Korporativna varnost

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

Letnik 2020, marec • št. 22



Podelitev nagrad »Slovenian Grand Security Award«

Zagotavljanje varnosti prenosnega omrežja prihodnosti

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

g. Robert Slodej, vodja Službe za korporativno varnost

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



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
marec 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.

Korporativna varnost je proces, ki ga v svojo procesno in organizacijsko strukturo vpeljujejo vse resne organizacije. K tem korakom jih seveda ni pripeljala ljubezen do varnosti, temveč potreba, ki jo prinaša zahtevno poslovno okolje. Vse bolj kompleksna tveganja, ki so v zadnjem času posebej povezana s kibernetskim okoljem in na drugi strani človekom, za podjetja predstavljajo pomembne izzive na poti k učinkovitemu obvladovanju le teh. Te potrebe prinašajo pomembne spremembe v organizacijskih okoljih, ki si jih še nekaj let nazaj nismo mogli zamišljati. Na eni strani je strateški management postal vedno bolj pozoren na področje obvladovanja tveganj in temu področju namenja tudi več pozornosti in več potrebnih virov. Na drugi strani pa zaznavamo izredno veliko potrebo po ustreznih strokovnjakih s področja korporativne varnosti, med katerimi so posebej izpostavljeni strokovnjaki za informacijsko varnost, ocenjevanje in upravljanje s tveganji, kakor tudi tisti, ki so sposobni strateško razumeti in upravljati zahteven sistem integralne korporativne varnosti. Vsa ta dejstva pomenijo nujne signale izobraževalnemu sistemu, da bo dovolj hitro sposoben izobraziti ustrezno količino usposobljenih strokovnjakov, ki bodo posedovali potrebna znanja za prevzem zahtevnih nalog v poslovnih in drugih organizacijskih sistemih. Če v ta okvir dodamo še organizacije, ki upravljajo kritično infrastrukturo ali so izvajalci bistvenih storitev in vzamemo v obzir še povprečni odliv kadra iz Slovenije, zelo hitro lahko zaključimo, da na tem področju sveti rdeča luč deficitarnosti poklica. To pred državo postavlja pomembno zahtevo, da čim prej spozna zahteve realnega okolja in tem oblikam izobraževanja nameni ustrezno veliko pozornost. Ta pozornost se mora reflektirati skozi jasno oceno, kateri programi bodo v prihodnje ustrezno finančno koncesionirani in podprti zaradi potreb realnega okolja. Trenutno na tem področju še vedno prevladuje okorelost, neodzivnost in usmerjanje javnih sredstev v tista področja izobraževanja, katera dinamično poslovno okolje ne potrebuje.

Tokratno številko revije Korporativna varnost namenjamo najpomembnejšemu regijskemu dogodku na področju korporativne varnosti, ki ga predstavljajo Dnevi korporativne varnosti. Poseben prostor bomo namenili pogovoru z nagrajenci, 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
mag. Matjaž Beričič, član uprave Telekom Slovenije d.d.

VARNOST SODI MED KLJUČNE VREDNOTE TELEKOMA SLOVENIJE

16



NEMOTENO POSLOVANJE PODJETJA IN POŽARNA VARNOST

Načrt neprekinjenega poslovanja podjetja lahko razumemo kot nadstandard, ki ga na ravni podjetja sprejmejo kot del poslovne politike. Je veliko več, kot zgolj zahteva predpisov. V podjetju vzpostavi sistem ravnanja s tveganji, ki je v današnjem konkurenčnem in globalno povezanem svetu eno od zagotovil, ki podjetju lažje omogoča trajnostni razvoj.

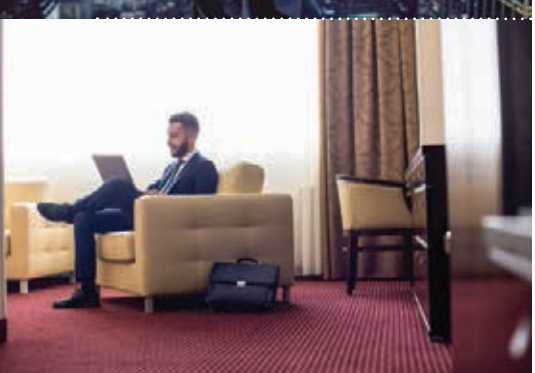
26



NEPREKINJENO POSLOVANJE: »NIČ NE DELA, KAJ PA ZDAJ?«

Izredne dogodke ne moremo načrtovati, lahko pa načrtujemo zmanjšanje njihovih posledic. Učinkovita odzivna struktura in postopki odziva na izredne dogodke predstavljajo predpogoj za učinkovito zagotavljanje neprekinjenega poslovanja.

30



INFORMACIJSKA IZPOSTAVLJENOST, OGROŽENOST IN TVEGANJA NA JAVNIH BREZŽIČNIH OMREŽJIH V HOTELIH

Dejstvo je, da imamo vsi radi brezplačen brezžični internet. Pa vendar, kolikokrat se vprašamo o varnosti uporabe brezžičnih dostopnih točk? Dandanes je to v hotelih zelo pomemben dejavnik za skoraj vsakega gosta. Obstajajo celo spletna mesta namenjena iskanju hotelov s hitrim brezžičnim internetom.

34



PRIJAVITE INCIDENT. SE SPLAČA.

Kibernetska varnost je marsikje že več let pomembna tema na delovnih mizah vlad različnih držav. V zadnjih letih se je prerinila tja tudi pri nas, saj smo morali udejaniti evropsko direktivo NIS. Zakon o informacijski varnosti sedaj določa med drugim tudi to, da so zavezanci po zakonu obvezani poročati o večjih incidentih pristojni CSIRT[1] skupini.

43

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
mag. Aleksander Mervar, direktor ELES d.o.o.
g. Robert Slodej, vodja Službe za korporativno varnost

ZAGOTAVLJANJE VARNOSTI PRENOSNEGA OMREŽJA PRIHODNOSTI

Podjetje ELES je dobitnik prestižne nagrade Slovenian Grand Security Award v kategoriji najbolj varno podjetje za leto 2019. Prizadevanja za zagotavljanje neprekinjenosti delovanja prenosnega omrežja prihodnosti bo predstavljalo velik izziv, ki bo poleg ostalega zahteval sistemski pristop upravljanja korporativne varnosti. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Aleksandrom Mervarjem in g. Robertom Slodejem.

Mag. Aleksander Mervar

Vodite podjetje, ki verjetno predstavlja eno od organizacij, od katere je najbolj odvisno strateško delovanje Republike Slovenije, kakor tudi širše regije zaradi kompleksne umeščenosti v prenosno elektro omrežje. Imate občutek, da so ta dejstva dovolj upoštevana pri podpori vseh nacionalnih institucij?

ELES d.o.o., sistemski operater prenosnega elektroenergetskega omrežja, je v 100 odstotni lasti države. Rekel bi, da je za ELES "ustava" Energetski zakon in iz njega izhajajoči podzakonski akti ter uredbe EU. Na drugi strani so za ELES zelo pomembni sporazumi, pogodbe, dogovori sklenjeni v okviru združenja ENTSO-E, Evropskega združenja sistemskih operaterjev elektroenergetskega omrežja, ki povezuje 42 (43 skupaj s turško družbo TEIAS, ki je trenutno članica opazovalka) sistemskih operaterjev prenosnega omrežja iz 35 (36) držav v Evropi in tudi izven meja Evropske unije. Poleg tega so tu še sporazumi in pogodbe s sosednjimi ter z ostalimi sistemskimi operaterji, proizvodnimi podjetji, operaterjem distribucijskega omrežja SODO in še bi lahko našteval. Gre za široko razvejano mrežo organizacij, ki so medsebojno tesno povezane. Menim, da pomen ELES-a za nemoteno delovanje naše države ni dovolj prepoznan. Ste mogoče kje zasledili zapis, da je ELES najpomembnejše infrastrukturno podjetje v naši državi ter zakaj?

> Uvajanje inovativnih rešitev bo med drugim omogočilo boljšo izrabo obstoječe infrastrukture, priključevanje večjega deleža obnovljivih virov energije in baterijskih hranilnikov v omrežje, s tem pa uresničevanje podnebnih in energetskih ciljev Evropske unije do 2030.

Kritična infrastruktura je nujna za nemoteno delovanje družbe. Kako ob tej predpostavki organizirati sistem obvladovanja tveganj, ki bo zagotavljal ustrezno varnost za nemoteno delovanje infrastrukture? Kakšne so vaše izkušnje sodelovanja z državnimi organi zadolženimi za pripravo sistemskih ukrepov za zaščito te infrastrukture?

Pomembna naloga je prepoznati ključna tveganja za varno, zanesljivo in učinkovito obratovanje in vzdrževanje prenosne-

*avtor je član Slovenskega združenja korporativne varnosti



ga sistema. Osnovno načelo pri načrtovanju prenosnega omrežja takšnega sistema je, da je v vsakem primeru mogoče vzpostaviti več napajalnih poti. Večina elementov sistema, ki so ključni, zaradi tega načela že danes dosega visoko raven neprekinjenega delovanja. Zaradi zanesljivosti napajanja je prenosni sistem zasnovan na načelu n-1. To pomeni, da izpad kateregakoli elementa sistema ne povzroči izpada napajanja. Vse napajalne poti so najmanj podvojene, razen v izjemnih primerih, kjer to ni mogoče. Konkretnen primer je napajanje Severne Primorske. Poleg zagotavljanja razpoložljivosti elementov sistema in storitev je pomembna tudi zasnova sistema: n-1 pravilo, zazankanost, ustrezen koncept zaščit, rezerva regulacijske delovne in jalove moči. Delovanje elektroenergetskega prenosnega sistema v Republiki Sloveniji je zaradi izpolnjevanja vseh zgoraj navedenih načel zelo zanesljivo. Potrebno pa se je zavedati, da stoodstotnega neprekinjenega napajana z električno energijo ni mogoče zagotoviti pod nobenimi pogoji. Sodelovanje z državnimi organi, s katerimi sodelujemo pri pripravi sistemskih ukrepov za zaščito prenosnega elektroenergetskega omrežja, ocenjujem kot uspešno.

Sistemi in procesi za obrambo pred kibernetskimi napadi so zagotovo področje, ki je strateški izziv Elesa. Prizadevamo si, da prek izzivov krepimo priložnosti, hkrati pa minimizirano tveganja za delovanje in poslovanje. Vzpostavitev varnega, fizično ločenega IT omrežja in storitev, za izmenjavo informacij med sistemskimi operaterji, je med drugim ena izmed prednostnih zahtev ENTSO-E.

Varnostna kultura in visoko varnostno zavedanje zaposlenih ločuje uspešne organizacije od manj uspešnih. Kako vi, kot strateški manager v tem hitrem dinamičnem okolju, kjer je mobilnost kadrovskega potenciala zelo visoka, zagotavljate osnovne varnostne vrednote in standarde varnostne kulture?

Zavedamo se, da infrastrukturna podjetja, za doseganje zastavljenih ciljev in strategije, potrebujejo usposobljene ter izobražene zaposlene, ki so motivirani za kakovostno izvajanje delovnih nalog. Z namenom spremljanja tehnoloških novosti hkrati pa tudi ohranjanja že pridobljenih znanj v Elesu precejšen del finančnih sredstev namenjamo strokovnemu usposabljanju zaposlenih. Na drugi strani se zavedamo tudi potrebe po povezovanju s perspektivnimi bodočimi kadri – dijaki in študenti elektroenergetike, informatike, telekomunikacij. V ta namen ELES omogoča praktično izobraževanje študentom zadnjih letnikov I. in II. stopenjskega bolonjskega študija, omogočamo študentsko delo za spoznavanje delovanja družbe in specifičnih delovnih mest. V začetku letošnjega februarja smo

prvič izvedli Hackathon-Elektrathon, katerega se je udeležilo 45 mladih tekmovalcev iz Slovenije, Hrvaške, Srbije, Severne Makedonije in Rusije, ki so bili razdeljeni v 11 ekip.

Razvoj in odvisnost od informacijske tehnologije postavlja kibernetske grožnje v posebno perspektivo. Kateri so po vašem mnenju tisti koraki, ki jih lahko storijo sistemski operaterji za učinkovito zavarovanje pred temi kompleksnimi grožnjami?

Kot izhaja tudi iz Resolucije o strategiji nacionalne varnosti Republike Slovenije, ki je temeljni razvojno usmerjevalni dokument na področju nacionalne varnosti, ključno grožnjo nacionalni informacijsko-komunikacijski infrastrukturi predstavljajo kibernetski vdori in napadi, kibernetski kriminal in druge oblike kibernetskih groženj. Sistemi in procesi za obrambo pred kibernetskimi napadi so zagotovo področje, ki je strateški izziv Elesa. Prizadevamo si, da prek izzivov krepimo priložnosti, hkrati pa minimizirano tveganja za delovanje in poslovanje. Vzpostavitev varnega, fizično ločenega IT omrežja in storitev, za izmenjavo informacij med sistemskimi operaterji, je med drugim ena izmed prednostnih zahtev ENTSO-E.

Raziskave in razvoj so ključ za doseganje boljše učinkovitosti tudi na področju zagotavljanja obvladovanja tveganj. Nameravate v družbi ELES tudi v prihodnje slediti tej poti?

V Elesu redno spremljamo dogajanja v domačem in mednarodnem okolju, ki vplivajo na prihodnost oskrbe z električno energijo. Z ustanovitvijo Področja za strateške inovacije smo uveljavili strateško usmeritev sistematično organiziranega dela na področju inovativnih projektov in programov ter sodelovanja na ravni Evropske unije. S tem smo postali prva energetska družba v Sloveniji, ki je inovacijsko dejavnost postavila v središče svojega delovanja. Glede uvajanja pametnih omrežij in pridobivanja evropskih sredstev se uvrščamo v vrh evropskih sistemskih operaterjev. Uvajanje inovativnih rešitev bo med drugim omogočilo boljšo izrabo obstoječe infrastrukture, priključevanje večjega deleža obnovljivih virov energije in baterijskih hranilnikov v omrežje, s tem pa uresničevanje podnebnih in energetskih ciljev Evropske unije do 2030.

ELES je pred časom prijavil/soprijavil dva razvojna projekta s področja pametnih omrežij za mednarodno nagrado ISGAN Award of excellence. Združenje ISGAN od leta 2011 deluje v okviru IEA (International Energy Agency) kot eden od forumov iniciative Clean Energy Ministerial (CEM). Je strateška platforma za promocijo na najvišjih nacionalnih državnih organih. Članice CEM so največje svetovne gospodarske velesile (ZDA; Japonska, EU, Rusija, Kitajska,...). ISGAN

S krovno varnostno politiko se strateško vodstvo družbe ELES zavezuje k izvajanju in razkriva ključne poudarke na področju zagotavljanja varnosti organizacije.



ELES je že dolga leta aktiven član Slovenskega združenja korporativne varnosti. Korporativna varnost v Elesu predstavlja eno od osnovnih funkcij za delovanje podjetja in se izvaja v tesnem sodelovanju z drugimi ključnimi funkcijami v podjetju.

nagrado za najboljše smart grid projekte podeljuje vsako leto. Prijavitelji so konkurenti iz vsega sveta. Prijavljena projekta sta zasedla prvo in drugo mesto, kar je skoraj »neverjetno«. Podelitev nagrad bo junija letos.

Ste letošnji prejemniki prestižne nagrade Slovenian Grand Security Award v kategoriji »Najbolj varno podjetje«. Nam lahko zaupate kaj vam pomeni prejem take nagrade?

Vsaka nagrad za podjetje pomeni priznanje za dosedanje delo, hkrati pa prinaša dodatno zavedanje, da je potrebno z delom nadaljevati in doseženo nadgrajevati. Zavedamo se, da v današnjem poslovnem okolju predstavlja varnost enega izmed ključnih, če ne celo ključni izziv, kar daje nagradi še posebno težo.

g. Robert Slodej

ELES predstavlja izredno kompleksno in razvejano organizacijo, ki je že zaradi svojih osnovnih procesov zelo izpostavljena celemu nizu tveganj. Kako se s stališča strateškega korporativno varnostnega managerja spopadate z uravnoteženjem razmerja med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov?

V družbi ELES, katere osnovno poslanstvo je skrb in odgovornost za nemoten prenos električne energije, je obvladovanje tveganj del vsakodnevnih procesov. Tveganja krovno obvladujemo preko sistemov upravljanja kakovosti, katerega sestavni del je Katalog tveganj na operativni ravni in na izvedbeni ravni s pomočjo obratovalnih navodil in drugih predpisov, ki urejajo obratovanje elektroenergetskega sistema. Neprestano izboljševanje delovnih procesov je naša stalna aktivnost, predvsem z namenom zmanjšanja tistih najpomembnejših tveganj, ki se nanašajo na delovanje najbolj vitalnih delov EES.

Za obvladovanje tveganj, povezanih z zaščito elektroenergetske infrastrukture, sprejema ELES obsežen nabor ukrepov, katere delimo na stalne in dodatne. Stalni ukrepi se izvajajo v vseh razmerah, ob povečani ogroženosti infrastrukture, ob izrednem dogodku ali krizi, pa se lahko njihovo izvajanje stopnjuje. Dodatni ukrepi se izvajajo ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi, če stalni ukrepi, tudi če se njihovo izvajanje stopnjuje, ne zadostujejo.



Trenutno opravljate vlogo nosilca procesov korporativne varnosti v podjetju ELES. Nam lahko bolj podrobno opredelite kakšne so strateške naloge vaše službe in njena organizacijska umeščenost?

Organizacije vseh velikosti in vrst se soočajo z notranjimi in zunanjimi dejavniki ter vplivi, ki jih postavljajo v negotovost. Ta negotovost ima lahko pomemben vpliv na doseganje ciljev in poslanstva organizacije. Tukaj ne govorimo samo o prenosu električne energije, proizvodnji in distribuciji, zavedati se je potrebno, da vse dejavnosti vključujejo določena tveganja. Pomembno je, da poskušamo ta tveganja obvladovati s sistemskim pristopom, ki obsega identifikacijo, analizo, vrednotenje in nenazadnje izvedbo ukrepov, ki tveganja zmanjšajo na sprejemljiv nivo. Zagotoviti je potrebno obvladovanje tveganj do te mere, da slednja nimajo pomembnega negativnega učinka na poslovne, finančne, proizvodne, delovne, logistične, informacijsko-komunikacijske, kadrovske in druge procese v organizacijah.

Na enak način je ocena tveganj elektroenergetske infrastrukture podlaga za oblikovanje ukrepov za zaščito vseh struktur tovrstne infrastrukture in temelji na identifikaciji, analizi in ovrednotenju različnih virov tveganj za delovanje le te. V tej smeri gredo tudi strateške aktivnosti službe za korporativno varnost, ki jo vodim.

Kakšno mesto in vlogo ima v hierarhiji strateških dokumentov v Elesu varnostna politika organizacije. Ali tak dokument predstavlja strateški pogled in usmeritve za postavitev in delovanje sistema korporativne varnosti v Elesu?

Direktor družbe mag. Aleksander Mervar je v začetku leta sprejel Krovno varnostno politiko družbe ELES, ki je eden od temeljnih aktov družbe. Krovna varnostna politika predstavlja temeljni usmerjevalni dokument, s katerim se določa poglavitne usmeritve za integracijo procesov, procesno-informacijske varnosti, poslovno-informacijske varnosti ter tehnične in fizične varnosti, ki predstavljajo za družbo ELES temeljna področja za delovanje in jih družba prepoznava v okviru sistema upravljanja družbe. Krovna varnostna politika je vpeta v vse pro-

cese družbe z namenom zagotavljanja varnega poslovanja in delovanja družbe, kakor tudi drugih deležnikov, ki sodelujejo pri njenem delovanju. S krovno varnostno politiko se strateško vodstvo družbe ELES zavezuje k izvajanju in razkriva ključne poudarke na področju zagotavljanja varnosti organizacije.

Standardizacija sredstev na področju tehničnega varovanja in varnostnih procesov na splošno je v tako razvejanem sistemu verjetno nujno potrebna. Kakšne so na tem področju vaše izkušnje in kakšne pristope uporabljate v Elesu?

Za objekte elektroenergetske infrastrukture je ELES vzpostavil sistem integriranega tehničnega varnostnega sistema, s katerim v največji možni meri zagotavljamo preprečevanje poškodovanja ali uničenja elektro energetskih naprav, ki so kritični in ključni za delovanje elektroenergetske infrastrukture. Tehnični varnostni sistem je kombiniran s fizičnim varovanjem objektov. Signali videonadzornega sistema, signali protivlomnega sistema, signali protipožarnega sistema in podatki kontrole vstopa se zbirajo in ustrezno obdelujejo v varnostno nadzornem centru, s čimer je v največji meri zagotovljena avtonomnost delovanja družbe, hkrati pa so izpolnjeni zakonski predpisi, ki jih družba, kot zavezanec za vzpostavitev zasebnega varovanja, v skladu z Uredbo o obveznem organiziranju varovanja in Zakonom o zasebnem varovanju, mora vzpostaviti in izvajati. Varnostno nadzorni center izvaja najzahtevnejše operacije v smislu kombiniranega fizičnega in tehničnega varovanja in predstavlja most med sprejetimi signali tehničnih sistemov za detekcijo na varovanih objektih in varnostim osebjem, ki izvede varnostne ukrepe.



Za objekte elektroenergetske infrastrukture je ELES vzpostavil sistem integriranega tehničnega varnostnega sistema, s katerim v največji možni meri zagotavljamo preprečevanje poškodovanja ali uničenja elektro energetskih naprav, ki so kritični in ključni za delovanje elektroenergetske infrastrukture.

ELES je eden izmed korporativnih članov Slovenskega združenja korporativne varnosti. Kakšen pomen pripisujete stanovskemu združevanju na področju korporativne varnosti? Je to dolgoročno lahko pomemben korak k dvigovanju varnostnega zavedanja in predvsem pomena korporativne varnosti?

ELES je že dolga leta aktiven član Slovenskega združenja korporativne varnosti. Korporativna varnost v Elesu predstavlja eno od osnovnih funkcij za delovanje podjetja in se izvaja v tesnem sodelovanju z drugimi ključnimi funkcijami v podjetju.Kot je opredeljeno v poslanstvu Slovenskega združenja korporativne varnosti, tudi v Elesu procesi zagotavljanja korporativne varnosti predstavljajo nedeljivo celoto krovnega modela upravljanja podjetja in se izražajo skozi korporativno upravljanje in korporativno družbeno odgovornost. Celovito področje korporativne varnosti, za ustrezno obvladovanje varnostnih tveganj, nujno vključuje področje fizične, tehnične in informacijske varnosti, procesa neprekinjenega poslovanja, risk managementa, varovanja ključnih informacij podjetja, varovanja zaposlenih in varnosti pri delu. Vsekakor je združevanje na področju korporativne varnosti ključno pri dvigovanju varnostnega zavedanja in celostnega pomena korporativne varnosti. ■

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.

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!«

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

NIJZ Nacionalni inštitut za javno zdravje

Pošta Slovenije

as

tuš

Občina Slovenska Bistrica

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: Vojko Volk, veleposlanik



KOLUMNA

PRIHODNOST EVROPSKE VARNOSTI

„Potrebujemo evropsko suverenost“.

/Emmanuel Macron/

O smega maja 2018 je ameriški predsednik Trump presenetil ves svet, napovedal je izstop ZDA iz jedrskega sporazuma z Iranom. A mnogo bolj kot Iran, ki je Trumpovo potezo zagotovo pričakoval, je Trump presenetil svoje zaveznike. Tako uradni NATO kot uradna EU sta še zbirala vtise, ko je bilo vsaj malo pozornejšim poznavalcem mednarodnih razmer že jasno, da se je zgodilo nekaj, kar bo močno premešalo veljavna mednarodna razmerja in nazadnje spremenilo svet. Predsedniku ZDA seveda ni šlo za iranski jedrski program ampak se je počutil ogrožen od izjemno uspešnega razvoja odnosov med EU in Iranom, ki niso bili samo gospodarski in samo naftni ampak tudi politični in kulturni. V Iranu je Evropa našla svojo „nadomestno Rusijo“, veliko državo z veliko nafte a tudi veliko civilizacijo z visoko izobraženo populacijo, ki izkazano stremi k napredku in demokraciji. Francija in Nemčija sta imeli z Iranom ob naftnih poslih še velike načrte na področju industrije in infrastrukture, Italija pa je z Iranom celo dosegla dogovor o visoko tehnološkem sodelovanju in izgradnji svetlobnega sinhrotrona. S svojo enostransko potezo je Trump v enem zamahu z evropsko-iranske mize pometal za najmanj 30 mrd evrov poslov, ki so padli v vodo. Ob tem je za ZDA nastala še postranska korist, ker se je iranski režim ponovno radikaliziral in zaprl sam vase, s tem pa je največ škode nastalo za iransko ljudstvo in posredno za EU. Trump ob sebi pač nima nikogar tako modrega, kot je bil svoje čase Henry Kissinger, ki je do Irana zagovarjal politiko, strnjeno v en sam stavek; „Iran se bo moral sam odločiti, ali bo narod, ali bo revolucija“. Z vsem tem laže razumemo, da je ta enostranski odstop od mednarodnega sporazuma, ki je obvezoval vse države podpisnice, v resnici pomenil Trumpov prestop Rubikona v odnosih do zahodnih zaveznic in s tem napoved, da bo njegov volilni slogan „Najprej Amerika“ v prihodnje postal le še „Samo Amerika“. Odtlej naprej so domala vsa ravnanja ZDA v mednarodnih odnosih povsem enostranska, ki prinašajo koristi izključno ZDA vsem ostalim pa v glavnem škodo, še posebej Evropi. Zadnji primer je enostranska odločitev o likvidaciji iranskega vojaškega poveljnika Soleimanija, ki jo predsednik Trump ob nagovoru podpornikov in donatorjev, 18. januarja letos, utemelji z argumentom, da je Soleimani „govoril grde reči o Ameriki“. Posledično so se razmere na Bližnjem vzhodu dodatno zaostrile, iz Iraka in Sirije pa se proti Turčiji in Evropi premikajo novi milijoni beguncev. Soleimanija pa je nadomestil nek nov Soleimani.

> EU medtem vztraja v otrpli neodzivnosti in kljub svoji ogromni gospodarski moči ostaja politični palček na svetovni sceni. Vsi se lahko dobesedno igrajo na evropskem dvorišču, Sredozemlju in Bližnjem vzhodu, od ZDA do Kitajske in zdaj po novem še Turčije, medtem ko EU nemo gleda in pospravlja posledice vseh vrst naftnih, verskih in interesnih spopadov.

Eden od ključnih razlogov, zaradi katerih se ZDA zadnja leta tako zlahka odpovedujejo veljavnim mednarodnim sporazumom in starim zavezništvom ter se predajajo povsem enostranskim početjem, je nafta. Res je, vedno je v ameriški politiki do Bližnjega vzhoda šlo za nafto, a je vedno šlo za to, kako si jo zagotoviti in zaščititi dobavo in rezerve. Zdaj je obratno, Amerika je pri oskrbi z nafto postala povsem samozadostna, tehnološki napredek pa počasi a zanesljivo odriva fosilna goriva na smetišče zgodovine. Najbolj živa priča posledic nezainteresiranosti ZDA za surovo nafto je usoda povsem obubožane Venezuele, od katere roke dvigujejo vsi, razen Rusije in Kitajske, ki nafto tam kupujeta po „sindikalnih“ cenah. Še prav posebej velik vpliv pa ima globalno segrevanje, saj zaradi vse bolj zelenih zim močno upada poraba vseh energentov, v prvi vrsti plina. Pogled na grafikon cen surove nafte v zadnjih petih letih zelo jasno pokaže, da se od drastičnega padca cen med leti 2013 in 2014, ko cene z dobrih 100 USD padejo na vsega 40 USD konec leta 2015, ne dogaja nič posebnega več. Postopnemu vzponu cen do 70 USD do konca leta 2017 je sle-

dil nov padec pod 50 USD v 2018 in odtlej so cene bolj ali manj stabilne. Stabilnost kljub izrazitim političnim turbulencam pa bržkone pomeni, da je svetovni trg nafte dokončno zaznal, da se nafta zlagoma res poslavlja. Zelo podobno je s plinom, ki pa ima še druge težave, v prvi vrsti ceno gradnje in vzdrževanja distribucijskega omrežja, ki ga manj razvite države niti v Evropi ne premorejo. V primerjavi z elektriko postajajo cene plina vse manj konkurenčne in pogosto že nevzdržne.

Kot vse kaže nam globalno segrevanje ozračja prinaša globalno ohlajanje cen fosilnih goriv. A slovo fosilnih goriv bo šlo stežka brez uporabe jedrske energije, seveda tehnološko naprednejše in varnejše od sedanje. Nedavno tega sem prvič obiskal nuklearko v Krškem in tam opravil vrsto pogovorov s strokovnjaki. Na vprašanje, kako daleč je v resnici pot od atomske elektrarne do atomske bombe sem dobil dogovor, da je v osnovi problem plemenitenja urana, kar pomeni zelo daleč, približno toliko kot od kolesa do Ferrarija. Doumel sem, zakaj Slovenci imamo atomsko elektrarno, nimamo pa atomske bombe, je pa bil odgovor vsekakor tudi v velikem nasprotju z mojim poznavanjem atomskih zadev iz romanov in filmov, v katerih lahko vsak malo bolj spreten znanstvenik zvečer v svoji kleti skuha atomsko bombo in zjutraj uniči človeštvo. A ne glede na to, ali se komu zdi pot od kolesa do Ferrarija kratka ali dolga, je na dlani eno; zaradi likvidacije enega vojaškega poveljnika zagotovo ne bo ustavljen iranski jedrski program, če tam res nastaja in res napreduje od civilne proti vojaški rabi. Vprašanje, ki se pri tem postavi je, nazadnje sila preprosto; je iranski jedrski program bolje nadzorovati tako kot doslej, ob sodelovanju in rednem nadzoru mednarodnih organizacij in držav ali pa z eliminacijo nevarnih posameznikov? Mnogi se še danes ne moremo otresti spomina na dan, ko je bil Collin Powell prisiljen zaigrati svoje človeško dostojanstvo, ko je v Združenih narodih mahal s stekleničko z belim prahom, ki naj bi dokazovala, da ima Irak orožje, ki lahko uniči človeštvo. Vehementna trditev se je izkazala za laž, Irak ni uničil človeštva je pa človeštvo skoraj uničilo Irak.

EU medtem vztraja v otrpli neodzivnosti in kljub svoji ogromni gospodarski moči ostaja politični palček na svetovni sceni. Vsi se lahko dobesedno igrajo na evropskem dvorišču, Sredozemlju in Bližnjem vzhodu, od ZDA do Kitajske in zdaj po novem še Turčije, medtem ko EU nemo gleda in pospravlja posledice vseh vrst naftnih, verskih in interesnih spopadov. Turški predsednik Erdogan ravna po starodavnem pravilu Otomanskega imperija, ki pravi, da kadar je vladar ogrožen doma je treba oblast utrditi s kampanjami na tujem. Ob prisotnosti v Siriji je bila turška vojska letos napotena še v Libijo, v podporo eni od sprtih strani. A vsaj v Libiji, če že ne tudi v Siriji, bi morala biti prisotna EU, delovati v zaščito miru in stabilnosti ter z investicijami v korist ljudi, da bi lahko ostali doma namesto bežali proti Evropi. Evropa že vse od vojaškega posega zoper Miloševićev režim leta 1999 ne zmore svetu pokazati, da zmore vzdrževati mir in stabilnost na lastnem dvorišču. Če tega ne zmore več niti na Balkanu lahko še manj opravi na Bližnjem vzhodu. Še več, EU ta hip ne zmore niti preboleti posledic brexita niti odzvati se na posledice tega, da ZDA in Turčija s svojimi ravnanji de facto zapuščata NATO in bo treba nekaj storiti. Prav nobenega razloga ni, da bi NATO moral EU pomeniti več, kot pomeni ZDA ali pa Turčiji. Seveda bi bila ustanovitev Evropske vojske daleč najboljši odgovor na razmere v svetu a preplašena in zbirokratizirana EU ta hip ne zmore več nič, ali pa še tega ne.

Naj ponovim; EU, takšna, kot je danes, ne bo mogla konkurirati ne ZDA ne Kitajski iz preprostega razloga, ker sta ZDA





Še bolj jasno pa je, da pot do evropske suverenosti vodi preko poraza aktualnih populističnih političnih sil, ki prihajajo iz nekdanjih komunističnih držav evropskega vzhoda, v katerih se je prebudilo nekdanje sovraštvo do zahoda in liberalne demokracije in se je skupaj z nikoli povsem zamrlo zvestobo do Moskve zmešalo v nevarno zmes nacionalizma, rasizma in vse bolj odkritega proti evropejstva.

in Kitajska državi, EU pa zveza držav. Države so za razliko od državnih zvez učinkovite pri odločanju, ko gre za vprašanja splošne varnosti, varovanja meja, obrambe in zunanje politike. Edina suverena učinkovitost, ki jo EU ima, so pristojnosti Evropske komisije na področju trgovinskih sporazumov s tretjimi državami, z ostalim svetom skratka. Zato ni čudno, da je predsednik Trump od prvega dne svojega mandata razveljavil vse trgovinske sporazume, ki jih je lahko brez škode za ameriške koristi. In zato je še manj čudno, da je francoski predsednik Macron skrajno jasen, ko zahteva „evropsko suverenost“. Pri tem je vse bolj jasno, da karkoli že lahko pomeni ta evropska suverenost, pot do nje vodi preko skupne varnosti in obrambe, torej skupne vojske, nazadnje pa do skupne zunanje politike. Kako ranljiva je EU brez lastne varnosti pa se je nazadnje izkazalo ob razkritju, da je švicarsko podjetje CryptoAG izpostava ameriške CIA, ki je skrbelo, da so se evropske države med seboj vzajemno „špijonirale“ in prepirale. Ena od posledic je prav lahko tudi hrvaška prisluškovalna afera, ki je hrvaško politiko zapeljala v zanikanje arbitražne sodbe, zaradi česar je Hrvaška ta hip edina evropska država, ki si privošči odklanjati izvedbo povsem zakonite in nesporno veljavne sodbe mednarodnega sodišča.

Države EU trenutno skupno porabijo za svoje vojske okrog 300 mrd evrov letno, skupna evropska vojska pa bi lahko ob večji racionalnosti in učinkovitosti stala precej manj. Pa ne gre samo za stroške ampak za vlogo EU kot igralca, ki je na mednarodnem prizorišču vsaj približno enakovreden svojim tekmecem, da lahko tako kot oni zelo hitro intervenira in pošlje svoje sile na zunanje meje EU ali pa v Sirijo ali Libijo, predvsem pa z veliko večjo težo podpore ali pa zavrne ambicije tekmecev, kadar ti želijo intervenirati ali likvidirati svoje nasprotnike na kateremkoli koncu sveta, v njihovo korist in tujo škodo. Še bolj jasno pa je, da pot do evropske suverenosti vodi preko poraza aktualnih populističnih političnih sil, ki prihajajo iz nekdanjih komunističnih držav evropskega vzhoda, v katerih se je prebudilo nekdanje sovraštvo do zahoda in liberalne demokracije in se je skupaj z nikoli povsem zamrlo zvestobo do Moskve zmešalo v nevarno zmes nacionalizma, rasizma in vse bolj odkritega proti evropejstva. Za določen čas bodo te sile morda celo prevladale, a cena bo visoka, plačalo jo bo gospodarstvo teh „suverenih“ držav, ki bo brez zaščite EU prepuščeno na milost in nemilost ameriškim in kitajskim trgovinskim izsiljevanjem. Na koncu bodo najvišjo ceno plačali ljudje, kot vedno, kadar se politiki namesto višjim ciljem podredijo ljudskim strahovom in strastem. Zato bo prihodnost Evrope evropska, ali pa je ne bo. ■

11. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 11.—12. MAREC 2020



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

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

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

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
mag. Matjaž Beričič,
član uprave Telekom Slovenije d.d.

VARNOST SODI MED KLJUČNE VREDNOTE TELEKOMA SLOVENIJE

Operativni center kibernetske varnosti Telekoma Slovenije je letos na mednarodni konferenci Dnevi korporativne varnosti prejel najvišje priznanje - Slovenian Grand Security Award« v kategoriji »najbolj inovativna varnostna rešitev«. Ob tej priložnosti smo se o pomenu kibernetske varnosti pogovarjali z mag. Matjažem Beričičem, članom uprave Telekoma Slovenije, ki je odgovoren za tehnologijo.

Telekom Slovenije sodi med vodilna regijska podjetja na področju telekomunikacij. Nam lahko podrobneje pojasnite, kaj vaše podjetje dela boljše od konkurence.

V Telekomu Slovenije uporabnikom zagotavljamo zmogljivo in pametno komunikacijsko infrastrukturo, prek katere omogočamo uporabo in razvoj najsodobnejših storitev in rešitev, ki so skladne z najvišjimi mednarodnimi standardi. Delujemo v eni od najbolj globaliziranih, konkurenčnih in hitro razvijajočih se dejavnosti. Slovenski uporabniki od operaterjev zahtevajo visoko kakovost storitev po nizkih cenah, ob tem pa trg postaja vse bolj zasičen, zaradi česar je prostora za rast vse manj. Kljub močni konkurenci smo na slovenskem trgu opredeljeni kot operater s pomembno tržno močjo, tako da smo edini reguliran operater. Vse to pomeni, da moramo v razvoj in uporabnike vlagati še bistveno več, kar nam, paradoksalno, na nek način pomaga, da smo še boljši. To je tako, kakor če bi v atletiki edini trenirali z utežmi na nogah. Hkrati pa sami odločamo o svojem razvoju, spoštujemo domače znanje, naši strokovnjaki imajo ogromno znanja in izkušenj, sodelujemo z ambicioznimi razvojnimi partnerji.

Pri tržnem nastopu smo osredotočeni na uporabnika, zagotavljanje odličnosti uporabniške izkušnje, vlagamo v razvoj omrežja in storitev, optimizacijo poslovanja, kakovost in seveda v varnost. Vse to nam omogoča, da je vrednost naših storitev največja, zato ostajamo prvi izbor uporabnikov in vodilni ponudnik naprednih IKT-storitev.

V Telekomu Slovenije področje kibernetske varnosti sodi med strateške prioritete, saj varnost sodi med naše osnovne vrednote. Zato skrbimo tako za varno poslovanje naše družbe in procesov kot za zaščito svojih uporabnikov.

S svojim poslovanjem ste močno prisotni v nacionalnem kakor tudi širšem regijskem področju telekomunikacijskih storitev, kjer so varnostna tveganja še posebej specifična. Ali svoje odločitve o širitvi poslovanja na določene trge temeljite na strateških analizah varnostnega okolja ali bolj upoštevate poslovne možnosti?

Skupina Telekom Slovenije deluje na trgih, na katerih prihaja do pospešene konsolidacije znotraj posameznih držav in tudi med državami, kar še dodatno zaostruje konkurenco. Pri tem se osredotočamo na naše ključne strateške smernice in skrbno analiziramo svoje poslovne priložnosti.

Ste podjetje, ki veliko sredstev vlaga v lasten razvoj novih tehnoloških reši-

*avtor je član Slovenskega združenja korporativne varnosti



tev. Nam lahko zaupate svojo vizijo na tem področju za prihodnje obdobje?

Naša vizija se glasi - digitaliziramo svet priložnosti. Ob tem poenostavljamo življenja in varujemo svet naših uporabnikov. Želimo ohranjati in krepiti svoj tržni položaj v vseh segmentih našega poslovanja, kar bomo dosegli s ponudbo celovitih storitev za pametno življenje, z razvojem edinstvene in uporabniku prilagojene uporabniške izkušnje, ki bo temeljila tako na preprosti uporabniški izkušnji kot vrhunskem omrežju, navdihujočih storitvah, prebojnih rešitvah in skrbnem ravnanju z uporabniki.

Kako so po vašem mnenju pomembne ključne informacije podjetja v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču? Ali varovanju teh informacij v podjetju Telekom Slovenije namenjate veliko pozornost?

Zagotavljanje informacijske varnosti sodi med naše prioritete. Pri tem gre za celoten sistem informacijske varnosti, katerega pomen se izrazito povečuje. Tudi zato smo ustanovili Operativni center kibernetske varnosti, ki predstavlja jedro operativnih zmogljivosti tako za Telekom Slovenije kot druge organizacije, javne ustanove in podjetja, ki jim storitve ponujamo. Aktivno spremljamo varnostne dogodke v IKT-sistemih ter jih ocenjujemo glede na izvor in nastanek. Ob tem izvajamo tudi testiranja, s pomočjo katerih odkrivamo morebitne ranljivosti. Naši strokovnjaki spremljajo stanje kibernetskih groženj v realnem času in so v stalni pripravljenosti, da se ob podpori najsodobnejše tehnologije takoj ustrezno odzovejo. Pri varnosti ni kompromisov.

Podjetje, kakršno je Telekom Slovenije, se nenehno sooča z različnimi varnostnimi tveganji, ki so v današnjem digitaliziranem svetu vse bolj pogosta, pa tudi vse bolj prefinjena in ciljno usmerjena. Pri tem je izredno pomembna ozaveščenost in lojalnost deležnikov, pa naj gre za zaposlene ali poslovne partnerje. Uveden imamo sistem upravljanja s ključnimi informacijami, prav tako sistem vodenja in varovanja informacij, s katerim skrbimo za razpoložljivost, celovitost in zaupnost informacij, ne glede na njihovo obliko. Z načrtno skrbjo za zagotavljanje kibernetske varnosti, pa skrbimo tako za zaščito digitalnih informacij, kot celotne infrastrukture.

V Sloveniji število kibernetskih incidentov, ki imajo za tarčo podjetja in posameznike, vsako leto narašča. Svetovni gospodarski forum in države skupine G20 kibernetska tveganja uvrščajo med najhitreje naraščajoče varnostne grožnje, globalno škodo zaradi varnostnih incidentov pa lahko merimo v več deset milijardah evrov. Ob tem imajo lahko hekerski napadi in druge oblike vdorov v IKT-sisteme za podjetja in organizacije resne posledice. Poleg poslovne škode gre tu še za tveganje izgube ugleda ali celo prenehanje poslovanja. Naši strokovnjaki spremljajo in zaustavljajo DDoS-napade, preučujejo neželeno elektronsko pošto (spletno ribarjenje), izvajajo teste ranljivosti, varnostne preglede, vdorna testiranja ipd. Vsi procesi so podprti z mednarodnima standardoma ISO 22301:2012 za sistem upravljanja neprekinjenega poslovanja ter ISO/IEC 27001:2013 za sistem vodenja in varovanja informacij.

Glede na to, da ste visoko tehnološko podjetje, ste vi, in posredno vaše stranke v svoji dejavnosti zelo izpostavljene kibernetskim tveganjem. Kakšne ukrepe v podjetju izvajate na področju zagotavljanja kibernetske varnosti?

V Telekomu Slovenije področje kibernetske varnosti sodi med strateške prioritete, saj varnost sodi med naše osnovne vrednote. Zato skrbimo tako za varno poslovanje naše družbe in procesov kot za zaščito svojih uporabnikov. Varnost zagotavljamo na več nivojih, in sicer na ravni procesov, kadrov in tehnologij. Dobro ogrodje za učinkovit sistem informacijske varnosti vzpostavljamo z normativno ureditvijo (varnostnimi politikami, pravilniki, postopki, načrti...), zaposlovanjem in izobraževanjem strokovnjakov s področja informacijske varnosti, dobro opredeljenimi procesi oz. zaščitnimi ukrepi ter z uvajanjem in nenehnim razvijanjem naprednih informacijskih tehnologij za zaznavo in preprečevanje varnostnih groženj.

Skrb za varnost se začne že pri sami izbiri opreme in dobaviteljev, kjer upoštevamo smernice Agencije Evropske unije za varnost omrežij in informacij (ENISA). Spremljamo varnostne dogodke in korelacije med njimi, preprečujemo širjenje zlonamernih dogodkov, uvedli smo sledljivost ukrepov in procesov, kar nam omogoča nadaljnje izboljšave, ter spremljamo vse informacijske sisteme, s katerimi razpolagamo. Sodelujemo z zunanjimi organizacijami in državnimi organi, kot so Ministrstvo za obrambo, Ministrstvo za notranje zadeve, Uprava RS za informacijsko varnost, Nacionalni odzivni center za kibernetsko varnost ter z mnogimi izobraževalnimi ustanovami, vpeti smo v mednarodne organizacije s področja varnosti. Veliko pozornosti namenjamo izobraževanju najšibkejšega člena kibernetske varnosti – uporabnika informacijskih storitev. Zato je veliko naših rešitev namenjenih poenostavitvi in zavarovanju uporabniškega okolja, opolnomočenju uporabnikov in boljše kibernetske ozaveščenosti. Organiziramo tudi različne predstavitve Operativnega centra kibernetske varnosti, s čimer širimo zavedanje o pomenu kibernetske varnosti in ustreznih zaščitah v podjetjih, javnih ustanovah in drugih organizacijah.

Kako uspete v podjetju zagotavljati uravnoteženost med, na eni strani zelo restriktivnimi varnostnimi zahtevami varovanja ključnih informacij organizacije, in na drugi strani raziskovalni iniciativnosti, ki je včasih zelo občutljiva na prevelike omejitve delovnega okolja?

To ni tako zelo težko, ker je varnost kot temelj zaupanja postavljena med strateške prioritete in ima visoko podporo vodstva. Kot operater zagotavljamo delovanje sistemov in storitev 24/7/365, tako da imamo varnostne omejitve v genih in nam predstavljajo izziv, ne pa oviro. Je pa upravljanje velik izziv, ki zahteva vrhunske strokovnjake. Ponosen sem, da lahko rečem, da je ekipa Telekoma Slovenije državna reprezentanca v telekomunikacijah: nenehno ji uspeva zagotavljati uravnoteženost med varnostnimi zahtevami in zahtevami razvoja. Vse to je možno zaradi visoke predanosti, motiviranosti, znanja in odgovornosti zaposlenih. Standardizaciji, razvoju metodologij in seveda avtomatizaciji, ki zmanjšuje možnost človeških napak, namenjamo zelo veliko pozornosti. Od varnostnih ukrepov ne odstopamo. Razvrščamo jih v tri glavne skupine: preventivne (zmanjšujejo število incidentov oziroma verjetnost za nastanek incidenta), korektivne (zmanjšujejo izgubo v primeru incidenta) in detekcijske (skrajšajo čas, v katerem se incident zazna in omogočajo zbiranje podatkov za nadaljnje analize). Med preventivne ukrepe uvrščamo varnostno politiko, kriptografijo, varno arhitekturo omrežja





in aplikacij, ažurno posodabljanje programske opreme, požarne zidove, sisteme za preprečevanje vdorov v omrežje, DDoS-zaščito, mehanizme overjanja in avtorizacije uporabnikov, protivirusno programsko opremo, testiranja ranljivosti sistemov ter izobraževanja zaposlenih glede odzivanja na različne tehnike napadov. Predpogoj za pravočasen in predvsem pravi odziv so izkušeni strokovnjaki, ki pri svojem delu uporabljajo ustrezne programske rešitve, saj lahko napačna interpretacija varnostnega dogodka vodi v iskanje izvora groženj, ki to niso. Zato je pomembno, da strokovnjaki najprej ugotovijo resnost grožnje in njen obseg, ter nato ustrezno ukrepajo. Pri grožnjah z visoko stopnjo resnosti, pa je potrebno najprej poskrbeti za njihovo zajezitev z ustrezno izolacijo sistema ter izvesti obveščanje in ostale aktivnosti za nemoteno izvedbo preiskav glede vira grožnje. Samo z ustrezno preiskavo lahko namreč podobne grožnje preprečimo tudi v prihodnje.

Ste letošnji prejemniki prestižne nagrade Slovenian Grand Security Awards v kategoriji »Najbolj inovativna rešitev«, ki ste jo prejeli za razvoj svojega Operativnega centra kibernetske varnosti. Nam lahko zaupate kaj vam pomeni prejem take nagrade?

Prejeto priznanje potrjuje kakovost in strokovnost našega dela in Operativnega centra kibernetske varnosti, inovativnost naših strokovnjakov ter zavzetost zaposlenih Telekoma Slovenije. V Telekomu Slovenije smo leta 2016 postavili večletno strategijo celovitega razvoja informacijske in kibernetske varnosti. Zavedali smo se, da je to sistematični tek na dolge proge. To je bilo obdobje naraščajočega zavedanja groženj, država je pri aktivnostih na tem področju nekoliko zamujala, ob tem pa je tudi okolje (uporabniki, tehnološki partnerji, država) od nas pričakovalo, da na tem področju naredimo naslednji korak, saj nas prepoznava kot tistega, ki to zmore. Uspeli smo angažirati najboljše strokovnjake ter pridobiti in dodatno usposobiti številne nove. Vzpostavili smo lasten Operativni center kibernetske varnosti, ker lahko le na ta način zagotovimo najvišjo stopnjo kibernetske varnosti. Prejem nagrade tako predstavlja tudi priznanje za pravilnosti naših odločitev in uspešnosti naših prizadevanj. Redno sicer izvajamo tudi zunanje presoje, ki nam dajejo smernice za nadaljnje izboljšave, a že sedaj kažejo visoko stopnjo zrelosti in zmogljivosti, zato nagrado prejemamo s ponosom. Nagrada pomeni tudi to, da smo najbolje možno pripravljeni na razvoj v dobi prihajajoče pete generacije mobilnih omrežij (5G), ki bo pomembno zaznamovala novo desetletje.

Kako pristopate k prenosu lastnih varnostnih standardov v produkte, ki jih ponujate kot podporo delovanja drugih pomembnih organizacij? Verjetno je to pri storitvah zagotavljanja kibernetske varnosti ključnega pomena saj jih zagotavljate med drugim tudi za deležnike kritične infrastrukture?

Z izvajanjem storitev kibernetske varnosti za podjetja Skupine Telekom Slovenije imamo najboljšo možno referenco. Vse več organizacij nas tako prepoznava kot najbolj usposobljene in zaupanja vredne izvajalce storitve Operativnega centra kibernetske varnosti. Smo edini, ki lahko na tem področju ponudimo celovito rešitev, kar je v dobi IoT in 5G še toliko pomembneje. V Telekomu Slovenije načrtovanje varnostnih kontrol vključujemo že v začetne faze načrtovanja. Opravimo oceno tveganj, izvedemo identifikacijo in implementacijo varnostnih kontrol ter ugotavljamo morebitne ranljivosti. Med testiranjem varnostnega vidika opravimo verifikacijo implementiranih varnostnih kontrol in ranljivosti, preverimo kakovost kode ter po potrebi izvedemo vdorna testiranja. Na podlagi pridobljenih rezultatov ponovimo načrtovanje za odpravo pomanjkljivosti, implementacijo in ponovni test. Pri tem uporabljamo tudi informacije o ranljivostih in varnostnih dogodkih, ki jih pridobimo s strani dobaviteljev opreme ali drugih organizacij.

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

Vsekakor. Pri zagotavljanju varnosti sta najpomembnejša elementa zaupanje in sodelovanje, zato je izmenjava informacij in izkušenj izjemnega pomena. Zaupanje si je seveda potrebno pridobiti in ga tudi ohranjati. Slovensko združenje korporativne varnosti opravlja izredno pomembno poslanstvo povezovanja ključnih akterjev zagotavljanja varne družbe. Na ta način nastajajo nove ideje, rešitve, razvijajo se nove oblike sodelovanja. To je na področju varnosti še posebej pomembno, saj ni neke dokončne rešitve, vedno je potrebno biti v koraku s časom, z novimi tehnologijami, varnostni izzivi itd. Bitka za varno sodobno družbo ni nikoli končana. ■

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:

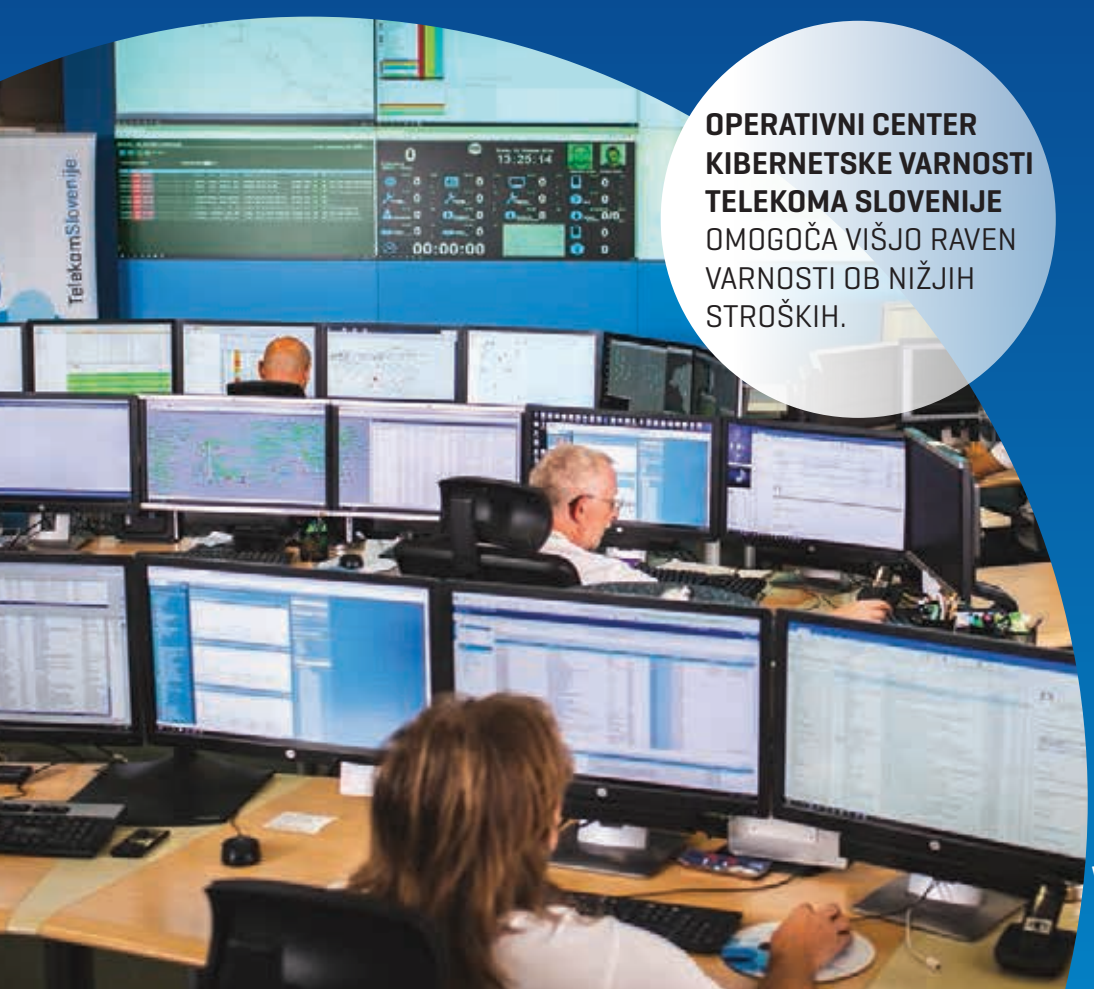
ZNIŽEVANJE OPERATIVNIH TVEGANJ POVEZANIH S KIBERNETSKO VARNOSTJO

+

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

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Andrej Maslo
direktor Korporativne varnosti in nadzora v Pošti Slovenije d.o.o.

KORPORATIVNA VARNOST KLJUČEN DEJAVNIK ZA OBVLADOVANJE TVEGANJ V POSLOVNIH OKOLJIH

V današnjem zahtevnem varnostnem okolju je zagotavljanje neprekinjenosti delovanja velikih poslovnih organizacij nujna za poslovno učinkovitost. Korporativna varnost ima v tem okviru posebej izraženo vlogo in odgovornost.

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

Izzivi obvladovanja široke palete varnostnih groženj v gospodarstvu, v moji dosedanji karieri predstavljajo pomemben del nalog in odgovornosti s katerimi sem se ukvarjal oz. se še vedno ukvarjam. Na začetku moje karierne poti sem se ukvarjal z načrtovanjem in izvajanjem različnih varnostnih ukrepov (ukrepi fizičnega in tehničnega varovanja, organizacijski ukrepi ipd.) za potrebe naročnikov varnostnih storitev, tudi takšnih, ki so danes upravljalci kritične infrastrukture. Izkušnje sem nato pridobival na specifičnem področju dela, in sicer na področju dela varnosti v igralništvu. Pri tem bi predvsem izpostavil, da sem sodeloval pri načrtovanju in vzpostavljanju sistema varnosti novega igralniško-zabaviščnega centra Mond v Šentilju, pod okriljem družbe HIT d. d., da bi nato tudi prevzel odgovornost za vodenje lastne varnostne službe v tem centru, kot tudi samega varnostnega sistema. Trenutno pa je moja kariera vezana na naloge korporativne varnosti in nadzora v Pošti Slovenije, kjer sem izvajal različne naloge - od strokovnega sodelavca do vodje oddelka korporativne varnosti, do nalog, za katere sem trenutno tudi odgovoren kot direktor korporativne varnosti in nadzora v Pošti. V tem okviru so moje glavne naloge in odgovornosti povezane z zagotavljanjem ukrepov obvladovanja groženj varnosti ljudi in premoženja, varnosti na področju varovanja podatkov in informacijske infrastrukture, obravnavo pojavov nezakonitih ravnanj zaposlenih, strank in tretjih oseb, izvajanjem ukrepov notranjega nadzora, zaradi preprečevanja neetičnih in nezakonitih ravnanj ter upravljanja procesa neprekinjenega poslovanja v Pošti Slovenije. Do reorganizacije strokovnih služb v Pošti Slovenije sem bil kot direktor tudi odgovoren za vodenje področja varnosti in zdravja pri delu ter požarne varnosti.

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

Razumevanje sprememb kompleksnega varnostnega okolja je po moji oceni zagotovo zelo pomemben dejavnik konkurenčne prednosti podjetij. Pa ne samo njihovo razumevanje,

g. Andrej Maslo je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2019«

*avtor je član Slovenskega združenja korporativne varnosti



ampak tudi ustrezno prilagajanje na te spremembe. Prožen sistem korporativne varnosti je praktično postal enakopravni in sestavni del vseh sistemov, ki potekajo znotraj vsakega sodobno naravnanega podjetja. Takšen sistem je v funkciji, da se učinkovito prilagaja aktualnostim sodobnega časa, da lahko tako uspešno obvladuje varnostne grožnje in s tem povezane izzive, ki se pojavljajo v podjetju in v njegovem okolju. S tem pa zagotavlja tudi nujno potrebne pogoje za nemoteno in razvojno usmerjeno delovanje vseh ostalih sistemov in procesov v podjetju. Še več, obvladovanje sodobnih varnostnih groženj je, poleg ustreznega razumevanja varnostnega okolja, podvrženo tudi razumevanju pomena vložkov v korporativni varnostni sistem oziroma njegove ukrepe skozi vrednotenje stroškovne upravičenosti posameznih vložkov in njihovih koristi, tudi v primerjavi z drugimi poznanimi načini obvladovanja tveganj. Slabo načrtovani in stroškovno nepremišljeni vložki pomenijo, da je podjetje neustrezno in neprimerno zaščiteno pred grožnjami in je zato tudi ranljivo ter visoko izpostavljeno tveganjem incidentov in drugih neželenih dogodkov. Hkrati pa to tudi pomeni, da so razpoložljivi viri neučinkovito porabljeni, kar v končni posledici tudi hromi tekoče poslovanje podjetja in njegovo sposobnost tržno naravnanega delovanja.

Prožen sistem korporativne varnosti je praktično postal enakopravni in sestavni del vseh sistemov, ki potekajo znotraj vsakega sodobno naravnanega podjetja. Takšen sistem je v funkciji, da se učinkovito prilagaja aktualnostim sodobnega časa, da lahko tako uspešno obvladuje varnostne grožnje in s tem povezane izzive, ki se pojavljajo v podjetju in v njegovem okolju.

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

Primarna dejavnost Pošte Slovenije je izvajanje univerzalne poštne storitve, ki je s strani države regulirana dejavnost, saj je izvajanje te dejavnosti v interesu države. Skladno s sprejetimi strategijami, pa se dejavnost Pošte Slovenije usmerja tudi v nadgradnjo obstoječih storitev in v nove storitve. Pri tem je ključni poudarek na storitvah prodaje blaga, paketne dostave, denarnega poslovanja, logistike ter e-storitvah za posameznike, podjetja in državo. Z nakupom logističnega podjetja Intereuropa d .d., pa je Pošta Slovenije svojo mrežo poslovanja razširila tudi daleč preko meja Republike Slovenije. Široka paleta dejavnosti, s katerimi se Pošta Slovenije ukvarja, razvejanost in geografska razpršenost mreže, del katere sta tudi oba poštno-logistična centra, kjer je med drugim organizirana obvezna služba varovanja, skladno z določili ZZasV, vpetost poštne mreže v sistem evropske in svetovne poštne zveze ipd. so samo nekateri od dejavnikov, ki predstavljajo kompleksne varnostne interese in potrebe ter zato tudi narekujejo različne pristope pri obvladovanju groženj. Pri tem je pomembno, da imamo za obvladovanje varnostnih groženj sprejete (minimalne) varnostne standarde, ki so skupni vsem dejavnostim in deležnikom, ki se pojavljajo v mreži Pošte Slovenije ter, da pri načrtovanju ukrepov izhajamo iz dobro zastavljenih varnostnih ocen ter na njih pripravljenih analizah, upoštevajoč tudi vse posebnosti, ki so značilne za okolje, dejavnosti in procese v Pošti Slovenije – npr. varnostni interesi in potrebe poslovalnice v Ljubljani so različni od poslovalnice v Murski Soboti, varnostni interesi in potrebe logistične dejavnosti so različni od dejavnosti denarnega poslovanja itd..

Kibernetska varnost je v vaši dejavnosti izrednega pomena. Kako v vašem podjetju ocenjujete izvajanje potrebnih ukrepov na tem kompleksnem področju?

V Pošti Slovenije se zavedamo pomembnosti informacijske varnosti, katere del je tudi kibernetska varnost. Vzpostavljen in vpeljan imamo celovit sistem upravljanja z informacijsko varnostjo, pri čemer je področje, ki ga vodim tudi odgovorno za upravljanje s tem sistemom v Pošti. V letu 2017 smo opravili tudi certifikacijo po standardu ISO/IEC 27001:2013 za del informacijskega sistema, ki ga tržimo kot storitev našim strankam. Ukrepe za varovanje informacij določamo na podlagi ocene in analize tveganj, obravnave preteklih dogodkov in na podlagi spremljanja dogajanja na področju kibernetskega kriminala pri nas in v svetu. Pri izvedbi izhajamo iz standardov in priporočil dobrih praks, ki veljajo na področju informacijske varnosti. Prizadevamo si, da so ukrepi učinkoviti, če je mogoče avtomatizirani, njihovo delovanje in učinkovitost pa spremljamo in po potrebi ukrepe tudi prilagajamo.

Se v Republiki Sloveniji po vaše dovolj zavedamo pomembnosti področja kibernetske varnosti? So ukrepi, ki jih izvaja država na tem področju ustrezni ali pogrešate konkretnejše ukrepe?

Mislim, da ni potrebno posebej poudarjati, da so kibernetske grožnje realnost. Samo delovanje družbe je danes v veliki meri odvisno od tehnologije in informacijskih storitev. Da je družba in posameznik premalo ozaveščen glede kibernetskih groženj, lahko sklepamo na podlagi dejstva, da tudi nekateri uspešni kibernetski napadi ter dogodki povezani s kibernetskim kriminalom, ki prizadenejo posameznike in tudi družbo kot celoto, niso dvignili zavedanja pomembnosti kibernetske varnosti. Država je prav gotovo tisti deležnik, ki lahko skozi regulativo in aktivno podporo pri izvajanju sprejete regulative pozitivno vpliva na zavedanje in odnos do informacijske in s tem tudi kibernetske varnosti. Imamo nacionalni odzivni center za kibernetsko varnosti (SI-CERT), ki je bil ustanovljen že davnega leta 1995 in, ki je vse od ustanovitve pa do danes praktično tudi edino operativno telo oz. inštitucija, ki ima razpoložljive vire, znanja in izkušnje, da podjetjem in posameznikom nudi ustrezno podporo in svetovanje v primeru kibernetskih incidentov. V letu 2018 je bil sprejet Zakon o informacijski varnosti, ki ni zaživel v celoti, saj je bil pristojni nacionalni organ Uprava za informacijsko varnost ustanovljen šele konec lanskega leta. Tudi na tem področju država z regulativo in izvajanjem le-te zaostaja za potrebami sodobne družbe. Aktualno dogajanje na tem področju sicer kaže pozitivne premike v smeri, da se bo država bolj sistematično lotila obvladovanja groženj kibernetske varnosti, kar je dejansko že nujno potrebno, ne samo iz vidika potreb posameznika in gospodarstva, ampak tudi z vidika nujnosti, da se zagotovijo ustrezni pogoji za nemoteno delovanje države in družbe.

Nam lahko zaupate kako pomemben je v takih primerih učinkovit sistem varovanja ključnih poslovnih informacij.

Ocenjujem, da se zavedanje strateškega managementa v slovenskih podjetjih, glede pomena korporativne varnosti ter njenega prispevka k učinkovitemu obvladovanju groženj, postopoma izboljšuje, čeprav je trenutno stanje še daleč od tistega, ki bi si ga mi v stroki verjetno tudi želeli.

Učinkovit sistem varovanja informacij je prav gotovo konkurenčna prednost. Danes ni dovolj samo, da podjetje posluje skladno z veljavnimi predpisi (varovanje poslovnih skrivnosti, varstvo osebnih podatkov) in hkrati izpolnjuje ključna načela informacijske varnosti – zaupnost, razpoložljivost in celovitost informacij. Vse to je potrebno početi tudi racionalno, torej tako, da so sredstva, ki jih namenimo varovanju informacij usmerjena v ukrepe, ki so učinkoviti in najbolj znižajo tveganja. Podatki, s katerimi podjetja razpolagajo, so postali tržno blago. Podjetja so vedno bolj odvisna od informacijskih storitev, kjer se podatke obdeluje in na podlagi tega sprejema odločitve. Če so bili podatki podjetja v preteklosti zanimivi recimo zgolj za poslovne konkurente, so danes podatki bistveno bolj zanimivi kibernetskemu kriminalu. Prav tako so se spremenili in prilagodili vzorci napadov. Danes ni več zanimiva vsebina podatkov, temveč je pogosto dovolj, da napadalec onemogoči dostop do podatkov in s tem ohromi poslovanje podjetja. Vse to zahteva, da podjetje vzpostavi var-



V pomanjkanju znanja in zavedanja strateškega managementa o pomenu korporativne varnosti, je pomembna vloga samih strokovnjakov korporativne varnosti, da najvišjemu managementu predstavijo prednosti in koristi, ki jih podjetju prinaša dobro zastavljen in delujoč sistem korporativne varnosti.

nostni sistem, ki učinkovito varuje podatke in se je sposoben prilagajati novim okoliščinam, hkrati pa ob incidentih zagotoviti hiter in učinkovit odziv ter čimprejšnje okrevanje.

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

Poslovodstvo Pošte Slovenije razume potrebe in izzive korporativne varnosti v sodobnem okolju ter kaže velik interes za aktivnosti, ki se izvajajo na tem področju. Generalni direktor Pošte Slovenije mag. Boris Novak je svojo kariero v Pošti Slovenije začel s postavljanjem okvirov sodobnega sistema korporativne varnosti Pošte, tako da iz tega vidika problemi in izzivi, s katerimi se srečujemo v področju, poslovodstvu tudi niso tuji. Poslovodstva zato ni potrebno prepričevati za vire, ki so potrebni za delovanje sistema korporativne varnosti Pošte, je pa potrebe potrebno ustrezno strokovno argumentirati in predstaviti, tako z vidika varnostnih ocen in analiz, ki so osnova vsakega načrtovanja, ciljev, ki jih pri tem zasledujemo in pričakovanih koristi, kakor tudi povratne zanke v smislu ocenjevanja učinkov izvedenih ukrepov in aktivnosti.

Verjetno redno spremljate stanje na področju korporativne varnosti v slovenskem okolju. Kako bi ocenili zavedanje strateškega managementa v slovenskih podjetjih o pomenu korporativne varnosti in učinkovitega obvladovanja tveganj?

Ocenjujem, da se zavedanje strateškega managementa v slovenskih podjetjih, glede pomena korporativne varnosti ter njenega prispevka k učinkovitemu obvladovanju groženj, postopoma izboljšuje, čeprav je trenutno stanje še daleč od tistega, ki bi si ga mi v stroki verjetno tudi želeli. Dejstvo je, da so bili v preteklosti narejeni pomembni koraki v smeri, da varnostni management v podjetjih vedno bolj pridobiva na vlogi in pomenu, možnosti napredka in dviga pomembnosti samega področja za učinkovito obvladovanje tveganj pa je še veliko. In s tem se bo tudi zavedanje samega strateškega managementa o pomembnosti korporativne varnosti, tudi kot orodja za uspešno upravljanje podjetja, samo še dvigovalo. Strateški management je zainteresiran za čim višjo dobičkonosnost podjetij, slednjo pa načenjajo tudi škode in izgube, ki so lahko posledica šibkega zavedanja korporativne varnosti v podjetjih. V pomanjkanju znanja in zavedanja strateškega managementa o pomenu korporativne varnosti, je pomembna vloga samih strokovnjakov korporativne varnosti, da najvišjemu managementu predstavijo prednosti in koristi, ki jih podjetju prinaša dobro zastavljen in delujoč sistem korporativne varnosti.

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

Nedvomno so podjetja, ki vlagajo v lastni kader v obliki izobraževanja in usposabljanja, dolgoročno uspešnejša od tistih, ki temu ne posvečajo dovolj velike pozornosti. Tega se vse bolj zaveda tudi večina podjetij, saj v izobraževanju lastnega kadra vidijo tudi konkurenčne prednosti pred svojimi tekmeci. Pri tem pa je tudi pomembno, da podjetja poskrbijo za ustrezno izobraževanja svojih zaposlenih o varnosti, varnostnih grožnjah in o ravnanju, ki lahko predstavlja tveganje tako za varnost posameznika kot tudi za podjetje, v katerem ta posameznik deluje. Tehnični ukrepi in zaščite pri obvladovanju varnostnih groženj so danes že zelo dobro razviti in jih je z vidika njihovega »premagovanja« težko zaobiti. Zato se fokus napada vedno bolj seli na človeka, ki je še vedno v celotnem sistemu prepoznan kot najšibkejši člen. Vložki v izobraževanje in ozaveščanje posameznikov, da v vsakdanjih okoliščinah ravnajo ustrezno, tudi z mislijo na varnost, so v primerjavi z vložki v tehnično zaščito relativno majhni. V kolikor je takšno izobraževanja izvedeno ciljno in vsebinsko dobro zastavljeno, je to tudi najbolj učinkoviti ukrep za obvladovanje groženj, s katerimi se lahko posamezniki srečajo pri izvajanju vsakodnevnih poslovnih opravil.

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

Že v sklopu enega izmed predhodnih vprašanj sem poudaril vlogo stroke pri aktivni promociji pomena in vloge korporativne varnosti pri obvladovanju groženj v podjetjih. Pri tem ne morem mimo poslanstva Slovenskega združenja korporativne varnosti, ki se je uveljavilo kot priznano strokovno združenje v slovenskem in širšem okolju. V sklopu združenja se združujemo strokovnjaki iz različnih področij obvladovanja tveganj v podjetjih in v javni upravi, s čimer je vzpostavljena tudi ustrezna platforma, ki na eni strani skrbi za izmenjavo izkušenj, primerov dobrih praks ipd., na drugi strani pa tudi skrbi za nujni nadaljnji razvoj stroke in njene promocije tako pri najpomembnejših odločevalcih kot tudi v širšem prostoru.

Kaj vam pomeni prejeta nagrada Slovenian Grand Security Award v kategoriji »korporativno varnostni manager leta«?

Nagrada mi predstavlja pomembno priznanje za opravljeno delo, še toliko bolj, ker je podeljena s strani strokovnega združenja, ki je referenca na področju korporativne varnosti tako v Sloveniji kot tudi v regionalnem in širšem mednarodnem okolju. Takšna nagrada pa mi tudi predstavlja veliko obvezo in odgovornost tudi za prihodnje delo. Hkrati pa moram tudi poudariti, da je ta nagrada tudi nagrada in priznanje ekipi mojih sodelavcev, s katerimi vsakodnevno sodelujemo pri aktivnostih in projektih na področju korporativne varnosti. ■

VI PROTI POŽARU

Bonpet - Najboljša zaščita življenj in premoženja.

18 LET TRADICIJE
MEDNARODNI CERTIFIKATI
PRISOTNI V VEČ KOT 25 DRŽAVAH IN 5 KONTINENTIH
MEDNARODNI IN SLOVENSKI CERTIFIKATI
REŠITVE ZA ZAŠČITO DOMA
PROFESIONALNE REŠITVE ZA INDUSTRIJO
SPECIALISTI ZA POŽARNI RAZRED F
REŠITVE Z AVTOMATSKIM DELOVANJEM

Bonpet systems

Zanesljivi gasilni sistemi



Ko ogenj že zagori, je razmišljanje o preventivi prepozno. Edino pravilno je, da smo na požar pripravljeni ves čas. Vendar ne na katerikoli način. Ker so najtežje ravno bitke s požarom, je treba v preventivo vložiti tista gasilna sredstva, ki se bodo aktivirala v pravem trenutku na pravem mestu. S ponosom in veseljem vam predstavljamo gasilna sredstva Bonpet.

BONPET SYSTEMS d.o.o.
Obrtniška cesta 30, 1420 Trbovlje
tel: +386-3-56-14-720
GSM: +386-51-630-209
info@bonpet.si

www.bonpet.si

Avtor: ddr. Aleš Jug / Becker College, Massachusetts, ZDA



NEMOTENO POSLOVANJE PODJETJA IN POŽARNA VARNOST

Načrt neprekinjenega poslovanja podjetja lahko razumemo kot nadstandard, ki ga na ravni podjetja sprejmejo kot del poslovne politike. Je veliko več, kot zgolj zahteva predpisov. V podjetju vzpostavi sistem ravnanja s tveganji, ki je v današnjem konkurenčnem in globalno povezanem svetu eno od zagotovil, ki podjetju lažje omogoča trajnostni razvoj.

Uvod

V interesu zagotavljanja varnosti se podjetja lotevajo več ukrepov. Tisti standardni in navadno prvi je skladnost s predpisi. Pogosto namreč po nezgodi zasledimo komentarje vodstva podjetja, češ saj smo imeli vse po predpisih. Kdor se vsaj malo ukvarja z varnostjo ve, da predpisi navadno ne zagotavljajo niti optimalne varnosti. So nek konsenz med stroški in stopnjo pričakovane varnosti, ki si jo država lahko privošči oz. jo izpogaja strokovna javnost. Pogosto so ukrepi za zagotavljanje varnosti na ravni podjetja kampanjski, vezani na trenutne trende (odziv na minule požare, spremembno predpisov, zahtevo zavarovalnic ali novega lastnika) in ne odraz načrtnega planiranja vezanega na presojo tveganj širšega spektra, kamor nedvomno spadajo tveganja, ki jih povzročajo tehnološki procesi a hkrati tudi finačna tveganja, ki jih predstavlja motnja v poslovanju. Proces analize motenj poslovanja in na to vezanih ukrepov ter podpornih sistemov imenujemo upravljanje nemotenega poslovanja podjetja.

Upravljanje nemotenega poslovanja podjetja

Živimo v zelo dinamičnem in povezanem svetu. Podjetja poslujejo tako preko potrošnikov kot oskrbovalnih verig, pogosto globalno. Ob veliko prednostih globalnega trga, pa ima le ta tudi nekaj pomanjkljivosti. Velika konkurenčnost hkrati pomeni tudi večja tveganja, ki se jh podjetja pogosto manj zavedajo in jih še težje napovejo oz. obvladajo. Ne glede na to, kakšnim tveganjem je izpostavljeno, mora podjetje za to, da ostaja likvidno, v oskrbovalno verigo dobavljati izdelke, storitve ali oboje. Nenazadnje je to edina aktivnost, ki omogoča priliv sredstev. Podjetje mora poslovati čim bolj stabilno, biti zanesljiv partner v oskrbovalni verigi in opravičevati zaupanje kupcev. Vse ostalo mora biti temu podrejeno. Lastnost podjetja, da posluje nemoteno ter na trg pošilja izdelke ali storitve, imenujemo nemotenost poslovanja podjetja. Nemoteno poslovanje je cilj, ki si ga mora podjetje zastaviti že v poslovnem načrtu. Je del vizije, poslanstva podjetja, ki ga pa v praksi ni tako enostavno izvajati. Tako na domačem kot globalnem trgu so podjetja izpostavljena tveganjem, ki lahko za podjetje povzročijo okoliščine, ki bolj ali manj vplivajo na poslovanje. Motnje poslovanja so lahko komaj opazne ali takšne, ki podjetje spravijo iz ravnovesja oz. v finančne težave. Izsledki raziskave revije Financial management (Amato 2019), izpostavljajo tveganja, ki v letu 2020 grozijo podjetjem.

Mednje prištevamo:
- pravočasno prepoznavanje kritičnih tveganj (npr. požari in eksplozije),
- ustreznost predlaganih procesov za obvladovanje tveganj,
- zmožnost prilagajanja vodstev podjetij varnostni kulturi in procesom za obvladovanje tveganj,
- vzpostavitev zadostne robustnosti sistemov,
- prilagajanje obstoječih operacij in infrastrukture digitalnim konkurentom,

Zagotavljanje neprekinjenega poslovanja zahteva ustrezno načrtovanje. Načrtovanje neprekinjenega poslovanja je postopek vzpostavitve mehanizmov prepoznavanja, preprečevanja in okrevanja v primeru, ko je podjetje izpostavljeno tveganjem.



- normativne spremembe in povečan normativni nadzor,
- kibernetska tveganja in informacijska varnost,
- odpor do sprememb in nove tehnologije,
- nezmožnost ravnanja z velikimi podatki z namenom poznavanja trga in povečanja produktivnosti in učinkovitosti
- ohranjanje zvestobe strank/negativna publiciteta.

Po opisu tveganj vidimo, da gre za mešana tveganja, vezana na sam tehnološki proces a hkrati tudi upravljanje podjetij, varnostno kulturo, spremljanje sprememb kot tudi odnos s kupci, ipd. Med navedenimi tveganji so tista, ki so najbolj verjetna in so se v obdobju nekaj zadnjih let najpogosteje pojavljala. Poleg naštetih so tudi tveganja, ki se pojavljajo redkeje in jih težje napovemo. Primer je izbruh korona virusa, ki je z žariščem v Kitajskem industrijskem centru v nekaj tednih na glavo postavil marsikakšen poslovni model podjetij ali oskrbovalnih verig širom po svetu, ki niso bile pripravljene na tveganje ter posledice in predvidene ukrepe, ki bi lahko vpliv tveganja zmanjšali.

Podobno je požar v ameriški tovarni avtomobilskih menjalnikov, pomembnem dobavitelju tovarne Ford, leta 2019 za več tednov ustavil proizvodnjo linijo Fordovih najbolje prodajanih vozil na ameriškem trgu, poltovornjaka F-150.

Zagotavljanje neprekinjenega poslovanja zahteva ustrezno načrtovanje. Načrtovanje neprekinjenega poslovanja je postopek vzpostavitve mehanizmov prepoznavanja, preprečevanja in okrevanja v primeru, ko je podjetje izpostavljeno tveganjem. Poleg samega preprečevanja tveganj, je cilj načrtovanja neprekinjenega ravnanja podjetja predvideti in omogočiti tekoče poslovanje podjetja v času okrevanja. Nekateri podatki kažejo, da se z motnjo poslovanja sooča skoraj vsako peto podjetje.

Motnje, ki lahko trajajo od nekaj minut do več mesecev, predstavljajo za podjetje predvsem veliko finančno breme. Le to se odraža v direktnih in indirektnih stroških. Nekatera podjetja se po motnji nikoli več ne postavijo na noge.

Nekatere lastnosti organizacij, pripravljenih na motnje poslovanja so:
- sposobnost prepoznavanja sprememb in dejavnikov, ki lahko vodijo v motnje poslovanja še preden se pojavijo,
- aktiven odziv na tveganja,
- sposobnost pridobivanja dobička, ko se zaradi izkazanih novih tveganj pojavijo priložnosti
- sposobnost preprečevanja nastanka kriznih dogodkov s preventivnimi aktivnostmi,
- sposobnost obvladovanja kriz, ko se le te pojavijo, z ustreznimi odzivi na podlagi vnaprej pripravljenih protokolov in usposabljanja.

Požarna varnost in nemoteno poslovanje podjetja

Pomemben del aktivnosti vezanih na načrtovanje nemotenega poslovanja podjetja so tudi požarna tveganja. Poleg neposredenega ogrožanja ljudi, živali in okolja ima požar na podjetje tudi manjše ali večje finančne posledice. Zaradi požara lahko nastajajo materialni, stroški poslovanja in razni drugi stroški (slika 1).



Slika 1: Struktura stroškov, ki lahko nastanejo zaradi požara



Tipični predstavniki materialnih stroškov so škoda na objektih, hranjenih dobrinah in napravah ter opremi. Med stroške poslovanja spada izpad prihodka, penali, zvišanje zavarovalnih premij, izguba trga, morebitni stroški kreditov, potrebnih za sanacijo. Med druge stroške spada popožarna sanacija, dodatna strokovna mnenja in ekspertize za povrnitev v prvotno stanje, stroški vezani na morebiten izpad zaposlenih (usposabljanje novih zaposlenih), odškodnine in kazni.

Večji del stroškov in morebitnih izgub, ki lahko bremenijo podjetje po požaru, klasičen pristop z upoštevanjem predpsiov ne pokrije. Zelo malo si lahko podjetje kljub izpolnjevanju normativov pomaga v smeri zaščite pred prekinitvijo poslovanja. Namen predpisov je namreč v zaščiti življenj in deloma premoženja. Vse, kar bo podjetje za varnost naredilo več, je del njihove politike, poslovnih strategij in vizij.

V požaru je lahko poškodovana nujno potrebna oprema za izdelavo proizvoda, ki ga podjetje uspešno prodaja na tujih trgih. Podjetje je del oskrbovalnih verig, kjer so obveznosti podrobno opredeljene. Neizpolnjevanje pogodbenih zahtev lahko pomeni popolno prekinitev sodelovanja oskrbovalne verige s podjetjem. Z vidika predpisov podjetju v prostor, kjer se nahaja pomembna oprema, morda sploh ni treba namestiti stabilnih sistemov za gašenje. Šele analiza nemotenosti poslovanja lahko pokaže, da je omenjena oprema za podjetje del kritične infrastrukture. V primeru izgube v podjetju opreme navadno ne morejo hitro in enostavno namestiti. Pogosto je treba zelo specialno opremo naročiti in nanjo čakati tudi eno leto ali več. Kako bo podjetje poslovalo v tem času? Imajo rezervni plan? Naredijo dovolj za požarno preventivo in ukrepe, ki bi že v osnovi preprečili nastanek požara in poškodbo opreme?

Ukrep, ki sistemsko rešuje ravnanje z ranljivo infrastrukturo, je načrt nemotenega poslovanja podjetja.

Ustrezno narejen načrt nemotenega poslovanja podjetja pomaga podjetju pri iskanju nekaterih ključnih odgovorov, kot npr.:

- odpornost podjetja na motnje - odpornost je sposobnost prilagajanja organizacije na motnje, katerim je izpostavljena. Načrtovanje odpornosti podjetja se nanaša na pripravo smernic in navodil za zagotavljanje sposobnosti osebja, da se po motnjah odzovejo in nadaljujejo ter obnovijo delovanje podjetja na vnaprej določeno raven. Med najpomembnejše elemente odpornosti podjetja na motnje, spada poslovanje s strankami in izpolnjevanje zahtev vezanih na stranke podjetja.
- identifikacija ključnih proizvodov/storitev, ki ustvarijo največ vrednosti za kupce (B to B in B to C model)
- iskanje povezav med ključnimi proizvodi/storitvami ter potrebnimi tehnologijami/procesi,
- odziv podjetja na odpovedi/izgube in grožnje,
- opredelitev glavnih tveganj,
- aktivnosti, ki jih izvajajo v podjetju za dosego neprekinjenega poslovanja.

Načrt neprekinjenega poslovanja podjetja lahko razumemo kot nadstandard, ki ga na ravni podjetja sprejmejo kot del poslovne politike. Je veliko več, kot zgolj zahteva predpisov. V podjetju vzpostavi sistem ravnanja s tveganji, ki je v današnjem konkurenčnem in globalno povezanem svetu eno od zagotovil, ki podjetju lažje omogoča trajnostni razvoj. ■

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"

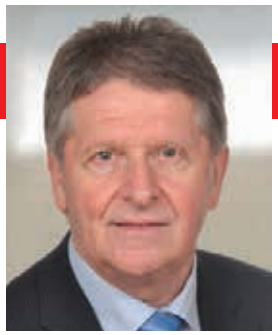
NAPREDNE TEHNOLOGIJE VAROVANJA

Smo ekskluzivni zastopnik za profesionalno opremo najvišjega kakovostnega razreda Tecnoalarm



ZARJA ELEKTRONIKA

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



NEPREKINJENO POSLOVANJE: »NIČ NE DELA, KAJ PA ZDAJ?«

Izredne dogodke ne moremo načrtovati, lahko pa načrtujemo zmanjšanje njihovih posledic. Učinkovita odzivna struktura in postopki odziva na izredne dogodke predstavljajo predpogoj za učinkovito zagotavljanje neprekinjenega poslovanja.

Uvod

Bivši državni sekretar ZDA H. Kissinger je nekoč dejal: »Prihodnji teden ne more biti nobene krize. Moj urnik je že poln!« Sedaj živimo v kaotičnem svetu, krize in izredni dogodki se skoraj tedensko pojavljajo, nevarnosti in ogrožanja so na vseh področjih družbenega življenja vse večja in vse bolj nasilna. Organizacije delujejo globalno, zato so nevarnosti in tveganja tudi globalna. Organizacije brez načrtov za primer realizacije izrednih dogodkov, zaradi človeškega ali naravnega dejavnika, lahko v skrajnem primeru svoje storitve ali izdelke prenehajo ponujati na trgu proti svoji volji in kasneje lahko tudi propadejo. Zato bi bilo skrajno neodgovorno in v neskladju z načeli dobrega gospodarja, da se ne pripravijo na te dogodke.

Neprekinjeno poslovanje

Vsaka organizacija mora imeti načrt neprekinjenega poslovanja. Učinkovit sistem za zagotavljanje neprekinjenega poslovanja in obnovo po izrednem dogodku, ki poslovanje čimprej povrne v normalne okvirje, je zahtevna naloga. Resnica glede rešitev za zagotavljanje neprekinjenega poslovanja je, da so organizacije najbolj zadovoljne, če jih ne bodo potrebovale. Številne organizacije tovrstne rešitve obravnavajo kot nujno zlo in jim ne posvetijo ustrezne pozornosti ter virov, zato pogosto odpovedo takrat, ko jih dejansko rabijo – v najbolj kritičnih trenutkih.

Upravljanje neprekinjenega poslovanja je definirano kot holističen pristop, ki identificira potencialne nevarnosti in grožnje organizacije ter njihov vpliv na vse poslovne procese. Upravljanje neprekinjenega poslovanja predstavlja osnovni okvir za vzpostavitev sistema poslovne odpornosti na vsa tveganja, ki vplivajo na ugled, finance, ključne nosilce organizacije, dodano vrednost in ostale pomembne elemente uspešnega ter stabilnega poslovanja organizacije.

Mednarodna raziskava ugotavlja (Business Continuity Institute, BCI, 2019), da bodo večje nevarnosti in tveganja v letu 2020 (po vrstnem redu verjetnosti): napadi na informacijsko varnost in zloraba osebnih podatkov, izpadi IT in telekomunikacij, naravne nesreče, okvare kritične infrastrukture, izguba ugleda, zakonske spremembe, pomanjkanje ključnih zaposlenih, motnje v oskrbi, prekinitve komunalne oskrbe, politične spremembe, uvedba novih tehnologij, zdravstvena in varnostna ogrožanja, strelski napadi, volatilnost valut, izbruhi bolezni, višji stroški zadolževanja, politično nasilje in državljanski nemiri, slabša kakovost izdelkov in pomanjkanje naravnih virov.

Navedeni dogodki kažejo na širok spekter ogrožanj, na katere se morajo odgovorne organizacije pripraviti, da ne bodo presenečene, saj se to ne dogaja samo drugim, lahko se tudi njim. Organizacije, ki navedeno ne bodo upoštevale kot resno grožnjo z visoko verjetnostjo, s katero se bodo lahko v prihodnosti soočile in pripravile načrte za njihovo upravljanje, se ne izpostavljajo samo izgubi ugleda, temveč tudi visokim finančnim stroškom.

Neprekinjeno poslovanje je sposobnost organizacije, da po izrednem dogodku nadaljuje z dobavo proizvodov ali storitev na sprejemljivi, vnaprej določeni

Vsaka organizacija mora imeti načrt neprekinjenega poslovanja. Učinkovit sistem za zagotavljanje neprekinjenega poslovanja in obnovo po izrednem dogodku, ki poslovanje čimprej povrne v normalne okvirje, je zahtevna naloga.

*avtor je član Slovenskega združenja korporativne varnosti



ravni. Letos je Mednarodna organizacija za standardizacijo objavila standard sistema upravljanja neprekinjenega poslovanja ISO 22301: 2019, Varnost in odpornost - Sistemi upravljanja neprekinjenega poslovanja – Zahteve. Standard določa zahteve za načrtovanje, vzpostavitev, izvajanje, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje upravljanja sistema za zaščito pred izrednimi dogodki, zmanjšanje verjetnosti njihovega pojava in priprave ter odzivanje nanje. Standard je sestavljen iz medsebojno povezanih elementov, ki jih organizacija uporablja za vzpostavitev sistema neprekinjenega poslovanja. V vse elemente so vključeni zaposleni, postopki, pravilniki, procesi, struktura in viri.

Za doseganje organizacijske odpornosti je potrebna identifikacija, ne samo velikih tveganj, ampak tudi premalo ocenjenih tveganj, ki se lahko zdijo samo kot »posel kot običajno«.

Odziv na izredne dogodke

Izredne dogodke ne moremo načrtovati, lahko pa načrtujemo zmanjšanje njihovih posledic. Učinkovita odzivna struktura in postopki odziva na izredne dogodke predstavljajo predpogoj za učinkovito zagotavljanje neprekinjenega poslovanja. Vprašanja, ki se ob tem porajajo, so npr.: kako določiti prijavno točko za izredne dogodke, kako ob njih čim hitreje obveščati relevantne deležnike v organizaciji in širše, kako razvrščati dogodke, kdo naj sprejema odločitve v tem obdobju, kako je z obveščanjem in poročanjem, kakšna je povezava z načrti neprekinjenega poslovanja ipd. Za vzpostavitev načrta neprekinjenega poslovanja so potrebne kot dobra praksa zlasti naslednje aktivnosti:

- določitev politike, namena, področja uporabe in cilji načrta,
- ključne vloge in odgovornosti,
- ocena ranljivosti in ogroženosti,
- analiza stanja in opredelitev ključnih poslovnih procesov,
- izvedba analize vplivov na poslovanje (BIA),
- ocenjevanje in upravljanje tveganj,
- načrt neprekinjenega poslovanja v skladu s standardom,
- krizni načrt,
- načrt kriznega komuniciranja,
- načrt evakuacije,
- avtonomni sistem energijske podpore,
- varnostne kopije,
- rezervna lokacija,
- scenariji obvladovanja izrednih dogodkov,
- testiranje načrtov neprekinjenega poslovanja,
- izobraževanje in ozaveščanje zaposlenih.

Sistem vodenja neprekinjenega poslovanja je metodologija in praksa, ki vzdržuje poslovanje organizacije v izrednih dogodkih in zmanjšuje njihov vpliv na stranke, delničarje in poslovni sistem. Predstavlja učinkovito pot za vzdrževanje varnosti, zagotavlja korporativno vodenje in skladnost poslovanja, ščiti ugled in hkrati vzpostavlja zaupanje strank v stabilnost poslovanja.



Rezultati analize vplivov na poslovanje so:
- opredelitev vplivov izpada poslovanja,
- opredelitev soodvisnosti poslovnih funkcij,
- opis najmanjšega možnega nabora virov za izvajanje poslovanja.

Iz rezultatov analize tveganj in analize vplivov na poslovanje se določi strategija neprekinjenega poslovanja. Na podlagi strategije vodstvo organizacije odloči, na kakšen način bo obvladovalo izredne dogodke.

Zaključek

Sistem vodenja neprekinjenega poslovanja je metodologija in praksa, ki vzdržuje poslovanje organizacije v izrednih dogodkih in zmanjšuje njihov vpliv na stranke, delničarje in poslovni sistem. Predstavlja učinkovito pot za vzdrževanje varnosti, zagotavlja korporativno vodenje in skladnost poslovanja, ščiti ugled in hkrati vzpostavlja zaupanje strank v stabilnost poslovanja.

Misel na možne izredne dogodke, katere si pred časom niti nismo znali predstavljati, je danes standard neprekinjenega poslovanja. Poslovanje organizacije ob izrednih dogodkih je za njo prej potreba in zahteva kot le želja.

Obstajajo vsaj štiri bistvene poslovne koristi, ki jih organizacija doseže z izvajanjem neprekinjenega poslovanja, in sicer: (i) upošteva zakonske zahteve, (ii) doseže tržno prednost, (iii) zmanjša posledice izrednega dogodka, (iv) obnovi in povrne poslovanje. Poudarek je na postopkih in navodilih. Pomembno je spoznanje, da neprekinjenega poslovanja ne moremo organizirati potem, ko se je izredni dogodek že zgodil; neprekinjeno poslovanje je potrebno načrtovati vnaprej.

Priprave obsegajo pregled poslovnih zahtev in ciljev, identifikacijo kritičnih poslovnih procesov, opredelitev sprejemljivega časa »neposlovanja«, načrt implementacije ukrepov in aktivnosti ter testiranje rešitev.

Ob morebitnem izrednem dogodku je treba nanj čim hitreje reagirati, zlasti: SPREJETI ODLOČITEV, DA GRE ZA IZREDNI DOGODEK, o tem obvestiti izvajalce poslovnih procesov, pričeti izvajati odziv nanj, obvestiti odgovorne za poslovanje in nadomestiti izpad zaposlenih ter sredstev (selitev na rezervno lokacijo, uporaba rezervnih zmogljivosti v oblaku ali hibridnem okolju, vključitev dodatnih izvajalcev ipd.). Biti zaskrbljen v razpravi o neprekinjenem poslovanju žal ni dovolj!

Vira:

- Business Continuity Institute (BCI, 2019), https://www.bsigroup.com/globalassets/documents/iso-22301, pridobljeno 11.11.2019,
- ISO 22301: 2019, Varnost in odpornost - Sistemi upravljanja neprekinjenega poslovanja – Zahteve. ■



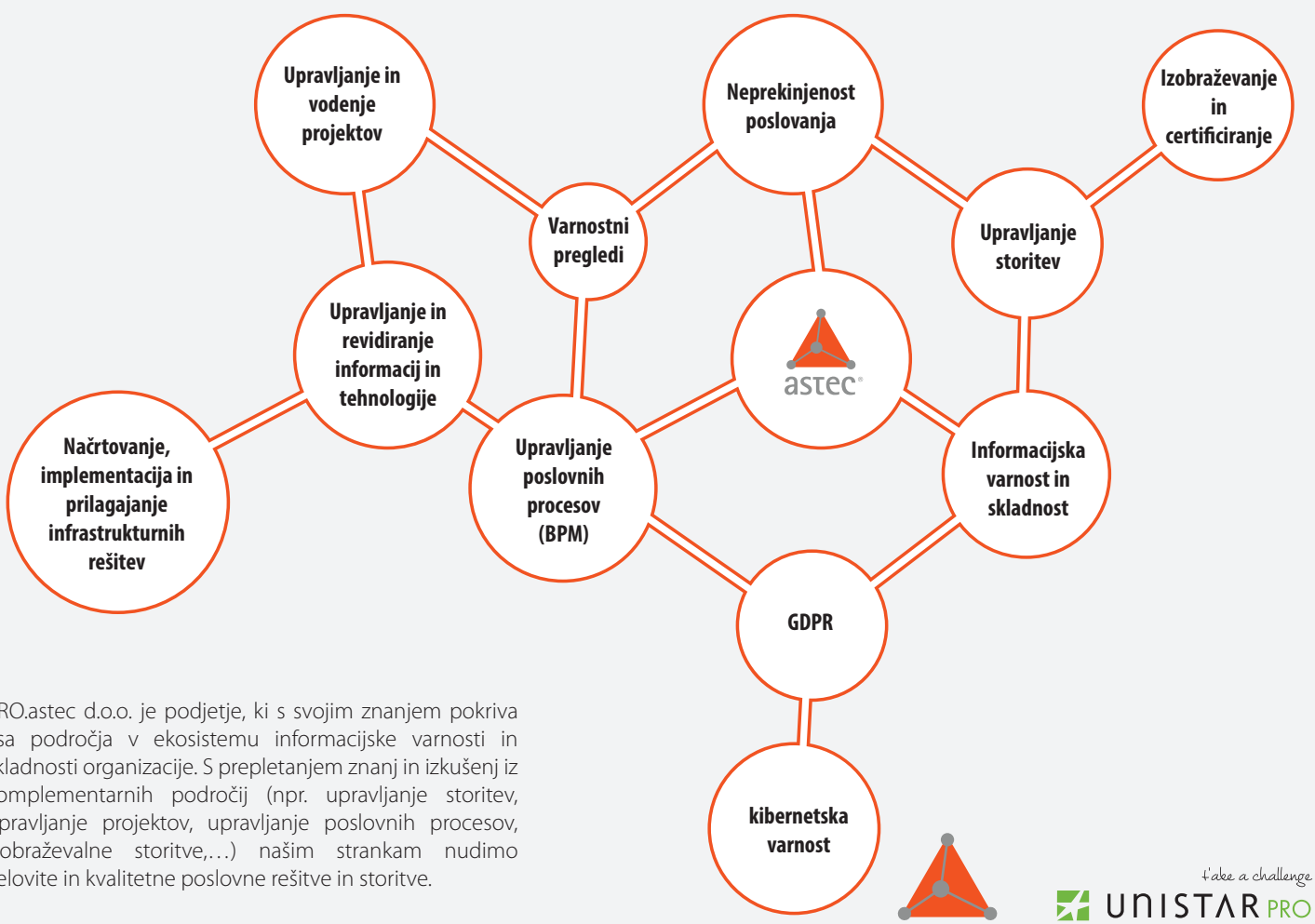
info@hsi.si
+386 7 600 19 60

HSI

CAPTIS®

License plate management solution

- Sledljivost
- ROI v kratkem času
- Stalna razpoložljivost
- Brez neavtoriziranih vstopov
- Velika prepustnost na vhodu
- Več varnosti za vaše podjetje
- Samodejno odpiranje zapornice
- Enostavno upravljanje parkirnih mest
- Olajšanje in razbremenitev zaposlenih



PRO.astec d.o.o. je podjetje, ki s svojim znanjem pokriva vsa področja v ekosistemu informacijske varnosti in skladnosti organizacije. S prepletanjem znanj in izkušenj iz komplementarnih področij (npr. upravljanje storitev, upravljanje projektov, upravljanje poslovnih procesov, izobraževalne storitve,…) našim strankam nudimo celovite in kvalitetne poslovne rešitve in storitve.

astec®

take a challenge
UNISTAR PRO
Challenge, Passion, Trust.

PRO.astec d.o.o., Dunajska cesta 158, 1000 Ljubljana | +386 1 320 71 33, info@astec.si, www.astec.si

Avtorja: mag. Miran Vršec in Žiga Podgoršek /
Institut za korporativne varnostne študije*





INFORMACIJSKA IZPOSTAVLJENOST, OGROŽENOST IN TVEGANJA NA JAVNIH BREZŽIČNIH OMREŽJIH V HOTELIH

Dejstvo je, da imamo vsi radi brezplačen brezžični internet. Pa vendar, kolikokrat se vprašamo o varnosti uporabe brezžičnih dostopnih točk? Dandanes je to v hotelih zelo pomemben dejavnik za skoraj vsakega gosta. Obstajajo celo spletna mesta namenjena iskanju hotelov s hitrim brezžičnim internetom in izsledki testiranja hitrosti v dotičnih hotelih, ki je pomemben dejavnik pri izbiri hotela med poslovnimi gosti. Vendar obstaja težava; brezžična omrežja so sama po sebi nevarna.

Wi-Fi omrežje v hotelih je pogosto zasnovan za enostaven in uporabnikom prijazen dostop. Naprave se lahko povezujejo v nevarna omrežja brez šifriranja brezžične komunikacije. Uporaba tovrstnih omrežij lahko uporabnika, ki je povezan na to omrežje, izpostavi prevaram, krajam, virusom ter napadom z zlonamerno programsko opremo. Ena od nedavnih študij je pokazala, da 78 odstotkov ljudi po vsem svetu aktivno išče javna Wi-Fi omrežja, od teh ima kar 72% uporabnikov popolno zaupanje v te vire, ne glede na dejansko varnost. Raziskava laboratorija Kaspersky je pokazala, da je ljudi precej lažje »oropati« njihovih podatkov, kot pa njihovega denarja. Med potovanjem so bili trije od desetih predstavnikov višjega menedžmenta žrtve kibernetskega kriminala.

Danes je uporaba javnega Wi-Fi omrežja sestavni del našega vsakdana. Brez tega praktično ne znamo več funkcionirati. Naj z nespametno uporabo ne postane to tudi naša nočna mora. Zato, preden se povežete v javno Wi-Fi omrežje, poskrbite, da bo varnost na prvem mestu, šele nato prijaznost in enostavnost uporabe.

Zakaj je pomembna varnost pri uporabi javnih Wi-Fi omrežij

Naj navedemo le nekaj pomembnih podatkov povezanih s kibernetskim kriminalom:

- Eden od odmevnejših kibernetskih napadov na hotelsko verigo je bil odkrit leta 2018, ko je svetovno znana hotelska veriga Marriot International odkrila napadalce, ki so v njihov sistem vdrli že leta 2014. Hekerji so ukradli številke kreditnih kartic in več kot 100 milijonov strank. Preostalih 400 milijonov je izgubilo samo del zasebnih podatkov (imena in številke potnih listov).
- Na vsakih 39 sekund se zgodi hekerski napad.
- Kibernetski kriminal je boj profiten, kot posli s prekupčevanjem droge.
- Ruski hekerji so najhitrejši – v vaš sistem v povprečju lahko vstopijo v 18 minutah.
- Dnevno se ustvari 300.000 novih zlonamernih programov.

*avtorja sta člana Slovenskega združenja korporativne varnosti



- Večfaktorska overitev in šifriranje sta največji hekerski oviri.
- Povprečni stroški kršitev podatkov bodo leta 2020 približno 150 milijonov USD.

Kje je težava?

Težava je v sami naravi Wi-Fi omrežja, kjer promet z vseh omrežnih naprav glasno oddaja zračne valove, kar naredi vsako javno Wi-Fi omrežje nevarno. S poceni Wi-Fi adapterjem in povsem brezplačno programsko opremo lahko vsak prisluškuje in prestreza vse komunikacije, ki so sprovedene med omrežnimi uporabniki brezžičnega omrežja in zunanjim svetom.

V hotelih se predvsem pogreša implementacijo segmentacije omrežja poslovnega razreda. Prav tako velika večina hotelov ne omejuje spletnih mest, ki si jih gost lahko ogleda preko njihovega omrežja, kar pušča široko odprto okno možnosti za zunanji dostop.

Če hotelska brezžična dostopna točka ne uporablja WPA zaščitnega protokola (ang. Wi-Fi Protected Access), lahko vsaka naprava, ki je povezana v to omrežje, preko njega pošilja vse podatke v jasnem nešifriranem besedilu in tako oddaljenemu napadalcu omogoča prepoznavo in črpanje informacij.

Zakaj Wi-Fi omrežja v hotelih veljajo za posebno tvegana?

Prefinjeni varnosti sistemi, ki običajno obstajajo v poslovnih omrežjih znotraj organizacij, niso prisotni na tovrstnih omrežjih. To pripelje do preprostejše izvedbe napadov kot sta MitM (ang. Man-in-the-Middle) ter MitB (ang. Man in the Browser) zaradi nizkega varnostnega standarda.

Prav tako višji kot je razred gostov v hotelu, večje so možnosti, ki jih imajo hekerji. Mamljive tarče so poslovni gostje.

Kdo prestreza hotelska brezžična omrežja?

Hoteli so mamljivi predvsem zaradi tega, kdo biva v njih. Hotelska omrežja predstavljajo zelo donosne cilje za kibernetske kriminalce. Kriminalci najprej sabotirajo hotelsko brezžično omrežje in nato čakajo na žrtve, da se povežejo v omrežje. Žrtve so nato pogosto zavedene v prenos in namestitev zlonamerne programske opreme na njihovo napravo, kar napadalcem odpre zadnja vrata in jim omogoči nadaljnje aktivnosti.

Hekerji se pogosto poslužijo tudi tako imenovanega napada zlobnega dvojčka (ang. Evil Twin) pri katerem vzpostavijo

novo ponarejeno omrežje, s katerim zrcalijo pravo omrežje. Uporabniki se nevede povežejo na ponarejeno omrežje in nato jim heker lahko ukrade uporabniška imena in gesla računov, preusmeri žrtve na spletna mesta s škodljivo zlonamerno programsko opremo in prestreže datoteke.

Kaj bi nas moralo najbolj skrbeti?

Najbolj bi nas moralo skrbeti za našo digitalno identiteto. Napadalcev ne zanimajo samo podatki, ki jih hranimo na naših napravah ali jih pošiljamo po omrežju, temveč jih zanima predvsem kraja spletnega identifikatorja žrtve ter dostop do vseh virov, s katerimi se lahko poveže. Tako lahko hitro postanejo ciljne tarče napadalcev npr.: strežniki v podjetju, službena elektronska pošta in drugi oddaljeni viri.

V kolikor uporabljamo spletna mesta z SSL zaščito (https) to ne pomeni, da smo popolnoma zaščiteni. Morda dobimo lažni občutek popolne varnosti vendar lahko napadalec preusmeri vaš promet preko njegove naprave v drugi hotelski sobi in zlahka premaga SSL zaščito.

Kako se ubraniti pred grožnjami na javnih Wi-Fi omrežjih?

Vedno več je sofisticiranih groženj, a vendar je rešitev lahko dokaj preprosta.

Z uporabo virtualnega zasebnega omrežja (ang. VPN) poskrbite, da bo celoten promet šifriran vse od vaše naprave do končnega VPN strežnika. Podjetja bi za te namene morala imeti VPN strežnike, kamor bi se v teh situacijah zaposleni lahko povezali in zaščitili. Na drugi strani pa si VPN strežnik lahko postavimo tudi sami ali ga najamemo drugje. V tem primeru je potrebno paziti na kar nekaj dejavnikov, da se po nepotrebnem ne izpostavimo drugim souporabnikom javnega VPN ponudnika, kjer med drugim tudi napadalci lahko čakajo na vašo povezavo. VPN šifrira podatke v omrežnem prometu ter s tem oteži vohunjenje.

Prav tako se svetuje, da na potovanjih izklopimo vso skupno rabo datotek, preverimo ali so požarni zidovi posodobljeni in pravilno nastavljeni, uporabimo različna gesla, vedno se poslužimo HTTPS, kadar je to le mogoče in izklapljamo Wi-Fi omrežje, ko ga ne uporabljamo.

Ali obstajajo tudi druge alternative hotelskemu brezžičnemu omrežju?

Velikokrat imamo na voljo tudi javni in mestni brezžični internet, ki je prav tako zelo tvegan. Velikokrat so ta omrežja odprta in brez mehanizma varnega šifriranja. S tem lahko ogrozimo korporativne podatke.

Veliko bolj varen način bi bila uporaba mobilnega omrežja 3G/4G. Na številnih lokacijah sta hitrost prenosa od strežnika in proti strežniku (ang. download and upload) enako dobra, če ne celo boljša kot na Wi-Fi povezavi. Mobilni podatki so praviloma bolj varni kot Wi-Fi omrežja zaradi šifriranja, ki ga mobilni operaterji samodejno uporabijo za tovrstne povezave.

Nekaj nasvetov za varno uporabo Wi-Fi omrežja

Da bo uporaba javnih mobilnih omrežij in dostopnost do naših baz podatkov čim bolj varna tudi v času, ko naše mobilne naprave uporabljamo izven varnih informacijskih omrežij, vam v nadaljevanju podajava nekaj uporabnih nasvetov za zagotavljanje višjega nivoja varnosti, in sicer:

- Na napravah vedno poskrbite, da imate nameščeno ustrezno zaščito.
- Poskrbite, da imate vedno nameščene najnovejše varnostne posodobitve in popravke. Pri tem je smiselno preverjati izvor posodobitve in s tem preprečiti zlonamerni programski opremi prikrito izdajanje kot posodobitev.
- Uporabljajte virtualna privatna omrežja VPN. Vsi operacijski sistemi ponujajo vrsto VPN rešitev.
- Poslužujte se uporabe močnih gesel. Gesla velikokrat prinašajo preglavice, vendar so še vedno glavni način prijave v storitve ali naprave. Predvsem ne uporabljajte istega gesla za vse prijave.
- Poskusite se navaditi brisanja poznanih Wi-Fi točk, predvsem, če so te bile javne. S tem preprečite, da se vaša naprava samodejno poveže na zlobnega dvojčka vaši napravi poznanega brezžičnega omrežja, katerega so napadalci uspeli prepoznati.
- Povezujte se samo na preverjena brezžična omrežja.
- Povezujte se samo na varna spletna mesta. Poskušajte se upreti skušnjavi preverjanja socialnih omrežij ali upravljanja spletnega bančništva, ko ste povezani na javna omrežja. V kolikor ne gre drugače, se poslužujte uporabe storitve HTTPS Everywhere.
- Namestite protivirusne programske rešitve.
- Izklapljajte vse možnosti skupne rabe, ki so lahko vrata za vdor v računalnik.
- Spremljajte aplikacije, ki jih uporabljate, ker so lahko izkoriščene kot vrata v vašo napravo.
- Nikoli ne odklepajte telefona z raznimi ti. Jailbreak kodami ali root-i. S tem onemogočimo vgrajeno varnost naprave.
- Izklapljajte Bluetooth, ko ga ne uporabljate. S tem preprečite napadalcu izvedbo BlueBorne napada, ki za uspešnost ne potrebuje uporabniške interakcije ali imeti napravo v vidnem stanju. Ne potrebuje niti predhodnega povezovanja z vašo napravo, temveč zgolj aktiven bluetooth. Zastrašujoče je tudi to, da je izvedljiv na vseh programskih verzijah.
- Šifrirajte občutljive podatke. Vsi podatki, ki so poslani preko VPN omrežja, bodo šifrirani. V kolikor nimamo te možnosti, je smiselno, da podatke šifriramo ločeno na napravi in jih nato že šifrirane in zavarovane pošljemo po nevarnem omrežju.

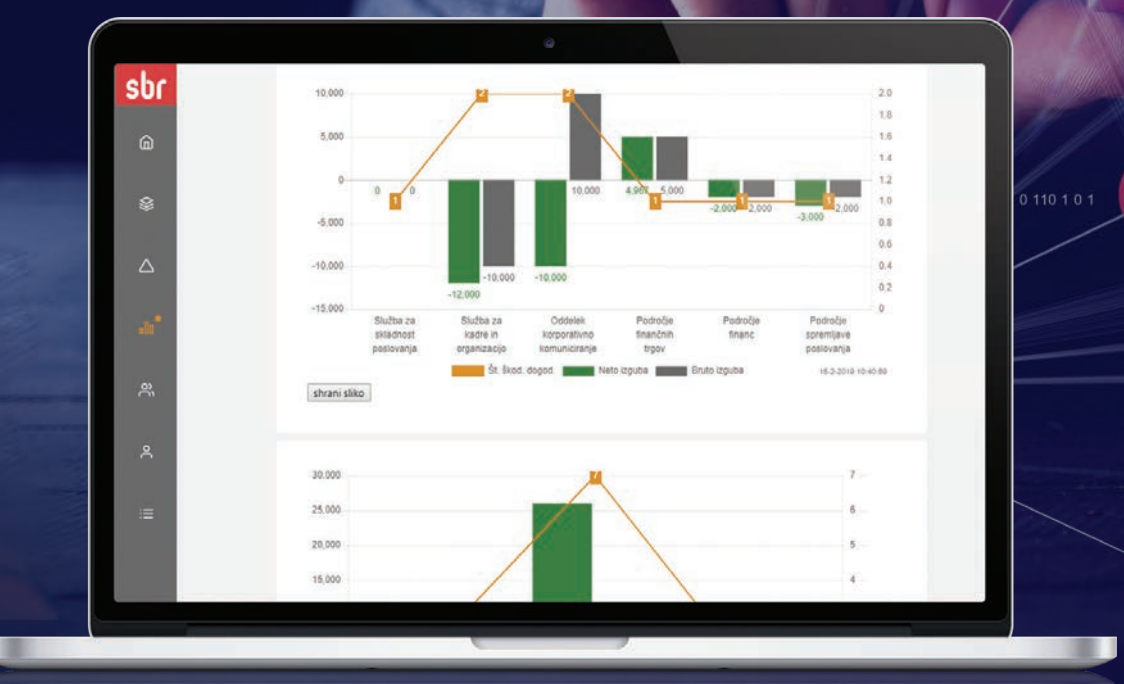
Danes je uporaba javnega Wi-Fi omrežja sestavni del našega vsakdana. Brez tega praktično ne znamo več funkcionirati. Naj z nespametno uporabo ne postane to tudi naša nočna mora. Zato, preden se povežete v javno Wi-Fi omrežje, poskrbite, da bo varnost na prvem mestu, šele nato prijaznost in enostavnost uporabe. ■

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: Igor Zgonc / ustanovitelj in direktor podjetja Silver Bullet Risk



KLJUČNI IZZIVI PRI UPRAVLJANJU TVEGANJ NA PODROČJU KRITIČNE INFRASTRUKTURE V LUČI ZAKONODAJE

V dobi digitalizacije in hitrih sprememb nam več kazalnikov doma in po svetu pritrjuje, da se bo stopnja nestanovitnosti v poslovnem svetu v letih in desetletjih, ki prihajajo, še povečala. Naj vas spomnim na nedavno motnjo pri oskrbi z zdravili v Ljubljani, ki je v le nekaj dneh povzročila milijonsko finančno škodo, skrhala je zaupanje kupcev in povzročila »neizmerljiv« padec ugleda same družbe v javnosti. Pomislite tudi, koliko poslovnih izgub se je na globalnem trgu zgodilo zaradi nedavnih posledic Korona virusa! Morda veste, da je kibernetski napad v Ukrajini leta 2015 povzročil izpad električnega omrežja pri skoraj 230.000 odjemalcih?



Večanje negotovosti pomeni tudi naraščanje groženj, kar predvsem od vodij, uprav in odločevalcev zahteva, da se tveganjem posvetijo celovito in na strateški ravni ter s tem v delovne procese sistematično uvedejo znanja in orodja, ki zaposlenim pomagajo obvladovati stroške ter sprejemati korake in ukrepe, ki lahko tvegane situacije vsaj ublažijo, če ne v celoti preprečijo. To je še posebej pomembno pri kritični infrastrukturi, ki lahko nemudoma destabilizira državno varnost in gospodarstvo. A vrnimo se na začetek.

S pojmom kritična infrastruktura opišemo tiste zmogljivosti, ki so ključnega pomena za našo državo, saj bi »prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice za nacionalno varnost, gospodarstvo in druge ključne družbene funkcije, s tem pa tudi na zdravje, varnost, zaščito in blaginjo ljudi«. Iz tega razloga je v interesu vsake države, širše pa tudi celotne Evropske unije, da se na področju upravljanja in zaščite kritične infrastrukture vzpostavijo enotni standardi in da vsaka država članica nacionalno kritično infrastrukturo ustrezno zaščiti.



Skupen evropski okvir, ki smo se mu v Sloveniji približali z nacionalnim programom za zaščito kritične infrastrukture, na podlagi Zakona o kritični infrastrukturi (ZKI, UR. I. RS, št. 75/17), pomeni poenotenje in večjo preglednost tega področja, saj prinaša standardizacijo postopkov in metodologij in nam s tem nudi oporo in usmeritev pri zagotavljanju ustreznih sistemskih rešitev.

Upravljalcem kritične infrastrukture pa hkrati prinaša nove odgovornosti in izzive, med katerimi je tudi sposobnost upravljanja z varnostnimi tveganji. To z drugimi besedami pomeni, da morajo zagotoviti strateško-operativno delovanje posamezne kritične infrastrukture pred, med in po kriznem dogodku, za kar morajo pri samem organiziranju, vodenju in nadzorovanju delovanja zmogljivosti poznati tudi obvladovanje različnih možnih in dejanskih nevarnosti, ogrožanja in varnostnega tveganja kot tudi izvajanja ukrepov in aktivnosti ob neposrednem nastanku izrednega varnostnega dogodka. V praksi to pomeni sledeče:

- Izdelati morajo **dokumente načrtovanja zaščite kritične infrastrukture**. To so ocena tveganja in ukrepi za zaščito kritične infrastrukture, za katere morajo pridobiti soglasje nosilca sektorja kritične infrastrukture.
- Izvajati morajo **ukrepe za zaščito kritične infrastrukture**, ki so stalni in dodatni. Stalni ukrepi se izvajajo v vseh razmerah. Dodatni pa ob povečani ogroženosti, izrednem dogodku, krizi, ali če stalni ukrepi ne zadoščajo.
- Tretja pomembna odgovornost upravljavcev pa **obveščanje in poročanje**. Obveščanje je namenjeno predvsem seznanitvi nosilca sektorja s prekinitvijo delovanja kritične infrastrukture in izvedenimi ukrepi za zaščito. Poročanje pa je letno poročilo, ki ga upravljavci posredujejo nosilcu sektorja do konca februarja za preteklo leto.

A vendar zakonske zahteve niso novost in formalno jim je moč zadostiti relativno hitro; praksa pa nas kljub temu opozarja, da področju upravljanja tveganj pogosto ne posvečamo dovolj pozornosti. Razlogov za to je veliko: najbolj univerzalen med njimi je, da je v naši človeški naravi, da na tveganja gledamo kot na nekaj, kar se v prvi vrsti dogaja drugim; zagotovo pa velja tudi, da na tem področju (še) nimamo razvite poslovne kulture niti dovolj strokovnega znanja. V večini organizacij pa to preprosto pomeni, da se s tveganji ukvarjajo posamezniki, ki so pri tem omejeni zgolj na področje varnosti oz. nadzorovanja in administrativnega upravljanja tveganj, kar pa še zdaleč ni dovolj.

Ko govorimo o upravljanju tveganj, večinoma govorimo o predvidevanjih, kaj je možno in na kaj morate biti kot organizacija pripravljeni, da s preventivnimi dejanji lahko preprečite ali vsaj blažite vrsto neželenih dogodkov, ki lahko vplivajo na poslovne izide, uspeh in kredibilnost organizacije. Celovito upravljanje tveganj pa je možno zgolj, ko področje upravljanja tveganj strateško umestite v samo jedro delovanja organizacije, kjer v procesu vzpostavite metodologijo neprekinjenega poslovanja, definirate strateško zunanje in notranje okolje posamezne kritične infrastrukture, analizirate tveganja in učinke ter na podlagi tega naredite načrt neprekinjenega poslovanja.

Ovira, ki jo bo pri tem morala prečkati večina, pa je sprememba v tradicionalni miselnosti upravljalcev tveganj in poslovnih funkcij, tako da bodo začeli tveganje dojemati kot strateško priložnost za dosego poslovnih ciljev na učinkovitejši način. Pri tem upravljanje s tveganji ne bo več zgolj poročanje informacij, temveč bo osredotočeno na posamezen problem in na razumevanje, kje in zakaj nastane ter kateri so potrebni izzivi za premagovanje podobnih problemov.



Naj opomnim tudi, da se ne glede na trud, ki ga kot organizacija že danes morda vlagate v preventivo, nekaterim incidentom ni moč izogniti. Ko se tveganje tudi realizira, govorimo o škodnem dogodku, ki večinoma prinaša finančno izgubo, v najhujših primerih pa lahko pomeni tudi izgubo človeških življenj.

Je škodne dogodke moč preprečiti? Nekatere zagotovo da; vsekakor pa se lahko ob dolgoročnem spremljanju dogajanja in posledic ter analizi ukrepov iz njih veliko naučimo. Pri tem so največji problemi, ki smo ga pri upravljanju tveganj identificirali tako v poslovnih okoljih v tujini kot doma, da vodstvo, uprava ter nadzorni svet, lastniki, notranji in zunanji revizorji nimajo celovitega pregleda nad ključnimi tveganji v organizaciji in morebitnimi posledicami odločitev.

To lahko pomeni veliko stvari: morda poročila o tveganjih niso podprta s finančnimi vplivi na samo organizacijo; v organizacijah nimajo ustrezne informacijske in metodološke podpore pri svojem delu, temveč večinoma uporabljajo preglednice, kot edino orodje za obravnavo tveganj. S tem je samo delo zamudno, nepregledno, obenem pa ni mogoče zagotavljati revizijskih sledi in preverjati zgodovine, priprava celovitih poročil na podlagi enovite metodologije pa je praktično nemogoča.

Pri upravljanju tveganj na »pravi« način, ki je celovit in strateški, zato velja pravilo, da se načrtovanje začne od zgoraj navzdol, izvajanje načrtovanih ukrepov pa od spodaj navzgor. Z drugimi besedami, resnično zmanjšanje tveganj dosežemo, ko postane del varnostne kulture vseh zaposlenih, ki jo upoštevamo vedno in povsod. Dobra novica je ta, da si v dobi digitalizacije pri tem lahko danes pomagamo s številnimi orodji, kot je Silver Bullet Risk, ki vam s celovitim vpogledom v tveganja in škodne dogodke ter avtomatizacijo postopkov pomaga, da upravljanje tveganj integrirate v samo jedro poslovanja in poslovnega odločanja. Na ta način se lahko organizacije premaknete od preventivnega ravnanja in razpravo glede apetita tveganj integrirate v fazo odločevanja, kar vam bo omogočilo, da tveganja in njihov vpliv zavestno upoštevate. ■


A1
Spreminjamo pravila poslovne varnosti!
Z A1 naprednimi varnostnimi rešitvami za vse vrste podjetij.
Vade Secure
Inteligentna zaščita elektronske pošte
F-Secure
Celovita zaščita pred virusi, vdori in nezaželeno pošto
Stormshield
Požarni zid naslednje generacije
iStor
Varnostno kopiranje podatkov v realnem času
Vectra
Zaznavanje kibernetskih napadov s pomočjo umetne inteligence
Wallix
Platforma za upravljanje privilegiranih dostopov
A1.si
Več o storitvah in vse Posebne pogoje uporabe storitev ter cene najdete na A1.si, 040 40 40 40 in na A1 prodajnih mestih. A1 Slovenija, d. d., Šmartinska 134b, 1000 Ljubljana.
A1 Slovenija, d.d., Šmartinska cesta 134b, 1000 Ljubljana
GREY

Avtor: Gorazd Božič / vodja SI-CERT*



PRIJAVITE INCIDENT. SE SPLAČA.

Kibernetska varnost je marsikje že več let pomembna tema na delovnih mizah vlad različnih držav. V zadnjih letih se je prerinila tja tudi pri nas, saj smo morali udejaniti evropsko direktivo NIS. Zakon o informacijski varnosti sedaj določa med drugim tudi to, da so zavezanci po zakonu obvezani poročati o večjih incidentih pristojni CSIRT[1] skupini.

Prostovoljna in obvezna priglasitev incidenta

Zakon o informacijski varnosti določa v 13. in 14. členu obvezo priglasitve incidenta na SI-CERT za vse zavezance, ki so bili določeni po sklepu Vlade RS kot izvajalci bistvenih storitev ali ponudniki digitalnih storitev. Vsi ostali poslovni subjekti, javne ustanove in fizične osebe lahko podajo prostovoljno prijavo incidenta na SI-CERT. Namen prijave je strokovna pomoč pri identifikaciji težave, pomoč pri njeni odpravi, zamejitvi in odpravi posledic. SI-CERT ni organ pregona, zato je pri sumu kaznivega dejanja potrebna prijava hkrati tudi policiji. Če gre za sum zlorabe osebnih podatkov, je potrebno podati prijavo tudi Informacijskemu pooblaščencu. SI-CERT ima z obema organoma vzpostavljeno operativno sodelovanje za skupno preiskovanje, kar nam omogoča, da problem »napademo« iz treh različnih vidikov.

Neredko pa na SI-CERT zaznamo zadržke pri priglasitvi incidenta, dostikrat s strani podjetij, manj pa v javnih ustanovah in državnih organih. Razlogi za to so lahko seveda različni, od strahu pred razkritjem v javnosti, nepoznavanjem delovanja SI-CERT, pa tja do refleksa »to lahko storimo sami«. Ob tem se pogosto zanemari dejstvo, da kvalitetno preiskovanje incidenta nujno zahteva ustrezno usposobljene strokovnjake, ki imajo na voljo primerna orodja. Najraje na predavanjih to ponazorim s pogovorom, ki sem ga imel v eni od slovenskih elektrarn. Vprašan sem bil, koliko sploh na SI-CERT vemo o njihovih SCADA sistemih (priznam, nič kaj dosti) in ali bomo sploh znali kaj prida pomagati ob varnostnem incidentu. Odgovoril sem nazaj z vprašanjem. Iz izkušenj vemo, da je običajni vstopni vektor okužba nadzornega Windows računalnika (in ne kakšnih PLC naprav). Koliko zaposlenih imajo v elektrarni usposobljenih za takojšnjo analizo škodljive kode in odvrženih artefaktov na računalnikih? Verjetno nikogar, saj se to stroškovno ne izplača. Zato države financirajo CSIRT skupine, kot je recimo SI-CERT, ki ta znanja imamo in lahko pomagamo žrtvam napada z analizo in poročilom o posledicah in bodoči zaščiti. Naša naloga je primarno pomoč prizadetim v incidentu.

Ob tem se pogosto zanemari dejstvo, da kvalitetno preiskovanje incidenta nujno zahteva ustrezno usposobljene strokovnjake, ki imajo na voljo primerna orodja.

V našem laboratoriju za analizo škodljive kode imamo recimo ustrezne *peskovnike*, kjer opazujemo delovanje virusov in trojancev, ustrezna orodja za dinamično in statično analizo, kjer gledamo v drobovje kode (ki jo avtor ponavadi nalašč izmaliči, da bi nam otežil delo), kazalce zlorabe (IoC, Indicators of Compromise) pa lahko takoj primerjamo z ostalimi odzivnimi centri preko mreže MISP (Malware Information Sharing Platform). S kolegi iz tujine si izmenjujemo tudi opažene TTP storilcev (TTP so taktike, tehnike in postopki). Zato prijava na pristojni CSIRT vsekakor pohitri in izboljša rezultate preiskave. Poudariti pa moram še enkrat, da so škarje in platno v rokah tistega, ki je vdor ali zlorabo utrpel.

Kaj sledi prijavi?

Po poslani prijavi iz SI-CERT odgovorimo v najkrajšem možnem času z obrazložitvijo incidenta in napotki, kako ukrepati naprej. Kot kaže naša statistika, lahko v večini primerov pričakujete odgovor v nekaj urah, v skoraj vseh primerih pa v manj kot 48 urah, pri čemer ravnamo glede na vrsto in nujnost incidenta, kot ju določimo po interni triaži in glede na zakonske obveznosti. Glede na vrsto incidenta po potrebi stopimo v stik s tujimi odzivnimi centri, kadar pa je to potrebno, prijavitelja napotimo na pristojne organe, ali pa jih sami kontaktiramo, če je to bolj smiselno.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

[1] CSIRT – Computer Security Incident Response Team

Kadar organizacija uporablja zunanjega izvajalca, ki nudi storitve varnostno-operativnega centra (SOC, Security Operations Centre), je nujno, da smo na SI-CERT takoj seznanjeni s tem, kdo to storitev nudi in pridobimo kontaktne podatke izvajalca. Učinkovita komunikacija je pomembna za hitro razreševanje inicidenta.

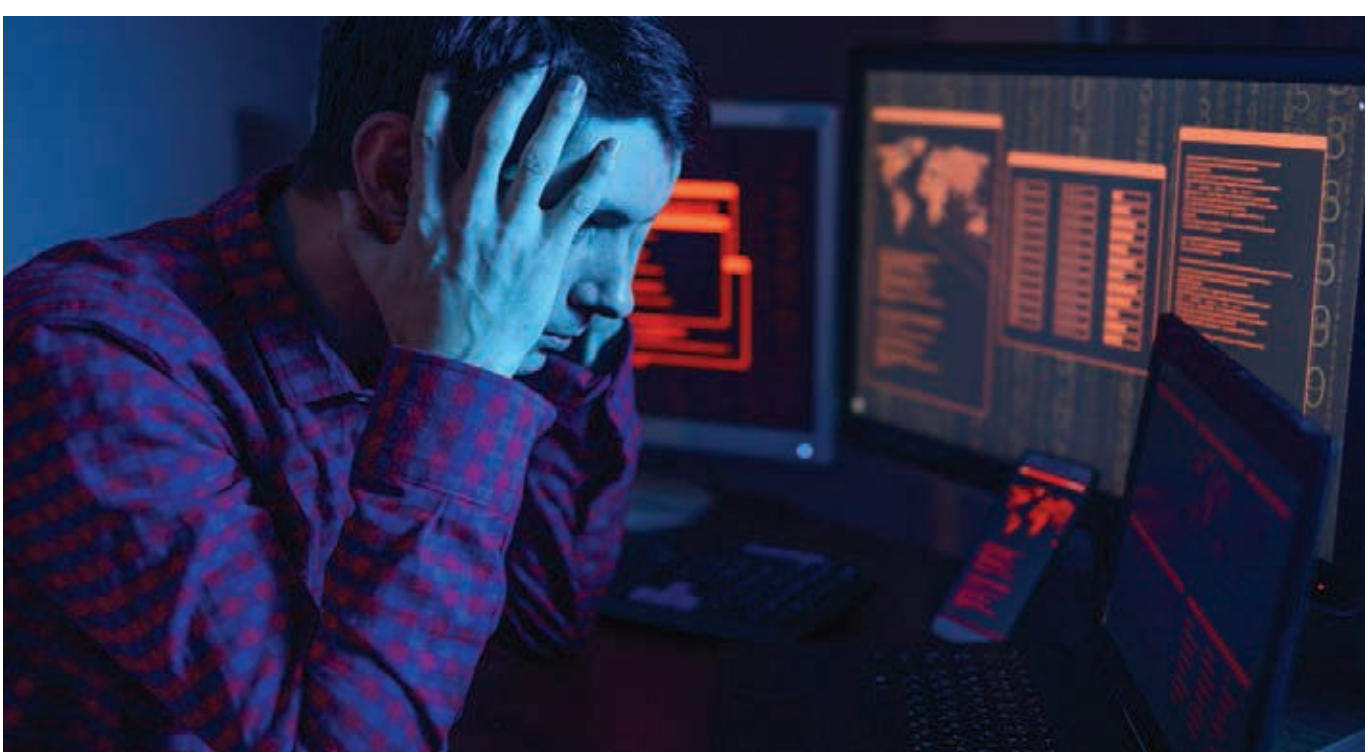
Letošnje leto smo začeli s priznanjem Ambasador zasebnosti, ki nam ga podeli Urad informacijske pooblaščenke.

Samopomoč

Splet predstavlja nove priložnosti tudi za spletne goljufe. Rast spletnih goljufij lahko opazujemo vseh zadnjih 10 let, zato smo podatke in nasvete za njihovo prepoznavo zbrali v programu ozaveščanja *Varni na internetu*, kjer lahko vsak uporabnik sam najde dovolj napotkov za ustrezno ukrepanje. Zaradi obilice pojavitev na priglasitve goljufij vsakemu prijavitelju posebej ne moremo več odgovoriti. Tveganja za tovrstne zlorabe lahko bistveno zmanjša vsak uporabnik sam, če ostane obveščen, recimo preko našega novičnika, v katerem obveščamo javnost o aktualnih opaženih goljufijah.

Kdaj prijaviti incident na SI-CERT?

Primer incidenta	**Pričakovane aktivnosti SI-CERT**
Okužba računalnika (izsiljevalski virusi, bančni trojanci, ciljani napadi, agenti za pošiljanje neželene elektronske pošte)	Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami. Svetovanje o ukrepih za sanacijo stanja.
Opažen vdor v strežnik (razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca)	Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.
Phishing elektronska sporočila (potvorjena elektronska sporočila, ki vas napeljujejo, da vpišete geslo na lažno spletno stran)	Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.
Napad onemogočanja (poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja)	Ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta in obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti.
Ranljive ali izpostavljene storitve (vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja)	Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.
Izguba gesel ali kraja omrežne identitete (zloraba preko phishing napada ali okužbe računalnika)	Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in možni identifikaciji storilca.





Funkcije SI-CERT

zavedanje o stanju	zdravje kibernetskega prostora	mednarodno sodelovanje	sodelovanje znotraj države	strokovna podpora	obveščanje javnosti
Na podlagi priglašenih incidentov, podatkovnih virov o okužbah in ranljivostih, izmenjave podatkov o aktualnih grožnjah z drugimi centri, se izdela slika stanja in ocene ogroženosti, ki je podlaga za odločitev o primernih ukrepih za zmanjševanje tveganj.	Podatki o ranljivih sistemih in videnih okužbah preko zaseženih botnet omrežij kažejo na zdravje omrežij in sistemov v Sloveniji in omogočajo distribucijo opozoril in navodil upraviteljem in končnim uporabnikom preko kontaktov pri operaterjih.	Redno operativno sodelovanje in izmenjava podatkov o opravljenih analizah in indikatorjih zlorab (IoC) krepi bazo znanja, potrebnega pri preiskovanju incidentov.	Preiskovanje incidenta lahko poteka iz različnih pogledov, zato je pomembno sodelovanje z organi pregona, inšpekcijskimi službami in sektorskimi regulatornimi organi.	Specializirana znanja preiskovanja vdorov, omrežne forenzike in analize zlonamerne kode omogočajo učinkovit in ustrezen odziv na zaznane varnostne incidente.	Obvestila za strokovno javnost, program ozaveščanja Varni na internetu, sodelovanje z mediji, koordinacija odgovornega razkrivanja ranljivosti zaokroža funkcije odzivnega centra.

25 letno delovanje SI-CERT

Jeseni bo minilo 25 let od pričetka delovanja SI-CERT in 10 let od snovanja programa ozaveščanja *Varni na internetu*. Letošnje leto smo začeli s priznanjem *Ambasador zasebnosti*, ki nam ga podeli Urad informacijske pooblaščenke. Letos pa sledi predsedovanje Svetu Evropske unije, ko vodenje prevzema trio Nemčija-Portugalska-Slovenija, kar bo za nas tudi na področju zagotavljanja kibernetske varnosti zelo velik strokovni zalogaj. ■


NAPREDNE REŠITVE IN STORITVE
ZA VARNO IN ZANESLJIVO
DIGITALNO PRIHODNOST
obvladovanje kibernetskih tveganj
za neprekinjeno delovanje
poslovno kritičnih okolij
avtonomna omrežja z uvedbo
konceptov umetne inteligence
avtomatizacija in orkestracija
varnostnih in omrežnih rešitev
SMART
COM
UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

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



UPORABA UMETNE INTELIGENCE ZA OBVLADOVANJE GROŽENJ V INDUSTRIJSKIH OKOLJIH

Kljub v preteklosti vztrajnemu trendu ločevanja procesnih oz. tehničnih sistemov (OT) od omrežij in sistemov namenjenih zagotavljanju poslovnih aplikacij (IT), prihaja do vse večjega prepletanja procesov in potreb po izmenjavi podatkov med različnimi aplikacijami na eni strani, na drugi pa se z digitalizacijo industrijskih okolij in pametnih omrežij v elektroenergetiki pojavlja čedalje več novih rešitev, ki zahtevajo povezljivost vedno večjega števila gradnikov v sistemu. Izkušnje kažejo na pojav stalno razvijajočih se naprednih in kompleksnih kibernetskih groženj, specializiranih za vdore v procesna omrežja.

Cilj vdorov v industrijska okolja in v kritično infrastrukturo, kot je elektroenergetski sistem, je prevzem kontrole nad napravami v tehničnih omrežjih in posledično ustavitve vitalnih procesov, kar vodi do poslovnega oškodovanja ali celo ogrožanja življenj. Za zagotavljanje kibernetske varnosti v teh sistemih je potrebno uvesti tehnološke rešitve, ki omogočijo razpoznavo skritih in kompleksnih groženj, usmerjenih v specifične sisteme, kot so npr. sistemi vodenja elektroenergetskih omrežij. Na podlagi ugotovljenih stanj, pa je potrebno zagotoviti povratno zanko in navzdolnjo integracijo z dosedaj uvedenimi mehanizmi kibernetske varnosti, kot so požarne pregrade, IPS sistemi ter navzgornjo integracijo s sistemi SIEM in nastajajočimi strukturami varnostno operativnih centrov (VOC). Algoritmi strojnega učenja so na tem področju že prevzeli pomembno vlogo, z njimi pa vzpostavljamo napredne rešitve za zaznavanje kibernetskih groženj v OT okoljih.

Podlago za obvladovanje velikih količin podatkov za obdelavo z vidika kibernetske varnosti je potrebno iskati v naprednih tehnoloških rešitvah, algoritmih umetne inteligence ter standardih za uporabo in strukturo kibernetske varnosti v OT sistemih.

Potek kibernetskega napada na kritično infrastrukturo

Prvi od resnejših napadov na industrijska okolja, posebej zasnovan za napad na elektroenergetske sisteme, ki se je zaradi svoje agresivnosti po uspešno izvedenem napadu razširil tudi izven segmenta elektroenergetskega proizvodnega objekta, je bil Stuxnet, ki se je v obliki, ki je povzročila uspešno izveden vdor in napad preko sistema za vodenje SCADA pojavil leta 2010. Tipičen potek in obnašanje novih vrst kibernetskih groženj, usmerjenih v OT okolja je bil demonstriran in preizkušen pri napadih na ukrajinski elektroenergetski sistem v letih 2015, 2016 in 2017. Prvi napad leta 2015, je pomenil tudi prvi znan kibernetski napad na obsežnejši elektroenergetski sistem, ki je povzročil izpad dobave električne energije za več kot 200.000 prebivalcev.

Napad na ukrajinski elektroenergetski sistem leta 2016 je povzročila zlonamerna programska koda z imenom Industroyer (poznana pa tudi pod imeni CrashOverride in Win32/Industroyer), katerega obnašanje je z vidika sodobnih kibernetskih groženj potrebno poznati, saj tako lahko načrtujemo ustrezne tehnološke rešitve za zaznavanje takšnih groženj in morebitnih kibernetskih napadov. Analiza poteka tega kibernetskega napada je pokazala, da takšni »uspešni« kibernetski napadi potekajo v treh fazah:

- okužba ciljnih sistemov z zlonamerno kodo,
- poizvedovanje in odkrivanje sistemov v OT okolju,
- napad.

Prva faza: Okužba sistemov z zlonamerno kodo

Glede na veljavno dobro prakso, da so OT sistemi ločeni od zunanjih IK omrežij ter IT sistemov pogostokrat velja prepričanje, da okužba preko zunanjih omrežij in oddaljenih dostopov do sistemov v OT okoljih ni možna ali pa je izredno težavna. Tega se zavedajo tudi kibernetski napadalci, ki si izberejo tarče v teh okoljih, zato način okužbe s ciljno zlonamerno kodo običajno izvedejo na drugačen, izredno prikrit način. S t. i. ‚spear phishing" napadi, ki so usmerjeni v določeno skupino uporabnikov računalniških sistemov, se pošlje običajna elektronska sporočila z legalnimi dokumenti v katerih je skrita zlonamerna programska koda, ki se ob odprtju dokumenta aktivira in prenese na osebni računalnik. Namesto okužbe preko napadov v elektronskih sporočilih, lahko pride na podoben način do okužbe tudi z uporabo USB ključkov ali do okužbe pri predhodnem dostopu do različnih virov v odprtem Internetnem omrežju. Ko se računalnik okužen z zlonamerno kodo znajde v zaprtem sistemu OT, le-ta poišče in se prenese na industrijske računalnike v sistemu, kot npr. na postajne računalnike in C&C (ang. Command and Control) strežnike. S tem je cilj prve faze dosežen, v drugi in tretji fazi se izvajajo nadaljnji koraki iz okuženih naprav.

Druga faza: Poizvedovanje in odkrivanje sistemov v OT okolju

Zlonamerna programska koda, s katero je okužen računalnik sproži poizvedovanje in odkrivanje naprav, njihovih povezav ter obnašanja le-teh. Zlonamerna koda se na ta način ‚nauči" značilnosti okolja in si sama gradi elemente za učinkovit napad. Že v tej fazi lahko zlonamerna koda prevzame kontrolo nad določenimi napravami v sistemu, vendar še vedno na posega v delovanje naprav, in je lahko prisotna v sistemu tudi mesece. Take kode ne moremo odkriti s klasičnimi mehanizmi kibernetske varnosti, saj le-ti nimajo vgrajenih mehanizmov za prepoznavanje vzorcev prometnih tokov v sistemu, ki se izvajajo med fazo poizvedovanja in jih primerjati z vzorci prometnih tokov in povezav, ki so prisotni v običajnem stanju in delovanju naprav in povezav med njimi. Cilj je identifikacija ciljnih tarč napada in priprava na kasnejšo izvedbo določenih ukazov nad spremenljivkami znotraj protokolov.





Tretja faza: Napad

Zlonamerna koda prevzame nadzor nad ciljnimi napravami in prične z izvajanjem ukazov, ki posledično vodijo do nekontroliranih stanj in posledično razpada sistema. Po izvršenem napadu in izvedenih manipulacijah na napravah se zlonamerna koda na okuženih sistemih samodejno izbriše in zakrije sledi za seboj. To izredno oteži kasnejšo forenziko in odkrivanje značilnosti napada, ki bi lahko koristile pri vgradnji zaščitnih mehanizmov za podobne napade v prihodnosti. Zato je raziskovanje in forenzika takih napadov dolgotrajen proces in zahteva visoko usposobljene strokovnjake s področja kibernetske varnosti, ki morajo hkrati poznati strukturo in delovanje procesnih protokolov značilnih za okolje.

Vloga umetne inteligence pri obvladovanju kibernetskih groženj

Podlago za obvladovanje velikih količin podatkov za obdelavo z vidika kibernetske varnosti je potrebno iskati v naprednih tehnoloških rešitvah, algoritmih umetne inteligence ter standardih za uporabo in strukturo kibernetske varnosti v OT sistemih. Z vzporednim razvojem algoritmov strojnega učenja in zajemom pretokov v OT omrežju ter njihovim globokim preverjanjem lahko zajemamo celoten nabor elementov v omrežju, njihovih značilnosti ter morebitnih varnostnih vrzeli, ključnega pomena pa je vzpostavitev slike prometnih pretokov in poznavanja le-teh do aplikacijske ravni OSI modela (L7), saj na ta način vzpostavimo možnost kontrole nad vrednostmi parametrov znotraj protokolov, ki se pretakajo v OT sistemu. Proti kibernetskim napadalcem, ki uporabljajo za napad tudi mehanizme umetne inteligence, se lahko učinkovito borimo le z uporabo varnostnih rešitev, ki za svoje delovanje uporabljajo enake metode.

Moderni sistemi, ki so namenjeni za preprečevanje naprednih kibernetskih napadov v OT okoljih, torej na podlagi algoritmov umetne inteligence in naprednih tehnik strojnega učenja določen čas le pasivno poslušajo in spremljajo promet v omrežju, v tem času za vsako zaznano napravo v svoji podatkovni bazi ustvarijo njen normaliziran prometni profil. Po fazi učenja se postavi naprave v fazo ščitenja oz. zaznave anomalij in varnostnih groženj. V primeru, da opazovani parametri niso več znotraj naučenih (ali ročno nastavljenih) meja, mora sistem javiti alarm, na katerega se ustrezno odzove operater v centru vodenja ali v varnostnem operativnem centru (VOC). Pomembno je, da se omenjeni procesi dogajajo v realnem času, saj je le tako možno dovolj zgodaj odkrivati dogajanje v OT okolju in zaznati morebitne kibernetske grožnje v sistemu.

Obvladovanje kibernetskih tveganj v prihodnosti

Zavedanje o nujnosti uvajanja naprednih sistemov kibernetske varnosti v OT okolja se je začelo bistveno spreminjati po uspešno izvedenih kibernetskih napadih, ki so povzročili znatne škode ali celo razpade sistemov, kot je npr. elektroenergetski.

Na podlagi forenzičnih raziskav teh napadov so bila pridobljena znanja o naravi in obnašanju kompleksnih in prikritih varnostnih groženj, ki so neposredno usmerjene na industrijska okolja in kritično infrastrukturo, predvsem na sisteme SCADA. Kompleksni kibernetski napadi na OT okolja potekajo v treh fazah, cilj prve faze je vnos in okužba računalniških sistemov z zlonamerno kodo, cilj druge faze je poizvedovanje in pridobitev podatkov o prometnih tokovih in napravah, ki so prisotne v sistemu in cilj tretje faze izvedba kibernetskega napada ter samouničenje zlonamerne kode, z namenom brisanja sledi.

Klasične metode kibernetske varnosti za primere takšnih varnostnih groženj in napadov ne zadoščajo več, zato je potrebno uvesti sisteme, ki izvajajo pasivni zajem in globoko preverjanje paketov komunikacijskih pretokov v sistemu, razpoznajo značilnosti protokolov v OT sistemu, z algoritmi umetne inteligence pa razpoznajo normalno delovanje v sistemu ter prisotnost zlonamerne kode v sistemu ter pošiljajo ustrezna sporočila ostalim aktivnim varnostnim sistemom, kot so požarne pregrade in sistemi v VOC.

Pogled na zagotavljanje celovite varnosti v OT okoljih je sicer širši, v prispevku je osvetljen predvsem vidik vzpostavitve identifikacije in upravljanja z viri ter zaznavanja anomalij na virih in prometnih tokovih v OT sistemu z uporabo umetne inteligence. Gre za ključen gradnik, ki ga je potrebno upoštevati pri načrtovanju arhitekture in ukrepov kibernetske varnosti v današnjih in prihodnjih okoljih OT. ■

SmartIS
PAMETNI INFORMACIJSKI SISTEMI

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

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



VAŠ SOPOTNIK NA POTI ZAGOTAVLJANJA KIBERNETSKE VARNOSTI

Avtor: Sašo Tomc / ekspert za kibernetsko varnost, SmartIS d.o.o.*



KIBERNETSKA VARNOST V KRITIČNI INFRASTRUKTURI

Kibernetski kriminal tesno sledi napredku novih tehnologij. Pri tem smo vsakodnevno pozorni na raznolikosti samih izvedb groženj in na anomalije, ki se nam pojavljajo. Hkrati pa moramo pozornost posvečati starejšim tehnologijam, ki so predvsem zelo ranljive. Med te vsekakor spadajo industrijsko-procesni deli omrežja ter OT naprave, ki veljajo za kritično infrastrukturo. Nikakor ne smemo dopustiti, da ICS/SCADA omrežja postanejo uspešna tarča kibernetskih napadalcev.

Nikakor ne bi smeli industrijskega okolja ali kritične infrastrukture prepustiti sami sebi in zaupati nešteto posameznim upravljalcem in proizvajalcem OT naprav, za katere vsak od njih odgovarja le za svoj košček celote v takšnem okolju.

Najpomembnejša funkcionalnost v kibernetskem svetu bi morala biti vidljivost. Namreč šele, ko si zagotovimo popolno vidljivost nad prometnimi tokovi, stanjem naprav, strežnikov, uporabniških računalnikov, senzorjev, strojev, terminalov, čitalcev, stikal, nad vzorci, ki jih te naprave vsakodnevno kreirajo s svojim obnašanjem in delovanjem, zatem lahko pričnemo razmišljati o zaščiti. Danes že obstajajo aktivne in pasivne zaščite ter rešitve na to temo in na nekatere od njih se lahko konkretno zanesemo. Navadno pri takšnih rešitvah njihovi proizvajalci za osnovo svojega razvoja uporabljajo umetno inteligenco.

Pa se najprej dotaknimo vprašanja, zakaj je vidljivost tako pomembna. Vsi dobro poznamo rek: "Kar ne veš, to ne bolí". V kibernetskem svetu bi ta rek lahko predrugačili v: "Kar ni vidljivo, to ni pomembno". Če pa se pogovarjamo o kibernetski varnosti in želimo dvigniti njen nivo, moramo začeti razmišljati o "Zero Trust" modelu. Gre za miselno ogrodje o tem, da se v nobenem trenutku nikakršni, bodisi notranji ali zunanji entiteti, uporabniku ali omrežni napravi ne sme zaupati. Tako pridemo do bistva, če nekaj v omrežju ni vidno ali poznano, to lahko že tretiramo, kot zelo kritično in nevarno. Naša prva stopnja pri zagotavljanju najvišjega nivoja kibernetske varnosti je torej povečevanje splošne vidljivosti vsega, kar zajema naše IT/OT okolje. Ko pričnemo izboljševati takšno vidljivost, navadno ugotovimo, da pred tem procesom nismo videli ničesar.

Drugi korak pri zagotavljanju najvišjega nivoja kibernetske varnosti je določanje stopnje tveganja in posledic, ki nas lahko doletijo ob morebitnem izpadu delovanja kritične infrastrukture.

Posamezni sektorji ter državne institucije, ki jih smatramo za kritično infrastrukturo in so na svetovnem nivoju že bili napadeni, so banke, jedrske in ostale elektrarne, državni zdravstveni sistem, petro-kemične tovarne, letališča in njihovi kontrolni stolpi, železniški promet, globalna transportno-logistična podjetja, vojska ter vlada. Večina informacij o uspešno izvedenih kibernetskih napadih na takšne institucije, zaradi državnega renoméja ter nivoja zagotavljanja varnosti prebivalcev ne pride v medije.

Poigrajmo se z domišljijo in si poizkusimo predstavljati, kako bi izgledal prometni kaos ob vsakodnevni jutranji prometni konici ob vstopu v veliko mesto, če bi bila vsa osvetlitvena in označevalna prometna infrastruktura onemogočena zaradi kibernetskega napada, ki mu ne bi zmogli slediti ali ga omejiti? Kaj bi se zgodilo, če bi bil državni zračni prostor več dni zaprt zaradi kibernetskega napada na kontrolo zračnega prometa in bi onemogočil komunikacijo vseh radarjev ter kontrolnih instrumentov? Kako bi zagotovili varnost in zdravje vseh državljanov, če bi bili napadeni telekomunikacijski sistemi, ki jih uporabljajo policija, vojska, gasilci, reševalci in ministrstvo, ki skrbi za obrambo države?

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Vsi skupaj si niti ne upamo predstavljati, da bi bila ogrožena varnost in stabilnost jedrske elektrarne, zato rajši zaupamo upravljalcem takšne zgradbe, da opravljajo svojo nalogo z najstrožjimi varnostnimi zahtevami, tudi kibernetskimi.

Število aktivnih IoT naprav po vsem svetu naj bi se po napovedih podjetja Gartner v letošnjem letu 2020 povzpelo na dobrih 20 milijard. Letni proračuni namenjeni zaščiti in varovanju naprav v kritičnih infrastrukturah se drastično zvišujejo. Danes je z najmanjšim možnim naporom in nizkim nivojem računalniškega znanja možno z mobilnim telefonom ter namensko aplikacijo manipulirati in upravljati klimatsko napravo v zdravstvenem domu, restavraciji ali baru. Če človeški možgani ne poznajo meja, si s to tezo niti ne moremo predstavljati, kaj vse se že dogaja na nivoju kibernetskega napadanja na tujo lastnino in na namenske naprave. Če razmišljamo eksponencialno ter realno za današnji čas rasti IoT sveta, smo vsako minuto in na vsakem koraku precej ogroženi.

Sedaj razumemo pomembnost vidljivosti, stopnje tveganja in možnih posledic kibernetskega napada. Naslednji korak pri zagotavljanju najvišjega nivoja kibernetske varnosti je analiza stanja lastnega IT/OT okolja s ključnimi elementi kritične infrastrukture, katere največkrat nadzirajo ICS/SCADA sistemi. V OT okolju obstaja teoretični vzorec nivojske porazdelitve elementov. Na spodnjem nivoju so končne naprave, senzorji, stroji, aktuatorji itd., na nivoju višje so programabilni logični kontrolerji, še višje so naprave z upravljalskimi vmesniki, nato SCADA sistemi, višje od tega nivoja pa že govorimo o IT okolju, kjer so soodvisne storitve za oba okolja, kot so recimo DNS, e-poštni strežniki, nadzorne postaje, namenski spletni strežniki in podobno.

Najpomembnejša funkcionalnost nadzora nad posameznimi OT nivoji je kontrola dostopanja, ki jo dosežemo z implementacijo požarne pregrade, ki prepoznava industrijske protokole. Vsak nivo in vsaka OT naprava bi morala imeti privzeti prehod na takšno požarno pregrado, ki zna prepoznati aplikacije, ki so značilne za industrijsko okolje in nikakor ne na splošno usmerjevalno napravo (OSI Layer 3), kot je bilo to nekoč običajno.

Segmentirati in s tem omejiti bi morali vsak posamezni sklop naprav in tako zagotoviti, da se jih nikakor se sme dosegati s protokoli ali aplikacijami, ki niso značilni za industrijsko OT okolje. Prav tako se s takšno segmentacijo naprav ali omrežja zagotovi vidljivost prometnih tokov glede na vrsto prometa in njihove časovne rezine ter alarmiranje v primeru anomalij, prometnih poplav in skeniranja omrežja od znotraj ali izven posameznega OT segmenta.

Še višja stopnja in naslednji korak pri zagotavljanju najvišjega nivoja kibernetske varnosti je poleg požarne pregrade naslednje generacije in njene podpore industrijskim protokolom, zelo priporočljivo še implementiranje namenske naprave, ki na podlagi spremljanja industrijskega prometa zagotavlja vidljivost in varovanje naprav. Spremljanje prometa se zagotovi s pošiljanjem podatkov preko zrcalnih vmesnikov na stikalih, kamor so priključene OT naprave (angl. SPAN ports). Takšna naprava nam služi za prepoznavanje neustreznih vzorcev in anomalij znotraj prenosa podatkov v paketih med napravami v OT okolju, opozarja nas na vse zaznane ranljivosti operacijskih sistemov OT naprav in nadzornih sistemov, predlaga nam izboljšave in implementacije popravkov za naprave, obvešča o zaznanih prenosih nekriptiranih gesel znotraj OT okolja, obvešča nas o poizkusih internetnega dostopanja OT naprav (uspešnih in neuspešnih), skeniranju omrežja in naprav, izriše časovne grafe o dogodkih, količini prometa, opozaja za vsako na novo zaznano napravo v OT okolju, nam z uporabo vektorskega

Na dolgi rok vedno prihranimo sredstva, če že v štartu zagotovimo najvišji možni nivo vidljivosti in zaščite našega IT/OT okolja. Morda se nam ravno sedaj pred očmi odvija trivialni ali sofisticirani kibernetski napad, pa tega ne moremo ali ga niti nočemo videti. Posledice so lahko katastrofalne.

prikaza omogoči teoretični vpogled na morebitni kibernetski napad v naše OT okolje, in podobne varnostne mehanizme. Hkrati je takšno napravo možno v korelaciji z napredno požarno pregrado naslednje generacije implementirati na način, da ta sistem v realnem času postane aktivna zaščita s takojšnjim odzivom glede na zaznane težave ter anomalije v OT okolju. Takšna naprava deluje na podlagi učenja z uporabo umetne inteligence in sicer s tem, da spremlja vzorce delovanja OT naprav in okolja ter nas v primeru odstopanja od standardiziranih ali povprečnih vrednosti na to redno opozarja in zaščiti.

Sklepna misel:

Nikakor ne bi smeli industrijskega okolja ali kritične infrastrukture prepustiti sami sebi in zaupati nešteto posameznim upravljalcem in proizvajalcem OT naprav, za katere vsak od njih odgovarja le za svoj košček celote v takšnem okolju. Pod nobenim pogojem ne smemo zaupati svoji lastni presoji, kaj je najbolje za varnost lastne ali državne imovine ter varnost vseh soljudi in državljanov. Vsi, ki imamo poslovno obveznost, da se ukvarjamo s kibernetsko varnostjo, smo družbeno odgovorni za posledice, ki lahko ob naši neprevidnosti ali ignoranci nastanejo v kritični infrastrukturi. Zato je potrebno upoštevati načelo, da se takšne zaščite in preverjanja OT okolja prepustijo najboljšim in certificiranim strokovnjakom, ki vsakodnevno vršijo nadzor, spremljajo novosti, incidente ter analize iz tega področja. Glede na rast svetovne populacije, glede na rast števila IoT naprav v svetu in glede na porast kibernetskega kriminala, nam vsekakor ne gre razmišljati o krčenju proračuna namenjenega za zaščito takšnega okolja. Na to tematiko se aktivno odzivajo tako posamezne države, kot celotna Evropska unija. Vsako leto bodo državni proračuni vsebovali višje zneske, ki so namenjeni kibernetski varnosti, saj nam realno gledano napadi na kritične infrastrukture ne uidejo. Na dolgi rok vedno prihranimo sredstva, če že v štartu zagotovimo najvišji možni nivo vidljivosti in zaščite našega IT/OT okolja. Morda se nam ravno sedaj pred očmi odvija trivialni ali sofisticirani kibernetski napad, pa tega ne moremo ali ga niti nočemo videti. Posledice so lahko katastrofalne.

Pojasnilo kratic:

IoT – Internet of Things (Internet stvari)

IT – Informational Tehnology (Informacijska tehnologija)

OT – Operational Technology (Operativna/Industrijska tehnologija)

ICS – Industrial Control Systems (Industrijski kontrolni sistemi)

SCADA – Supervisory Control and Data Acquisition (Centralni nadzorni sistem)





BeyondHumanVision

MOBOTIX

tend

/ IT rešitve / IT solutions /

ORG. TEND d.o.o.
Kraljevica Marka ulica 19
SI-2000 Maribor
E: mobotix@tend.si
W: www.tend.si

Kontrola pristopa z mobilnim telefonom

spica

Door Cloud je najnovejša generacija kontrole pristopa s katero lahko opustite kartice brez potrebe po posebnih čitalcih, pri tem pa še vedno lahko ohranite uporabo kartic in čitalcev v poljubni meri.

Poleg vsega tistega, kar nudijo tudi klasični sistemi kontrole pristopa, Door Cloud omogoča še:

- Pristopne točke brez čitalcev kartic
- Uporabo mobilnega telefona namesto kartic na vseh točkah pristopa
- Upravljanje z alarmi in incidenti z mobilno aplikacijo
- Upravljanje s sistemom kadarkoli od koderkoli
- Pošiljanje pristopnih pravic s preprostim linkom
- Uporaba pristopnih pravic brez mobilne aplikacije

Večja učinkovitost,
večja varnost,
več možnosti!

Door Cloud



Kontrola pristopa | Storitev v oblaku | HID čitalci in Špica krmilniki | Pristop brez čitalca | Brezžične ključavnice Aperio

www.DoorCloud.com

Špica international d.o.o., Pot k sejmišču 33, 1000 Ljubljana, www.spica.si, info@spica.si, 01 568 08 00

Avtor: Dušan Podbelšek / vodja projektive Zarje Elektronike, d.o.o.*



SISTEM JAVLJANJA POŽARA NA ZBIRALIŠČIH ZA ODPADKE

V Sloveniji vsako leto nastane nekaj milijonov ton odpadkov. Poraba na prebivalca se povečuje, zato se povečuje tudi količina odpadkov. Čeprav vedno več odpadkov predelamo, se količina zavrženih odpadkov ne zmanjšuje. V zadnjih letih je bilo v skladu z zakonodajo EU pri ravnanju z odpadki uvedenih kar nekaj sprememb. Na podlagi odgovornosti so bile vzpostavljene sheme za zbiranje in obdelavo posameznih odpadkov. Prepovedano je odlaganje neobdelanih odpadkov na komunalnih odlagališčih. Zato je v Sloveniji več odlagališč, ki so v fazi obratovanja ali zapiranja.

Z naraščanjem števila odlagališč in kopičenjem odpadkov se požarna obremenitev posameznih odlagališč povečuje, hkrati pa se slabša njihova požarna varnost.

Požari, do katerih v zadnjem obdobju v zbirnih centrih za odpadke vedno pogosteje prihaja, kažejo tudi na pomanjkljivo regulacijo požarne varnosti pri skladiščenju in predelavi odpadkov. Požarna varnost je v veliki meri prepuščena lastnikom, ki bi morali več vlagati v preventivo, v aktivno požarno zaščito, sisteme za samodejno odkrivanje in javljanje požara, alarmiranje, obveščanje in tudi v sisteme za samodejno gašenje požarov.

Bistvo sistema za samodejno odkrivanje in javljanje požara je, da požar zaznamo že v njegovi najzgodnejši fazi, v času pregrevanja, tlenja. Začetni požar lahko pogasimo s »kozarcem vode«, razviti požar pa se lahko razširi do ogromne razsežnosti in katastrofalno obremeni okolje. Odlagališča odpadkov glede požarne varnosti uvrščamo med izjemno zahtevne objekte. Posebnosti takih objektov predstavljajo deponije, ki so največkrat na odprtem in so pod vplivom mraza, vročine, pregrevanja, vlage, kemičnih reakcij, umazanije in prahu, neprestanega spreminjanja količine gorljivega materiala, prisotnosti delovnih in obdelovalnih strojev ter ljudi.

Odlagališča odpadkov glede požarne varnosti uvrščamo med izjemno zahtevne objekte. Posebnosti takih objektov predstavljajo deponije, ki so največkrat na odprtem in so pod vplivom mraza, vročine, pregrevanja, vlage, kemičnih reakcij, umazanije in prahu, neprestanega spreminjanja količine gorljivega materiala, prisotnosti delovnih in obdelovalnih strojev ter ljudi.

Če na odlagališču nastane požar, se lahko zelo hitro širi. Razvit požar lahko doseže zelo visoke temperature. Zaradi velike količine odpadkov so takšni požari lahko dolgotrajni, pri tem pa se sprošča veliko dima, poraba gasilnih sredstev je velika, pri tem pride tudi do velike onesnaženosti naravnega okolja (zrak, tla, voda).

Pri sprejemanju ukrepov požarne varnosti se nenehno srečujemo z različnimi dejavniki, ki se med delovanjem odlagališča odpadkov nenehno spreminjajo. Že zaradi neustreznega razvrščanja odpadkov pogosto ne vemo, kaj se skriva med odpadki. Nastajajo kemične reakcije (samovžigi), eksplozije prahu ali plina, ki se sprošča, sproščajo se strupeni produkti, ki vplivajo na okolje (podtalnico, zrak).

Požarna varnost je danes sestavni del sodobne strategije preživetja in konkurenčnosti na trgu.

V ta namen je bila sprejeta smernica CFPA-E št. 32F Obdelava in shranjevanje odpadkov in gorljivih odpadnih materialov.

Smernica je namenjena predvsem osebam, odgovornim za varnost v podjetjih

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



in organizacijah, ki upravljajo zbirne centre. Namenjena je tudi reševalnim službam, svetovalcem in podjetjem, ki se ukvarjajo z varnostjo, da bodo lahko pri svojem delu ukrepali in prispevali k večji požarni varnosti.

Najpogostejši vzroki za nastanek požara na odlagališčih odpadkov so vandalizem, namerni požigi, kajenje, vroče naprave ali vroča dela, eksplozije prahu ali plina, napake na električnih napravah ali vodnikih, samovžigi, gradbena mehanizacija, atmosferske razelektritve.

Pri načrtovanju in izvedbi sistemov za zgodnje odkrivanje in javljanje tovrstnih požarov je treba pogosto posegati po najzahtevnejši namenski opremi, ki skupaj s splošnim sistemom za samodejno odkrivanje in javljanje požara, alarmiranje, obveščanje in po potrebi tudi za aktivno gašenje, predstavlja aktivno požarno zaščito.

Najučinkovitejša oprema za zgodnje odkrivanje in javljanje požara na odlagališčih za odpadke temelji na brezkontaktnem merjenju termičnega (IR - infrardečega) sevanja premikajočih se ali mirujočih objektov.

Ker se objekti med seboj razlikujejo, je treba pri načrtovanju primerne in zanesljive zaščite posegati tudi po drugi opremi, kot so javljalniki požarnih plinov, IR-javljalniki odprtega plamena in izjemno občutljivi aspiracijski javljalniki dima (ASD), ki so primerni tudi za vgradnjo v prostore s temperaturo pod lediščem do -30 °C.

Če na odlagališču nastane požar, se lahko zelo hitro širi. Razvit požar lahko doseže zelo visoke temperature. Zaradi velike količine odpadkov so takšni požari lahko dolgotrajni, pri tem pa se sprošča veliko dima, poraba gasilnih sredstev je velika, pri tem pride tudi do velike onesnaženosti naravnega okolja (zrak, tla, voda).

IR-javljalnik z infrardečo merilno tehnologijo in inteligentno analizo signala hitro odkrije vse vrste žarečih in odprtih požarov, tudi v razvojni fazi. Vgrajen senzor termične slike ima več kot 1000 toplotno občutljivih slikovnih pik, katerih pragi se lahko prosto parametrirajo. Infrardeči javljalnik je optimalno prilagodljiv aplikaciji, ki jo je potrebno doseči glede na okolje. Odzivni čas 100 milisekund omogoča spremljanje tekočih trakov ali drugih transportnih sistemov. Uspešno signalizira tudi vroč tek (ležaji, gredi, valji). IR-javljalnik uspešno signalizira tudi razsuti material. Njegova trdna konstrukcija in standardno integrirano tesnjenje varuje javljalnik pred prahom, umazanijo in vlago.

Idealni javljalniki za zaznavanje požarov vzdolž zaprtih transportnih trakov, zabojnikov, silosov in podobno so javljalniki požarnih plinov.

Javljalnik požarnih plinov je na čelu naprednega sistema za zaznavanje in odkrivanje požara. Odprte in prikrite požare zazna že v začetni fazi požara. Nove generacije javljalnikov imajo štiri polprevodniške senzorje plina, katerih parametre je mogoče spreminjati. Z njimi po večkriterijski tehnologiji spremljajo in ocenjujejo koncentracijski profil požarno značilnih plinov. Njihova robustna konstrukcija jih varuje pred poškodbami, ki jih povzročajo prah,

umazanija in vlaga. Večkriterijsko vrednotenje omogoča natančno prenašanje motenj, ki jih povzročajo naravno prašenje ali izpušni plini transportnih vozil in delovnih strojev. Z upoštevanjem razmer na objektih (pretok zraka in podobno) lahko javljalnike uporabimo na skoraj vseh področjih notranjega sistema.

Odlagališča odpadkov se največkrat razprostirajo na velikih odprtih površinah, ki dosegajo tudi več 10.000 m2 površine. Dostop je otežen, inštalacijska dela nedostopna. V teh primerih so edina primerna zaščita javljalniki odprtega plamena.

Javljalniki plamena delujejo v najtežjih okoljskih razmerah in so samostojne naprave, zasnovane za neposredno povezavo s krmilnimi in alarmnimi sistemi ali avtomatskimi sistemi za gašenje požara. Zagotavljajo najbolj celovito zaščito pred požari goriv in plinov. Zaznavajo požare na velikih razdaljah. Javljalniki imajo kompaktno, lahko in zelo trpežno ohišje iz nerjavečega jekla, odporno proti vremenskim vplivom, in ogrevano okno, ki preprečuje kondenzacijo in v zimskem času zaledenitev.

Vsak požar spremlja tudi dim. V velikih pokritih skladiščnih halah je eden od ključnih elementov zaščite zelo občutljiv aspiracijski javljalnik dima. Posamezen javljalnik lahko spremlja velike prostore s površino preko 5.000 m^2. Je idealen za okolja, kot so območja z globokim zmrzovanjem, eksplozijsko nevarna območja ali prostori z visoko stopnjo onesnaženosti in visoko vlago.

Ventilator sesa zrak iz opazovanega prostora ali objekta skozi odprtine za odvzem vzorcev. Izsesani zrak se po cevi dovaja v procesno enoto za vrednotenje, kjer vgrajeni senzor dima nenehno analizira prisotnost dimnih delcev in na podlagi parametrirane vrednosti tudi javi požarni alarm. Zaslon na nadzorni plošči prikazuje koncentracijo dima v vzorčenem zraku in druge alarme ali napake. Aspiracijski javljalnik dima lahko deluje kot samostojna enota, lahko se poveže v mrežo več enot ali pa neposredno s požarnim alarmnim sistemom.

Z nevarnimi odpadki moramo ravnati še posebej pazljivo. Nevarni ali posebni odpadki so tisti, ki imajo eno ali več lastnosti nevarnih snovi in z neprimernim ravnanjem lahko škodljivo vplivajo na okolje in zdravje ljudi.

Tudi ko nevarne snovi niso več uporabne, moramo uporabniki poskrbeti, da ne pridejo v stik z ljudmi ali okoljem. Če takšni odpadki končajo na odlagališčih, lahko pride do sproščanja nevarnih snovi iz teh odpadkov v okolje, zlasti v tla in v podzemne vode. Pri nevarnih odpadkih pogosto prihaja do sproščanja škodljivih, strupenih in eksplozivnih plinov, zato se v njihovih odlagališčih vgrajujejo javljalniki za zaznavanje takih plinov.

Skupaj moramo na področju ravnanja z odpadki narediti več, da bodo naša odlagališča in narava varna. Z odgovornostjo in strokovnostjo lahko preprečimo, da bi do požara sploh prišlo. Če se to zgodi, pa da ga čim prej odkrijemo. ■

Tudi ko nevarne snovi niso več uporabne, moramo uporabniki poskrbeti, da ne pridejo v stik z ljudmi ali okoljem. Če takšni odpadki končajo na odlagališčih, lahko pride do sproščanja nevarnih snovi iz teh odpadkov v okolje, zlasti v tla in v podzemne vode.





INFORMACIJSKE STORITVE IN INŽENIRING, D.D.

INFORMATIKA

www.informatika.si

Celovite rešitve
po meri naročnika



www.posita.si

PS POSITA

Postavljamo nova merila poslovne varnosti.

Zaupajte najboljšim med najsodobnejšimi

- Najsodobnejši sistem v Sloveniji,
- najvišja raven varnosti in
- možnost stalnega nadzora ter dostopa do lastne opreme.

PODATKOVNI CENTER POŠTE SLOVENIJE

Izberite med različnimi tipi podatkovnih centrov in stopnjami varovanja.

posita@posta.si

Pošta Slovenije
Zanesljivo z vami!

Avtor: mag. Martin Logar / vodja štabne službe za skladnost poslovanja in obvladovanje tveganj, Slovenske železnice d.o.o.*



ALI TVEGANJA ŽE OBVLADUJEJO NAS?

Pristopi k obvladovanju tveganj se zaradi spremenjene dinamike okolja hitro spreminjajo. V preteklosti prepogosto uporabljena taktika s področja prepoznave in obvladovanja novih tveganj po sistemu »počakajmo, bomo videli« (ang. wait and see) ne zaščiti gospodarske družbe pred ekonomskimi vplivi tveganj za njihovo poslovanje. Nujno je sprejeti drugačno dinamiko tveganj in posledično spremeniti strategijo/ukrepe obvladovanj ključnih tveganj, torej tistih, ki imajo ocenjeno škodo najslabšega scenarija nad sprejemljivo mejo apetita.

Gospodarske družbe, ki danes še nimajo razvitega samostojnega področja obvladovanj tveganj, so v situaciji, da za pravočasno prepoznavo in sprejem ustreznih strategij ščitenja pred bodočimi tveganji, ne bodo imele več dovolj časa, saj jih bodo nova tveganja prehitela in jih (družbe) pričela obvladovati.

Manjša tveganja

pogosto je opaziti taktiko gospodarskih družb, da prepoznajo večje število manjših, za stabilno ekonomsko poslovanje družb nepomembnih tveganj, katerih obvladovanje je relativno enostavno in učinkovito. Na ta način poskušajo dokazati, da so prepoznali vsa tveganja (tako imenovani »audit universe«), kar seveda ni res. Osredotočamo se na manjša tveganja, ki so v bistvu bolj motnje v procesu, zato, da se hitro vidijo rezultati aktivnosti, pozabljamo pa na določanje in spremljanje aktivnosti obvladovanja ključnih tveganj, ki imajo lahko na družbo občutno večji vpliv z vidika ekonomskih kazalnikov.

Diskretna in zvezna tveganja

Po drugi strani v matrikah tveganj pogosto naletimo na kombinacijo ocen in verjetnosti tveganj, kjer imata oba kazalnika največje vrednosti, kar je lahko le izjema, ne sme pa biti pravilo. Tak pristop je uporabljen kadar želimo poudariti resnost tveganja. Vendar gre za napačno taktiko obvladovanja, predvsem pa komuniciranja o resnosti ocenjene situacije. Vsak dan pač ne more priti do recesije, izgube ključnega trga in podobno. Po navadi se takšni katastrofalni dogodki zgodijo zelo poredko, ko pa nastopijo, pa imajo dolgoročne posledice. Velikokrat spregledamo, da imajo nekatera tveganja po svoji naravi dolgoročne posledice in ne samo enkratno poslovno škodo (razlika med zveznimi in diskretnimi tveganji). Ocena učinka takšnega tveganja se seveda izračunava na drugačnih parametrih (ocena persistentnosti).

> Prej ko bomo prevzeli dejstva, da gre za popolnoma drugačno dinamiko tveganj in posledično drugačno strategijo obvladovanj kot v preteklosti, prej bomo lahko razvili in sprejeli ustrezno poslovno strategijo ključnih ukrepov za obvladovanja tveganj.

Tveganja včeraj

V preteklosti smo tveganja prvenstveno povezovali s finančno stabilnostjo družbe v odvisnosti od likvidnostnih, obrestnih, valutnih tveganj. Obvladovanje tveganj je bila domena finančnih oddelkov. Z vpeljavo raznih mednarodnih standardov s področja vodenja kakovosti, so v registre tveganj prišla še mnoga procesna tveganja.

Družbe, ki delujejo v kapitalsko intenzivnih panogah (npr: v avtomobilski nabavni verigi, farmaciji, zavarovalnice, banke), so ponotranjile principe obvladovanj tveganj, ki jih nalagajo mednarodni standardi (pomembnejši napredek na tem področju se je zgodil v 80 letih prejšnjega stoletja) in jih dejansko uvedle v svojo procesno urejenost.

Velika večina ostalih družb, ki jim to še ni bilo potrebno z vidika zahtev ostalih partnerjev (dobavitelji, kupci, lastniki, regulatorji),

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

pa je le ohlapno sprejela navodila in usmeritve zunanjih presojevalcev, ki preverjajo stanje in podajajo ocene enkrat letno. To je bil v večini primerov tudi edini čas, ko so se interni deležniki vpleteni v proces zagotavljanja skladnosti s standardi zganili, preverili kaj so naredili in podali usmeritve za preverjanje naslednjega leta. Proces ocenjevanja in usmeritev večinoma poteka brez prepoznave ključnih kazalnikov. Prevladovati bi morali kvantitativni (ocena ekonomskih vplivov sprejetih ukrepov na poslovanje družbe), izjemoma pa tudi kvalitativni kazalniki.

Tveganja, ki niso ocenjena v denarnih enotah težko predstavljajo otipljivo, pomembno informacijo. Nasprotno so finančna tveganja vedno izražena v denarnih enotah in lahko zavzamemo stališče ali so sprejemljiva ali ne. Zato je večina poslovodstev družb ohranila fokuse na finančnih tveganjih.

Operativna tveganja, ki so bila posledica vpeljav raznih standardov so postala domena služb za kakovost, certificiranje in podobnih, ki pa običajno nimajo direktnega dostopa do poslovodstev, oziroma ne ocenjujejo tveganj z vidika poslovne škode. Takšna tveganja se po navadi poročajo enkrat letno ob izvedbi zunanje presoje standarda.

Danes se zato v večini družb, kjer še ni razvitega ustreznega okolja prepoznave tveganj, še vedno primarno ukvarjajo s tveganji, ki nimajo večjih ekonomskih učinkov na poslovanje.

Šele pred kratkim se je z uvedbo različnih statističnih modelov vrednotenja ocen tveganj v denarnih enotah, tudi pri nas spremenilo dojemanje pomembnosti sprejetih strategij obvladovanja tveganj tudi v družbah, ki niso del industrijsko intenzivnih panog.

Če je prejšnja skupina tveganj lahko prepoznana bolj kot akademska skupina tveganj neskladij s standardi, pa nas v prihodnje čakajo izzivi, ki jih ne bomo mogli spregledati ali jim ne nameniti dovolj velike pozornosti. Bodoča tveganja ne sprašujejo za dovoljenje (akreditacijski postopki so izbira družbe), ampak so že tukaj (zakoni, nasprotja interesov) in pri nas naseljena (virusi).

Tveganja so neločljivo povezana s poslovnimi cilji. Njihova verjetnost in ocena pa sta odvisna od notranjega in zunanjega okolja. Zato je še toliko bolj potrebno jasno opredeliti postopek ocenjevanja in izvajanje nadzora posameznih vplivov tveganja.

Mnogi današnji zakoni (ZSDH, ZIntPK, ZPPDFT idr.) predpisujejo vlogo pooblaščencev poslovodstev za integriteto in upravljanje tveganj. To naj bo samostojni strokovni organ, ki ocenjuje tveganje skladnosti poslovanja z zakoni in internimi dokumenti, vzpostavitvi notranjega nadzora za prepoznavo in preprečevanje tveganj korupcije, nasprotja interesov, nedovoljenih interesnih vplivov ter drugih neetičnih ravnanj.

Tveganja prihodnosti

Bodoča ključna tveganja ne temeljijo le na predvidevanju razvoja makroekonomskih kazalnikov posameznih regij ali industrijskih panog, temveč so povezana z vedno večjimi regulatornimi zahte-



vami (ki so predvidljive, saj lahko aktivno sodelujemo pri pripravi zakonov, podzakonskih aktov…), vedno bolj dinamično kibernetsko nevarnostjo (vsak dan se dogodi nekaj novega) in vedno bolj sofisticiranimi načini prevar, zlorab in korupcije.

Ključna tveganja, ki jim bomo morali torej v prihodnosti nameniti posebno pozornost so po številnih raziskavah v svetu in doma povezana s stalno spremenljivimi regulatornimi tveganji, makroekonomskimi spremembami, kibernetično varnostjo, ter tveganji prevar in korupcije.

Obvladovanje teh tveganj je povezano izključno s pripravljenostjo družb po soočenju s svojimi internimi problemi in vzpostavitvijo pravih kontrolnih mehanizmov, izobraževanjem, korporativno kulturo, dobrega internega komuniciranja ter vzpostaviti linije poročanja domnevnih kršitev korporativne integritete.

Realizirana tveganja - prijave domnevnih kršitev

Slednje bo še posebej pomembno ob vpeljavi nove Regulative o zaščiti oseb, ki prijavijo kršenje prava EU. Družbe bodo morale vzpostaviti varne kanale za prijavo nepravilnosti, korupcije in goljufij, poleg tega pa vzpostaviti tudi jasne postopke poročanja o prijavah in obravnavah, ter zagotoviti preprečevanje povračilnih ukrepov in učinkovito zaščito za žvižgače.

Navkljub prepričanju, da večina prevar nastane na spletu (z zlorabo identitete, kibernetičnimi vdori), kar lahko preprečimo le z učinkovito in stalno nadgradnjo informacijske zaščite, pa je dejstvo, da do večine prevar in zlorab še vedno prihaja interno s tradicionalnimi metodami.

Vzpostavitev varnih linij javljanja domnevnih kršitev je učinkovito orodje za prepoznavo tveganj, saj poročane domnevne prevare in prekrški pomenijo realizirano tveganje. Identificiranje teh tveganj in sprejem ustreznih ukrepov je stroškovno učinkovito, saj pridobimo večinoma zelo točne in pravilne podatke o prevarah in zlorabah, torej udejanjenih tveganjih.

Obravnava večine (≥70%) prijav (zbiranje podatkov, preskus trditev ipd.) se lahko izvede v manj kot 30 dneh. Delež sprejetih ukrepov (≥30%) in delež nepopolnih prijav (≤10%) sta pokazatelja resnosti in vsebine prijav. Vse prijave, ki imajo znake možnih kaznivih dejanj takoj predamo v obravnavo ustreznim zunanjim inštitucijam in tako učinkovito obvladamo izkazano tveganje, ki so ga prepoznali sodelavci. S tem tudi pozitivno vplivamo na kulturo družbe, vzpostavitev in potrditev etičnih norm in vsekakor povečamo uspešnost delovanja družbe. Prej ko bomo prevzeli dejstva, da gre za popolnoma drugačno dinamiko tveganj in posledično drugačno strategijo obvladovanj kot v preteklosti, prej bomo lahko razvili in sprejeli ustrezno poslovno strategijo ključnih ukrepov za obvladovanja tveganj. Prav tako pa moramo biti pozorni na preprečevanje drobljenja posameznih tveganj na pod nivoje in s tem relativizacijo posameznega tveganja (nižja parcialna ocena) in predvsem na preprečevanje ponavljanje istih operativnih tveganj v različnih procesih. ■



Vse bo v redu.

triglav

www.triglav.si



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 OSCP

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

BUREAU VERITAS

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

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Upravljanje s tveganji in korporativna varnost

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

Omogočiti obvladovanje poslovno varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Zakaj Upravljanje s tveganji in korporativna varnost?

- **Študij za poklic prihodnosti.** Študij daje multidisciplinarna teoretična in praktična znanja s področja managementa in obvladovanja najrazličnejših tveganj v podjetju.
- **Nadgradnja širokega poslovnega znanja.** Študij omogoča spoznavanje vsebin, ki so značilne za korporativno varnost: geostrateški in politični vidiki varnostnih tveganj, varnostni standardi v poslovnih procesih, upravljanje varnostnih tveganj, načrtovanje in razvoj korporativne varnosti na vseh nivojih, procesi nadzora, gospodarsko poizvedovanje in mehanizmi za obvladovanje najrazličnejših tveganj.
- **Spoznavanje globalnega poslovnega okolja.** Tekom študija se obravnava številne primere iz domačih in mednarodnih podjetij, ki jih predstavljajo vrhunski strokovnjaki na področju varnosti v regiji.
- **Mreženje in osebni pristop.** Študij poteka v manjših skupinah, ki omogočajo neposredno sodelovanje predavateljev in študentov.

Komu je študij namenjen?

- Managerjem in strokovnjakom s področja korporativne varnosti, ki si želijo razširiti svoje poslovno znanje in pridobiti širšo perspektivo za dobro razumevanje globalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja.
- Tistim, ki si želijo pridobiti znanje za vodenje oddelkov na področju korporativne varnosti v javnem in gospodarskem okolju ter mednarodnih korporacijah.
- Podjetnikom in zaposlenim v sistemih, ki delujejo na področju energetike, telekomunikacij, informatike, transporta, financ in vsem, ki se srečujejo z vprašanjem varnosti ter tveganj v organizacijah.



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

- **RAZPISANE SMERI:**
  - **Korporativni varnostni manager**
  - **Korporativni varnostni manager - podjetnik**
- **POGOJI ZA VPIS:** diploma 1. stopnje ali starega visokošolskega strokovnega študijskega programa. Možen je tudi vpis neposredno v 2. letnik. Podrobnosti o vpisnih pogojih so na voljo na spletni strani: www.gea-college.si.
- **TRAJANJE ŠTUDIJA:** študij traja 2 leti in obsega 120 kreditnih točk po ECTS.
- **PRIDOBLJENI NAZIV:** magister/magistrica korporativne varnosti.
- **IZREDNI ŠTUDIJ:** izvaja se po razporedu, ki je prilagojen zaposlenim (študentom). Predavanja potekajo med tednom v popoldanskem času in ob sobotah dopoldne.
- **PRIZNAVANJE ZNANJ IN SPRETNOSTI:** na podlagi znanj, ki jih je posameznik pridobil s formalnim ali neformalnim izobraževanjem na tečaju, delavnici ali seminarju, se lahko prizna del študijskih obveznosti.
- **DODATNE AKTIVNOSTI IN PREDNOSTI:** mednarodna izmenjava (študij ali praksa) na več kot 30 partnerskih institucijah, podpora Kariernega centra, mednarodna konferenca, Alumni klub, ekskurzije in druge študentske aktivnosti. Študij je podprt tudi s sodobnim e-portalom, ki nudi študijske vsebine 24 ur na dan.



"Velika dinamika poslovnega okolja in stanje kriznih razmer sta danes postali stalnici. Tisti, ki tega ne razumejo, ostajajo v preteklosti. Ujemite prihodnost in dovolite, da vas s pomočjo interdisciplinarnih znanj, ki temeljijo na prenosu dobrih praks iz neposrednega poslovnega okolja, opremimo, da boste sposobni obvladovati tveganja in ustvarjati nove poslovne priložnosti."

izr. prof. Denis Čaleta, predavatelj, predsednik Slovenskega združenja korporativne varnosti

Predmetnik

I. LETNIK

Skupni obvezni predmeti

- *Management korporativne varnosti*
- *Geostrateški in politični vidiki varnostnih tveganj v mednarodnem poslovnem okolju*
- *Pravni vidiki korporativne varnosti*
- *Ekonomika obvladovanja tveganj v poslovnem okolju*

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

- *Varnostni standardi v poslovnih procesih*
- *Upravljanje varnostnih tveganj*
- *Načrtovanje in razvoj korporativne varnosti*

Smer Korporativni varnostni manager – podjetnik

- *Trženje/Marketing*
- *Finance*
- *Procesi nadzorstva v korporativnem varnostnem okolju*

Izbirni predmeti (študent izbere dva):

- *Management človeških virov*
- *Okoljski vidiki korporativne varnosti*
- *Metode raziskovanja varnostnih pojavov*
- *Zavarovalništvo v procesih zagotavljanja gospodarske varnosti*
- *Gospodarsko poizvedovanje in varovanje poslovnih informacij*
- *Informacijska varnost*

- *Študijski praktikum opravlja študent v 1. in 2. letniku*
- *Magistrsko delo*

GEA College je sodoben izobraževalni center in vodnik na poti k poslovni odličnosti.

GEA College nudi uporabna znanja s poudarkom na podjetništvu in managementu. Preko vpetosti v poslovno okolje spodbuja razvijanje inovativnih idej ter širjenje znanja in zavesti o tem, da je podjetništvo gonilna sila razvoja gospodarstva.

CENTER VIŠJIH ŠOL

Višješolski programi
(2 letni študij):
- Ekonomist
- Poslovni sekretar
- Informatika
- Organizator socialne mreže
- Gostinstvo in turizem

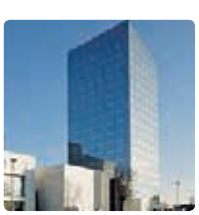
FAKULTETA ZA PODJETNIŠTVO

Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

Magistrski programi
(2 letni študij):
- Podjetniški management
- Management korporativne varnosti

POSLOVNO-IZOBRAŽEVALNI CENTER

- Poslovni seminarji in delavnice
- Usmerjena poslovna izobraževanja
- Izobraževanja v podjetjih





GEA College - Fakulteta za podjetništvo
Dunajska cesta 156
1000 Ljubljana
T: (01) 588 13 00
F: (01) 568 82 13
E: podiplomski@gea-college.si
www.gea-college.si

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo


ELES
Prenašamo energijo, ohranjamo ravnovesje.
WWW.ELES.SI