Korporativna varnost

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

Letnik 2021, december • št. 27

Tradicionalna 13. mednarodna konferenca »Dnevi korporativne varnosti 2022«

Ljubljana, 24-25. maj 2022

Prihodnost Evrope in Slovenija

Veleposlanik Vojko Volk

VAŠA 360° VARNOST 365 DNI V LETU

MODRO JE IZBRATI OPERATIVNI CENTER KIBERNETSKE VARNOSTI

360° varnost vam zagotavlja **najsodobnejšo kibernetsko zaščito**. Na mobilni, stacionarni, oblačni in lastni infrastrukturi, ki je lahko tarča kibernetskega napada ali zlorabe. Zaradi vedno večje kompleksnosti kibernetskega okolja in varnostnih groženj brez kibernetske varnosti digitalni razvoj ni mogoč. Človekova zmožnost uvida v dogodke in povezovanje informacij pa je kljub vsej tehnologiji nepogrešljiva. Zato naj za vas vse dni in noči skrbijo naši **strokovnjaki Operativnega centra kibernetske varnosti (OCKV)**, ki ves čas spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske napade.

Ob morebitnem kibernetskem napadu vam zagotovijo omejitev napada in zmanjševanje škode, zbiranje in zavarovanje dokazov, zagotavljajo revizijsko sled in vas sproti seznanijo s pomembnimi dogajanji, ki jih zaznajo. OCKV Telekoma Slovenije je certificiran **po mednarodnem standardu za informacijsko varnost ISO 27001**, ob tem pa ima Telekom Slovenije tudi **certifikat za neprekinjeno poslovanje ISO 22301**. Naše storitve s področja 360° varnosti so tako primerne za podjetja vseh velikosti, saj OCKV za vsakogar poišče ustrezne rešitve.

telekom.si/poslovni

TelekomSlovenije

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:
december 2021

Izvod revije je brezplačen

Naslovnica in slike:
ID 136191118 © Alexandersikov | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

Obdobje pandemije se nadaljuje z vedno novimi modalitetami in mutacijami virusa, kar je dobesedno postalo naša nova realnost. Ta realnost pa nima samo zdravstvenega predznaka, temveč vedno bolj vpliva tudi na socialno in psihološko področje delovanja družbe. Korporativna varnost kot proces, je bila primorana svoje organizacijske pristope kar najhitreje prilagajati, da se je v organizacijah lahko zagotovilo varno in neprekinjeno poslovanje. Vendar pomembni izzivi, vezani na medosebne odnose v kolektivih, šele prihajajo. Nestrpnost ter fizična in psihična agresivnost, bosta v po pandemičnem obdobju postali pomemben izziv, s katerim se bodo soočali strokovnjaki s področja korporativne varnosti. Če te izzive postavimo v širši geostrateški prostor, kjer poteka neizprosen konkurenčen boj med gospodarskimi velesilami, informacije v digitaliziranih procesih pa postajajo pomembna strateška prednost, lahko zelo hitro ugotovimo, da je ravno človek tista komponenta, ki ima tukaj še vedno osrednjo vlogo. Ustrezno varnostno zavedanje pri upravljanju s ključnimi informacijami ima, zaradi različnih modalitet delovnega okolja, v katerega smo bili zaradi epidemije primorani, še dodaten pomen. S stališča strokovnjakov, ki zagotavljajo vzpostavitev varnostnih procesov, pa to postavlja vedno težje enačbe z dokaj neznanim rezultatom. Upam, da je sedaj strateškemu vodstvu organizacij dokončno jasno, da bo potrebno z vso resnostjo začeti naslavljati individualizem novih generacij in ga poskušati usmerjati v razumevanje pomembnosti zasledovanja skupnih ciljev. Seveda je to samo del širše družbene potrebe in preobrata, ki ga bo potrebno narediti v celotni družbi, če želimo, kot nacija, preživeti v tem zahtevnem varnostnem okolju. Za spremembo te paradigme moramo najti ustrezno razumevanje in podporo v vseh delih družbe še posebej zaposlenih na organizacijskem nivoju. V tem primeru nikakor ne pride v poštev, da se teh procesov lotevamo s figo v žepu, ker bodo posledice tega nepopravljive. Dober primer, ki je močno soodvisen z napisanim, predstavlja zaveza držav za ohranjanje okolja in zmanjšanja segrevanja ozračja. Ohranjanje okolja, ali če hočete družbenih odnosov, je naš skupni izziv in potreba. V tem je torej vsak posameznik izrednega pomena. Samo v skupnost usmerjeno razumevanje nadaljnjega razvoja bo prineslo pomembne pozitivne korake v družbenih odnosih, kar se bo na mikro ravni reflektiralo v razumevanju varnosti primarnega okolja v naših organizacijah.

V tokratni številki revije smo, ravno zaradi tega, želeli vsebinsko osvetliti dovolj širok spekter strokovnih prispevkov, da v tem okviru prenesemo določene nove vidike in izkušnje tudi na področja, ki jih prinaša uvajanje novih pristopov in tehnologij. Posebej bi želel izpostaviti strateško geopolitično oceno, ki jo tudi tokrat prinaša kolumna. Izkoristili smo priložnost in se pogovorili s pomembnimi strateškimi voditelji in strokovnjaki z različnih področij, ki so z nami delili svoje izkušnje in strateške poglede.

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. Ob tem nam dovolite, da vam ob prihajajočih božičnih in novoletnih praznikih zaželimo vse dobro ter veliko zdravja in osebne sreče.

izr. prof. dr. Denis Čaleta
Glavni urednik

KOLUMNA
Vojko Volk, veleposlanik

PRIHODNOST EVROPE IN SLOVENIJA

INTERVJU
Rajko Novak, direktor, Smart Com

KORPORATIVNA VARNOST NUJNI POGOJ DELOVANJA MODERNIH ORGANIZACIJ

VARNOST DOBAVNE VERIGE

V zadnjih dveh letih smo bili vključeni v številne razprave o varnosti dobavne verige 5G z različnimi evropskimi deležniki. Po vseh teh mesecih nam ne da miru eno vprašanje – ali pozornost usmerjamo v pravo smer, imenovano »zaupanja vreden dobavitelj«.

PRENOSI PODATKOV V TRETJE DRŽAVE

V današnjem svetu smo vse bolj povezani, zato ni nenavadno, da je prenos podatkov v tujino vse bolj običajen tako za multinacionalna podjetja kot tudi za številna majhna podjetja, javni sektor in druge organizacije. Evropski pravni okvir zagotavlja relativno visoko raven varstva osebnih podatkov – izven EU je ta raven različna in marsikje ne dosega evropskih standardov.

NOTRANJA PREVARA: KAKO ZMANJŠATI NJENO VERJETNOST

Mednarodni teden ozaveščanja o prevarah, letos v novembru v Sloveniji obeležujemo že četrtič, s sloganom “Skupaj v boju proti prevaram”. Obravnava zlasti notranjih prevar je zelo aktualna, saj se te dogajajo v velikih, srednjih ali malih organizacijah, v različnih panogah in geografskih lokacijah. Notranja prevara lahko povzroči velike finančne izgube1, pravne stroške in uniči ugled organizacije.

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

Enzo Smrekar, podpredsednik Atlantic Grupe za delikatesne namaze, Donat in internacionalizacijo

UPRAVLJANJE ORGANIZACIJ VEDNO BOLJ PODVRŽENO VARNOSTNIM IZZIVOM

Razumevanje varnostnega okolja postaja pomemben dejavnik za učinkovito odločanje strateškega managementa v poslovnih organizacijah. Ob tej priložnosti smo se o pomenu upravljanja tveganj, med katerimi imajo varnostna tveganja vedno večji pomen, pogovarjali z g. Enzom Smrekarjem, podpredsednikom Atlantic Grupe za delikatesne namaze, Donat in internacionalizacijo.

V svoji karieri ste opravljali strateške funkcije v različnih poslovnih okoljih. Lansko leto ste tudi prejeli laskavi naziv manager leta 2020. Bodite tako prijazni in nam zaupajte kako pomembno je za strateškega managerja, da pravilno razume varnostno okolje v katerem posluje njegova organizacija?

Kako je varnost pomembna pove že to, da je potreba po varnosti ena osnovnih človekovih potreb. Ko so zadovoljene osnovne potrebe, se lahko razmahne kreativnost, drznost, radovednost.

V poslovnem okolju ni nič bistveno drugače. Upravljanje s tveganji je ključni element vodenja. Pravilno razumevanje varnostnega okolja v katerem poslujemo je osnova, da lahko tveganja predvidimo in se ustrezno odzovemo. Temu namenjamo res veliko pozornosti in energije.

Katerim virom ste pri svojih analizah največkrat zaupali, da ste lahko dobili relevantne informacije na podlagi katerih ste sprejemali ustrezne odločitve?

> Cilj, ki si ga je postavilo vodstvo Atlantic Grupe je bil zaščititi zdravje zaposlenih, zagotoviti nemoteno oskrbo kupcev in potrošnikov ter ohraniti poslovanje podjetja. Zagrizli smo vsi, od prvega do zadnjega zaposlenega in v zares težkih situacijah se potrdi, kako pomemben varnostni dejavnik so lojalni in zavzeti zaposleni v podjetju.

Smo marketinško orientirano podjetje, navajeni smo na svoj bazen informacij, na podlagi katerih sprejemamo relevantne odločitve, pridobljene iz najrazličnejših virov. Vemo kako jih ovrednotiti in filtrirati in kako na podlagi tega ukrepati. Tudi glede varnosti upoštevamo tako sistemske vire, relevantne za različna področja poslovanja, kot tudi izkušnje, znanje zaposlenih in strokovne ekspertize.

Upravljanje s tveganji, ki niso samo finančne narave, je verjetno za vsakega managerja postala stalnica. Kako pristopate do tega pomembnega varnostnega procesa v svojem poslovnem okolju, ki ga vodite?

Upravljanje s tveganji je sestavni del tako strateškega, kot letnega načrtovanja. Tveganja obstajajo na vseh področjih poslovanja, ne samo na finančnem, kot ste omenili. Na področju nabave surovin, embalaže, transporta, dela, političnega in gospodarskega okolja, sko-

*avtorica je članica Slovenskega združenja korporativne varnosti

Težko najdem dovolj močno besedo, s katero bi poimenoval skrb za informacijsko varnost v Atlantic Grupi. Močan in številčen oddelek visoko usposobljenih strokovnjakov skrbi za digitalno varnost v Atlantic Grupi.

raj neskončna vrsta jih je. Za tista, ki jih teoretično lahko opredelimo, lahko predvidimo tudi posledice, preventivne in sanacijske ukrepe. Za tista, ki pa jih težko konkretno opredelimo, pa jih obravnavamo bolj abstraktno. Vendar se na podlagi izkušenj in različnih vnaprej pripravljenih scenarijev lahko odzovemo tudi na take šoke, kot je na primer nenadna pandemija.

Neprekinjenost delovanja ključnih procesov v organizaciji, ki jo vodite, je zelo pomembna, še posebej v času epidemiološke krize. Kakšen pomen ima v vaši organizaciji proces neprekinjenega poslovanja in kako pristopate k ocenjevanju, kaj je zares kritično za vašo poslovno organizacijo?

Prehrambna industrija je vitalnega pomena za oskrbo prebivalstva v vseh kriznih situacijah, zato je še kako pomembno, da poslujemo neprekinjeno. Spremljamo dogajanja v svetu, predvsem na področju surovin, ki jih uporabljamo za svojo proizvodnjo. Seveda smo takoj zaznali tudi novi korona virus na Kitajskem, ko pa se je začel širiti v sosednji Italiji, smo bili že v stanju visoke pripravljenosti. Naš obrat za proizvodnjo Argete v Izoli je blizu meje z Italijo, naši zaposleni oziroma njihovi družinski člani pogosto prehajajo iz države v državo, nekatere surovine in velik del embalaže uvažamo iz Italije. Okrepili smo nabavo, uvedli smo dodatne delovne izmene, povečali proizvodnjo, gotove izdelke smo prepeljali do naših kupcev, za primer, da bi bil transport otežen in sprožili ter prilagodili varnostne načrte za zaščito zaposlenih. Kljub vsemu opravljenemu smo imeli tudi mi vrsto izzivov, predvsem z dozicami in pokrovčki za Argeto, s pomanjkanjem razkužila in zaščitnih mask za zaposlene, kar so do neke mere reševali naši laboratoriji na vseh proizvodnih lokacijah. Cilj, ki si ga je postavilo vodstvo Atlantic Grupe je bil zaščititi zdravje zaposlenih, zagotoviti nemoteno oskrbo kupcev in potrošnikov ter ohraniti poslovanje podjetja. Zagrizli smo vsi, od prvega do zadnjega zaposlenega in v zares težkih situacijah se potrdi, kako pomemben varnostni dejavnik so lojalni in zavzeti zaposleni v podjetju.

Procesi v podjetjih se vedno bolj digitalizirajo, kar na drugi strani prinaša določena nova tveganja na področju informacijske varnosti. Kakšen pomen dajete informacijski varnosti v vaši organizaciji?

Težko najdem dovolj močno besedo, s katero bi poimenoval skrb za informacijsko varnost v Atlantic Grupi. Močan in številčen oddelek visoko usposobljenih strokovnjakov skrbi za digitalno varnost v Atlantic Grupi.

Človeški potencial je vedno bolj pomemben za uspešno delovanje podjetij. Določena varnostna tveganja, kot so socialni inženiring, pa človeški faktor postavljajo tudi v položaj, ko nizko varnostno ozaveščen posa-

meznik, za organizacijo lahko predstavlja pomembno tveganje. Kakšne pristope uporabljate za dvigovanje varnostnega zavedanja kolegov, ki v organizaciji delajo na različnih strateških pozicijah in kako pristopate v razmerju do vsakega zaposlenega?

Kot že rečeno, pri informacijski varnosti ni popuščanja, ker so pogosto napake nepopravljive, včasih tudi usodne. Naša ekspertna skupina ne dopušča nobenih dvomov, sistemske zaščite so na najvišji možni ravni in se neprestano posodabljajo. To so procesi, ki jih ostali zaposleni niti ne poznamo, smo pa obveščeni, da se nadgrajujejo. Ve se, da je sistem tako močan, kot je močan njegov najšibkejši člen, zato v neprestana ozaveščanja, izobraževanja in testiranja vključujemo vse zaposlene, ki imajo pri svojem delu stik z računalnikom. Ne samo z stalnim periodičnim izobraževanjem, tudi s številnimi navideznimi t.i. phishing akcijami ostrimo pozornost svojih zaposlenih, da imajo IT varnostni inženirji čim manj dela.

Ste tudi predsednik Smučarske zveze Slovenije. Smučanje je še vedno eden od paradnih športov v Sloveniji. V zadnjem času vidimo, da je tudi na smučarskih prireditvah varnost udeležencev in tekmovalcev postala vedno pomembnejša komponenta. Imate v sami zvezi posebnega strokovnjaka, ki se ukvarja tudi z varnostnim področjem?

Ne, so pa tovrstni strokovnjaki del vsakega organizacijskega komiteja za posamezna smučarska tekmovanja in druge dogodke pod okriljem SZS.

Uvajanje novih tehnologij na smučarska tekmovanja, poleg pozitivnih učinkov, prinaša tudi določena varnostna tveganja. Spomnimo se nesreče z brezpilotnim letalnikom, ko je le ta skoraj padel na avstrijskega smučarja Marcela Hirscherja v Madonni di Campiglio. Kakšno je vaše stališče do uvajanja novih tehnologij na smučarska tekmovanja?

Uvajanje novih tehnologij je nujno potrebno, tudi na smučarskih tekmovanjih. Nudijo izboljšanje tehničnih rešitev prikaza tekmovanja, predvsem mlajša publika si želi in pričakuje čim bolj atraktivne posnetke, grafične prikaze, hitrost informacij ... prav je, da gremo v korak s časom. Seveda sodobna tehnologija, poleg vseh prednosti, prinese tudi določena tveganja, ampak tako je pravzaprav v življenju. Na čisto vse se pač ne moreš pripraviti.

Tudi smučanje ni imuno na prirejanje športnih rezultatov in s tem povezanih stav. Ali temu področju na SZS namenjate kakšno pozornost?

Nismo zasledili, da bi se v zimskih športih dogajale zlorabe, povezane s prirejanjem rezultatov. Pravzaprav se mi zdi nemogoče tovrstno taktiziranje pri športu, ko se znotraj ene sekunde skozi cilj pripelje deset ali več tekmovalcev.

Slovensko združenje za korporativno varnost predstavlja eminentno združbo najpomembnejših slovenskih podjetij in tudi javnih institucij. Menite, da bi z vašo vključitvijo lažje prihajali do dobrih praks in izmenjave izkušenj na področju obvladovanja varnostnih tveganj?

Povezovanje in deljenje dobrih praks je vedno dobrodošlo, čeprav se praviloma povedanega ne da dobesedno presaditi iz ene situacije na drugo. A izkušnje drugih lahko vedno sprožijo nek nov, inovativen način razmišljanja ali pa opozorijo na skrite nevarnosti. ■

Foto: arhiv Atlantic Grupe

Avtor: Vojko Volk / veleposlanik

KOLUMNA

PRIHODNOST EVROPE IN SLOVENIJA

„Evropa ni nikoli obstajala. Evropa bo ustvarjena.“

/Jean Monnet, ustanovni oče Evropske unije/

Največji dosežek EU po tem, ko je v zadnjih letih preživela in kar dobro prestala tri zahtevne preizkušnje, je že v tem, da prihodnost sploh še ima. Ima pa tudi preteklost, ki je v prvi vrsti preteklost imperijev na današnjih ozemljih EU. Značilnost imperijev pa je prevlada ene države ali naroda nad drugimi, utemeljena na vojaški, politični ali pa gospodarski premoči. In prav zato je imel Jean Monet prav, ko se je projekta združene Evrope lotil iz predpostavke, da Evrope v resnici nikoli ni bilo in da bo Evropo kot zvezo svobodnih narodov šele potrebno ustanoviti. Gledano z današnjimi očmi se nam EU zdi samoumevnost, do katere smo vsi močno kritični, a je zgodovinski uspeh EU v resnici velikanski. Nikoli prej ni na svetu obstajala delujoča in gospodarsko uspešna zveza narodov ali držav, ki bi bila utemeljena na demokratičnih načelih enakopravnosti in svobodi tako vstopanja vanjo kot izstopanja iz nje. V letih po gospodarski krizi leta 2008, ko je kazalo, da utegne finančni virus iz Amerike izzvati bankrot nekaterih članic EU in ogroziti obstoj evra, se je izkazalo, da je EU v resnici trdnejša kot se nam zdi in da je rešitev evra pomenila tudi rešitev EU. Potem so v vsega petih letih sledile še tri zahtevne preizkušnje za obstoj EU.

Gledano z današnjimi očmi se nam EU zdi samoumevnost, do katere smo vsi močno kritični, a je zgodovinski uspeh EU v resnici velikanski. Nikoli prej ni na svetu obstajala delujoča in gospodarsko uspešna zveza narodov ali držav, ki bi bila utemeljena na demokratičnih načelih enakopravnosti in svobodi tako vstopanja vanjo kot izstopanja iz nje.

Prva in najtežja preizkušnja je bila strahovit begunski val iz leta 2015, ki je dokončno sprl države vzhodne Evrope z zahodnimi, kar velja zlasti za Poljsko in Madžarsko. Z begunskim valom in prepiri znotraj EU je bil trajno poškodovan šengenski prostor, kot ena od največjih - poleg evra - pridobitev EU. Nemčija in Avstrija sta takrat uvedli „začasni“ suspenz šengenske ureditve na svojih mejah, sledilo jima je še pet držav, vse skupaj pa še danes vztrajajo pri tej „začasnosti“. Danes povsem zanesljivo vemo, da begunski val ni bil naključen in da je imel svoje botre, ki so zaradi svojih interesov dobesedno razstrelili Sirijo in praktično ves Bližnji vzhod, vedoč, da begunci od tam ne bodo bežali ne v Moskvo, ne v Washington, ampak preko Turčije v Evropo. Danes se ta hibridna vojna z usmerjanjem migracij proti EU ne nadaljuje samo po balkanski poti in po morju, ampak po novem tudi na meji med Poljsko in Belorusijo. Očitno je, da se Moskva še kar ne more upreti skušnjavam, da EU drži v nenehnih napetostih in razpihuje notranje prepire, pri čemer se poslužuje vseh vzvodov, ki jih ima na razpolago. Ker nas z dobavami plina ne more več izsiljevati, ker ga preprosto mora prodajati ali pa tvega finančni kolaps Rusije, se Putin posveča izzivanjem političnih napetosti na Balkanu, v Ukrajini in zdaj še z Lukašenkom. Če bi Putin toliko energij, kot jih vlaga v hibridno vojno z Evropo, vložil v razvoj lastnega gospodarstva in države, potem Rusija ne bi bila več med najrevnejšimi evropskimi državami.

Druga huda preizkušnja za EU je bila izvolitev Donalda Trumpa, ki si je tako kot Putin za cilj zadal razbitje EU, spodbujal je brexit in v Evropi podpiral najradikalnejše protievropske politike. Kot slon v trgovini s porcelanom je sesuval ključne mednarodne pogodbe, ki so svet držale v krhkem ravnovesju, od pariškega okolijskega sporazuma do jedrskega sporazuma z Iranom. K sreči je Trump izgubil volitve, pogodbe so bile obnovljene in svet se je vsaj za silo znova postavil v red, šibak a vendar. Tretja preizkušnja, ki je bila izstop Velike Britanije iz EU oziroma brexit, ki se je pravno zgodil 31. januarja 2020,

praktično pa že prej, se je nazadnje izkazala za daleč najlažjo preizkušnjo za EU. Zdaj bi že celo lahko rekli, da so vsaj gospodarske posledice takšne, da brexit lahko precej bolj obžalujejo otočani, kot pa tisti, ki smo v EU ostali. O tem ne pričajo samo zgodbe o hudem pomanjkanju „poljskih vodovodarjev“, voznikov tovornjakov in medicinskega osebja iz vzhodne Evrope, ampak še bolj dejstvo, da medtem, ko Velika Britanija gospodarsko izgublja, sosednja Irska pridobiva in se krepi, ker ostaja v EU in ima evro. Če bi se ta trend še okrepil, bo to lahko imelo neposreden vpliv na odločitev Škotov na prihodnjem referendumu za izstop iz Združenega kraljestva in posledično njihovo zaprosilo za vstop v EU. Kakorkoli se bodo stvari razvile, pa je že danes jasno vsaj to, da so težave Velike Britanije po brexitu neprimerno večje od težav, ki jih imamo zaradi brexita danes v EU.

Za EU pa bo ključno, da ob vseh reformah ostane odprta in svobodna zveza držav, ki o ključnih političnih in varnostnih rečeh odloča s kvalificirano večino, upravlja pa se kot delniška družba, na podlagi sorazmerja vloženih deležev. Sliši se preprosto, a je strahotno težko izvedljivo. A če bo volja, bo tudi pot.

Pred nami se medtem že povsem jasno oblikuje čas četrte hude preizkušnje za EU, ki bo oblikovanje novih zavezništev med državami znotraj EU in se bo odločalo o tem, kdo bo vstopil v skupino držav, ki se bo zavezala za še bolj povezano EU in kdo bo ostal v skupini Poljske in Madžarske, ki vztrajata, da ima EU že zdaj preveč moči nad članicami. Ta čas bo dobesedno padel na nas takoj po francoskih volitvah prihodnjo pomlad in v čas preoblikovanja evropskega Pakta za stabilnost in rast, ko se bo odločalo o gospodarski usodi držav in o prihodnosti skupnega trga. Hkrati bo to tudi čas, ko bo postalo jasno, kako se bo Francija razumela z Nemčijo brez Merklove, oziroma z novo nemško vladno koalicijo. Nemčija utegne imeti v prihodnje bistveno manj razumevanja za politične provokacije, s katerimi Poljska in Madžarska preizkušata trdnost Bruslja in enotnost EU. Še več, to bo čas, ko se bodo pričeli kazati prvi rezultati državnih politik tistih vzhodnih članic EU, ki so zaradi svojih političnih izbir na kocko postavile tudi svoj gospodarski položaj znotraj EU.

Ena od bolj pomenljivih aktivnosti je aktualno dogovarjanje Francije in Italije o strateškem zavezništvu, ki mu opazovalci rečejo «kvirinalska pogodba“ in zajema celo vrsto konkretnih pobud na področjih, ki so za mediteranski državi še posebej pomembna in pri katerih želita skupno nastopiti do nove vlade v Berlinu. Nova nemška vlada naj bi se po napovedih bolj posvetila gospodarskim in okoljskim vprašanjem sveta, manj zanimanja pa bo izkazovala do Mediterana in Balkana. V pri-

meru zmage Macrona na francoskih volitvah bo nova naveza Berlin, Pariz in Rim poseben poudarek dala prav temam, ki so bile doslej ob strani zaradi interesov Velike Britanije, ki pa je v EU ni več. Angleži so bili zadnja leta vselej tisti, ki so prvi zavirali vse pobude za večjo učinkovitost EU in bili s tem zavezniki vzhodno evropskih članic, v prvi vrsti Poljske in Madžarske. Gre za teme, ki utegnejo EU de facto razdeliti na zahodno in vzhodno, oziroma na EU prve in druge hitrosti;

- priprava reforme EU v smislu večje povezanosti;
- poenostavitev odločanja znotraj EU in širitev področij, kjer se odloča z večino glasov namesto s soglasjem;
- zaostritev pravil glede spoštovanja pravne države in evropskih norm in pravil, ter jasnejše finančne in druge sankcije do kršiteljev.

S tem bodo vse ostale članice, slej ko prej, postavljene pred jasne izbire. Odsotnost Velike Britanije je na stežaj odprla vrata možnosti, da se EU temeljiteje preobrazi in postane politično in gospodarsko še bolj povezana kot doslej. Države, ki bodo pri reformah sodelovale in jih sprejemale, zagotovo bo to velika večina zahodnih članic, bodo ohranile mesto pri mizi odločevalcev. Nekdanji poljski zunanji minister Radek Sikorski je bil glede tega zelo jasen; če nisi pri mizi si lahko na jedilniku!

Vzhodne članice bodo glede na dosedanja stališča do reform EU imele s tem kar nekaj težav, posebej države, ki jim suverenost pomeni več kot evropski združevalni projekt. Nekoč je to bila celotna Višegrajska skupina, zadnja leta sta to le še Poljska in Madžarska. Obe vidita nevarnost pred preveliko močjo Nemčije, bojita se nove nemške imperialne prevlade nad Evropo. A v resnici so ti časi mimo, strah pa je utemeljen le deloma; prvič zato, ker Nemčija brez EU ni konkurenčna ne ZDA ne Kitajski in je v njenem interesu, da EU obstane in se razvija, drugič pa zato, ker za ravnotežje moči skrbi Francija, po novem v zavezništvu z Italijo, kot tudi vsemi ostalimi članicami.

Slovenija pri vsem skupaj ne bo imela težke izbire, dovolj bo ravnati po zdravi pameti ter čim manj politično ali bog ne daj ideološko. Nemčija je že stoletje in pol naš prvi gospodarski partner in smo ena od vsega štirih članic EU, ki ima z njo presežek v menjavi. Italija pa je ves ta čas naš drugi gospodarski partner. Izkušnja našega zdaj že 17 letnega bivanja v EU nam dokazuje, da v teh letih niti malo niso bile ogrožene ne naša narodna zavest, ne naša kulturna ali verska identiteta in še najmanj naša varnost, prej obratno. Sta pa bila močno okrepljena naš jezik in naša samozavest, o čemer pričajo naši dosežki na vseh področjih, od gospodarstva, znanosti in kulture, do športa. Slovenija po svoji zgodovini, kulturi, tradicijah in tudi po običajih, predvsem pa po gospodarski umeščenosti pripada zahodu. In še bolj kot v srednje evropski, sodimo v alpsko-jadranski prostor, v katerem uživamo bogastvo sožitja z gorami in morjem.

Za EU pa bo ključno, da ob vseh reformah ostane odprta in svobodna zveza držav, ki o ključnih političnih in varnostnih rečeh odloča s kvalificirano večino, upravlja pa se kot delniška družba, na podlagi sorazmerja vloženih deležev. Sliši se preprosto, a je strahotno težko izvedljivo. A če bo volja, bo tudi pot. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Matic Naglič, vodja Službe za korporativno varnost skupine HSE*

KORPORATIVNA VARNOST V KRIZNIH RAZMERAH POMEMBNO ORODJE ZA UPRAVLJANJE SITUACIJE

Izzivi varnostnega okolja kažejo na dejstvo, da je ustrezno delovanje korporativne varnosti v organizaciji nujen predpogoj za zagotavljanje učinkovitosti in neprekinjenosti delovanja. O izzivih, ki jih je prineslo obdobje epidemije, smo se pogovarjali z g. Maticem Nagličem.

Obdobje epidemije COVID-19 je močno vplivalo na vse segmente naše družbe. Glede na to, da smo že močno zakorakali v drugo leto življenja s tem tveganjem, me zanima kakšne so vaše izkušnje pri zagotavljanju procesov varnosti v HSE?

V družbi Holding Slovenske elektrarne d.o.o., kot obvladujoča družba skupine HSE, smo se zaradi svojega poslanstva neprekinjenega obratovanja in proizvodnje električne ter toplotne energije za celotno Slovenijo zavedali nevarnosti izbruha in širjenja novega koronavirusa, saj smo že pred samim pojavom suma okužbe znotraj države spremljali in analizirali dogajanja po svetu. Glede na informacije in dogodke smo se odločili, da začnemo z vsemi aktivnostmi za zaščito zaposlenih in delovnih procesov proizvodnje električne in toplotne energije. Ob prvi javni informaciji februarja 2020, da obstaja sum okužbe znotraj Slovenije, smo zaposlene seznanili in v ravnanje posredovali več preventivnih in zaščitnih ukrepov za preprečitev širjenja virusa, ter sprejeli še določene varnostne oz. zaščitne ukrepe in naloge za zmanjšanje tveganja pred okužbo, vse z namenom zagotavljanja nemotene proizvodnje električne in toplotne energije na eni, ter zaščite sodelavk in sodelavcev na drugi strani. Vse poslovne procese družb smo uspeli organizirati tako, da so potekali razmeram primerno, a nemoteno.

Elektro energetsko področje je ključno pri zagotavljanju neprekinjenega delovanja družbe. Kako ste se v podjetju lotili zagotavljanja neprekinjenosti delovanja ključnega kadra brez katerega nekateri procesi in infrastruktura težko deluje?

Delovanje vseh elektroenergetskih sistemov je zahtevno, zato je bistvenega pomena, da imamo v skupini HSE definirane ključne kadre, ki so jih v kriznih ali drugih, nevsakdanjih situacijah, sposobni upravljati in vzdrževati. V skupini HSE ključni kader opravlja nujna dela, med katera sodijo, redno vzdrževanje proizvodnih objektov ter proizvodnja električne

> Varnostna tveganja so bila izziv, saj smo se v skupini HSE prvič soočali s situacijo, ko bi lahko bila zaradi širitve virusa med zaposlenimi ogrožena proizvodnja električne in toplotne energije. V tej krizi se je izkazalo, da nič ni več samoumevno, saj smo se bili primorani znajti sami.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Delovanje družb skupine HSE je v veliki meri odvisno od tehnologije in informacijskih storitev, zato je zagotavljanje ustreznega nivoja informacijske oz. kibernetske zaščite večni izziv, s katerim se bomo spoprijemali v prihodnosti.

in toplotne energije. Center vodenja pa skrbi za optimalno in kakovostno vodenje proizvodnje električne energije ter upravlja obratovanja vseh, v skupino vključenih elektrarn, s ciljem zagotavljanja zanesljivega in optimalnega obratovanja proizvodnih objektov skupine HSE. Za preprečitev potencialnih vnosov okužb v delovno okolje ključnega kadra v družbah skupine HSE, smo poleg preventivnih zaščitnih ukrepov zagotovili tudi nadomestne, rezervne centre vodenja in vzpostavili delovanje rezervne lokacije za potrebe Sektorja prodaje in trženja HSE, katerih ekipe so se izmenjevale brez neposrednih stikov. Prav tako smo omejili vstop in gibanje v območja pomembnih lokacij samo na zaposlene, ki opravljajo delovne naloge ter tako poskušali preprečiti oz. omejiti fizični stik z ostalimi zaposlenimi.

So se v tem obdobju pojavila kakšna posebna varnostna tveganja na katere bi morali biti pozorni tudi drugi kolegi na področju korporativne varnosti?

Varnostna tveganja so bila izziv, saj smo se v skupini HSE prvič soočali s situacijo, ko bi lahko bila zaradi širitve virusa med zaposlenimi ogrožena proizvodnja električne in toplotne energije. V tej krizi se je izkazalo, da nič ni več samoumevno, saj smo se bili primorani znajti sami. Organizirali smo se tako, da smo se še tesneje povezali s pristojnimi državnimi organi oz. službami in drugimi družbami s področja elektroenergetike, ter tako zagotavljali neprekinjeno delovanje elektrarn in proizvodnjo električne ter toplotne energije. Od začetka pojava novega koronavirusa in kljub zaostrenim ukrepom, nam je uspelo izvesti vse prej dogovorjene remonte oz. revizije proizvodnih objektov s tujimi izvajalci, prav tako smo uspeli zagotavljati vse potrebne surovine, ki jih potrebujemo v procesih pridobivanja električne energije. Ob tem smo se zavedali, da je sodelovanje med ključnimi dejavniki bistveno, saj neprekinjeno poslovanje družbe skupine HSE ni odvisno samo od lastnih virov, ampak tudi od vseh zunanjih sodelujočih izvajalcev oz. partnerjev, s katerimi sodelujemo, zato smo bili z njimi tudi ves čas v navezi in spremljali njihovo razpoložljivost.

Navsezadnje pa varnostno tveganje vsekakor predstavljamo zaposleni, saj je dolgo trajajoča situacija pustila spremembo tudi pri vseh nas. Zato je bilo pomembno, da smo za ohranitev pozitivnega vzdušja v skupini, zaposlene redno in pravočasno obveščali o novicah in ukrepih, ki so se sprejemali na nivoju skupine HSE. Izkazalo se je, da je človek, kljub novim tehnologijam, še vedno ključen del vsakega delujočega sistema.

Smo v polni meri uvajanja digitalizacije v naše procese. S tem kibernetska varnost dobiva še na večjem pomenu. Kako na področju zagotavljanja korporativne varnosti v HSE razvijate ta segment povezan s kibernetsko varnostjo?

Tudi v skupini HSE se zavedamo nevarnosti, ki jih prinaša digitalizacija procesov, zato smo že pred časom pristopili k dvigovanju nivoja zagotavljanja informacijske varnosti. Oddelek za informacijsko varnost skupine HSE poleg osnovnega poslanstva skrbi za ozaveščanje zaposlenih z izobraževanjem, redno se izvajajo pregledi stanja informacijske varnosti, ugotavljanje pomanjkljivosti in odprava le-teh v obstoječih sistemih, hkrati pa sproti uvajamo novosti s področja zaščite informacijske oz. kibernetske varnosti. Na nivoju skupine HSE pa se v sodelovanju z ostalimi službami dnevno operativno izvajajo vsi sprejeti ukrepi za preprečevanje vdorov.

Je razumevanje strateškega vodstva do potreb korporativne varnosti dovolj izraženo, da vam to omogoča uvajanje novih tehnoloških rešitev za dvigovanje nivoja varnosti v podjetju?

Vodstvo vseh družb skupine HSE podpira naše aktivnosti ter ima razumevanje za uvajanje novih tehnološko naprednih tehnologij, ki povečujejo nivo varnosti v posamezni družbi in skupini HSE, ter zagotavljajo večjo odpornost pred dejavniki, ki bi z namernim poškodovanjem in/ali uničenjem vplivali na nemoten proces proizvodnje električne in toplotne energije.

Varnostno zavedanje zaposlenih je v vsaki organizaciji eden od ključnih dejavnikov, ki loči uspešne organizacije od tistih z veliko varnostnimi problemi. Kako v HSE

pristopate do zaposlenih in zagotavljate njihovo pravilno dojemanje pomena varnosti?

V skupini HSE se zavedamo, da so zaposleni ključni za izvajanje vseh delovnih procesov pri zagotavljanju neprekinjene proizvodnje električne in toplotne energije. Ključno je torej vlaganje v izobraževanje; le tako so zaposleni lojalni in prispevajo k njenemu uspehu. K temu pripomore tudi redno ozaveščanje o pomenu zavedanja varnosti v delovnem okolju, saj se na takšen način varnostna tveganja med zaposlenimi zmanjšujejo.

Ste se v vaši organizaciji že začeli ukvarjati z razumevanjem hibridnih groženj, med katerimi je širjenje lažnih novic izredno izpostavljen dejavnik. HSE je bil skozi analizo obdobja 10 let že večkrat načrtna tarča takega delovanja. Se s strateškim vodstvom pogovarjate in analizirate tudi tovrstne varnostne dejavnike?

Skupina HSE se zaveda ugleda v družbi v kateri deluje, zato dnevno spremljamo vse novice, povezane z našimi družbami. V poplavi vseh novic poskušamo kar najbolj hitro odreagirati v primeru lažnih oz. škodljivih, neresničnih novic. Zavedamo se, da vsaka lažna novica kvari ugled HSE in lahko vpliva tudi na poslovanje same družbe, ki deluje tudi izven meja Republike Slovenije. Tudi naše vodstvo se zaveda pomembnosti hibridnih groženj in jim namenja ustrezno pozornost.

Kje v prihodnosti na varnostnem področju pričakujete največje izzive, katerim bo potrebno posvetiti posebno pozornost?

Delovanje družb skupine HSE je v veliki meri odvisno od tehnologije in informacijskih storitev, zato je zagotavljanje ustreznega nivoja informacijske oz. kibernetske zaščite večni izziv, s katerim se bomo spoprijemali v prihodnosti. Zavedamo se, da smo ranljivi pred napadalci, ki poskušajo vdreti v naše omrežje in najti očitne pomanjkljivosti. Zato je nenehno izobraževanje zaposlenih eden najboljših in bistven način obrambe, poleg vseh rednih varnostnih popravkov, ki se nameščajo na omrežje.

Največji izzivi pa se nam v prihodnosti predstavljajo na kadrovskem področju. Korona virus je spremenil vse nas, naš način življenja, razmišljanja in obnašanja. Vsi smo bili posredno ali neposredno udeleženi v procesu »preoblikovanja«, zato si upam trditi, da je edina gotovost v teh časih negotovost, saj se je izkazalo, da se je v vseh nas naselil strah pred vsem in vsakomur, zato sem mnenja, da bo potrebno z raznimi izobraževanji odpraviti ta strah. Odgovor na to je, da stroka mora prevzeti pobudo in odpraviti oz. povrniti ljudem zaupanje, na nas samih pa je, da smo pripravljeni na spremembe. Zato ni vprašanje, ali bomo preživeli pandemijo - kajti vem, da jo bomo, ampak vprašanje pa je kakšne bodo posledice in kako se bomo odzivali na prihodnje izzive, ki nas čakajo. ■

Foto: Aleš Lamot, Slobodan Mrkonjic

Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

www.ics-institut.si

Članstvo v združenju vam lahko olajša obvladovanje tveganj v vaših organizacijskih sredinah. SKUPAJ SMO MOČNEJŠI!

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

www.ics-institut.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
Rajko Novak, direktor, Smart Com

KORPORATIVNA VARNOST NUJNI POGOJ DELOVANJA MODERNIH ORGANIZACIJ

Razumevanje pomena kibernetske varnosti je postala neločljiva stalnica za uspešno delovanje naših organizacij. Še posebej je to zavedanje potrebno uvajati v organizacije, ki upravljajo s kritično infrastrukturo ali izvajajo bistvene, za družbo pomembne storitve. O priložnostih, ki jih prinašajo novi izzivi na področju kibernetske varnosti, smo se pogovarjali z g. Rajkom Novakom, direktorjem podjetja Smart Com.

Pospešeni procesi digitalizacije in drugi tehnološki razvojni procesi, kibernetsko varnost postavljajo na vedno bolj pomembno mesto. Imate občutek, da smo v Sloveniji že dojeli pomen kibernetske varnosti in ji na vseh nivojih namenjamo dovolj pozornosti ?

Na osnovi izkušenj, ki jih je Smart Com pridobil z izvedbo številnih varnostnih pregledov IT in procesnih (OT) okolij, opravljenimi forenzičnimi analizami v primerih dejanskih varnostnih incidentov in izvedenih varnostnih projektih, ter zagotavljanja storitev obratovanja končnim naročnikom na teh področjih, lahko dokaj dobro ocenimo nivo zavedanja o pomembnosti kibernetske varnosti v slovenskih podjetjih. Menim, da se danes večina slovenskih podjetij do neke mere zaveda pomena kibernetske varnosti svojega poslovnega okolja.

Menim, da je ključ do uspeha v sodelovanju gospodarstva, države in izobraževalnega sistema. Le skupaj lahko pridemo do večjega nabora mladih, ki bodo zainteresirani za študij in kasneje za delo na področju kibernetske varnosti.

Vendar še prevečkrat naletimo na razmišljanje poslovodstva, da je njihovo informacijsko okolje dovolj varno in, da se njim ne more zgoditi varnostni incident ali, da bi postali tarča hekerjev. A ravno poslovodstvo je tisto, ki je v organizacijah odgovorno za zagotavljanje ustreznega nivoja kibernetske varnosti in ne zaposleni v IT oddelku.

Naj omenim še en vidik kibernetske varnosti, ki postaja vse pomembnejši, in to je varnost OT okolij oz. procesnih sistemov v industrijskih okoljih in kritični infrastrukturi, kjer do pred kratkim vlaganja v kibernetsko varnost niso bila prav pogosta, saj so bila ta okolja ločena od poslovnih IT okolij. Prav digitalizacija je povzročila odpiranje ter povezovanje teh sistemov navzven, s tem pa so postali privlačna tarča za napadalce.

Kibernetska varnost tako postaja temelj vsake sodobne organizacije in zanemarjanje tega področja ima lahko hude negativne posledice na poslovanje.

Kot ste sami izpostavili, zagotavljanje ustreznega kadrovskega potenciala na področju zagotavljanja kibernetske varnosti predstavlja vedno večji izziv. Katerim korakom v procesu pridobivanja tega kritičnega kadra bi veljalo posvetiti posebno pozornost?

Za nas kot ponudnika varnostnih rešitev in storitev je ta vidik izrednega pomena in mu tako posvečamo veliko pozornosti.

*avtorica je članica Slovenskega združenja korporativne varnosti

Zavedamo se, da so potrebe po kadru s kompetencami na področju kibernetske varnosti velike, kadra na trgu pa je malo oz. ga ni. V Smart Comu preko različnih projektov in aktivnosti, ki naslavljajo tiste, ki so še v procesu izobraževanja, identificiramo tiste posameznike, za katere menimo, da jih vodijo iste vrednote in bodo obogatili našo ekipo z vedoželjnostjo ter z željo po doprinosu k dvigovanju nivoja kibernetske varnosti v okolju.

Področje kibernetske varnosti se nenehno spreminja in nadgrajuje, zato je potrebno konstantno spremljati in nadgrajevati znanja. Za podjetja, ki se dnevno ne posvečajo kadrom s področja kibernetske varnosti, je težka naloga – kako poiskati, pridobiti v svoje okolje kader in ga potem tudi uspešno razvijati in zadržati. Rešitev te dileme je zagotovo, da se vzpostavitev in upravljanje kibernetske varnosti zaupa podjetju oz. partnerju, ki je specialist na tem področju. S tem podjetje pridobi specializiran tehnični kader, ki spremlja in pravočasno zazna nevarnosti, se takoj odzove na morebitne incidente, izvaja forenzične analize in remediacijo.

Kako v Sloveniji izoblikovati izobraževalni sistem, ki bi ponujal večji kadrovski bazen na področju kibernetske varnosti, ki bo sposoben z manjšimi prilagoditvami zadovoljevati potrebe na celem nizu informacijskih področij?

Sistema se seveda ne da spremeniti čez noč. Je pa potrebno pričeti z uvajanjem sprememb takoj in to z novimi izobraževalnimi vsebinami že v osnovnih šolah (ne samo na fakultetah in srednjih šolah). Menim, da je ključ do uspeha v sodelovanju gospodarstva, države in izobraževalnega sistema. Le skupaj

> Potreben je strateški pristop pri obvladovanju vseh varnostnih tveganj. To je proces, ki se začne na strateški ravni in ga je potrebno skrbno načrtovati.

lahko pridemo do večjega nabora mladih, ki bodo zainteresirani za študij in kasneje za delo na področju kibernetske varnosti. Podjetja, ki delujemo na tem področju, lahko k temu veliko prispevamo. Na primer s praksami in mentorstvom, štipendijami, zanimivimi dogodki ter predavanji iz prakse.

Če smo že začeli razumevati pomen kibernetske varnosti v okoljih poslovne informatike, nam področje operativnih informacijskih tehnologij pri razumevanju resnosti tega področja še vedno predstavlja določen problem. Kje vidite glavne probleme pri dvigovanju varnostnega zavedanja, da je informacijska varnost v operativnih okoljih izrednega pomena?

Tako je, ko govorimo o poslovanju podjetij v kritični infrastrukturi ali industriji oz. proizvodnih podjetjih, kjer se običajno nahaja OT okolje oz. okolje operativne tehnologije, je ključnega pomena zagotavljanje razpoložljivosti in neprekinjenega poslovanja. V preteklosti so podjetja enostavno ločila IT in OT okolje, s prihodom IoT in digitalizacije v okviru industrije 4.0, pa je to nemogoče. Marsikdaj se ob združitvi teh dveh okolij, brez ustreznih varnostnih načrtovanj, hekerjem nevede na široko odpre vrata v najbolj kritična okolja. Zato potreba po kibernetski varnosti v OT okoljih eksponentno narašča.

Potreben je strateški pristop pri obvladovanju vseh varnostnih tveganj. To je proces, ki se začne na strateški ravni in ga je potrebno skrbno načrtovati. Ključen je tudi strokovni kader, saj klasični IT kader ne pozna specifik procesnih sistemov in okolij, zaposleni, ki skrbijo za OT okolja, pa nimajo znanj in kompetenc o kibernetsko varnostnih sistemih, saj tega do sedaj niso potrebovali. Prav zato smo v Smart Comu zasnovali izobraževanje za naročnike, ki združuje oba vidika in preko prenosa izkušenj v obliki predavanj in praktičnih primerov z laboratorijskimi vajami prinaša napredno poznavanje specifičnih protokolov, varnostnih ranljivosti, delovanja naprav, načrtovanja in povezovanja IT in OT omrežij, s poudarkom na kibernetski varnosti.

Kje na tem kompleksnem področju informacijskih tehnologij OT okolja vidite največje varnostne izzive?

Različne študije analitskih hiš potrjujejo, da se je število kibernetskih napadov na OT okolja v zadnjih dveh letih drastično povečalo in tudi uspešnost napadov je večja. Varnost v OT okoljih za približno 5 do 10 let zaostaja za varnostjo v IT okoljih, kjer se je zavedanje o varnosti skozi zadnja leta zelo krepilo in je na višjem nivoju. V OT okoljih te potrebe do sedaj ni bilo, saj so bili to izolirani sistemi, zato moramo začeti na vrhu organizacije, pri poslovodstvu, ki mora razumeti in s konkretnimi potezami podpreti pomembnost zavedanja o kibernetski varnosti.

Druga stvar, na katero želim opozoriti je, da težko varuješ informacijsko strukturo, če ne veš povsem, kaj vse imaš v njej. Globlje poznavanje informacijskega sistema z vidika varnostne ogroženosti je nujno potrebno. To lahko relativno hitro in enostavno dosežemo z izvedbo varnostnega pregleda OT okolja. Naslednja zadeva, ki je s tem povezana je ozaveščanje zaposlenih o pomembnosti kibernetske varnosti. Neozaveščeni uporabniki so največje varnostno tveganje, zato je njihovo izobraževanje o potencialnih nevarnostih ob uporabi informacijskih tehnologij izrednega pomena.

S tehničnega vidika naj izpostavim še dve pomembni, ampak osnovni varnostni pomanjkljivosti, na kateri se morajo podjetja najprej osredotočiti. In sicer velikokrat omrežja v industrijskih okoljih in okoljih kritične infrastrukture niso dovolj segmentirana, kar pomeni, da, če heker pridobi vstop v delovno postajo ali računalnik zaposlenega v podjetju, od tam lahko enostavno dostopa do drugih delov proizvodnje. Druga pa je, da v teh sistemih še vedno najdemo veliko starejših operacijskih sistemov (npr. Windows XP), za katere varnostni popravki niso več na voljo in bi morala podjetja čimprej poiskati alternativne rešitve.

Menite, da je v slovenskem prostoru dovolj priložnosti za sodelovanje na področju kibernetske varnosti, ki bi omogočale resneje nastopati tudi v širšem mednarodnem poslovnem okolju?

S krepitvijo sodelovanja lahko prenašamo znanje in dosežemo cilje, ki jih drugače ne bi. Zato je najprej potrebno vzpostaviti dialog in okrepiti zaupanje vseh deležnikov, tako iz zasebnega, kot javnega sektorja. Imamo že nekaj primerov dobrih praks, na primer na Ministrstvu za javno upravo, kjer smo se podjetja povezala, da smo lahko ponudila ustrezno rešitev na nivoju države. Sodelovanje je nujno potrebno, saj podjetja iz stroke sledimo dogajanju in smo vedno v koraku z najnovejšimi trendi, s tehnološkim napredkom in najsodobnejšimi rešitvami, ki jih lahko implementiramo in tako poskrbimo za dvig kibernetske zaščite.

Kakor koli pogledamo je Slovenija majhna in le s povezovanjem strokovnjakov bomo lahko reševali izzive, ki jih imamo. Izkoriščanje vseh priložnosti za sodelovanje in skupen nastop je pomemben že na slovenskem trgu, še toliko bolj pa to velja za širše mednarodno poslovno okolje.

Kakšna je vaša strategija pri vključevanju v raziskovalno-razvojne mednarodne projekte. Menite, da je to lahko dodaten potisk pri razvoju tehnologij in storitev na področju kibernetske varnosti v vašem podjetju?

Na področju raziskav in razvoja v Smart Comu že vrsto let delujemo sistematično. Imamo močno razvojno ekipo, ki se vključuje v mednarodne razvojne projekte. Osrednje vodilo pri izbiri projektov in partnerstev je, da se rezultati raziskav in razvoja v končni fazi v čim večji meri prenesejo v prakso. Projekti so odlična priložnost, da s pomočjo mednarodnih konzorcijev nadgradimo ter razvijemo znanja in kompetence, ki so strateškega pomena v prihodnje, tako za nas kot ponudnika, kot tudi za naše naročnike.

Menite, da je vaša vključitev v okvir Slovenskega združenja korporativne varnosti za vas prinesla dodatno kvaliteto na področju izmenjave dobrih praks in izkušenj?

Vsako povezovanje zagotovo prinese nove poglede, nova strokovna in poslovna poznanstva s podobnega področja, a z drugačnim pogledom, saj se vsak od članov združenja osredotoča na lastno področje odličnosti. Povezujemo se s potencialnimi naročniki, spoznamo njihove specifične izzive in pričakovanja, na osnovi katerih oblikujemo in ponudimo kvalitetno storitev, ki je podkrepljena z izkušnjami in poglobljenim poznavanjem problematike. ■

Foto: Aleš Rosa

Okrepite varnost

21. - 24. marec 2022

4-dnevni tečaj

KIBERNETSKA VARNOST ICS/OT/IoT OKOLIJ

Kibernetski napadi na kritično infrastrukturo predstavljajo 5. največje globalno tveganje.

V obdobju enega leta od 2019 do 2020 so hekerski napadi porasli za kar 485 %.

Spoznajte, kako učinkovito vzpostaviti zaščito pred zlorabami in hekerskimi napadi za zagotovitev neprekinjenega delovanja industrijskih okolij in kritične infrastrukture.

Skenirajte za prenos programa

https://bit.ly/program-OT

info@smart-com.si

01 561 16 06

SMART COM

Zanesljiv, tehnološko napreden partner za kibernetsko varnost, informacijsko-komunikacijska omrežja in podatkovne centre.

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

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

INTERVJU
Aleksandar Todorovski, direktor podjetja Ericsson d.o.o.

CELOVITO UVAJANJE TEHNOLOGIJ 5G PRED NAS POSTAVLJA POMEMBNE IZZIVE

Kljub izzivom, ki jih je prineslo obdobje pandemije COVID-19, se postopek digitalizacije procesov v naši družbi nadaljuje s pomembno časovno dinamiko. V tem okviru ima ravno uvajanje tehnologij 5G posebno pomembno mesto. O izzivih in priložnostih smo se pogovarjali z g. Aleksandrom Todorovskim.

Ste eni od vodilnih tehnoloških podjetij v hitro spreminjajočem se okolju. Ali nam lahko kaj več poveste o vaših izkušnjah z uvajanjem 5G tehnologije? Kakšen je bil vaš pristop k širitvi 5G omrežja?

Prva komercialna 5G omrežja so se po svetu začela uvajati od leta 2019. Trenutno ima Ericsson 149 5G pogodb, od tega je 97 aktivnih komercialnih 5G omrežij v 46 državah. Te številke nam povejo, da se je uvajanje 5G v letih po 2019 samo pospešilo, kar smo priča tudi v Sloveniji, kjer trije največji operaterji že ponujajo komercialna omrežja, Telekom Slovenije pa je to kot prvi naredil že v letu 2020. Ericsson je globalno najprej sodeloval pri razvoju tehnologije v sklopu standardizacijskih teles kot 3GPP. Potem je aktivno sodeloval tudi z naprednimi operaterji v Švici, Južni Koreji, ZDA in Kitajski za implementacijo te tehnologije.

Če pogledamo malo v prihodnost so naša pričakovanja, da imamo do konca leta 2026 3.5 milijard 5G naročnin in, da bo okoli 50 procentov mobilnega podatkovnega prometa prek 5G omrežji.

5G predstavlja evolucijo obstoječih mobilnih tehnologij. Zgrajena je na osnovi že postavljene 4G tehnologije. Če jo razumemo kot evolucijo, bomo lažje razumeli tudi mite, ki nastajajo okoli 5G tehnologije.

Kako nam bo tehnologija 5G spremenila življenje?

5G je platforma, ki bo omogočala velike inovacije in je bila zasnovana tako, da je odprta od samega začetka. Prejšnje generacije so bile osredotočene na potrošniško in osebno komunikacijo. 5G bo služil potrošnikom in podjetjem ter bo na višjo raven povzdignil internet stvari, kjer je vrhunska povezljivost predpogoj. Verjamemo, da je tako močan, da bo v ozadju naslednjega velikega družbenega premika – 4. industrijske revolucije. Odgovoril bo praktično na vse digitalne potrebe sodobne družbe in industrije.

Kateri so po vašem mnenju največji miti, ki so povezani s 5G-tehnologijo?

5G predstavlja evolucijo obstoječih mobilnih tehnologij. Zgrajena je na osnovi že postavljene 4G tehnologije. Če jo razumemo kot evolucijo, bomo lažje ra-

*avtor je član Slovenskega združenja korporativne varnosti

zumeli tudi mite, ki nastajajo okoli 5G tehnologije. Ti miti so bili po mojem mnenju vezani na dve smeri:

Prvi mit je predvsem vezan na to, da bo 5G tehnologija takoj spremenila naše življenje, in da bo vklop te tehnologije takoj prinesel nekatere od bolj naprednih use-case-ov baziranih na ultra nizki latenci. Boste vprašali zakaj? Ker je to odvisno od več faktorjev (nekateri so vezani na dodelitev ustreznih frekvenc, nekaj jih je vezano na samo evolucijo tehnologije skozi čas, ker nekatere faze ni možno preskakovati). To bo gradualna evolucija glede možnosti te tehnologije.

Drugi mit je bil vezan na nekatere t.i. teorije zarote okoli potencialnega učinka te tehnologije, na zdravje, za kar pa ni nobenih validnih znanstvenih dokazov.

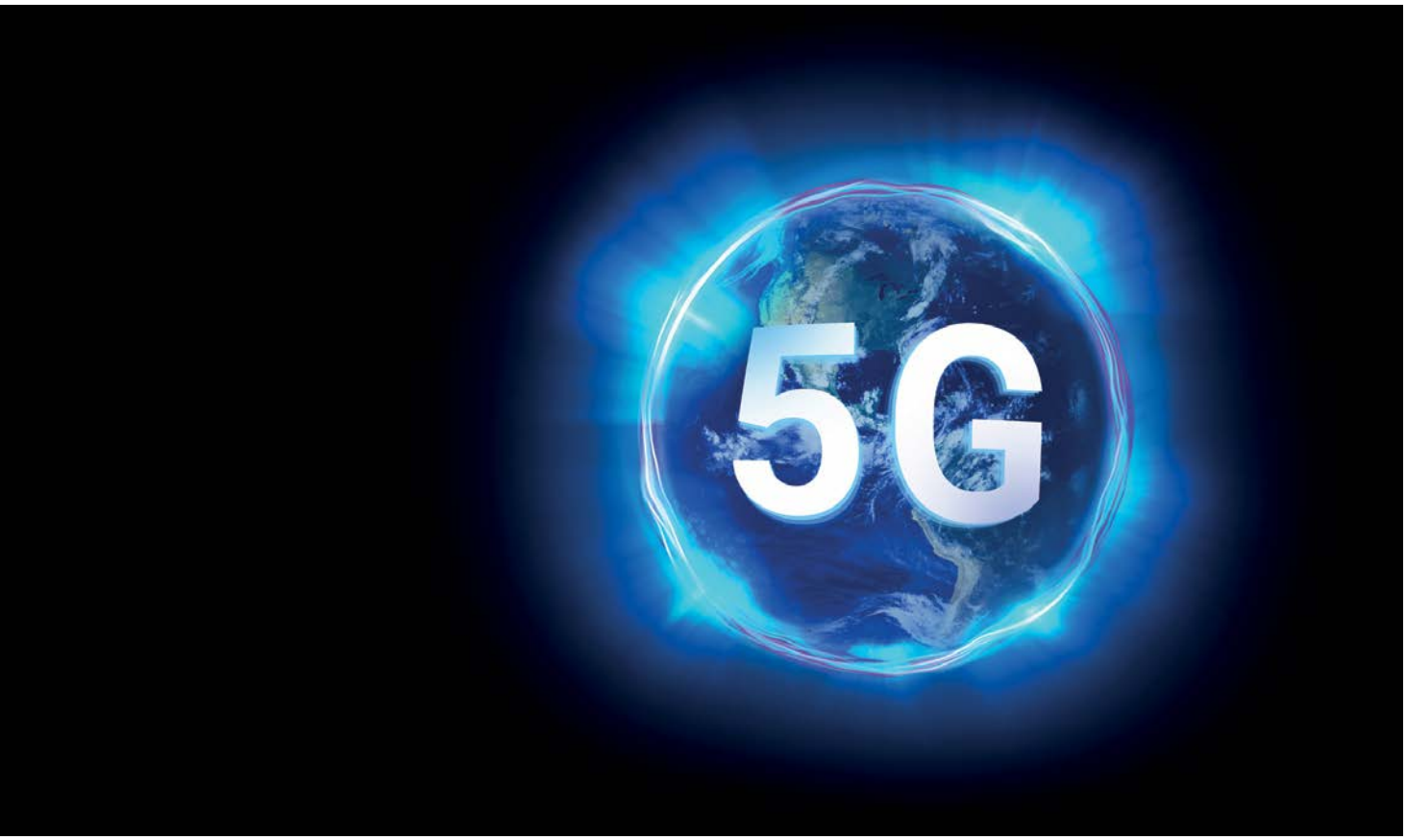
V zadnjem obdobju je glavna mednarodna tema kako razviti čim več tehnologij, ki bodo puščale manjši ogljični odtis. Ali lahko z uvedbo 5G omrežja zmanjšamo porabo energije v mobilnih omrežjih?

Prvič v zgodovini, zahvaljujoč pripravljenosti obstoječih omrežij, katera so bazirana na Ericsson opremi in so že pripravljena na 5G, nam uvedba naslednje mobilne generacije daje priložnost, da zmanjšamo podnebni odtis mobilnih omrežij. Prihranki, ki jih je mogoče doseči s pripravo omrežja z najnovejšimi tehnološkimi rešitvami, aktiviranjem programske opreme za varčevanje z energijo in natančno gradnjo 5G ter inteligentno obratovanje, bodo veliki. Vsaka prejšnja nova generacija mobilnih omrežij je povečala porabo energije in emisije ogljika, zato je ključnega pomena, da prekinemo energetsko krivuljo. 5G lahko s preoblikovanjem industrije omogoči 10-kratno zmanjšanje emisij ogljika, kot ga oddaja sam sektor IKT.

Kakšen je vaš pogled na 5G omrežja in kibernetsko varnost ter kakšen vpliv ima to na celotno družbo?

Tako kot predhodniki, bo tudi sistem 5G kmalu nepogrešljiv del naše povezane družbe. 5G bo omogočil različne primere uporabe, nekateri pa bodo zahvaljujoč 5G končno videli luč dneva. Ericsson meni, da 5G varnost zagotavlja raven zaupanja, ki omogoča, da sistem 5G izpolnjuje zahteve velike večine teh primerov uporabe od končnega uporabnika, ponudnika storitev in regulativnih vidikov. Zanesljivost ne izvira le iz sklopa varnostnih značilnosti, temveč tudi iz načel zasnove sistema, ki so bila vsa uporabljena s celovito in na tveganju temelječo miselnostjo.

Kje so tisti ključni dejavniki, ki jih želite kot eden izmed ponudnikov 5G izpostaviti na področju zagotavljanja kibernetske varnosti.



Kibernetska varnost končnega uporabnika v uvedenem omrežju 5G mora biti zagotovljena s štirih vidikov: tehnološki standardi, postopek razvoja ponudnika, postopek uvajanja in operativni postopek ponudnika storitev. Ta pristop odraža tudi zbirka orodij katero definira EU t.i. »EU Toolbox«.

Če začnemo od začetka, telekomunikacijski standardizacijski procesi bi skrbeli za razvoj varnih protokolov in algoritmov, kateri se uporabljajo. V tem procesu se operaterji in proizvajalci opreme strinjajo o tem, kako bodo omrežja po vsem svetu delovala skupaj in kako je mogoče omrežja in uporabnike zaščititi pred zlonamernimi akterji.

Potem govorimo o produktnem razvojnem procesu, ki je sestavljen od razvoja varnih strojnih in programskih komponent, varnih razvojnih procesih ter kontrolo strojnih verzij in varnih programskih izboljšav t.i. »update«. Proizvajalci opreme prevedejo dogovorjene standarde v funkcionalne omrežne elemente in sisteme. Zasnova in razvoj, ki ga izvaja omrežni dobavitelj, je ključni del s tem, da končni izdelek deluje in je varen.

Tretja raven pogleda na varnost 5G so procesi za uvajanje, konfiguracijo in robustnost omrežja. Pri tem je potrebno posebej upoštevati varnost, odpornost in konfiguracijo varnostnih parametrov v fazi uvajanja omrežja. Torej pomembno je zavedanje, da so omrežja zasnovana in konfigurirana za ciljno raven varnosti.

Operativni procesi – To so varne operativne procedure, nadzorovanje delovanja varnostnih funkcij, upravljanje s tveganji in ranljivostmi (vulnerability management) in odkrivanje napadov, odzivanje in obnova sistemov po vdoru. V operativni fazi so pomembni procesi, ki olajšajo in omogočajo ciljno raven varnosti in so zelo odvisni od uvajanja in delovanja omrežja.

Kakšne so vaše izkušnje v mednarodnem okolju, kako ustrezno izgraditi zaupanje med regulatorji, operaterji in ponudniki tehnologij 5G?

Standardiziran pristop je pomemben za doseganje globalne interoperabilnosti in izogibanje dodatnim stroškom. Ericsson aktivno prispeva k varnostnim standardom v organizacijah za standardizacijo, kot so 3GPP SA3, ETSI NFV / SEC in IETF. Trenutni predsednik 3GPP SA3 je predstavnik Ericssona.

Združenje GSMA je industrijska organizacija, ki zastopa interese operaterjev mobilnih omrežij po vsem svetu. Več kot 750 mobilnih operaterjev je polnopravnih članov GSMA, nadaljnjih 400 podjetij v širšem mobilnem ekosistemu pa pridruženih članov.

Podpiramo pristop kateri je opredeljen z GSMA NESAS in 3GPP SECAM / SCAS okvirom za ocenjevanje varnosti.

Kako bi ocenili stopnjo razvoja kibernetske varnosti v slovenskem okolju?

Ocenjujem, da se tudi v slovenski javnosti pospešeno razvija zavedanje glede kibernetskih groženj ter kako na njih pravočasno in uspešno odgovoriti. Kibernetska varnost mora biti prioriteta tako za kritično infrastrukturo kot za podjetja, ker lahko bistveno vpliva na njihovo funkcioniranje. Vsi deležniki v tem eko-sistemu preprečevanja kibernetskih groženj, to so državni organi, regulatorji, operaterji in proizvajalci opreme, bodo morali v prihodnosti sodelovati pri izvajanju EU strategije na področju kibernetske varnosti. V skladu z novo strategijo bo v prihajajočem obdobju fokus na uvajanju sklopa orodij EU za kibernetsko varnost 5G, celovitega in objektivnega pristopa na podlagi tveganj za varnost omrežij 5G in omrežij prihodnjih generacij. ■

Foto: arhiv Ericsson d.o.o.

Cyber Security Is What We Do

SmartIS

PAMETNI INFORMACIJSKI SISTEMI

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

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

FIZIČNO VAROVANJE ŠE VEDNO POMEMBEN SEGMENT ZAGOTAVLJANJA INTEGRALNE VARNOSTI

V dobi digitalizacije velikokrat pozabljamo, da je fizično varovanje in s tem zagotavljanje nemotenih dostopov do naših ključnih objektov in lokacij, še vedno osnovni temelj za zagotavljanje učinkovite integralne varnosti v naših organizacijah. O pomenu tega področja in o priložnostih, ki jih nove tehnologije na področju mehanskih sistemov zaklepanja prinašajo, na področju učinkovitega upravljanja z dostopnimi pravicami do naših ključnih objektov, smo se pogovarjali z g. Predragom Petrovičem, direktorjem podjetja ID Shop.

Obdobje epidemije je pred nas postavilo nove zahteve razumevanja prioritet, ki so pomembne za neprekinjeno delovanje naših organizacij. Katere so tiste prioritete, ki ste jih poudarili v vašem podjetju?

Izpostavil bi dve prioriteti, ki smo se jih in se jih še vedno držimo: zagotoviti varno delovno okolje, se pravi zaščititi zaposlene in vse, s katerimi s(m)o prihajali v stik, kakor tudi zagotavljati nemoteno servisno podporo našim partnerjem.

Na začetku tega negotovega obdobja, ko nihče ni točno vedel, kako se bo vse skupaj odvijalo, je bil naš prvi ukrep to, da smo se organizirali v dve skupini, ki sta se menjavali (delo na domu in v pisarni) z namenom, da se izognemo morebitnim množičnim okužbam zaposlenih.

Poleg zdravja zaposlenih je bilo najpomembneje ohraniti polno operativnost servisne ekipe z namenom, da našim partnerjem lahko izvršimo vse dogovorjene montaže ter zagotovimo vso podporo in storitve, v kolikor bi jih potrebovali. Zavedamo se namreč odgovornosti in svoje vloge pri zagotavljanju nemotenega delovanja na področju kontrole dostopa in zaklepanja, ne glede na to, ali naši partnerji spadajo v kritično infrastrukturo, šolstvo, zdravstvo, ali pa gre za industrijo ali druga podjetja. Videli smo, kako so delovni procesi na hitro postali precej bolj fleksibilni in to so morale podpreti in omogočiti tudi naše rešitve za kontrolo dostopa in zaklepanja prostorov.

Kljub hitremu razvoju in digitalizaciji velikega števila procesov, ki imajo pomemben učinek tudi na področje varnosti, pa si varnosti vendarle ne moremo v celoti zamišljati brez mehanskih sistemov, med katerimi so mehanski sistemi za zaklepanje, še vedno izredno pomembni. Kakšna je vaša percepcija tega stanja in potreb na varnostnem tržišču?

Ocenil bi, da je trenutno stanje takšno, da ima približno 30% podjetij urejene sisteme zaklepanja. V preostalih podjetjih sistemi niso poenoteni, niso patentno zaščiteni ali pa je podjetje že preraslo obstoječi sistem, zato ‚key management' več ni urejen in pregleden. Vse našteto pomeni večje varnostno tveganje za podjetje. Veliko podjetij podcenjuje mehanske sisteme zaklepanja in od njih slišimo, da imajo že urejeno elektronsko kontrolo dostopa, kartični pristop,

*avtorica je članica Slovenskega združenja korporativne varnosti

videonadzor ipd. Ko jih postavimo pred dejstvo, da lahko v njihovem primeru še vedno vsakdo, ki pride do ključa, kadarkoli vstopa v njihove prostore brez, da bi bilo to kje zabeleženo, šele takrat se začnejo zavedati, da je mehanika osnova za vse nadaljnje kontrole pristopa.

Kljub vsemu je pohvalno to, da se podjetja ozaveščajo o tem in posledično se tudi povečuje število sistemov zaklepanja. Veseli nas, ker opažamo, da prihaja do porasta povpraševanja po mehanskih sistemih zaklepanja, še pomembneje po patentiranih. To pomeni, da naše delo ni zaman. Pohvaliti pa moramo tudi konkurenčna podjetja, ki so prav tako aktivna in se vidi, da opravljajo enako nalogo kot mi, torej izobražujejo trg na tem področju.

V času pandemije je bil ravno človeški potencial najbolj na udaru. Zmanjšanje angažiranosti kadra, težje zagotavljanje zamenljivosti in potreba po čim manjšem številu kontaktov je bila na področju zagotavljanja servisiranja določenih dislociranih lokacij infrastrukturnih operaterjev zelo zahtevna. Kakšne so vaše izkušnje z uveljavljanjem digitalnega sistema zaklepanja z lastnim napajanjem za kritično infrastrukturo?

Uspeli smo se organizirati v več servisnih skupin, ki so se izmenjevale, da smo lahko nemoteno zagotavljali storitve servisa, odzivnost in zagotavljanje podpore 24/7. Veseli nas, da smo lahko večino dogovorjenih montaž nemoteno opravili, saj so se izvajale na zunanjih površinah in ne v poslovnih prostorih. Tiste, ki so se izvajale v notranjih prostorih, smo ob upoštevanju zaščitnih ukrepov prav tako izvedli po planu, saj je bilo tudi v tem primeru možno delati brez fizičnih stikov, oziroma smo se dogovorili, da so v času montaže prostori prazni, kar je bilo v tem obdobju relativno lahko.

Ena od izredno dobrih strani iLOQ digitalnega zaklepanja s katerim rešujemo problematiko kontrole pristopa podjetjem iz kritične infrastrukture je ta, da lahko večino stvari opravimo na daljavo. Tako smo lahko preko on-line sestankov pripravili sistem zaklepanja, namestitev programske opreme in vnos dostopnih pravic za različne skupine uporabnikov. Prednost iLOQ sistema je modularnost digitalnih cilindrov, zato predhodne izmere sploh niso bile potrebne, saj smo cilinder sestavili kar na lokaciji. Tudi sama montaža je enostavna, saj niso potrebne predelave vrat ali kakršnokoli kabliranje. Že pred montažo smo poskrbeli tudi za programiranje digitalnih cilindrov, tako, da smo na lokaciji dejansko samo namestili komponente in šli naprej.

Pritisk na zmanjševanje stroškov poslovanja je postala konstanta pri poslovanju organizacij. Kje so po vaši oceni še priložnosti, ki lahko z uvedbo novih tehnologij zmanjšajo stroške poslovanja in povečajo nivo varnosti pri vstopu v različne dislocirane enote naših organizacij?

Razvoj, inovacije in digitalizacija prinašajo novosti tudi na področju sistemov zaklepanja in kontrole pristopa. Velikokrat se novosti zdijo visoka investicija, vendar je pomembno upoštevati tudi druge operativne stroške (CAPEX, OPEX) in stroške celotnega življenjskega cikla sistema (TCO), na katere pa

pogosto pozabimo, a se ravno tukaj dela razlika. Priložnosti so torej v sistemih, ki odpravljajo stroške izdelave novih ključev in menjave cilindričnih vložkov ter v sistemih, katerih delovanje ni odvisno od vira napetosti in so minimalno zahtevni z vidika vzdrževanja in tudi samega upravljanja. Takšen primer je digitalni sistem zaklepanja iLOQ, ki temelji na lastnem napajanju in odklepanju z mobilnim telefonom ali z digitalnim ključem, komunikacija pa temelji na AES-256 bitnem šifriranju, kar zadostuje najzahtevnejšim kriterijem glede informacijske varnosti.

Definitivno je prihodnost v mobilnem odklepanju in možnosti pošiljanja posodobitev dostopnih pravic neposredno v mobilni telefon, ter v oddaljenem upravljanju sistema. Če vzamemo za primer organizacijo z velikim številom dislociranih enot, moramo pomisliti na stroške, ki nastanejo v primeru distribucije ključev na različne lokacije, stroški za spremstva zunanjih partnerjev na lokacijo, letni stroški vzdrževanja komponente, stroški samih baterij in menjave baterij na komponentah... Če imamo sistem kot iLOQ, ki omogoča oddaljeno in centralizirano upravljanje komponent, dostopnih pravic, časovnih profilov, pregleda revizijske sledi v realnem času in pošiljanje dostopnih pravic na mobilni telefon, potem lahko hitro izračunamo, da so OPEX stroški takšnega sistema minimalni v primerjavi s klasičnimi mehanskimi in elektronskimi sistemi zaklepanja. Obenem takšen sistem zmanjšuje varnostna tveganja v primeru nepooblaščene uporabe ali izgube ključa, saj je možno pravice v hipu blokirati. Varnost sistema zato nikoli ni posebej ogrožena in ostaja vsa leta na enakem nivoju, kar pri klasičnih mehanskih sistemih težko dosežemo. Vse to je tisto, kar na dolgi rok dela razliko in ustvarja dodano vrednost.

Smo ravno v obdobju kjer je zmanjševanje vpliva na okolje izrednega pomena. Kako pri vas dojemate ta pomemben izziv in kako ga zagotavljate pri svojih produktih?

Naše stranke so manjša ali večja podjetja in menim, da imamo največji vpliv prav preko njih – tako, da jim ponudimo trajnostno rešitev. Tudi s tega vidika bi izpostavil digitalno zaklepanje iLOQ, ki je trenutno naša ‚najbolj zelena' rešitev, ki jo strankam lahko ponudimo. Ne samo, da zmanjšuje baterijski in kovinski odpad, ker temelji na mobilnemu odklepanju in brez baterijskih komponentah, ampak tudi zmanjšuje vpliv na okolje, ki ga povzročijo službene poti zaradi distribucije ključev, vzdrževanja sistema ipd. Poleg tega govorimo o digitalnih ključih in cilindrih za večkratno uporabo, ko jih nekje ne potrebujemo več, jih lahko ponovno programiramo in uporabimo v drugem sistemu.

Kaj bi bilo po vašem mnenju še možno storiti za povečanje varnostnega zavedanja v pomembnih organizacijskih okoljih in boljše razumevanje prednosti, ki jih prinašajo nove tehnologije?

Že dolgo opažamo, da naša naloga ni zgolj prodaja in zagotavljanje storitev. Potrebno je tudi izobraževanje tržišča o novostih, dodanih vrednosti in prednosti tako mehanskih sistemov zaklepanja, kot tudi novejših digitalnih sistemov. Potrebe po zagotavljanju varnosti se namreč povečujejo, vendar kljub temu, da je trg dovolj razvit in ponudbe ne manjka, tržišče ni dovolj informirano o vseh rešitvah, ki so na voljo.

Pri strankah se velikokrat srečujemo z dvema poljema: en del je naklonjen spremembam, drugi del pa ne. Od njihove poslovne strategije je potem odvisno v katero smer se zadeve odvijajo. Toda prej ali slej bodo podjetja postavljena pred dejstvo, da je potrebno v tehnično varovanje vlagati in ga posodabljati, ker potrebe po zagotavljanju varnosti rastejo skupaj s podjetjem. Tako kot vse drugo, se tudi na tem področju trendi menjajo, tehnologija napreduje, zahteve postajajo vse kompleksnejše in sprejeli smo dejstvo, da je na nas naloga, da trg seznanimo z njimi.

Kaj vam v vašem podjetju pomeni partnerstvo, ki ga gojite z večletnim sodelovanjem na pomembnem mednarodnem dogodku Dnevi korporativne varnosti?

Na dogodku smo prisotni od leta 2015/2016. Že od samega začetka nam sodelovanje pomaga pri prepoznavnosti in sklepanju novih poznanstev, ter poglobitvi odnosov z obstoječimi strankami na varnostnem področju. Zaradi sodelovanja na Dnevih korporativne varnosti so nas začeli prepoznavati kot resnega igralca na trgu, pripomoglo je k naši kredibilnosti v očeh poslovnih partnerjev. Lahko rečem, da je konferenca v vseh teh letih vplivala tudi na poglobitev našega znanja o varnostni tematiki, pridobili pa smo tudi marsikatero koristno informacijo in znanje, da vidimo da gremo v pravo smer. Prav tako lahko izpostavim korektno sodelovanje Inštituta za korporativne varnostne študije za izkazan odnos do svojih partnerjev. Z njihovimi informacijami, znanjem in poznanstvi so nas uspeli povezati, oziroma odpreti marsikatera vrata, ne samo na področju Slovenije, ampak tudi na ex-YU trgu, kar nas zelo veseli. ■

Foto: arhiv ID Shop

Digitalno zaklepanje nove generacije

iLOQ je sinonim za najsodobnejšo digitalno kontrolo dostopa, ki nadomešča mehanske in elektronske sisteme zaklepanja z okolju prijaznimi, brezbaterijskimi in brezžičnimi komponentami.

Dovolj je en ključ ali mobitel na uporabnika!

iLOQ, prvi digitalni sistem zaklepanja na svetu brez baterijskega napajanja.

- Deluje brez baterij in brez kablov.
- Odklepanje z mobitelom (NFC tehnologija) ali z digitalnim ključem.
- Brez stroškov vzdrževanja in minimalnimi stroški življenjskega cikla sistema zaklepanja.
- Oddaljeno upravljanje preko iLOQ Manager programske opreme v oblaku.
- Revolucionarna rešitev, primerna tudi za zahtevna varnostna okolja (PKI in AES – 256 šifriranje).
- Zelena, trajnostna rešitev.

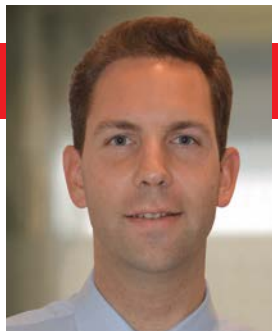
Prednosti uvedbe iLOQ digitalnega sistema zaklepanja

- **Hitro povračilo investicije (ROI) in nizki operativni stroški (OPEX)**; ni baterij, ni predelave vrat, ni potrebe po vzdrževanju sistema.
- **Preprečuje zlorabe sistema in varnostna tveganja**; revizijska sled in blokiranje dostopnih pravic v realnem času rešujejo problematiko nepooblaščene uporabe in izgubljenih ključev.
- **Okolju prijazna rešitev za podjetja, ki sledijo trajnostnemu razvoju;** minimalen vpliv na okolje; brez baterijskega odpada, upravljanje na daljavo in posledično manj potreb po vzdrževanju sistema in distribuciji ključev med lokacijami.
- Na voljo **digitalni cilindri, obešanke, polcilindri, pohištvene ključavnice, cilindri za zidne trezorje in čitalci**, ki jih je možno nadgraditi v kontrolo pristopa.

IDealni partner za identifikacijo in varnost

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

Avtor: dr. Andrej Bregar / Informatika d.o.o.*



PROGRAM UPRAVLJANJA KIBERNETSKE VARNOSTI – CELOVIT PRISTOP K IZBOLJŠANJU ODPORNOSTI ORGANIZACIJE

Zaradi razmaha kibernetskih tveganj in kriminala se organizacije ne soočajo več zgolj z vprašanjem, ali bodo napadene, temveč predvsem z vprašanjem, kdaj bodo napadene. Kibernetska in informacijska varnost tako postaja ključni dejavnik, ki ga mora vsaka organizacija vkomponirati v svoje delovanje in poslovanje.

Uvod

Poglavitni izzivi so zagotavljanje varnosti zaupnih informacij in virov, preprečevanje in hitro zaznavanje vdorov, učinkovito odpravljanje posledic vdorov ter omejevanje potencialne škode. Še posebej pomembno je varovati ključne atribute informacij – zaupnost, razpoložljivost in integriteto. To je možno v največji meri doseči z uvedbo učinkovitega in trajnega programa upravljanja kibernetske varnosti, ki zahteva dobro poznavanje podatkov in infrastrukture organizacije, kontrolnih mehanizmov ter zakonodajnih zahtev. Le na tej osnovi lahko zagotovimo visoko stopnjo zaščite. V širši družbi in v poslovnih okoljih, katerih obstoj in delovanje sta odvisna od informacijske tehnologije, tako postaja učinkovit program kibernetske varnosti pomemben integralni del poslovanja vsake organizacije, ne glede na njeno velikost. Takšen program omogoča prehod praks izvajanja kibernetske varnosti iz primarno tehnološkega nivoja, v strateški koncept, kar je pomembno v sodobnem svetu, ki sloni na digitalizaciji, informatizaciji, industriji 4.0 in vseprisotnosti na spletu, zaradi česar je potrebno med osnovne stebre kibernetske varnosti poleg tehnologije enakovredno povezovati tudi ljudi in procese.

Cilj programa kibernetske varnosti je, da vpelje formalen pristop k sistematičnemu in celovitemu upravljanju kibernetske varnosti, hkrati pa do njega vzpodbudi pozitiven odnos. Takšen program oblikujemo, uvedemo in izvajamo kot eno od poslovnih funkcij organizacije.

Kaj je program kibernetske varnosti?

Cilj programa kibernetske varnosti je, da vpelje formalen pristop k sistematičnemu in celovitemu upravljanju kibernetske varnosti, hkrati pa do njega vzpodbudi pozitiven odnos. Takšen program oblikujemo, uvedemo in izvajamo kot eno od poslovnih funkcij organizacije. Ima merljivo učinkovitost in sloni na standardnem

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

ogrodju, ki predstavlja dobro prakso, saj ga je možno konsistentno integrirati v obstoječi program poslovanja organizacije. Ogrodje je torej podlaga za to, da se kibernetska varnost osredotoči na poslovanje in poslovne funkcije organizacije. S tem so mehanizmi kibernetske varnosti neposredno integrirani v poslovne procese in poslovne modele organizacije, in sicer na takšen način, da postanejo njihov osrednji sestavni del. To pa lahko bistveno izboljša odpornost organizacije.

Kot navaja ISACA, ima program upravljanja kibernetske varnosti številne prednosti:
- uvaja procese, ki so ključnega pomena za izvajanje in nadziranje varnostnih aktivnosti ter za odzivanje na spremembe, ki jih povzročijo varnostna tveganja;
- podpira vizijo in cilje organizacije, pri čemer lahko zagotovi sredstva za kibernetsko varnost izven osnovnih sredstev za informacijsko tehnologijo;
- z integracijo posameznih parcialnih varnostnih mehanizmov v koherentno celoto zagotovi funkcionalno in tehnološko optimizacijo kibernetske varnosti;
- zagotavlja skladnost s standardi in poslovno vizijo ter omogoča upravljanje projektov in stroškov.

Implementacija takšnega ogrodja sicer zahteva več časa in virov, vendar se je potrebno zavedati, da doseganje želenega nivoja kibernetske varnosti ni zgolj cilj, temveč potovanje, ki sloni na opredelitvi začetne in končne točke, med katerima definiramo časovnico. Končno točko določa varnostna politika, ki ščiti informacijske vire organizacije. Če je možno, naj bi bila politika statična in s tem podvržena čim manj potencialnim spremembam. Vendar je v praksi program kibernetske varnosti redko statičen, ker se pojavljajo nove ranljivosti, tehnologije, tehnike kibernetskih napadov, naprednejše zmožnosti za varovanje pred napadi idr. Zato je potrebno program kibernetske varnosti iterativno nadgrajevati in izboljševati na osnovi specifikacije novih zahtev, preoblikovanja varnostnih politik, ozaveščanja ljudi o njihovih odgovornostih ter ocenjevanja tveganj in napredka. Pomembno je, da napori, ki jih v to vlagamo, obsegajo kompetence celotne organizacije, s čimer postane obvladovanje kibernetskih tveganj bistven element obvladovanja vseh organizacijskih in poslovnih tveganj, kakor tudi poslovanja na splošno.

Obstaja več različnih ogrodij, ki predstavljajo dobro osnovo programa kibernetske varnosti. Najbolj pogost pristop je uporaba standardov iz družine ISO 27000, med drugimi modeli pa so še posebej zanimivi NIST CSF, ITIL in COBIT. Kot navaja CISCO, mora ogrodje kibernetske varnosti pokrivati več temeljnih vidikov.

Primarni namen programa kibernetske varnosti je zagotoviti visoko stopnjo kibernetske odpornosti. Trije temeljni elementi kibernetske odpornosti so tako tudi ključne aktivnosti programa kibernetske varnosti, in sicer preprečevanje, zaznavanje in odzivanje na kibernetske grožnje.

Organizacije in izvršni kadri, ki vodijo uspešne programe kibernetske varnosti, se tega lotevajo na enak način kot upravljanja ostalih poslovnih funkcij. Ključni dejavnik uspeha je osredotočenost na možnosti izboljšave organizacije in ne zgolj na neposredne pritiske, ki jih prožijo kibernetske grožnje in tveganja.

Program kibernetske varnosti kot poslovna funkcija

Organizacije in izvršni kadri, ki vodijo uspešne programe kibernetske varnosti, se tega lotevajo na enak način kot upravljanja ostalih poslovnih funkcij. Ključni dejavnik uspeha je osredotočenost na možnosti izboljšave organizacije in ne zgolj na neposredne pritiske, ki jih prožijo kibernetske grožnje in tveganja. Skladno s tem so na področju kibernetske varnosti nujne veščine projektnega vodenja, ki vključujejo mehanizme upravljanja tveganj, s katerimi zmanjšamo vpliv groženj in ranljivosti. Osnovni pristop je, da planiramo upravljanje tveganj vnaprej, namesto da se ukvarjamo z grožnjami stohastično, šele v trenutku, ko se pojavijo. Zlasti je pomembna pro-aktivnost, ki pomeni, da razmišljamo o varnostnih dogodkih vnaprej in v širšem kontekstu. To daje organizacijam sposobnost bolj jasnega razumevanja varnostnih problemov, saj njihovo videnje ni omejeno zgolj na tiste grožnje in ranljivosti, ki so se že pojavile v preteklosti in jih je organizacija takrat zaznala. Gre za koncept inteligence kibernetskih groženj in tveganj, ki postaja vse bolj bistven in relevanten v sklopu področja kibernetske varnosti. Tako za oblikovanje verodostojnih zahtev, kot tudi za uspešno realizacijo strategije, pa je najpomembnejši dejavnik zavezanost vodstva, ki mora za varnost namenjati zadostne kadrovske in finančne vire.

Človeški vidik programa kibernetske varnosti

Ekipe za kibernetsko varnost se v številnih organizacijah pogosto soočajo s težavami pri komunikaciji o problemih in vidikih kibernetske varnosti z vodstvenim kadrom. Hkrati ima tudi vodstvo nemalokrat težave z usklajevanjem strategije kibernetske varnosti s tehničnim osebjem, zaposlenim v ekipah za kibernetsko varnost. Razumevanje kibernetske varnosti se lahko torej na različnih nivojih organizacije bistveno razlikuje, kar preprečuje uspešen dialog. Nezmožnost komuniciranja o kibernetski varnosti je tako eno ključnih in najresnejših tveganj programov za upravljanje kibernetske varnosti.

Implementacija programa kibernetske varnosti na različnih ravneh organizacije zaobjema tri bistvene nivoje. Izvršni nivo je pooblaščen za strateško odločanje in upravljanje organizacijskih tveganj. Na tem nivoju usmerja program kibernetske varnosti najvišje vodstvo, in sicer na podlagi jasno opredeljenih organizacijskih politik in zahtev za vodenje. Vmesni poslovno-procesni nivo se sooča z upravljanjem infrastrukturnih in operativnih tveganj ter z vpeljavo mehanizmov informacijske in kibernetske varnosti. Za ocenjevanje in analizo tveganj ter oblikovanje politik, postopkov in nadzornih mehanizmov skrbi usposobljena varnostna ekipa. Na najnižjem implementacijsko-operativnem nivoju je nazadnje potrebno realizirati mehanizme informacijske in kibernetske varnosti, ki so bili predlagani in definirani na višjih nivojih. Pomembno je, da so ti mehanizmi v največji možni meri in karseda transparentno integrirani v vse poslovne procese in delovne tokove organizacije.

Inteligenca kibernetskih tveganj in groženj

Ker obstaja velika verjetnost, da bo vsaka organizacija izpostavljena kibernetskim napadom, je zlasti pomembno, da vzpostavimo ustrezne načrte in postopke odzivov. Odzivanje na incidente je eno temeljnih področij kibernetske varnosti, katerega prakse in postopki morajo biti sestavni del vsakega programa kibernetske varnosti, saj so podlaga za sistematičen pristop k odpravljanju posledic napadov, incidentov in vdorov. Na ta način omejimo škodo kibernetskih napadov, skrajšamo čas okrevanja in zmanjšamo stroške. V programu za zagotavljanje kibernetske varnosti moramo pokriti vse korake generičnega postopka odziva na kibernetski incident. Po zaznavi varnostnega dogodka tako opravimo identifikacijo incidenta, pripravimo načrt odziva, izvedemo aktivnosti načrtovanega odziva ter sprožimo nadaljnje korake okrevanja po incidentu. Načrt odziva vključuje več aktivnosti, kot so vzpostavitev varnostne ekipe za izvedbo odziva, implementacija protokolov nadzora, ocenjevanje obsega in vpliva napada, obveščanje vodstva in odzivnih skupin na višjem nivoju, koordinacija med deležniki, usklajevanje s pravnimi telesi in zavarovalnicami ter analiza in premostitev vzrokov napada.

Ključnega pomena za to, da se je organizacija zmožna v okviru področja inteligence kibernetskih groženj na proaktiven način soočiti z nepoznanimi grožnjami, je implementacija varnostnih kontrol. Le-te je potrebno z izvedbo kontrolnega in penetracijskega testiranja redno in periodično verificirati, ocenjevati njihovo učinkovitost ter zagotoviti, da se izvajajo, kot je bilo v organizaciji predvideno.

Zrelost programa kibernetske varnosti

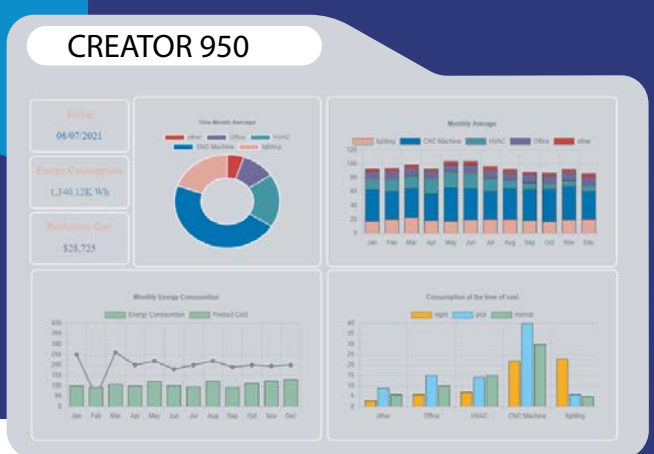
Proces transformacije kibernetske varnosti v sistemu ali organizaciji zahteva spremljanje, merjenje in izboljševanje nivoja zrelosti kibernetske varnosti z upoštevanjem različnih vidikov. V ta namen lahko uporabimo zmožno-zrelostni model (*Capability Maturity Model*), katerega namen je, da dvignemo postopke in prakse od neplaniranih do formaliziranih, upravljanih in optimiziranih na osnovi rezultatov metrik, ki jih vpeljemo v okviru razvoja programa upravljanja kibernetske varnosti. Model NIST CSF tako npr. definira štiri nivoje zrelosti, in sicer delnega, informiranega, ponovljivega in prilagodljivega. Stopnja zrelosti doseganja nivojev se meri glede na učinkovitost izvedbe več funkcionalnih sklopov in komponent, ki naslavljajo identifikacijo kibernetskih tveganj in groženj, zaščito, zaznavanje varnostnih dogodkov in anomalij, odzivanje na varnostne incidente ter okrevanje po incidentih. Razvoj vzdržnega in zrelega programa kibernetske varnosti mora tako upoštevati funkcionalne zahteve in potrebe vseh deležnikov, posameznikov in skupin v organizaciji.

Sklep

Program upravljanja kibernetske varnosti lahko na sistematičen, strukturiran in celovit način privede do izboljšanja odpornosti organizacij, zlasti v kompleksnih poslovnih sistemih in v povezavi z drugimi naprednimi pristopi, kakršen je varnostni operativni center. V aktivnosti kibernetske varnosti vpelje standardizacijo, poveča zaupanje v varnostne mehanizme, izboljša postopke odzivanja na incidente ter vzpodbuja inteligentno, proaktivno in od konteksta odvisno zaznavanje tveganj in groženj. Kljub temu, da umesti kibernetsko varnost kot eno osnovnih poslovnih funkcij organizacije in prinaša številne koristi, pa odpira tudi nekatere izzive ter zahteva ustrezne vire in znatno mero vloženega truda. Tako moramo oblikovati primerno strategijo, vzpostaviti ustrezno ogrodje, spremljati in dosegati zadostno stopnjo zrelosti, se prilagajati dinamično spreminjajočim se funkcionalnim zahtevam ter zagotoviti polno podporo na vseh nivojih organizacije. ■

Green Twin

DIGITALNI DVOJČEK
kontrola vsega z enim klikom



- nadzor tehničnega varovanja
- povezljivost z vsemi sistemi in obstoječo programsko opremo

- dostopnost kjerkoli in kadarkoli (WEB)
- upravljanje energije
- 4D poslovna analitika
- učinkovitost strojev
- digitalna servisna knjiga
- avtomatizirano vzdrževanje

031 648-702 info@greentwin.eu www.greentwin.eu

Avtor: Rafal Jaczynski / direktor za kibernetsko varnost za Srednjo in Vzhodno Evropo ter Nordijsko regijo pri Huawei Technologies

VARNOST DOBAVNE VERIGE

V zadnjih dveh letih smo bili vključeni v številne razprave o varnosti dobavne verige 5G z različnimi evropskimi deležniki. Po vseh teh mesecih nam ne da miru eno vprašanje – ali pozornost usmerjamo v pravo smer, imenovano »zaupanja vreden dobavitelj«.

Nadzorovanje tveganj, kjer je to mogoče

Dobavna veriga telekomunikacijske industrije je namreč iz vseh praktičnih vidikov neskončno zapletena in se nenehno širi. Kljub temu pa je presenetljivo pogosto prisotno prepričanje, da je enostavno praktično preverjati, potrjevati in razlikovati med dobavitelji na podlagi (ex ante) predhodne analize tveganja.

Takšno predvidevanje je napačno. Vse, kar lahko v resnici naredimo in je obenem učinkovito je, da izvedemo preprost pregled in zavrnemo dobavitelje, ki o kibernetski varnosti vedo premalo. Ločimo lahko strokovnjake od laikov – a nadaljnje razlikovanje, sploh znotraj »Fortune 500 dobaviteljev tehnologije«, preprosto ni realno. Sprva si iskreno odgovorite na vprašanje, ali ste dejansko videli notranjost tovarn ali razvojnih centrov vaših dobaviteljev in zmogljivosti njihovih poddobaviteljev? Ste preverili končno oceno tveganja vašega dobavitelja za podjetje z imenom SolarWinds Inc, s katerim ste zagotovo sodelovali? Čas je za budnico - po raziskavi Extended Enterprise Risk Management Survey 2020, ki jo je izvedel Deloitte, le 20 % anketirancev pravi, da lahko učinkovito spremlja bodisi vse ali samo bolj kritične podizvajalce.

Kaj lahko namesto tega storite? Vzpostavite nadzor zaupanja in zmanjšajte tveganje na točki, kjer se – po definiciji – manj zaupanja vredna domena poveže z vašo. Obstajajo trije načini, kako lahko dobavitelj škoduje varnosti vašega omrežja:

- Preko ljudi ali sistemov, ki imajo dostop do vašega omrežja;
- Preko ranljivosti izdelkov, ki vam jih dobavljajo;
- Preko neuspešnega zagotavljanja vsega, kar je in ko je potrebno za delovanje omrežja.

Dobavitelj vas ne more napasti z raketami ali vojaki, niti ne more čudežno posegati v vaše omrežje 5G. Za dejanski poseg nekaj potrebuje - kos tehnologije ali pa par rok, ki se dejansko lahko dotikajo omrežja. To predstavlja točko, kjer lahko, oziroma bi morali nadzorovati tveganje.

Nobeno varnostno testiranje vam ne bo dalo 100-odstotnega zagotovila, da izdelek ne vsebuje ranljivosti, lahko pa vam pomaga omejiti njihovo število. Za varnostno ozaveščene operaterje ali države načeloma nobena različica kritičnega omrežnega elementa ali posodobitve ne bi smela končati v delujočem omrežju brez varnostnega preverjanja, in noben omrežni element ne bi smel biti izvzet iz vzorčnega varnostnega preverjanja, kar velja za izbrane posodobitve.

Ljudje so pomembni

Za nadzor ljudi, ki imajo dostop do omrežja, so potrebne tri stvari:

- Osebe, katerim izdate dovoljenje za dostop do kritičnih omrežnih funkcij, je potrebno predhodno preveriti, če je mogoče, tudi preko vladnih postopkov preverjanja;
- Dovoljenja, ki jih dodelite kot omrežni operater, morajo biti izrecna, ne implicitna. Vezana morajo biti na določene posameznike s časovnimi, namenskimi in lokacijskimi omejitvami;
- Med dostopom do vašega omrežja, sistemov in naprav je treba nenehno spremljati individualno operativno vedenje. To velja tudi za takšne storitvene modele, kjer je vzpostavljena tehnična povezava s sistemi, ki so pod nadzorom dobavitelja.

Medtem, ko sta zadnji dve orodji splošno sprejeta primera dobrih praks, prvo ni. Razumem nasprotovanje, češ da bi to zagotovo povečalo delovno obremenitev organov, ki vodijo postopek preverjanja – a ker so omrežja 5G obravnavana kot vprašanje nacionalne varnosti, ni smiselno, da ljudje, ki jih vodijo in vzdržujejo, niso.

Najhujša ranljivost je tista, za katero ne veste

Z vidika razpleta ni pomembno, ali so ranljivosti namerne ali posledica iskrene napake. Pomembno je, da jih je v primeru, ko obstajajo, mogoče uporabiti za dostop do omrežja in za različne zlonamerne dejavnosti. Ponovno obstajajo zgolj trije pogoji, pod katerimi lahko nepridiprav z izkoriščanjem ranljivosti poškoduje vaše omrežje:

- ko ranljivost obstaja v izdelku, ki ste ga prvotno kupili, ali je nastala ob posodobitvi;
- ko gre za del funkcionalnosti, ki je vnaprej programirana za delovanje na podlagi posebnih pogojev, tj. časa ali datuma, ali pa jo je mogoče aktivirati znotraj ali zunaj omrežja;
- ko ne morete pravočasno zaznati ali se odzvati, da bi popolnoma ublažili ali vsaj omejili posledice izkoriščanja ranljivosti.

Nobeno varnostno testiranje vam ne bo dalo 100-odstotnega zagotovila, da izdelek ne vsebuje ranljivosti, lahko pa vam pomaga omejiti njihovo število. Za varnostno ozaveščene operaterje ali države načeloma nobena različica kritičnega omrežnega elementa ali posodobitve ne bi smela končati v delujočem omrežju brez varnostnega preverjanja, in noben omrežni element ne bi smel biti izvzet iz vzorčnega varnostnega preverjanja, kar velja za izbrane posodobitve. Za omrežja 5G bi na primer v skladu s specifikacijami ETSI/3GPP in orodji EU 5G Toolbox takšni kritični elementi omrežja bili podmnožica osnovnih funkcij 5G.

Bistveno je, da imajo operaterji dostop do testnih plošč, ki jih je mogoče uporabiti kot „omrežne dvojčke“. Poleg tega je treba nadzorni promet v in iz omrežnih elementov v delujočem omrežju vsaj spremljati in filtrirati, glede skladnosti s pričakovanim prometom profila. Ti ukrepi so nedvomno naporni in naložbeno intenzivni. Operaterji in regulatorji bi morali zato razmisliti o nekaterih vrstah skupnih organizacij, osredotočenih na varnostno preverjanje izdelkov mobilnega omrežja – podobno kot skupna podjetja, ki so jih mnogi ustanovili za načrtovanje in delovanje omrežij za radijski dostop.

Za manjše operaterje ali tiste, ki so pripravljeni sprejeti več tveganj, bi lahko zadostovala osnovna raven zagotovila, ki ga zagotavljajo sheme certificiranja in zavarovanj, kot so EECC, GSMA NESAS, kot tudi ti, ki jih trenutno razvija ENISA. Zapomniti si moramo, da je treba vsako certificiranje razumeti kot dokaz sposobnosti dobavitelja in ne kot jamstvo za varnost izdelka skozi celotno življenjsko dobo.

Varnost preko anonimnosti je preteklost

Potreba po odkrivanju in zajezitvi zlonamernih dejanj je ključnega pomena – noben dobavitelj ne bi smel omrežnemu operaterju onemogočati razumevanja specifikacij vmesnikov ali običajnega pretoka profila, niti ne bi smel zavrniti zahtev operaterjev po dostopu do pomembnih varnostnih informacij. Za omrežja 5G bi to lahko pomenilo naslednje varnostne zahteve, ki bi morale biti vključene v razpise in po možnosti podprte z zakonodajo države:

1. Vsi elementi omrežja 5G morajo prek varnega kanala, v skoraj realnem času in brez uporabe relejev, poročati v centralni arhiv.
2. Vsi elementi omrežja 5G morajo podpirati namestitev omrežnih sond tretjih oseb in t.i. endpoint agentov, kot je npr. zaznavanje in odziv končne točke (EDR).

Koncept »zaupanja vrednega dobavitelja« je še eno področje, ki se mu ne bi smeli toliko posvečati. Ne samo, da ne naslavlja niti enega tveganja kibernetske varnosti, ampak dejansko vodi do nazadovanja sodobnega razmišljanja o kibernetski varnosti.

3. Vsi omrežni elementi morajo zagotavljati odprt vmesnik za namensko programiranje (API) za pridobivanje podrobnega popisa strojne in programske opreme omrežnih elementov.
4. Vsi omrežni elementi morajo poročati o dogodkih AAA, varnostnih dogodkih, nenormalnem vedenju, stanju delovanja (naloge, CPU/pomnilnik, seznam procesov, uporaba).
5. Vsi omrežni elementi morajo zagotavljati podroben obračun svoje matrike omrežnega prometa (protokoli, vrata itd.).
6. Vsi omrežni elementi morajo zagotavljati vodnik najboljših praks in operativni priročnik za varno uvajanje.
7. Vsi omrežni elementi morajo imeti nameščeno samo programsko ali strojno-programsko opremo, ki je digitalno podpisana s strani dobavitelja in nameščena z namenskimi računi, pri čemer so le ti računi dovoljeni za izvajanje te operacije, postopek same namestitve pa bi moral zahtevati več faktorsko preverjanje pristnosti.
8. Vsi binarni artefakti programske in strojno-programske opreme morajo biti binarno enakovredni, to pomeni, da se kompilacija izvorne kode izdelka ujema z binarnimi artefakti, ki jih dostavi dobavitelj.
9. Varnostni popravki so ločeni od funkcionalnih popravkov in imajo omejen obseg.
10. Dobavitelji morajo brez nepotrebnega odlašanja razkriti vse šibke točke ali slabosti, ugotovljene v njihovih izdelkih, zagotoviti napotke za morebitne ublažitve, če obstajajo, in razviti varnostne popravke za ublažitev teh šibkih točk, v razumnem času.

Če so odkrite ranljivosti, jih je treba takoj odpraviti. Na to se seveda nanašajo tudi vidiki vzdrževanja produkta, konca podpore in življenjske dobe – načeloma pa mora biti pogodba o ravni storitve za dostavo varnostnih posodobitev ne le sklenjena, ampak tudi izvršljiva.

Kaj pa, če dobavitelj preneha poslovati?

Izbira dobavitelja le na podlagi tega, kakšne možnosti preživetja ima ta dobavitelj, je kot stava. Ob predpostavki, da je opravljena skrbna finančna analiza glede najboljše dobaviteljeve zmožnosti dostave, obstajata še dva varnostna ukrepa, ki ju mora operater omrežja sprejeti, da se ne zanašate na izid omenjene stave:

- poskrbite, da imate zagotovljeno zadostno zalogo rezervnih delov;
- poskrbite, da je izvorna koda omrežne programske opreme, ki jo uporabljate – skupaj z orodji in navodili za njeno gradnjo – deponirana, pogodba v posebnih okoliščinah pa operaterju omogoča dostop do nje.

Zaupanja vreden dobavitelj je, kot drevo brez mačke

Kar me pripelje do teme »zaupanja vrednega dobavitelja« – ali izključitve »nezaupanja vrednega dobavitelja«, kot metode obvladovanja tveganja dobavne verige. Pogosto je napačno prepričanje, da je izključitev dobaviteljev najboljša možnost za zmanjšanje tveganja. Vsekakor deluje, če izključimo VSE dobavitelje, saj potem lahko trdite, da je bilo tveganje vaše dobavne verige učinkovito zmanjšano, ker ni dobavne verige. Vendar, če se pametno odločite, da ne boste šli po tej poti, je v panogah z malo dobavitelji izključitev dobavitelja preprosto slaba strategija za zmanjšanje tveganja. Točno to velja za dobavitelje omrežij 5G, kjer bi v večini realnih primerov, operater izbiral med največ petimi dobavitelji, od katerih so le štirje dobra izbira za uvedbo popolnoma nove dejavnosti 5G. Napačno je prepričanje, da omejevanje izbire z javno izključitvijo dobaviteljev iz skupine zmanjša tveganje – če je edino, kar lahko naredimo, da izberemo dva dobavitelja, izmed le dveh razpoložljivih, v resnici pa nimamo izbire, niti ni nobene spodbude za te dobavitelje, da izboljšajo varnost ali izboljšajo svoje izdelke z dodatnimi varnostnimi funkcijami. Denar je bolje vložiti v ukrepe za obvladovanje tveganja, o katerih smo razpravljali prej, z delčkom nepovratnih stroškov, ki so posledica izključitve in zamenjav dobaviteljev.

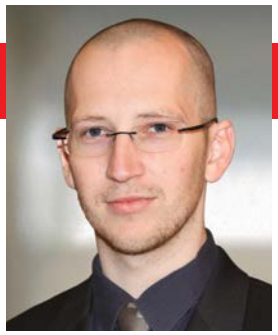
Izključitev dobavitelja ima svoje mesto kot oblika kazni za tiste, ki nenehno ne izpolnjujejo obljub ali zavračajo sodelovanje pri varnostnem testiranju ali pravočasnem reševanju šibkih točk. Ogroženost tržnega deleža je lahko močan motivator, zlasti, če ga podpira zakonodaja države – vendar kazen nikoli ne bi smela biti izrečena preden je kaznivo dejanje storjeno kar enako velja za izključitev dobaviteljev.

Posledice pozornosti na napačnem mestu

Industrije kibernetske varnosti (in zasebnosti) vedno znova prizadanejo priljubljene ideje, ki pogosto obravnavajo agendo (komercialno ali politično). Vendar z vidika kibernetske varnosti in zasebnosti te, tako imenovane izboljšave niso nič drugega, kot ogromna potrata časa, ki vodi do zadrege. Razmislite o fiasku »varnega pristana«. Spomnite se na zasebnostni ščit. Ne pozabite na več faktorsko preverjanje pristnosti, ki temelji na kodah SMS ali omrežni obrambi, ki temelji na obodu. Vsem tem idejam je skupno to, da nikoli niso bile zasnovane za zagotavljanje zasebnosti ali varnosti.

Koncept »zaupanja vrednega dobavitelja« je še eno področje, ki se mu ne bi smeli toliko posvečati. Ne samo, da ne naslavlja niti enega tveganja kibernetske varnosti, ampak dejansko vodi do nazadovanja sodobnega razmišljanja o kibernetski varnosti. ■

Avtor: mag. Matjaž Drev / Center za informatiko v zdravstvu, NIJZ*



VGRAJENA ZASEBNOST

Za razumevanje trenutnega stanja na področju varstva osebnih podatkov in s tem povezane informacijske zasebnosti, je treba v grobih orisih razumeti razvoj pravnega okvira. Pravila na področju varstva osebnih podatkov v EU trenutno določa GDPR, ki predstavlja najbolj obsežen in temeljit poizkus pravnega varovanja informacijske zasebnosti v svetu.

Začetki pravnega varstva osebnih podatkov v Evropski Uniji (EU) segajo v leto 1953, ko je bila sprejeta Evropska konvencija o človekovih pravicah (Svet Evrope, 1950). Ta v 8. členu uveljavlja »pravico do spoštovanja zasebnega in družinskega življenja«. Varovanje zasebnosti se je utrdilo z Direktivo 95/46/ES leta 1995. Direktiva je določila konkretna pravila v zvezi z varstvom osebnih podatkov, ki so jih članice EU morale upoštevati, poleg tega je še določila, da posamezne države sprejmejo nacionalne zakone s področja varstva osebnih podatkov ter nadzorne organe z inšpekcijskimi pooblastili. Zadnji premik v razvoju tega področja predstavlja Splošna uredba o varstvu podatkov (GDPR), ki je stopila v veljavo leta 2016, neposredno pa se je začela uporabljati 25. maja 2018. Pravila na področju varstva osebnih podatkov v EU trenutno določa GDPR, ki predstavlja najbolj obsežen in temeljit poizkus pravnega varovanja informacijske zasebnosti v svetu.

Področje varstva osebnih podatkov se je torej izoblikovalo iz pravnih zahtev, ki naj bi jih organizacije izpolnjevale. Vendar je kmalu postalo jasno, da bo pri tem treba posebej upoštevati tako družbene kot tehnološke vidike. Zaradi odločilne vloge informacijsko komunikacijske tehnologije (IKT) ni bilo mogoče spregledati področja informacijske varnosti, ki postaja vse pomembnejši element v procesu varstva osebnih podatkov. Vzpostavitev državnih nadzornih organov je vprašanju (ne)upoštevanja pravil dodalo posebno težo, saj se kršitve določb GDPR sankcionirajo, v najhujših primerih celo z milijonskimi globami. Zato so organizacije, ki se kakorkoli ukvarjajo z obdelavo osebnih podatkov, še posebej, če gre za množično in čezmejno obdelavo podatkov, postale pozorne na zagotavljanje skladnosti z zahtevami GDPR. Teh zahtev ni malo: od pravne podlage za obdelavo podatkov, omogočanja posameznikom, da uveljavljajo svoje pravice, zagotavljanja ustrezne pogodbene obdelave podatkov, iskanja načinov za iznos podatkov izven območja EU, imenovanja pooblaščene osebe za varstvo podatkov (DPO), poročanja o hujših kršitvah, sprejemanja kodeksov in certifikatov o skladnosti, vzpostavljanja mehanizmov za zagotavljanje zavarovanja podatkov, do upoštevanja načel zagotavljanja vgrajenega ter privzetega varstva podatkov.

Čeprav se morda na prvi pogled zdi, da projekten in sistematičen pristop vnaša dodatno kompleksnost, se v praksi kaže, da je izvedba DPIA ena bolj smotrnih in učinkovitih potez pri zagotavljanju skladnosti obdelave podatkov z zahtevami GDPR. Nemalokrat tudi zato, ker nekaterih razsežnosti (npr. iskanja ustrezne pravne podlage) obdelave podatkov »za nazaj« pogosto ni več mogoče ustrezno popraviti.

Kaj je vgrajena zasebnost?

Prvi resni premisleki o vgrajeni zasebnosti so se oblikovali v začetku 90. let dvajsetega stoletja. Glavna pobudnica ideje je bila kanadska informacijska pooblaščenka, Ann Cavoukian (2009). Zastopala je stališče, da bi morali upravljavci osebnih podatkov že v samem začetku načrtovanja procesov obdelave osebnih podatkov razmisliti o načinih in ukrepih, ki bi omogočali doseganje legitimnih ciljev na način, ki bi predstavljal kar najmanjši poseg v zasebnost posameznikov. Cavoukian (2009) je določila naslednja načela: (1) proaktivnost namesto reaktivnosti; (2) zasebnost kot privzeto izbiro; (3) zasebnost, ki je sestavni del zasnove rešitve; (4) polno funkcionalnost – igro s pozitivno vsoto; (5) zavarovanje podatkov v celotnem ciklu obdelave podatkov; (6) transparentnost; (7) spoštovanje posameznika.

Kljub pomislekom nekaterih avtorjev (Gurses, Tronsco in Diaz, 2011), ki so

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

kritično opozorili na preveliko splošnost temeljnih načel vgrajene zasebnosti, se je ideja ohranila in v bolj konkretizirani obliki dobila mesto v GDPR, ki sicer ne uporablja izraza vgrajena zasebnost, pač pa vgrajeno in privzeto varstvo podatkov. GDPR (2016) v 78. uvodnem stavku pojasni, da je »zaradi varstva pravic in svoboščin posameznikov v zvezi z obdelavo osebnih podatkov treba sprejeti ustrezne tehnične in organizacijske ukrepe /.../, ki spoštujejo zlasti načela vgrajenega in privzetega varstva podatkov. Ti ukrepi bi med drugim lahko vključevali minimizacijo obdelave osebnih podatkov, čimprejšnjo psevdonimizacijo osebnih podatkov, preglednost pri nalogah in obdelavi osebnih podatkov, omogočanje posameznikom, na katere se nanašajo osebni podatki, da spremljajo obdelavo podatkov, in omogočanje upravljavcu, da vzpostavi in izboljša varnostne ukrepe«.

Vgrajevanje zasebnosti v procese obdelave podatkov

Zagotavljanje skladnosti procesov obdelave osebnih podatkov z zahtevami določb GDPR zahteva iskanje konkretnih rešitev. Zato je koncept vgrajene zasebnosti smotrno razumeti predvsem kot niz usmeritev: prizadevanje po udejanjanju načela sorazmernosti pri obdelavi podatkov, vzpostavljanju mehanizmov za čim bolj učinkovito uresničevanje pravic posameznikov, ter uvajanju nekaterih specifičnih tehničnih rešitev, predvsem psevdonimizacije in šifriranja podatkov. Vse naštete usmeritve je mogoče pregledno in sistematično izvesti skozi izdelavo ocene učinkov na varstvo podatkov (DPIA). Gre za projekten pristop, ki upravljavce in obdelovalce že v fazi načrtovanja procesov obdelave osebnih podatkov usmeri k premisleku o ključnih vprašanjih obdelave: kdo je kdo; katere podatke se bo obdelovalo in na kakšen način; ali obstajajo ustrezne pravne podlage za obdelavo; kako zagotoviti uresničevanje pravic posameznikov; urejanje pogodbenih razmerij; določitev organizacijskih in tehničnih varnostnih ukrepov; uresničevanje koncepta vgrajene zasebnosti (predvsem minimizacije obdelave podatkov, psevdonimizacija in šifriranje podatkov). Ustrezno začrtanemu kontekstu obdelave podatkov sledi določitev tveganj in sprejetje ukrepov za zmanjšanje tveganj, ki grozijo različnim vidikom obdelave podatkov. Čeprav se morda na prvi pogled zdi, da projekten in sistematičen pristop vnaša dodatno kompleksnost, se v praksi kaže, da je izvedba DPIA ena bolj smotrnih in učinkovitih potez pri zagotavljanju skladnosti obdelave podatkov z zahtevami GDPR. Nemalokrat tudi zato, ker nekaterih razsežnosti (npr. iskanja ustrezne pravne podlage) obdelave podatkov »za nazaj« pogosto ni več mogoče ustrezno popraviti. Tako je koncept vgrajene zasebnosti, ki se v veliki meri udejanja skozi instrument DPIA, praktična spodbuda k premišljenemu načrtovanju procesov obdelave podatkov.

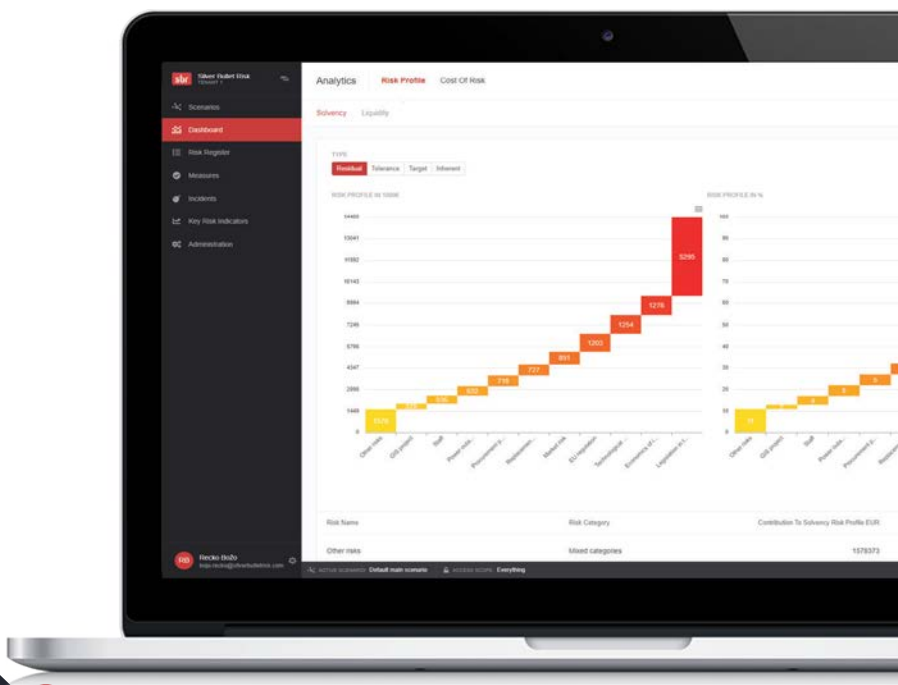
Viri

- Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.
- Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
- Cavoukian, A. (2009) Privacy by Design. The 7 Foundational Principles.
- Gurses, S., Troncoso, C., Diaz, C. (2011). Engineering Privacy by Design.
- Informacijski pooblaščenec (2019). Ocene učinkov na varstvo podatkov. Ljubljana: Informacijski pooblaščenec. ■

WWW.SILVERBULLETRISK.COM

Tveganja povežite s poslovnimi kazalniki uspešnosti

Kulturo upravljanja tveganj pa vpeljite v čisto vse organizacijske procese



SVETOVANJE O UPRAVLJANJU TVEGANJ

CELOVITO **UPRAVLJANJE TVEGANJ**

UPRAVLJANJE **ŠKODNIH DOGODKOV**

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.

UČINKI IN IZBOLJŠAVE ZA VAŠO ORGANIZACIJO

- 30-50% učinkovitejša izraba časa za upravljanje tveganj
- Nižji stroški realiziranih tveganj
- Spremljanje finančnih in drugih vplivov
- Gradnja lastne baze znanja o tveganjih
- Ustrezno ukrepanje v realnem času
- Zagotovljena skladnost z zahtevami in predpisi

Avtorica: Neja Domnik / asistentka svetovalca, Urad Informacijskega pooblaščenca*

PRENOSI PODATKOV V TRETJE DRŽAVE

V današnjem svetu smo vse bolj povezani, zato ni nenavadno, da je prenos podatkov v tujino vse bolj običajen tako za multi-nacionalna podjetja kot tudi za številna majhna podjetja, javni sektor in druge organizacije. Evropski pravni okvir zagotavlja relativno visoko raven varstva osebnih podatkov – izven EU je ta raven različna in marsikje ne dosega evropskih standardov. Zato Splošna uredba o varstvu podatkov (Splošna uredba) predvideva posebne varovalke v primerih, ko se osebni podatki iz EU prenašajo v tretje države, ki same ne zagotavljajo ustrezne ravni varstva osebnih podatkov.

Uvodno

Pomembno je, da družba, javni organ ali druga organizacija prepozna, kdaj določena obdelava podatkov predstavlja prenos podatkov v tretjo državo, na kateri mehanizem za prenos podatkov, se za konkretni prenos lahko opre, ter kdaj je treba sprejeti morebitne dopolnilne zaščitne ukrepe. Ob tem pa tudi upošteva Sodišče Evropske unije (SEU), ki je v svoji sodbi v zadevi Schrems II[1] jasno poudarilo, da se lahko podatki prenašajo v tretjo državo le, če se s prenosom dejansko ne ogrozi raven varstva podatkov, ki jo zagotavlja Splošna uredba.

Kdaj gre za prenos podatkov v tretje države?

O prenosu osebnih podatkov v tretje države govorimo takrat, ko upravljavec ali obdelovalec iz Slovenije ali druge države znotraj Evropskega gospodarskega prostora[2] (to je lahko tudi podružnica; EGP) osebne podatke iz takega ali drugačnega razloga posreduje v države izven EGP ali mednarodni organizaciji.[3] O prenosu govorimo tudi takrat, ko je dostop do osebnih podatkov omogočen organizacijam, podjetjem, posameznikom ali drugim subjektom iz tretjih držav izven EGP, pa čeprav so podatki fizično hranjeni znotraj EGP.

Kot tipičen primer prenosa podatkov si lahko zamislimo podjetje iz Slovenije, ki uporablja oblačni sistem za upravljanje odnosov s strankami podjetja iz ZDA, ta pa te podatke obdeluje na strežnikih izven EGP. Za prenos pa gre tudi v primeru, ko podjetje iz Slovenije materinski družbi iz Avstralije kot obdelovalcu omogoči dostop do podatkov svojih zaposlenih.

V nadaljevanju vas bomo po korakih popeljali skozi analizo, ki je lahko v pomoč vaši organizaciji pri zagotavljanju skladnosti z načelom odgovornosti v primeru prenosov podatkov.

Prvi korak: Preučite svoje prenose

Prvi korak pri zagotavljanju skladnosti je evidentiranje oziroma preučitev prenosov. Torej, izvoznik podatkov mora biti povsem seznanjen s tem, katere podatke prenaša oziroma bo prenašal v tretje države.

Ob tem je treba opozoriti, da je izvoznik podatkov dolžan zagotoviti, da osebne podatke obdeluje in drugemu upravljavcu posreduje zakonito, torej da ima za to ustrezno pravno podlago. To podrobneje ureja člen 6(1) Splošne uredbe (npr. privolitev, pogodba, zakonska podlaga). Za obdelovalca podatkov pa bo pravna podlaga temeljila na pogodbi o obdelavi podatkov, ki jo je v skladu s členom 28 Splošne uredbe sklenil z upravljavcem, ki mu je podatke zaupal v obdelavo.

Za izvoznike podatkov je najbolj enostavno prenašati podatke v države ali mednarodne organizacije, za katere je Evropska komisija s sklepom ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Drugi korak: Opredelite orodja za prenos, na katera se zanašate

Po prenosu podatkov v tretjo državo mora biti zagotovljena ustrezna raven varstva podatkov. To je mogoče izvesti s pomočjo orodij iz V. poglavja Splošne uredbe, ki bi jih lahko razdelili v tri skupine: sklepi o ustreznosti Evropske komisije, ustrezni zaščitni ukrepi (z morebitnimi dopolnilnimi zaščitnimi ukrepi) in odstopanja v posebnih primerih.

Prenosi na podlagi sklepa o ustreznosti
Za izvoznike podatkov je najbolj enostavno prenašati podatke v države ali mednarodne organizacije, za katere je Evropska komisija s sklepom ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov. V te države je podatke mogoče prenašati brez posebnih formalnosti ali morebitnih dovoljenj nadzornih organov. Situacija je podobna, kakor da bi se podatki posredovali med organizacijami znotraj EGP. Takšen sklep je Evropska komisija med drugim sprejela za Združeno kraljestvo, Izrael, Japonsko in še nekatere druge države.[4] V kolikor organizacija prenaša podatke na podlagi sklepa o ustreznosti, ji ni treba opraviti nadaljnjih korakov, temveč se analiza na tem mestu konča.

Odločba Evropske komisije o zasebnem ščitu (angl. *Privacy Shield*), v okviru dogovora EU-ZDA ki je omogočala prenose v ZDA, je bila lansko poletje s strani SEU v zadevi Schrems II razveljavljena. To pomeni, da morajo organizacije, ki prenašajo podatke v ZDA, zagotoviti drug ustrezni mehanizem za prenose podatkov v to državo, o čemer več v nadaljevanju.

Prenosi na podlagi ustreznih zaščitnih ukrepov
Kadar sklep o ustreznosti za določeno državo ni bil sprejet, je mogoče podatke prenašati na podlagi člena 46 Splošne uredbe. V takem primeru mora izvoznik podatkov zagotoviti ustrezne zaščitne ukrepe ter posameznikom zagotoviti izvršljive pravice in učinkovita pravna sredstva. Ustrezni zaščitni ukrepi se lahko zagotovijo:

- s standardnimi pogodbenimi določili,
- z zavezujočimi poslovnimi pravili (angl. *Binding Corporate Rules – BCR*),
- s kodeksi ravnanja,
- z mehanizmi certificiranja,[5]
- z ad hoc pogodbenimi določili (potrebno je predhodno dovoljenje Informacijskega pooblaščenca (IP)).

Člen predvideva tudi dva mehanizma, ki sta namenjena le prenosu podatkov s strani javnih organov in teles:

- pravno zavezujoči in izvršljivi instrument, ki ga sprejmejo javni organi ali telesa,
- določbe, ki se vstavijo v upravne dogovore med javnimi organi ali telesi (potrebno je predhodno dovoljenje IP).

Za prenos podatkov na podlagi ustreznih zaščitnih ukrepov predhodno dovoljenje IP ni potrebno, obvezno je le pri uporabi dveh mehanizmov, za katera je to zgoraj izrecno navedeno. V nadaljevanju bosta na kratko predstavljena dva mehanizma, ki se ju evropska podjetja pri prenosih v praksi najpogosteje poslužujejo.

Prenos na podlagi standardnih pogodbenih določil
Standardna pogodbena določila pridejo v poštev za izvoznike podatkov, kateri želijo podatke prenesti točno določeni organizaciji iz tretje države, za katero sklep o ustreznosti ni bil sprejet. Gre za tipske pogodbe, ki jih je sprejela Evropska komisija. Komisija je dne 4. 6. 2021 sprejela nova standardna

pogodbena določila, ki so usklajena s Splošno uredbo in sodbo SEU v zadevi Schrems II.[6]

Standardna pogodbena določila so modularnega značaja in vključujejo različne scenarije obdelave osebnih podatkov, ki jih pogodbeni stranki izbereta glede na to, kdo sta stranki pogodbe. Kadar je uvoznik (pod)obdelovalec, nova standardna določila že vključujejo tudi vse pogodbene zahteve iz člena 28 Splošne uredbe, zato pogodbenima strankama ni treba sklepati dveh ločenih pogodb. Nova določila tudi omogočajo dodajanje več kot dveh strank v pogodbeno ureditev, tako med njenim sklepanjem, kot tudi kasneje (npr. s pogodbo se lahko naknadno zaveže pod obdelovalec).

Prenos na podlagi zavezujočih poslovnih pravil
Zavezujoča poslovna pravila predstavljajo interni akt multi-nacionalne korporacije – skupine podjetij, od katerih so določena podjetja locirana v tretjih državah, kateri ne zagotavljajo ustreznega varstva osebnih podatkov. Namen zavezujočih poslovnih pravil je, da je v korporaciji, ki ima lahko člane tudi v tretjih državah, omogočen prost pretok osebnih podatkov. Podrobneje so urejena v členu 47 Splošne uredbe, ki v drugem odstavku določa minimalno vsebino pravil. Predpogoj za prenos podatkov v tretjo državo, na podlagi zavezujočih poslovnih pravil, je predhodna odobritev zavezujočih poslovnih pravil v skladu z mehanizmom za skladnost iz člena 63 Splošne uredbe.

Prenosi na podlagi odstopanj v posebnih primerih
Splošna uredba poleg sklepa o ustreznosti orodij za prenos iz člena 46 vsebuje še tretjo možnost, ki omogoča prenos v nekaterih posebnih, izjemnih primerih. Odstopanja iz člena 49 Splošne uredbe je treba razlagati restriktivno, nanašajo se v glavnem na dejavnosti obdelave, ki so občasne in se ne ponavljajo. V kolikor bi konkretni prenos temeljil na odstopanjih v posebnih primerih, nadaljnji koraki iz prispevka niso potrebni in se analiza za izvoznika na tem mestu konča.

Tretji korak: Ali je orodje za prenos iz člena 46 dejansko učinkovito?

Ključen je tretji korak, v okviru katerega mora izvoznik, ki prenaša podatke na podlagi ustreznih zaščitnih ukrepov iz člena 46, oceniti, ali so ustrezni zaščitni ukrepi delujoči tudi v praksi.[7] Torej, ali na primer z uvoznikom sklenjena standardna pogodbena določila tudi v praksi zagotavljajo, da se s prenosom ne ogrozi raven varstva, ki jo zagotavlja Splošna uredba.

Izvoznik mora (po potrebi v sodelovanju z uvoznikom) oceniti, ali je v okviru konkretnega prenosa podatkov morda kar koli v pravu ali praksi tretje države, kar posega v učinkovitost ustreznih zaščitnih ukrepov iz člena 46, na katere se izvoznik opira. Posebno pozornost je treba nameniti zlasti zakonodaji, ki določa zahteve za razkritje podatkov javnim organom ali jim daje pooblastila za dostop do podatkov (npr. za namene nacionalne varnosti). Oceno mora izvoznik dokumentirati ter na podlagi nje sprejeti odločitev, ali bo prekinil prenos podatkov, bo prenašal podatke ali pa bo prenašal podatke in ob tem sprejel ustrezne dopolnilne zaščitne ukrepe. Za izvedbo konkretne presoje je v skladu z načelom odgovornosti odgovoren izvoznik podatkov.

Četrti korak: Sprejmite dopolnilne ukrepe

Če je to mogoče, in je na podlagi ocene, v skladu s korakom 3 potrebno, izvoznik sprejme ustrezne dopolnilne zaščitne ukrepe, s pomočjo katerih bo prenos podatkov izpolnjeval standard v bistvu enakovrednega varstva, ki se zahteva s pravom EU. Dopolnilni zaščitni ukrepi po svoji naravi dopolnjujejo varovalke, ki jih že vsebujejo orodja za prenos iz člena 46 in druge zahteve glede varnosti podatkov iz Splošne uredbe. Ti ukrepi so lahko na primer tehnične narave, organizacijske narave ali v obliki dodatnih pogodbenih zavez.[8]

Pomembno je, da izvoznik redno spremlja razvoj v tretji državi, ki bi lahko vplival na oceno glede ravni varstva osebnih podatkov v tretji državi in na odločitev, ki je bila na podlagi tega sprejeta.

Sklepno

Da bi v polni meri izkoristili potenciale digitalne obdelave podatkov in možnosti, ki jih odpira, morajo obstajati varovala za zaščito posameznika pri prenosu podatkov. Zato je pomembno, da se, preden podatke posredujemo v svet, prepričamo, da bo njihovo varstvo še naprej zagotovljeno.

1 Sodba Sodišča Evropske unije z dne 16. 7. 2020, Data protection Commissioner proti Facebook Ireland Ltd, Maximillian Schrems, št. C-311/18 (v nadaljevanju: Schrems II).

2 Evropski gospodarski prostor (EGP) poleg vseh držav Evropske unije zajema še: Islandijo, Norveško in Lihtenštajn.

3 Četudi se besedilo prispevka v nadaljevanju nanaša zgolj na prenos podatkov v tretje države, veljajo enaka pravila tudi za prenos podatkov v mednarodne organizacije.

4 Komisija seznam držav redno posodablja na svoji spletni strani: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

5 Trenutno v EU še ni razvit in potrjen noben mehanizem certificiranja po členu 42 Splošne uredbe.

6 Veljavna standardna pogodbena določila so dostopna na spletni strani: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0031.01.SLV&toc=OJ%3AL%3A2021%3A199%3ATOC. Do dne 27. 12. 2022 morajo biti vse pogodbe prilagojene novim standardnim pogodbenim določilom.

7 Pri oceni si je mogoče pomagati s Priporočili 02/2020 Evropskega odbora za varstvo podatkov glede evropskih bistvenih jamstev, Evropski odbor za varstvo podatkov, sprejeto 10. 11. 2021: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sl.pdf.

8 Konkretne primere dopolnilnih ukrepov vsebuje Priloga 2 Priporočil 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU, Evropski odbor za varstvo podatkov, sprejeto 18. 6. 2021: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Primož Sušnik, vodja avtomatizirane proizvodnje pri Zarja Elektroniki in
Luka Suhadolnik, mladi raziskovalec pri Institutu Jožef Stefan

PRIHAJA SLOVENSKA INOVACIJA, KI OBETA 10-KRAT HITREJŠO POT DO UPORABE NOVIH MATERIALOV

Na Odseku za nanostrukturne materiale Instituta Jožef Stefan (IJS) postavljajo robotiziran laboratorij za avtonomno odkrivanje novih materialov. Pri izpeljavi tega zahtevnega in obsežnega projekta, ki je edinstven na svetu, tesno sodelujejo tudi z Zarja Elektroniko, ki jim kot veliki partner pomaga na več pomembnih področjih zaradi njenih izkušenj z roboti. Skupaj usklajujejo naloge robota, jih optimizirajo in mu z razvojem namenskih priprav pomagajo, da jih lažje izvaja. Na projektu je še dobrih pet velikih partnerjev, večinoma iz Slovenije, pa tudi iz Švedske, Finske in Nemčije. Sodelovanje se je začelo konec maja, projekt pa nameravajo zaključiti do naslednjega poletja, ko bo sistem postavljen na IJS in bo deloval.

Kako je prišlo do sodelovanja med IJS in Zarja Elektroniko pri tem projektu?

Suhadolnik: Sodelujemo pri postavljanju avtomatiziranega laboratorija za odkrivanje novih materialov, v katerem bomo razvijali nanostrukturne materiale za bodoče zelene tehnologije. Da bo to lahko počel robot, moramo povezati veliko tehnologij, oziroma razviti nove, saj trenutno nikjer na svetu še nihče v taki meri ne raziskuje na tak način. Na Zarja Elektroniki testiramo najnaprednejše produkte, ki jih nameravamo vključiti v robotiziran laboratorij, ter izdelujemo in testiramo prototipe, ki jih razvija ona in drugi partnerji na projektu.

Sušnik: Ob vzpostavitvi kontakta z IJS, smo jim pokazali, kako smo razvili avtomatiziran proces izdelovanja tiskanih vezij. Ta naš projekt je soroden tistemu na IJS, zato smo se odzvali na povabilo k sodelovanju in sprejeli izziv. S postavitvijo avtomatiziranega procesa, ki smo ga vzpostavili na Zarji Elektroniki, smo pridobili zelo veliko praktičnih izkušenj, zato smo vedeli, kako lahko pomagamo pri projektu IJS. Pri robotizaciji se namreč velikokrat izkaže, da stvari, ki bi morale v teoriji delovati, v praksi ne delujejo povsem. Robot pa bo pri tem projektu opravljal vsaj 15 različnih nalog.

Torej uporabljate enega od dveh robotov za proizvodnjo tiskanih vezij?

Sušnik: Tako je, enega od teh uporabljamo za občasno testiranje na tem projektu, kar je možno, ker imamo fleksibilno proizvodnjo. Ni pa to robot, ki bo na koncu vgrajen v avtomatiziran laboratorij na IJS. Z našim robotom v fazi razvoja iščemo različne rešitve, kot je na primer, kako bomo izvajali menjavo orodij v kompleksni postavitvi avtomatiziranega laboratorija na IJS. Gre za neobičajno menjavo zaradi položaja prijemal, ki smo jih postavili tako, da bomo najbolje izkoristili prostor, ki je na voljo na IJS. Testi so pokazali, da je menjalni mehanizem učinkovit, poleg tega pa smo za namen optimizacije avtomatiziranega procesa na IJS, zelo učinkovito prilagodili tudi električno prijemalo, ki omogoča, da

*avtor je član Slovenskega združenja korporativne varnosti

robot z le enim prijemalom izvede veliko različnih prijemov. To je pomembno zaradi več razlogov, med drugim gre za prihranek časa in denarja. Prijemala so pri robotiziranih procesih ključna.

Suhadolnik: Na Zarja Elektroniki imajo izkušnje z adaptivnim električnim prijemalom, ki smo ga izbrali tudi za naš projekt. To je velika prednost, saj z enakim prijemalom, kot bo uporabljeno v končnem laboratoriju, testiramo delo robota z različnimi prototipi komponent, ki jih razvijajo drugi partnerji iz Slovenije in tujine.

Ne gre za samo učečega robota?

Sušnik: V smislu razvoja koncepta, se ne uči sam. Gre pa za robota, ki bo glede na eksperimentalne parametre, ki jih vnese uporabnik ob željenem novonastalem materialu, sam izvedel proces. Šlo bo za začetno učenje robota, oziroma shranjevanja različnih procesov na novoodkritih materialih, iz katerih bo robot nato sam sestavil proces, s tem pa bo nastal material ali analiza, kot je bilo zahtevano iz strani uporabnika oz. naročnika.

Suhadolnik: Trenutni avtonomni sistemi na trgu so veliko manj avtonomni od tistega, ki ga bomo imeli že v prvi fazi projekta. Gremo po korakih. Strojno učenje in umetna inteligenca bosta v kasnejšem obdobju prav tako pripomogla k uresničitvi zastavljenega cilja.

Rezultat projekta in sodelovanja bo postavitev enega najsodobnejših raziskovalnih laboratorijev na svetu, kar nam bo omogočilo odlično razumevanje procesov odkrivanja nanostrukturnih materialov in mehanizmov delovanja razvitih materialov. Razvoj bo v novem laboratoriju občutno hitrejši.

Kaj je končni cilj IJS s tem sistemom?

Suhadolnik: Cilj inštituta je postaviti nov način znanstvenega raziskovanja, ki deluje. To pomeni, da smo hitreje in z več razumevanja sposobni razviti nove materiale, kakor na stari način. Potem bomo s partnerji videli, ali bi lahko podobne sisteme ponudili tudi drugim. Dobro delujoči razviti materiali bodo z novim sistemom enostavno in veliko hitreje preneseni v industrijo, saj bomo imeli vse ključne podatke o vseh parametrih sinteze in karakterizacije. Zdaj velja, da traja 20 let, da razviješ nek material in ga potem vgradiš v del ali napravo, medtem ko bi po novem celoten proces trajal do dve leti. Od začetka, pa do tega, da je material uporabljen v industrijski proizvodnji.

V kateri fazi projekta ste zdaj in kako gotovi ste, da bo ta uspel?

Suhadolnik: Konceptualna zasnova laboratorija je že v celoti zaključena. Zaključili smo fazo razvoja komponent , zdaj smo že globoko v fazi konkretne implementacije in sem prepričan, da bo laboratorij za avtomatizirano raziskovanje v prihodnjem letu polno funkcionalen. Res pa je, da bo potrebno še veliko sprotne optimizacije, ker gre za kompleksen projekt z veliko komponentami, ki jih je potrebno združiti v koherentno celoto.

In kaj sledi temu?

Suhadolnik: Potem bomo izvajali eksperimente in hkrati nadgrajevali sistem. Na IJS bi radi postavili veliko večji laboratorij za avtonomno raziskovanje. To nam bo omogočalo, da bomo lahko izva-

Postavitev najsodobnejšega laboratorija je močno povečala prepoznavnost Instituta Jožef Stefan in zelo pripomogla k uspešnemu pridobivanju evropskih sredstev, kar je pomemben vir financiranja Odseka za nanostrukturne materiale.

jali še več raziskovalnih procesov. Na ta način bomo lahko znatno pospešili in diverzificirali razvoj visoko-funkcionalnih materialov za napredne bodoče tehnologije. Za zdaj se bomo osredotočili zgolj na elektro-katalitične in foto-katalitične aplikacije, denimo za razgrajevanje onesnažil, in na vse reakcije, ki potekajo v elektrolizerju. Kasneje bi radi pripravljali tudi nanostrukturne prahove, in ne le imobiliziranih katalizatorjev.

Kaj bo naslednji korak Zarje?

Sušnik: Čeprav je naša osnovna dejavnost tehnična zaščita, bi se radi dokazali tudi na področju razvoja avtomatiziranih tehnologij. S tem še bolj vstopamo v razvojno okolje in bi lahko sodelovali pri avtomatizacijah določenih procesov v podjetjih. Imamo znanje in izkušnje, danes pa konec koncev vse stremi k avtomatizaciji in digitalizaciji. S tem kompleksnim projektom bomo pridobili tudi sami marsikatero izkušnjo in dodatno znanje, da bomo lahko pohitrili tudi katerega od naših trenutnih procesov.

Torej po proizvodnji tiskanih vezij razvijate še eno novo vejo vašega poslovanja?

Sušnik: Tako je. Proizvodnjo tiskanih vezij smo sicer pred leti razvili za lastne potrebe, zdaj pa sodelujemo tudi z zunanjimi naročniki. Zaenkrat to storitev nudimo zgolj partnerjem, s katerimi sicer tesno sodelujemo. Glede na večje povpraševanje, bo potrebno zmogljivosti povečati, obenem pa bomo najverjetneje šli tudi v smer, da drugim nudimo testiranje vezij, ki jih kupijo na trgu. V zadnjem času se namreč pojavlja vse več ponaredkov elektronskih komponent. Je pa to vsekakor odločitev našega vodstva in lastnikov podjetja.

Kakšen pa bo naslednji skupni korak?

Suhadolnik: Zarja Elektronika bo pomemben partner pri uresničitvi postavitve želenega večjega prostora na IJS za razvoj več vrst materialov. Skupaj bomo delali tudi na vzpostavljanju novih tehnologij in novih procesov. Prijavljali bomo projekte, da pridobimo evropska sredstva, s katerimi bomo financirali nadaljnji razvoj.

Kaj je bil sicer do zdaj največji izziv pri projektu?

Suhadolnik: Kako zagotoviti, da bo sistem res univerzalen. To smo rešili s pomočjo avtomatskega menjalnega mehanizma robotskih prijemal. Izzivi so sicer na vseh področjih razvoja avtomatiziranega laboratorija, med drugim tudi pri razvoju posebne priprave za odpiranje vial, priprave za odpiranje škatlic za vzorce, pri zaznavanju nivoja tekočine pri avtomatskem pipetiranju, pri razvoju elektrokemijskih celic, itn.

Sušnik: Celotni sistem bo vseboval veliko število kontrol pri vsakem procesu, tudi na prijemalih in posebej razvitih pripravah za robota. Obenem celotni razvoj strmi k optimizaciji robotske manipulacije, in zato sistem načrtujemo tako, da sama prijemala optimiziramo, da lahko opravljajo več funkcij ter skrbimo, da bo robot opravljal samo ključne funkcije. Menim pa, da bo strojni vid nepogrešljiv del procesa, a hkrati tudi najbolj kompleksen. ■

Foto: arhiv Zarja Elektronika d.o.o.

ZARJA ELEKTRONIKA

Varno v nov dan.

- razvoj
- inženiring
- proizvodnja
- projektiranje

sistemov za tehnično varovanje

60 LET TRADICIJE

www.zarja.com

Avtorica: mag. Ana Robnik / svetovalka za raziskave in strateški razvoj, Iskratel, d.o.o., Kranj*

DRŽAVE EU PRI UVAJANJU SISTEMA JAVNEGA OPOZARJANJA VODITA SKRB ZA DOBROBIT DRUŽBE IN TRAJNOSTNA NARAVNANOST REŠITVE

Cel niz groženj ima izjemno velik vpliv na javno varnost, zaščito in reševanje, zato je EU sprejela normativno podlago za uvedbo Sistema javnega opozarjanja (angl. Public Warning System s kratico PWS) v državah Evropske unije do 21. junija 2022.

Uvod

Svetovna skupnost, države in njihove povezave se vse pogosteje soočajo z raznorodnimi oblikami groženj, od vse obsežnejših in pogostejših naravnih nesreč kot so požari, poplave, velika neurja in potresi, do terorističnih in ostalih digitalnih napadov, izbruhov bolezni in virusnih pandemij, do dogodkov z množično udeležbo, industrijskih in drugih nesreč, ki jih povzroči človek ali stroj. Takojšnje opozarjanje državljanov, prebivalcev, obiskovalcev in turistov v določenih geografskih področjih na prihajajoče in nastale nesreče večjega ali manjšega obsega skupaj z jasnimi navodili za ukrepanje, rešuje življenja in blaži posledice udejanjenih groženj.

O zakonodajnih in regulatornih okvirih Sistema javnega opozarjanja

Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta [ref. 1] z dne 11. decembra 2018 je vzpostavila prenovljen Evropski zakonik o elektronskih komunikacijah, ki v svojem 110. členu opredeljuje Sistem javnega opozarjanja. S tem je zakonsko predpisan sodoben način javnega opozarjanja, kjer morajo imeti javni organi v vseh državah članicah možnost pošiljanja javnih opozoril na mobilne naprave ljudi, na določenem območju, z uporabo javno dostopnih elektronskih komunikacijskih storitev, ki jih ponujajo mobilni operaterji in ostali ponudniki elektronskih storitev. Ta opozorila morajo biti razumljiva, nedvoumna in jasna ter povezana z navodili, kako ravnati pred, med ali po nastalih nesrečah, torej taka, da jih vsak z lahkoto sprejme, razume in se po njih ravna. Poleg opozarjanja na mobilnih in stacionarnih elektronskih napravah so ponekod na voljo klasični kanali opozarjanja, kot so sirene, radio, televizija, družbeni mediji in drugi.

Skladno z obvezo iz 110. člena je Organ evropskih regulatorjev za elektronske komunikacije BEREC po posvetovanju z organi, ki so odgovorni za centre za obveščanje, do 21. junija 2020 objavil smernice [ref. 2] o tem, kako oceniti, ali je učinkovitost sistemov javnega opozarjanja iz drugega odstavka 110. člena (označimo jih 110(2)-PWS) enakovredna učinkovitosti sistemov iz prvega odstavka 110. člena (označimo jih 110(1)-PWS). V dokumentu je navedeno, da med 110(1)-PWS potencialno spadata tudi tehnologija oddajanja prek mobilnih baznih postaj (angl. Cell Broadcast s kratico CB) po standardu EU-ALERT (ETSI TS 102 900) in tehnologija pošiljanja kratkih sporočil na podlagi lokacije končne naprave (angl. Location Based SMS s kratico LB-SMS). V 110(2)-PWS so vključene aplikacije, ki temeljijo na storitvah dostopa do interneta

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

(angl. Internet Access Service PWS z oznako IAS-PWS). Če se bralec želi seznaniti s tehnološkimi rešitvami pošiljanja javnih opozoril, torej s komunikacijskimi kanali, so v dokumentih [ref. 2, 8] na pregleden način obravnavane tehnologije CB, LB-SMS in IAS-PWS(aplikacije) in druge. V tabeli [ref. 7] so navedeni primerjalni kriteriji, na podlagi katerih so ocenjene posamezne tehnološke rešitve CB, LB-SMS in IAS-PWS (aplikacije). Tehnologija CB zahteva najmanj dodatnih aktivnosti pri uporabnikih, je standardizirana in skladna z GDPR, vendar uporabniška izkušnja ni običajna. LB-SMS ne zahteva dodatnih aktivnosti pri uporabnikih, zahteva SIM kartico, ni povsem skladna z GDPR in lahko povzroča prezasedenost omrežja, vendar pa je uporabniku izkušnja rabe znana in domača. Aplikacije so po lastnostih bližje LB-SMS kot CB, vendar pri uporabnikih zahtevajo dodatne aktivnosti v zvezi z nadgradnjami in stalno rabo.

Slovenija je bila zavezana prenesti Evropski zakonik o elektronskih komunikacijah v Zakon o elektronskih komunikacijah ZEKom-2 [ref. 3]. Pripravljeni predlog je bil posredovan v obravnavo na Vlado RS in v času priprave tega prispevka postopek na Vladi RS še ni zaključen. V 201. členu ZEKom-2 so določene obveze za izvajalca javno dostopnih mobilnih medosebnih komunikacijskih storitev na podlagi številke. Navedimo še nekaj pomembnejših dejstev, ki izhajajo iz predloga ZEKom-2 v povezavi s Sistemi javnega opozarjanja:

- pri prenosu 110. člena v ZEKom-2 se uporablja pojem javno obveščanje in alarmiranje in ne pojem javno opozarjanje. Utemeljitev rabe pojma javno obveščanje in alarmiranje je povezana z zahtevo po skladnosti z ostalo področno zakonodajo, kot je Uredba o organizaciji in delovanju sistema opazovanja, obveščanja in alarmiranja;
- pomembni kriteriji obveščanja in alarmiranja v primeru naravnih ali drugih nesreč so zagotovo hitrost, zanesljivost in doseg;
- v skladu z načelom tehnološke nevtralnosti način pošiljanja javnih opozoril, oziroma izbrana tehnologija, v predlogu zakona ni določena;
- izvajalcem iz 201.člena je prepuščena izbira izmed možnosti, ki omogočajo izpolnitev obveznosti (npr. »cell broadcast«, »location based SMS«), oziroma kombinacija različnih tehnoloških rešitev;
- platforma, ki jo je obvezana vzpostaviti Uprava Republike Slovenije za zaščito in reševanje (URSZR), omogoča priključitev različnih vmesnikov in je, kot taka primerna za uporabo različnih tehnoloških rešitev.

Tehnološki in ostali aspekti pri uvajanju PWS

Z zornega kota tehnološke naprednosti razvrščamo sisteme za javno opozarjanje v tri generacije:

- starejši sistem (angl. legacy-PWS), ki temelji na analognih napravah, kot so sirene, megafoni in podobno, te naprave so v nekaterih evropskih državah že prepovedane ali v opuščanju;
- sodoben sistem (angl. Electronic Communications Service PWS z oznako ECS-PWS), ki temelji na elektronskih komunikacijskih storitvah in uporabi mobilnih naprav,
- izboljšan sistem (angl. enhanced PWS z oznako ePWS), kjer bodo standardizirane razširitve omogočale sprejem opozoril tudi na ostalih mobilnih napravah, kot so pametne ure in druge nosljive naprave.

Kot je navedeno v predstavitvi [ref. 5], je pri uvajanju PWS potrebno upoštevati naslednje aspekte:

- tehnološki aspekt, kjer ostaja izziv koordinacije tehnoloških rešitev, ki so sicer vse bolj učinkovite in hitre, vendar je potrebno le-te uskladiti znotraj večkanalne in enotne platforme;
- človeški aspekt, kjer je še vedno izziv prilagoditev varnostnih navodil potrebam ljudi in njihovemu razumevanju situacije;
- kontekstualni aspekt, kjer je izziv prilagoditev tehnologije na tip dogodka in na ciljno javnost;
- strukturni aspekt, kjer je izziv prilagoditev tehnologije za vsako organizacijsko obliko in vsako državo, pri čemer je potreben ustrezen čas, da se tak sistem dejansko pripravi.

Pregled implementacije po državah EU

Po pregledu stanja v zvezi z implementacijo različnih tehnologij po državah Evropske unije iz junija 2021 [ref. 6] in po podatkih, ki so na voljo na domačih straneh posameznih držav, lahko zaključimo z oceno, da sta tehnologiji CB in LB-SMS približno enako zastopani po državah, aplikacije pa so primarni komunikacijski kanal le na Finskem in v Nemčiji, v ostalih državah pa so pomemben sekundarni komunikacijski kanal. Tudi v Nemčiji so po katastrofalnih poplavah sprejeli zakon, ki uvaja CB.

Literatura in viri

- Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah.
- BEREC Guidelines on how to assess the effectiveness of public warning systems transmitted by different means.
- ZEKom-2: Zakon o elektronskih komunikacijah – 2.
- Domača stran Uprave Republike Slovenije za zaščito in reševanje pod vsebinskim področjem "Opazovanje, obveščanje in alarmiranje".
- Way to Go. Combining Technical, Human, Contextual and Structural Aspects for Effective National IPAWS, Johnny Douvinet, University of Avignon, France, EENA Webinar about Public Warning Systems 8.12.2020.
- Twit Johnny Douvinet "We have just completed the review of Public National Warning Systems in Europe currently deployed (June 2021)".
- Twit Ricardo Saraiva Cell Broadcast vs SMS Broadcast (LB-SMS) vs Mobile APP.
- EENA, dokument Public Warning Systems, update 2019. ■

Avtor: doc. dr. Brane Bertoncelj / Slovensko združenje za korporativno varnost

NOTRANJA PREVARA: KAKO ZMANJŠATI NJENO VERJETNOST

Mednarodni teden ozaveščanja o prevarah, letos v novembru v Sloveniji obeležujemo že četrtič, s sloganom "Skupaj v boju proti prevaram". Obravnava zlasti notranjih prevar je zelo aktualna, saj se te dogajajo v velikih, srednjih ali malih organizacijah, v različnih panogah in geografskih lokacijah. Notranja prevara lahko povzroči velike finančne izgube[1], pravne stroške in uniči ugled organizacije.

Uvod

Možnosti za prevare so brezmejne, omejene so le z domišljijo zaposlenega, motivom in priložnostjo, zato notranje prevare ne smemo utemeljevati z njeno verjetnostjo, da se bo nekaj zgodilo, ampak z možnimi posledicami. Razprava o notranji prevari (predvsem kako zmanjšati njeno verjetnost) postaja vse bolj interdisciplinarna, saj je lahko obravnavana iz različnih družbenih pogledov.

Notranja prevara ima izrazito negativen vpliv na vodstvo organizacije, lastnike, pristojne državne organe, borzo in na zaposlene (zlasti povečanje kontrole in nadzora poslovnih procesov, delovni pritisk, vpliv na produktivnost), na organizacijsko kulturo organizacije ter na podobo organizacije v javnosti. Notranja prevara je zmnožek vsaj treh dejavnikov: (i) motivirani storilec, (ii) materialni vidik škodnega dogodka in (iii) odsotnost nadzora, ki posledično omogoči deviantno vedenje zaposlenega. Menim, da je notranjo prevaro lažje preprečevati kot odkriti in nato pravno sankcionirati.

Tveganja zaposlenega

Obravnava tveganja zaposlenega ni nova, se pa je zaradi novih poslovnih strategij organizacij, zmanjševanja stroškov poslovanja, poslovnih in varnostnih zahtev ter škodnih dogodkov v zadnjem obdobju zanimanje za navedeno področje dramatično povečalo.

Pri ocenjevanju izpostavljenosti tveganju zaposlenega se preverja tudi: (i) možnost izkoriščanja slabosti v sistemu notranjih kontrol, (ii) možnost izogibanja aktivnostim vodstvenega nadzora in (iii) možnost prikritja kaznivega dejanja.

Motiv za notranjo prevaro

Motiv je psihološki nagib, iz katerega se stori kaznivo dejanje notranje prevare. To je tisto, kar v zaposlenem spodbuja, izzove ali opraviči kaznivo dejanje prevare, oziroma tisto, kar zaposlenega vodi, da stori navedeno kaznivo dejanje. V večini primerov je temeljni motiv, zaradi katerega se zaposleni odloči za prevaro, pridobitev denarja ali drugih materialnih sredstev in dobrin. Objektivno gledano je nezakonito pridobivanje premoženjske koristi, s stališča zaposlenega protipravno, subjektivno pa je lahko zaposleni prepričan, da ima "pravico" pridobiti nekaj od organizacije v zameno za svoje delo (morda slabo plačano).

Obravnava tveganja zaposlenega ni nova, se pa je zaradi novih poslovnih strategij organizacij, zmanjševanja stroškov poslovanja, poslovnih in varnostnih zahtev ter škodnih dogodkov v zadnjem obdobju zanimanje za navedeno področje dramatično povečalo.

[1] Stroški neposrednih škod so preko 3,6 milijarde $ v letu 2020, ACFE, Association of Certified Fraud Examiners.

Obstaja t. i. “trikotnik prevar” (nekateri govorijo tudi že o štirikotniku prevar). S tem modelom je možno preveriti ali obstaja povezava med individualnim in korporativnim vedenjem. Elementi trikotnika so: (i) priložnost, (ii) pritisk in (iii) racionalizacija (nekateri dodajajo tudi razvade).

Racionalizacija je ključni sestavni del večine notranjih prevar, saj storilec potrebuje uskladitev svojega ravnanja s splošno sprejetimi predstavami o etiki, morali, spodobnosti, lojalnosti in zaupanju. Nekateri primeri racionalizacije so:

- »Ne vem, da je to dejanje res škodljivo«,
- »Res potrebujem ta denar in ga bom vrnil, ko dobim plačo«,
- »Verjamem, da bom denar vrnil«,
- »Drugi zaposleni so še več ukradli«,
- »Ukradeni denar sem si zaslužil«,
- »Nihče od sodelavcev ni bil pri tem prizadet«,
- »Ne morem si privoščiti, da bi izgubil: dom, avto, vse!«.

Storilec

Obstajajo vsaj tri skupine storilcev, in sicer: (i) zaposleni, ki ima vrojeno težnjo po goljufanju in notranji prevari, (ii) zaposleni, ki je v bistvu pošten, vendar zaradi določenih zunanjih okoliščin ali pritiskov stori kaznivo dejanje, (iii) največji delež zaposlenih pa zaradi delovnih pogojev ali odnosov racionalizira svoje neetično vedenje (npr. neprimeren oseben dohodek, premestitev, neprimerni disciplinski ukrep, slabi delovni pogoji, neprimerno vedenje nadrejenega ipd.).

Storilec notranje prevare deluje “znotraj varnostnega sistema” organizacije (zunanji storilec prevare ima bistveno težje delo za storitev kaznivega dejanja). Ima pooblaščen dostop do njenega premoženja in varnostna polja, pristopno pravico za vstop v informacijski sistem, strokovno znanje, pozna poslovne procese, ima prijatelje in zaupnike.

Model preprečevanja notranjih prevar

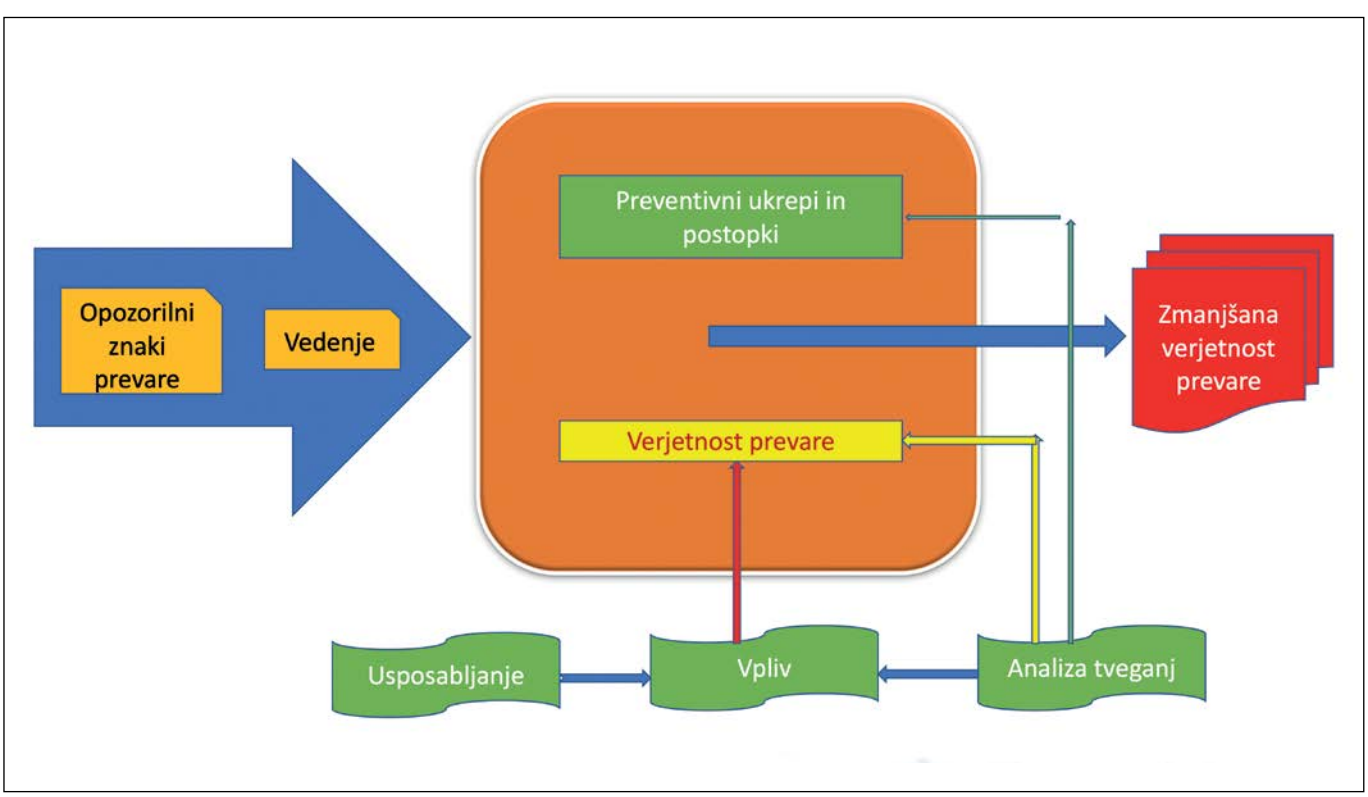
Menim, da obravnavanje preprečevanja notranjih prevar zahteva interdisciplinarni pristop, saj so za obravnavanje tega problema potrebna tako družboslovna kot tudi znanja s področja korporativne varnosti, tehnična znanja in izkušnje (dobra in slaba praksa).

Verjetnostna analiza je eno od možnih orodij za proučevanje preprečevanja prevar. V tem okvirju se ugotavlja, kateri so (i) opozorilni znaki prevare (razni možni scenariji prevar), (ii) kako verjetno je, da jih opazimo (zaznamo neobičajno vedenje zaposlenega v določenem časovnem intervalu) in (iii) kako velike so lahko njihove posledice (neposredna in posredna materialna škoda, izguba ugleda, notranji problemi v organizaciji ipd.).

Kot prispevek k obravnavi navedenega področja na spodnji sliki prikazujem lastni model preprečevanja notranjih prevar.

Model po eni strani obsega vhodne podatke (možni opozorilni znaki notranje prevare in vedenje zaposlenega). Na drugi strani je skupni vpliv navedenih komponent povezan z anali-

Model preprečevanja notranjih prevar:



zo tveganj, ki je soodvisna od vpliva usposabljanja zaposlenih, verjetnost storitve kaznivega dejanja zaposlenega in vpliva preventivnih ukrepov**,** ter postopkov na zmanjšanje verjetnosti notranje prevare. Osrednji del modela je označen kot verjetnost notranje prevare zaposlenega, ob "preboju" (premajhne učinkovitosti) preventivnih ukrepov in postopkov se izhod (rezultat) iz modela odraža v skupni oceni verjetnosti prevare.

Posamezni deli modela vsebujejo naslednje indikatorje.

Opozorilni znaki notranje prevare
Opozorilni znaki storilca so lahko: življenje nad svojimi finančnimi možnostmi, finančne težave (npr. visok osebni dolg ali kreditne težave ipd.), je vpleten v goljufije s posojili, ima visoko hipoteko, špekulira na borzi, je pohlepen, ima nenavadne sorodstvene, prijateljske povezave s strankami, ima družinske ali zdravstvene težave, se je ločil, je zasvojen z igrami na srečo, drogo, alkoholom, je manično depresiven, je psihopatska osebnost, kriminalna dejanja v preteklosti, giblje se v dvomljivi družbi, se neprimerno obnaša v socialni okolici (npr. izposoja si denar ipd.), spremenil je življenjski slog (npr. nabava dragega avtomobila, morskega plovila, izgradil je luksuzno hišo, nosi drag nakit in oblačila ipd.), nastopile so nepričakovane vedenjske spremembe.

Znaki prevare za vodstvo organizacije: koruptivni postopki, pomanjkanje ločitve nalog na kritičnih poslovnih procesih, vodstvo je pogosto v sporu z revizorjem, decentralizacija poslovanja brez ustreznega nadzora, obstaja šibko okolje notranjih kontrol, sredstva organizacije se prodajajo pod tržno vrednostjo, visoka fluktuacija zaposlenih (zlasti na tistih področjih, ki so bolj dovzetna za notranje prevare), izplačane odškodnine so v nesorazmerju s stanjem na trgu, sklepanje sumljivih servisnih pogodb, manjka pomembna poslovna dokumentacija ipd.

Znaki prevare za zaposlene v nabavi: povečanje števila pritožb glede kvalitete proizvodov ali storitev, povečana nabava sredstev, njihova prodaja pa se ni povečala, nenormalen popis sredstev za nabavo (ki niso potrebna za poslovanje), pomanjkanje fizične varnosti nad sredstvi / inventarjem, izplačila stroškov brez ustreznega dokumenta ali pravne podlage, plačila dobavitelju, ki ni na odobrenem seznamu dobaviteljev, velik obseg nabav pri novih dobaviteljih, netransparentna nabava, dobavitelji so brez fizičnih naslovov, naslov dobavitelja se ujema z naslovom zaposlenega ipd.

Posebno obravnavo zahteva vprašanje percepcije opozorilnih znakov notranje prevare. To je kognitivni proces, pri katerem zaposleni interpretira podatke in informacije iz poslovnega okolja in si na njihovem temelju oblikuje lastno sliko o tem okolju. Problem se pojavi, ko se percepcija razlikuje od objektivne stvarnosti (lahko sledijo lažne ovadbe ali anonimna pisma ipd.). Percepcijo opozorilnih znakov prevare dodatno otežuje pretirana prepričanost o pravilnosti lastne sodbe. Taka pretirana prepričanost je lahko nevarna, saj kaže na pogosto nezavedanje nevarnosti in škodljivosti notranje prevare za poslovanje organizacije.

Aktivnosti za preprečevanje prevare so pretežno prostovoljna dejanja, pri katerih sta ključna pojma "pripravljenost in volja nekaj dobrega delati za organizacijo", da ne bi prihajalo do nezaželenih posledic. Za učinkovito preprečevanje notranje prevare pa moramo imeti vizijo za prihodnost, kot strokovni izziv. Kaj lahko naredimo? Zmanjšajmo tveganje, povečajmo odpornost.

Vedenje

Kateri dejavniki so najpomembnejši za razumevanje in napovedovanje vedenja? Univerzalnega odgovora na to vprašanje ni in presega obseg članka.

Osveščanje in usposabljanje zaposlenih za preprečevanje prevar

Za ustrezno pripravljenost na notranjo prevaro je pomembno tudi osveščanje in usposabljanje zaposlenega. Ta zajema niz profesionalnih znanj in veščin, ki imajo zlasti dva cilja: (i) omogoča zaposlenemu, da prepozna opozorilne znake notranje prevare in o tem obvesti pristojne nadrejene, (ii) je psihološke narave: zaposleni, ki se zaveda svojih obveznosti in moralno-etičnih norm, pozna potrebne ukrepe in postopke, ki jih mora opraviti v primeru prevare, bo v navedenih razmerah lažje obvladal psihološki pritisk, dvom in strah. Gre za situacijo, s katero se običajno ne soočamo, zato je ni mogoče upravljati na rutinski način.

Analiza tveganja zaposlenih

V razvitem svetu postopno vse bolj prodira spoznanje, da so v sodobnih pogojih poslovanja na eni strani glavna konkurenčna prednost organizacij njihovi zaposleni, na drugi strani pa predstavljajo veliko tveganje, zato je razumljivo, da se za upravljanje tega področja vzpostavlja varna kadrovska politika. Brez tveganja bi bilo vse vnaprej jasno in tako bi bili vsi dogodki pri poslovanju odvisni le od sosledja vzrokov in posledic.

Verjetnost notranje prevare

Tradicionalno pojmovanje verjetnosti prevare vključuje predvidevanje, da se bo prevara zgodila, njena škoda in možni časovni interval med dvema dogodkoma. Razprava o teoriji verjetnosti, teoriji zanesljivosti in teoriji odločanja presega obseg članka.

Preventivni ukrepi in postopki

O preventivi se v zadnjem obdobju veliko govori. V poplavi besed je težko izluščiti tiste ukrepe in postopke, ki največ prispevajo k preprečevanju možne notranje prevare oziroma k ublažitvi njenih posledic. Menim, da je treba pri tem izhajati iz pripravljenosti na možne najtežje oblike. Neposredni cilji preventivnega delovanja naj bodo usmerjeni v:

- identificiranje slabosti, pomanjkljivosti in občutljivosti pri poslovanju organizacije z vidika možnosti za notranjo prevaro,
- načrtovanje in razvijanje odzivov na notranjo prevaro,
- pripravi "scenarijev" zaznavanja in odzivanja (določanje odgovornosti posameznih strokovnih služb organizacije),
- usposabljanje zaposlenih in njihovo osveščanje za preventivne aktivnosti ter tudi za ustrezno delovanje v primeru prevare.

Zaključek

Potrjuje se teza, da smo vstopili v zelo občutljivo obdobje tveganj notranje prevare, ki so vgrajena v koncept razvoja socialne, pravne in gospodarske dejavnosti družbe. Iz statističnih podatkov (ACFE, 2020) je odkrita notranja prevara dostikrat le "vrh ledene gore", saj obstaja velika verjetnost storitve še več drugih kaznivih dejanj v organizaciji. Velikokrat ne gre za zgolj enkratno aktivnost, ampak se nedopustno ravnanje zaposlenega, kot storilca notranje prevare, ponavlja. Osnovna podmena za ocenjevanje verjetnosti notranje prevare je, da morajo biti obrambne linije organizacije, pravila poslovanja, delovni postopki, notranja kontrola in računalniška tehnologija dovolj vzdržljivi, da se lahko uprejo številnim "neprimernim" posegom zaposlenega, bodisi naključnim ali zlonamernim. Navedeno ocenjevanje pa zahteva presojo verjetnostne narave poslovnega okolja in procesov ter zmožnost deduktivnega razmišljanja o malo verjetnih, toda pomembnih odklonskih dogodkih pri poslovanju.

Aktivnosti za preprečevanje prevare so pretežno prostovoljna dejanja, pri katerih sta ključna pojma "pripravljenost in volja nekaj dobrega delati za organizacijo", da ne bi prihajalo do nezaželenih posledic. Za učinkovito preprečevanje notranje prevare pa moramo imeti vizijo za prihodnost, kot strokovni izziv. Kaj lahko naredimo? Zmanjšajmo tveganje, povečajmo odpornost. ■

13. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 24.—25. MAJ 2022

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!

Avtorja: Andrija Pušić in Matjaž Zupan / Špica international d.o.o.*

TRANSFORMACIJA UPRAVLJANJA ALARMOV

Na področju upravljanja alarmov je pred nami nekaj zares razburljivih trenutkov. Senzorji postajajo brezžični in povezani neposredno v oblak, mobilni telefon pa je naša »nova normalnost« kot platforma za upravljanje. Vse to močno vpliva na način, kako zaznavamo, distribuiramo in upravljamo alarme.

Celotno področje varnostnih alarmov je bilo vse do danes nekako zaščiteno pred vplivom mobilne revolucije, ki je zajela drugi dve področji tehničnega varovanja – kontrolo pristopa in videonadzor. Morda je temu tako, ker se obstoječa tehnologija, čeprav sorazmerno nizko tehnološka, dobro ujema z obstoječim modelom upravljanja alarmov in obstoječim poslovnim modelom varnostnih podjetij, ki upravljajo alarme kot storitev.

Običajno gre takole - alarm se sproži, in signal potuje po namenski liniji v nadzorni center varnostnega podjetja. Dežurni varnostnik običajno ukrepa tako, da pokliče stranko in po potrebi napoti intervencijsko ekipo na določeno lokacijo. Tak način upravljanja alarmov deluje odlično že leta, celo desetletja. Kakšne so torej sile, ki tičijo za novim pristopom in novo generacijo rešitev, ter kako močne so?

Oddaljeni nadzor

Začnimo z najbolj očitnim. Oddaljeni dostop in nadzor sta »novi normalnosti« za vse, kar je povezano s tehnologijo. Informacije smo navajeni prejeti takoj. Torej takoj, ko se določen dogodek zgodi. In ne želimo se odpraviti na pot samo zato, da bi na neki oddaljeni lokaciji aktivirali krmilnik ali izklopili alarm. Vse želimo narediti od tukaj in zdaj.

Mobilni telefon

In ravno zato je mobilnost neizogibna. Včasih smo se šalili, da imamo mobilno aplikacijo za vse. To ni več šala. Zdaj imamo mobilno aplikacijo dejansko za vse. Pravzaprav imamo zdaj na izbiro več mobilnih aplikacij za vse, tudi za dejavnosti kot je recimo sprehajanje pasjega ljubljenčka. Zato ni čudno, da želimo upravljati alarme tukaj, zdaj in s telefona.

Oblak

Prej ali slej se bo vse premaknilo v oblak. Nekateri razlogi so tako očitni, da jih lahko prepoznajo tudi tisti, ki niso blizu IT industriji. Na primer zahteve, kot so »brez strežnikov«, »brez licenc« ali »nič IT-ja«. Oblak je tudi ključnega pomena za širšo poslovno uporabnost mobilnih naprav, saj brez oblaka ne moremo več zagotavljati opravljanja določenih nalog od koder koli. Oblak in mobilni telefon tako postajata ena in ista stvar.

IoT (internet stvari)

Ko gre za senzorje in ostalo tehnologijo za zaznavanje vlomov, se v resnici ni spremenilo veliko. Nekaj nalog morda sedaj prevzame videonadzor (inteligentne kamere), a segment trga, ki temelji na poceni nizko tehnoloških senzorjih, ostaja skoraj enak. Novost je zgolj brezžično delovanje. V kombinaciji z vedno nižjimi cenami senzorjev in povezljivostjo interneta stvari lahko pričakujemo, da bo število senzorjev eksponentno raslo, in s tem soglašajo vse napovedi. Z velikim številom senzorjev pa postane ozko grlo njihovo upravljanje. Tega ni več mogoče izvajati ročno, ampak zahteva napreden avtomatiziran sistem upravljanja, ki temelji na pravilih. In obstaja samo ena rešitev za to zahtevo – oblak in mobilni telefon.

Decentralizacija

Centralni nadzorni sistem – CNS, se še spomnite? To je precej impresivna zadeva z vsemi temi velikimi zasloni, zaposlenimi operaterji, utripajočimi lučmi in rdečimi telefoni. Razen občutka, da ga ne potrebujemo več. Zahvaljujoč pande-

Celotno področje varnostnih alarmov je bilo vse do danes nekako zaščiteno pred vplivom mobilne revolucije, ki je zajela drugi dve področji tehničnega varovanja – kontrolo pristopa in videonadzor.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

miji so ljudje odkrili, da je mogoče marsikaj narediti tudi, če ne sedimo skupaj. Še posebej, če tehnologija podpira delo na daljavo, kar je seveda ena izmed osnovnih značilnosti rešitev v oblaku. Zato vstopamo v obdobje, ko vaša fizična lokacija ne bo več pomembna.

Porazdeljeno upravljanje

To nas pripelje do porazdeljenega upravljanja alarmov. Z rešitvami za sočasno upravljanje je mogoče potek dela poenostaviti, optimizirati in prenesti na posameznike z različnimi vlogami, dovoljenji, nalogami, dolžnostmi in odgovornostmi. Upravljanje si lahko delijo končni uporabniki in zunanji strokovnjaki. Tako so vsi v realnem času na tekočem, kljub različnim lokacijam in fizičnim razdaljam.

Integracija

Ko gre za integracijo, prinaša oblak nova pravila igre. Pričakuje se, da bodo aplikacije v oblaku ponujale API-je za integracijo, veliko lažjo in varnejšo metodo integracije kot zloglasni SDK-ji. Platforme za avtomatizacijo, kot je Zapier, gredo še dlje, saj ponujajo rešitve za integracijo brez ene same vrstice računalniške kode.

Integracija postaja velik strateški izziv – nujno potreben za sinhronizacijo s platformami za upravljanje identitete, logičnim dostopom, rešitvami SSO itd. Da sploh ne omenjamo integracije z video nadzornimi sistemi, aplikacijami za upravljanje delovne sile in celo različnimi rešitvami za kontrolo pristopa med seboj. Oblak naredi vse to cenejše in enostavnejše za razvoj, uvajanje, vzdrževanje in uporabo.

Transformacija upravljanja alarmov je torej sedanjost in ne prihodnost. Nove tehnologije so že na voljo, tako strojna oprema kot tudi programska, tako da nam manjka zgolj še miselni preskok in sprememba obstoječih poslovnih modelov.(tekst za okvir) Predvsem zato, ker na ta način zmanjšujemo stroške, izboljšujemo zanesljivost in razširjamo prilagodljivost tehničnega varovanja. ■

Transformacija upravljanja alarmov je torej sedanjost in ne prihodnost. Nove tehnologije so že na voljo, tako strojna oprema kot tudi programska, tako da nam manjka zgolj še miselni preskok in sprememba obstoječih poslovnih modelov.

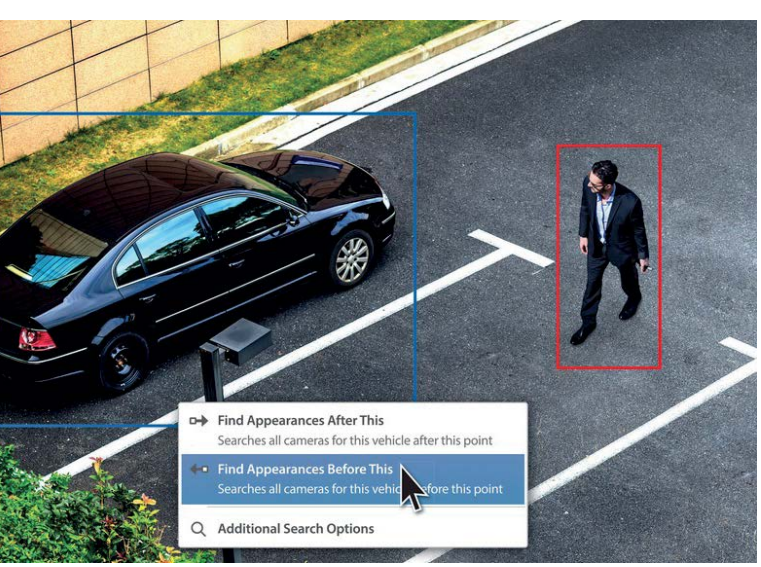
Avtor: Uroš Cvelbar / HSI d.o.o.*

VIDEO ANALITIKA V SODOBNIH VIDEO NADZORNIH SISTEMIH

V začetku leta 2021 je Elon Musk »presenetil« z najavo, da Tesla Model 3 in Model Y za avtonomno vožnjo ne bosta več imela vgrajen radar, saj prehajajo na »Tesla Vision« avtopilotni sistem, ki ga sestavljajo kamere, ki v realnem času analizirajo slike, ki jih nato semantično segmentirajo ter izvajajo zaznavo objektov in monokularno oceno globine. Ti podatki se nato prenašajo tudi v centralni podatkovni center, kamor se v realnem času stekajo podatki več kot milijon vozil. Na podlagi teh podatkov se izboljšuje algoritem, ki bo v prihodnosti omogočal popolno avtonomno vožnjo.

Tehnologija prepoznavanja objektov s kamerami je že kar nekaj časa dostopna tudi pri nekaterih vodilnih proizvajalcih video nadzornih sistemov. Analitika je usmerjena predvsem na zaznavo in razlikovanje med osebami in vozili (s podkategorijami, kot so kolesar, motorist, tovornjak...). Te informacije pa niso same sebi namen, temveč pripomorejo k hitrejši odzivnosti dogodkov v realnem času in znajo celo že predvideti nenavadne dogodke v prihodnosti.

Osnova delovanja te analitike je v prepoznavanju vzorcev (značilnosti posameznega objekta tako v statiki kot gibanju), ki se jih nato zapiše v binarni obliki. Ob tem pa ima tudi možnost (samo)učenja na način, da več kot različnih posameznih primerov vnesemo, večja je natančnost in hitrost delovanja sistema.



Varovanje zunanjega perimetra

Kamera, ki zanesljivo prepozna ljudi omogoča različne scenarije, ki povečajo varnost, saj imamo možnost uporabiti le te informacije v realnem času.

Varovanje zunanjega perimetra je bil vedno izziv predvsem zaradi objektivnih okoliščin zunanjega okolja (nizke/visoke temperature, dež, sneg, veter, živali...), ki vplivajo na lažne alarme. Lažne dogodke se danes sicer poizkuša verificirati preko video nadzornega sistema na način, da povežemo alarmni in video nadzorni sistem z PTZ kamero, ki se avtomatsko obrne proti sproženem predelu. Slabost tega sistema je, da kamera vedno lahko spremlja le en določen segment hkrati.

To nas pripelje do optimalne rešitve, ki pomeni uporabo video sistema z napredno analitiko. Le ta lahko zanesljivo loči osebe in vozila. Analitika se lahko izvaja na sami kameri ali na snemalniku.

S to rešitvijo lahko zelo enostavno pridobimo zunanjo cono varovanja objekta, ki se jo lahko poveže z obstoječim notranjim alarmnim sistemom, na način, da se zunanja cona avtomatsko vklopi z vklopom alarmnega sistema (lahko tudi z zamikom, po urniku ali končno upravljalno cono...).

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Alarmi se v realnem času pošljejo v nadzorni center, v varnostno službo ali celo na mobilni telefon uporabnika s tem, da vsi dobijo video verifikacijo dogodka z možnostjo takojšnjega ogleda žive slike in dodatno možnostjo avtomatske ali ročne sprožitve luči ali sirene oz. varnostnih elementov.

Video verifikacija alarmnih dogodkov pomeni, da za vsak posamezni dogodek, tudi če je lažen, varnostnik v realnem času odreagira situaciji primerno.

Ko to analitiko združimo s termalno kamero pa se nam odpre možnost uporabe v najbolj zahtevnih situacijah, kot je npr. varovanje državnih meja ali kritične infrastrukture, saj nam termalna kamera omogoča spremljanje situacije tudi v popolni temi in na zelo velikih razdaljah.

Iskanje incidentov po posameznih karakteristikah

Nadgradnja takega sistema je, da zna določiti tudi karakteristike posamezne osebe ali vozila, ki jih nato lahko iščemo po vseh kamerah, v celotnem video nadzornem sistemu, znotraj več lokacij. To nam omogoča, da npr. označimo osebo oz. vozilo in zahtevamo, da nam sistem pokaže to osebo oz. vozilo po vseh kamerah do tega trenutka (v primeru da gledamo živo slike) ali pa od določenega trenutka naprej (pri pregledovanju posnetkov od trenutka, ko npr. oseba vstopi na neko območje).

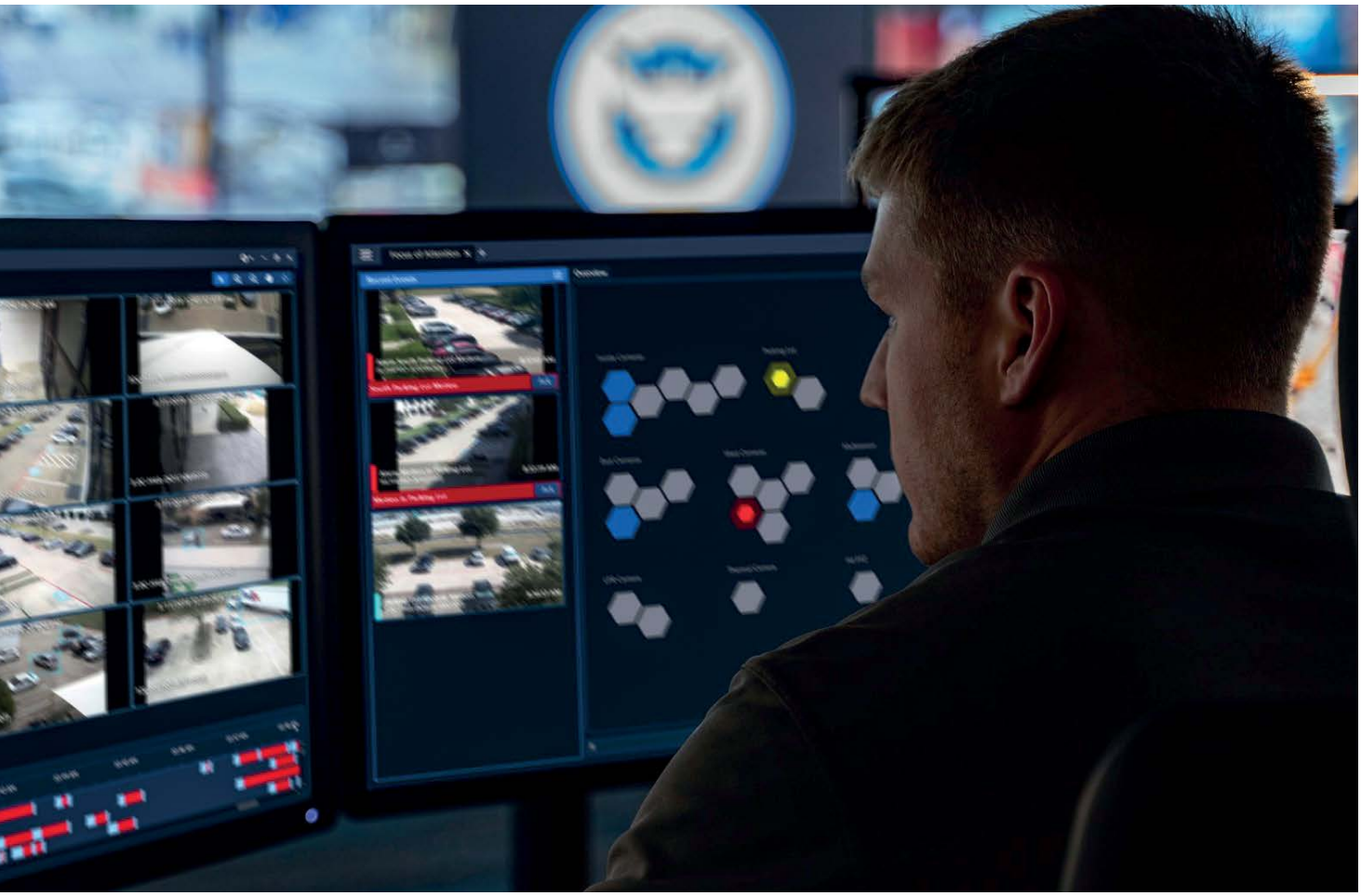
Opcijsko pa nam ta nadgradnja omogoča tudi, da iščemo direktno po karakteristikah, kot so spol, barva spodnjega ali zgornjega dela oblačil, barvi las in pod kategorijami vozil, kot so kolesar, motorist, tovorno vozilo in druga prevozna sredstva.

> Vsak varnostni sistem je uporaben, če na dogodek nekdo učinkovito in hitro odreagira. Sam video nadzorni ali alarmni sistem torej ni učinkovit brez hitrega ukrepanja.

Preprečevanje incidentov v prihodnosti

Razvoj video analitike je zelo hiter in danes že imamo proizvajalce, ki omogočajo preprečevanje neželenih dogodkov v prihodnosti. Recimo, da imamo kamero na letališču, ki med drugim pokriva tudi npr. električno omarico ali prezračevalni element, okoli katerega se običajno ljudje ne pojavljajo, saj hodijo po bližnjem stopnišču. Toda, ker se nenadoma na tej lokaciji pojavi človek, je to lahko že potencialen nenavaden dogodek, ki se v realnem času pošlje varnostnemu osebju, ta pa se nato odloči ali gre za varnostno sporen in nenavaden dogodek, ali pa gre morda le za serviserja prezračevalnega sistema.

Algoritmi delujejo na način, da so za kamero referenčni običajni dogodki, tisti, ki se dogajajo zadnjih štirinajst dni, v kolikor pa posamezni dogodek odstopa po lokaciji, smeri ali hitrosti, pa je to za sistem nenavadni dogodek, ki morda pot-



rebuje takojšnjo reakcijo (predvsem neobičajna hitrost ali smer) ali dodatno pozornost oz. varnostni operater odloči, da dogodek ni pomemben.

COVID-19 rešitve

Mnogi proizvajalci kamer so se odzvali tudi na COVID-19 situacijo, in sicer s pripravo sistemov za merjenje temperature preko termalnih kamer, katere so bile deležne tudi upravičene kritike, in sicer zaradi nenatančnega delovanja in celo algoritma, ki je popravljal vrednosti k običajni temperaturi. To je naredilo sisteme neuporabne oz. celo nevarne, hkrati pa sistemi, ki znajo dejansko natančno izvajati meritev zaradi »slabe reklame«, niso bili deležni ustrezne pozornosti. Te rešitve, ki dajejo zelo natančne rezultate merjenja telesne temperature prepoznate po tem, da je del sistema tudi »blackbox« to je referenčni izvor temperature, po katerem se kamera kalibrira v realnem času in pa funkcijo, da se temperatura meri v kantusu očesa, saj je to najbolj relevantna točka za zunanje merjenje telesne temperature.

Večina proizvajalcev omogoča tudi štetje oseb (npr. koliko oseb je trenutno v trgovini). Napredni proizvajalci pa omogočajo tudi, da kamere zaznajo ali osebe nosijo maske in celo v realnem času merijo razdaljo med dvema osebama (razdaljo se poljubno nastavi).

Seveda je ob vseh omenjenih rešitvah potrebno upoštevati tudi zakonodajo o varovanju osebnih podatkov in GDPR smernicah. Poleg utemeljitve uporabe posamezne rešitve je pomembno, da tudi sam sistem, ki ga uporabljamo, omogoča avtomatsko brisanje meta podatkov.

Vendar pa nam vsi možni alarmni dogodki, ki jih omenjamo, ne pomenijo veliko, v kolikor za njih nimamo izvedenega protokola o tem, kdo jih sprejme in kakšni so nadaljnji koraki ob posameznem dogodku oz. incidentu. Da se na incidente hitro in učinkovito odreagira, mora upravljalec razmisliti o interni nadzorni sobi, v kateri se zbirajo informacije iz vseh objektov in vseh sistemov tehničnega varovanja. Tak sistem se imenuje centralno nadzorni sistem (CNS) oziroma v angleškem jeziku Physical Security Information Management (PSIM). Tak sistem zagotavlja hiter pregled stanja nad vsemi objekti, tako v smislu video nadzora, pristopne kontrole, protivlomnih sistemov, sistemov za zgodnje odkrivanje požara, domofonskih sistemov, nadzor klimatov, UPS in drugih. Nadzornik, ki ima pregled nad sistemom PSIM, ima pregled tudi nad zemljevidi in tlorisi objektov, kjer se vizualno prikažejo spremembe stanja.

Nadzornik se na podlagi vseh sistemov, do katerih ima dostop, in na podlagi jasnih navodil o prioritetnih ukrepih, odloča in obvešča o situaciji in jo spremlja v realnem času.

Vsak varnostni sistem je uporaben, če na dogodek nekdo učinkovito in hitro odreagira. Sam video nadzorni ali alarmni sistem torej ni učinkovit brez hitrega ukrepanja. ■

Foto: Avigilon by Motorola

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

EC-Council CEH CERTIFIED

EC-Council ECIH CERTIFIED

OFFENSIVE security OSCP

ISO 27001

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

BUREAU VERITAS 1828

DPO

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

13. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 24. - 25. MAJ 2022

DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI