrologijo in kakovost na Fakulteti za elektrotehniko Univerze v Ljubljani pripravili nekaj pojasnil glede tehnologij za merjenje telesne temperature, ki jih povzamemo v nadaljevanju in so pomembne za razumevanje te problematike. Njihov osnovni namen je zagotoviti točnost meritve, pravilnost interpretacije merilnih rezultatov in na podlagi tega pravilno odločanje in pravilno nabavo ustrezne merilne opreme.

Potreba je čez noč spodbudila povpraševanje, ki ga je le še pospešil sklep vlade, da naj se ob vstopu v delovne prostore redno meri temperatura zaposlenih in obiskovalcev, le-ta pa ponudbo različnih brezstičnih rešitev merjenja temperature, ki omogočajo hiter zajem podatka o telesni temperaturi posameznika.

Telesno temperaturo lahko izmerimo zelo točno. Kakovostna meritev je odvisna od več dejavnikov in sicer: od termometra, od usposobljenosti izvajalca meritve, od merjenega posameznika in od mesta izvedbe meritve (v ušesu, pod pazduho, pod jezikom, na čelu ipd.). Pri tem je potrebno še posebej poudariti, da se telesna temperatura glede na čas meritve v dnevu, z letnimi časi, s starostjo, s spolom, z utrujenostjo, s telesno aktivnostjo in z zdravstvenim stanjem ves čas spreminja, torej ni konstantna, kar je lahko bistvenega pomena pri interpretaciji odčitanih meritev. Prav tako je potrebno izpostaviti dejstvo, da tudi različni načini izvajanja meritev telesne temperature ne dajejo istih rezultatov, tako kot ne dajejo istih rezultatov

*avtorji so člani Slovenskega združenja korporativne varnosti

različna merilna sredstva (termometri), s katerimi izvajamo meritve telesne temperature. Stari Grki, so telesno temperaturo »izmerili« z dlanjo, v današnjem času pa poznamo različne merilne naprave za merjenje telesne temperature, med katere sodijo živosrebrni (tekočinski) termometri, digitalni termometri, ušesni termometri, čelni termometri in v zadnje popularne termovizijske kamere. Delovanje teh naprav se razlikuje glede na fizikalni princip in tehnologijo merjenja. Vsak izmed termometrov različno zanesljivo oziroma točno meri telesno temperaturo, pri tem pa je potrebno upoštevati tudi tolerančno polje meritve termometra, točnost zapisa odčitka in interpretacijo meritve. S staranjem se lahko termometrom spreminja njihova natančnost delovanja, zato je potrebno redno preverjati (kalibrirati) njihovo točnost delovanja.

Ko govorimo o brezstičnem merjenju telesne temperature obstaja veliko dejavnikov, ki jih je potrebno posebej poudariti in so pomembni za doseganje čim bolj natančnih rezultatov merjenja telesne temperature. Naj izpostavimo predvsem naslednje dejavnike:

- za točnost merjenja mora biti razdalja med napravo in osebo relativno kratka,
- termovizijska kamera mora biti natančno umerjena,
- meritev mora potekati v notranjih prostorih, temperatura prostora, kjer se izvaja merjenje, pa mora biti nadzorovana in stabilna (pod določenimi pogoji, je uporaba nekaterih tehničnih rešitev meritev lahko izvedena tudi v zunanjem okolju),
- za točno meritev oseba pred izvajanjem meritve ne sme biti izpostavljena velikim temperaturnim razlikam (mraz, sonce) vsaj nekaj časa (priporočljivo vsaj 5 minut),
- oseba mora gledati pravokotno v kamero,
- oseba se mora pred kamero ustaviti ali zelo upočasniti premikanje,
- priporočljivo je, da so oči in čelo osebe dobro vidni,
- v primeru povišane temperature je treba dosledno upoštevati veljavna navodila in priporočila za ravnanje z morebitnimi prenašalci nalezljivih bolezni.

Za brezstično merjenje temperature je več različnih možnosti. Glede na zahteve po natančnosti in hitrosti izvajanja meritve telesne temperature, lahko izpostavimo izvajanje meritve telesne temperature z ročno termovizijsko kamero, terminalom za merjenje temperature ali videonadzorno kamero. Nekaj značilnosti prej omenjenih rešitev podajamo v nadaljevanju.

Ročna termovizijska kamera se uporablja na mestih, kjer število prehodov ni veliko, uporablja se lahko kot ročna kamera za merjenje temperature ali pa se jo pritrdi na ustrezen nosilec/stojalo. Povezana je s programsko opremo in meri telesno temperaturo samo pri eni osebi z natančnostjo merjenja ± 0,5 stopinje.

Videonadzorna kamera uporablja funkcije, ki so primarno namenjene zaznavanju parametrov za potrebe varovanja ljudi in premoženja, imajo vgrajeno umetno inteligenco ter termalno ali kombinirano optično in termalno zaznavanje slike. Namesti se kot samostojna nadzorna enota in se poveže na računalnik, preko katerega se omogoči ogled slike s pomočjo programske opreme. Gre lahko za dokaj enostavno rešitev, ki lahko meri temperaturo nekaj osebam hkrati in v večini primerov zagotavlja natančnost merjenja ± 0,5 stopinje ali kot bolj kompleksno rešitev v obliki sistema, ki ga sestavljajo kamera, snemalnik in blackbody (za umerjanje kamere med uporabo), s čemer se doseže zagotavljanje natančnosti merjenja ± 0,3 stopinje. Sistem s pomočjo programske opreme omogoča ogled dogodkov za nazaj, prednost pa je tudi ta, da omogoča večji pretok oseb, ker istočasno lahko izvaja merjenje temperature do 30 oseb.

Delodajalci načeloma niso upravičeni do obdelave zdravstvenih podatkov delavcev. V času pojava virusa COVID-19, ko je zaradi hitrega širjenja virusa ogroženo tako zdravje posameznika kot tudi javno zdravje, lahko posebne okoliščine narekujejo ukrepe, ki posegajo tudi v segment obdelave posebnih vrst osebnih podatkov, kot je npr. merjenje telesne temperature zaposlenih.

Terminal za merjenje temperature, v katerega je lahko vgrajena tudi kamera za prepoznavo obraza in se lahko uporablja v kombinaciji s kontrolo pristopa ima vgrajen senzor za merjenje ciljne temperature. Bistvene značilnosti te rešitve so naslednje: meritve se praviloma lahko izvajajo v območju temperature od 30°C do 45°C, natančnost merjenja je 0,1°C, odstopanje je ± 0,5°C, razpoznavna razdalja, na kateri se lahko izvaja merjenje, je od 0,3 do 1,8 m. V načinu hitrega merjenja temperature zazna obraz in meri temperaturo brez preverjanja pristnosti identitete, omogoča več kombiniranih načinov preverjanja (kartica in temperatura, obraz in temperatura, kartica in obraz in temperatura ipd.). V primeru zaznane povišane temperature lahko prepreči avtentikacijo in s tem prehod, in z zvočnim opozorilom opomni, da je potrebno ukrepanje. Če zazna nenormalno temperaturo, sproži glasovni poziv, in s tem sproži stanje vrat (odprtost/zaprtost). Omogoča ogromno število možnih obrazov za prepoznavo (do 10.000 oseb) in ogromno število možnih kartic za avtentikacijo. Optimalna višina postavitve terminala za prepoznavanje obrazov je med 1,4 in 1,9 m. Nastavitve programske opreme so dostopno le z posebno kodo/geslom. Sinhronizacija podatkov je lahko ročna, časovna in samodejna. Pri tem je potrebno poudariti, da tovrstni izdelki za biometrično prepoznavanje niso namenjeni zaščiti, pač pa predstavljajo le dopolnilno in podporno funkcijo ostalim sistemom tehničnega varovanja.

Pri izboru ustrezne rešitve pa ne smemo pozabiti tudi na zakonodajni okvir uporabe tovrstne rešitve. Tu gre izpostaviti predvsem zakonitost uporabe z vidika varstva osebnih podatkov. Informacijski pooblaščenec opozarja na previdnost pri uvajanju termokamer in merjenju telesne temperature posameznikov. Informacijski pooblaščenec še posebej opozarja na problematiko oglaševanja nekaterih proizvajalcev oziroma ponudnikov tovrstne opreme, ki v svojih oglaševalskih sporočilih navajajo, da so njihovi sistemi in rešitve v celoti skladni z zagotavljanjem zasebnosti in Uredbo o varstvu podatkov (GDPR), ker da termalna kamera ne prikazuje podrobnosti, na osnovi katerih bi lahko prišlo do prepoznave obraza in s tem posameznika. Informacijski pooblaščenec opozarja, »da nobena tehnologija sama po sebi ne more že vnaprej zagotavljati skladnosti s pravili glede varstva podatkov, saj so vedno ključni nameni in ostale konkretne okoliščine uporabe tehnologije. V primeru termo kamer je namen njihove uporabe identifikacija posameznika s povišano temperaturo in pravočasno ukrepa-



nje, torej gre neizogibno za obdelavo osebnih podatkov.«. Pri tem je potrebno posebej izpostaviti dejstvo, da podatki o izmerjeni telesni temperaturi sodijo med posebne vrste osebnih podatkov, za katere splošna uredba določa, da je njihova obdelava prepovedana, če ni podana katera od izjem. Pri izvajanju meritev telesne temperature je torej nujno potrebno spoštovati vse določbe splošne uredbe. Predvsem gre tu za spoštovanje načel varstva osebnih podatkov, za ustrezno obveščanje posameznikov o izvajanju tega ukrepa in izvedbi vseh potrebnih nujnih ukrepov za zaščito podatkov, kot so minimizacija in sorazmernost obsega obdelave osebnih podatkov in rokov hrambe, varnost podatkov, ter njihovo točnost in ažurnost. Še posebej je to pomembno v primeru, ko se tehnologija merjenja telesne temperature integrira v sistem kontrole pristopa z namenom ugotavljanja identitete posameznika in izpolnjevanja pogojev upravičenosti vstopa v varovana območja.

Implementacija in uporaba naprav za merjenje telesne temperature v praksi

Pred implementacijo in uporabo posamezne tehnične rešitve merjenja telesne temperature v delovnih sredinah je potrebno v izhodišču presojati dvoje elementov (skladno z določili Zakona o nalezljivih boleznih, Zakona o varnosti in zdravju pri delu, Zakona o delovnih razmerjih):

- zakonite interese in obveznosti delodajalcev, da spremljajo in sprejemajo ustrezne ukrepe za zagotavljanje varnosti in zdravja pri delu zaposlenih, glede na nove pojave in spremenjene okoliščine, s čimer se posledično tudi nalaga uvajanje morebitnih (dodatnih) novih preventivnih ukrepov za varovanje zdravja delavcev (v trenutni situaciji pojava novega virusa COVID-19 in nevarnosti njegovega širjenja med prebivalstvom, je ta element zagotovo prisoten);
- zakonite interese in obveznosti vsakega posameznika in s tem tudi zaposlenega, da v primeru pojava nalezljive bolezni, pripomore k preprečevanju in obvladovanju širjenja nalezljive bolezni (kar je že spet element, ki je prisoten v trenutni situaciji pojava novega virusa COVID-19), med drugim tudi z izvajanjem preventivnih ukrepov za varovanje zdravja.

Ob ustrezni presoji zgoraj navedenih zakonitih interesov in obveznosti, se v povezavi z vidiki varstva osebnih podatkov, odprejo aktualna vprašanja in dileme, ki so povezana z:

- merjenjem telesne temperature zaposlenih;
- merjenjem telesne temperature obiskovalcev;
- zajema in obdelave fotografij oseb.

Merjenje telesne temperature zaposlenih

Delodajalci načeloma niso upravičeni do obdelave zdravstvenih podatkov delavcev. V času pojava virusa COVID-19, ko je zaradi hitrega širjenja virusa ogroženo tako zdravje posameznika kot tudi javno zdravje, lahko posebne okoliščine narekujejo ukrepe, ki posegajo tudi v segment obdelave posebnih vrst osebnih podatkov, kot je npr. merjenje telesne temperature zaposlenih. Informacijski pooblaščenec je pri tem jasen. Upravičenost ukrepov, ki posegajo na področje obdelave posebnih vrst osebnih podatkov, je potrebno presojati od primera do primera; in v tem pogledu je od primera do pri-

mera potrebno tudi presojati dopustnost uporabe naprav oz. tehničnih rešitev za merjenje telesne temperature. Glede na konkretne okoliščine, lahko o utemeljenosti ukrepa merjenja telesne temperature zaposlenih, mnenje v prvi vrsti poda le zdravstvena stroka – pooblaščeni izvajalec medicine dela. Delodajalec mora od pooblaščenega izvajalca medicine dela pridobiti mnenje:

- ali je takšen ukrep res nujen in primeren pri vseh zaposlenih ali le pri delu zaposlenih;
- ali je nujno in primerno te podatke hraniti, ob upoštevanju specifičnih okoliščin;
- ali obstajajo drugi manj invazivni ukrepi, ki so morda celo bolj učinkoviti z vidika dejanskega preprečevanja širjenja okužbe in zagotavljanja nemotenega delovnega procesa.

Če se pri tem ugotovi, da je merjenje telesne temperature zaposlenih upravičeno, mora delodajalec izvesti še vse druge aktivnosti, da bo izvajanje ukrepa merjenja telesne temperature oz. s tem povezana obdelava osebnih podatkov skladna z določili varstva osebnih podatkov (izdelava ocene učinkov glede varstva osebnih podatkov, obveščanje zaposlenih, minimizacija in sorazmernost obsega obdelave osebnih podatkov itd.).

Merjenje telesne temperature obiskovalcev

Tudi glede merjenja telesne temperature obiskovalcev velja, da je tudi tu pomembno predhodno pridobljeno mnenje zdravstvene stroke, ali je merjenje temperature obiskovalcev, glede na konkretne okoliščine primerno in ustrezno ali pa bi se enak namen dosegel na manj invaziven način. Če zdravstvena stroka meni, da je ukrep merjenja telesne temperature obiskovalcev upravičen, je potrebno izvesti še druge aktivnosti, da bo izvajanje takšnega ukrepa skladno z določili varstva osebnih podatkov (obvestilo obiskovalcem, minimizacija in sorazmernost obdelave osebnih podatkov in rokov hrambe, varnost podatkov ipd.).

Zajem in obdelava fotografij oseb

Glede na to, da so naprave za avtomatično merjenje telesne temperature lahko tudi integrirane v sisteme pristopne kontrole, registracije delovnega časa, lahko v teh primerih tudi govorimo o obdelavi biometričnih podatkov (zajem in obdelave fotografije osebe) za namene celovitega delovanja tako integriranih sistemov. Fotografija osebe ima značaj biometričnih podatkov, pri čemer pa se v zasebnem sektorju takšen ukrep sme izvajati, če je nujno potreben za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Pri tem je še dodatna omejitev, da se takšen ukrep sme izvajati le nad svojimi zaposlenimi, če so bili o tem predhodno tudi seznanjeni. Pred začetkom obdelave biometričnih podatkov pa je potrebno tudi izpeljati postopek priglasitve Informacijskemu pooblaščencu in pridobiti odločbo o odobritvi ukrepa.

Pred implementacijo naprave za merjenje telesne temperature v prakso je ključno, da si predhodno pojasnimo namene ter pogoje uporabe in delovanja takšne naprave. V pogojih varstva osebnih podatkov je uporabo naprave za merjenje telesne temperature mogoče zasnovati na namenu, da se posamezniku (zaposlenemu in obiskovalcu), ki vstopa v poslovne prostore omogoči možnost preverbe svoje telesne temperature na diskreten način, ob jasnem sporočilu in navodilu odgovornih, kako ravnati v primeru izmerjene povišane telesne temperature. Pri tem je pomembno, da takšno ravnanje posameznika izhaja iz njegove svobodne volje (posameznik ima možnost, da se prostovoljno odloči ali si bo temperaturo pred vstopom izmeril ali ne, kar tudi ni pogoj za vstop v poslovne prostore) ter, da je predhodno samo merjenje telesne temperature tudi medicinsko indicirano s strani pooblaščenega izvajalca medicine dela z mnenjem, da je takšen ukrep potreben za zajezitev širitve virusa COVID-19. Na takšen način se posamezniku da možnost, da v primeru znakov obolelosti/okuženosti, ki jih lahko indicira izmerjena povišana telesna temperatura, takoj zapusti zaprt poslovni prostor in se za nadaljnje napotke takoj obrne na zdravniško osebje. Nedvomno pa je, da je učinkovitost ukrepa merjenja telesne temperature z uporabo naprav, v takšnem primeru pomembno odvisna od odgovornega ravnanja vsakega posameznika, ne samo do sebe, ampak tudi do svoje okolice. Dejstvo je namreč, da aktualna zakonodaja na področju varstva osebnih podatkov ni pisana za situacije, kot smo jim priča v trenutnih zaostrenih okoliščinah pojava novega virusa COVID-19, kar pomeni, da iščemo ustrezne rešitve za obvladovanje tveganj povezanih s COVID-om v okviru dopustnosti, tudi na račun manjše učinkovitosti posameznih ukrepov.

Kmalu po sprejemu sklepa vlade, naj se »ob vstopu v delovne prostore redno meri temperatura zaposlenih in obiskovalcev« je postalo jasno, da gre za ukrep, katerega učinkovitost, zanesljivost in s tem smiselnost izvedbe v praksi so vprašljive.

Kmalu po sprejemu sklepa vlade, naj se »ob vstopu v delovne prostore redno meri temperatura zaposlenih in obiskovalcev« je postalo jasno, da gre za ukrep, katerega učinkovitost, zanesljivost in s tem smiselnost izvedbe v praksi so vprašljive. Dejstvo je namreč, da je izmerjena telesna temperatura ob upoštevanju vseh dejavnikov, ki lahko vplivajo na meritev, v praksi zelo nezanesljiv podatek. Dejstvo je tudi, da natančno kalibriran inštrument sam po sebi še ne zagotavlja točnega merjenja, tudi izkušen strokovnjak pa meritev ne more izvajati z nekalibriranim inštrumentom. Ob uporabi tehnologij za brezstično merjenje je to lahko še toliko večji problem. Zato so iz Laboratorija za metrologijo in kakovost pri Fakulteti za elektrotehniko Univerze v Ljubljani sporočili naslednje: »Meritve kažejo, da je za množični nadzor mogoče uporabiti najsodobnejšo tehnologijo brezstičnega merjenja, vendar z najmanjšo točnostjo in posledično možnim neustreznim odločanjem. Zato je v naslednjem koraku identifikacije obolelih za točnejše merjenje treba uporabiti stično merjenje temperature.« Priporočilo o merjenju telesne temperature je tako mogoče razumeti kot dodaten ukrep za preprečevanje prezentizma, prisotnosti na delovnem mestu kljub bolezni, ki je v številnih delovnih okoljih pod pritiskom zviševanja produktivnosti postal norma. A glede na to, koliko potencialnih zapletov lahko za sabo potegne tak ukrep, se je smiselno vprašati o njegovi sorazmernosti. ■

SmartIS
PAMETNI INFORMACIJSKI SISTEMI

SmartIS d.o.o.
Ameriška 8
Ljubljana, Slovenija

T 01 601 0650
E info@smartis.si
www.**smartis**.si



VAŠ SOPOTNIK NA POTI ZAGOTAVLJANJA KIBERNETSKE VARNOSTI

Avtor: mag. Marjan Kavčič / Uprava za informacijsko varnost Republike Slovenije



STRATEGIJA KIBERNETSKE VARNOSTI 2020/21

Letos oktobra so stekle aktivnosti za pripravo nove strategije kibernetske varnosti, ki bo gradila na izkušnjah obstoječe, hkrati pa upoštevala tudi številne spremembe na tem področju.

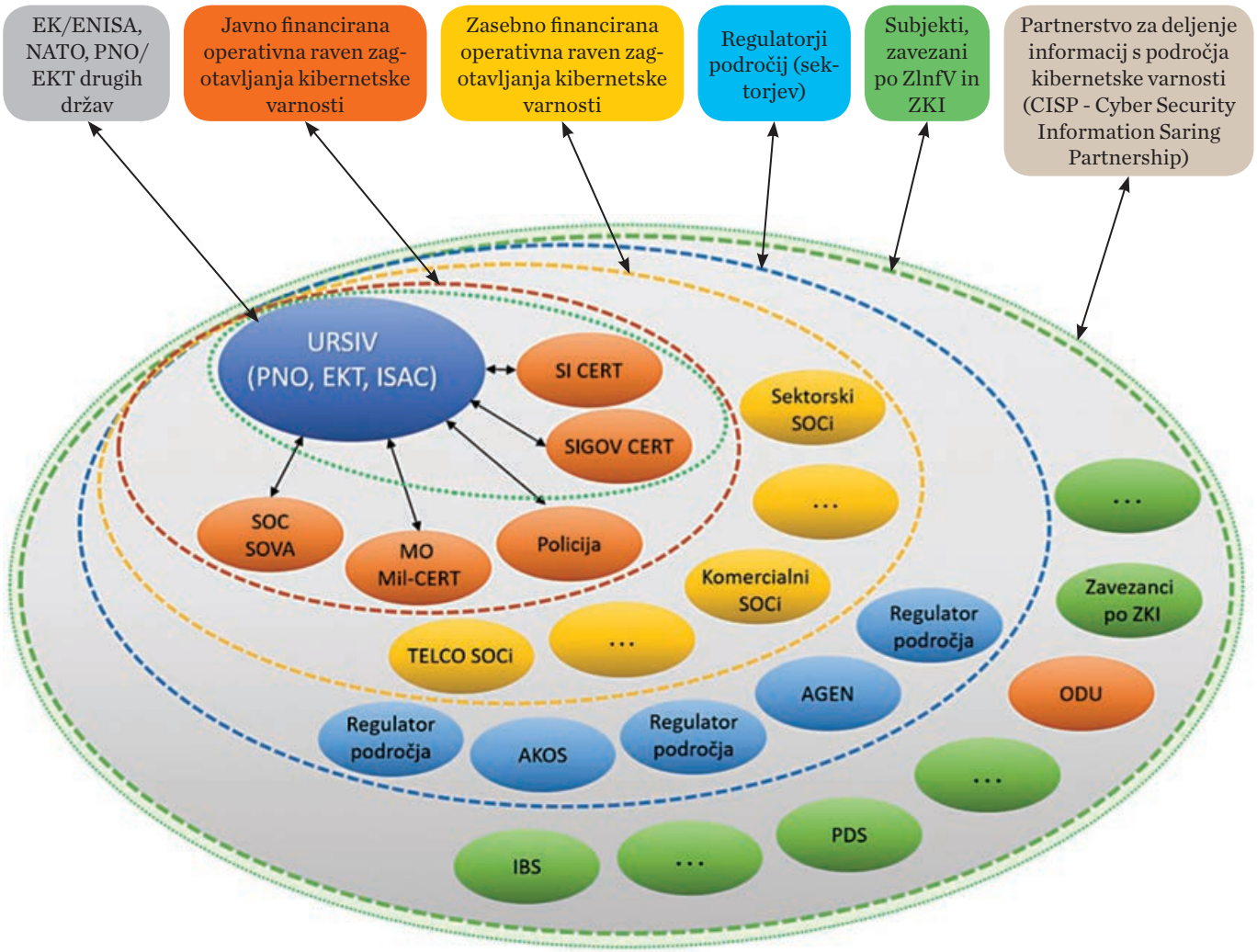
Slovenija je leta 2016 sprejela krovno strategijo Digitalna Slovenija 2020 in dve področni strategiji, Strategijo kibernetske varnosti in Načrt razvoja širokopasovnih omrežij naslednje generacije. Strategija kibernetske varnosti je bila sploh prva s tega področja, v njej pa si je država zadala cilj okrepitve sistema zagotavljanja kibernetske varnosti ob hkratni sistemski ureditvi področja. Oblikovan je bil nabor ukrepov, ki naj bi pripomogel k doseganju ciljev na različnih področjih. Lahko ugotovimo, da so bili nekateri ukrepi uspešno izvedeni oziroma se izvajajo. Na kar nekaj področjih pa napredek ni bil zadosten in bo v prihodnje treba narediti več.

Letos oktobra so stekle aktivnosti za pripravo nove strategije kibernetske varnosti, ki bo gradila na izkušnjah obstoječe, hkrati pa upoštevala tudi številne spremembe na področju. Krovni cilj nove strategije je zagotovitev skupnega in celovitega pristopa na področju kibernetske varnosti in s tem dvig nivoja kibernetske varnosti v Republiki Sloveniji v vseh segmentih družbe. Priprava strategije je naloga Uprave Republike Slovenije za informacijsko varnost (URSIV), ki pa bo pri tem poskusila vključiti kar najširši krog deležnikov s področja kibernetske varnosti v Sloveniji.

Slovenija ima kot majhna država omejene vire na tako rekoč vseh področjih, tudi na področju kibernetske varnosti, vendar pa to ne pomeni, da teh virov ni mogoče bolje izkoristiti. Pri tem bo v pomoč dejstvo, da se je zavedanje o pomenu zagotavljanja kibernetske varnosti pri odločevalcih na nacionalni ravni in v gospodarstvu izboljšalo. Na temu bo gradila tudi URSIV pri pripravi nove strategije. URSIV si želi bolje povezati najprej javno financirane subjekte, kasneje pa tudi subjekte iz zasebnega sektorja, ki na operativni ravni zagotavljajo kibernetsko varnost. V za-

Uprava Republike Slovenije za informacijsko varnost si bo prizadevala, da bo strategija kibernetske varnosti pripravljena in sprejeta še pred predsedovanjem Slovenije Svetu EU v drugi polovici leta 2021.





LEGENDA

URSV strateška raven:

PNO	Pristojni nacionalno organ
EKT	Enotna kontaktna točka
ISAC	Center za analizo in izmenjavo informacij
SOC	Varnostno operativni center
TELCO	Operater elektronskih komunikacij

Primer regulatorjev področij:

AKOS	Agencija za komunikacijska omrežja in storitve RS
AGEN	Agencija za energijo

Primer subjektov zavezancev:

IBS	Izvajalci bistvenih storitev
PDS	Ponudniki digitalnih storitev
ODU	Organi državne uprave
ZKI	Zakon o kritični infrastrukturi

sebnem sektorju so že nastali varnostno operativni centri (SOC), ki svoje storitve zagotavljajo svojim strankam, med katerimi so tudi subjekti s področja kritične infrastrukture. Prav tem, pa tudi izvajalcem bistvenih storitev (IBS) in organom državne uprave (ODU), ki so pomembni za nemoteno delovanje družbe, bo treba nameniti še posebno pozornost. Zato URSIV načrtuje vzpostavitev centra za izmenjavo in analizo informacij (ISAC) ter omrežja zaupanja, ki bo subjektom, pa tudi regulatorjem področij, omogočila izmenjavo informacij in preventivno delovanje.

Za dvig odpornosti na kibernetske grožnje bodo potrebni različni podporni ukrepi. Za splošno odpornost družbe je treba teme s področja kibernetske varnosti vključiti v izobraževalne programe na osnovnošolski in srednješolski ravni. Prav tako je treba nadaljevati s programi ozaveščanja, pri tem pa vključiti tudi nekatere dodatne ciljne skupine (npr. starejše). Načrtovani so ukrepi za spodbujanje zanimanja za poklice na področju kibernetske varnosti med mladimi. Povečanemu povpraševanju bo morala slediti tudi ustrezna ponudba slovenskih visokošolskih ustanov.

Na osnovi nekaterih načrtovanih ukrepov strategije je mogoče razbrati jasne vzročno posledične povezave, kar olajša razumevanje, pa tudi zasledovanje ciljev. Poenostavljeno povedano, če izvedemo določen ukrep, lahko s precejšnjo gotovostjo pričakujemo določen rezultat, oziroma obratno, če ukrepa ne izvedemo, bo izostal tudi rezultat.

URSIV si bo prizadevala, da bo strategija kibernetske varnosti pripravljena in sprejeta še pred predsedovanjem Slovenije Svetu EU v drugi polovici leta 2021.

Zgornja skica kaže prikaz povezav med subjekti na strateški in operativni ravni zagotavljanja kibernetske varnosti, tako v javnem kot tudi zasebnem sektorju. Na zunanjih mejah so prikazani subjekti, pomembni za nemoteno delovanje družbe, ki so zavezanci po Zakonu o informacijski varnosti (ZInfV) in Zakonu o kritični infrastrukturi (ZKI) ter njihovi regulatorji, kot pomemben vmesni člen. ■

Avtorica: Mateja Mirtič / Skrbnica ključnih kupcev, ID Shop d.o.o.



DIGITALNI SISTEMI ZAKLEPANJA Z LASTNIM NAPAJANJEM ZA KRITIČNO INFRASTRUKTURO

V prispevku bo predstavljena študija primera implementacije inovativnega digitalnega sistema zaklepanja v zahtevnem varnostnem okolju na primeru Telekoma Slovenije.

Ne moremo se izogniti dejstvu, da je COVID -19 vplival na veliko vidikov našega delovnega in osebnega življenja. Kar se ni spremenilo, je to, da smo še vedno, morda celo bolj, odvisni od storitev in dobrin, ki jih zagotavljajo organizacije kritične infrastrukture. Podjetja za oskrbo z energenti, proizvodnjo in distribucijo električne energije, komunalna podjetja, ponudniki telekomunikacijskih storitev ter podjetja, ki zagotavljajo transport in skladiščenje, so v trenutnih razmerah še bolj pod pritiskom, da nemoteno ohranjajo in zagotavljajo svoje storitve tako, da njihovo delovanje ni ogroženo v nobenem trenutku.

Digitalni sistemi zaklepanja z lastnim napajanjem za kritično infrastrukturo (v nadaljevanju iLOQ)

Brez baterij. Brez skrbi.
V podjetju ID Shop smo ravno v najbolj kritičnih časih uspešno začeli z implementacijo inovativnega digitalnega sistema zaklepanja iLOQ S50, in sicer na tehnoloških objektih Telekoma Slovenije. Gre za prvi digitalni sistem zaklepanja na svetu, ki temelji na odklepanju s pametnim telefonom in NFC tehnologijo, ki za delovanje ne potrebuje ne baterij ne kablov. Kljub temu, da je bil poglavitni cilj Telekoma Slovenije poenotiti sistem zaklepanja, optimizirati njegovo upravljanje ter zmanjšati stroške upravljanja, kot ena od prednosti v trenutnih razmerah pa izstopa možnost oddaljenega upravljanja sistema zaklepanja na tehnoloških objektih širom Slovenije in v realnem času.

Pri vseh podjetjih, še posebej, če zagotavljajo kritično infrastrukturo, je zagotavljanje neprekinjenih storitev prioriteta in hkrati izziv, saj morajo pri tem vzdrževati razpršeno mrežo tehnoloških objektov. Vsak mehanski ključ predstavlja visok nivo zaščite sistema le, dokler se ne izgubi oziroma je zagotovljen učinkovit nadzor nad tem, kje se nahaja. Možnost odklepanja z mobilnimi ključi je zato prednost.

iLOQ 5 Series - rešitev za zahtevna varnostna okolja v kritični infrastrukturi

Podjetjem, ki delujejo v segmentu kritične infrastrukture, je skupno to, da praviloma upravljajo večje število dislociranih enot, ki zahtevajo visoko zaščito pred nepooblaščenimi dostopi (bazne in transformatorske postaje, plinohrami, telekomunikacijski stolpi, vodna zajetja, elektro omarice...) in imajo posledično v obtoku veliko število ključev. Značilno je, da so lahko te posamezne enote locirane na težko dostopnih krajih, daleč od centrale in bolj izpostavljene vremenskim vplivom. Stroški vzdrževanja takšne infrastrukture so posledično visoki; tako z denarnega kot s časovnega in z administrativnega vidika. V primeru Telekoma Slovenije infrastrukturo sesta-



vlja več kot 2000 tehnoloških objektov, zato je bilo podjetju še toliko bolj pomembno, da je nov sistem zaklepanja funkcionalno in stroškovno učinkovit. Področja, kjer je največ možnosti za izboljšave z vidika obstoječega sistema zaklepanja na tehnoloških objektih:

- zmanjševanje stroškov, ki so povezani z mehanskimi sistemi zaklepanja (stroški vzdrževanja sistema, menjave ključev in okvarjenih cilindrov);
- zmanjševanje stroškov, ki so povezani s časom in kilometrino na poti do tehnološkega objekta ter distribucijo ključev (prevzem, predaja ključev na centrali);
- zmanjšanje internih procesov dela in organizacije servisov;
- zmanjšanje stroškov pri izvajanju del zunanjih pogodbenih partnerjev,
- zmanjševanje stroškov in skrb za nivo varnosti sistema zaklepanja v primeru izgube ključa (potrebna izdelava novega ključa, cilindra ali celotnega sistema);
- zagotavljanje revizijske sledi nad dogodki, boljši nadzor nad izdajo in uporabo ključev (pregled, pri kom se ključ trenutno nahaja in kdo ima dostop do določene lokacije), s čimer se krepi zaščita sistema;
- večja centralizacija in preglednost upravljanja sistema, kar je povezano z administrativnimi postopki, časom in stroški idr.

Glede na navedeno je sistem iLOQ 5 Series najučinkovitejši odgovor na potrebe in visoke varnostne zahteve podjetij, saj je bil ustvarjen ravno za potrebe kritične infrastrukture.

Digitalni in mobilni sistemi za kontrolo dostopa z lastnim napajanjem

Sistem iLOQ S10 temelji na digitalnih cilindrih z lastnim napajanjem, ki energijo za odklepanje črpa iz kinetične energije (ta se ustvari ob vstavljanju digitalnega ključa v cilinder). Sledila je rešitev iLOQ S50 za odklepanje z mobilnim telefonom na podlagi NFC-tehnologije. Oba sistema so združili v eno inteligentno rešitev iLOQ 5 Series, ki je namenjena podjetjem v kritični infrastrukturi. Revolucionarna je zato, ker pri obeh sistemih za delovanje niso potrebne ne baterije in ne kabli.

Zamenjava tradicionalnih ključev za sistem mobilnih ključev s tehnologijo NFC

Pri vseh podjetjih, še posebej, če zagotavljajo kritično infrastrukturo, je zagotavljanje neprekinjenih storitev prioriteta in hkrati izziv, saj morajo pri tem vzdrževati razpršeno mrežo tehnoloških objektov. Vsak mehanski ključ predstavlja visok nivo zaščite sistema le, dokler se ne izgubi oziroma je zagotovljen učinkovit nadzor nad tem, kje se nahaja. Možnost odklepanja z mobilnimi ključi je zato prednost.

Mobitel kot ključ in vir energije

Kontrola dostopa iLOQ S50 temelji na digitalnem cilindru, ki se aktivira z NFC-tehnologijo pametnega telefona ter ustvarja dovolj energije za prepoznavanje dostopnih pravic in odklepanje cilindra. To pomeni, da iLOQ S50 pametni telefon uporabi kot vir energije in kot ključ, baterije in kabli pri tem niso potrebni. iLOQ S50 deluje prek mobilne aplikacije, ki je na voljo za pametne telefone Android in iOS, ki so združljivi z NFC. Alternativa pametnim telefonom je obesek iLOQ (BLE).

Varno in uporabniku prijazno upravljanje kontrole dostopa na daljavo

Sistem iLOQ S50 ponuja popolnoma nove priložnosti za upravljanje mreže dislociranih enot. V primeru uporabe sistema iLOQ S50 so digitalni cilindri na različnih lokacijah širom Slovenije povezani v en sistem zaklepanja, pri čemer tudi velike razdalje in oddaljenost lokacij ne predstavljajo težav, saj programska oprema iLOQ Manager (v oblaku) omogoča centralno upravljanje dostopov za več objektov ali sistema z več tisoč cilindri. Dostopne pravice lahko preko iLOQ Manager uporabniki pošljejo tisti osebi, ki je najbližje lokaciji. Na ta način ne samo, da se zmanjša potovalni čas zaposlenih in prihrani denar, odpravljena je tudi potreba po ročnem uvozu

ali izvozu podatkov v ključavnice in čitalce, ker digitalni cilindri zbirajo in samodejno pošiljajo revizijske sledi v oblak. Skrbniki sistema imajo v realnem času pogled nad tlorisom objekta, ki prikazuje lokacije digitalnih cilindrov ter kdo ima dostopne pravice do določenega objekta. Vnašanje novih uporabnikov, avtorizacij, pošiljanje pravic skupini uporabnikov, blokiranje pravic ali določanje časovnih omejitev je hitro in enostavno in tako so administrativni postopki optimizirani in poenostavljeni.

Visoka varnost, nizki stroški
Telekom Slovenije je sinonim za najsodobnejšo IKT-tehnologijo, zato so imeli v podjetju visoke zahteve in standarde glede uporabe mobilnih ključev. iLOQ uporablja najvišji nivo varnosti v digitalnem ekosistemu: pametni telefon je overjen s sistemom šifriranja PKI (Public Key Infrastructure), medtem ko digitalni cilinder in mobitel za vzajemno avtentikacijo uporabljata šifriranje AES-256.

Zmanjšani stroški življenjskega cikla in vzdrževanja sistema zaklepanja
Sistem iLOQ slovi po nizkih stroških vzdrževanja, ker vzdrževanje sistema v veliki meri sploh ni več potrebno. Digitalne komponente so zasnovane tako, da so lahko izpostavljene težkim okoljem in ekstremnim podnebnim razmeram. Ker nimajo izpostavljenih odprtin za ključe, ne potrebujejo čiščenja in so odporne na vodo in prah. Zamenjava baterij, cilindrov in ključev v primeru izgube ali okvare ni več potrebna, posledično se ustvarjajo znatni prihranki pri velikih sistemih zaklepanja, kjer je nameščenih veliko cilindrov in v uporabi veliko ključev. Velike organizacije z razpršeno infrastrukturo potencialno prihranijo na tisoče evrov pri stroških vzdrževanja v celotnem življenjskem ciklu sistema, ob čemer se stopnja varnosti sistema v nobenem trenutku ne zmanjša.

Zaklepanje, ki se prilagaja spremembam v objektih
Digitalni sistem zaklepanja iLOQ 5 Series je mogoče razširiti v kontrolo dostopa iLOQ S5 Online, ki ga lahko v celoti upravljamo na daljavo. Razširitev omogoča, da v isti sistem dodamo digitalne cilindre, obešanke, pohištvene ključavnice, zidne trezorje za ključe, čitalce RFID ali PIN... Standardni odprti aplikacijski programski vmesnik (API) iLOQ 5 Series omogoča integracijo s sodobnimi sistemi za izmenjavo informacij ter z različnimi nadzornimi centri za kontrolo pristopa. Tudi v teh primerih brez kablov in gradbenih posegov.

Trajnostna tehnologija
Sistemi iLOQ so za podjetja pomembni tudi z vidika trajnostnega razvoja. Produkt podjetjem omogoča pristop k varovanju okolja in učinkoviti rabi energije (Sustainable Development Goals). Podjetjem sistem omogoča implementacijo načela trajnostnega razvoja, hkrati pa omogoča odpravo potrebe po fizičnih mehanskih ključih. Z uporabo iLOQ 5 Series podjetja prispevajo k zmanjšanju vpliva svojega delovanja na okolje, saj je iLOQ sinonim za zeleno, samozadostno in trajnostno rešitev.

Ključne prednosti za implementacijo iLOQ sistema zaklepanja

Z uporabo iLOQ S50 sistema zaklepanja lahko podjetje poskrbi za prilagoditev organizacije dela v trenutni situaciji, ki stremi k čim bolj brezkontaktnim delovnim procesom, omejuje osebno interakcijo, poudarja delo na daljavo, velikokrat pa so ob tem na voljo omejeni človeški viri. Oddaljeno upravljanje sistema zaklepanja je le ena od točk na obsežnem seznamu prednosti. Največje prednosti rešitve sistema iLOQ se kažejo kot:



- enostavno in centralizirano urejanje avtorizacij za vse tehnološke objekte v realnem času ter učinkovitejši nadzor nad izdajo in porabo ključev;
- dostop na lokacijo ni več vezan na fizični ključ, zato ni potrebe po distribuciji ključev po terenu, osebne interakcije med zaposlenimi so zmanjšane;
- omogočen je dostop pogodbenim partnerjem, pri čemer spremstvo in nadzor s strani podjetja več ni potrebno;
- prihranek pri potnih stroških, kilometrini, amortizaciji vozil;
- ekonomska učinkovitost sistema zaklepanja zaradi zmanjšanih stroškov vzdrževanja: sistemski ključi in cilindri so po navadi zaščiteni in posledično dragi. S sistemom iLOQ celotni strošek izdelave ključev in zamenjave cilindrov odpade, prav tako ni več čakanja na izdelavo ključev, montažo cilindra;
- zagotavljanje visoke varnosti sistema zaklepanja skozi celotni življenjski cikel (ni bojazni za izgubo ključev, nepooblaščene vstope, revizijska sled je vedno zagotovljena, pregled nad dostopnimi pravicami je centraliziran in omogoča pošiljanje ali blokiranje dostopnih pravic v realnem času...);
- manjša odgovornost posameznikov v primeru izgube ključev;
- zaščita proti tiskanju ključev 3D,
- učinkovitejše razporejanje dela zaposlenim, zmanjšan potovalni čas ter posledično večja izkoriščenost delovnega potenciala.

Podjetje ID Shop že več kot 18 let sledi smernicam na področju identifikacije in varnosti, s posebnim poudarkom na mehanskem in elektronskem zaklepanju ter kontroli pristopa. Zaradi dodane vrednosti sistemov zaklepanja iLOQ se je tudi Telekom Slovenije skupaj z ID Shop odločil storitve digitalnega sistema zaklepanja približati svojim poslovnim uporabnikom, podjetjem in drugim organizacijam. ■



iLOQ 5 Series

Digitalni sistem zaklepanja za kritično infrastrukturo

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



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

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

Telekom Slovenije

Avtor: Peter Ceferin / tehnični direktor, Smart Com d.o.o.



KIBERNETSKA VARNOST JE NEPOGREŠLJIV DEL SODOBNEGA POSLOVANJA

Ne glede na to, v kateri gospodarski panogi posluje vaše podjetje, mora skrb za kibernetsko varnost postati temeljni gradnik strategije poslovanja. Kraje podatkov in/ali denarja, izklopa sistemov ter izgube ugleda si danes zares nihče ne more privoščiti, še toliko manj industrijska okolja in podjetja, ki upravljajo kritično infrastrukturo države.

Frekvenca in obseg napadov na podjetja ne glede na gospodarsko panogo in velikost, se povečujeta in vse več jih bo. Ne smemo se slepiti, da bodo hekerji Slovenijo zaobšli le zato, ker je majhna in govori nek svetu nerazumljiv jezik. Ko je v uporabi tehnologija, se globalni trendi preslikajo tudi k nam, in tudi slovenska podjetja postanejo tarče hekerjev.

IBM-ovo poročilo o kibernetski varnosti za leto 2019 priča o tem, da danes pred napadalci ni varno nobeno podjetje, na globalni ravni pa so strokovnjaki za informacijsko varnost zaznali daleč največji porast napadov na industrijska okolja, saj je rast števila napadov presegla 2.000 % ali, povedano drugače, hekerji so na proizvodna in industrijska okolja sprožili kar 20-krat več napadov kot leto poprej.

Slovenska podjetja so za napadalce vedno bolj privlačna. Lani smo obeležili deseto obletnico »slavnega« Stuxneta, prvega črva, ki je ciljal na kritične sisteme in izkoriščal luknje v sistemih SCADA. Danes pa smo priča specializiranim napadom in škodljivim kodam, ki so optimizirana prav za industrijska okolja in posamezna ciljana podjetja. Zemljevid groženj, ki targetirajo industrijska okolja, je izredno velik.

Kritična infrastruktura je še toliko bolj zanimiva za napadalce, saj če lahko prevzamejo nadzor nad delom procesnih sistemov v industriji ali elektrogospodarstvu, imajo veliko moč in vpliv – kar pa vpliva tudi na višino odkupnine, ki jo zahtevajo in jo podjetja plačajo, da bi si povrnila nadzor nad ugrabljenimi sistemi, datotekami ali podatki. Odkupnino plačajo skoraj vsi, alternativa je le, da prenehajo poslovati. Veliko podjetij namreč nima vzpostavljenega sistema redne izdelave varnostnih kopij podatkov in vpeljanega scenarija za obnovitev poslovanja ob uspešno izvedenem kibernetskem napadu.

Frekvenca in obseg napadov na podjetja ne glede na gospodarsko panogo in velikost, se povečujeta in vse več jih bo. Ne smemo se slepiti, da bodo hekerji Slovenijo zaobšli le zato, ker je majhna in govori nek svetu nerazumljiv jezik.

Hekerji v takšnih okoljih ciljajo na nadzorne sisteme in starejše, ranljive sisteme. Sistemi so čedalje bolj povezani. S tem se pojavlja veliko večja izpostavljenost novim ranljivostim, ki so prisotne v vsakem informacijskem sistemu. V industrijskih okoljih, zaradi narave samih procesov, obratuje še vedno veliko operacijskih sistemov, kjer pogostih nadgradenj ni mogoče izvajati, ali celo sistemov, za katere varnostni popravki niso več na voljo (na primer za Windows XP), kar dodatno vnaša pomemben delež ranljivosti, ki se jih moramo zavedati. Ti sistemi so bili do nedavnega v izoliranem sistemu okolja operativne tehnologije (OT) in zato ni bilo potrebe po varnostnih nadgradnjah. Delovali so po principu, ki pravi, da stvari ne popravljaj, če niso pokvarjene. Posledično so danes takšni sistemi in s tem podjetja izpostavljena izjemno visokemu varnostnemu tveganju. Danes se namreč v industrijskih okoljih in kritični infrastrukturi vedno bolj prepletata IT- in OT-okolje, priča pa smo kibernetskim napadom, ki prehajajo iz enega v drugo okolje in obratno.

Kibernetska varnost zadeva prav vse

Lahko rečemo, da so za kibernetske kriminalce bolj privlačne tiste gospodarske panoge, ki imajo širši vpliv na življenje ljudi, zaradi česar lahko naredijo večjo škodo. Zato je tako imenovana kritična infrastruktura vse pogosteje tarča napadov. Na primer farmacija, energetska infrastruktura, železnice ...

Vendar pa je človek tisti, ki najhitreje podleže skušnjavam, ni ozaveščen, je tisti, ki je radoveden in zaradi tega nepazljiv pri uporabi IKT naprav. Ljudje smo pogosto neprevidni – nevede in mimogrede ustvarimo varnostno luknjo. In ne mislimo na zaposlene s povprečnim informacijskim znanjem, temveč tudi na tiste, ki imajo več ali veliko tehničnega znanja. Velikokrat smo priča primerom, ko vzdrževalci IKT sistemov, zaradi lastnega udobja pustijo odprta »vrata« za vstop v sisteme podjetja preko spleta ipd., ki predstavljajo varnostno tveganje in ‚raj za hekerje'.

Najboljši varnostni pregled je tisti, ki vključuje tudi testiranje zaposlenih, saj izkušnje potrjujejo, da so najbolj uspešni kibernetski napadi izvedeni s tehnikami socialnega inženiringa, te pa lahko odbijemo le, če so zaposleni ustrezno izobraženi in osveščeni o pomembnosti kibernetske varnosti.

Začne se že na osnovni ravni, saj opažamo, da industrijsko okolje ni segmentirano. To pomeni, da so stroji in računalniki v takšnem okolju povezani v enotno omrežje, brez osnovnih mehanizmov ločevanja v virtualne domene že na omrežni ravni.

Segmentacija omrežja na virtualne domene pomeni, da so določeni segmenti ali sklopi proizvodnje ločeni drug od drugega že na ravni tako imenovanih VLAN-domen, da med različnimi napravami ali računalniki že na tej ravni ni povezljivosti, če za to ni potrebe. Če nekdo vstopi v neki računalnik, od tam pa lahko dostopa do kateregakoli dela proizvodnje, ker omrežje ni segmentirano, potem imamo že v osnovi varnostno težavo. Marsikatero podjetje to osnovno pomanjkljivost sicer že odpravlja. Naslednji korak je zagotoviti ločevanje od zunanjih omrežij, v prvi vrsti od javnih omrežij oziroma internetnega omrežja ter omrežja oziroma segmenta, kjer tečejo poslovne aplikacije (IT).

Ko poskrbimo za segmentacijo omrežja in ločevanje od zunanjih omrežij, pa je treba najprej ugotoviti, kje so morebitne ranljivosti. Proizvodne linije so avtomatizirane in vodene z računalniškimi sistemi, vemo pa, da so v vseh operacijskih sistemih določene varnostne pomanjkljivosti. V te sisteme se, ko so enkrat nameščeni, praviloma veliko ne posega, saj posodobitve in nadgradnje pomenijo prekinitev



proizvodnega procesa, kar pa v podjetjih ne pride v poštev. In zato vse varnostne vrzeli ostajajo. Na podlagi analize in ugotovitev se potem poskrbi za ustrezne varnostne rešitve, ki posegajo do aplikativne (vsebinske) ravni podatkovnih pretokov, ki tečejo v procesnem sistemu.

Zato morata krepitev kibernetske varnosti in kibernetske higiene zaposlenih postati prioriteti podjetij vseh velikosti, tako v okolju IT in OT. Ta bi morala najprej ugotoviti, kakšna je sploh njihova varnostna slika. Šele, ko se podjetja odločijo za varnostni pregled, dobijo nazorno sliko in pregled, kako zaščitena oziroma izpostavljena so. Strokovnjaki za kibernetsko varnost jim pojasnijo, kje so varnostna tveganja, kje smo zaznali šibkosti in ranljivosti, ki jih lahko izrabijo nepridipravi, in podajo priporočila za zmanjšanje tveganj in odpravo ranljivosti.

Najboljši varnostni pregled je tisti, ki vključuje tudi testiranje zaposlenih, saj izkušnje potrjujejo, da so najbolj uspešni kibernetski napadi izvedeni s tehnikami socialnega inženiringa, te pa lahko odbijemo le, če so zaposleni ustrezno izobraženi in osveščeni o pomembnosti kibernetske varnosti. Ko pride do vdora v informacijski sistem, je treba ugotoviti in analizirati incident, da se v prihodnosti prepreči in zmanjša varnostna tveganja.

Omrežje kot temeljni kamen poslovanja in varnosti

Večina napadov na sodobna IT in OT-okolja se zgodi prek omrežja. Sodobna tehnologija z vpeljanimi algoritmi strojnega učenja, umetne inteligence in globokega preverjanja paketov stalno spremlja prometne tokove, se stalno uči in v realnem času zaznava varnostne grožnje, tveganja in sistemske anomalije. Tako je v pomoč varnostim analitikom, saj jim avtomatizacija zamudnih varnostnih operativnih nalog sprosti dragoceni čas, da lahko opravljajo pomembnejša dela. Ti sistemi se lahko tudi integrirajo z drugimi omrežnimi in IT-sistemi, kot so požarne pregrade, omrežne naprave, SIEM, sistemi za orkestracijo.

S tehnologijami strojnega učenja in z napredno analitiko podprta orodja so varnostnim strokovnjakom v pomoč pri odkrivanju napadov. Stalno učeči se model analize obnašanja naprav, povezav in podatkov napadalce odkriva v realnem času, hkrati pa omogoča hiter in učinkovit odziv na varnostne incidente. Pravočasna zaznava in hiter ter ustrezen odziv sta ključna elementa informacijske varnosti, saj hitro zaznan napadalec v omrežju ali sistemu podjetja ne more narediti velike škode.

Cilj zlonamernežev je vdreti v okolje podjetja in tam ostati neopažen. Grožnje so zato vse bolj sofisticirane in prikrite, odkrijejo jih lahko predvsem algoritmi s področja strojnega učenja in umetne inteligence, ki hitro analizirajo ogromne količine podatkov, ter skrbnike za informacijsko varnost opozorijo na odkrite anomalije. Danes se umetna inteligenca uporablja za nadgradnjo varnostnih rešitev. Takšne rešitve uporabljajo predvsem podjetja, ki so že tradicionalno izpostavljena kibernetskim napadom, že jutri pa jih bodo morala uporabljati vsa podjetja.

S takim pristopom pomembno skrajšamo čas zaznave groženj, kar je odločilnega pomena. Zato je zelo pomembno, da



S tehnologijami strojnega učenja in z napredno analitiko podprta orodja so varnostnim strokovnjakom v pomoč pri odkrivanju napadov. Stalno učeči se model analize obnašanja naprav, povezav in podatkov napadalce odkriva v realnem času, hkrati pa omogoča hiter in učinkovit odziv na varnostne incidente.

si podjetja v prvi vrsti sama ustvarijo koncepte in vizijo razvoja kibernetske varnosti v lastnih okoljih.

Žal pa ugotavljamo, da zaščita pred kibernetskimi napadi še vedno ni prioriteta, saj v povprečju napadalci v omrežju in sistemih napadenega okolja organizacije ostanejo neodkriti kar 280 dni. V tem času pa lahko odtujijo občutljive podatke, zlorabijo sisteme, skratka povzročijo visoko poslovno škodo. ■

www.smart-com.si

22. Tehnološka konferenca Smart Com

NAPREDNE REŠITVE ZA NOVO ERO

Zagotovite celovito kibernetsko varnost in zanesljiva omrežja za neprekinjeno poslovanje

Kibernetska varnost

Poslovno kritični sistemi (ICS)

Omrežne tehnologije

Prenesite video posnetke strokovnih predstavitev.

Vaš dostop

bit.ly/2Udqros

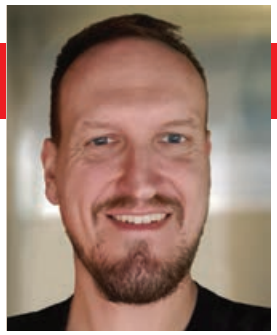
30 SMART COM

Organizator konference

Extreme networks · Juniper Networks · NOKIA · Nozomi Networks · RAPID7 · Trend Micro · WALLIX · VECTRA · Vade Secure

Tehnološki partnerji konference

Avtor: dr. Matej Drašček / vodja službe notranje revizije v LON, d.d.*



SODELOVANJE NOTRANJE REVIZIJE IN INFORMACIJSKE VARNOSTI PRI OBVLADOVANJU TVEGANJ KIBERNETSKE VARNOSTI

Tveganja postajajo v sodobnem poslovnem okolju čedalje bolj prepletena, kar pomeni, da je obvladovanje vseh tveganj postalo prioriteta vseh organizacij, če želijo preživeti. Pri uspešnem obvladovanju tveganj sodeluje celotna organizacija, pri čemer imajo različne funkcije v organizaciji različne vloge.

Eden izmed najbolj uporabljenih modelov obvladovanja tveganj je model treh linij IIA[1], ki organizacijo in njene procese/funkcije razdeli glede na njihove vloge na tri linije. V tem članku predstavljamo, kako ta model uporabimo za obvladovanje tveganj kibernetske varnosti, pri čemer se bomo osredotočili na različno, a obenem podobno ciljno usmerjeni funkciji, informacijsko varnost in notranjo revizijo.

Model treh linij IIA

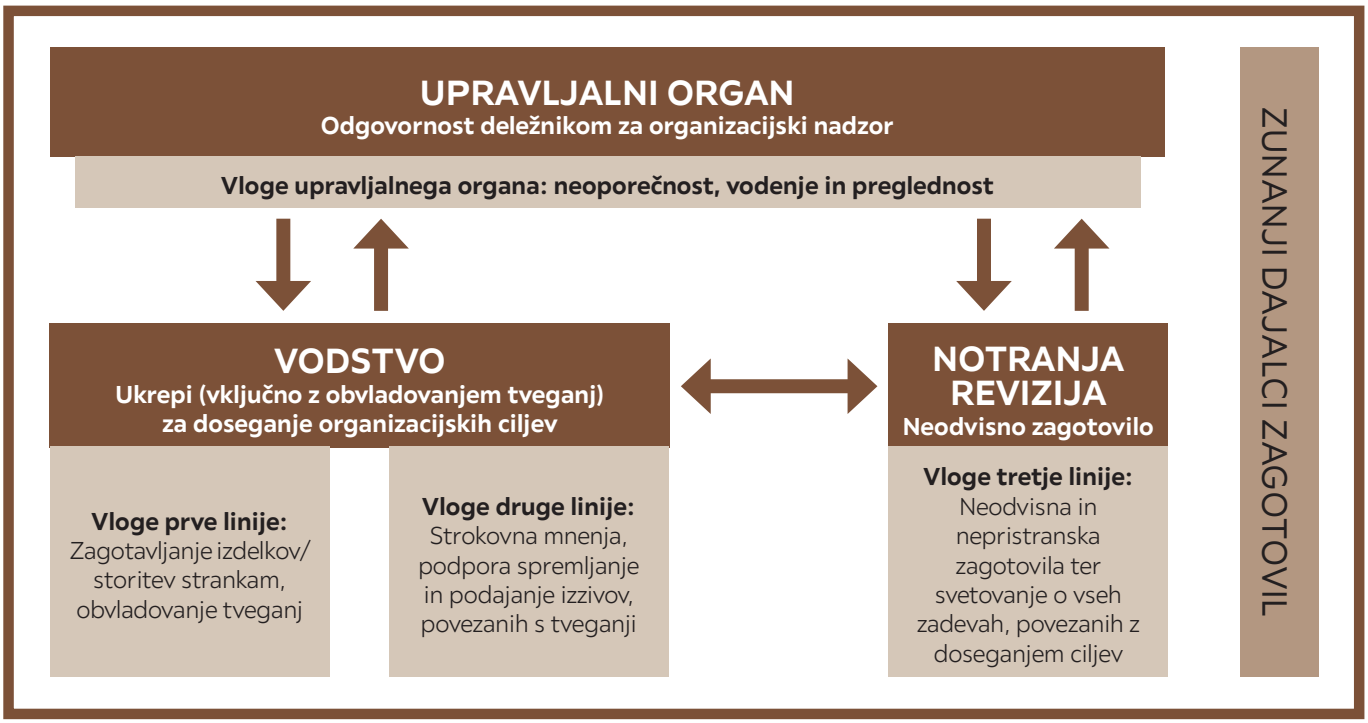
Spremembe v regulativi, tehnologiji, socialna omrežja, družbene spremembe, COVID-19 je le nekaj razlogov, zakaj organizacije potrebujejo učinkovite postopke in procese, da dosežejo zastavljene cilje. Z modelom treh linij (Slika 1) organizacije določijo strukture in postopke, ki jim pomagajo, da dosežejo cilje in hkrati zagotavljajo uspešno obvladovanje tveganj.

Napake informacijske varnosti se največkrat pojavijo, ko nadzor ni nenehni proces kibernetskega procesa.

V modelu imamo tri linije z različnimi vlogami. Odgovornost za doseganje organizacijskih ciljev imata tako prva kot druga linija. Vloge prve linije so neposredno usklajene z zagotavljanjem izdelkov oz. storitev kupcem organizacije, kar obsega tudi vloge podpornih funkcij. Vloge druge linije zagotavljajo pomoč pri obvladovanju tveganj. Vloge druge linije so zagotavljanje strokovnih mnenj, podpora in spremljanje izvajanja nalog prve linije. Vloge druge linije so ponavadi usmerjene k bolj določenim ciljem obvladovanja tveganj, kot so: skladnost poslovanja, notranji nadzor, informacijska varnost in zagotavljanje kakovosti. Pri tem je pomembno, da odgovornost za obvladovanje tveganj še vedno ostaja del vlog prve linije in pripada vodstvu, pri čemer pa so lahko vloge prve in druge medsebojno prepletene ali ločene.

Vloge tretje linije, ki je notranja revizija, so zagotavljanje neodvisnih in objektivnih zagotovil ter svetovanj glede uspešnosti upravljanja organizacije, obvladovanja tveganj ter notranjih kontrol. To notranja revizija dosega z ustreznim izvajanjem sistematičnih in disciplinirani procesov, podajanjem strokovnih mnenj in z vpogledi v delovanje organizacije. O svojih ugotovitvah poroča vodstvu in upravljalnemu organu (upravi in nadzornemu svetu), s čimer spodbuja in omogoča nenehne izboljšave.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Slika 1: Model treh linij IIA

Vloga informacijske varnosti[2] pri obvladovanju kibernetskih tveganj

Kibernetska tveganja so precej bolj dinamična kot ostala tradicionalna tveganja, zato ta tveganja zahtevajo hitre in učinkovite rešitve. Ker se ta tveganja hitro spreminjajo in kot tudi izpostavljenost organizacij do njih, je druga linija kritična, da nadzoruje zadostno pripravo in zagotovi odgovor organizacije na ta tveganja. Že majhne ranljivosti lahko organizaciji povzročijo nevšečnosti, kar lahko vodi tudi do izgube ugleda, kaznim regulatorjev in velikim finančnim izgubam.

Informacijska varnost v drugi linji ponavadi vključuje funkcijo celovitega obvladovanja tveganj in skladnosti IT tveganj in igra pomembno vlogo pri odnosu organizacije do kibernetskih tveganj in notranjih kontrol. Med tipične vloge informacijske varnosti spadajo:

- Oblikovanje politik, usposabljanj in testiranj za kibernetsko varnost;
- Izvajanje rednih ocen tveganja kibernetske varnosti;
- Zbiranje informacij o nevarnostih kibernetske varnosti;
- Klasifikacija podatkov in oblikovanje priviligiranih vlog za dostope;
- Nadziranje incidentov, glavnih kazalcev tveganj in korektivnih ukrepov;
- Zadržanje IT talentov;
- Ocenjevanje odnosov z zunanjimi izvajalci, dobavitelji in drugimi ponudniki storitev;
- Načrtovanje in testiranje načrta neprekinjenega poslovanja in sodelovanje pri vajah in testih obnovitvenega načrta (ang. Disaster recovery)

Da te naloge izpolnjuje, mora informacijska varnost tesno sodelovati s prvo in tretjo linijo, saj s tem zagotovi ozaveščenost upravljalnega organa (bodisi nadzornega sveta in uprave) in tako zagotovi poročanje, o kibernetskih tveganjih in notranjih kontrolah ter njihovi učinkovitosti, odločevalcem v organizaciji. Pri tem mora biti vloga informacijske varnosti jasno opredeljena. Npr. pooblaščenec za informacijsko varnost mora imeti vnaprej opredeljeno vlogo, ki jo ima pri nujnih varnostnih incidentih.

Ker igrajo zunanji izvajalci v zagotavljanju delovanja ITja pomembno vlogo, mora informacijska varnost oceniti kibernetska tveganja takega sodelovanja, predvsem kadar imajo zunanji izvajalci dostop do zaupnih in kritičnih informacij preko neposrednega dostopa do mreže ali drugih metod podatkovnih prenosov. Tehnične in pogodbene kontrole zahtevajo pregled, zato je naloga informacijske varnosti, da te kontrole preverja in po potrebi poroča upravljalnemu organu.

Napake informacijske varnosti se največkrat pojavijo, ko nadzor ni nenehni proces kibernetskega procesa. Nove nevarnosti na področju kibernetskih tveganj se pojavljajo vsak dan, zato je nenehno usposabljanje, izobraževanje in nadzor nujno potreben za zagotovitev obvladovanja teh tveganj in zaščite podatkov ter sistemov. Da se to zagotovi, organizacije ponavadi oblikujejo kibernetske odbore, ki jih vodi pooblaščenec za informacijo varnost in v katerem sodelujejo tudi drugi deležniki organizacije. Ena pomembnih odgovornosti takih odborov je prepoznati glavna sredstva, oceno tveganja, verjetnost tveganj in njihov vpliv ter notranje kontrole, ki zagotovijo zaščito teh pomembnih sredstev

Kibernetska tveganja so precej bolj dinamična kot ostala tradicionalna tveganja, zato ta tveganja zahtevajo hitre in učinkovite rešitve.



pred kibernetskimi napadi. Ta odbor razglablja tudi o novih tveganjih in pomembnih matrikah, vključno z rezultati penetracijskih testov, ki preverjajo uspešnost varnostnih obramb pred napadi.

Druga pomembna tveganja informacijske varnosti, katere se jih velikokrat spregleda, so tudi:
- Nejasno opredeljene vloge pri obvladovanju tveganj med različnimi linijami, da se zagotovi, da so tveganja učinkovito in uspešno prepoznana in obvladovana;
- Pomanjkljivo vključevanje višjega vodstva in uprave, da se zagotovi uresničevanje aktivnosti kibernetske varnosti;
- Pomanjkljivi odziv organizacij na varnostne incidente in neanaliziranje temeljnih vzrokov le teh;
- Neopredeljeni protokoli in odgovornosti pri odzivu in poročanju incidentov;
- Pomanjkljive kompetence zaposlenih;
- Pomanjkljivo izmenjavanje informacij o novih tveganjih znotraj in med panogami;
- Pomanjkljiva sredstva (čas, denar in viri) za vpeljavo notranjih kontrol, vključno z rednim vzdrževanjem in posodabljanjem.

Vloga notranje revizije pri obvladovanju kibernetskih tveganj

Kot tretja linija, notranja revizija igra pomembno vlogo pri obvladovanju tveganj kibernetske varnosti, pri čemer:
- Podaja neodvisne in sprotne ocene preventivnih in detektivih kontrol glede kibernetskega tveganja;
- Ocenjuje IT sredstva s privilegiranimi dostopi glede standardnih varnostnih konfiguracij, problematične strani, zlonamerne programske opreme in pridobivanje podatkov;
- Neodvisno pregleduje vpeljane ukrepe v organizaciji;
- Izvaja oceno kibernetskega tveganja glede izvajanja storitev organizacije, zunanjih izvajalcev in dobaviteljev.

Notranja revizija lahko pomaga informacijski varnosti pri izboljšanju obvladovanja tveganj kibernetske varnosti:
- Z ocenjevanjem odnosa med kibernetskim in ostalimi tveganji organizacije;
- Pri prioritizaciji odzivov in kontrolnih aktivnosti;
- Pri podajanju neodvisnih zagotovil za zmanjševanje tveganj v celotni organizaciji: privilegirani dostopi, mreža, zunanji izvajalci itd.;
- Z dajanjem zagotovil pri korektivnih ukrepih;
- Z dvigovanjem zavedanja in koordinaciji obvladovanja kibernetskih tveganj, predvsem tam, kjer organizacija nima vlog za ta tveganja v prvi in drugi liniji;
- Z validacijo procesov kibernetskega tveganja, kar vključuje tudi preverjanje načrta neprekinjenega poslovanja in obnovitvenega načrta organizacije.

Notranja revizija ob tem ocenjuje uspešnost notranjih kontrol, ki jih izvaja tako prva kot druga linija. Splošne IT kontrole so osnova za obvladovanje kibernetskih tveganj, vendar ne nudijo popolne zaščite. Kompleksnost kibernetskih tveganj zahteva dodatne plasti kontrol, kot so nadzor nad tveganji, odkrivanje novih nevarnosti in izvajanja preventivnih ukrepov. Ker tradicionalna notranja revizija tu ni uspešna, mora biti tudi notranja revizija pri revidiranju kibernetskih tveganj inovativna. Nenehno revidiranje, med drugim ne samo kibernetske

Med notranjo revizijo in informacijsko varnostjo mora potekati redna komunikacija, ki zagotavlja usklajenost dela obeh funkcij s strateškimi in operativnimi potrebami organizacije. Obe funkciji s tem pridobivata znanje in razumevanje organizacije, kar pripomore k dodani vrednosti organizacije.



varnosti, ampak tudi kibernetskih tveganj na drugih področjih pri vsakem notranje revizijskemu pregledu, je zato nujno potrebno, da se zagotovi zadostna zaščita pred kibernetskimi tveganji.

Sodelovanje notranje revizije in informacijske varnosti

Upravljalni organ, vodstvo, informacijska varnost in notranja revizija imajo sicer različne odgovornosti, vendar morajo biti vse njihove dejavnosti usklajene s cilji organizacije. Osnova uspešne usklajenosti je redna in učinkovita koordinacija, sodelovanje in komunikacija.
Kar notranjo revizijo razlikuje od ostalih funkcij je njena objektivnost in nepristranskost pri načrtovanju in izvajanju svojega dela. Odgovorna je upravljalnemu organu, vendar to ne pomeni osamitve od drugih funkcij. Med notranjo revizijo in informacijsko varnostjo mora potekati redna komunikacija, ki zagotavlja usklajenost dela obeh funkcij s strateškimi in operativnimi potrebami organizacije. Obe funkciji s tem pridobivata znanje in razumevanje organizacije, kar pripomore k dodani vrednosti organizacije.

Zaključek

Kibernetska tveganja se po vseh raziskavah, pri katerih sodelujejo notranji revizorji, uvrščajo v vrh najpomembnejših tveganj, katerim je podvržena vsaka organizacija. Model treh linij pomaga obvladovati ta tveganja na način, da organizacija dosega svoje cilje. Pri tem je pomembno, da vse linije med seboj sodelujejo. Čeprav imajo linije različne vloge, kot tudi odgovornosti, je skupni imenovalec vseh cilj dodajanja vrednosti organizaciji. Informacijska varnost zagotovo pri tem igra eno pomembnejših vlog, saj je njena glavna odgovornost obvladovanje tveganj informacijske varnosti, kamor spada tudi kibernetska varnost. Sodelovanje med informacijsko varnostjo in notranjo revizijo, pa mora potekati na odprtem in strokovnem dialogu, ki obema funkcijama lahko prinese samo dobrobit. Čeprav sodelovanje med obema funkcijama v slovenskem prostoru še ni tako razvito, pa model treh linij ponuja enostaven pristop, ki je prilagodljiv vsaki organizaciji, glede na njene cilje. Začeti pa je potrebno na začetku, kjer se določijo vloge in naloge vsake linije. To pa, kar smo predstavili v tem članku, model tudi že ponudi.

Viri:

Institute of Internal Auditors. IIAjev model treh linij. Posodobitev IIA modela Tri obrambne linije.

Dostopno: https://global.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Slovenian.PDF

Institute of Internal Auditors. Assessing Cybersecurity RiskRoles of the Three Lines of Defense. Dostopno: vhttps://global.theiia.org/standards-guidance/Member%20Documents/GTAG-Assessing-Cybersecurity-Risk.pdf

1 The Institute of Internal Auditors (IIA) je najbolj prepoznan inštitut na področju notranje revizije na svetu, ki tudi izdaja Mednarodne standarde strokovnega ravnanja pri notranjem revidiranju, ki jim sledijo tudi notranji revizorji v Sloveniji.

2 V članku uporabljamo termin informacijska varnost, pri čemer mislimo neodvisno funkcijo informacijske varnosti, ki ni del operativnih nalog ITja. Ponavadi je to delovno mesto v organizaciji opredeljeno kakor tudi pooblaščenec za informacijsko varnost. ■

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

VSAK VAREN DAN SE ZAČNE KOT VSAK SKRBNO NAČRTOVAN VARNOSTNI SISTEM



ZARJA ELEKTRONIKA

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

INTEGRACIJSKI SISTEMI:

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

"IZDELAVA SISTEMOV PO MERI KUPCA"

NAPREDNE TEHNOLOGIJE VAROVANJA

Smo ekskluzivni zastopnik za profesionalno opremo najvišjega kakovostnega razreda Tecnoalarm



ZARJA ELEKTRONIKA

Avtorja: Rafal Jaczynski in mag. Gašper Cotman / Huawei





OSNOVNI OKVIR ZA ZAGOTAVLJANJE VARNOSTI V OMREŽJIH 5G

Varnost katerega koli telekomunikacijskega omrežja - in 5G ni nobena izjema - zahteva učinkovito sodelovanje operaterjev, ponudnikov rešitev in regulatorjev trga, prav tako pa mora obravnavati tveganja, ki se pojavljajo v celotnem življenjskem ciklu telekomunikacijskega omrežja.

Za pravilno razumevanje vlog vseh posameznih deležnikov, ki imajo pomemben vpliv na zagotavljanje varnosti v 5G omrežjih, bomo v nadaljevanju podrobneje pojasnili njihove vloge in možne pristojnosti. Seveda se je potrebno zavedati, da se poleg teh splošno opredeljenih pristojnosti, lahko pri uvajanju novih tehnologij, vsekakor srečamo tudi s posameznimi specifikami, ki jih ima v svoj normativni sistem vpeljana posamezna država.

Vloga operaterja pri zagotavljanju varnosti omrežij 5G je ključnega pomena. Telekomunikacijski operater je odgovoren za varnost omrežja in opravljenih storitev. Vloga upravljavca omrežja je zlasti:

- Opredelitev zahtev za kibernetsko varnost za ponudnike rešitev 5G;
- Oblikovanje nadzornih mehanizmov omrežja, ki temeljijo na lastnih procesih ponudnikov rešitev 5G in tujih rešitvah;
- Nadzor dostopa do omrežnih naprav in podatkov 5G;
- Nadzor omrežne varnosti in ravnanja z incidenti;
- Zagotavljanje zahtevanih parametrov kakovosti in neprekinjenost storitve.

Vloga ponudnikov rešitev je pomagati omrežnim operaterjem pri zagotavljanju njihove varnosti, predvsem pa:

Omrežja 5G bodo z občutno boljšimi tehničnimi parametri, omogočala podporo novim aplikacijam, ki s prejšnjimi generacijami mobilnih komunikacijskih tehnologij še niso bile izvedljive.



- Popolna uporaba 3GPP[1] varnostnih mehanizmov v fizični strojni in programski rešitvi;
- Oblikovanje izdelkov ob upoštevanju najboljših praks, standardov in regulativnih zahtev za kibernetsko varnost;
- Razvoj izdelka v skladu z najboljšo prakso - vključno s stalno analizo varnosti programske opreme, medtem ko je izdelek še v razvoju oz. v dobavni verigi;
- Preverjanje varnosti rešitev v skladu z zahtevami trga - ob upoštevanju ustreznega certificiranja, če je le to potrebno;
- Vpeljava rešitev v omrežje operaterja in njihov prenos v skladu z varnostnimi pravili;
- Obravnavanje ranljivosti, prepoznanih v izdelkih, in posredovanje varnostnih popravkov;
- Upoštevanje operaterjevih varnostnih zahtev v primeru podpornih ali nadzornih storitev, zlasti skrb za obdelavo podatkov v skladu s pogodbo in zahtevami veljavne zakonodaje posamezne države.

Regulatorji trga imajo ravno tako izjemno pomembno vlogo pri zagotavljanju varnosti 5G - glavne naloge javnih uprav so:



- Določitev varnostnih zahtev, ki jih morajo izpolnjevati omrežja 5G, zgrajena v Republiki Sloveniji;
- Opredelitev pravil za varnostno preverjanje omrežij in omrežnih naprav, ki zajemajo vse udeležence na trgu;
- Zagotoviti delovanje sistema za preverjanje varnosti s posebnim poudarkom na uporabi ustreznega programa certificiranja.

Tveganja v dobavni verigi ponudnikov rešitev omrežij 5G

Oskrbovalna veriga vseh ponudnikov rešitev 5G je ranljiva na grožnje, ki jih predstavlja mednarodna mreža dobaviteljev. Te lahko izhajajo iz eksteritorialne zakonodaje, politik, ki jih izvajajo države, ki niso članice EU, svetovne trgovinske vojne in naravne nesreče, ki bi lahko motile neprekinjeno dobavo.

Stopnja tveganja v globalizirani dobavni verigi proizvajalcev opreme 5G zahteva posebno skrb pri upravljanju varnosti - telekomunikacijski operaterji morajo od proizvajalcev zahtevati, da upoštevajo najboljše prakse, vključno s certificiranjem v skladu z ustreznimi mednarodnimi standardi (npr. ISO 28001).

Kibernetska varnost 5G

Omrežja 5G bodo z občutno boljšimi tehničnimi parametri, omogočala podporo novim aplikacijam, ki s prejšnjimi generacijami mobilnih komunikacijskih tehnologij še niso bile izvedljive. Zelo verjetno je, da bo število različnih omrežnih aplikacij 5G bistveno večje kot pri omrežjih 3G in 4G, kar pomeni tudi, da se bo znatno povečalo tudi število in raznolikost naprav, ki uporabljajo to novo omrežje. Ta dva dejavnika povzročata večjo prožnost in zapletenost, s tem pa tudi večjo »površino napada« za omrežja 5G.

Praviloma se glavne tehnološke grožnje varnosti omrežij pete generacije ne razlikujejo od tistih, ki so že prisotne v omrežju 4G. Zelo verjetno je, da s pojavom omrežij 5G v Sloveniji ne bo novih, neznanih groženj s področja kibernetske varnosti.

Ta učinek je 3GPP[1] ugotovil že zelo zgodaj - zato tehnični varnostni standardi 5G, ki se začnejo z R15, zagotavljajo pomembne izboljšave omrežja 4G in obravnavajo nekatera ključna tveganja že na ravni standardizacije. Poleg tega je sodelovanje znotraj ekosistema operaterjev, ponudnikov rešitev in neodvisnih ponudnikov storitev pripeljalo do tržnih rešitev, ki dopolnjujejo mehanizme, določene v tehničnih standardih 5G.

Izpostaviti velja štiri ključne izboljšave varnostnih mehanizmov v primerjavi s standardom četrte generacije:

1. Enotna overitev - v primerjavi z mehanizmi, specifičnimi za dostop 4G;
2. Prilagodljiva varnostna politika omrežja za prilagajanje različnim omrežnim aplikacijam - v odsotnosti takšne prilagodljivosti v omrežjih 4G;

Dostop do znanja je prav tako pomembna prednost. Zahvaljujoč uporabi tehnologije, ki je že na voljo drugje (kot na primer v zasebnih ali javnih oblakih ali programsko definiranih omrežjih podatkovnih centrov), je število strokovnjakov z ustreznim strokovnim znanjem, ki je koristno za zaščito omrežja 5G, preprosto večje kot v prejšnjih generacijah mobilnih omrežij.

3. Boljša zaščita zasebnosti uporabnika omrežja - s šifriranjem njegove identifikacijske številke, da se zagotovi višja raven varnosti kot psevdo-animacijski mehanizem, uporabljen v prejšnji generaciji;
4. Uvedba dodatnega elementa arhitekture, ki omogoča filtriranje signalnih sporočil in »skrivanje topologije operaterjevega omrežja pred zunanjim svetom - v omrežjih 4G te funkcije standardi še niso zahtevali;

Rezultat teh izboljšav je že peta generacija standarda, ki zagotavlja najvišjo raven varnosti obstoječih javnih mobilnih komunikacijskih sistemov. Seveda sami varnostni mehanizmi, ki jih predvidevajo standardi 3GPP, ne zadoščajo za odziv na tveganja, ki se lahko pojavijo v omrežjih 5G - zato tako operaterji kot dobavitelji uporabljajo rešitve, ki presegajo varovala, predvidena s standardi.

Prav tako je treba poudariti, da se ponudnik aplikacij, ki uporablja 5G, ne sme zanašati samo na omrežne varnostne mehanizme, če ne izpolnjujejo zahtev svojih strank (npr. zaupnost od konca do konca ni zagotovljena). Mehanizmi aplikacijskega sloja bi morali v takem primeru zagotavljati raven zaščite, ki jo zahteva storitev.

Občutljivi 5G omrežni elementi

Osnovno izhodišče varnostnih mehanizmov 5G je bila razdelitev omrežnih elementov na zaupanja vredne domene. Čim dlje kot je jedro omrežja, tem nižja je lahko stopnja zaupanja. Ta koncept omrežne funkcije, kot sta UDM (Unified Data Management) in ARPF (Authentication Credential Repository & Processing Function), zahtevajo najvišjo stopnjo zaupanja. GNB (gNodeB) predstavljen v DU/CU (distribuirana enota/centralizirana enota) pa velja za precej manj občutljiv element omrežne arhitekture. Tu je treba poudariti, da se elementi evolucijskega pristopa k izvajanju omrežja 5G v Sloveniji ne bodo pojavili prej kot v nekaj letih - v prvi fazi gradnje 5G omrežja bodo operaterji preprosto razširili obstoječa 4G omrežja na nove 5G (gNodeB) oddajnike.

Tako arhitektura kot tudi poslovni ekosistem 5G vsebujeta elemente, ki so kritični za varnost, in niso vključeni v zgoraj omenjeni model zaupanja - na primer aplikacije, ki delujejo na podlagi tehnologije selitve računalniških zmogljivosti na rob (Multi-Access Edge Computing) lahko zagotovijo partnerji ali kupci operaterjev, kar zahteva od operaterjev, da zagotovijo dodatno varnostno analizo.





Tehnološka tveganja

Praviloma se glavne tehnološke grožnje varnosti omrežij pete generacije ne razlikujejo od tistih, ki so že prisotne v omrežju 4G. Ravno tako se ne razlikujejo od tveganj, znanih iz drugih ključnih aplikacij za uvajanje 5G (virtualizacija, programsko določena omrežja, mikro storitve itd.). Zelo verjetno je, da s pojavom omrežij 5G v Sloveniji ne bo novih, neznanih groženj s področja kibernetske varnosti. Poleg tega operaterji v nasprotju z informacijami, ki se pojavljajo v javnem prostoru, že uporabljajo tehnologije jedrnega omrežja pete generacije - na primer, tehnologija virtualizacije omrežnih funkcij (NFV - Network Function Virtualization) se že uporablja v virtualiziranih osrednjih omrežjih 4G.

Glavne kategorije tehničnih tveganj, ki se lahko pojavijo v omrežjih 5G povezujemo s scenariji tveganj. Scenariji tveganj so načeloma razdeljeni v dve skupini: tiste, ki izhajajo iz omrežnih vmesnikov 5G proti zunanjemu svetu (grožnje zunaj domene), in tiste, ki so prisotni v notranji 5G povezani arhitekturi (grožnje znotraj domene).

Zunanje grožnje omrežjem 5G so enake nevarnostim omrežij prejšnje generacije - z izjemo, da imajo napadi vrste DDoS (Distributed Denial of Service) večji vpliv na samo varnost omrežja. Le ti se pojavljajo kot posledica potencialno nezavarovanih internetnih naprav v omrežju, ki ima večjo zmogljivost. Okolje MEC zahteva pozornost tudi v smeri zagotavljanja izolacije virov, ki jih upravlja omrežni operater, ponudnik oblačne infrastrukture ali ponudnik aplikacij (v primeru, da gre za ločene organizacije). V takem primeru lahko pričakujemo verjetno nižjo stopnjo fizične varnosti, kot je pričakovana v podatkovnem centru centralnega operaterja.

Varnostni mehanizmi, uvedeni v standardih in izdelkih 5G, v večji meri obravnavajo zunanja tveganja kot v omrežjih 4G, kar ima za posledico nižjo stopnjo tveganja za telekomunikacijsko omrežje. Seveda mora biti zaradi široke uporabe 5G njegova uporaba za določene aplikacije predmet analize tveganja. V nekaterih primerih bo za aplikacijo morda treba uporabiti dodatne varnostne mehanizme.

Nevarnosti znotraj omrežja so povezane s komunikacijo med omrežnimi elementi, ki v osnovi temeljijo na IP protokolu, tehnologijah, ki se uporabljajo za izpolnjevanje funkcionalnih zahtev omrežja 5G (npr. NFV – Network Function Virtualization, SDN – Software Defined Network, SBA – Software-based Architecture) ali lokaciji posameznih elementov (npr. v primeru selitve tehnologij računalniških zmogljivosti na rob).

Jedro računalniškega omrežja v oblaku lahko temelji na strojni platformi s prostim dostopom (Commercial-Off-The-Shelf - COTS) ali pa na uporabi namenske platforme s pomočjo specializiranih elektronskih verzij FPGA (Field-programmable gate array). Obe rešitvi imata svoje prednosti in slabosti, in pri opremi COTS je treba upoštevati tveganja, povezana z večjo heterogenostjo celotne rešitve, vključno z verjetno uporabo odprtokodnih rešitev.

Omeniti velja, da 5G, medtem ko v mobilno omrežje vse bolj vnaša svetovne grožnje, ki so značilne za internet in poslovno okolje. Ravno to pa na drugi strani omogoča uporabo najboljših varnostnih praks, ki so bile razvite v IT sektorju. Dostop do znanja je prav tako pomembna prednost. Zahvaljujoč uporabi tehnologije, ki je že na voljo drugje (kot na primer v zasebnih ali javnih oblakih ali programsko definiranih omrežjih podatkovnih centrov), je število strokovnjakov z ustreznim strokovnim znanjem, ki je koristno za zaščito omrežja 5G, preprosto večje kot v prejšnjih generacijah mobilnih omrežij.

1 The 3rd Generation Partnership Project je okvirni naziv za cel niz standardizacijskih organizacij, ki razvijajo protokole za mobilne telekomunikacije. ■


Z željo, da bi ustvarili popolnoma povezan in
pametnejši svet, smo zavezani k digitalizaciji vsakega
posameznika, doma in organizacije.
V SLOVENIJI. ZA SLOVENIJO.
20 YEARS
OF CONNECTING
EUROPE
HUAWEI

Avtor: izr. prof. dr. Marko Gerbec / Institut Jožef Stefan



O VARNOSTNIH IZZIVIH PREHODA NA VODIKOVO EKONOMIJO

Pojem prehoda naše družbe na vodikovo ekonomijo pomeni, prehod od uporabe fosilnih goriv na vodik, kot gorivo za naše stroje, ki pri uporabi ne sproščajo toplogrednih plinov. V nadaljevanju si oglejmo, kje so glavni izzivi omenjenega prehoda.

Vodik je najlažji, najstarejši in najbolj razširjen element v vesolju in na našem planetu ga imamo na srečo obilico. Vodiku bi pravzaprav morali reči vodonosec, ker pri njegovem gorenju nastaja (le) voda – od tod njihov simbol H vezano na njegov izvor iz grških besed »Hydro« in »genes« (dela vodo), ki je tudi blizu imenu v angleščini Hydrogen. Vodik se nahaja vedno le v spojinah, predvsem v vodi, pa tudi v nafti, zemeljskem plinu, ipd., uporablja pa se predvsem v proizvodnji goriv (čiščenje naftnih derivatov), osnovnih kemikalij, npr., amonijaka (in najprej umetnih gnojil), metanola (osnova za umetne snovi/lepila), vodikovega peroksida, ipd. V tem smislu torej uporaba vodika v industrijskih obratih ni nič novega.

Pojem prehoda naše družbe na vodikovo ekonomijo pomeni prehod od uporabe fosilnih goriv (predvsem premog, naftni derivati, zemeljski plin) na vodik kot gorivo za naše stroje, ki pri uporabi (gorenju) ne sproščajo toplogrednih plinov (predvsem ogljikov dioksid). V čem je problem? Problema sta vsaj dva.

Prvi je ta, kot že omenjeno na začetku, da imamo le vodikove spojine, ne pa elementarnega vodika. To pomeni, da ga moramo najprej proizvesti iz spojin, kar pa pomeni da moramo uporabiti energijo, kjer pa večinoma še vedno uporabljamo fosilna goriva. Običajno industrija proizvaja vodik iz zemeljskega plina s t.i. postopkom reforminga pri visoki temperaturi (~1000 °C) z vodno paro pri čemer na koncu nastaneta vodik in ogljikov dioksid. Težava je le v tem, da za 1 tono vodika nastane tudi ~10 ton ogljikovega dioksida [International Energy Agency, stran 38], kar seveda ni v skladu s ciljem zmanjševanja emisij. Upoštevati je potrebno tudi energetske izkoristke za alternativno direktno uporabo fosilnih goriv in alternativno uporabo poti preko vodika, npr., v obeh primerih za pogon vozil. V tem smislu je alternativa preko vodika dražja in primerjalno prevozimo manj (res pa je, da med uporabo



ni omembe vrednih emisij). Rešitev, vsaj na dolgi rok, je videti v tem, da preidemo na proizvodnjo vodika iz obnovljivih virov energije (sonce/fotocelice, vetrnice, biomasa) preko elektrolize (razkroja vode do vodika in kisika z električno energijo), kjer so izzivi predvsem ekonomske (cena, investicije) in logistične (skladiščenje, distribucija) narave.

Drugi problem je v tem, da prehod od rabe fosilnih goriv na vodik, oziroma na obnovljive vire energije zahteva korenito spremembo energetske infrastrukture, kar obsega vsaj proizvodnjo, skladiščenje, distribucijo in končno uporabo (npr., v vozilih ali gospodinjstvih). Pri tako veliki spremembi, ki se obeta, le te uspejo in padejo na podrobnostih. Ker je to osrednja tema tega prispevka, primerjajmo najprej nekatere lastnosti (Hydrogen Fuel Cell Engines and Related Technologies) najčistejšega fosilnega goriva - zemeljskega plina in vodika, ki je resen kandidat za naslednika[1]:

Lastnost	Enota	Zemeljski plin	Vodik
Sestava	-	metan [a] (CH_4)	H_2
Agregatno stanje (25 °C, 1 bar)	-	plin	plin
barva, vonj	-	brez [b]	brez
Tališče	°C	-182	-259
Vrelišče	°C	-162	-253
Gostota plina (20 °C, 1 bar)	kg/m^3	0.65	0,0838
Gostota tekočine (pri 1 bar; vrelišče)	kg/m^3	422,8	70,8
Zgornja meja vnetljivosti v zraku	vol. %	15	75
Spodnja meja vnetljivosti v zraku	vol. %	5	4
Hitrost plamena	m/s	0,45	3
Temperatura plamenišča	°C	-183	-253
Min. energija vžiga	mJ	0,28	0,018
Barva plamena	-	svetleč	slabo viden
Spodnja/zgornja energetska vrednost	MJ/kg	50/55,5	120/142
UN GHS nevarnosti	-	H220, H230, H380	H220, H230
Povzroča krhkost	-	ne	da (kovine)

Opombe: [a] – običajno vsaj 95 %; [b] – odoriran v končni distribuciji.

Primerjavo lahko strnemo v naslednjih točkah:

- Vodik je plin brez barve ali vonja, ki se utekočini šele pri zelo nizki temperaturi. Njegova energetska vrednost pri gorenju je glede na težo skoraj trikrat večja od zemeljskega plina (velja tudi v primerjavi z bencinom ali dizelskim gorivom), toda ne smemo pozabiti da gre za plin. Plinasti vodik ima zelo nizko specifično gostoto, zato ga moramo hraniti bodisi v stisnjeni obliki (npr., jeklenke pri 700 bar) ali kot ohlajena (kriogena) tekočina pri -253 °C; tako se prostornina zmanjša za faktor približno 700.
- Vodik je vnetljiv (gori) v izjemno širokem območju v zmesi z zrakom, kar je primerjalno neugodneje v primerjavi z zemeljskim plinom, a ima še nižjo gostoto, zato se zaradi vzgona zelo hitro razredči.
- Vodik je zelo lahko vnetljiv (to je njegova bistvena nevarna lastnost), zadošča že bistveno nižja energija (vir vžiga). Posebnost je njegov plamen, ki skoraj ne sveti, zato ga je na svetlem težko opaziti. Hitrost plamena pri vodiku je veliko večja v primerjavi z zemeljskim plinom, kar pomeni da gorenje lažje preide v eksplozijo, ko so zato izpolnjeni pogoji (od tod tudi njegova sopomenka „pokalni plin“).
- Zemeljskemu plinu v končni distribuciji dodajajo minimalne količine odorantov (običajno žveplove spojine), da ga lažje zavohamo v primeru puščanja. Vodik je v vozilih (Kernc, 2020:68-75) običajno namenjen za proizvodnjo električne energije v t.i., gorivnih celicah, kjer pa odoriranje ni primerno, zato se ne more izvajati (potrebni so drugi ukrepi).



Iz navedenih pristopov in prepoznanih izzivov lahko povzamemo, da se je potrebno prehoda na vodikovo ekonomijo lotiti sistematično.

- Na začetku smo omenili da je vodik najlažji element. To je zato, ker ima najmanjšo molekulo. Ta lastnost ima posledico, da zelo lahko pronica skozi konstrukcijske materiale (predvsem pri višjih pritiskih in temperaturah), kar ima pomen tudi pri pojavu, ki se mu reče vodikova krhkost. Pri določenih kovinah (jeklo, baker, aluminij) lahko pride do prehajanja vodika v kovino, reakcijo s sestavinami zlitin, ter njihovo razslojevanje (nastanek razpok).

Iz zapisanega izhaja, da uvajanje uporabe vodika namesto klasičnih fosilnih goriv prinaša marsikatero tehnično in varnostno spremembo, predvsem tam, kjer do sedaj (še) ni izkušenj z njegovo uporabo (ogrevanje, uporaba v vozilih, ipd.). Tako prepoznani glavni izzivi in primerni pristopi k njihovemu upravljanju so:

Posebnost/izziv	**Pristop**
Ø Tekoči vodik kot kriogena (zelo hladna tekočina)	• Uporaba primernih materialov • Dobra toplotna izolacija rezervoarjev
Ø Komprimirani vodik (700 bar)	• Uporaba kompozitnih jeklenk
Ø Zaznavanje potencialnih puščanj	• Uporaba posebnih senzorjev za vodik
Ø Zelo široko območje vnetljivosti v zraku	• Skladiščenje na prostem, dobro zračenje prostorov, izpust zraka na vrhu prostora
Ø Eksplozivnost zmesi z zrakom	• kot zgoraj; • Izogibanje prostorski utesnjenosti opreme in objektov
Ø Slabo viden plamen	• IR senzorji plamena
Ø Vodikova krhkost	• Uporaba primernih materialov, nadzor

Ignoriranje posebnosti vodika lahko vodi do neljubih incidentov, nesreč, padca ugleda in motivacije za spremembe, ki jih bo težko spet spraviti v tek.

Iz navedenih pristopov in prepoznanih izzivov lahko povzamemo, da se je potrebno prehoda na vodikovo ekonomijo lotiti sistematično. Spremembe na ravni goriva, tehnologije, konstrukcijskih materialov in postopov k uporabi skoraj ne bi mogle biti obsežnejše. Takšen obseg tehničnih sprememb se bo logično navezoval tudi na potrebne organizacijske ukrepe v organizacijah, vsaj na ravni zagotavljanja potrebnih specifičnih kompetenc zaposlenih in pogodbenih izvajalcev (npr., potrebna izobrazba, specifična izobraževanja, certifikacije). No, da nismo čisto na začetku poti kažejo nekatera dejstva, kot so dosegljivi specifični standardi za industrijsko opremo, ter izobraževanih programi (glej priložen spisek literature).

Naj zaključim z mislijo, da je vsak začetek težak, a vsaka pot se začne s prvim korakom. Za uspešen, dovolj hiter prehod v vodikovo ekonomijo, bo potrebno zadovoljivo odgovoriti na obe že omenjeni težavi, a zavedajmo se, da nista edini. Ekonomski uspeh je odvisen od primerjave z drugimi alternativami (obnovljivi viri energije, npr., direktna uporaba biomase, električni avtomobili), a tudi ti so povezani z viri primarne energije, torej gre za konkurenčne poti npr., »od sonca do koles«. Vezano na vodikovo infrastrukturo se obeta sprememba od sedanje uporabe pretežno fosilnih goriv, na (najbolj verjetno) uporabo sonca, foto-celic in elektrolize vode, kjer bo to geografsko, ekonomsko in politično izvedljivo. Ne pozabimo tudi na potrebne varnostne prilagoditve v energetski infrastrukturi (plinovodi, prevoz tekočega vodika s tankerji, ipd.[2]), kot tudi spremembe navad pri uporabnikih. Nenazadnje bodo tu imele veliko vlogo vlade, oziroma zakonodaja, industrijska združenja in sektorske smernice & priporočila, ki bodo morale spremljati tehnološke spremembe v vlogi pospeševanja in spodbujanja prehoda. Ignoriranje posebnosti vodika lahko vodi do neljubih incidentov, nesreč, padca ugleda in motivacije za spremembe, ki jih bo težko spet spraviti v tek.

Literatura

- International Energy Agency, 2019. The Future of Hydrogen. https://webstore.iea.org/download/summary/2803?-fileName=English-Future-Hydrogen-ES.pdf
- Hydrogen Fuel Cell Engines and Related Technologies. Module 1: Hydrogen Properties. U.S. DOE. 2001, http://www.eere.energy.gov/hydrogenandfuelcells/tech_validation/pdfs/fcm01r0.pdf
- Vinko Kernc, *Vodik – avtomobilsko gorivo prihodnosti?* Življenje in Tehnika, št. 10, 2020. 68-75.
- ISO/TC197 Hydrogen technologies, spisek aktualnih 17 in 6 standardov v razvoju je dosegljiv na https://www.iso.org/committee/54560.html
- https://webstore.ansi.org/Standards/ASME/ASMESTPPT0172008
- https://h2tools.org/codes-standards
- Hydrogen Fuel Cell Engines and Related Technologies Course, https://www.energy.gov/eere/fuelcells/hydrogen-fuel-cell-engines-and-related-technologies-course
- Introduction to Hydrogen for Code Officials, https://www.hydrogen.energy.gov/code_official_training.html
- Hydrogen Safety Panel, https://h2tools.org/hsp

1 V vozilih je neposredna konkurenca skladiščenje električne energije v baterijah in uporaba elektromotorjev.

2 Primer je aktualni prehod na uporabo utekočinjenega zemeljskega plina kot čistega goriva v pomorstvu, glej EU projekt Super-LNG na https://superlng.adrioninterreg.eu/ ■

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



IZOBRAŽEVANJE V ELEKTRONSKI OBLIKI

Dinamika dela in aktivnosti se v zadnjem obdobju povečujejo, hkrati pa jih situacija s korona virusom dela še bolj kompleksne, ker smo zaposlene iz delovnih organizacij prestavili v domača okolja. To na drugi strani pomeni, da še težje dobimo vse zaposlene v realnem okolju na eno fizično lokacijo. Zato je bistveno, da organizacije pričnejo pospešeno razvijati možnosti e-izobraževanja zaposlenih na področju informacijske varnosti, kar bo omogočalo večplastne učinke in možnosti.

Danes lahko rečemo, da so skoraj vsi, ki uporabljajo računalnik, že zaključili ali se udeležili neke vrste e-izobraževanja. Morda se je imenovalo spletno usposabljanje, spletno učenje ali karkoli drugega, vendar imajo vsi skupini imenovalec e-izobraževanje. E-izobraževanje deluje z uporabo elektronskih naprav (računalniki, tablični računalniki, mobilni telefoni, idr.) za zagotavljanje izobraževalnih vsebin slušateljem. Mnogi si kot e-izobraževanje predstavljajo okolje, ki temelji na diapozitivih in vsebuje preproste krmilne gumbe (npr. naprej in nazaj), ter reševanje izpitnih vprašalnikov z možnostjo izbire poljubnega pred definiranega odgovora. Toda vsi programi e-izobraževanja nimajo istega koncepta. Na primer, lahko gre za sam po sebi odziven spletni tečaj, ki slušateljem omogoča odlično izobraževalno izkušnjo, ne glede na to, katero napravo uporabljajo za opravljanje izbranega izobraževanja. Lahko gre za programsko simulacijo ali pa interaktivni tečaj, ki vključuje igranje vlog in zapletenejše odločanje. E-izobraževanje poznamo v neskončno in nenehno razvijajočih se oblikah. Ima številne prednosti, ki jih tradicionalni načini usposabljanja ne omogočajo. E-izobraževanja so tradicionalno asinhrona, kar pomeni, da ni vnaprej določenega časa izobraževanja. Vsak lahko s svojim tempom napreduje skozi program usposabljanja kakor mu ustreza v danem časovnem intervalu. Vendar je v zadnjem času na voljo več sinhronega e-izobraževanja prek spletnih konferenc, ki imajo možnost interaktivnega sodelovanja ter uporabo klepetalnika in drugih načinov interakcije. Odlična stvar e-izobraževanj je ta, da se lahko poslužimo ene ali druge oblike, ali pa kar obeh. Prav tako ima tak način izobraževanja globalni doseg. Do njega lahko dostopajo ljudje po vsem svetu. Ni potrebe po dragih potovanjih ali sestankih v različnih časovnih pasovih. Podpirajo vse vrste elektronskih naprav. Delujejo tako na računalnikih kot tudi na mobilnih napravah, kot so pametni telefoni in tablični računalniki. To pomeni, da so e-izobraževanja na voljo ljudem kjerkoli in kadarkoli jih potrebujejo. Programska oprema za e-učenje je tako enostavna za uporabo, da lahko vsakdo v nekaj urah ustvari, objavi in deli tečaje, kar vam omogoča, da ljudem zagotovite vire ter usposabljanje, do katerega lahko dostopajo kadarkoli in od kjerkoli želijo. Med drugim tovrstna izobraževanja zmanjšajo stroške pri organizacijah, ki uporabljajo e-izobraževalne tečaje, s katerimi nadomeščajo nekatera tradicionalna izobraževanja, pod vodstvom usposobljenega kadra. To se je na račun trenutne situacije, ki jo preživljamo, zaradi novega korona virusa, izkazalo kot trenutno edini način izobraževanja, ki ga lahko izpeljemo na daljavo, ter s tem ne dopustimo zanemarjanja izobraževanja zaposlenih. E-izobraževanja omogočajo dosledno kakovost in vsebino v razvitih tečajih e-učenja. Razvoj tečajev se nenehno razvija. Avtorske aplikacije se bodo še naprej izboljševale, vendar se je potrebno osredotočiti na uporabo teh aplikacij za ustvarjanje najboljšega e-izobraževanja. V svoji razmeroma kratki zgodovini je e-izobraževanje precej napredovalo in ponuja neizmerne priložnosti, ki nam vsem skupaj pomagajo do boljšega učenja.



*avtor je član Slovenskega združenja korporativne varnosti



Zakaj je izobraževanje zaposlenih ključnega pomena?

- Izobražuje zaposlene o učinkoviti uporabi tehnologije,
- Zmanjšuje tehnične nezgode, ter spodbuja varnost in zdravje med zaposlenimi,
- Zagotavlja konkurenčno prednost na trgu,
- Ustvarja možnosti za karierni razvoj in osebno rast zaposlenih,
- Izobraževanje je neposredno povezano z boljšo produktivnostjo in prav tako povečuje učinkovitost zaposlenih in s tem produktivnost in donosnost,
- Izobraževanja oskrbujejo zaposlene z boljšim znanjem, ki jim pomaga na karierni poti,
- Usposobljeni zaposleni kažejo večjo motivacijo in se za delo bolje angažirajo.

Ljudje pogosto mislijo, da bo učenje preko spleta omejilo učenje, ker bodo morali vse prebrati. Pravzaprav pa je ravno nasprotno. S tako številnimi možnostmi za večpredstavnost je mogoče v spletno učenje vključiti različne bralne, slušne ter vadbene module. Te moduli sočasno omogočajo branje ali gledanje, poslušanje, demonstriranje, ter izvajanje vaj in izpolnjevanje testov. E-izobraževanje je prihodnost.

Kakšne so prednosti in slabosti e-izobraževanj?

Prednosti e-izobraževanja:
Med prednosti e-izobraževanja sigurno štejemo dejstvo, da ga lahko izvajate po delih, ki se prilega vašemu že tako zasedenemu urniku. V nasprotju s tradicionalnimi internimi šolanji nimate strukturiranega urnika, ki bi narekoval, kdaj lahko (morate) dostopate do vsebine e-izobraževanja. Spletno izobraževanje omogoča popolno prilagodljivost ter omogoča izobraževanje kjerkoli in kadarkoli. Z izjemo lastnega računalnika ali mobilne naprave ni drugih omembe vrednih stroškov. Namesto v zaprtih prostorih tradicionalne učilnice pa imate zdaj na voljo možnost prostega učenja kjerkoli želite. E-izobraževanje vam omogoča, da v celoti izkoristite svoj čas in opravite izobraževanje, ki ga običajno ne bi mogli. Prinaša bolj zanimiv način učenja, ki ponuja možnost globljega učnega pristopa in povezovanja. Ima več vizualnih elementov kot besedilnih. Pri e-izobraževanju ne obstaja en način, ki ustreza vsem, ampak obstaja možnost, ki ustreza željam vsakega.

> To se je na račun trenutne situacije, ki jo preživljamo, zaradi novega korona virusa, izkazalo kot trenutno edini način izobraževanja, ki ga lahko izpeljemo na daljavo, ter s tem ne dopustimo zanemarjanja izobraževanja zaposlenih.

Slabosti e-izobraževanja:
Včasih udeleženci e-izobraževanj, ki imajo nizko motivacijo, hitro zaostajajo pri spletnem izobraževanju. Brez določenega urnika ali rutine lahko e-učenje ljudem oteži doseganje zahtevanega rezultata v zahtevanem roku. Prav tako je pomembno, da se na začetku ali na tečaju predstavijo tehnološke zahteve



izobraževalne platforme, saj še vedno najdemo veliko število zastarelih računalnikov, z zastarelo programsko opremo, ki otežijo ali celo onemogočijo tekočo izvedbo e-izobraževanja. Tukaj je potrebno tudi izpostaviti internetno povezavo ter zanesljivost vira napajanja. Seveda ne gre zanemariti računalniškega znanja ter dejstva, da uporabi računalnikov starejši generaciji morda ni preveč naklonjena. Tudi če je programska oprema uporabniku prijazna, je za nekatere zastrašujoča naloga izvedba tovrstnega izobraževanja.

Varnost e-izobraževanj?

Okolje je enostavno tako dinamično, da se odkrivajo vedno nove grožnje s prihodom novih tehnologij. V obstoječih sistemih se odkrivajo nove ranljivosti. Varnost informacij je mogoče doseči z uporabo kriptografskih metod ter z uporabo ustreznih omrežnih protokolov. Ker je internet skozi katerega e-izobraževanja potekajo, tudi mesto napadalcev, so te platforme enako izpostavljene grožnjam, kot vse ostale omrežene naprave. Z namenom zagotavljanja razpoložljivosti, celovitosti ter integritete informacij in gradiv v virtualnih okoljih, je potrebno izvesti protiukrepe, kot so implementacija strojne in programske opreme varnostnih tehnologij.

Varnost je zelo pomembno vprašanje, ker e-izobraževanje narašča in vedno več ljudi obiskuje spletne tečaje. Upoštevati je potrebno veliko pomembnih elementov;
- Preverjanje pristnosti,
- Nadzor dostopa do platforme,
- Celovitost podatkov,
- Zaščita vsebine,
- Varen prenos podatkov,
- Nemoten dostop do platforme,
- In druge,..

Ker se dinamika dela povečuje, hkrati pa jo situacijo z korona virusom dela še bolj kompleksno, ker smo zaposlene iz delovnih organizacij prestavili v domača okolja, še težje dobimo vse zaposlene v realnem okolju na eno fizično lokacijo. Zato je bistveno, da organizacije pričnejo pospešeno razvijati možnosti e-izobraževanja zaposlenih na področju informacijske varnosti, ki bodo več plastni. Sistem usposabljanja in izobraževanja mora biti tako narejen, da se ob pojavi nove pomembne zadeve takoj obvesti vse uporabnike izobraževalne platforme. Npr. V primeru na novo odkrite grožnje ali v primeru napada, so zaposleni takoj obveščeni. Potem imamo tukaj tudi ciljno usposabljanje, ki ga moramo prestaviti v virtualno okolje. Ljudje se morajo še naprej izobraževati ter seznanjati z novostmi. Bistveno pa je, da se ta proces izvaja kontinuirano.

Dotakniti se moramo težave, ki jih imajo organizacije in to je primanjkljaj kadrovskih virov. Pravočasna in dosledna izobraževanja so ključnega pomena. Smiselno se je vprašati ali lahko zunanji sodelavec ponudi tovrstna izobraževanja v virtualnem okolju za določene organizacije? Menim, da ni smiselno znotraj vsake organizacije razvijati tovrstnih sistemov, temveč se je bolje poslužiti že obstoječih, dobro razvitih, preverjenih ter stabilnih sistemov in orodij.

Za konec naj še omenim, da tudi e-izobraževalne platforme niso imune na hekerske napada, saj so bile najrazličnejše izobraževalne platforme že tarče hekerskih napadov. Najpogostejše tehnike napada na izobraževalne platforme so sledeče; Pridobitev nedovoljenega in nepooblaščenega dostopa, cross-site request forgery, SQL injection, cross-site scripting, izguba podatkov, vsiljevanje ukazne vrstice, onemogočanje storitve, poskus prijave s surovo silo, uhajanje zaupnih konfiguracijskih informacij ter seveda različne tehnike socialnega inženiringa. ■



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

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

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

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

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

ICS

C|EH™ Certified Ethical Hacker

OFFENSIVE SECURITY OSCP

ISO 27001

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

BUREAU VERITAS 1828

DPO

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

Avtor: Marko Zavadlav / PRO.Astec d.o.o.



NADZORNI SVETI IN KIBERNETSKA VARNOST

Kibernetska tveganja so dejstvo. Nobena organizacija, ki je povezana v internet, ni imuna na kibernetske grožnje. Razviti mora uspešen in učinkovit sistem zagotavljanja kibernetske varnosti. Nadzorni sveti so tisti, ki morajo dajati prave usmeritve upravam, da lahko preprečijo oziroma se na ustrezen način odzovejo na kibernetske varnostne incidente.

V letu 2019 je ENISA (Evropska agencija za varnost omrežij) poročala, da se je v tem letu močno spremenil obseg kibernetskih napadov. Stalno povečevanje opažamo tudi v letošnjem letu. Kibernetske grožnje so najhitreje rastoče grožnje, ki grozijo organizacijam danes. Upravni odbori morajo najti način za naslavljanje le-teh. Tveganja, ki izhajajo preko kibernetskega prostora so relativno mlada, predvsem za tradicionalna podjetja, saj v preteklosti ni bilo tako velike stopnje digitalizacije in tako velike odvisnosti od informacijske tehnologije. Varovanje informacij je bilo in na žalost še vedno je v zaostanku z novimi kibernetskimi grožnjami, saj te neprestano izkoriščajo ranljivosti, ki jih organizacije pridelajo s pomanjkljivim upravljanjem informacijske varnosti.

Recept za Nadzorne svete sestoji iz petih načel pri naslavljanju kibernetskih groženj. Nadzorni sveti so odgovorni za varnostne incidente in stroške, ki nastajajo zaradi slabe varnostne politike. Pri tem morajo seveda ustrezno vplivati na uprave.

Uprave morajo sprejemati odločitve o naslavljanju informacijske varnosti na enak način, kot sprejemajo ostale strateške odločitve. Čeprav informacijska tehnologija ni ključni proizvod organizacije, pa je v moderni organizaciji en najpomembnejših, če ne najpomembnejši podporni dejavnik, ki omogoča poslovanje in bi bilo poslovanje brez njega onemogočeno.

- Načelo številka 1: uprave se morajo zavedati, da je kibernetska varnost del korporativnega upravljanja tveganj in ne osamljena naloga IT oddelkov.
- Načelo številka 2: uprave morajo razmisliti, kako kibernetska tveganja vplivajo na zakonske posledice, kakor tudi na ugled organizacije.
- Načelo številka 3: uprave morajo vpeljati poročanje s področja kibernetske varnosti, tako na nivoju vodstvenih poročil upravam kot tudi nadzornim svetom.
- Načelo številka 4: nadzorni sveti morajo zagotoviti, da uprave vzpostavijo celovit okvir za upravljanje kibernetskih varnostnih tveganj, ki vključujejo kulturo organizacije, zmožnosti preprečevanja, odkrivanja in odziva na zaznane kibernetske varnostne incidente, nadzor in komunikacijo na vseh nivojih. Skladno s sprejeto strategijo morajo zagotoviti zadostno količino ustreznih virov.
- Načelo številka 5: nadzorni sveti in uprave morajo med sabo razpravljati o kibernetskih tveganjih in vključevati načela za njihovo upravljanje (zmanjševanje, prenos ali sprejem določenih tveganj).

V Agenciji Evropske Unije za varnost omrežij in informacij (ENISA) so zapisali: »Organizacije si morajo prizadevati za aktivno udeležbo kot le zagotavljanje skladnosti pri naslavljanju hitro nastajajočih groženj. Uprave imajo ključno vlogo pri razvoju učinkovitega in uspešnega sistema kibernetske varnosti. Omogočiti morajo delo strokovnjakom, predvsem pa morajo voditi z zgledi. Ukrepi za izboljšanje korporativne kibernetske varnosti morajo biti stalni, interaktivni in podprti. Človeški faktor je in bo ostal glavni izvor ranljivosti, zato mora biti poseben poudarek na dvigovanju zavesti vseh posameznikov. Bodi zgled, obnašaj se skladno z varnostnimi politikami, saj si glavna tarča, sodeluj s strokovnjaki informacijske varnosti pri iskanju najučinkovitejših rešitev za zagotavljanje varnega poslovanja, morajo biti načela vsakega člana uprave.« Enako velja tudi za člane nadzornih svetov. Le z zgledom lahko dvigujemo zavest posameznikov »od zgoraj navzdol«.

V nadaljevanju pojasnjujemo našteta načela, ki jih nadzorni sveti morajo upoštevati pri upravljanju informacijske in kibernetske varnosti. Informacijska in kibernetska varnost nista tehnična izziva, ki sta prepuščena tehničnim oddelkom. Tehnični oddelki ne poznajo celotnega poslovanja in izzivov organizacije, zato se naslavljanje groženj s tehničnega vidika običajno ne nanaša na ključna poslovna tveganja, torej so viri razporejeni neučinkovito, poleg tega pa se lahko spregleda večje ranljivosti. Upravljanje tveganj informacijske varnosti mora biti vključeno v korporativno upravljanje tveganj in imeti enak nivo zavedanja, kot na primer strateška, finančna, okoljska ali tržna tveganja, da naštejemo le nekatera od njih. Nadzor nad tveganji mora vršiti uprava družbe, saj je odgovorna za ustrezno upravljanje le-teh. Ni dovolj, da pogledamo rešitve ostalih organizacij. Vsaka organizacija je posebna, zato potrebuje prilagojen pristop k upravljanju tveganj. Kar je za eno organizacijo veliko tveganje, pa naj bo zaradi ranljivosti ali zaradi morebitnih posledic, je lahko za drugo popolnoma nepomembno in je vsak vložek neracionalen. Uprave morajo razviti kulturo v podjetju, ki bo imela informacijsko varnost za vrednoto. Uprave morajo redno poročati nadzornim svetom in pri tem biti odkrite in ne prikrivati ranljivosti ali incidentov. Ravno tako morajo pri poročanju razmišljati o celotnem ekosistemu, ne le o njihovih domenah.

Kibernetska varnost ni samo stvar ugleda, ampak lahko nosi tudi zakonske posledice. Vedno več evropske in lokalne zakonodaje naslavlja vidike informacijske varnosti, zato zanemarjanje informacijske varnosti vodi k nezakonitim ravnanjem. Kot primer samo omenimo zakonodajo s področja varovanja osebnih podatkov ali varovanja poslovne skrivnosti. Nadzorni sveti morajo poznati vso zakonodajo, ki vpliva na delovanje sistema varovanja informacij organizacije, redno spremljati spremembe in zahtevati od uprav, da se odzivajo na njih.

Uprave morajo sprejemati odločitve o naslavljanju informacijske varnosti na enak način, kot sprejemajo ostale strateške odločitve. Čeprav informacijska tehnologija ni ključni proizvod organizacije, pa je v moderni organizaciji en najpomembnejših, če ne najpomembnejši podporni dejavnik, ki omogoča poslovanje in bi bilo poslovanje brez njega onemogočeno. Nadzorni sveti morajo jasno sporočiti pričakovanja in usmeritve, ki jih morajo uprave pri načrtovanju upoštevati. Običajno nadzorni sveti za upravljanje informacijske varnosti pooblastijo organ (Odbor za informacijsko varnost). S tem dosežejo, da se s področjem ukvarjajo običajno kompetentni ljudje. Ne glede na to, pa morajo nenehno spremljati delovanje odborov, kajti svojih odgovornosti ne morejo prenesti na tak način. Informacijska in kibernetska varnost nista in ne moreta biti ločeni zadevi, saj sta močno vključeni v vse aktivnosti v organizaciji, torej mora biti tudi razpravljanje o njih vključeno v vse aktivnosti organizacije. Uprave morajo zagotoviti vire za upravljanje informacijske varnosti. Hkrati morajo zagotoviti tehnične zmogljivosti, ki omogočajo nadzornim svetom nenehno spremljanje stanja tveganj in ukrepov, ki se nanašajo na informacijsko varnost. Razviti morajo jasen sistem odgovornosti in postopkov, jih spremljati in po potrebi posodabljati. Vsi postopki morajo biti sporočeni vsem, ki sodelujejo v njih. Omogočeno mora biti ustrezno ozaveščanje in usposabljanje za naloge, ki so zapisane v postopkih. Kibernetska varnost in odpornost mora biti zapisana v sam genetski zapis organizacije. Uprave morajo omogočiti zbiranje dogodkov, tveganj, groženj in ranljivosti po načelu »od spodaj navzgor«. Uprave in nadzorni sveti se ne bodo ukvarjali s posameznimi incidenti, ki ne povzročijo velike škode, vendar pa morajo biti obveščeni o celotnem stanju na primeren, strnjen način.

> Brez ustrezne ocene tveganja ne moremo upravljati informacijskih tveganj. Organizacija mora sprejeti metodologijo, ki omogoča želeno natančnost in ponovljivost. V oceno tveganja morajo biti vključeni vsi lastniki tveganj. Tveganja je potrebno oceniti, predlagati ustrezne ukrepe in spremljati njihovo uspešnost.

Poročanja se lahko združujejo na več načinov, ravno tako se lahko na več načinov združujejo usmeritve. Varnostna vprašanja lahko na primer združujejo po naslednjih področjih upravljanja IT:
- upravljanje virov,
- varnost naprav,
- upravljanje identitet in dostopa,
- varnost v omrežjih,
- varnost v programski opremi,
- politike in postopki,
- prepoznavanje groženj.

Seveda lahko glede na naravo dela, stopnjo zrelosti ali specifične dejavnike, organizacije izbirajo lastna področja delovanja in zagotavljanja informacijske varnosti. Nadzorni sveti morajo ocenjevati učinkovitost vložkov v informacijsko varnost (ROI). Preverjati morajo učinkovitost naložb po načelu bodočih izgub. Uporabiti morajo tako imenovani Risk-based pristop. Uprave in nadzorni sveti morajo imeti verodostojne podatke, ki se nanašajo na stroške zagotavljanja informacijske varnosti, ki jih morajo oceniti v luči tveganj in njihove morebitne realizacije. Ocena tveganj mora biti izvedena na način, ki lahko čim bolj natančno izračuna verjetnost in posledico uresničitve posamezne grožnje v določenem času. S tako pridobljeno oceno lahko uprave potrjujejo posamezne ukrepe in uveljavljajo lastni apetit po tveganju. Naj še enkrat spomnimo, če bi bile te odločitve prepuščene tehničnim oddelkom, potem bi prišlo v tem delu do velikega razkoraka.





Pri določanju apetita po tveganju naj organizacije odgovorijo na naslednja vprašanja:
- Vrednote organizacije – katera tveganja so absolutno nesprejemljiva?
- Strategija – katera tveganja želimo sprejeti ?
- Deležniki – katera tveganja so pripravljeni sprejeti ali prenesti nase in do kakšne mere?
- Zmogljivosti – Kateri viri so potrebni za upravljanje posameznih tveganj?
- Finance – ali smo sposobni natančno oceniti vrednost tveganj in jih uskladiti s predvidenimi vložki v njihovo upravljanje?
- Merjenje – ali smo sposobni uvesti ustrezno merjenje in poročanje, ki zagotavlja nadzor, spremlja trende in zagotavlja ustrezno komunikacijo med deležniki?

Brez ustrezne ocene tveganja ne moremo upravljati informacijskih tveganj. Organizacija mora sprejeti metodologijo, ki omogoča želeno natančnost in ponovljivost. V oceno tveganja morajo biti vključeni vsi lastniki tveganj. Tveganja je potrebno oceniti, predlagati ustrezne ukrepe in spremljati njihovo uspešnost. Nadzorni sveti morajo imeti sprotne in pravilne podatke, uprave jim morajo te podatke zagotoviti. Obstajajo različni načini in orodja, ki jih nadzorni sveti pri tem lahko uporabijo. Delimo jih lahko na 5 orodij:
- Vprašanja, ki jih uprave postavijo nadzornemu svetu (ali pa si jih člani nadzornih svetov sami postavijo in odgovarjajo na njih); s tem se pokaže poznavanje nadzornega sveta o IKT infrastrukturi in zrelosti organizacije glede informacijske varnosti. Hkrati lahko nadzorni svet vidi, katere podatke sploh zahteva od uprav
- Vprašanja, ki jih nadzorni sveti postavijo upravam; s tem nadzorni svet oceni zrelost organizacije, sistem upravljanja varovanja informacij, lahko oceni natančnost in verodostojnost informacij, ki jih prejme od uprav.
- Metrike, ki jih spremlja nadzorni svet; metrike, ki se merijo in poročajo, morajo biti natančno opredeljene in dajati podatke, ki so uporabni za odločanje. Metrika, kot je na primer število zaznanih incidentov, nam ne pove praktično ničesar.
- Zahteve informacijske varnosti pri prevzemih in združevanjih; v modernem ekonomskem okolju so prodaje, nakupi, prevzemi in združitve nenehno prisotni. Ali se nadzorni sveti znajo ustrezno pripraviti in oceniti informacijska tveganja pri teh aktivnostih? Znano je načelo, da pri grožnjah in ranljivostih 1 + 1 ni 2, ampak več.
- Skladnost s standardi; ali organizacija pri upravljanju tveganj in informacijske varnosti upošteva načela katerega od standardov, kot npr. ISO/IEC 27001? Ali je organizacija certificirana po katerem od standardov?

Kibernetska tveganja so dejstvo. Nobena organizacija, ki je povezana v internet, ni imuna na kibernetske grožnje. Razviti mora uspešen in učinkovit sistem zagotavljanja kibernetske varnosti. Nadzorni sveti so tisti, ki morajo dajati prave usmeritve upravam, da lahko preprečijo oziroma se na ustrezen način odzovejo na kibernetske varnostne incidente. Samo sistem, ki deluje z vrha navzdol, je pri naslavljanju kibernetske varnosti lahko uspešen in učinkovit. Ne delujmo po principu »imamo varnostne politike, vsi se jih moramo držati, seveda pa se jih meni, ker sem uprava, ni treba.« ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*



REPORTAŽA:

MEDNARODNA KONFERENCA DNEVI KORPORATIVNE VARNOSTI 2020

11. mednarodna konferenca „Dnevi korporativne varnosti“ je tokrat zaradi razmer, ki so v Sloveniji in svetu, potekala v dveh ločenih dogodkih. Svečana otvoritev in podelitev letnih nagrad Slovenian Grand Security Awards se je odvila v živo, 9. septembra, sam vsebinski del pa je potekal 21. in 22. septembra v obliki on-line konference preko spletne platforme.

Mednarodna konferenca Dnevi korporativne varnosti 2020, ki jo organizirajo Inštitut za korporativne varnostne študije, Slovensko združenje korporativne varnosti in regijsko združenje SE Europe Corporate Security Association, je potekala v nenavadnih razmerah, saj je letošnje leto v vseh pogledih posebno leto. Konferenca bi se morala po prvotnem načrtu odviti v mesecu marcu. Žal je bila zaradi izrednih razmer, ki jih je prinesel COVID-19, dva dni pred dogodkom odpovedana in prestavljena. V čakanju na ugodne epidemiološke razmere, se je le ta večkrat prestavila. Luč na koncu predora pa je ugledala v hibridni izvedbi v mesecu septembru. Svečana otvoritev, s podelitvijo letnih nagrad Slovenian Grand Security Award, se je odvila 9. septembra v živo. Na tem dogodku, ki je bil organiziran v sicer strogih okvirjih Nacionalnega inštituta za javno zdravje (NIJZ), je sodelovalo kar nekaj vidnih odločevalcev iz javnega in korporativnega okolja.

Otvoritveno slovesnost so s svojimi nagovori odprli dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti, g. Alojz Kovšca, predsednik Državnega sveta Republike Slovenije, mag. Matej Tonin, minister za obrambo RS, g. Jože Senica, namestnik generalnega direktorja Policije in predstavnik ge-







*avtor je član Slovenskega združenja korporativne varnosti







neralnega sponzorja, g. Aleksander Mervar, direktor Elektro Slovenije (ELES).

Po svečani podelitvi nagrad Slovenian Grand Security Award, o kateri smo v tej reviji že pisali (več o nagrajencih v junijski številki), sta se odvili dve okrogli mizi, ki ju je moderiral dr. Denis Čaleta, predsednik sveta ICS Ljubljana in predsednik Slovenskega združenja korporativne varnosti. Na prvi okrogli mizi se je pogovarjal z letošnjimi prejemniki prestižne nagrade. Na tej so sodelovali g. Andrej Maslo iz Pošte Slovenije, g. Matjaž Beričič iz Telekoma Slovenije, župan občine Tržič, g. Borut Sajovic, županja Mestne občine Ptuj, ga. Nuška Gajšek, ga. Jasmina Mešič iz ustanove SI-CERT in urednik časnika Finance, g. Borut Hočevar.

Na drugi okrogli mizi pa so dobili besedo vidni gostje iz gospodarskega okolja. Na njej so sodelovali direktor ELES-a mag. Aleksander Mervar, predsednik uprave DARS-a, mag. Valentin Hajdinjak, član uprave Telekoma Slovenije, mag. Matjaž Beričič in direktor kontrole zračnega prometa Slovenije, dr. Franc Željko Županič. Tema okrogle mize je odprla poglede strateškega managementa na informacijska tveganja, ter s tem povezane izzive za varno in učinkovito poslovanje v organizacijah.

Celoten dvourni dogodek je bil posnet in predvajan 21. septembra ob otvoritvi on-line konference.

Vsebinski dogodek se je izvedel 21. in 22. septembra v on-line obliki in sicer preko spletne platforme. Konferenca je ponudila vrsto odličnih predavanj priznanih gostov iz Slovenije in tujine in dodatno še dve vsebinsko zelo bogati okrogli mizi. On-line oblika je omogočila, da je bila konferenca spremljana v širšem mednarodnem prostoru, saj je bilo letos na dogodku zastopano občinstvo in predavatelji kar iz 15 držav.

Letošnja rdeča nit konference je bila zagotovo povezana z zaščito kritične infrastrukture v povezavi s kibernetsko varnostjo. Naj omenimo nekaj predavanj, ki so se navezovala na to področje.

Spoznali smo lahko, kakšno vlogo pri zaščiti kritične infrastrukture ima kibernetska varnost in kaj lahko prinese dober operativni center. Ravno tako je lahko celovito upravljanje tveganj pomemben dejavnik zaščite kritične infrastrukture, ter učinkovito načrtovanje in izbira ustreznih produktov.

Konferenca se je dotaknila izziva, ki ga prinaša tehnologija 5G pri zaščiti kritične infrastrukture, ni pa pozabila na požarno varnost, ki je pomemben člen pri načrtovanju neprekinjenega poslovanja. Pogledali pa smo tudi, kaj se lahko naučimo iz primerov groženj korporativni varnosti v mednarodnem okolju. Naj omenimo močno mednarodno zasedbo predavateljev. Predstavljen je bil zelo odmeven primer kibernetskega vdora v energetski sistem Ukrajine, ki se je zgodil v bližnji preteklosti in je lahko vzorčni primer ranljivosti kritične infrastrukture.

Na konferenci smo imeli priložnost slišati tri predavanja vezana na izsledke evropskih projektov, ki potekajo pod okriljem Evropske komisije in so financirani v okviru programa Horizon 2020. Tako smo lahko spoznali glavne tehnološke in procesne poudarke projekta Defender (Defending the European Energy Infrastructures), kateri se je ravno uspešno zaključil. Predstavil jih je dr. Gabriele Guinta, koordinator projekta iz Italije. Druga dva predavanja pa sta bila vezana na projekt













InfraStress, v katerem sodeluje 28 različnih partnerjev in je trenutno ravno na polovici. Dr. Jovanović iz Nemčije je predstavil področje vezano na oceno odpornosti kritične infrastrukture in njenih glavnih funkcij, ter pristope, ki jih je projekt ubral v ta namen. Drugo predavanje iz tega projekta, pa je predstavil gost iz Grčije, g. Syngelakis, in sicer izzive kibernetske varnosti v okolju grške kritične infrastrukture. Naj omenimo, da ima v obeh projektih vidno vlogo tudi Institut za korporativne varnostne študije.

V nadaljevanju ni manjkalo niti vsebin s področja prava in varstva osebnih podatkov. Predstavnik informacijskega pooblaščenca nam je še enkrat osvetlil, kdaj je upravljavec podatkov obvezan narediti oceno učinka v zvezi z varstvom podatkov (DPIA). Slišali smo, s katerimi pravnimi odgovornostmi se lahko srečamo pri uvajanju novih tehnologij v varnostne sisteme organizacij. V tej luči naj omenimo še dva predavanja, ki sta osvetlila prihod novih tehnologij kot so uporaba umetne inteligence za obvladovanje groženj v industrijskih okoljih in pomoč umetne inteligence pri varovanju elektronske pošte.

Dr. Bertoncelj, vidni predstavnik Slovenskega združenja korporativne varnosti, je predstavil najbolj izpostavljene varnostne izzive, ki smo jim bili priča v tem letu in nekatere, ki nas čakajo v bližnji prihodnosti.

Na koncu vsebinskega dela smo prisostvovali dvema okroglima mizama. Na prvi so udeleženci osvetlili izzive na poti dokončne uveljavitve zahtev Zakona o informacijski varnosti in EU NIS direktive. Vsebina te razprave je razgrnila izzive na poti dokončnega vzpostavljanja sistema kibernetske varnosti v Republiki Sloveniji. Na drugi okrogli mizi, pa se je moderator pogovarjal s korporativno varnostnimi managerji in strokovnjaki za upravljanje tveganj. Pogovor je bil usmerjen v poenotenje postopkov ocenjevanja tveganj v kritični infrastrukturi in pri izvajalcih bistvenih storitev.

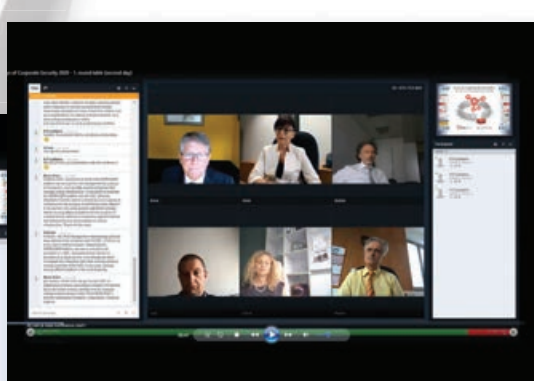
Seveda ne gre pozabiti na sponzorje konference brez katerih takega dogodka ni mogoče izpeljati. Ti so nam skozi različne kanale in oblike predstavili najnovejše produkte na tehnološkem in procesnem delu, ki bodo v prihodnosti lahko v pomoč pri učinkovitem obvladovanju tveganj na področju korporativne varnosti s posebnim poudarkom na kibernetski varnosti.

V zaključku se je dr. Denis Čaleta vsem, ki so bili del tega odličnega dogodka, še enkrat iskreno zahvalil. Konferenca je, kljub oteževalnim okoliščinam, ponovno potrdila ugled najpomembnejšega dogodka v regiji. Hkrati je pozval vse udeležence na naslednjo mednarodno konferenco Dnevi korporativne varnosti, ki se bo predvidoma odvila 25. in 26. maja 2021.

Za konec naj pohvalimo ekipo Instituta za korporativne varnostne študije za odlično organiziran hibridni dogodek, ki je pokazala, da se kljub trenutni situaciji, tak dogodek lahko izvede na ustrezno visokem nivoju, tako v odnosu do udeležencev, kot pokroviteljev. Celoten dogodek je v posnetku dosegljiv na spletnih straneh Instituta za korporativne varnostne študije in na YouTube kanalu (ICS Ljubljana). ■







12. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 25. - 26. MAJ 2021



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