Korporativna varnost

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

Letnik 2020, junij • št. 23



Razglašeni nagrajenci »Slovenian Grand Security Award«

Pomen delovanja kritične infrastrukture v obdobju kriznih razmer

mag. Matej Tonin, minister za obrambo Republike Slovenije



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



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
JUNIJ 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.

Obdobje razglašene svetovne pandemije COVID-19 je pred nas postavilo pomembne izzive, ki so bili v prvi vrsti prvenstveno varnostni in zdravstveni, v nadaljevanju pa je omenjeno obdobje izpostavilo celo vrsto dejavnikov, ki imajo in bodo tudi v bližnji prihodnosti imeli pomembne učinke na normalno funkcioniranje moderne družbene skupnosti. Tudi v Sloveniji se tem vplivom nismo mogli izogniti, zato je prav, da sedaj poskušamo na preteklo obdobje pogledati s potrebno stopnjo distance, analizirati naše ukrepe za zagotavljanje neprekinjenega delovanja družbe in zagotavljanja varnosti njenih pripadnikov, ter se poskušati še bolje pripraviti na prihodnje izzive, ki jih prinaša obdobje življenja s tveganji okužbe s koronavirusom. Vsekakor pa smo v preteklem obdobju spoznali, da je zagotavljanje neprekinjenosti delovanja kritične infrastrukture nujno za ustrezno delovanje naše družbe. Tiste priprave in procese, ki smo jih zamudili, ali jih nismo opravili v času normalnega delovanja družbe, je težko nadomestiti v kriznih časih, ko je pritisk različnih negativnih dejavnikov še toliko večji in zahtevnejši. Spoznanje, da smo v preteklosti zanemarjali ključni človeški potencial, še posebej na kritičnih procesih, je vsekakor pomemben del izkušenj, ki jih moramo začeti takoj ustrezno upravljati. Ponovno pa se je pokazalo tudi polno pozitivnih lastnosti različnih strokovnjakov, ki so s svojim učinkovitim delovanjem in iznajdljivostjo reševali še tako zahtevne situacije. Veseli nas, da so se v tem delu še posebej izkazali tisti deli naših organizacij, ki so zadolženi za korporativno varnost. Vsaka kriza je lahko tudi priložnost za iskanje novih pristopov, kako še bolj učinkovito zagotavljati neprekinjenost in robustnost delovanja naših organizacij.

Tokratno številko revije Korporativna varnost namenjamo obdobju epidemije, izkušenj, ki smo jih potegnili iz analiz našega delovanja in izzivom, ki nas v bližnji prihodnosti čakajo, da bomo delovanje družbene skupnosti vrnili v normalne tirnice. 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 nagrajencem, ki so v posameznih kategorijah prejeli nagrado Slovenian Grand Security Award in s svojim ravnanjem oz. aktivnostmi predstavljajo zgled za ostalo strokovno javnost. Revija pa prinaša tudi druge odlične in strokovno informativne teme, ki bodo strokovnjakom različnih profilov pomagale pri širitvi njihovega strokovnega razumevanja varnostnega okolja in procesov, ki stojijo pred njimi.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
g. Blaž Košorok, državni sekretar na Ministrstvu za infrastrukturo

V ČASU KRIZE SMO USPELI ZAGOTOVITI NEPREKINJENO DELOVANJE KRITIČNE INFRASTRUKTURE

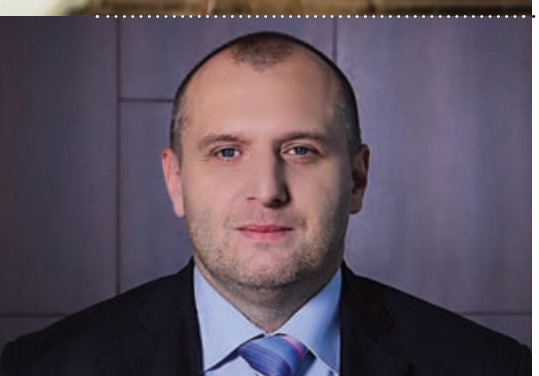
14



POMEMBNOST UPRAVLJANJA KLJUČNIH ČLOVEŠKIH VIROV V ČASU KRIZE

V tokratnem članku se bomo dotaknili pomembnosti ustreznega pristopa k upravljanju človeških virov za zagotavljanje neprekinjenosti delovanja kritične infrastrukture (KI) in izvajanja bistvenih storitev (IBS) v času aktualne krize, ki je nastala zaradi izbruha koronavirusa SARS Cov-2 in posledično bolezni COVID-19.

19



INTERVJU
Dr. Jurij Klančnik, direktor Področja za obratovanje, ELES d.o.o.

ELES IN NJEGOVA VLOGA PRI NEPREKINJENOSTI DELOVANJA ELEKTROENERGETSKEGA SISTEMA

25



VARNOST OSEBNIH PODATKOV V BITKI S COVID-19

S pojavom koronavirusa COVID-19 smo se znašli v krizni situaciji, ki je zahtevala takojšnje ukrepanje in razne tehnološke rešitve so se pokazale kot ena izmed možnosti. V tem kontekstu so že v začetni fazi obvladovanja epidemije vzniknile ideje o aplikacijah in storitvah za omejevanje širjenja okužb s COVID-19, ki bi temeljile na obdelavi podatkov.

33



DELOVANJE KRITIČNE INFRASTRUKTURE V ČASU EPIDEMIJE – PRIMER UKC LJUBLJANA

Univerzitetni klinični center Ljubljana (UKCL) je osrednja zdravstvena ustanova v Republiki Sloveniji. UKCL predstavlja kritično infrastrukturo saj je ključnega pomena za državo, tudi s področja obrambe, zaščite in reševanja.

43

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
mag. Matej Tonin, minister za obrambo Republike Slovenije

POMEN DELOVANJA KRITIČNE INFRASTRUKTURE V OBDOBJU KRIZNIH RAZMER

Pogovarjali smo se z ministrom za obrambo, mag. Matejem Toninom, o pomenu sprejetja ustrezne zakonodaje s področja kritične infrastrukture in ukrepih, ki jih bo, na podlagi zahtev zahtevnega varnostnega okolja, potrebno izpeljati na tem področju.

Počasi prehajamo v obdobje po epidemiji COVID-19, ki bo s stališča zagotavljanja neprekinjenega delovanja kritične infrastrukture ravno tako pomembno. Kako lahko s strateškega nivoja ocenite učinkovitost odzivanja upravljavcev kritične infrastrukture na nastalo situacijo?

Ob prevzemu funkcije ministra za obrambo sem se skupaj s sodelavci z vso odgovornostjo in polno angažiranostjo soočil z razmerami ob epidemiji COVID-19 ter izvajanjem ukrepov za zajezitev širjenja okužbe in blažitev posledic epidemije. S tem v zvezi je bil pripravljen tudi pregled stanja na področju kritične infrastrukture.

Ocenim lahko, da so upravljavci kritične infrastrukture Republike Slovenije z izvedenimi ukrepi, zaščito zaposlenih in preudarnim razporejanjem ključnega kadra zagotavljali neprekinjeno delovanje. To je najbolj pomembno. V prvi vrsti so nudili podporo zdravstvenemu sektorju, pa tudi vsem drugim zmogljivostim, ki opravljajo ključne funkcije za državo in družbo. Pri tem je največjo težavo predstavljalo pomanjkanje zaščitnih sredstev, predvsem ustreznih mask, rokavic in razkužil. Zagotovitev slednjih je bila naša prva skrb. Izvedeni ukrepi upravljavcev kritične infrastrukture glede zaščite zaposlenih pred širjenjem okužbe so bili učinkoviti. Nimam informacij, da bi težave upravljavcev zaradi izolacije ali celo obolelosti zaposlenih imele za posledico oteženo opravljanje njihove dejavnosti.

> Potem, ko so upravljavci kritične infrastrukture zaključili z izdelavo dokumentov načrtovanja zaščite kritične infrastrukture in nanje tudi pridobili soglasje pristojnih nosilcev sektorjev kritične infrastrukture, je zdaj čas, da se ukrepi različnih sektorjev medsebojno uskladijo.

Na ministrstvu za obrambo smo pristojnim ministrstvom, kot nosilcem sektorjev kritične infrastrukture, posredovali priporočila in predloge ukrepov za odzivanje v proučitev ter za čas postopnega ponovnega zagona posameznih dejavnosti. Predvsem je bilo pomembno zagotoviti nadaljnje neprekinjeno izvajanje storitev. Verjamem, da smo se v času soočanja z epidemijo veliko naučili ter pridobili veliko novih izkušenj in spoznanj, ki nam bodo vsem, predvsem pa upravljavcem in nosilcem sektorjev, koristile pri nadaljnjem načrtovanju učinkovite zaščite kritične infrastrukture.

Kako v prihodnje zagotoviti, da bodo upravljavci kritične infrastrukture, s strani države v kriznih razmerah, deležni večje podpore za izvajanje tistih procesov, ki so nujno potrebni za nemoteno delovanje družbe. Lahko ocenimo, da tukaj obstajajo še pomembne rezerve v organizaciji, ki bi zagotovile boljše delovanje državnih funkcij na tem področju?

*avtor je član Slovenskega združenja korporativne varnosti



Ministrstvo za obrambo in pristojna ministrstva, kot nosilci sektorjev kritične infrastrukture, upravljavcem redno podajajo usmeritve ter jim nudijo strokovno pomoč pri izvajanju nalog, ki izhajajo iz Zakona o kritični infrastrukturi.

za obrambo lani izvedlo usposabljanje za zaščito kritične infrastrukture za vse akterje na tem področju. Podobna usposabljanja in tudi vaje nameravamo organizirati tudi v prihodnje. Hkrati načrtujemo tudi vključitev vseh upravljavcev kritične infrastrukture in nosilcev sektorjev v Informacijsko-sporočilni sistem Nacionalnega centra za krizno upravljanje. Ta vključitev jim bo omogočala varno izmenjavo podatkov, informacij ter medsebojno delitev izkušenj in dobrih praks. Seveda bo tudi olajšala postopek obveščanja v primeru izrednih dogodkov ali prekinitve delovanja kritične infrastrukture.

Pričakujem, da bi se v primeru izrednih dogodkov in krize na področju kritične infrastrukture, ko bi se glede na razmere pokazale potrebe po dodatnih ukrepih – podobno kot je bilo to v primeru soočanja z epidemijo COVID-19 – iskalo rešitve, ne samo v okviru posameznega sektorja kritične infrastrukture, pač pa v vseh medsebojno odvisnih sektorjih in na ravni vlade. Upravljavci bodo v takih situacijah deležni podpore in iskanja rešitve za blaženje posledic prekinitve delovanja oziroma za zagotovitev čimprejšnjega ponovnega nemotenega delovanja. Ti ukrepi, prilagojeni obstoječim razmeram, bodo na primer prednostno zagotavljanje goriva, električne energije in omrežnih priključnih točk, sproščanje državnih blagovnih rezerv, podpora s finančnimi sredstvi - tudi s sredstvi Evropske unije, zagotovitev materialnih sredstev in opreme, zagotovitev zaščitnih sredstev, okrepitev varovanja, prerazporeditev oziroma zagotovitev dodatnega kadra ter vzpostavitev nadomestnih elektronskih povezav.

Strokovna javnost ves čas opozarja, da se pojavljajo težave na posameznih področjih sektorskih koordinatorjev v resornih ministrstvih, katerim zakon prinaša pomembne pristojnosti usklajevanja zaščite kritične infrastrukture v posameznih sektorjih. Kaj bi bilo po vašem mnenju potrebno narediti, da bi na ta odgovorna mesta prišli ustrezno usposobljeni strokovnjaki?

Ministrstvo za obrambo, ki usmerja in usklajuje dejavnosti na področju kritične infrastrukture, ni prejelo takih opozoril, kot jih navajate v vašem vprašanju. Menim pa, da se morajo nosilci sektorjev kritične infrastrukture in upravljavci kritične infrastrukture nenehno prilagajati, izobraževati in usposabljati, že zaradi pojavljanja vedno novih tveganj in groženj ter njihove kompleksnosti. Slednje lahko pomembno prispeva k učinkoviti zaščiti kritične infrastrukture, krepitvi njene odpornosti, prepoznavanju in upravljanju groženj, usklajenemu odzivu v primeru izrednih dogodkov ter hitrejši vzpostavitvi njenega ponovnega nemotenega delovanja po takšnih dogodkih.

Ocenjujem, da se na Ministrstvu za obrambo daje ustrezna pozornost usposabljanju na področju kritične infrastrukture. V pristojnosti posameznih ministrstev pa je, da za izvajanje nalog na področju dejavnosti sektorja kritične infrastrukture imenujejo izkušene, strokovne in kompetentne javne uslužbence. Ministrstva so namreč skladno z Zakonom o kritični infrastrukturi odgovorna za stanje v »svojem« sektorju kritične infrastrukture z vidika njegove zaščite.

Kako v prihodnje vidite vlogo Ministrstva za obrambo, kot ministrstva, ki koordinativno usklajuje ukrepe na

področju zaščite kritične infrastrukture? Kje bodo tisti poudarki nadaljnjega razvoja tega področja, tudi v luči izkušenj, ki jih je prineslo obdobje epidemije COVID-19?

Ključen izziv, ki je pred nami, je uskladitev ukrepov za zaščito kritične infrastrukture med sektorji kritične infrastrukture. Potem, ko so upravljavci kritične infrastrukture zaključili z izdelavo dokumentov načrtovanja zaščite kritične infrastrukture in nanje tudi pridobili soglasje pristojnih nosilcev sektorjev kritične infrastrukture, je zdaj čas, da se ukrepi različnih sektorjev medsebojno uskladijo. V skladu z načelom celovitega pristopa k zaščiti kritične infrastrukture se bomo osredotočili na medsebojno odvisnost sektorjev kritične infrastrukture. V določeni meri bomo povratno informacijo dobili tudi prek Inšpektorata Republike Slovenije za obrambo, po izvedenih inšpekcijskih nadzorih.

Glede na pridobljene izkušnje v času epidemije COVID-19 bi v prihodnjem obdobju veljalo opraviti ponovno presojo določenih kriterijev za ugotavljanje kritične infrastrukture državnega pomena, na tej podlagi pa tudi postopek ugotavljanja potencialne kritične infrastrukture Republike Slovenije.

Menite, da je v prihodnje potrebno procese zaščite kritične infrastrukture in nacionalnega sistema kriznega upravljanja še tesneje povezati?

V Republiki Sloveniji je v kriznih razmerah vsako ministrstvo odgovorno za izvajanje nalog na svojem področju, glavni organ za usklajevanje kriznega odziva v državi pa je vlada. Upravljavci kritične infrastrukture se na izredne dogodke in krizo po Zakonu o kritični infrastrukturi odzivajo z izvajanjem načrtovanih ukrepov za zaščito, ki jih stopnjujejo skladno z razmerami. Če stalni ukrepi, tudi če so stopnjevani, ne zadostujejo, lahko upravljavci in po potrebi tudi nosilci sektorjev kritične infrastrukture sprejmejo dodatne ukrepe. Ko gre za ukrepe, ki presegajo pristojnost posameznega nosilca sektorja kritične infrastrukture, lahko dodatne ukrepe na njihov predlog sprejme tudi vlada. Svojo vlogo ima tudi Nacionalni center za krizno upravljanje, ki v takih razmerah nudi podporo v skladu s svojimi pristojnostmi.

Menim, da sta, kljub določeni stopnji različnosti oziroma njuni precejšnji strokovni posebnosti področji kritične infrastrukture in krizno upravljanje na nacionalni ravni povezana procesa. Ko je to potrebno, omogočata spremljanje aktivnosti ter morebitnih težav in kriz na področju kritične infrastrukture tudi z vključevanjem teles kriznega upravljanja.

Pomembno se mi zdi določilo Zakona o kritični infrastrukturi, ki nosilcem sektorjev kritične infrastrukture nalaga obveznost, da pri pripravi ali dopolnjevanju predpisov s področja sektorja iz svoje pristojnosti, upoštevajo tudi vidik zaščite kritične infrastrukture.

Kako bomo v prihodnje zagotovili, da procesi v ministrstvih ne bodo tako močno silosno usmerjeni? Trenutno se nam še vedno prevečkrat pojavlja, da vsako resorno ministrstvo ureja svoj zakon ni pa potrebnega medsebojnega sodelovanja? Tveganja so namreč danes tako kompleksna, da posamezen del države nikakor ne more avtonomno obvladati zahtevnih situacij.

Dejstvo je, da je zaradi značilnosti, ki jih ima vsak posamezni sektor, zelo težko urediti vsa področja delovanja v enem samem zakonu.

V Zakonu o kritični infrastrukturi so, po moji oceni, v največji možni meri opredeljene naloge in obveznosti, ki so skupne vsem nosilcem sektorjev oziroma upravljavcem kritične infrastrukture, ne glede na njihova različna področja dela. Na podlagi navedenega zakona upravljavci kritične infrastrukture v dokumentih načrtovanja zaščite kritične infrastrukture združujejo različne ocene tveganj, ukrepe za zaščito, rešitve in načrte, ki jih načrtujejo na podlagi področnih sektorskih predpisov in aktov ter svojih poslovnih odločitev, standardov in priporočil mednarodnih organizacij in združenj, aktov institucij Evropske unije, in predvsem navedenega zakona. S tem sledijo tudi določilu zakona, da se upoštevajo že uveljavljene rešitve in postopki, ki izhajajo iz druge zakonodaje. Temu je bila pri pripravi zakona dana posebna pozornost, z namenom, da ne bi prihajalo do podvajanj nalog in administrativnega dela.

Pomembno se mi zdi določilo Zakona o kritični infrastrukturi, ki nosilcem sektorjev kritične infrastrukture nalaga obveznost, da pri pripravi ali dopolnjevanju predpisov s področja sektorja iz svoje pristojnosti, upoštevajo tudi vidik zaščite kritične infrastrukture. Pri normativnem urejanju posameznih sektorjev kritične infrastrukture je, v luči zaščite kritične infrastrukture in tudi drugih medresorskih vsebin, ključno povezovanje določil in medresorsko usklajevanje vsebinsko sicer različnih predpisov.

Kako lahko Ministrstvo za obrambo preko Inšpektorata za obrambo Republike Slovenije zagotovi, da se bodo predpisani akti učinkovito implementirani v praksi? Je lahko učinkovit nadzor eno od orodij države za povečanje učinkovitosti ukrepov zaščite kritične infrastrukture?

Inšpektorat RS za obrambo izvaja nadzor nad izvajanjem določb Zakona o kritični infrastrukturi in aktov, izdanih na njegovi podlagi. Primarna naloga inšpektorata na področju kritične infrastrukture je in bo usmerjena v preverjanje izvajanja nalog, ki jih imajo nosilci sektorjev kritične infrastrukture, torej ministrstva, in lastniki ali upravljalci kritične infrastrukture po Zakonu o kritični infrastrukturi.

Učinkovit inšpekcijski nadzor na področju kritične infrastrukture bo pripomogel k premostitvi razlike med želenim in obstoječim, torej k spoštovanju določil predpisov s področja kritične infrastrukture pri zavezancih nadzora. Hkrati pa bo s povratnimi informacijami prispeval k morebitnemu učinkovitejšemu oblikovanju zaščite kritične infrastrukture v državi.

Potrebno pa se je zavedati, da gre pri načrtovanju zaščite kritične infrastrukture in njenem upravljanju za izrazito kompleksno in soodvisno dejavnost različnih sektorjev in upravljavcev. Zato učinkovita zaščita kritične infrastrukture ne bo mogoča brez tvornega medresorskega sodelovanja, vključno s sodelovanjem med različnimi inšpekcijskimi službami v državi. Sodelovanje različnih inšpektoratov pri izvajanju nadzora kritične infrastrukture bo prispevalo ne le k celovitosti pregleda o dejanski pripravljenosti nosilcev in upravljavcev kritične infrastrukture za delovanje v različnih kriznih stanjih oziroma varnostnih raz-



merah, ampak tudi k razumevanju zavedanja o soodvisnosti njihove dejavnosti v različnih kriznih stanjih oziroma v vseh varnostnih razmerah. Le tako bo mogoče zagotoviti načrtovanje in upravljanje kritične infrastrukture po načelih celovitega pristopa, neposredne odgovornosti, zaščite pred različnimi vrstami nevarnosti, stalnega načrtovanja, podprtega s stalnim procesom ocenjevanja tveganj za zaščito kritične infrastrukture, ter izmenjave podatkov in informacij.

Kaj bi bilo po vašem mnenju potrebno narediti, da bo razumevanje pomena javno-zasebnega partnerstva na področju zaščite kritične infrastrukture prešlo na višji novo?

Zakon o kritični infrastrukturi je vzpostavil temeljno podlago, tako za boljše razumevanje pomena javno-zasebnega partnerstva, kot za samo vzpostavitev partnerskih razmerij. Načelo izmenjave podatkov in informacij ter varovanja podatkov zahteva od vseh pristojnih organov in organizacij medsebojno zaupanje. Potreba po medsebojnem sodelovanju se je pokazala še zlasti v času soočanja s pandemijo COVID-19. Verjamem, da se bo slednje krepilo na vseh ravneh. Pomen javno-zasebnega partnerstva se kaže tudi v odzivanju na aktivnosti Evropske komisije, ki vsebine v zvezi s krepitvijo zaščite kritične infrastrukture v Evropski uniji preko Ministrstva za obrambo, ki je kontaktna točka za zaščito evropske kritične infrastrukture v Sloveniji, vedno pogosteje naslavlja tudi na nacionalne upravljavce ter jih vključuje v delavnice in razprave. Predstavniki slednjih, med drugim tudi zasebniki, se redno odzivajo.

Kaj bi bilo za konec vaše sporočilo za prihodnost učinkovitega obvladovanja tveganj s katerimi se srečuje Republika Slovenija?

Pojavljanje novih tveganj in groženj vseh vrst nam vsem narekuje njihovo ocenjevanje in vrednotenje. Ocenjevanje že znanih in novih tveganj je in mora biti stalen proces, prav tako presojanje ustreznosti že načrtovanih ukrepov za zaščito in njihova nadgradnja. Pričakujem, da bodo po pridobljenih izkušnjah ob epidemiji COVID-19 nosilci sektorjev kritične infrastrukture upravljavcem podali usmeritve za dopolnitev njihovih že izdelanih ocen tveganj. Prav tako pričakujem, da bodo upravljalci dopolnili svoje ocene ter nadgradili obstoječe ukrepe oziroma oblikovali nove, tudi v smislu potrebnih sprememb v organizaciji in razporejanju kadrovskih in materialnih virov, za zagotavljanje neprekinjenega delovanja. V procesih upravljanja tveganj se je treba osredotočiti ne zgolj na konkreten sektor in medsebojno odvisnost sektorjev kritične infrastrukture, pač pa upoštevati tudi vpliv posledic morebitnega nedelovanja posameznega sektorja kritične infrastrukture na druga področja države in družbe. Prepričan sem, da bo na tem področju Evropska unija podala nekatere rešitve, tudi izhajajoč iz izkušenj pandemije COVID-19. ■

Pojavljanje novih tveganj in groženj vseh vrst nam vsem narekuje njihovo ocenjevanje in vrednotenje. Ocenjevanje že znanih in novih tveganj je in mora biti stalen proces, prav tako presojanje ustreznosti že načrtovanih ukrepov za zaščito in njihova nadgradnja.

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



KOLUMNA

KAJ SMO SE IZ EPIDEMIOLOŠKE KRIZE NAUČILI?

Ob krizah in družbenih pretresih, ki smo jim bili piča skozi zgodovino človeštva, se vedno vprašamo ali smo se iz tega kaj novega naučili. Ob umirjanju epidemiološke slike v Sloveniji, in tudi v mednarodnem okolju, je čas za izvajanje analiz o preteklih dogodkih in ukrepih. Optimalno stanje bi bilo, da se iz preteklosti nekaj naučimo, odpravimo napake in izboljšamo stanje, ter tako zagotovimo, da bodo ključni družbeni in poslovni procesi v prihodnje bolj pripravljeni in dovolj robustni za zagotavljanje neprekinjenosti delovanja ključnih segmentov družbe tudi v prihajajočih krizah.

Za poglobljene ocene bo čas šele prišel, vendar lahko že sedaj ocenimo nekaj ključnih dejavnikov, ki jih je izpostavila trajajoča svetovna pandemija koronavirusa. Glavna ugotovitev je vsekakor, da je človek še vedno ključni del vsakega delujoče sistema. Kljub obsežnemu uvajanju novih tehnoloških rešitev, kot so umetna inteligenca in druge na informacijskih rešitvah temelječe tehnologije, človek še vedno predstavlja najpomembnejši del tega sistema. Torej je kadrovski potencial, še posebej na tistih delovnih mestih, ki so pomembna za to, da določeni ključni procesi neprekinjeno delujejo, izredno pomemben. V preteklosti temu ni bilo namenjeno dovolj pozornosti in je bilo večino virov usmerjenih v nadgradnjo tehnoloških rešitev, pozabljalo pa se je na zagotavljanje neprekinjenosti delovanja in zamenljivost ključnih kadrov v naših organizacijah. V preteklosti so se določeni muzali ob strokovnih razpravah, da je kadrovski potencial ravno tako potrebno umestiti v kategorijo kritične infrastrukture. Na tem mestu ne bi želel odpirati terminoloških izzivov ali je lahko človek kritična infrastruktura. Želim le poudariti pomen človeškega potenciala za neprekinjeno delovanje družbe. V omenjeni krizi smo imeli srečo, da je obseg okužb in tudi smrtnih primerov ostal omejen. To je pomenilo tudi, da so bile težave, ki bi lahko nastale zaradi okužb in smrti med ključnimi kadrovskimi viri, obvladljive. Zamislite si situacijo, ko bi nam v hujši eskalaciji razmer zmanjkalo ustreznih kadrov na ključnih področjih, kot je neprekinjeno zagotavljanje elektrike, vode, upravljanja zračnega prometa, da o ključnih kadrih v zdravstvu sploh ne govorim. Torej prva ključna ugotovitev je vsekakor povezana z dejstvom, da bo potrebno v prihodnosti na področjih ključnih kadrov narediti veliko več, kot se je izvajalo do sedaj. Seveda je potrebno z aktivnostmi začeti takoj, saj je za izgradnjo ključnih kadrovskih zmogljivosti potrebno daljše časovno obdobje.

Glavna ugotovitev je vsekakor, da je človek še vedno ključni del vsakega delujoče sistema. Kljub obsežnemu uvajanju novih tehnoloških rešitev, kot so umetna inteligenca in druge na informacijskih rešitvah temelječe tehnologije, človek še vedno predstavlja najpomembnejši del tega sistema.

Naslednja pomembna ugotovitev, ki smo jo lahko zaznali v odzivanju in učinkovitosti organizacij, še posebno tistih, ki upravljajo kritično infrastrukturo in bistvene storitve, je bila povezana s procesi korporativne varnosti. Tiste organizacije, ki so v preteklem obdobju korporativni varnosti v svojih poslovnih procesih namenile dovolj pozornosti in jo ustrezno umestile v svoje delovanje, so v času krize bolj učinkovito in hitreje zagotavljale varnost in neprekinjenost svojega delovanja. Službe za korporativno varnost so v vseh večjih pomembnejših sistemih prevzele ključno vlogo koordinacije zagotavljanja neprekinjenosti delovanja organizacije. V tem je bilo še posebej izpostavljeno zagotavljanje varnosti vseh zaposlenih, spoštovanje usmeritev za preprečevanje širjenje

*avtor je član Slovenskega združenja korporativne varnosti

Neprekinjeno poslovanje organizacije ni odvisno samo od lastnih resursov, temveč tudi od celotne verige tistih partnerjev in zunanjih izvajalcev, ki smo jim v preteklosti prepustili pomembne procese in kateri imajo velik vpliv za naše delovanje.

okužbe COVID-19, uporabe zaščitnih sredstev in kar je tudi zelo pomembno zagotavljanje vzpostavitve varnih komunikacij za delo od doma.

Pomen sodelovanja korporativne varnosti z ostalimi segmenti v organizaciji, pri zagotavljanju obvladovanja tveganj in neprekinjenosti poslovanja, je v tem obdobju dobil še dodaten pomen. To pomeni, da je za učinkovito poslovanje bilo potrebno preseči vsakdanje birokratske ovire in navidezne ograje, ki so jih posamezniki ustvarjali okoli svojih pristojnosti v sami organizaciji. Praksa v kriznih situacijah v ospredje postavi osebe, ki so dovolj prožne in sposobne hitrega odzivanja in sprejemanja pravih na potrebe situacije temelječih odločitvah. Ali so v poslovnih organizacijah strokovni kadri s področja korporativne varnosti izkoristili to priložnost za uveljavljanje svojega ugleda in prepoznavnosti, bo zelo hitro pokazal čas. Še posebej bo tej kritični presoji dojemanja pomena posameznih procesov izpostavljeno obdobje po epidemiji, ko se bodo organizacije soočile z nujno potrebnimi novimi pristopi za povrnitev v normalno stanje delovanja. Trditev, da kriza predstavlja tudi priložnost je za strokovnjake s področja korporativne varnosti v tem kontekstu še kako na mestu.

Naslednja ugotovitev povezana z učinkovitim odzivanjem na stanje krize je usmerjena v načrtovanje neprekinjenega poslovanja. V preteklosti je velika večina organizacij načrtovanja neprekinjenega poslovanja dojemala kot birokratsko komponento, kjer je bilo važno, da v organizaciji obstaja načrt. Ni bilo pa resnih analiz in preverjanj, ali je to načrtovanje realno, in predvsem, ali to načrtovanje omogoča organizaciji lažji prehod iz normalnega stanja v stanje krize in zagotavljanje neprekinjenega delovanja ključnih procesov organizacije. Neprekinjeno poslovanje organizacije ni odvisno samo od lastnih resursov, temveč tudi od celotne verige tistih partnerjev in zunanjih izvajalcev, ki smo jim v preteklosti prepustili pomembne procese in kateri imajo velik vpliv za naše delovanje. To pomeni, da moramo v prihodnosti proces zagotavljanja neprekinjenega delovanja gledati mnogo širše in temu, skupaj s ključnimi partnerji, namenjati veliko več pozornosti, kot do sedaj. V naslednji krizi ne bomo imeli toliko sreče, kot v tej odhajajoči. Naše organizacije pa so preveč pomembne, da bi se z njihovim preživetjem igrali kot z igrami na srečo.





Ugotovitve vezane na javno zasebno sodelovanje, predvsem pa na vlogo države v kriznem odzivanju niso tako vzpodbudne. V določenih delih imamo procese kriznega odzivanja v državi še vedno zelo razdrobljene, birokratski postopki dušijo momente, kjer so potrebne hitre odločitve in odzivanje. Tisti organi, ki so namenjeni kriznemu odzivanju in kriznemu upravljanju, so v zadnji krizi odigrali obrobno vlogo in kar je s stališča zagotavljanja neprekinjenosti delovanja kritične infrastrukture zelo pomembo, upravljalci so bili v večini primerov odvisni od svoje iznajdljivosti, kako zagotavljati zaščitna sredstva za zaposlene na ključnih funkcijah, ki so morali neprekinjeno opravljati svoje delo. Vse ključne strateške organizacije v državi bodo v prihodnje morale biti sposobne bolj podrobno analizirati trende v mednarodnem varnostnem okolju in dovolj kmalu strateške odločevalce opremljati z informacijami, ki bodo omogočale predhodne priprave na krizo in manjši obseg presenečenj v katerih se je znašla država. V luči epidemije novo nastalega virusa, pa je bil razgaljen tudi celoten zdravstveni sistem, kjer lahko najdemo mnogo pozitivnih stvari, ki nas navdajajo z zaupanjem v javni sistem slovenskega zdravstva, ne smemo pa prezreti tudi veliko negativnih stvari, ki jih je potrebno v čim krajšem času odpraviti. Tudi v državni upravi se je ponovno izpostavil pomen človeškega potenciala, kjer je razumevajoči, strokoven in odgovoren posameznik lahko s svojim delovanjem opravil odlično delo, ki je močno pomagalo ostalim organizacijam pri zagotavljanju neprekinjenosti delovanja. Imamo pa tudi veliko primerov birokratskega pristopa, ki je v danem trenutku s popolnoma neživljenjskimi zahtevami in rešitvami ohromil in spravil v nevarnost delovanje pomembnih procesov za funkcioniranje družbe. Tej kritični analizi bi veljalo posvetiti več energije in v prihodnje tudi v državni upravi uveljaviti selekcijski postopek za osebe na ključnih delovnih mestih, ki ne bo temeljil samo na birokratskih temeljih, temveč na realni oceni sposobnosti kandidatov.

> Tiste organizacije, ki so v preteklem obdobju korporativni varnosti v svojih poslovnih procesih namenile dovolj pozornosti in jo ustrezno umestile v svoje delovanje, so v času krize bolj učinkovito in hitreje zagotavljale varnost in neprekinjenost svojega delovanja.

Za konec je potrebno razumeti tudi spremembe, ki jih je v naše okolje prinesla spremenjena dinamika dela naših organizacij in nove oblike poslovanja, ki smo jih bili primorani uveljaviti zaradi zagotavljanja neprekinjenosti delovanja naših organizacij. Določene oblike dela, kot so delo od doma in koordinacija določenih procesov z uporabo informacijske in komunikacijske tehnologije, so vsekakor pozitivni moment teh kriznih časov, ki jih bo treba ohraniti tudi v prihodnje. Tako bomo zagotovili, da se bodo procesi racionalizirali in v določenem delu tudi pospešili. Nikakor pa ne smemo spregledati nekaj novih groženj in ranljivosti naših organizacijskih sistemov, ki jim bomo v bližnji prihodnosti morali nameniti dovolj veliko pozornosti, da ne bomo spet negativno presenečeni. ■

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.

ICS

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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

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

ZDRUŽENJE KORPORATIVNE VARNOSTI · CER CENTER ENERGETSKO UČINKOVITIH REŠITEV · T2 · sij skupina · HSI HARDWARE SOFTWARE INOVATIONS

CETIS · ELES · NZS NOGOMETNA ZVEZA SLOVENIJE · elektro gorenjska · ISKRATEL

hse Holding Slovenske elektrarne d.o.o. · AKOS AGENCIJA ZA KOMUNIKACIJSKA OMREŽJA IN STORITVE REPUBLIKE SLOVENIJE · LUKA KOPER Port of Koper · lek član skupine Sandoz

REISSWOLF secret. service. · A1 · BTC · MARIBORSKI VODOVOD · KONTROLA ZRAČNEGA PROMETA SLOVENIJE · PHILIP MORRIS LJUBLJANA D.O.O.

univerzitetni klinični center ljubljana · GASILSKA ZVEZA SLOVENIJE · si-cert · INFORMACIJSKI POOBLAŠČENEC

www.ics-institut.si

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

Članstvo v združenju vam lahko olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

Mestna občina Ljubljana

Občina Slovenska Bistrica

NIJZ Nacionalni inštitut za javno zdravje

Pošta Slovenije

as

tuš

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
g. Blaž Košorok,
državni sekretar na Ministrstvu za infrastrukturo

V ČASU KRIZE SMO USPELI ZAGOTOVITI NEPREKINJENO DELOVANJE KRITIČNE INFRASTRUKTURE

G. Blaž Košorok, državni sekretar na Ministrstvu za infrastrukturo je v pogovoru z nami analiziral stanje in ukrepe na področju ključnih infrastrukturnih sektorjev v Republiki Sloveniji. V pogovoru je posebno težišče namenil tudi ukrepom, ki jih bo v prihodnosti potrebno narediti za povečanje razumevanja vloge varnosti pri upravljanju kritične infrastrukture.

Ministrstvo za infrastrukturo je resorno ministrstvo za dva ključna sektorja in sicer za energetiko in transport. V okviru teh dveh sektorjev so umeščene vse ključne infrastrukturne zmogljivosti, ki predstavljajo tudi kritično infrastrukturo in izvajalce bistvenih storitev Republike Slovenije. Kako bi preliminarno ocenili ustreznost robustnosti teh organizacij za izvajanje neprekinjenega delovanja?

Tak preizkus je bil zagotovo trenutna situacija s krizo COVID-19, energetika se je pokazala kot zelo močna in odporna, neprekinjeno delovanje pa ni bilo ogroženo niti v enem trenutku. Tako Eles pri prenosu energije, kot v distribuciji in proizvodnji električne energije ni bilo zaznati nobenih pomembnejših težav. Ravno tako je brezhibno delovalo v sektorju oskrbe s plinom, ki je tudi eden od energetskih stebrov. Ekipa na Ministrstvu za infrastrukturo ter zavedanje o področjih, ki obvladujejo kritično infrastrukturo in ukrepi pred sprejetjem izrednih razmer, so bili ustrezni in učinkoviti. Poskrbljeno je bilo za zaposlene v kritični infrastrukturi (KI) in za nemoteno delovanje sistema. Lahko rečem, da so bila podjetja oz. organizacije, ki obvladujejo KI na področju energetike, na prihod krize zelo dobro pripravljena. Izkazala so pravo mero pripravljenosti, prožnosti in odpornosti.

Potrebovali bomo tudi predloge s področja učinkovite zaščite KI. V teh projektih pa naj zasebni sektor pride z dobrimi idejami in na ministrstvu bomo imeli posluh za tovrstne pobude.

Podobno je bilo na področju transporta. Kljub bojazni, da bo primanjkovalo osnovnih dobrin v trgovinah, se to ni zgodilo. Kljub ustavitvi javnega potniškega prometa in ustavitvi letalskega prometa, je ostali tovorni promet potekal normalno. Lahko rečem, da smo bili na tem področju dobro pripravljeni, so pa seveda možnosti za izboljšave.

Seveda je bil v tokratni krizi predvsem na udaru kadrovski potencial, kar predstavlja samo en pomemben vidik zagotavljanja neprekinjenega delovanja, drugi vidik, ki bi ga posebej želel izpostaviti je področje kibernetske varnosti, kjer vidim možnosti za izboljšave. V bodoče bo potrebno temu področju posvečati še več pozornosti, še posebej na področju energetike, ki je eden od stebrov nacionalne varnosti.

*avtor je član Slovenskega združenja korporativne varnosti



Trenutna kriza COVID-19 je pred nas ponovno postavila ugotovitev, da so zaposleni v organizacijah, ki upravljajo s kritičnimi procesi države, izrednega pomena. Kaj lahko ministrstvo za infrastrukturo, poleg razvoja infrastrukture, stori tudi na področju razvoja kritičnih kadrov, kot pomembnega dela kritične infrastrukture?

To je naloga izobraževalnega sistema in inštitutov, kot je vaš, ki mora širiti pomen takih zaposlitev. Kaj si predstavlja povprečni slovenski manager pod kratico CSO (Chief Security Officer) ali CISO (Chief Security Informational Officer)? Kdo je korporativno varnostni manager, ali mora imeti tehnična znanja, IT znanja? Seveda se področja močno prepletajo. Naj omenim primer iz Luke Koper, ko je prišla v pristanišče ameriška vojaška ladja, so po naših informacijah zabeležili povprečno 4 kibernetske napade na dan. To pomeni, da živimo v zahtevnem varnostnem okolju in temu so podvržene tudi naše organizacije, ki upravljajo KI. Seveda je zelo pomembno, da imamo v organizacijah nekoga, ki je zadolžen za korporativno in posledično tudi kibernetsko varnost. V tujini je to le nekoliko drugače, vem da vi, ki ste v stroki, na to že vrsto let opozarjate in osveščate deležnike v slovenskem okolju.

Kdaj se zavemo neke dobrine, kot je varnost? Takrat, ko se nam nekaj zgodi, vendar je takrat največkrat že prepozno. Druga pomembna stvar pa je potreba po sistemskem pristopu, saj nam veliki vložki na področju obvladovanja tveganj ne bodo veliko pomagali, če jih ne uvajamo sistematično tam, kjer so nujno potrebni. V nasprotnem primeru se nam lahko hitro zgodi, da so resursi uporabljeni na nepravi način.

Če pogledamo nekoliko širše, kritični kadri so na vseh tistih procesih, kot je zagotavljanje neprekinjenega poslovanja elektro energetskega sistema. Ravno ti tehnični specialisti so problematični, ker jih verjetno ni dovolj, da bi v primeru nekega večjega izrednega dogodka imeli zamenjave v smislu zagotavljanja neprekinjenosti.

Trenutna krizna situacija je pokazala, da si marsikatera organizacija, vsaj v sektorju energetike, želi biti del KI. Pa se sprašujem, ali vsak, ki bi to želel, izpolnjuje kriterije za umestitev v KI?

V okolju KI je pomembno, da managerji prepoznajo pomembnost kritičnega kadra, da so nekateri procesi ključni (npr. operaterji dispečerskem centru), specifika znanja, leta šolanja in spoznavanja specifičnega delovnega okolja, so kadri, ki jih moramo znati identificirati, kdo so in dodatno vlagati v njihovo izobrazbo oziroma najti za njih ustrezno zamenjavo v takih izrednih razmerah.

Kako v prihodnosti, pri umeščanju novih ključnih infrastrukturnih objektov, upoštevati tudi vse zahteve, ki jih pred neprekinjeno delovanje države postavlja kompleksno varnostno okolje? Menite, da bi vključevanje varnostnih dejavnikov v fazo načrtovanja in-

Brez izmenjave dobrih praks, sodelovanjem z Evropsko unijo, sodelovanjem z mednarodnimi deležniki, se bojim, da bomo stopicali na mestu. V tej luči ponujamo na ministrstvu pomoč, kjer koli lahko pomagamo in smo vedno na voljo.

frastrukture lahko izboljšalo kvaliteto in robustnost te infrastrukture?

Predvsem z enotnim ali usklajenim delovanjem v fazi načrtovanja. Pri nas nimamo izgrajenega sistema »top to down«. Vsak poskuša urejati zadeve parcialno, nimamo pa organa ali institucije, ki bi lahko poskrbela za povezanost. Primer varnostno operativnega centra v energetiki, kdo bi lahko to izvajal? Kdo je tisti prvi med enakimi, ki bi zaradi procesne umeščenosti lahko tak center zagotavljal tudi za vse ostale, kdo ima nadzor nad celotnim delovanjem? Pred časom smo se na to temo pogovarjali in dali nalogo direktorju ELES-a, da naredijo projektno nalogo in poskušajo poiskati odgovore kako poenotiti proces, kjer bi se ključne varnostne informacije zbirale na enem mestu, kakor tudi koordinacija odzivanja na tveganja in grožnje v celotnem energetskem sistemu. Kar se tiče tega področja, sem optimist.

Kakšni so načrti v naslednjem obdobju vezano na izdelavo potrebnih normativnih predpisov, ki bodo sistemske ukrepe na področju neprekinjenosti delovanja infrastrukture postavili na višji nivo?

Management mora prepoznati, kaj je nujno potrebno. Vsake življenjske situacije s predpisi ne moremo urediti. V Sloveniji imamo že sedaj problem, da smo prenormirani. Potrebno je pravilno razumeti vsebino ali namen nekega zakonodajnega akta, naj bo to zakon, uredba ali odlok. Poudaril bi, da je potrebno prepoznati pomen varnosti in to potrebo znati razbrati iz zakona. Težko je v naprej predvideti, pred katerimi konkretnimi grožnjami se je treba varovati. Potrebno je razumeti pomen celovite varnosti naših ključnih organizacij, pa naj bo to v sektorju energetike ali prometa.

To zavedanje bi hitro prišlo v prakso tudi pri managementu, če bi le ta odgovarjal za ne sprejemanje določenih procesov ali ukrepov. Kdaj? Takrat, ko do škodnega dogodka pride. Dobrina je v tem primeru varnost in potrebna je primerna zaščita. Primer pri mamagementu je, da ko nastane neka posledica, management odide, ne ogovarja za nastalo škodo, posledice slabega upravljanja, pa ostanejo v podjetju.

Naloga takega instituta, kot je vaš in vaše revije je, da na take stvari opozarja.

Za usklajevanje tako pomembnega procesa, kot je neprekinjeno delovanje infrastrukture, bo verjetno potrebno zagotoviti dodatne kadrovske vire. Menite, da boste us-



peli znotraj ministrstva temu področju, kot pomembni sektorski koordinatorji, dati večjo težo, ki bo podprta z ustreznimi kadrovskimi viri?

To bomo dosegli ravno in samo v sodelovanju s pristojnimi institucijami. Mislim, da znamo identificirati, kaj je KI, ampak ali imamo ustrezne strokovnjake, ki bi nam pomagali udejanjiti tisto, kar smo predpisali, je drugo vprašanje. Se pa bojim, da brez sodelovanja s stroko in na drugi strani s ključnimi deležniki, tistimi, ki bodo morali vpeljati oz. udejanjiti zadeve v praksi, ne bo šlo. Zato bi si želeli k izvajanju tega projekta čim prej pristopiti in zbrati široko strokovno podporo. Samo taka projektna zgodba, kjer neposredno sodelujejo tako neposredni upravljalci KI v posameznem sektorju kakor tudi sektorski koordinatorji, lahko pripelje do nekih rešitev. V nasprotnem se spet lahko postavimo v vlogo odredbodajalca in ne poznavajoč dejansko stanje v praksi, poskušamo odrejati določene ukrepe. Tega si ne želimo saj ne prinaša ustreznih rezultatov. Tu vidim koristno izmenjavo informacij npr. z Institutom za korporativne varnostne študije ali tistimi, ki to v praksi izvajajo in imajo ustrezno znanje in informacije.

Kaj bi bilo po vašem mnenju potrebno narediti, da bo razumevanje pomena javno-zasebnega partnerstva na področju zaščite kritične infrastrukture prišlo na višji nivo?

Nova finančna perspektiva in Evropska kohezijska politika bosta v projekciji 2021 -27 v sektorju za varnost predvidela kar nekaj sredstev za to področje. Ključno pa je, da se pripravijo ustrezni projekti. Tu je del, ki odpade na zasebni sektor, ki lahko na nek način vzpodbudi državo, ki ima za to področje resurse, da se državi pomaga pripraviti vsebino določenih razpisov. Iniciativa naj bo tu na zasebnem partnerju, ker lahko le ti iz vsakodnevnega življenja, iz operative identificirajo, kaj bi bil možen projekt, ki bi imel smisel in potrebo za kvalitetnejšo zaščito KI. Mi na ministrstvu trenutno vemo, kaj je energetska učinkovitost, obnovljivi viri energije, trajnostna mobilnost in podobni pomembni procesi. Potrebovali bomo tudi predloge s področja učinkovite zaščite KI. V teh projektih pa naj zasebni sektor pride z dobrimi idejami in na ministrstvu bomo imeli posluh za tovrstne pobude.

Kakšno stališče imate na Ministrstvu za infrastrukturo vezano na sodelovanje v različnih evropskih projektih s področja obvladovanja tveganj in zagotavljanja neprekinjenosti delovanja? Menite, da lahko skozi take projekte pridemo do nujno potrebnih novih znanj, ki bodo našo pripravljenost v infrastrukturnih organizacijah postavilo na višji novo?

Na ministrstvu bomo take projekte maksimalno podpirali, oziroma še več, jih spodbujali.

Poznam dobro vaš projekt DEFENDER, ki ga ICS pelje skupaj z ELES-om in Institutom Jožef Stefan in je, kot vem, trenutno v zaključni fazi. Brez izmenjave dobrih praks, sodelovanjem z Evropsko unijo, sodelovanjem z mednarodnimi deležniki, se bojim, da bomo stopicali na mestu. V tej luči ponujamo na ministrstvu pomoč, kjer koli lahko pomagamo in smo vedno na voljo.

Večina upravljalcev pomembne infrastrukture je združena v Slovenskem združenju korporativne varnosti. Menite, da bi lahko Ministrstvo za infrastrukturo s formalnim vstopom v tako obliko združevanja napravilo pomemben korak k tesnejšim povezavam in približevanju procesov neposredne izmenjave dobrih praks in izkušenj na področju obvladovanja tveganj za neprekinjeno delovanje infrastrukture?



Ne vidim nobenih zadržkov, da bi se, kot Ministrstvo za infrastrukturo, povezali v tako združenje, ali v neki vlogi patronata prevzemali kakšne vidnejše vloge. S tem bi lahko dali jasen signal, kako pomembno je področje korporativne varnosti.

Zagotovo. Ministrstvo za infrastrukturo pokriva izredno široko področje, tako imamo področje cestnega, železniškega, letalskega prometa, energetiko, imamo področje prometne politike. Ne vidim nobenih zadržkov, da bi se, kot Ministrstvo za infrastrukturo, povezali v tako združenje, ali v neki vlogi patronata prevzemali kakšne vidnejše vloge. S tem bi lahko dali jasen signal, kako pomembno je področje korporativne varnosti. ■

Vsa vaša tveganja
na enem mestu

UPRAVLJANJE TVEGANJ

UPRAVLJANJE ŠKODNIH DOGODKOV

SVETOVANJE



Silver Bullet Risk je vodilno podjetje na področju celovitega upravljanja in obvladovanja tveganj v Sloveniji.

Izkoriščamo moč znanja, izkušenj in tehnologije, da lahko podjetjem in organizacijam ponudimo najcelovitejši nabor storitev s področja upravljanja tveganj na enem mestu. V zadnjih nekaj letih je našo programsko opremo in svetovalne storitve uporabilo več kot 100 največjih podjetij v Sloveniji.

sbr

info@silverbulletrisk.com
www.silverbulletrisk.com

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



POMEMBNOST UPRAVLJANJA KLJUČNIH ČLOVEŠKIH VIROV V ČASU KRIZE

V tokratnem članku se bomo dotaknili pomembnosti ustreznega pristopa k upravljanju človeških virov za zagotavljanje neprekinjenosti delovanja kritične infrastrukture (KI) in izvajanja bistvenih storitev (IBS) v času aktualne krize, ki je nastala zaradi izbruha koronavirusa SARS Cov-2 in posledično bolezni COVID-19. V času epidemije in pandemije in tudi po tem, je upravljanje človeških virov strateško vprašanje za državne institucije, gospodarske in druge družbe, še posebej pa za upravljavce kritične infrastrukture.

Uvodna misel

Sedanja kriza - zaradi svoje specifike in intenzivnosti širitve - predstavlja še toliko večji izziv tako za državo, posameznika, kot tudi za organizacije in družbo kot celoto. Čas v katerem živimo, je potemtakem čas velikih preizkušenj in treznega premisleka. Ni bilo veliko podobnih obdobij v razvoju človeške zgodovine, ko je bilo zaradi takšnih ali drugačnih razlogov zdravstvenim, ekonomskim, finančnim, socialnim, političnim in drugim tveganjem izpostavljeno praktično celotno človeštvo in celoten svet. V tem kontekstu in ob spoznanju, da je pri upravljanju in obvladovanju aktualne krize, še vedno veliko neznank, se med drugim kaže tudi potreba po upravljanju človeških virov, ki zagotavljajo neprekinjeno delovanje in poslovanje KI in IBS.

Vrste kriz in njihov vpliv na organizacije

Krize in krizne situacije se lahko pojavljajo v različnih oblikah. Vsak posameznik, skupina, organizacija ali pa družba se lahko s krizo sooča različno široko in globoko. Ob vsakem pojavu krize ali krizne situacije so v prvi vrsti na preizkušnji človeški odnosi in njegov odnos oziroma odziv na krizo ali krizno situacijo. Ko govorimo na splošno o krizah se soočamo s prepletom več vrst kriz, med katerimi bi posebej izpostavil predvsem tiste vrste kriz, ki imajo širši vpliv na ljudi in okolje in povzročajo dolgoročnejše posledice na stanje in nadaljnji razvoj človeka kot posameznika, in družbe kot celote. V mislih imam predvsem naslednje vrste kriz: pandemija, epidemija, naravne katastrofe, globalne gospodarske in finančne krize, globalne humanitarne in politične krize. Pri omenjenih krizah gre predvsem za zunanje dejavnike/povzročitelje, na katere se morajo upravljavci KI in IBS ter vodstva drugih organizacij, načrtno odzivati v smeri obvladovanja lastne ranljivosti ter zunanje ogroženosti in tveganja. Gre torej za ključne instrumente odzivanja kot so ocena ranljivosti, ogroženosti in tveganj (OROT), krizni načrt, načrt neprekinjenega poslovanja in načrt kriznega komuniciranja.

Kakorkoli, kriza COVID-19 je področju upravljanja s človeškimi viri dvignila njeno pomembnost za organizacijo in njeno neprekinjeno delovanje. Svet na račun pandemije COVID-19 spoznava, da je proces upravljanja s človeškimi viri ključnega pomena za učinkovito obvladovanje kriznih situacij.

*avtor je član Slovenskega združenja korporativne varnosti



Pandemija je epidemija nalezljive bolezni, ki zajame človeško populacijo na velikem geografskem območju, npr. na eni celini ali celem svetu. Po kriterijih Svetovne zdravstvene organizacije (WHO) je pandemija epidemija, ki izpolnjuje naslednje pogoje: 1. je bolezen za določeno populacijo nova, 2. povzroča resne zdravstvene težave pri ljudeh in 3. se z lahkoto in v več primerih širi med ljudmi. V novejši zgodovini je zaradi razumevanja razsežnosti posledic potrebno izpostaviti naslednje pandemije: španska gripa (v letih med 1918 in 1921 je zahtevala vsaj 50 milijonov življenj), azijska gripa (1957 zahtevala 1,1 mio življenj), hongkonška gripa (1968 , cca. 1 milijon življenj), nova gripa (2009), pandemija COVID-19 in še vedno prisotna pandemija aidsa (uradno začela leta 1981 in še traja in je do sedaj vzela 25 milijonov življenj). Za vse te pandemije je značilna hitra širitev, velika intenzivnost in velik odstotek obolelih, ki potrebujejo nujno medicinsko oskrbo (po podatkih WHO 5% obolelih).

Direktor Hidria holdinga, dr. Iztok Seljak je v intervjuju na portalu Slovenec objavljenem dne 30.3.3020 med drugim izpostavil nekaj spoznanj do katerih je prišel v procesu soočanja in obvladovanja epidemije COVID-19. V nadaljevanju povzemam nekaj njegovih spoznanj, ki so pomembna z vidika tveganj in upravljanja človeških virov, ki jih je potrebno ustrezno opredeliti in obravnavati že v fazi izdelave OROT. Po njegovih besedah je bila prva reakcija vseh v podjetju verjetno upravičen strah, za svoja lastna življenja in za življenja vseh z njimi povezanih in s tem povezana odgovornost za njihovo zaščito. Neposredno s tem se je hitro dodatno mešal strah in odgovornost za njihova delovna mesta in njihovo prihodnost. V roku nekaj dni so tako vsi kolektivno dozoreli in doumeli, da morajo za zagotovitev njihovega obstoja ustrezno zaščititi zdravje ljudi in s tem omogočiti njihovo nadaljnje delovanje. Zavedali so se, da je zaradi značilnosti epidemije delovanje vseh procesov ogroženo zaradi potencialnega in dejanskega izpada zaposlenih v primerih, da se jih bolezen neposredno dotakne. Zaradi navedene nevarnosti so med drugim v vodstvu sprejeli sklep o kompleksni delitvi družbe na mikropodjetja – organiziranje manjših skupin zaposlenih, ki delujejo samostojno in se nikakor ne mešajo z drugimi. Bistveno za njih je bilo, da so se od prvega trenutka naprej na polno posvetili zagotavljanju osnovne varnosti zaposlenih tudi z uvajanjem za njih potrebnih specifičnih internih ukrepov. Ključni cilj je bil tekoče pokrivanje vseh potreb njihovih kupcev, s čimer se kratkoročno izognejo sicer izjemno visokim pogodbenim kaznim. S tem krepijo zaupanje kupcev v njih in ostajajo kredibilni in zaupanja vredni partnerji. Njihovo pomembno zavedanje je, da je to žal šele začetek. Prehajajo v fazo zagotavljanja nujne vzdržnosti takega pristopa, v »novo normalo«, v svet, ki nikoli več ne bo tak, kot je bil prej. Ta bitka se s tem še ne bo zaključila, ampak šele dobro začela. Še posebej je izpostavil spoznanje, da je pri reševanju organizacije nujna potrebna koordinacija vseh ključnih podjetij v njihovi idrijsko-cerkljanski regiji ter zdravstvenega doma in obeh občin v smislu medsebojne pomoči in z izmenjavo najboljših praks.

Upravljanje človeških virov kot sestavni del operativnih tveganj in korporativne varnosti

Najprej upravljanje ključnih človeških virov razumemo kot pomembno vrsto operativnih tveganj, kajti gre za proces razumevanja odnosov med posamezniki, nalogami in organizacijo, za splet različnih programov in dejavnosti, s katerimi želimo doseči uspešno poslovanje tako, da so zadovoljni vsi deležniki, ki v tem procesu sodelujejo: to so vodstva, srednji in operativni menedžment, drugi zaposleni, pogodbeni partnerji, zunanji izvajalci, zainteresirane javnosti idr. Sicer pa proces upravljanja človeških virov obsega naslednje aktivnosti: prepoznavanje kadrovskih tveganj, načrtovanje kadrovskih sprememb, izbor in sprejem novih kadrov, nameščanje, premeščanje in nadomeščanje kadrov, napredovanje posameznikov ter izobraževanje, izpopolnjevanje in usposabljanje kadrov. Ko ta proces obravnavamo tudi z vidika neprekinjenosti delovanja KI in IBS je pomembno, da je proces upravljanja s človeškimi viri neločljivo povezan s področjem korporativne varnosti in kot tak neposredno vpet v proces upravljanja s tveganji na strateškem in operativnem nivoju. Gre za pomembnost upravljanja lastnih ključnih kadrov in ključnih kadrov pogodbenih izvajalcev, ki zasedajo tista delovna mesta in delovne naloge, ki zagotavljajo neprekinjeno delovanje KI in IBS v kriznih okoliščinah. Odgovorna oseba področja upravljanja s človeškimi viri mora biti stalni član kriznega štaba in odbora ali službe upravljanja s tveganji.

10 ključnih ugotovitev kadrovskih strokovnjakov poveznih z obvladovanjem krize COVID-19

V mesecu marcu 2020 je bila organizirana 90 minutna spletna oddaja z več kot 2000 udeleženci, na kateri je sedem vodilnih kadrovskih voditeljev (IBM, MBA, dva iz Novartisa, Nextdoor, PHV Evrope, United Help Group na svetu (povzeto po Joshbersin, 1.4.2020) razpravljalo o aktivnostih, ki so jih njihova podjetja izvajala za obvladovanje krize COVID-19 in izkušnje, ki so jih imeli z vidika upravljanja s človeškimi viri. Izpostavljenih je bilo 10 ključnih ugotovitev, ki jih v obliki povzetka podajam v nadaljevanju:

- izjemen porast dela na daljavo – v IBM je več je kot 95% ljudi delalo od doma, v Novartisu je bil najbolj iskan tečaj »How to use Microsoft Teams« in takoj za tem »Time Management: Working From Home",
- najpomembnejša sta osebna varnost in zdravje, tako z vidika posameznika kot tudi z vidika delovnega okolja in z vidika družbenih odnosov,
- nujnost digitalizacije komunikacij in določenih procesov in postopkov – tečaji in sestanki na daljavo z uporabo sodobnih komunikacijskih tehnologij (tečaji, ki so se prej izvajali dve leti, so se sedaj izvedli v dveh tednih),
- medsebojna skrb, razumevanje in sočutje – ljudje smo kljub izoliranosti na nek način postali bolj povezani,
- razpršitev odločanja s centralno koordinacijo – vsaka funkcija mora imeti strategijo za centralno usklajevanje in lokalno odločanje in lokalni nadzor, ki temelji na skupnih platformah, strategijah in vrednotah,
- narediti manj z bistveno manj viri – zmanjšan obseg povpraševanja narekuje manjšo porabo virov, ki z njihovo optimalno izrabo kljub zmanjšanju povpraševanja ustvarjajo boljšo dodano vrednost na vloženo enoto kapitala - brezplačni programi, večje projekte razdeliti na manjše in tako hitreje in učinkoviteje dosegati dolgoročne strategije in cilje,
- deluj hitro in se povezuj – prehod iz projektnega načina delovanja na krizno delovanje v manjših skupinah (prioritetni timi, globalni sveti, ki se sestajajo vsak dan),
- pomembnost dostopa do podatkov od kjerkoli v realnem času – na ta način se kljub razpršenosti odločanja dosega hiter prenos informacij in učinkovito sprejemanje odločitev,
- načrtovanje neprekinjenosti delovanja je vitalnega pomena za organizacije - dogodki »črnega laboda« se dogajajo ves čas (»črni labod« je metafora za dogodek, za katerega je značilno troje: je redek, ima izjemno velik učinek in je retrospektivno predvidljiv – po dogodku se potrudimo poiskati razlage za njegov obstoj in ga skušamo narediti razumnega in predvidljivega), zato je nujno v vsakdanjem življenju predvideti, da bodo lahko šle stvari kljub temu, da tečejo nemoteno, kljub vsemu narobe. Organizacije, ki so v svoje delovanje vpeljale to filozofijo razmišljanja in delovanja, se s krizami in kriznimi situacijami spopadajo učinkoviteje, posledice na njihovo poslovanje pa so zaradi tega bistveno manjše. Prožnost delovanja, hitra odzivnost na spremembe in sposobnost prilagajanja je v takšnih situacijah izjemnega pomena za zagotavljanje neprekinjenega delovanja organizacije.
- izpostavljena je pomembnost vodstva – poudarja se zavedanje ustreznosti vodenja in sprejemanja pravih odločitev v ključnih trenutkih in njihov pomen za neprekinjenost delovanja organizacije, odnose v organizaciji in socialno varnost zaposlenih.



Zato je nujno potrebno v organizacijah vzdrževati čim bolj stabilna okolja v katerih se ključni kader razvija tudi v smeri obvladovanja tveganja in zagotavljanja neprekinjenega delovanja. S tem povezano je nujno vzpostaviti ustrezno vrednotenje ključnih kadrov in investicij v njihov razvoj in ustrezno razpoložljivost.

»Rdeča nit« navedenih ugotovitev je priprava takšnih človeških virov, ki so v kriznih razmerah sposobni zagotavljati neprekinjeno poslovanje in varne delovne pogoje.

Upravljanje človeških virov in skrb za varnost je ključna za neprekinjenost delovanja KI in IBS

Ugotovitve priznanih strokovnjakov s področja upravljanja s človeškimi viri, priznanih in uspešnih gospodarstvenikov ter nenazadnje tudi moja spoznanja, do katerih sem prišel pri izvajanju številnih znanstveno-raziskovalnih in strokovnih projektov na področju ocenjevanja ranljivosti, ogroženosti in tveganj, pri vzpostavljanju integralnih varnostnih sistemov v KI ter pri izvajanju izobraževalnih programov, kažejo na dejstvo, da je ključ uspeha za zagotavljanje dolgoročne neprekinjenosti delovanja KI in IBS, zagotavljanje zadostnega števila ustrezno usposobljenih in ustrezno motiviranih ključnih kadrov. Izrednega pomena je sistemska urejenost področja upravljanja varnostnih tveganj, ki jim je treba - v času krize, s pomočjo menedžmenta korporativne varnosti ter z aktiviranjem sodobnih sredstev informacijske, fizične in tehnične varnosti - posvečati maksimalno pozornost. Kajti z obvladovanjem varnostnih tveganj zagotavljamo neprekinjenost delovanja gospodarskih in drugih družb, ki upravljajo s KI in IBS.

Da bi lahko dosegali ta cilj pa je potrebno pravočasno in sistemsko pristopiti k vzpostavitvi okolja, ki takšno delovanje omogoča. Pri tem morajo upravljavci KI in IBS organizirati izvajanje predvsem naslednjih aktivnosti:

- Določiti vitalne in kritične poslovne procese, sredstva in kadrovske resurse, ki so nujni za neprekinjeno delovanje posameznih sektorjev KI in IBS.
- Določiti bistvene storitve, ki morajo delovati neprekinjeno.
- Izdelati register kritičnih procesov in postopkov, ki morajo delovati neprekinjeno.
- Izdelati register sredstev (kritične programske in strojne opreme), ki mora zagotavljati podporo za neprekinjeno delovanje KI in IBS.
- Izdelati register kritičnih delovnih mest, ki morajo biti stalno zasedena za zagotavljanje neprekinjenega delovanja KI in IBS.
- Izdelati register ključnih kadrov, ki morajo zasedati kritična delovna mesta z naborom njihovih znanj, kompetenc, spretnosti in razpoložljivosti, ki zagotavljajo neprekinjeno delovanje KI in IBS:
- Zagotoviti ustrezen sistem nagrajevanja ključnih kadrov, ki bo podlaga za njihovo stalnost, razpoložljivost in psihofizično sposobnost izvajati naloge na kritičnih delovnih mestih neprekinjeno, tudi v času krize in kriznih situacij.
- Zagotoviti ustrezne podporne in od ostalih prostorov izolirane prostore za neodvisno delovanje KI in IBS v krizi in v kriznih situacijah – tudi ločeni prostori za ključne kadre namenjene počitku, sprostitvi, prehrani, higieni, sanitarije ipd,
- Zagotoviti ustrezen izobraževalni sistem (notranja in zunanja izobraževanja, izpopolnjevanja in treningi), ki bo zagotavljal ustrezno usposobljenost ključnih kadrov (znanj, spretnosti in veščin) in zagotavljajo njihovo neodvisno in suvereno izvajanje nalog na ključnih delovnih mestih tudi v času krize in kriznih situacij.
- Določiti, kateri so soodvisni sektorji oziroma procesi znotraj organizacije, ki morajo zagotavljati neprekinjeno delovanje KI in IBS.
- Izdelati register kritičnih dobaviteljev, ki morajo zagotavljati zanesljive in neprekinjene dobave za potrebe zagotavljanja zanesljivega in neprekinjenega delovanja KI in IBS.
- Zagotoviti ustrezna finančna sredstva ključnim pogodbenih izvajalcem, ki jim omogoča zagotavljanje ustreznih kadrov za njihovo neprekinjeno delovanje in podporo upravljavcem KI in IBS tudi v času krize in kriznih situacijah – plačilo ustreznih nadomestil za zagotavljanje stalnih in ustrezno usposobljenih kadrovskih rezerv, ki so nujne za neprekinjeno delovanje pogodbenih izvajalcev tudi v času krize in kriznih situacij.
- Izdelati register kritičnih odjemalcev (kupcev), katerim je potrebno zagotavljati neprekinjene dobave tudi v času krize in kriznih razmer.
- Določiti kriterije sprejemljivosti motenj in izpadov delovanja iz vidika zagotavljanja zanesljivega in neprekinjenega delovanja KI in IBS.
- Vzpostaviti proces izvajanja rednih letnih penetracijskih testov IKT, njihove varnosti, dostopnost, razpoložljivosti, zanesljivosti in neprekinjenosti delovanja.
- Pri izdelavi OROT upoštevati verjetnost pojava najslabšega možnega scenarija in s tem povezanih medprocesnih, medsektoskih in čezmejnih vplivov na delovanje in upravljanje KI in IBS.
- Izdelati Načrt odzivanja na incidente v katerem je treba posebno pozornost posvetiti ključnim kadrom in njihovi razpoložljivosti (dosegljivosti) v času krize.

Izpostavil sem le tiste bistvene aktivnosti v katerih glavno izvršilno vlogo predstavljajo ključni kadri, ki s svojimi znanji, kompetencami, spretnostmi in ustrezno razpoložljivostjo skrbijo za izvajanje ključnih nalog na delovnih mestih in s tem zagotavljajo neprekinjeno delovanje KI in IBS.

Sklepna beseda

V aktualni zdravstveni, psihosocialni in gospodarski koronavirusni krizi svetovnih razsežnosti se politiki, gospodarstveniki, strokovnjaki, raziskovalci, znanstveniki in drugi soočajo z negotovostjo, motnjami v preskrbovalnih verigah, izpostavljenostjo nepreverjenimi informacijami, prepočas-

nim odzivanjem na spremembe, pomanjkanjem strategij in problemi kriznega vodenja. To so soočanja strateške narave, ki jih prvenstveno mora obvladovati krizni, varnostni in politični menedžment, ki mora skrbeti za vzdržljivost, odpornost in neprekinjeno delovanje KI in IBS. Z vidika zagotavljanja ključnih človeških virov in kontinuiranega zagotavljanja neprekinjenega delovanja je najbolj izpostavljen zdravstveni sektor, ki v tej fazi krize učinkovito obvladuje nastalo situacijo. Drugi izpostavljeni sektor je informacijsko-komunikacijski sektor, ki vlaga maksimalne napore za neprekinjeno delovanje mobilnih, elektronskih in drugih komunikacij. Tudi ostali sektorji kot so energetika, promet, prehrana, finance, varovanje okolja, doživljajo organizacijsko, ekonomsko in kadrovsko preobrazbo za obvladovanje nastale krize v smeri zagotavljanja neprekinjenega delovanja.

Kakorkoli, kriza COVID-19 je področju upravljanja s človeškimi viri dvignila njeno pomembnost za organizacijo in njeno neprekinjeno delovanje. Svet na račun pandemije COVID-19 spoznava, da je proces upravljanja s človeškimi viri ključnega pomena za učinkovito obvladovanje kriznih situacij. Je pa dejstvo, da se je premalo pozornosti posvečalo področju upravljanja s človeškim viri in njihovi realni vrednosti za organizacije. Vendar pa sodoben pristop k upravljanju s človeškimi viri in njihov razvoj ni možen čez noč. Zato je nujno potrebno v organizacijah vzdrževati čim bolj stabilna okolja v katerih se ključni kader razvija tudi v smeri obvladovanja tveganja in zagotavljanja neprekinjenega delovanja. S tem povezano je nujno vzpostaviti ustrezno vrednotenje ključnih kadrov in investicij v njihov razvoj in ustrezno razpoložljivost.

Pravijo, da je po vojni lahko biti general. Res je, zato je pomembno da pridobljena spoznanja in izkušnje v obvladovanju nastale krize smiselno uporabimo za izboljšave, s katerimi bomo v primeru ponovitve krize v takšni ali drugačni obliki učinkoviteje obvladovali novo nastale krizne razmere in s tem zmanjšali njihov negativni vpliv na posameznika, organizacije in družbo kot celoto. Slovenija je imela tokrat srečo (ob upoštevanju dejstva, da je bilo tudi ukrepanje vlade za zajezitev širitve COVID-19 ustrezno in učinkovito), saj do pravega razvoja epidemije sploh ni prišlo. Dokazano okužena je bila le peščica prebivalstva. Naj nas to ne zavede. Naj bo to naša motivacija za to, da se v času do morebitne naslednje krize ustrezno pripravimo, odpravimo ugotovljene vrzeli in tako novo krizo pričakamo v boljši organizacijski, psihosocialni, ekonomski, poslovni in kadrovski kondiciji. ■

Dokazano okužena je bila le peščica prebivalstva. Naj nas to ne zavede. Naj bo to naša motivacija za to, da se v času do morebitne naslednje krize ustrezno pripravimo, odpravimo ugotovljene vrzeli in tako novo krizo pričakamo v boljši organizacijski, psihosocialni, ekonomski, poslovni in kadrovski kondiciji.



Čas je za FABRIC*

Inovativna omrežna arhitektura – hrbtenica sodobnega poslovanja

SMART COM

NAREDITE VEČ, HITREJE

Prožno, avtomatizirano in prilagodljivo virtualizirano omrežje za hitrejše uvajanje aplikacij.

IZBOLJŠAJTE VARNOST

Odprava vstopnih točk na zadnjih vratih, s preprečitvijo bočnih premikov in z izolacijo potencialno nevarnih IoT naprav.

POENOSTAVITE UPRAVLJANJE

Racionalizacija in poenostavitev omrežja z znatno manjšim številom protokolov in točk dotika.

**slo. matričje*

E-knjiga:
10 prednosti Fabric Connect

UDEJANJAMO VAŠE VIZIJE

www.smart-com.si

Extreme networks
Tehnološki partner

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Dr. Jurij Klančnik,
direktor Področja za obratovanje, ELES d.o.o.

ELES IN NJEGOVA VLOGA PRI NEPREKINJENOSTI DELOVANJA ELEKTROENERGETSKEGA SISTEMA

Na kratko smo se pogovarjali z dr. Klančnikom o pomenu neprekinjenosti delovanja ELES-a in njegovega pomena za celoten elektro-energetski sistem Republike Slovenije.

Podjetje ELES d.o.o. je letošnji prejemnik prestižne nagrade »Slovenian Grand Security Award« v kategoriji »Najbolj varno podjetje«.

Vsaka kriza predstavlja resen izziv za zagotavljanje neprekinjenega delovanja kritične infrastrukture. Kako analizirate tveganja, ki bi lahko vplivala na neprekinjeno obratovanje sistema prenosa električne energije?

Področje obvladovanja tveganj, predvsem tveganja vezana na delovanje kritične infrastrukture so v podjetju ELES prepoznana kot eno pomembnejših področij. Negativni vplivi v primeru uresničenih tveganj lahko namreč prizadenejo velik del prebivalstva Slovenije in sežejo celo preko državnih meja, zato v družbi ELES vsa tveganja obvladujemo sistematično preko vzpostavljenih sistemov upravljanja kakovosti. Pristop k obvladovanju tveganj temelji tudi na analizi tveganj, ki vključuje preučevanje vzrokov in virov tveganja, pozitivnih in negativnih posledic, verjetnosti uresničitve tveganj ter posledice, ki jih lahko tveganja povzročijo.

Epidemija COVID-19 je bila specifična v dejstvu, da je bilo posebej izpostavljeno ključno osebje, ki zagotavlja neprekinjenost delovanja elektro-energetskega sistema (EES). Kako ste v ELES-u obvladali to situacijo v času epidemije?

Na krizno situacijo smo se odzvali hitro in efektivno, k čemur so v veliki meri pripomogle tudi pretekle izkušnje in priprave na izredna stanja. Vsi ključni procesi delovanja ELES so se v času koronavirusa izvajali nemoteno. S ciljem preprečevanja širjenja epidemije smo za zaposlene uredili delo od doma, približno 15% zaposlenih je opravljalo delo na naših lokacijah. Posebne ukrepe smo sprejeli za zaposlene v centrih vodenja, še posebej v Republiškem centru vodenja, ki nadzira obratovanje prenosnega elektroenergetskega sistema. Zaradi nevarnosti okužbe smo določili dve ekipi po šest operaterjev. Določili smo 14 dnevne izmene, ena ekipa je opravljala svoje delo v povsem izoliranem Republiškem centru, druga ekipa je bila ta čas doma v karanteni. Pred nastopom dela v izolaciji so bili operaterji testirani na COVID-19.

Bo po vašem mnenju to vplivalo na večjo pozornost za razvoj ključnega kadra v ELES-u?

ELES je v skladu z zakonodajo upravljalec kritične infrastrukture in izvajalec bistvenih storitev, zato je moral že pred epidemijo v vsakem trenutku poskrbeti za nemoteno delovanje elektroenergetskega sistema Slovenije. Zavedamo se, da zato med drugim potrebujemo tudi visoko usposobljene in izobražene zaposlene, ki so motivirani za kakovostno izvajanje delovnih nalog. V ta namen

*avtor je član Slovenskega združenja korporativne varnosti



Zavedamo se, da zato med drugim potrebujemo tudi visoko usposobljene in izobražene zaposlene, ki so motivirani za kakovostno izvajanje delovnih nalog. V ta namen smo že v preteklosti dobršen del finančnih sredstev in časa namenjali strokovnemu usposabljanju zaposlenih. Enako bo ostalo tudi v prihodnosti.

smo že v preteklosti dobršen del finančnih sredstev in časa namenjali strokovnemu usposabljanju zaposlenih. Enako bo ostalo tudi v prihodnosti.

Informacijska in komunikacijska tehnologija je vedno bolj prisotna pri podpori delovanja tehnoloških sistemov. Kako zagotavljate ustrezno kibernetsko varnost tehnološkemu procesu v ELES-u?

ELES ima vgrajeno najsodobnejšo opremo za vodenje prenosnega omrežja. Prenosni sistem elektroenergetskega omrežja in sistem informacijsko komunikacijskih storitev in omrežij, zato deluje brezhibno. Smo v fazi snovanja in uvajanja CSOC (Cyber Security Operations Center), ki bo optimalno izkoristil različne varnostne podsisteme, ki jih že imamo ali jih bomo uvedli v kratkem, saj ocenjujemo, da je možnost kibernetskih napadov v takšnih situacijah, kot je COVID-19, povečana. Zagotavljanje kibernetske varnosti je proces, ki se nikoli ne zaključi in zahteva stalne izboljšave. In to je naša pot.

Katera tveganja bi izpostavili kot tista najbolj izpostavljena za prihodnje učinkovito delovanje EES v katerem ima ELES ključno vlogo?

ELES posebno pozornost namenja tistim tveganjem, ki bi v primeru uresničitve ogrozila delovanje kritične infrastrukture oziroma izvajanje bistvenih storitev. Med ta gotovo sodijo nerazpoložljivost ključnih elementov EES. Do tega bi lahko prišlo zaradi različnih vzrokov, ki jih v ELES-u nenehno spremljamo, ocenjujemo in z ustreznimi preventivnimi ukrepi zmanjšujemo verjetnost uresničitve teh oziroma vplivamo na zmanjševanje potencialne škode, če bi se tveganja uresničila. Kot je bilo že omenjeno, so v zadnjem času vse bolj pereča tveganja na področju informacijskih in komunikacijskih tehnologij, kjer z ustreznimi konfiguracijami sistemov in njihovih zaščit sledimo naprednim trendom v Evropi in svetu. Tveganje pri izvajanju naših nalog predstavlja tudi nerazpoložljivost ključnih zaposlenih, na kar nas je zelo resno opozorila epidemija COVID-19. ■

Avtor: DDr Aleš Jug / Becker College, Massachusetts, ZDA



NEMOTENO POSLOVANJE PODJETJA V LUČI COVID-19

Živimo v prav posebnem času, ki si ga še v začetku tega leta, nihče, niti v najbolj drznih sanjah, ni uspel predstavljati. Domala dva meseca je že, ko zaradi pandemije koronavirusa ostajajo zaprte meje, stojijo podjetja, ljudje pa smo doma v karanteni.

Glede na to, da imamo opravka s pandemijo, je vpliv globalen. Vpliv pandemije koronavirusa na podjetja je vsaj tronivojski:

- motene so oskrbovalne verige na področju surovin in repromaterialov, kar posledično pomeni, da se v podjetjih lahko ustavi proizvodnja ali pa mora podjetje iskati druge dobavitelje,
- motena je logistika dostave končnih proizvodov na trg, kar pomeni zmanjšan obseg prodaje,
- zaradi ukrepov vlad ljudje ostajajo v karanteni, kar posledično pomeni zmanjšano potrošnjo. Prav tako lahko za CO

VID-19 zbolijo zaposleni, kar seveda pomeni motnjo v samem delovanju obrata.

Poleg navedenih motenj se podjetja soočajo tudi z nezanesljivostjo napovedi, kdaj bodo prenehale veljati razne omejitve, postavljene zaradi preprečevanja širitve koronavirusa. Nassim Nicholas Taleb, profesor in bančnik iz Wall Streeta je v svoji knjigi (The Black Swan: The Impact of the Highly Improbable, 2007) prvi pisal o dogodkih, ki jih je sam označil s „črnimi labodi“. Taleb je trdil, da dogodkov, kot so črni labodi zaradi njihove izjemne redkosti ni mogoče predvideti, imajo pa katastrofalne posledice.

Zgodovina kaže, da so bile nalezljive bolezni, epidemije in pandemije vedno razlog za veliko smrtnih žrtev, ki so prekašale celo naravne katastrofe in vojne. Čeprav ni za pričakovati, da bo imel COVID-19 posledice podobne tistim, zaradi izbruha španske gripe leta 1918 (vsaj 50 milijonov smrtnih žrtev), pa ni dvoma v tem, da bo sedanja pandemija imela izjemno velik vpliv, tako na ljudi, kot na nacionalna gospodarstva. O tem ali spada med ti. črne labode je več nasprotujočih se mnenj.

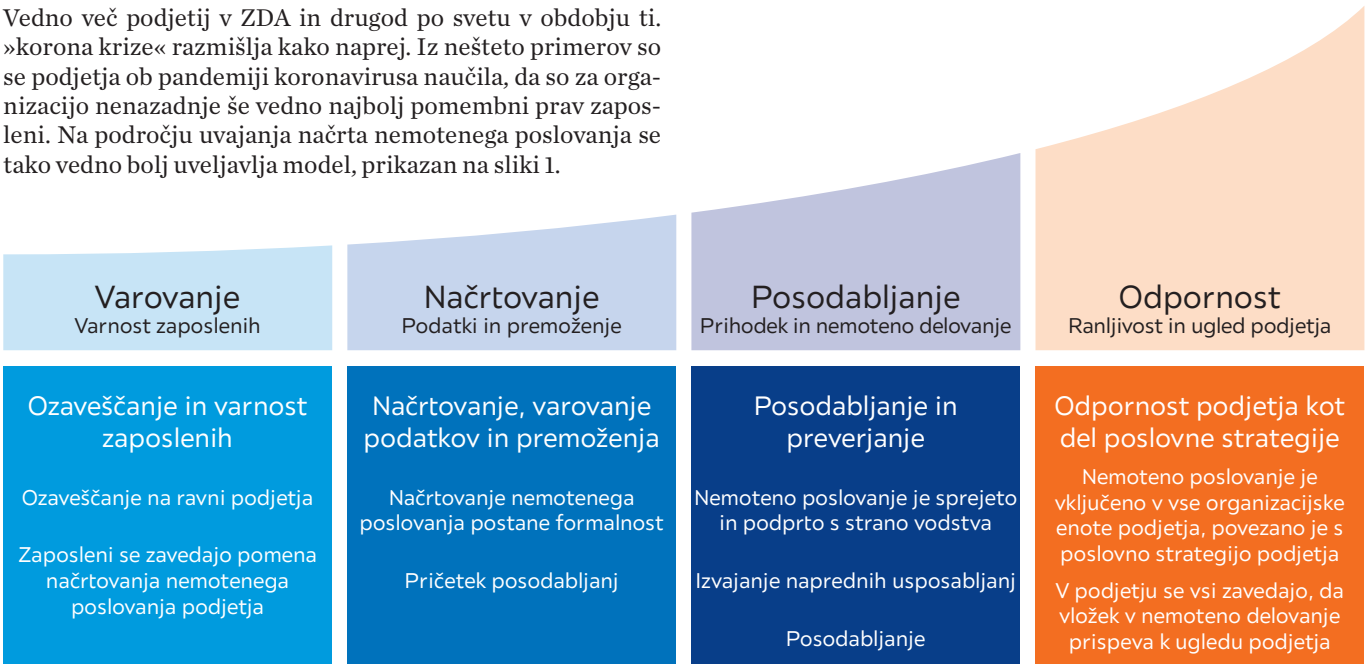
Kakorkoli že, je jasno, da podjetja na pandemijo koronavirusa niso bila pripravljena. Pa bi se lahko pripravila?

> Pričakovati je, da bodo podjetja po svetu v prihodnje več vlagala in razmišljala o procesu zagotavljanja nemotenega poslovanja. To še posebej velja ob dejstvu, kjer se še letos pričakuje nove lokalne izbruhe virusa, s tem pa potencialne motnje na domačih in globalnih trgih.

Eno od doslej manj znanih orodij za pripravo podjetja na motnje, kot so naravne in druge nesreče, je načrt nemotenega poslovanja podjetja. Gre za postopek oblikovanja sistemov preprečevanja, in okrevanja podjetja, ki je izpostavljeno potencialnim grožnjam. Poleg preprečevanja je cilj načrtovanja nemotenega poslovanja omogočiti tekoče operacije pred in med motnjo ter čim hitrejše okrevanje. Pred obdobjem koronavirusa je v mednarodnem obsegu le okoli 30% večjih in 20% manjših podjetij vsaj razmišljalo o postopkih, ki jih morajo sprejeti za dosego nemotenega poslovanja podjetja.

Nekatere prehodne analize kažejo, da se stanje ozaveščenosti podjetij na temo nemotenega poslovanja spreminja. To je pomembno toliko bolj, če se zavemo že opisanega tronivojskega vpliva pandemije koronavirusa, ki je predvsem globalen. Po koncu pandemije bodo podjetja aktivnosti iz faze zasilnega zagona preusmerila v fazo okrevanja. To je hkrati tudi zelo primeren čas, ko se na ravni podjetja lahko vprašajo, kako se bolje pripraviti na podobne scenarije. Krizni čas namreč lahko deluje kot katalizator za inovacije in nove načrte.

Vedno več podjetij v ZDA in drugod po svetu v obdobju ti. »korona krize« razmišlja kako naprej. Iz nešteto primerov so se podjetja ob pandemiji koronavirusa naučila, da so za organizacijo nenazadnje še vedno najbolj pomembni prav zaposleni. Na področju uvajanja načrta nemotenega poslovanja se tako vedno bolj uveljavlja model, prikazan na sliki 1.

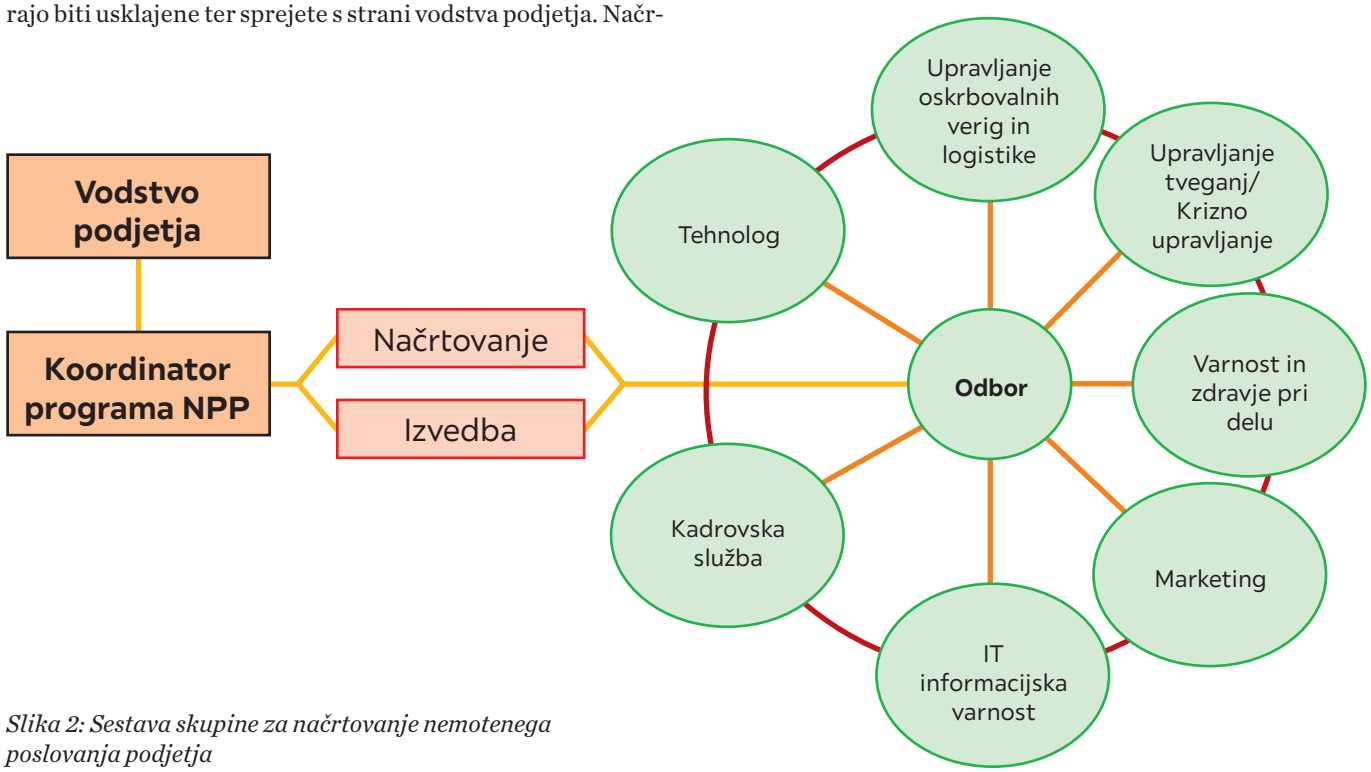


DDr. Aleš Jug, Februar 2020, povzeto po Agility Recovery

Slika 1: Proces uvajanja politike nemotenega poslovanja podjetja

Po modelu z zgornje slike se izgradnja odpornosti podjetja prične s procesom varovanja zaposlenih ter ozaveščanjem o pomenu nemotenega poslovanja na ravni podjetja. Proces se nadaljuje z usklajenim načrtovanjem, ki mora postati del politike podjetja in mora biti podprt s strani vodstva podjetja.

Smernice in strategije nemotenega poslovanja podjetja morajo biti usklajene ter sprejete s strani vodstva podjetja. Načrtovanje nemotenega poslovanja podjetja zahteva celovit pristop širše skupine zaposlenih (slika 2), ki skupaj lahko realno ocenijo tveganja, politiko nemotenega poslovanja podjetja in sisteme, postopke in protokole, s katerimi se lahko podjetje izogne prekinitvi poslovanja, v primeru prekinitve poslovanja pa to v najkrajšem možnem času ponovno vzpostavijo.

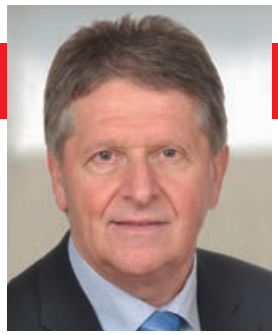


Slika 2: Sestava skupine za načrtovanje nemotenega poslovanja podjetja

Delo od doma, težave z oskrbovalnimi verigami, absentizem zaposlenih, pomanjkljiva komunikacija s potrošniki so vse elementi, kjer so imela podjetja ob trenutni pandemiji veliko težav. Prav zato velja v skupino, ki načrtuje nemoteno poslovanje podjetja vključiti vsaj deležnike, prikazane na sliki 2.

Pričakovati je, da bodo podjetja po svetu v prihodnje več vlagala in razmišljala o procesu zagotavljanja nemotenega poslovanja. To še posebej velja ob dejstvu, kjer se še letos pričakuje nove lokalne izbruhe virusa, s tem pa potencialne motnje na domačih in globalnih trgih. ■

Avtor: doc. dr. Brane Bertoncelj / Slovensko združenje korporativne varnosti*



KAKO SE SPOPASTI Z UČINKI VIRUSA COVID-19: OBVLADOVANJE PANDEMIJE OB GRADNJI PRIHODNOSTI

Upravljanje s tveganji se bo moralo v prihodnosti spremeniti in dopolniti. Sposobnost scenarijskega razmišljanja in zaznavanja lahko okrepi analizo razmer v spopadu z negativnimi učinki pandemije. Že dalj časa poslujemo in preživljamo obdobje, za katerega smo verjeli, da je negotovo. Nenehni preobrati, globalni premiki, kot so digitalizacija, preobrazba tehnologije, spreminjanje geopolitike in ogrožanj, razvijajoči se poslovni modeli in spreminjajoča soglasja o globalizaciji, varstvu okolja in trgovini, že zadnje desetletje intenzivno izpodbijajo pojem sprejemanja racionalnih izvršilnih odločitev v svetu.

Uvod

»Obstajajo tudi neznane neznanke - tiste, za katere ne vemo, da jih ne poznamo. In če pogledamo zgodovino, so te kategorije najbolj težke.«[1]

Nobena država, organizacije in vodstva niso zaščiteni pred vplivi virusa COVID-19 (v nadaljevanju: pandemija). Gre za to, da se nam je »zalomila« vsakdanja rutina, da živimo na prelomnici, ko se lahko razvoj družbe zasuče v katerokoli smer. Ujeti smo v zanko raznih predvidevanj in razpoloženj, od upanja do odpora sprejemanja sprememb dosedanjega načina življenja. To pomeni, da imperativu načela ugodja ni zadoščeno.

V negotovih časih vodstvom držav in organizacij ni prizanesena odgovornost kritičnega odločanja. Časovni okvir za odločanje se je skrajšal, kontekstna negotovost odločanja pa je še težja. Izkušnje kažejo nagibanje k enemu od dveh vrst odzivanja na negotovost. Prva je, da prepoznamo njen obstoj, globino in kompleksnost, vendar jo želimo zmanjšati ali ohromiti. Druga možnost pa je drznost (tveganost) pred negotovostjo, kot da bi želeli odpraviti neprijetnost zapletenih razmer.

Črni labod

Pandemija je dogodek, ki je popolnoma presenetil svet in je značilen primer »črnega laboda«. Korporativna varnost to metaforo uporablja za analizo verjetnosti tveganja[2], ki opisuje izredni dogodek z velikim učinkom, ki je pozneje neustrezno racionaliziran, da bi bil v prihodnosti bolj predvidljiv in manj naključen. Teorija temelji na dejstvu, da je dolgo veljalo, da obstajajo le beli

V negotovih časih vodstvom držav in organizacij ni prizanesena odgovornost kritičnega odločanja. Časovni okvir za odločanje se je skrajšal, kontekstna negotovost odločanja pa je še težja.

*avtor je član Slovenskega združenja korporativne varnosti

Delovanje v razmerah negotovosti je ključna tema sodobnega poslovanja. Sprejemanje temeljnega preoblikovanja življenja pomeni soočanje z negotovostjo in njeno vključitev v odločanje.

labodi, in šele po odkritju Avstralije je prišlo do spoznanja, da obstajajo tudi črni. To potrjuje, da ima vsako pravilo izjeme. Avtorjeva osnovna teza je, da so, v nasprotju z današnjimi spoznanji, dogodki, ki opredeljujejo svetovne trende, nepredvidljivi, oziroma da na svetovno gospodarstvo nesorazmerno vplivajo težko predvidljivi dogodki, ki presegajo običajna znanstvena, družboslovna in finančna pričakovanja. V današnjem svetu se človeška misel osredotoča na ponavljajoče se in poznane dogodke, medtem ko se izredni dogodek razlaga kot izjemo. Avtor po drugi strani meni, da so prav takšni izredni dogodki ključni pri ustvarjanju prihodnosti, oziroma da bo prihodnost vse bolj nepredvidljiva.

Spremembe miselnosti: od danes do jutri

Delovanje v razmerah negotovosti je ključna tema sodobnega poslovanja. Sprejemanje temeljnega preoblikovanja življenja pomeni soočanje z negotovostjo in njeno vključitev v odločanje. Perspektive, kako to storiti v primeru pandemije, vključujejo interdisciplinarni pristop, in sicer (podrobnejša pojasnitev opomnika presega obseg članka):

- razmislite o negotovosti v različnih časovnih obdobjih,
- ugotovite najpomembnejše negotovosti za svojo panogo in poslovanje organizacije,
- proučite spremembe vlog in pravil države ter organizacij,
- uporabite negotovosti za analizo več različnih prihodnosti,
- upoštevajte nepredvidljivost pri financiranju virov in porab ter na kapitalskih trgih,
- ponovno presodite načrte poslovanja, denarne tokove in neprekinjenost delovanja organizacije,
- pravočasno si zagotovite dodatne vire kapitala,
- preverite posojilne in kreditne pogodbe,
- ostanite v stiku s ključnimi deležniki in dobavnimi verigami,
- preverite ukrepe države (npr. razne pomoči),
- iščite različne perspektive poslovanja (npr. ureditev dela na daljavo),
- vključite razne možne scenarije v odločanje in proučite posledice različnih odločitev,
- sproti preverjajte in presojajte plane poslovanja,
- pričakovanja glede fizične, čustvene, finančne in informacijske varnosti (npr. kako se je spremenila socialna pogodba z zaposlenimi),
- izboljšajte vodenje poslovanja, s poudarkom na varnosti zaposlenih in kontinuiteto delovanja,
- upoštevajte zaupanje kot katalizator okrevanja (zaupanje je lepilo življenja in je najpomembnejša sestavina učinkovite komunikacije),
- proučite, kako so kriminalne družbe prilagodile svoje aktivnosti novim razmeram (pokazale so prilagodljivost in prožnost, da izkoristijo pandemijo),
- upoštevajte, da povečana tesnoba, stres in strah lahko ustvarijo ranljivost za izkoriščanje.





Zaključek

Edina gotovost je... negotovost**.** Pričakuje se povečanje števila »neznanih neznank«, ali vsaj naglo zmanjšanje zaupanja v tisto, za kar smo v preteklosti vedeli ali verjeli, da je resnično. Od sveta široko dogovorjenih absolutov smo prešli v relativni svet.

V aktivnostih proti pandemiji, ki je preplavila svet, moramo razumeti, da to ni le ena okužba. V resnici sta najmanj dve. Ena okužba je novi koronavirus, nov patogen. Druga okužba pa je starodavna, bolj razrešljiva in tudi bolj nalezljiva: človeški strah.

To ni samo metafora. Strah spremeni človeško vedenje, na boljše ali na slabše. Medtem, ko se strokovnjaki borijo proti pandemiji, bo po mojem mnenju največji izziv postal obvladovanje druge epidemije - širjenje strahu. Vsak od teh premikov predstavlja pomembno območje negotovosti za vodstva in zaposlene, ko se bo svet usmeril v prihodnost in v novo negotovost. Obstajajo razni modeli, ki proučujejo, kako deluje strah na človeka in kako se širi po družbi. Najboljši nasvet, ki ga ti modeli ponujajo je, da moramo o pandemiji razmišljati kot o *štirih* ločenih vidikih: poleg bolezni, ki jo povzroča virus, obstajajo tudi epidemije strahu pred virusom, strah za gospodarske posledice, in verjetno kmalu, strah pred novim cepivom. Vse navedene oblike so tesno prepletene in se bodo med seboj zapleteno tudi širile.

Za povrnitev sveta v novo realnost po pandemiji bo potreben nadzor vseh štirih konjenikov apokalipse[3], zaradi česar je odziv veliko bolj kompleksen in zapleten. Povrnitev se bo nanašala na: (i) pretok ljudi, blaga in storitev po zemeljski obli ne bo več takšen, kot je bil v preteklosti; (ii) sledila bodo nadaljnja testiranja ljudi na okužbo; (iii) testiranja testov na protitelesa za določitev imunosti; (iv) razvoj varnega in učinkovitega cepiva in (v) kar je pomembno, prepričljiva informativna kampanja proti strahu pred cepljenjem.

Pandemija je univerzalen lakmusov papir, ki kaže, kakšni smo in kakšni so drugi, v kakšnem času živimo in kaj se nam obeta. Spoznali smo, kakšni smo kot zaposleni, partnerji, starši, prijatelji, koliko česa in koga lahko prenašamo, kdo nam gre na živce bolj, kot je to normalno, koliko smo razumevajoči in strpni. Testirali smo vse in vsi so testirali nas.

Vse organizacije so tudi pred varnostnimi izzivi, zato ni vprašanje ali bodo preživele pandemijo, ampak »kdaj«, »kako« in »kakšna bo škoda«. Na žalost idealnih rešitev ni!

[1] Izjava ameriškega obrambnega ministra Donalda Rumsfelda (2002).

[2] To teorijo (2007) je populariziral Nassim Nicholas Taleb, libanonsko-ameriški publicist, filozof, statistik

[3] Štirje konjeniki apokalipse so znaki, ki simbolizirajo glavne nesreče človeštva: vojne, kuge, smrti in lakote. ■

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

Avtorica: mag. Polonca Štrekelj / državna nadzornica za varstvo osebnih podatkov, Informacijski pooblaščenec*



VARNOST OSEBNIH PODATKOV V BITKI S COVID-19

S pojavom koronavirusa COVID-19 smo se znašli v krizni situaciji, ki je zahtevala takojšnje ukrepanje in razne tehnološke rešitve so se pokazale kot ena izmed možnosti. V tem kontekstu so že v začetni fazi obvladovanja epidemije vzniknile ideje o aplikacijah in storitvah za omejevanje širjenja okužb s COVID-19, ki bi temeljile na obdelavi podatkov (bodisi anonimiziranih bodisi t.i. surovih osebnih podatkov, vključno s posebnimi vrstami osebnih podatkov, kot so podatki o zdravstvenem stanju).

Informacijski pooblaščenec pozdravlja in spodbuja iniciative organizacij javnega in zasebnega sektorja za sprejemanje ukrepov za zajezitev in ublažitev posledic virusa COVID-19, tudi s pomočjo sodobne tehnologije, vendar mora kljub temu opozoriti na dejstvo, da so upravljalci in obdelovalci osebnih podatkov tudi v teh izjemnih časih dolžni zagotoviti varstvo osebnih podatkov posameznikov, na katere se nanašajo osebni podatki, še posebej takrat, ko se zbirajo podatki o zdravstvenem stanju, saj pravila s področja varstva osebnih podatkov (Splošna uredba o varstvu podatkov, Zakon o varstvu osebnih podatkov-ZVOP-1) ne ovirajo sprejemanja ukrepov, potrebnih v boju proti pandemiji koronavirusa. Nasprotno, predpisi s področja varstva osebnih podatkov, so bili vzpostavljeni in sprejeti kot prilagodljiv branik temeljne človekove pravice do zasebnosti in varstva osebnih podatkov, ob hkratnem zagotavljanju učinkovitega ogrodja ukrepom, katerih namen je obvladovanje širjenja virusa. Kot taki zagotavljajo izhodišče za krepitev zaupanja vseh deležnikov, njihovo spoštovanje s strani predlagateljev posameznih ukrepov, pa vzpostavlja okvir za širšo družbeno sprejemljivost katerekoli rešitve in posledično tudi učinkovitosti le te.

V povezavi z obvladovanjem širjenja okužb s koronavirusom in tehnologijami, ki temeljijo na obdelavi osebnih podatkov, je potrebno poudariti, da so sicer lahko zelo pomembno orodje pri zajezitvi širjenja virusa, vendar imajo omejitve in kot take nudijo zgolj podporo pri učinkovitosti drugih javnozdravstvenih ukrepov (testiranje, klasično sledenje stikom okuženih posameznikov, izolacija, socialna distanca), ne morejo pa jih nadomestiti. Zato bi morala biti **splošna načela učinkovitosti**, **potrebnosti** (kjer ključno vlogo igra epidemiološka stroka) in **sorazmernosti,** ključna vodila pri sprejemanju kateregakoli ukrepa za zajezitev širjenja virusa, ki temelji na obdelavi osebnih podatkov.

Tehnološke rešitve, ki so se pojavile, o nekaterih pa še tečejo razprave, tako na ravni EU, kot na ravni posameznih držav, so zelo raznolike, tako glede njihovega namena in pričakovanega rezultata, glede načina pridobivanja podatkov, uporabe različnih vrst osebnih podatkov (npr. lokacijskih, kontaktnih, o zdravstvenem stanju), kot tudi z vidika posega v temeljne pravice posameznikov, predvsem v zasebnost in varstvo osebnih podatkov. Namen nekaterih je analiza vzorcev mobilnosti v družbi, za pomoč pri načrtovanju ukrepov in spremljanja

Pri razvoju tehnologij in različnih pristopov je nujno treba stremeti k usklajevanju ukrepov znotraj držav članic EU, saj raznolike ali neusklajene pobude posameznih držav članic ne morejo biti učinkovite, po drugi strani tudi ne pripomorejo k vzpostavljanju zaupanja v prilagodljivost predpisov o varstvu osebnih podatkov ali celo v splošno stanje varstva osebnih podatkov v posameznih državah članicah.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



njihove učinkovitosti, kot npr. anonimizirani podatki, ki jih je razkril Google. Namen drugih je omogočiti posameznikom boljše informiranje o obolelosti na podlagi samoporočanja simptomov, kot npr. COVID-19 VSAK ČLOVEK ŠTEJE[1], VirusTracker[2], itd. Najbolj žgoča razprava pa poteka o aplikacijah za iskanje stikov okuženega posameznika, ki so lahko izvedene na različne načine in z različno invazivnimi posegi v pravice posameznikov. Nekatere nevladne in druge organizacije so o tem pripravile tudi omejene analize, kot npr. Privacy International[3], vzpostavljajo pa se tudi repozitoriji in primerjalne analize posameznih aplikacij, kot npr. Law, Science, Technology and Society Research Group[4].

Pri razvoju tehnologij in različnih pristopov je nujno treba stremeti k usklajevanju ukrepov znotraj držav članic EU, saj raznolike ali neusklajene pobude posameznih držav članic ne morejo biti učinkovite, po drugi strani tudi ne pripomorejo k vzpostavljanju zaupanja v prilagodljivost predpisov o varstvu osebnih podatkov ali celo v splošno stanje varstva osebnih podatkov v posameznih državah članicah. S tem namenom je Evropska Komisija sprejela priporočila glede uporabe tehnologij in podatkov za boj proti epidemiji koronavirusa[5], v katerih se opredeljuje do rešitev, ki bi lahko bile v tem okviru učinkovite, in glede varovalk, ki morajo biti vpeljane za varstvo pravic posameznikov. V smislu še izrazitejšega skupnega evropskega pristopa je smernice o obdelavi podatkov o lokaciji in orodjih za sledenje stikom v okviru izbruha COVID-19[6] izdal tudi Evropski odbor za varstvo podatkov (EDPB), ki ga sestavljajo predstavniki nacionalnih organov za varstvo podatkov in Evropski nadzornik za varstvo podatkov.

Izhajajoč iz zgoraj navedenih načel učinkovitosti, potrebnosti in sorazmernosti ima uporaba ukrepov, ki temeljijo na anonimnih podatkih, vsekakor prednost pred uporabo surovih podatkov, saj je nedopustno posegati v pravico do zasebnosti posameznikov, če določen cilj (zagotovitev javnega zdravja) lahko dosežemo z manj invazivnim posegom, kot je uporaba anonimnih podatkov (kar pomeni, da se Splošna uredba o varstvu podatkov in ZVOP-1 ne uporabljata), še posebej če govorimo o uporabi lokacijskih podatkov ali podatkov o zdravstvenem stanju. Ključno vprašanje je sicer, ali je, še posebej pri uporabi lokacijskih podatkov, anonimnost le teh sploh možno zagotoviti. Vsa tveganja v povezavi z anonimizacijo so zelo dobro razdelana v **smernicah EDPB glede anonimizacijskih metod in tehnik**[7].

V kolikor zasledovanega cilja ukrepa ni mogoče doseči na podlagi anonimnih podatkov, temveč le z uporabo osebnih podatkov, je treba dosledno upoštevati določbe Splošne uredbe o varstvu podatkov in ZVOP-1. Kot izhodišče in orodje za pravočasno identifikacijo tveganj in za sprejem ustreznih ukrepov za obvladovanje tveganj, s čimer lahko upravljavci preprečijo, da bi prišlo do kršitve zakonodaje s področja varstva osebnih podatkov, Informacijski pooblaščenec izpostavlja nujnost izvedbe **ocene učinkov v zvezi z varstvom podatkov** (člen 35 Splošne uredbe o varstvu podatkov) z jasnimi tehničnimi parametri predlagane tehnične rešitve (aplikacije).

Osebni podatki morajo biti obdelani **zakonito, pošteno in na pregleden način** (člen 5(1)(a) Splošne uredbe o varstvu podatkov), kar pomeni, da mora za ob-

delavo podatkov preko aplikacije obstajati **jasna pravna podlaga**, določena v členu 6 Splošne uredbe ter (v primeru obdelave posebnih vrst osebnih podatkov, npr. zdravstvenih) v členu 9 Splošne uredbe o varstvu podatkov. V primeru obdelave lokacijskih osebnih podatkov (npr. lokacija mobilnega telefona) je treba upoštevati tudi Zakon o elektronskih komunikacijah, ki postavlja določene omejitve za obdelavo podatka o lokaciji uporabnika terminalne opreme oz. pametnega telefona. Preglednost obdelave so upravljavci dolžni zagotoviti na način, da posameznikom podajo **izčrpne in jasne informacije** (člena 13 in 14 Splošne uredbe o varstvu podatkov). Ta del je ključen pri vzpostavljanju zaupanja v tehnološko rešitev kot ukrep in krepitev »legitimnosti« le tega. V povezavi s tem mora biti posameznikom zagotovljeno tudi izvajanje pravic v zvezi s podatki, ki se nanašajo nanje (členi 15 do 22 Splošne uredbe).

Osebni podatki smejo biti zbrani le za **določene, izrecne in zakonite namene** ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni (člen 5(1)(b) Splošne uredbe o varstvu podatkov). V tem okviru je potrebna skrbna presoja, ali je predlagana tehnična rešitev ustrezna in učinkovita pri zasledovanju opredeljenega cilja (zajezitev širjenja epidemije), pri čemer ima tu ključno vlogo epidemiološka in širša zdravstvena stroka, ki lahko poda ustrezno oceno. Sem sodi tudi presoja **najmanjšega možnega obsega podatkov**, s katerim je možno doseči zasledovani namen (člen 5(1)(c) Splošne uredbe o varstvu podatkov).

Pomembno je zagotoviti **točnost osebnih podatkov, in kadar je to potrebno, njihovo posodobitev** (člen 5(1)(d) Splošne uredbe o varstvu podatkov).

Eden izmed ključnih elementov je **določitev roka hrambe**, ki mora ustrezati opredeljenemu namenu obdelave podatkov (člen 5(1)(e) Splošne uredbe o varstvu podatkov), saj je ena izmed resnih nevarnosti tovrstnih aplikacij in podatkov, ki se hranijo v njih, nevarnost kasnejše uporabe za druge namene (npr. za izvajanje ukrepov na podlagi odločbe o karanteni, čeprav podatki niso bili zbrani za ta namen ipd.).

Osebni podatki morajo biti nenazadnje obdelani na način, ki zagotavlja njihovo **varnost** (člen 5(1)(f) Splošne uredbe o varstvu podatkov), vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi. Prav zagotavljanje varnosti tehnoloških rešitev je lahko »žrtev« preuranjenih in slabo premišljenih ukrepov, k čemur posamezne razvijalce aplikacij sili nujnost razvoja in čimprejšnje implementacije določene rešitve. V povezavi z varnostjo podatkov se najpogosteje omenja (in v zadnjem času tudi razdvaja raziskovalce in razvijalce rešitev) tudi t.i. centralizirana (npr. podatke centralno hrani zdravstvena institucija, odgovorna za obvladovanje epidemije) oz. decentralizirana hramba osebnih podatkov (na posameznikovi napravi), predvsem z vidika možnosti zlorab in uporabe podatkov za drug namen.

Sklepno

Kljub uspešni omejitvi širjenja koronavirusa, obeti glede vrnitve v duh časa pred njim, niso pozitivni in kot kaže, bodo določeni ukrepi za njegovo zajezitev, postali del našega vsakdana. Prav zaradi tega je še kako pomembno, da smo ob vsakokratni presoji potrebnosti, nujnosti in učinkovitosti določenega ukrepa, sposobni ohranjati krhko ravnovesje med pravico do zasebnosti in poskusi njene omejitve, ki se nehote zgodi v zasledovanju cilja zagotavljanja javnega zdravja. Saj vemo, »pot v pekel je tlakovana z dobrimi nameni«.

[1] https://covid-19-stats.si/, pridobljeno 13.5.2020.

[2] https://www.virustracker.si/, pridobljeno 13.5.2020.

[3] https://privacyinternational.org/examples/tracking-global-response-covid-19, pridobljeno 13.5.2020.

[4] https://lsts.research.vub.be/en/corona-apps, pridobljeno 13.5.2020.

[5] PRIPOROČILO KOMISIJE (EU) 2020/518 z dne 8. aprila 2020 o skupnem naboru orodij za uporabo tehnologije in podatkov za boj proti krizi zaradi COVID-19 in izhod iz nje, zlasti v zvezi z mobilnimi aplikacijami in uporabo anonimiziranih podatkov o mobilnosti, Uradni list Evropske Unije, L 114/7, z dne 14.4.2020, https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32020H0518&from=EN.

[6] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[7] Delovna skupina za varstvo podatkov iz člena 29, Mnenje št. 5/2014 o anonimizacijskih tehnikah, sprejeto 10.4.2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sl.pdf. ■





V kibernetsko varnost vložili več sredstev kot kdorkoli drug

Kot vodilni svetovni ponudnik IKT infrastrukture in pametnih naprav, ima Huawei Technologies aktivno vlogo tudi pri digitalni preobrazbi industrij s ciljem, da digitalizacija doseže vsakega posameznika, dom in organizacijo. Naši prednostni nalogi ostajata zagotovitev kibernetske varnosti in zaščita zasebnosti, zato smo vzpostavili celovit sistem, ki vsem uporabnikom zagotavlja kibernetsko varnost.

Zadnja tri desetletja uspešno ohranjamo zelo dobre rezultate na področju varnosti. Huawei je vodilni ponudnik in oblikovalec rešitev izboljšane varnosti 5G omrežij. Mednarodnim organizacijam smo zagotovili več pomoči in sredstev kot kdorkoli drug, prav tako pa smo prispevali največ predlogov s področja varnosti 5G omrežij, ki jih je industrija tudi sprejela. Na primer, združenje 3GPP je sprejelo kar 385 Huaweijevih predlogov, kar predstavlja 24,6 odstotka vseh predlogov sprejetih v letu 2019. S tem je Huawei prispeval največji delež predlogov s področja varnosti.

Huawei aktivno sodeluje tudi pri standardizaciji telekomunikacijske kibernetske varnosti, ki jih vodijo ITU-T, 3GPP in IETF, ter se pridružil varnostnim organizacijam kot je FIRST. Huawei za zagotovitev kibernetske varnosti svojih strank in pospeševanja zdravega razvoja industrije sklepa partnerstva z vodilnimi podjetji s področja varnosti.

Pri potrebah kibernetske varnosti in zasebnosti v naše procese vključujemo najboljše prakse, izhodišča, politike in pravila. Zaradi tega je kibernetska varnost in zaščita zasebnosti v središču vsakodnevnega poslovanja družbe Huawei.

Postavitev in celovita izvedba globalnega sistema zagotavljanja kibernetske varnosti in zaščite zasebnosti je ena izmed ključnih strateških usmeritev družbe Huawei. Pri tem se navezujemo na najboljše prakse v industriji za izgradnjo sistema, ki je trajnosten, zanesljiv in skladen z veljavnimi zakoni ter mednarodnimi telekomunikacijskimi standardi. Huawei odprto sodeluje z vladami, strankami in partnerji pri reševanju izzivov kibernetske varnosti in zasebnosti ter izpolnjevanju njihovih zahtev.

Več: https://www.huawei.com/en/sustainability/stable-secure-network/cyber-security.

HUAWEI

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



INFORMACIJSKA VARNOST V LUČI PANDEMIJE COVID-19

Zaradi vse večje zaskrbljenosti zaradi izbruha novega koronavirusa (COVID-19) in potencialnega vpliva na poslovanje po vsem svetu, je informacijska varnost v odločilnem zgodovinskem trenutku. Hitra in nepričakovano obsežna motnja na organizacije po vsem svetu nas je potisnila v položaj, kjer se borimo za ohranjanje varnosti in hkrati neprekinjenega poslovanja. Da bi organizacije ostale kompetentne in konkurenčne, so se bile primorane reorganizirati ter prilagoditi hibridnemu okolju, ki nam prinaša večjo odvisnost od sodelavcev, ki delajo od doma ter zunanjih partnerjev. To pa ima seveda lahko varnostne posledice. Pogledali si bomo nekaj ključnih nasvetov, ki se tičejo CISO, CIO, in lastnikov podjetij.

Pomembno je, da ponovno ocenite svojo izpostavljenost kibernetskim grožnjam. Napadalci bodo še naprej in še bolj poskušali izkoriščati spremenjene delovne procese, prilagojene delovne ureditve in seveda iskali človeške napake pri ranljivih zaposlenih, kot najšibkejšemu členu varnostne verige. Priporoča se revidiranje vseh nedavnih sprememb tehnične arhitekture ter infrastrukture. Pregledati je potrebno v naglici sprejete odločitve, ki so zagotovile in zagotavljajo dostopnost oddaljenih storitev, kot posledic potrebe dela na daljavo.

Uskladiti je potrebno neskladja s pravnimi in regulativnimi zahtevami. Potrebno je razumeti, kako spremenjeni in prilagojeni varnostni ukrepi vplivajo na skladnost organizacije s pravnimi zahtevami, kot npr. zaščita osebnih podatkov.

Potrebno je identificirati skrite stroške, ki lahko nastajajo pri tovrstnih spremembah.

Prav tako je potrebno revidirati posledice dobavnih verig. Spremljanje dobaviteljev in vplivov pandemije na njihovo poslovanje je ključno za zagotavljanje ne motene dobave storitev, ter identifikacijo potencialnih izpadov in zmanjšanega obsega nudenih storitev s strani dobaviteljev. Prav tako se je potrebno zavedati možnosti prenehanja poslovanja določenih zunanjih sodelavcev, zaradi posledice trenutne krize, ter vplive, ki se lahko posledično pokažejo v naših organizacijah.

Znova preučite varnostne politike in ozaveščenost. Predpostavljajmo, da bodo elementi COVID-19 vztrajali in se posledično pokazali v trajno spremenjenem vedenju celotne delovne sile. Pripravljeni moramo biti na naslednjo krizo z načrtovanimi scenariji, ko bodo skladni s trenutnimi trendi in kljubovali potencialnim nevarnostim. Posodobite svoje strategije in jih prilagodite za boljše spopadanje z vplivom na poslovanje podjetja v luči potencialno prihajajočih dogodkov, ki povzročajo široko razširjenost motenj pri izvajanju bistvenih operacij. Preverite ali je med drugim zagotovljeno zadosti finančnih sredstev za zagotavljanje potrebnih zaščitnih ukrepov za kritična digitalna sredstva.

Pomembno je, da ponovno ocenite svojo izpostavljenost kibernetskim grožnjam. Napadalci bodo še naprej in še bolj poskušali izkoriščati spremenjene delovne procese, prilagojene delovne ureditve in seveda iskali človeške napake pri ranljivih zaposlenih, kot najšibkejšemu členu varnostne verige.

*avtor je član Slovenskega združenja korporativne varnosti

Priporočila in nasveti:

- Dosledno skrbite za varnostne kopije podatkov, tako v oblaku, kot na lokalnih medijih, ki naj bodo ustrezno zaščitene in shranjene neodvisno od sistema,
- Dvignite nivo varnosti v svojih domačih okoljih in omrežjih,
- Pred vsako spletno prijavo preverite ali ste na legitimnem spletnem mestu,
- Uporabljajte močna gesla s kombinacijo velikih in malih črk, številk ter posebnih znakov,
- Redno preverjajte za posodobitve programske opreme,
- Skrbite, da imate na napravah vedno nameščeno najnovejšo protivirusno programsko opremo,
- Revidirajte nastavitve varnosti in zasebnosti tako v svojih napravah, kot na računih na socialnih omrežjih,
- Ne odpirajte sumljivih e-poštnih sporočil ali pripadajočih priponk,
- Prenašajte aplikacije ali drugo programsko opremo samo z zaupanja vrednih platform,
- Pogovorite se s svojimi bližnjimi, vključno z otroci, o tem, kako ostati varen na spletu,
- Če menite, da ste žrtev kaznivega dejanja, kot vedno, obvestite pristojne organe.

Orodja za komuniciranje preko spleta

Vsi se poslužujemo takšnih ali drugačnih programskih rešitev, ki nam omogočajo komuniciranje in sestankovanje na daljavo preko svetovnega spleta. Tukaj je potrebno poudariti, da niso vse rešitve zaščitene z enako stopnjo varnosti. Težko se je odločiti za najbolj varno, vendar pa je potrebno izpostaviti, da imata tako **Skype** kot **Zoom** zgodovino več varnostnih pomanjkljivosti, za katere so bili prav tako izdani varnostni popravki; ne zaščiteni klici, prodaja podatkov svojih uporabnikov tretjim osebam, idr. Priporočamo izogibanje uporabe **Google Hangouts**, **Facebook Messenger** ter **Whatsapp** aplikacij, ker imajo skoraj neobstajajočo politiko zasebnosti, niso odprto kodni, poskusi slabenja šifriranja, zgodovina odlivov informacij, primarna tarča hekerjev, idr. Verjetno v to kategorijo spada tudi katera druga prej ne omenjena aplikacija. Predvsem je pomembno, da se dobro pozanimamo o ozadju in celovitosti delovanja programske rešitve, ki jo uporabljamo za komuniciranje v poslovne ali privatne namene.

Kot predlog lahko omenim **Jitsi Meet** (https://meet.jit.si/). Gre za spletno aplikacijo, ki jo uporablja tudi vsem poznani Edward Snowden. Šifriranje uporablja od konca do konca (ang. End-to-End), za uporabo ne potrebujete nikakršnih uporabniških računov. Ob vsaki seji, ki ima po privzetem kompleksno ime, se ta zaščiti še z geslom. Poleg zgoraj omenjene aplikacije, se lahko poslužimo tudi uporabe mobilne aplikacije **Signal** (https://www.signal.org/) ali **Telegram** (https://telegram.org/), ki sta odprtokodni aplikaciji za pošiljanje sporočil in vzpostavitev glasovnega klica na mobilnih napravah. Signal je aplikacija,





ki jo prav tako uporablja Edward Snowden. Slabost teh mobilnih aplikacij je, da jo morata imeti tako pošiljatelj/klicatelj, kot prejemnik nameščeno na napravi.

COVID-19 kot vzvod hekerjev

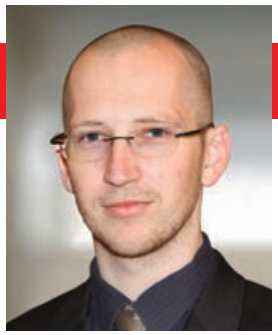
Hekerske skupine izkoriščajo pandemijo COVID-19 kot del svojih kibernetskih operacij. Ti akterji se pogosto navzven predstavljajo kot zaupanja vredni subjekti. Njihova dejavnost vključuje uporabo phishing tehnike socialnega inženiringa, ki je tesno povezana s koronavirusom (COVID-19). Končni cilj je enak kot pri vseh kibernetskih napadih, to sta vohunjenje ter kraja podatkov. Kibernetski kriminalci uporabljajo pandemijo za dobičkonosne koristi. Razvijajo različne kripto viruse in druge zlonamerne programske kode.

Opaža se porast lažnega predstavljanja z uporabo tematike koronavirus ali COVID-19 kot vaba. Prav tako je v porastu distribucija zlonamerne programske opreme z uporabo tovrstne tematike. Tudi registracija novih domen, ki vsebuje besedila povezana s koronavirusom ali COVID-19 niso izvzeta iz tega trenda. Zlonamerni kibernetski kriminalci se zanašajo na osnovne metode socialnega inženiringa, da uporabnika zavedejo, da izvrši določeno dejanje njim v korist. Ti akterji izkoriščajo človeške lastnosti, kot so človeška radovednost, naivnost, zaupljivost in skrb glede pandemije koronavirusa. Gre za psihološko umetnost napadanja človeške komponente, ki bo vedno najšibkejši člen v varnostni verigi. Dokler bo človek del organizacije, bo vedno najbolj ranljiva tarča ravno on.

Da bi napadalci ustvarili vtis pristnosti, lahko v e-poštnem sporočilu ponaredijo podatke o pošiljatelju, da se na prvi pogled zdi, da prihaja iz zaupanja vrednega vira, na primer Svetovna zdravstvena organizacija (WHO) ali posameznik z »dr.« titulo v svojem nazivu. V več primerih akterji pošiljajo phishing e-poštna sporočila, ki vsebujejo povezave do ponarejene strani za prijavo po e-pošti.

Zaposleni so prva obramba vaše organizacije. Podjetja se lahko zaščitijo tako, da spodbudijo zaposlene h skeptičnosti in previdnosti. Skupine za informacijsko varnost bi morale sodelovati s skupinami za upravljanje s tveganji, da bi usklajevale aktivnosti odkrivanja ter odzivanja na novo nastale grožnje. Nikakor pa ne smemo zanemariti konstantnih preverjanj varnosti informacijskih sistemov in odkrivanja varnostnih ranljivosti. Še posebej pride to do izraza v kriznih situacijah, ko zaradi neprekinjenosti izvajanja poslovnih procesov, uporabljamo različne pristope delovanja. Primer zadnje krizne situacije je to vsekakor povečan obseg dela izven lokacij našega podjetja. ■

Avtor: mag. Matjaž Drev / Nacionalni inštitut za javno zdravje*



INFORMACIJSKA VARNOST PO EPIDEMIJI

V tem nenavadnem in za marsikoga kaotičnem času so se zastavljala ključna družbeno politična vprašanja: kdo je in kdo ni kriv, kaj bi lahko naredili, kaj smo naredili, smo bili pripravljeni, smo se ustrezno odzvali, kdaj bo konec epidemije, kakšen bo svet jutri?

Svet se je v zadnjih mesecih soočal z nevarnostjo, ki v širši perspektivi zgodovine ni nova, a smo nanjo skoraj pozabili – epidemijo nalezljive bolezni. Tokrat se imenuje COVID-19, povzroča jo nov koronavirus SARS-CoV-2, znaki so podobni kot pri pljučnici. Nov koronavirus je bil januarja 2020 potrjen v kitajskem mestu Wuhan, nato se je po zaslugi mednarodnega potniškega prometa zelo hitro razširil še v Evropo in ZDA. Na območju EU je prvo in glavno žarišče postala Italija, ki se na začetku ni dovolj resno lotila omejevanja širjenja bolezni. Slovenija je v tem pogledu ravnala precej bolj odločno. 12. marca je bila razglašena epidemija, dosledno so se začeli izvajati čedalje strožji ukrepi: stroge omejitve pri prečkanju državne meje, omejevanje gibanja med občinami, obvezno nošenje mask v trgovinah, prepoved zbiranja na javnih krajih, prepoved izvajanja gostinskih, turističnih in številnih drugih dejavnosti – za dva meseca je javno življenje zamrznilo. Tak pristop je ubrala večina evropskih držav.

Čas za trezen premislek

Čeprav so nove (upajmo, začasne) razmere za večino neprijetne in za nekatere tragične, je pomembno, da močna čustva – zaskrbljenost, strah, paniko – potisnemo ob stran in situacijo pogledamo kolikor mogoče neprizadeto. Zato, da ocenimo ali smo se kot družba pri zagotavljanju varnosti prebivalcev ustrezno odzvali. In zato, da se zdaj, ko imamo več izkušenj, pripravimo na morebitne hujše scenarije. Za boleznijo COVID-19 je zaenkrat po svetu umrlo skoraj 300.000 ljudi, kar ni malo, toda številka še zdaleč ne dosega pandemičnih razsežnosti kuge, španske gripe ali črnih koz, ki so v preteklosti prav tako pustošile po Evropi.

Ključno vprašanje torej je ali smo se na nove razmere pravočasno, ustrezno in dovolj uspešno prilagodili. Splošen odgovor bi moral biti pritrdilen.

Glede na trenuten razvoj dogodkov (število okuženih, ki umrejo, pospešen razvoj cepiva, ukrepi za upočasnjevanje širjenja okužbe) je mogoče domnevati, da si bo svet v letu ali dveh opomogel od nove bolezni in da kljub precejšnji gospodarski škodi zahodna družba še ne bo doživela svojega zatona. To pa ne pomeni, da je nevarnosti konec. Prav nasprotno, verjetno je le vprašanje časa, ko se bo pojavil nov virus, ki bo bistveno bolj smrtonosen. Zato je zdaj najbolj primeren čas, da ocenimo (ne)učinkovitost izvedenih ukrepov in razmislimo kaj storiti, da bomo naslednjič bolje pripravljeni.

Človek je prilagodljiva žival

Ključno vprašanje torej je ali smo se na nove razmere pravočasno, ustrezno in dovolj uspešno prilagodili. Splošen odgovor bi moral biti pritrdilen. Politični sistem ni razpadel, čeprav so se zamenjali nekateri predstavniki. Gospodarstvo se ni zdrobilo, čeprav je vrednost borznih indeksov skokovito padla. Ljudje kljub prisilni osamitvi niso zabredli v kolektivno psihozo. To seveda ne pomeni, da žrtev ni: zaradi zamrznitve gospodarstva so številni ekonomsko propadli, zaradi bolezni so nekateri umrli.

Po drugi strani je v kontekstu rabe informacijske tehnologije ta čas prinesel nekatere nove uvide. Kot posamezniki in kot družba smo bili prisiljeni uporabljati informacijske storitve, ki smo se jim sicer izogibali ali jih uporabljali v omejenem obsegu. Tokrat je v ospredje stopilo spletno poslovanje, naročanje izdelkov na dom, virtualni dogodki (od sestankov do porok), učenje in delo od doma. V praksi se je pokazalo, da lahko velik del tega, kar razumemo kot »službo«, »šolo« in »druge storitve«, v množičnem obsegu izvajamo od doma. In da vse to deluje. V veliki meri zato, ker smo bili kot družba sorazmerno dobro informatizirani. Zanimivo bo opazovati ali se bomo po normalizaciji razmer znova vrnili v stare vzorce dela v pisarni in šolanja v učilnici. In če da, zakaj?

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



BYOD v praksi

Pred leti se je zelo pogosto govorilo o konceptu »BYOD« (ang. Bring Your Own Device), ki označuje rabo zasebnih informacijskih naprav (računalnikov, tablic, telefonov in drugih bolj ali manj pametnih dodatkov) v delovnem okolju. Osnovna ideja je bila, da se ekosistem delovne organizacije dopolni z zasebnimi informacijskimi napravami. Zagovorniki so poudarjali prednosti takšnega hibridnega pristopa (delo od doma, boljša uporabniška izkušnja, manj stroškov za delodajalca), nasprotniki pa so opozarjali na nova varnostna tveganja, ki jih prinaša službena raba zasebnih naprav (manj nadzora nad varovanjem informacij, razdrobljena varnostna politika, novi vektorji napada).

Na srečo je »koronakriza« pokazala predvsem prednosti uporabe zasebnih naprav v službenih in šolskih okoljih. Zasebne računalnike, tablice in telefone smo dovolj uspešno vpeli v delovne in učne procese, da so se ti bolj ali manj posrečeno preselili iz fizičnega v virtualni svet. To seveda odpira številne varnostne izzive, ki jih bo prej ali slej treba reševati – če ne drugače v situaciji, ko bo namesto epidemije svet morda pretresala kibernetska vojna.

Kaj torej storiti? Izkušnje so pokazale, da je kombinirana uporaba službenih in zasebnih informacijskih sredstev lahko zelo koristna, omogoča namreč bistveno bolj učinkovito prilagajanje na nepredvidljive razmere. Hkrati odpira nova varnostna tveganja, ki znova poudarjajo pomen dobrih osnov: posodobljene protivirusne zaščite, požarnih zidov, varnostnih kopij podatkov, vse bolj pa tudi varnih (VPN) povezav, ki omogočajo šifriran prenos podatkov med centralno in oddaljenimi lokacijami. V jedru nič novega: preizkušeni recepti, ki jih poznamo, vendar bi jih morali – množična uporaba zasebnih naprav v službene namene to le še potrjuje – dosledno izvajati na kolektivni ravni. To je izziv, ki ga moramo naslavljati vedno znova. Tudi zato, ker je zgolj vprašanje časa, kdaj nas bo doletela nova kriza – tokrat ne nujno v obliki epidemije, ampak morda množičnih napadov na informacijsko infrastrukturo.

Izkušnje so pokazale, da je kombinirana uporaba službenih in zasebnih informacijskih sredstev lahko zelo koristna, omogoča namreč bistveno bolj učinkovito prilagajanje na nepredvidljive razmere.

Viri

- Nacionalni inštitut za javno zdravje: https://www.nijz.si/sl/koronavirus-2019-ncov
- Vlada RS: https://www.gov.si/teme/koronavirus/
- Univerza Johns Hopkins: https://coronavirus.jhu.edu/map.html
- Dnevnik: https://www.dnevnik.si/1042686275 ■

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

Avtorji: Matjaž Tavčar, Simon Hercog, Bojan Peršl /
Služba za korporativno varnost, Univerzitetni klinični center Ljubljana*

DELOVANJE KRITIČNE INFRASTRUKTURE V ČASU EPIDEMIJE – PRIMER UKC LJUBLJANA

Univerzitetni klinični center Ljubljana (UKCL) je osrednja zdravstvena ustanova v Republiki Sloveniji. UKCL predstavlja kritično infrastrukturo saj je ključnega pomena za državo, tudi s področja obrambe, zaščite in reševanja. Posledično je zakonsko obvezana pripravljati ustrezne načrte delovanja in varovanja, ki izhajajo iz področnih zakonov in uredb.

Med tveganji s katerimi se lahko UKCL sreča, so seveda poleg potresov, požarov, terorističnih napadov, stavk, tudi epidemije. Izkustveno smo se redno srečevali z epidemijo gripe, tako smo načrte na nivoju zavoda, kot države koncipirali za primer te epidemije in so se, kot tak izkazali za uporabne.

Prejšnji generalni direktor UKCL, Aleš Šabeder, je imel v letu 2018 posluh za oblikovanje Službe za korporativno varnost UKCL, ki se je dejansko oblikovala 1.1.2019. Ob ustanovitvi njena vloga ni bila vsebinsko povsem dorečena, se je pa tekom leta 2019 oblikovala in dopolnjevala. Služba za korporativno varnost je prevzela področja obrambe, zaščite, reševanja in varovanja zavoda. Prav tako je prevzela nadzor nad izvajanjem in spoštovanjem internih aktov, kot na primer povračila stroškov prevoza na delo, upravičenosti bolniških staležev, delovanja Civilne zaščite, koordinacija dela s Policijo in Slovensko vojsko in podobno. Izkušnje z delovanja na omenjenih področjih so nam v primeru epidemije COVID-19 prišle zelo prav.

V okviru revitalizacije delovanja Civilne zaščite UKCL smo maja 2019 prečistili zaloge zaščitnih sredstev in zdravil, ter vzpostavili delovanje centralnega zaklonišča in Štaba Civilne zaščite UKCL. Glede na podatke, ki smo jih dobivali s terena, smo na sestankih z državnimi službami, ki delujejo na varnostnem področju, preverjali stopnjo tveganja za prenos okužb ošpic in garij (oboje sta virusni obolenji) zaradi ilegalnih migracij. Ker smo bili tudi v UKCL deležni okužbe z ošpicami, smo se pospešeno pripravili na morebitno karanteno in temu primerno nabavili zaščitno opremo. Prav tako smo začeli s prenovo načrtov delovanja ter v tem sklopu pripravili Strategijo varovanja UKCL z izvedbenimi načrti in na podlagi Zakona o kritični infrastrukturi tudi Oceno tveganja delovanja kritične infrastrukture s predlogi stalnih in začasnih ukrepov za neprekinjeno delovanje le – te.

V oktobru 2019 smo v Izobraževalnem centru Uprave Republike Slovenije za zaščito in reševanje na Igu organizirali razširjen posvet na temo načrtov delovanja bolnišnic v primeru prihoda večjega števila obolelih ali poškodovanih (masovna nesreča, epidemija). Posveta so se udeležili poleg ključnih predstavnikov UKCL tudi predstavniki Policije (z vseh nivojev), Centra za zaščito Mestne občine Ljubljana, gasilcev, Ministrstva za zdravje, SB Celje in UKC Maribor ter Civilne zaščite Republike Slovenije. Dvodnevni posvet je bil izjemno uspešen in odlična podlaga za to, kar nismo vedeli, da nas čaka.

Žal niso vsi prisotni povsem resno vzeli zaključkov posveta ali pa so jih preslišali. Velika večina pa je sledila dogovorjenemu in tako smo bili v UKCL, Policiji, Civilni zaščiti in nekaterih bolnišnicah nehote pripravljeni na COVID-19.

Izziv delovanja bolnišnice v primeru epidemije ni samo zdravstveni. V primeru epidemije je potrebno bolnišnico »zapreti«,

> COVID-19 pa je imel precej koristnih stranskih učinkov med katerimi velja izpostaviti izjemno odzivnost za vzpostavitev tehničnega varovanja, spoznavanje odziva sodelavcev v času krize in pravih partnerjev.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



prepoved obiskov nadzorovati, izhode pacientov prepovedati in vse to z varnostno službo nadzorovati.

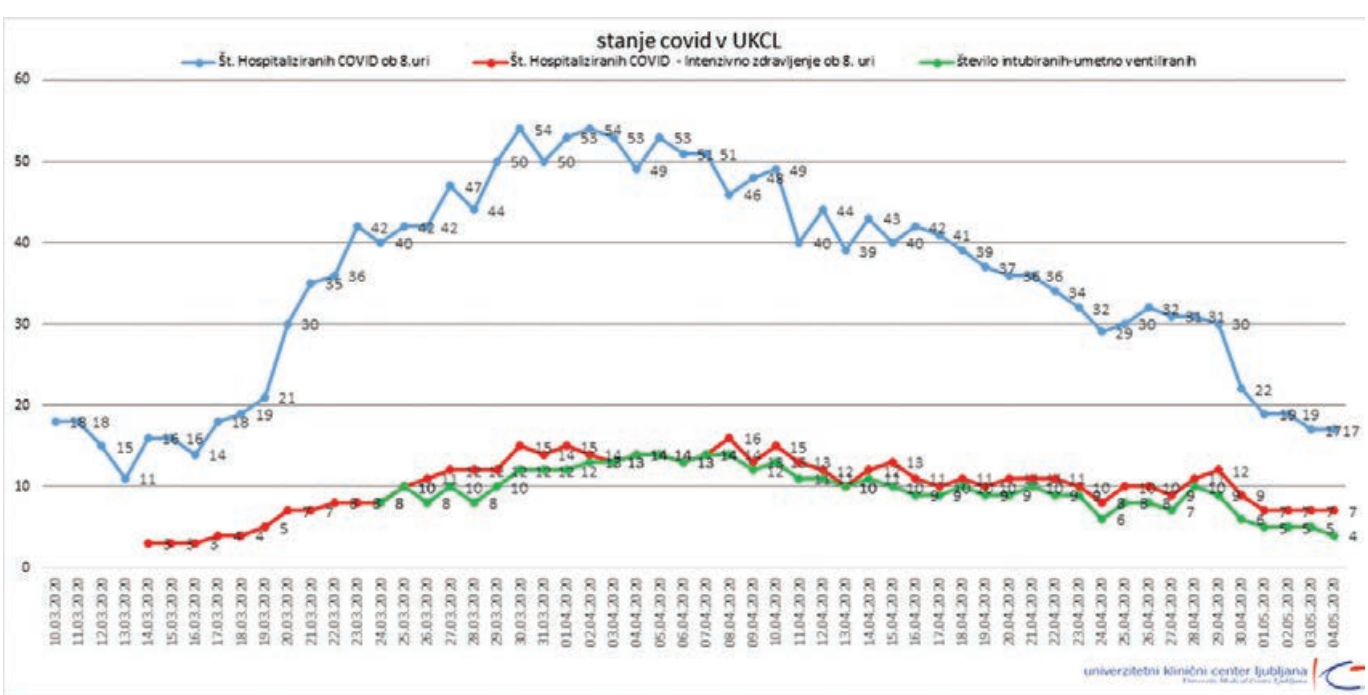
Dne 4.3.2020 smo organizirali strokovno srečanje s kolegijem direktorja Policijske uprave Ljubljana, ki je bilo načrtovano pred izbruhom epidemije, vendar je tako dobilo pomembno konotacijo glede uporabe prave in primerne zaščitne opreme ter morebitnega delovanja Policije, tako za zaščito UKCL, kot za preprečitev okužb znotraj policijskih vrst. In prav na ta dan smo potrdili tudi prvo okužbo z virusom COVID-19 v Sloveniji.

Že konec februarja so, na podlagi ocen Službe za preprečevanje bolnišničnih okužb, stekle priprave na delovanje UKCL v času pričakovane epidemije, ki so bile razdeljene na tri faze. V prvi fazi smo prepovedali vse obiske ter z zaprtjem vhodov omejili vstop v ustanovo na minimum. Na vhodih smo vzpostavili zdravstveni nadzor (merjenje temperature in preverjanje simptomov) in presenetljivo, da zaposleni tem ukrepom niso nasprotovali, temveč ravno nasprotno.

Ob ukinitvi nenujnih posegov in zapiranju klinik, kjer ni nujnih obravnav (ortopedska, dermatološka, stomatološka klinika) smo zagotovili potrebno število postelj za morebitne bolnike COVID-19+. Takoj na začetku, kot ob vsaki epidemiji gripe, je problem predstavljalo število ventilatorjev (respiratorjev) za mehansko predihavanje. Slovenija se s tem problemom srečuje že vsaj deset let in ga do sedaj ni uspela rešiti. Tako zgodbe o morebitnem »odklapljanju« pacientov niso povsem iz trte izvite. K sreči je Vlada sprejela potrebne ukrepe za zaustavitev širjenja okužbe in s tem razbremenila pritisk na zdravstveni sistem, ki je ob začetku razpolagal s 179 respiratorji za vse potrebe, ne samo COVID-19.

Ob vsem je potrebno imeti v mislih tudi logistiko, prevoze obolelih s sumom na okužbo v reševalnih vozilih ter potrebne zaščitne ukrepe. Že kmalu po začetku epidemije se je izkazalo, da ne moremo izvajati »taxi prevozov« pacientov na testiranje, saj je razkuževanje vozil preveč dolgotrajno (dve uri). Odločili smo se za prevoz ekip za testiranje na dom obolelega. Predvidevali smo, da lahko v času zaprtja pride do incidentov, kot na primer, da bodo državljani sami prihajali na infekcijsko kliniko in zahtevali testiranje, kar bi bilo ob večjem številu težko obvladovati. Hkrati pa smo predvidevali tudi nenadzorovan prihod pacientov na urgenco, ki bi želeli obravnavo za nenujno zdravstveno oskrbo. Kot smo na začetku pričakovali, smo imeli nekaj manjših incidentov, zato smo v sodelovanju s Policijo pripravili načrt nadzornih točk za dostop do UKCL, s katerimi bi preprečili dovoz do urgence in Infekcijske klinike. Tega načrta nam k sreči ni bilo potrebno uporabiti, imamo pa ga.

Gibanje številk:





v takih razmerah in v zaščitni opremi (skafandri, maske,…) je bilo in je izjemno naporno. Že v samem začetku se je pokazala potreba po psihološki pomoči zaposlenim, ki je UKCL formalno ni imel vzpostavljene. V sodelovanju s psihologinjami Generalne policijske uprave nam je v trenutku uspelo zagotoviti pomoč zaposlenim in hkrati vzpostaviti pomoč preko naših psihologinj, ki so primarno namenjene pomoči bolnikom. Ta pomoč je bila izjemnega pomena za nadaljnje delovanje ustanove.

Zanimivo je, da smo imeli največ težav z zaposlenimi na organizacijskih enotah, kjer praviloma ne obravnavajo urgentnih stanj in jih je ta epidemija najbolj »prizadela«, čeprav z bolniki COVID-19 pravzaprav niso imeli opravka, imeli pa so čas.

COVID-19 pa je imel precej koristnih stranskih učinkov med katerimi velja izpostaviti izjemno odzivnost za vzpostavitev tehničnega varovanja, spoznavanje odziva sodelavcev v času krize in pravih partnerjev. Tu so se izkazali Policija, Civilna zaščita, Mestna občina Ljubljana, ponudniki namestitev v Ljubljani, ki so zagotovili stanovanja za naše zaposlene, Občina Kranjska Gora, ki je sprejela naše COVID-19+ bolnike brez simptomov in še nekateri. Vsem smo neizmerno hvaležni.

Ker je bila v času epidemije povečana potreba po samozaščitni opremi, smo se srečali tudi z odkloni, kot je tatvina zaščitne opreme. V sodelovanju s Policijo smo tatvine uspešno preiskali in osumljene tudi kazensko ovadili.

Celovito gledano se je izkazalo, da je korporativna varnost tista, ki lahko v kriznem trenutku ali času poveže vse potrebne deležnike in s tem ustvari odlično povezovalno in motivirano, ter k rezultatom usmerjeno delo vseh.

Celovito gledano se je izkazalo, da je korporativna varnost tista, ki lahko v kriznem trenutku ali času poveže vse potrebne deležnike in s tem ustvari odlično povezovalno in motivirano, ter k rezultatom usmerjeno delo vseh. Nikoli v tem času nismo slišali stavka, ki ga sicer pogosto: »To se ne da, to ni mogoče«.

In očitno je marsikaj mogoče. Edino kar nam ostane je, da pomen korporativne varnosti v kritični infrastrukturi prepozna tudi država, ki v času krize na marsikaterem področju ni bila pripravljena. In da obudimo sistem zaščite po načelu »Nič nas ne sme presenetiti«. ■

Avtorica: Alenka Glas / višja svetovalka, PRO.astec d.o.o.

NEPREKINJENO POSLOVANJE V ČASU ZDRAVSTVENE KRIZE

Zdravstvena kriza, povzročena zaradi COVID-19, nas je na neprijeten način opomnila, da je pripravljenost na drugačno izvajanje poslovnih procesov nujnost za vsako organizacijo. Mnogo je bilo zapletov in nerazumevanja in marsikdo sedaj bolje ve, kako bi se morala organizacija odzivati v primeru krize. Preden to pozabimo, preden se spet zgodi nepričakovano, bi morala vsaka organizacija svoja spoznanja in vedenja strukturirano dokumentirati. Samo tako lahko nova spoznanja uporabi še kdaj. Pravi odziv je priprava načrtov neprekinjenega poslovanja.

Odziv na zdravstveno krizo

Zdravstvenih kriz se vsi upravičeno bojimo, saj smo od njih ogroženi, tako osebno s svojim zdravjem, kot čustveno zaradi skrbi za tiste, ki jih imamo radi, ter tudi zaradi ekonomskih pretresov, ki jih te lahko povzročijo.

Tisto, česar smo se potihoma bali in se na to nikoli nismo prav zares pripravljali, je tu. Razglašena je bila pandemija in v Sloveniji epidemija COVID-19.

Če bi imeli narejene načrte neprekinjenega poslovanja tudi za primer pomanjkanja človeških virov, torej izvajalcev poslovnih procesov, potem bi sedaj vedeli:
- kateri so ključni poslovni procesi, katere so nujne aktivnosti, ki jih mora organizacija izvajati, da preživi;
- kdo, kje in kako bo izvajal ključne procese in aktivnosti;
- kako bo organizacija komunicirala z različnimi javnostmi;
- kako bo teklo krizno vodenje.

Vsaka organizacija z nekaj truda lahko vzpostavi ključne procese upravljanja neprekinjenega poslovanja. To so krizno vodenje, krizno komuniciranje in organizacija dela v krizni situaciji.

Priprava na delovanje med zdravstveno krizo

Vsaka organizacija z nekaj truda lahko vzpostavi ključne procese upravljanja neprekinjenega poslovanja. To so krizno vodenje, krizno komuniciranje in organizacija dela v krizni situaciji.

Krizno vodenje

Krizno vodenje naj vključuje vsaj:
- hierarhijo vodenja;
- jasna pooblastila za sprejemanje odločitev;
- jasne odgovornosti za poročanje;
- natančne urnike in načine komuniciranja kriznega managementa.

Krizno komuniciranje

Krizno komuniciranje naj bo usmerjeno v različne javnosti, predvsem pa:
- sporočanje vseh dejanj zainteresirani javnosti;
- sporočanje dejstev brez prikrivanja resnice, laž ni primerna in je škodljiva;
- sporočila naj bodo kratka in jasna, zapleten strokovni jezik in predloga sporočila niso primerna;
- komuniciranje naj bo redno, vsebuje naj informacije o tem, kdaj bo objavljeno naslednje sporočilo;
- načrt komuniciranja naj bo pripravljen vnaprej, seveda ga je treba spoštovati;
- komunicira naj en govorec, ki je vešč podajanja informacij;

- zanemariti se ne sme nobena javnost: stranke, zaposleni, dobavitelji, lastniki, itd.
- seznami prejemnikov sporočil za vsako skupino oziroma javnost naj bodo pripravljeni vnaprej;
- improvizacija ni primerna za krizno komuniciranje.

Organizacija dela v krizni situaciji

Organizacijo dela v krizni situaciji predstavljajo naslednje aktivnosti:
- organizirajo naj se izmene in delo izven rednega delovnega časa za zdravo osebje;
- prestavijo se vnaprej napovedane odsotnosti, kot so dopusti, izobraževanja in podobno;
- izvede se navzkrižno usposabljanje, kjer je to mogoče tako, da so nadomeščanja odsotnih lažje izvedljiva;
- uvede se mentorstvo za boljše navzkrižno izmenjavo znanj med zaposlenimi;
- ugotovijo se možnosti za začasno zaposlitev študentov, podpišejo se ustrezne pogodbe, zaposlijo se delavci za določen čas;
- pripravijo se seznami upokojenih zaposlenih in njihovih znanj, sklenejo se dogovori z upokojenimi bivšimi zaposlenimi za vpoklic v primeru potrebe;
- uvede se različen delovni čas, da se omeji medsebojni kontakt med zaposlenimi in njihova gostota na delovnih mestih;
- zagotovi se mehanizem za vzpostavitev stikov z zaposlenimi in njihovo lociranje izven delovnega časa;
- premakne se delovna mesta kritičnih zaposlenih (tistih, ki so nujni za nadaljevanje poslovanja) na druge lokacije;
- zamakne se načrtovane vzdrževalne projekte na kasnejši čas;
- zaposlenim se omogoči, da delajo od doma. Pripravijo se ustrezni postopki za delo od doma;
- spoštuje se polno plačilo tudi za zaposlene, ki ostanejo doma zaradi bolezni (da ne bi zaradi razlike v plači vztrajali na delovnih mestih in širili okužbe). Natančno se opredeli plačilo za prisotne, za tiste, ki delajo od doma, ostanejo doma zaradi potrebne nege otrok ali staršev, ostanejo doma zaradi zaprtja šol ali javnega prevoza in vse ostale možnosti.

Vračanje v normalno poslovanje

Ob zaključevanju zdravstvene krize mora organizacija načrtovati vračanje v normalno poslovanje. V ta namen je smiselno razmišljati o postopnem vključevanju zaposlenih v normalno poslovanje, o zagotavljanju varnostnih ukrepov varovanja zdravja, o spoštovanju notranje in zunanje regulative in o specifičnih pričakovanjih deležnikov.

Tako naj podjetje pred zagonom normalnega poslovanja zagotovi vsaj naslednje:
1 Pripravi se nabor poslovnih funkcij glede na njihovo kritičnost, najprej se v normalno poslovanje vrnejo najbolj kritične funkcije, nato ostali. Verjetno se v tem trenutku za najbolj kritične funkcije smatrajo tiste, ki že sedaj delajo od doma in njihovo delovanje nikoli ni bilo prekinjeno. Izvajalci teh funkcij se najprej vrnejo na delovna mesta. Za ostale zaposlene se pripravi urnik vračanja na delovna mesta.
2 Pripravi se seznam zaposlenih, ki se najlažje vrnejo v običajno delovno okolje. Ob tem se upošteva rizičnost posameznika za izpostavljenost okužbi. Zaposlenim, ki sodijo v rizične skupine (kronični bolniki, starejši zaposleni), se omogoči nadaljevanje dela od doma dokler traja večja verjetnost okužbe.
3 Dokler veljajo zdravstveno pogojeni varnostni ukrepi v državi, se zaposlenim omogoči fleksibilen delovni čas. Na ta način se zmanjšuje koncentracija zaposlenih v poslovnih prostorih. Možne oblike dela so:
   - Oblikovanje izmenskega dela, kjer se vnaprej opredeli izmenski delovni čas za zaposlene, ki delajo na običajnih delovnih mestih
   - Oblikuje se delna prisotnost na delovnem mestu v okviru tedna (polovica zaposlenih dela prvo polovico tedna na običajnem delovnem mestu, polovico tedna pa od doma; druga polovica zaposlenih dela v obratnem režimu)
4 Oblikujejo se seznami tistih zaposlenih, ki zaradi drugih vzrokov ne morejo izvajati svojega dela na običajen način. Sem štejemo predvsem:
   - Starše otrok, ki zaradi neizvajanja šolskih in predšolskih dejavnosti ne morejo na delo, ker morajo varovati otroke.
   - V isto skupino štejejo tudi tisti zaposleni, ki na delovno mesto ne morejo, dokler ni zopet vzpostavljen javni prevoz.

Za te zaposlene se pripravijo individualni dogovori, možne rešitve so: delo od doma, čakanje na delo in podobno.
5 Na delovnih mestih se predpiše, organizira nabava in zagotovi uporaba zaščitnih sredstev, kot so:
   - Zaščitne maske,
   - Razkužila za roke,
   - Higienske papirne brisačke v toaletnih prostorih,
   - Namenski koši za smeti za odvržene maske, brisače, robčke in podobno.
6 Do preklica se kot obvezno uporablja konferenčne klice namesto sestankov za interne in eksterne zadeve.
7 Zagotovi se brezplačna parkirna mesta za vse zaposlene, dokler ne začne delovati javni prevoz.
8 Začasno se ukine dostop do avtomatov s kavo in drugo ponudbo.



9 Zaposlenim se svetuje, da se ne družijo ob malici ali kavi.
10 Predpiše se redna uporaba razkužil za izpostavljena mesta, kot so kljuke na vratih, registrator delovnega časa, konzola za upravljanje alarma. Predpiše se redno zračenje delovnih prostorov vsako uro.

Ob koncu zdravstvene krize

Ob zaključku krizne situacije naj organizacije oblikujejo načrte neprekinjenega poslovanja, ki vključujejo tudi izvajalce poslovnih procesov in ne le delovanje informacijsko komunikacijske podpore.

Celovito načrtovanje neprekinjenega poslovanja je najlažje izvedljivo, če spoštujemo dobre prakse. Te so običajno zapisane v standardih in za načrtovanje neprekinjenega poslovanja je najbolj znan standard ISO 22301. Prva izdaja tega standarda je iz leta 2012, v letu 2019 pa je bil dopolnjen.

Oblikovanje načrtov neprekinjenega poslovanja

Če želimo vzpostaviti primerne načrte neprekinjenega poslovanja je, tako kot običajno treba najprej ugotoviti, kaj in v kolikšni meri dejansko ogroža organizacijo. To ugotovimo z analizo operativnih tveganj, samo ocena informacijskih varnostnih tveganj ni dovolj. Druga nujna analiza je analiza vplivov na poslovanje, ki poda jasno sliko o tem, kako časovna komponenta zastoja poslovanja vpliva na organizacijo. Na podlagi obeh se oblikuje strategija neprekinjenega poslovanja. Strategija postavi okvire za postavitev načrtov neprekinjenega poslovanja in tudi za postavitev rezervne lokacije.

Strategijo naj odobri vodstvo organizacije, temu sledijo konkretno načrti neprekinjenega poslovanja. Konkretnost načrtov neprekinjenega poslovanja zagotovi jasna opredelitev odgovornosti in pooblastil pred, med in po razglasitvi krize.

In na koncu, ne smemo pozabiti na najpomembnejši del načrtovanja neprekinjenega poslovanja: usposabljanje. Usposabljanje za delovanje v krizni situaciji mora temeljiti na izvajanju vaj. Izvedba vaje neprekinjenega poslovanja pa je zgodba, ki jo vsi prav dobro poznamo že iz principov testiranja. Vaje načrtujemo tako, da jasno vnaprej opredelimo pričakovan potek in rezultate. Vsa odstopanja med izvedbo vaje beležimo, kasneje analiziramo in kadar je to treba, popravimo načrte neprekinjenega poslovanja. To pa je že vsem dobro poznan cikel neprestanih izboljšav.



Slika 1: Shema vpeljave Načrtov neprekinjenega poslovanja

Za konec

Vsaka organizacija naj razmisli, katere aktivnosti so tiste, ki jih lahko izvede sama. Ob tem ne gre zanemariti, da prava metodologija in izkušnje lahko prihranijo veliko časa in energije in seveda tudi denarja. Pripravljeni načrti neprekinjenega poslovanja morajo organizacijo pripraviti na morebitne krizne dogodke v bodočnosti. In samo to naj bo cilj vsake organizacije. ■

Varnostni prehodi za kontrolo dostopa v nadzorovana območja



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

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

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

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



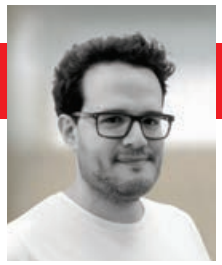
ID Shop nudi različne nivoje in mehanizme za zagotavljanje kontrole pristopa:

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

IDealni partner za identifikacijo in varnost

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

Avtorja: Jaka Čović, Gašper Pintarič / Špica International d.o.o.*





BREZKONTAKTNA EKONOMIJA KOT SKUPNI IMENOVALEC PREVENTIVNIH UKREPOV

V zadnjih dveh mesecih smo bili, predvsem na področju preventive na delovnem mestu, soočeni z vrsto ukrepov, ki so odločilno vplivali na zajezitev širjenja COVID-19 v Sloveniji. Zaradi navedenega smo posebno pozornost namenili trem segmentom: higieni, distanci in temperaturi, saj menimo, da so ključni za prilaganje novi realnosti, ki smo jo poimenovali brezkontaktna ekonomija. V uvodu sva na kratko predstavila različne tehnološke rešitve za prva dva segmenta, strokovno in podrobneje pa sva se posvetila brezkontaktnemu merjenju temperature oseb v povezavi s kontrolo dostopa.

Samo tehnološke rešitve ne zadostujejo

Ukrepi na področju preventive predstavljajo poleg prave tehnološke rešitve v prvi meri predvsem organizacijske spremembe. Mnoga podjetja se ob vrnitvi zaposlenih na delovna mesta srečujejo z vprašanji, kako zagotoviti primerno varnost zaposlenih, kot tudi drugih deležnikov v njihovih procesih (zunanji izvajalci, prevozniki, obiskovalci). Na področju higiene se srečamo s tem vprašanjem že pri prihodu v podjetje, ko moramo odpreti vhodna vrata. Pred začetkom in ob koncu delovnega časa se tam pogosto nabere veliko število ljudi (registracija delovnega časa). Organizacijsko se to lahko reši s povečanjem števila prehodov, kjer je to seveda fizično mogoče. Alternativo predstavljajo avtomatska vrata, fizične zapore ter sistemi za kontrolo pristopa, ki temeljijo na brezkontaktni tehnologiji. Identifikacija preko RFID kartic deluje na primer na razdalji nekaj centimetrov, odpiranje vrat lahko opravimo tudi z uporabo mobilnih telefonov. Veliko zanimanja v tem času predstavljajo sistemi za prepoznavo obraza, ki prav tako delujejo zelo zanesljivo. Uporaba termalnih kamer za merjenje temperature na vhodih ter integracija s sistemom za kontrolo pristopa oziroma registracijo delovnega časa predstavlja poleg tehnološke rešitve tudi določen organizacijski izziv. Več o tem v nadaljevanju. Tretji segment preventive se dotika distance. Vsi smo bili soočeni z delom od doma, kjer lahko registracijo delovnega časa opravimo preko spleta ali mobilnega telefona ter beležimo čas po projektih. Na področju interne logistike lahko robotski avtonomni vozički povečajo produktivnost. Naj gre za oskrbo delovnih mest v proizvodnji ali pa prevoz artiklov od skladiščnih lokacij do vhodno-izhodnih ramp, robotski vozički poskrbijo za hiter, varen in učinkovit prevoz materialov. Pri natančem lociranju opreme pa si lahko pomagamo z natančnimi RTLS sistemi in sledenjem preko BLE in UWB tehnologije ter tako posredno omogočimo večjo distanco v skladiščih.

Pomembno je vzeti v zakup, da se določene tehnološke rešitve dotikajo tudi področja obravnave osebnih podatkov, kjer je trenutno zakonodaja v Sloveniji precej ostra ter postavlja tudi določene omejitve pri implementaciji takšnih rešitev v praksi.

Brezkontaktno merjenje temperature kot pomoč pri zajezitvi širjenja Covid-19

Do sedaj zbrane informacije strokovnjakov kažejo, da je povišana temperatura najpogostejši simptom okužbe s COVID-19. Študija, narejena v sodelovanju 522 bolnišnic iz 30 provinc Kitajske, kaže, da je kot simptom bila prisotna pri

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

88,7 % obolelih. Naslednja najpogostejša simptoma sta bila kašelj s 67,8 % in utrujenost s 38 %. Ta podatek izpostavi dve pomembni dejstvi.

Prvo je, da obstaja vzorec okuženih, ki ne kažejo simptomov. Študije si trenutno niso enotne, kakšen naj bi bil točen odstotek asimptomatičnih okuženih, potrjujejo pa njihov obstoj. To poudari dejstvo, da 100 % metode omejevanja virusa zaenkrat še ne poznamo in je pomembna uvedba več ukrepov za omejevanje širitve virusa.

Drugo dejstvo pa je, da je spremljanje povišane temperature najučinkovitejši indikator morebitne okuženosti z novim koronavirusom. Če želimo učinkovito obvladovati tveganja, povezana z morebitno širitvijo virusa, je povišana temperatura simptom, ki ga je vredno nadzirati.

Sistemi za merjenje telesne temperature oseb

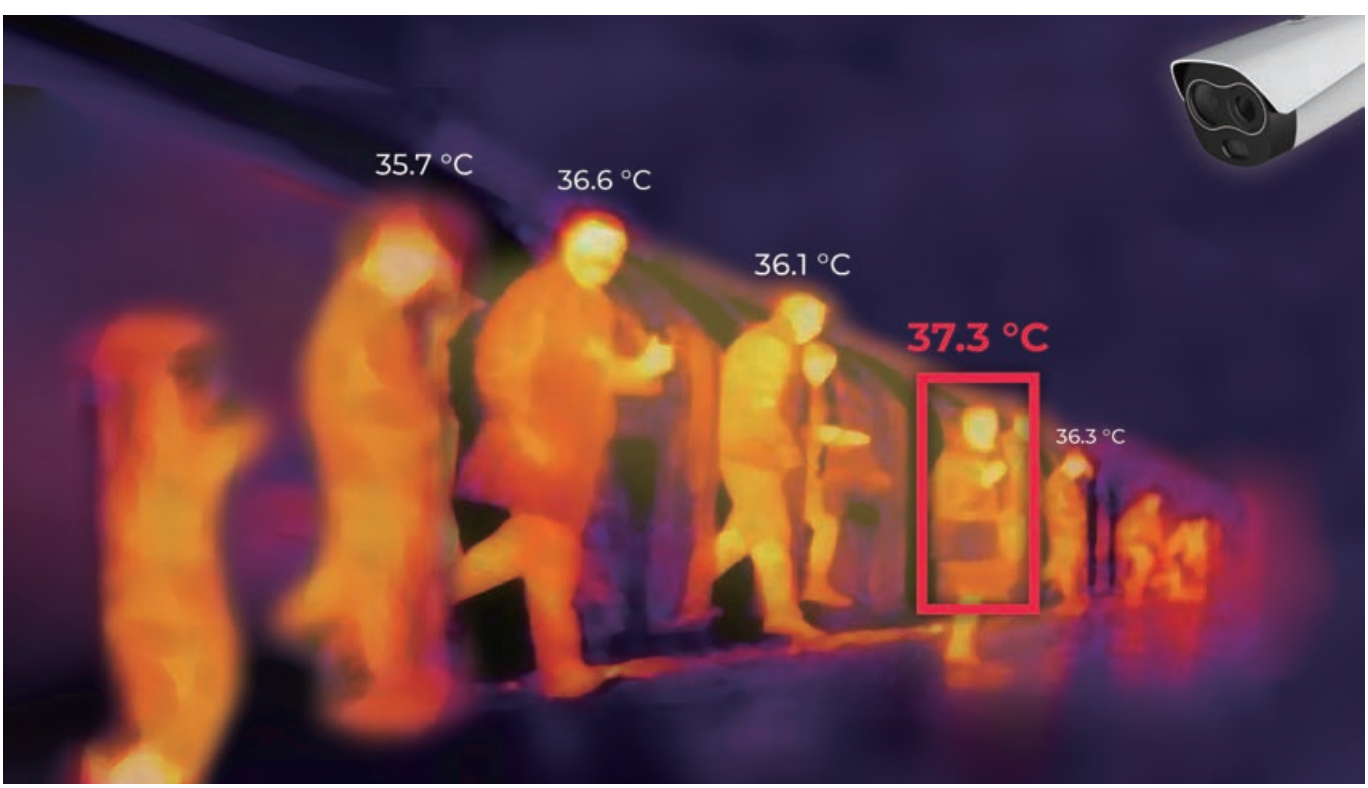
Dober začetek za snovanje vsakega merilnega sistema je poznavanje zahteve po njegovi točnosti. Za merjenje telesne temperature obstaja več tehnik z različno točnostjo. Zahtevano točnost lahko izračunamo/določimo na podlagi strokovnih podatkov o povišanih temperaturah med obolelimi. To je namreč temperaturni obseg, ki ga želimo z našim merilnim sistemom čim natančneje zaznavati.. Študija navaja sledečo porazdelitev povišane temperature med obolelimi:

°C	Odstotek obolelih
manj od 37,5	9,9%
od 37,5 do 38	30,9%
od 38,1 do 39	46,9%
več kot 39	12,3%

Preventiva je glavni skupni imenovalec ter predstavlja novo realnost. Ključni dejavnik je še vedno zavedanje vseh vpletenih v procese, da moramo na delovno mesto prihajati le zdravi. V podjetjih si lahko pomagamo tudi z različnimi tehnološkimi reštvami, ki zmanjšujejo tveganja ter pripomorejo k dvigu korporativne varnosti.

Telesna temperatura zdravega človeka znaša med 36,5 °C in 37,5 °C. Zahtevano natančnost lahko torej ocenimo glede na statistiko. Z merilnim sistemom, ki ima natančnost 1 °C, lahko napačno ocenimo povišano telesno temperaturo skoraj 40 % ciljne populacije. Natančnost merilnega sistema mora biti torej mnogo višja.

Ko izberemo natančnost merilnega sistema, je zelo pomembno razumeti vplive okolja, v katerem izvajamo meritev. Natančnost same merilne opreme je namreč podana v nadzorovanih pogojih. Glede na to, da je cilj merjenja nadzor nad tveganjem širitve novega koronavirusa in ozaveščanje zaposlenih, da s povišano temperaturo ne smemo na delovno mesto ter, tako lahko predpostavimo dve merilni okolji. Najboljša opcija je, da si zaposleni telesno temperaturo spremljajo doma, vendar tega žal ne moremo niti nadzirati niti zagotavljati. Alternativa je merjenje telesne temperature ob vstopu v delovne prostore, pred stikom s sodelavci. To je postavitev, ki jo organizacija lahko nadzira in s tem občutno pripomore k zmanjšanju tveganja širjenja virusa med zaposlenimi. Ima pa takšna postavitev nekaj zahtev oziroma lastnosti. Posamezna meritev mora zaradi prehoda večjega števila zaposlenih pote-



Uporaba termalnih kamer za merjenje temperature na vhodih ter integracija s sistemom za kontrolo pristopa oziroma registracijo delovnega časa predstavlja poleg tehnološke rešitve tudi določen organizacijski izziv.

kati hitro. Zaradi želje po spoštovanju priporočila o ohranjanju distance proces merjenja ne sme povzročati čakalne vrste oziroma zbiranja zaposlenih. Prav tako je zaželeno, da v izogib povečanja možnosti širjenja okužb meritev poteka brezkontaktno in brez vpletenosti dodatnega osebja, da preprečimo stik vseh zaposlenih z eno osebo oziroma predmetom.

Cenovno najdostopnejša tehnologija, ki omogoča brezkontaktno merjenje temperature, je zaznavanje moči infrardečega valovanja. Takšni merilni sistemi merijo moč infrardečega valovanja, ki ga oddaja površina človeške kože. Pojem telesna temperatura se običajno nanaša na temperaturo »jedra« človeka. Zaradi zunanjih dejavnikov okolja, kot so veter, sonce, mraz, vlaga in podobno, sta temperaturi v jedru in na površini kože lahko različni. Na razliko vpliva tudi izbrana točka merjenja. Slabše prekrvavljeni deli človeške kože (na primer sredina človeškega čela) so bolj izpostavljeni zunanjim vplivom. Vpliv okolja na temperaturo površine kože je pogosto veliko večji kot pa deklarirana natančnost merilne opreme. To postavlja zelo pomembne omejitve na sam proces merjenja. Merjenje se mora izvajati v brezvetrnem in zaprtem prostoru s čimbolj konstantno temperaturo in vlažnostjo. Pomembno je tudi, da se osebe pred izvedbo meritve v tem prostoru aklimatizirajo. Priporoča se ustrezno obdobje mirovanja. To deloma izniči vplive zunanjega okolja in naredi izvedbo meritve smiselno.

Najpogostejši brezkontaktni merilni pripomočki za to so t.i. čelni termometri in termovizijske kamere. Fizikalni princip merjenja obeh je podoben in poenostavljeno povedano, čelni termometer meri temperaturo v eno točki, medtem ko termovizijska kamera zajame več vrednosti in jih sestavi v termično sliko.







V podjetju Špica International smo na podlagi teh izhodišč za merilni sistem izbrali merjenje s pomočjo termovizijske kamere. Takšno merjenje poteka:

- brezkontaktno (na razdalji od 0,8 m do 3 m),
- brez približevanja tretjih oseb, ki izvajajo meritve,
- učinkovito, saj sodobne termovizijske kamere temperaturo eni osebi izmerijo v manj kot sekundi.

Natančnost merjenja, ki smo jo prepoznali kot ključni preventivni faktor, nas je spodbudila, da smo varnost zaposlenih okrepili še z integracijo s sistemom za kontrolo pristopa in evidenco delovnega časa. Integracija omogoča avtomatski nadzor povišane telesne temperature zaposlenih ob prihodu v podjetje. Ob registraciji se izmeri tudi telesna temperatura zaposlenega, na registracijskem terminalu pa se prikažejo obvestila. Poleg tega povezava s sistemom za kontrolo pristopa zagotavlja upravljanje in avtorizacijo pristopa glede na temperaturo zaposlenega. Prednosti takšne rešitve se kažejo zlasti v naslednjih točkah:

- zanesljivo in dosledno merjenje temperature vsakega zaposlenega,
- meritev se izvaja kot del registracije delovnega časa, ki ga zaposleni že poznajo,
- meritev upošteva, da je telesna temperatura osebni podatek in se zato njena vrednost nikjer ne shranjuje niti ne posreduje v kak drug sistem,
- obveščanje usposobljene osebe o primerih povišanih vrednosti telesne temperature.

Zaključek

Preventiva je glavni skupni imenovalec ter predstavlja novo realnost. Ključni dejavnik je še vedno zavedanje vseh vpletenih v procese, da moramo na delovno mesto prihajati le zdravi. V podjetjih si lahko pomagamo tudi z različnimi tehnološkimi rešitvami, ki zmanjšujejo tveganja ter pripomorejo k dvigu korporativne varnosti. Nekatere izmed njih so sicer na prvi pogled cenovno neprivlačne, a dodajo kamenček v mozaiku pri krepitvi zaupanja zaposlenih in vodstvenega kadra pri vračanju na delovno mesto, zagotavljanju nemotenega poslovanja ter varovanju kritične infrastrukture. ■

Avtorji: dr. Andrej Bregar, Sašo Gjergjek, mag. Miran Novak, Damir Orlić / Informatika d.d.*

STANDARDIZACIJA KIBERNETSKE VARNOSTI KLJUČNI DEJAVNIK DIGITALNE PRILAGODITVE V KRIZI

V družbi Informatika d.d. smo v večletni praksi vpeljali varnostne, procesne in organizacijske standarde ter z njimi skladne tehnologije, ki izpolnjujejo te zahteve ter predstavljajo dobro osnovo za hitro in uspešno digitalno prilagajanje novim okoliščinam poslovanja znotraj družbe in v širšem poslovnem elektroenergetskem sistemu, v katerega je družba vpeta. Izkušnje z vpeljanimi standardi in procesi kibernetske varnosti ter vzpostavljeno tehnološko arhitekturo kažejo, da je možno na takšni osnovi opraviti učinkovito prilagoditev na izredne razmere.

Uvod

V izrednih razmerah, do kakršnih je v času epidemije COVID-19 prišlo, tako v nacionalnem prostoru kot na globalni ravni, predstavlja kibernetska varnost prav poseben izziv, saj se je potrebno zelo hitro in učinkovito prilagoditi na spremenjene oblike dela, specifične nove tipe kibernetskih groženj ter posledično na povečane varnostne ranljivosti. Ključ za premagovanje tega izziva je vpeljava mehanizmov kibernetske varnosti kot enega osrednjih elementov vseh procesov poslovanja. To vključuje standardizacijo mehanizmov varnosti, doseganje visokega nivoja zrelosti na področju varnosti, ustrezno upravljanje kompetenc in odgovornosti ljudi v procesih dela, predvsem pa vpeljavo robustne arhitekture informacijskih in komunikacijskih tehnologij, ki omogočajo neprekinjeno in varno poslovanje, oddaljeno delo ter visoko stopnjo digitalizacije poslovanja.

Poslovni procesi v sodobnih organizacijah v vedno večji meri temeljijo na informatizaciji in avtomatizaciji, zaradi česar so vse bolj podvrženi kibernetskim tveganjem in ranljivostim. Ko se tveganja povečujejo, so organizacije primorane neprestano in konsistentno izboljševati varnostno strategijo in arhitekturo.

Standardizacija in osredinjenost procesov poslovanja na elemente kibernetske varnosti

Poslovni procesi v sodobnih organizacijah v vedno večji meri temeljijo na informatizaciji in avtomatizaciji, zaradi česar so vse bolj podvrženi kibernetskim tveganjem in ranljivostim. Ko se tveganja povečujejo, so organizacije primorane neprestano in konsistentno izboljševati varnostno strategijo in arhitekturo. Kibernetska varnost je tako nujen strateški dejavnik, ki na različnih nivojih preprečuje napade, vdore in tveganja. Organizacije so ranljive tako dolgo, dokler ne postane kibernetska varnost osrednji steber njihovega delovanja

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



in poslovanja. To zahteva transformacijo organizacij na takšen način, da so mehanizmi in elementi kibernetske varnosti neposredno vpeti v jedro njihovega poslovanja. Podproces kibernetske varnosti je s tem vpeljan kot integralni in osrednji sestavni del poslovnih modelov in procesov.

Potrebo po vzpostavljanju arhitekture kibernetske varnosti je ključno prepoznati že takrat, ko nismo izpostavljeni večjim neposrednim grožnjam. V izrednih, neutečenih razmerah skušajo specifične ranljivosti, ki so nastale zaradi takšnih pogojev, izkoristiti tudi napadalci, pri čemer praviloma ciljajo na najbolj ranljive. Da se prilagodimo tako obsežnim spremembam in da premostimo varnostne luknje, moramo biti z odzivi hitri in agilni. Pogoj za to je, da dobro poznamo potencialne grožnje, imamo vzpostavljeno tehnologijo, ki omogoča oddaljeno delo in neprekinjeno poslovanje, ter imamo vpeljane ustrezne delovne tokove, poslovne procese in podporne procese za zagotavljanje kibernetske varnosti. Podporni procesi vključujejo zaznavo, analizo in upravljanje incidentov, pravila odzivanja na incidente, postopke okrevanja in ukrepanja po incidentih, mehanizme preprečevanja vdorov, postopke izmenjave varnostnih podatkov, procese implementacije varnostnih priporočil ter pristope k prenosu znanja.

Najbolj ranljiv element z vidika varnosti so ljudje, zato je potrebno procese in informacijsko tehnologijo zasnovati tako, da zmanjšamo tiste odvisnosti poslovanja od človeških virov, ki so najbolj podvržene varnostnim tveganjem. Bistveno je upravljanje odgovornosti in vlog, ker imajo le-te dostop do informacijskih virov in so posledično vezane na različna varnostna tveganja. Pomembno je določiti in upravljati, kdo ima dostop do česa. Zagotoviti je potrebno, da pravi ljudje z ustreznimi znanji opravljajo primerne naloge na pravilen način in s primerno tehnologijo. Prav tako je potrebno poskrbeti za celosten vpogled v to, kaj se dogaja v organizaciji. To pomeni, da se ne smemo osredotočiti zgolj na nekaj temeljnih strateških procesov z največjo dodano vrednostjo, temveč tudi na vse ostale procese, ki sestavljajo mozaik poslovanja. To je ključno, da ugotovimo, kje in kako smo izpostavljeni varnostnim tveganjem, kako se pravilno zaščititi ter kako vzpostaviti celovit sistem kibernetske varnosti.

Procesi morajo planirati izpade zaradi varnostnih incidentov in potrebne ukrepe. Predvidevati morajo alternativne pristope k delu, na primer iz oddaljenih lokacij. Ta način dela mora biti v celoti podprt s tehnologijo, v sklopu katere so implementirani ustrezni varnostni mehanizmi. Procesi, ki so osredotočeni na vidik varnosti, določajo tudi jasna pravila dostopa do podatkov, da zagotovijo zaupnost, integriteto in polno razpoložljivost le-teh. Izguba integritete podatkov je namreč velikokrat posledica človeške napake, zlorabe ali neustreznega procesa dela.

Priporočljivo je definirati standarde glede nameščanja in uporabe programske opreme. Dobra praksa je vzpostaviti standarden proces, ki obravnava licence, pravila namestitve in uporabe ter določa odgovornosti nadrejenega kadra, pooblaščenega za odobritve, kaj sme kdo narediti. Na ta način so opredeljena varnostna tveganja in je oblikovan sistematičen pristop k njihovi zajezitvi in obravnavi, hkrati pa je zagotovljena fleksibilnost dela.

Program kibernetske varnosti je lahko učinkovit le, če se neprenehoma razvija in izboljšuje. To pomeni, da mora organizacija vselej vedeti, kje se nahaja in kako naj napreduje. Za napredovanje so ključnega pomena celovite meritve in oce-

nitve trenutnega stanja, kar pomeni, da ne zadošča, če spremljamo samo nekaj metrik, kot je npr. število odkritih ranljivosti ali incidentov. Ogrodje, ki omogoča merjenje zrelosti programa kibernetske varnosti in usmerja k doseganju višjega nivoja varnosti, je zrelostni model kibernetske varnosti. Le-ta pove, kaj je potrebno storiti, da napredujemo iz enega nivoja na drugega. Obstaja več zrelostnih modelov, med katerimi veljata za najbolj verodostojna C2M2 (*Cybersecurity Capability Maturity Model*) in NIST CSF (*National Institute of Standards and Technology Cybersecurity Framework*). Oba sta dovolj učinkovita, tako da ni toliko pomembno, po katerem posežemo, kot je pomembno, da se odločimo enega vpeljati in mu slediti. Model C2M2 definira deset domen, na osnovi katerih ocenimo doseženo stopnjo vzpostavljene kibernetske varnosti. Model NIST CSF pa odraža napredek na podlagi petih varnostnih funkcij – identifikacije, zaščite, odkrivanja, odzivanja in okrevanja.

Meritve zrelosti so zgolj prvi korak v iterativnem procesu. Na osnovi meritev sledi vpeljava mehanizmov, ki izboljšajo rezultate. Gre torej za kontinuirano pot doseganja napredka, ki mora biti podprta s celovitim programom kibernetske varnosti. Poslovanje, ki je osredinjeno na kibernetsko varnost, integrira takšen program in zrelostni model v svoje jedro. Tehnologija, procesi ter vloge in odgovornosti ljudi so vzpostavljeni in upravljani tako, da so usklajeni s programom varnosti in so podvrženi kontinuiranim ocenitvam na osnovi zrelostnega modela.

Neprekinjeno poslovanje in potencial kontinuiranega upravljanja kibernetske varnosti za učinkovito prilagoditev poslovanja na izredne razmere

Varovanje podjetja se je izkazalo za neločljiv del poslovanja. Spremembe, usmerjene zgolj na en vidik poslovanja, niso bile

> Program kibernetske varnosti je lahko učinkovit le, če se neprenehoma razvija in izboljšuje. To pomeni, da mora organizacija vselej vedeti, kje se nahaja in kako naj napreduje.

tako učinkovite kot spremembe, ki so upoštevale vse vidike poslovanja. Prav zaradi tega se zahtevi po neprekinjenem poslovanju in kibernetski varnosti obravnavata v kontekstu celote poslovnega modela. Inherentnost postopkov za vzpostavitev neprekinjenega poslovanja in neprekinjenega upravljanja kibernetske varnosti je potrebno upoštevati pri načrtovanju sprememb v poslovnem modelu.

Prav v današnjem času, času pandemije, sta se ti dejstvi izkazali za ključni. Podjetja so morala čez noč nadaljevati poslovanje v povsem novih pogojih. To je odprlo veliko vprašanj glede kibernetske varnosti v aktualni situaciji. Po drugi strani so istočasno koncepti s področja kibernetske varnosti močno vplivali na potrebo po spremembi določenih poslovnih procesov.

Ključnega pomena v nedavnih dogajanjih je pripravljenost sistema kibernetske varnostni na spremembe. To vključuje dobro kadrovsko, organizacijsko in tehnološko kondicijo, tako sistema kibernetske varnosti, kakor tudi poslovnega modela podjetja v celoti. Pri tem nam lahko pomagajo štirje principi: načrt, dinamika, predpripravljalni ukrepi in kontinuiteta.

Izrednih dogodkov se ne da predvideti, ampak se lahko na njih pripravimo. Pomembno vlogo pri tem ima načrt. Načrt za neprekinjeno poslovanje namreč obravnava vse vidike poslovanja v primeru nepredvidenega dogodka. Po drugi strani pa sam načrt ne pomeni veliko, saj je potrebno nenehno spre-



Za doseganje visoke stopnje kibernetske varnosti moramo združiti procese, standarde, ljudi in tehnologijo. Ti štirje dejavniki se morajo med sabo povezovati in dopolnjevati. Visoka stopnja kibernetske in informacijske varnosti omogoča tako normalno poslovanje kot neprekinjeno poslovanje.

mljati spremembe, ter načrt ustrezno posodabljati in spreminjati glede na bistvene okoliščine. Dinamika je pomembna tudi zaradi kondicije poslovnega sistema.

Predpripravljalni ukrepi so izjemno pomembni ukrepi, ki jih izvedemo na podlagi verjetnosti nepredvidljivega dogodka ter ocene tveganja, in sicer še preden se sam dogodek zares zgodi. Kontinuiteta predstavlja povezanost med vsemi zgodovinskimi in aktualnimi poslovnimi artefakti.

Tehnologije za udejanjanje neprekinjenega poslovanja v izrednih razmerah

Za zagotavljanje neprekinjenega poslovanja v izrednih razmerah je zraven standardov in procesov ključnega pomena še informacijska tehnologija. Z njeno pomočjo zagotavljamo, tako informacijsko in kibernetsko varnost lastnega podjetja, kot varnost uporabnikov storitev. Prav tako je pomembna tudi komunikacija med zaposlenimi v podjetju in z uporabniki storitev. Zato je potrebno v izrednih razmerah, ko smo primorani opravljati delo na daljavo, omogočiti zaposlenim uporabo ustrezne strojne opreme (npr. prenosnikov), varen dostop do podatkov in komunikacijo. Med ključne informacijske tehnologije za neprekinjeno poslovanje spadajo:

- *Požarni zid* je eden najosnovnejših sistemov za doseganje omrežne varnosti. Spremlja vhodni in izhodni omrežni promet in na podlagi definiranih pravil spušča ali blokira ta promet. Zagotavlja nekakšno pregrado med zavarovanim in nadzorovanim notranjim omrežjem ter zunanjim nenadzorovanim in nezaupnim omrežjem, kot je internet.
- *VPN* (*Virtual Private Network*) ohranja varno komunikacijo in omogoča uporabnikom, da se lahko povežejo v interno omrežje svojega podjetja ali organizacije.
- *Varnostna oprema za preprečevanje zlonamerne kode* so zaščitni sistemi, ki preprečujejo okužbo računalnika ali mobilnega telefona pred zlonamerno programsko opremo, kot so virusi, trojanski konji, črvi, vohunski in izsiljevalski programi ... Polno licencirani in funkcionalni sistemi vključujejo celotno zbirko varnostnih mehanizmov, od preiskovanja zlonamerne programske kode do protivohunske in druge opreme.
- *Sistemi za upravljanje varnostnih informacij in dogodkov* (*SIEM*) so sistemi, ki zbirajo podatke iz različnih naprav ter ustvarjajo povezave med podatki. Na podlagi tega obveščajo, ali gre za varnostni incident.
- *Komunikacijski sistemi* (Skype, MS Teams in drugi) omogočajo komunikacijo med zaposlenimi v podjetju in uporabniki storitev.
- *Konferenčni sistemi* (Webex, Zoom in drugi) omogočajo izobraževanje na daljavo ter udeležbo na konferencah, srečanjih in drugih dogodkih, izvedenih na daljavo.
- *Sistemi za oddaljeni dostop* (*Remote Desktop Systems*) omogočajo oddaljeni dostop do internega računalnika ter s tem do podatkov in orodij z zaščitenim dostopom na njem.
- Prek *storitev v oblaku* dostopamo do internih aplikacij, internih informacij in internih podatkov, ki jih lahko obdelujemo, zbiramo, shranjujemo ali uporabljamo.

Kot učinkovita podpora pri zagotavljanju neprekinjenega poslovanja se je izkazal *varnostni operativni center* (*VOC*). Glavni gradnik VOC je sistem SIEM, s katerim nadzorujemo in varujemo varovano omrežje. Na sistem SIEM se lahko vežejo različne naprave, pri čemer so najpogosteje priključene varnostne naprave, aplikacije, mrežne naprave in strežniki. Iz teh naprav SIEM pridobiva podatke, kot so dnevniki prijav in odjav, varnostni dogodki, spremembe v sistemih in drugi. Podatki se zbirajo v realnem času kot dogodki in tokovi, vendar je omogočen tudi pogled za nazaj. S pomočjo nadzorovanja in varovanja omrežja lahko odkrivamo varnostne incidente in anomalije ter na podlagi tega poskušamo preprečiti, da bi se varnostni incidenti uresničili. Tako odpravljamo ranljivosti. SIEM omogoča tudi izvedbo digitalne forenzike, ki je ključnega pomena pri raziskovanju varnostnih incidentov.

Za doseganje visoke stopnje kibernetske varnosti moramo združiti procese, standarde, ljudi in tehnologijo. Ti štirje dejavniki se morajo med sabo povezovati in dopolnjevati. Visoka stopnja kibernetske in informacijske varnosti omogoča tako normalno poslovanje kot neprekinjeno poslovanje.

Sklep

Kot smo pojasnili v članku, je v izrednih razmerah, npr. v kontekstu situacije, ki je vezana na epidemijo COVID-19, ključnega pomena združevanje vidika kontinuitete pri standardizaciji in upravljanju kibernetske varnosti z vidikom hitrih sprememb in prilagoditev, katerih osnova je prav predhodna kontinuiteta in posledično visoka stopnja pripravljenosti na izredne razmere. Tako je potrebno zagotoviti usklajen preplet dveh »rdečih niti«. Prva je kontinuirana vpeljava elementov kibernetske varnosti v jedro vseh ključnih in tudi obrobnih procesov poslovanja, vpeljava podpornih procesov za zagotavljanje kibernetske varnosti ter ustrezna standardizacija na področju varnosti in neprekinjenega poslovanja. To je vezano na standarde in model zrelosti kibernetske varnosti v poslovnem okolju, upravljanje kompetenc in odgovornosti zaposlenih, varovanje informacij ter na funkcijo varnostnega operativnega centra. Na drugi strani je nabor ključnih informacijskih tehnologij, ki so osnova za neprekinjeno poslovanje in sledijo vpeljanim standardom kibernetske varnosti. Med njimi so orodja za oddaljeni dostop, sistemi za virtualizacijo, sistemi za upravljanje s podatki, komunikacijsko-konferenčni sistemi, storitve v oblaku, požarni zidovi itd. Te tehnologije predstavljajo potencial in osnovo za hitro, učinkovito in predvsem varno prilagoditev poslovanja na izredne razmere. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*



RAZGLASITEV PREJEMNIKOV PRESTIŽNIH NAGRAD »SLOVENIAN GRAND SECURITY AWARDS 2020«

Letošnji nagrajenci so g. Andrej Maslo iz podjetja Pošta Slovenije, podjetje ELES, podjetje Telekom Slovenije, Mestna občina Ptuj, Občina Tržič, Časnik Finance in projekt SI-CERTa »Varni na internetu«.

Slovenska velika nagrada varnosti je najpomembnejša nagrada s področja varnosti v Republiki Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado v sodelovanju s Slovenskim združenjem korporativne varnosti podeljuje Institut za korporativne varnostne študije.

Letošnji nagrajenci so zaradi izredne situacije izjemoma predstavljeni na nekoliko drugačen način. Svečana podelitev nagrad se bo sicer zgodila 21. septembra 2020 v okviru otvoritve prestavljene mednarodne konference Dnevi korporativne varnosti 2020.



Neodvisna komisija je letos izbrala tiste najboljše in najbolj inovativne, ki s svojim zgledom in aktivnostmi na področju zagotavljanja varnosti v svojih sredinah, predstavljajo primer dobrih praks in inovativnih rešitev. Letošnji prejemniki prestižnih nagrad *»Slovenian Grand Security Award«* za dosežke v preteklem letu so:

Nagrado za KORPORATIVNO VARNOSTNEGA MANAGERJA leta prejme g. Andrej MASLO iz podjetja Pošta Slovenije d.o.o.

G. Maslo ima večletne interdisciplinarne izkušnje, ki so vezane tako na področje javnega, kakor tudi poslovnega korporativno varnostnega okolja. Ravno to delovanje v različnih korporativnih in javnih okoljih mu je dalo tisto priložnost za nadgrajevanje znanj in izkušenj, ki jih s pridom izkorišča pri svojem delu, in katere tvorijo posebno kvaliteto, ki ga ločuje od ostalih kolegov. Ravno v korporativnem okolju v zadnjih letih izredno aktivno deluje kot direktor področja korporativne varnosti in nadzora. Varnost in obvladovanje kompleksnih varnostnih tveganj, med katerimi so posebej izpostavljena specifična tveganja, katerim je izpostavljena poštna dejavnost, so za Pošto Slovenije, ključnega pomena. S svojimi bogatimi izkušnjami in znanjem pomembno sooblikuje in vpliva na učinkovito obvladovanje tveganj, katerim je organizacija, zaradi specifične dejavnosti in mednarodnega okolja, zelo močno izpostavljena.

*avtor je član Slovenskega združenja korporativne varnosti



Nagrado za NAJBOLJ VARNO PODJETJE prejme podjetje ELES d.o.o.

Družba ELES je sistemski operater prenosnega elektroenergetskega omrežja, ki skrbi za varen, zanesljiv in neprekinjen prenos električne energije po Sloveniji in prek meja, ter je pomemben predstavnik kritične infrastrukture. Obvladovanje tveganj in s tem zagotavljanje neprekinjenosti delovanja sistema je v ELES-u ključni proces, ne samo v sami družbi, temveč v širši nacionalno-varnostni dimenziji.

Pravilna ocena strateškega vodstva je, da je obvladovanje varnostnih tveganj eno od ključnih področij za zagotavljanje neprekinjenosti delovanja procesov varnega prenosa električne energije. Tako s sistemskim pristopom že daljše časovno obdobje vzpostavlja učinkovite okvire varnostne arhitekture. Gre za vzpostavljanje integralnega korporativno varnostnega sistema, ki temelji na profesionalnosti in celovitosti, v povezanosti fizične ter informacijske varnosti, varnostnih standardov, visoki stopnji organizacijske in varnostne kulture ter poslovne etike in ne nazadnje tudi na zavidljivo visoki pripadnosti zaposlenih. Novo nastajajoči integralni varnostni sistem poskuša zagotavljati tudi širši okvir upravljanja korporativne varnosti, in sicer s stalnim izboljševanjem organiziranosti in varnostne kadrovske strukture. Posebni napori so bili v zadnjem obdobju namenjeni dvigovanju varnosti in zanesljivosti informacijskih sistemov v podjetju, sistemu varovanja ključnih podatkov in inovacij podjetja ter varnostnemu zavedanju zaposlenih.

Posebej velja izpostaviti ukrepe, ki jih podjetje izvaja na področju prenosa najnovejših spoznanj iz znanstveno-raziskovalnega področja in mednarodno primerjalnega okolja v svoje procese delovanja.

Nagrado za INOVATIVNO VARNOSTNO REŠITEV prejme podjetje TELEKOM SLOVENIJE d.d.

Informacijsko-varnostna rešitev Operativni center kibernetske varnosti (OCKV), ki ga je razvilo in vpeljalo podjetje Telekom Slovenije, predstavlja pomembno dodano vrednost na področju zagotavljanja kibernetske varnosti v Republiki Sloveniji.

Telekomov operativni center kibernetske varnosti predstavlja centralno enoto, ki v obsegu 24/7 vse dni v letu na organizacijski in tehnični ravni obravnava kibernetsko varnostna tveganja in incidente. Omenjeni OCKV ima implementirano visoko zmogljivo tehnologijo, ki je podprta z urejenimi in certificiranimi procesi ter kompetentnimi zaposlenimi. V tem

trenutku Operativni center kibernetske varnosti predstavlja največji Security Operational Center v Republiki Sloveniji. Omenjeni center ima vzpostavljene polne operativne zmogljivosti za operativno izvedbo aktivnosti zagotavljanja kibernetske varnosti na 1 in 2 ravni delovanja. 3 in 4 raven pa je urejena v sodelovanju med strokovnjaki centra in ostalimi področnimi specialisti v Republiki Sloveniji ter tujimi strateškimi partnerji. Ustrezno podporo nudi tudi sektorski CSIRT predvsem na področjih omejitve varnostnih incidentov, zavarovanju dokazov za kasnejšo forenzično analizo in najhitrejšim možnim vzpostavljanjem delovanja IKT storitev. Procesi in zaposleni so ustrezno certificirani z vsemi najvidnejšimi certifikati in standardi s področja informacijske varnosti.

Pri razvoju so razvijalci zasledovali tudi dejavnike kot so hitrost, odzivnost, preglednost, enostavnost, zanesljivost ter povezljivost sistemov. Poseben poudarek je v inovacijski rešitvi namenjeni interoperabilnosti delovanja. Rešitev se že uporablja s strani različnih organizacijskih okolij po vsej Sloveniji, kar še dodatno potrjuje visoko kvaliteto varnostne rešitve.

Nagrado za najbolj varno mesto v kategoriji mestnih občin letos prejme MESTNA OBČINA PTUJ.

Mestna občina Ptuj je leta 2019 med ostalimi občinami, ki so izpolnile anketni vprašalnik ter glede na statistiko kaznivih dejanj, pokazala nekaj dodatnih pristopov, ki kažejo na njihovo aktivno vlogo pri zagotavljanju čim višje stopnje varnosti svojim občanom. Mestna občina Ptuj je izstopala v domala vseh statističnih primerjalnih kazalnikih, ki skupaj prinašajo polovico celotne ocene.

Izpeljali so kar nekaj projektov oz. dobrih praks na področju lokalne varnosti, ki so pripomogli k tej odločitvi. Vse to nam kaže na dejstvo, da se v vodstvu te občine zavedajo pomena varnosti in s svojimi aktivnostmi zagotavljajo varno življenjsko okolje.

Nagrado za najbolj varno mesto v kategoriji majhnih in srednje velikih občin prejme OBČINA TRŽIČ

V kategoriji manjših in srednje velikih občin je prvo mesto drugič zapored osvojila Občina Tržič**.** Stanje na področju varnosti se vztrajno izboljšuje, kar kažejo tudi statistični podatki in kazalniki na področju števila storjenih kaznivih dejanj, ki so bili med prijavljenimi občinami najboljši.

Zelo poudarjeno je izvajanje celega niza lokalnih projektov, ki so usmerjeni v zagotavljanje bolj varnega lokalnega okolja. Posebni pozitivni trendi so zaznani tudi na področju trajne mobilnosti z vplivom na prometno varnost. Skozi projekt »Zelena luč za trajnost« se zrcali celotna prometna strategija Občine Tržič, ki glede na rezultate zagotavlja zelo učinkovite rešitve, ki dajejo zelo dobre rezultate.

To so tiste kvalitete in dobra praksa, ki so poleg statističnih podatkov, tudi letos prepričale komisijo, da se občini Tržič podeli omenjena nagrada.

Nagrado za NAJBOLJŠI STROKOVNI PRISPEVEK s področja korporativne varnosti prejme projekt SI-CERTa »Varni na internetu«

Neodvisna komisija se je odločila, da v tokratnem izboru, za najboljši strokovni prispevek na področju varnosti, pogleda daljše obdobje in oceni aktivnosti izvajalcev, ki so s svojimi prispevki na področju varnosti pomembno sooblikovali strokovni prostor v Sloveniji. Projekt Varni na internetu izvaja Nacionalni odzivni center za kibernetsko varnost SI-CERT, ki deluje pod okriljem javnega zavoda Arnes. Skozi navedeni projekt SI-CERT zasleduje ključne cilje dvigovanja stopnje zavedanja ciljnih javnosti o različnih nevarnostih, katerim so izpostavljeni na spletu, informira o varni uporabi spletnega bančništva in spletnega nakupovanja, informira o različnih oblikah spletnih prevar in ponuja praktične rešitve, kako jih prepoznati in se zavarovati, in informira o zaščiti identitete na družbenih omrežjih.

S pomočjo različnih poti posredovanja strokovnih interaktivnih vsebin je projekt dosegel zelo široko družbeno skupnost, kar daje projektu še posebno težo na področju osveščanja uporabnikov pri varni uporabi interneta.

Nagrado za INOVATIVNO MEDIJSKO PROMOCIJO VARNOSTI prejme poslovni dnevnik FINANCE

Poslovni dnevnik FINANCE je slovenski poslovni medij, ki je v dolgih letih svojega delovanja pomembno oblikoval razvoj slovenskega poslovnega medijskega prostora. Vsebine v zadnjem obdobju obsegajo tudi vedno več strokovnih vsebin povezanih z zagotavljanjem korporativne varnosti in s tem povezanih vsebin od informacijske varnosti, varnosti ključnih podatkov, neprekinjenosti poslovanja in drugih pomembnih področij. Prispevki v programskem okolju vsebujejo ustrezne informativne vsebine povezane s širšim področjem varnosti in obvladovanjem varnostnih tveganj s poudarkom na gospodarskih okoljih. Nepristransko podajanje kredibilnih informacij s pomočjo novinarskega kolektiva in zunanjih strokovnjakov, ki z zadostno mero pronicljivosti zagotavljajo, da so upoštevani visoki profesionalni novinarski standardi pri poročanju vsebin, ki se dotikajo problemov povezanih z varnostjo. Z inovativnim, fleksibilnim, kredibilnim in ustvarjalnim pristopom do medijskih vsebin predstavlja zelo pomemben dejavnik za dvigovanje varnostne kulture in splošnega zavedanja o pomenu varnosti v poslovnem okolju.

Več o obrazložitvi nagrajencev si lahko preberete na spletni strani Instituta za korporativne varnostne študije. Za konec naj ponovimo, da bo uradna podelitev nagrad 21. septembra v okviru otvoritve prestavljene mednarodne konference Dnevi korporativne varnosti 2020. ■

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:

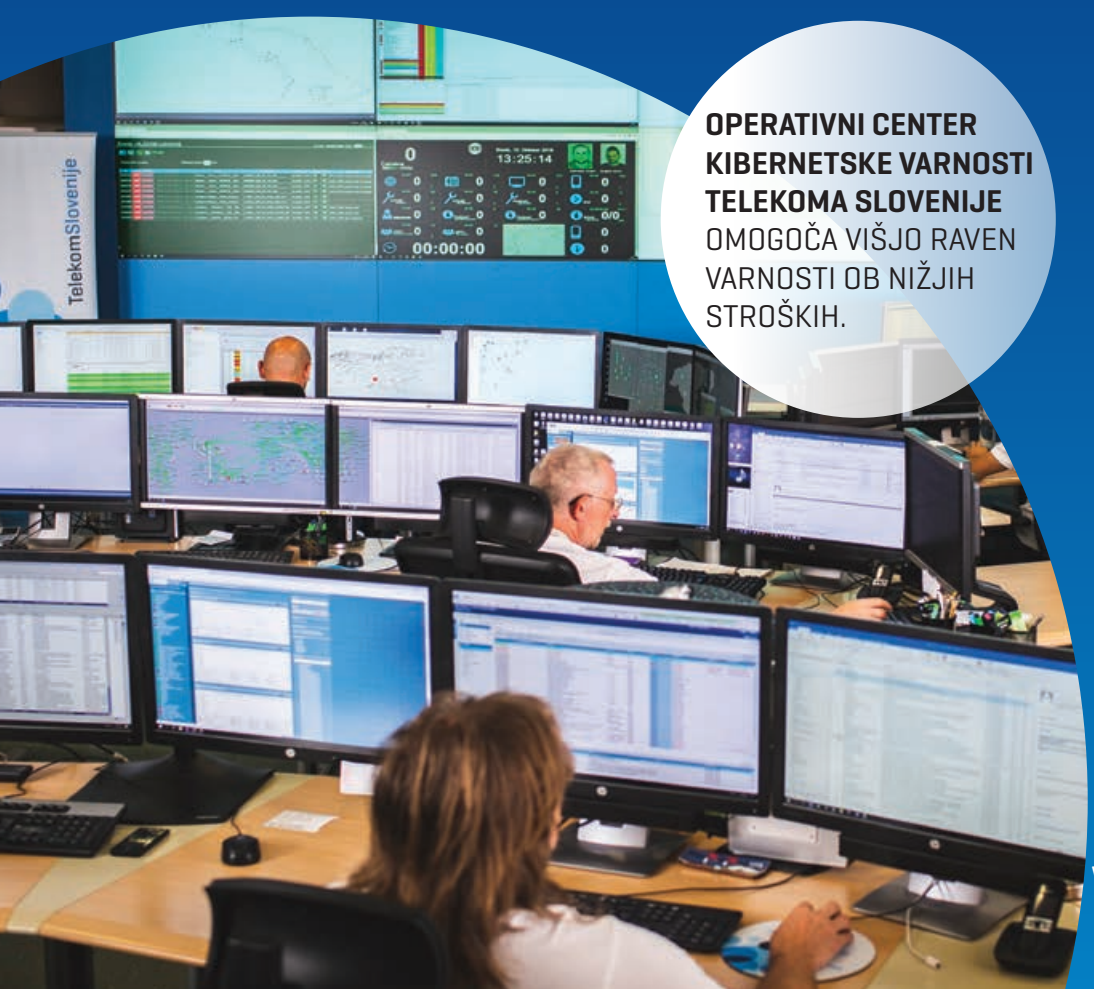
ZNIŽEVANJE OPERATIVNIH TVEGANJ POVEZANIH S KIBERNETSKO VARNOSTJO

+

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