ODRŽANA KONFERENCIJA "IZAZOVI U ZAŠTITI INDUSTRIJE I INFRASTRUKTURE"

Zaštita kritične infrastrukture je izazovna, ali ostvariva!

U lipnju ove godine je finaliziran Prijedlog Zakona o KI. Riječ je o novim podzakonskim aktima, odnosno četiri Pravilnika: poslovi sigurnosnog koordinatora za KI; metodologija za izradu analize rizika poslovanja KI; klasificiranje podataka i kriteriji za određivanje stupnja tajnosti za podatke iz područja ZKI

Nataša Gajski Kovačić

U ORGANIZACIJI časopisa Zaštita, 27. i 28. listopada 2021. je u hotelu Westin u Zagrebu održana dvodnevna konferencija „Izazovi u zaštiti industrije i infrastrukture" na kojoj su stručnjaci iz Republike Hrvatske i inozemstva govorili o ključnim sigurnosnim izazovima s kojima se susreću u industriji i zaštiti kritičnih infrastruktura. U ime Ravnateljstva civilne zaštite i ravnatelja dr.sc. Damira Truta, sudionicima se pozdravno obratio načelnik Sektora za smanjenje rizika od katastrofa Dražen Štajduhar koji je govorio o prilagodbi nacionalnih zakonskih okvira u zaštiti kritičnih infrastruktura odredbama nove EU direktive o otpornosti kritičnih subjekata kako bi se postigla maksimalna kompatibilnost s modelima i rješenjima koja se propisuju i primjenjuju u Eu. Ravnateljica Uprave unutarnje plovidbe Ministarstva mora, prometa i infrastrukture Duška Kunštek rekla je da je nesmetano funkcioniranje cijelog niza usluga i kompleksnih sustava izuzetno bitno za održavanje normalnog svakodnevnog života i gospodarske aktivnosti o kojima ovisi dobrobit naših građan, pojašnjavajući da je posebno važno osigurati da najvažniji sektori budu zaštićeni na višoj razini te da se, i u slučaju krize, mogu oporaviti u najkraćem roku, bez ugrožavanja ostalih sektora.

Republika Hrvatska prepoznala je važnost kritične infrastrukture još kroz donošenje Zakona o kritičnim infrastrukturama 2013., a spomenuti Zakon prepoznaje sljedeće sektore: energetika, komunikacijska i informacijska tehnologija, promet, zdravstvo, vodno gospodarstvo, hrana, financije, proizvodnja, skladištenje i prijevoz opasnih tvari, javne službe, te nacionalni spomenici i vrijednosti.

„Ministarstvo mora, prometa i infrastrukture nadležno je za sektor prometa u cijelosti te za elektroničke komunikacije u sektoru komunikacijskih i informacijskih tehnologija", pojasnila je Kunštek i dodala kako ovako širok obuhvat različitih sektora zahtijeva i međuresornu suradnju koja se odvija uz koordinaciju Ministarstva unutarnjih poslova, odnosno Ravnateljstva civilne zaštite. „Kritična infrastruktura zauzima važno mjesto u Strategiji nacionalne sigurnosti Republike Hrvatske, gdje se naglasak stavlja na prevenciju, uklanjanje ili ublažavanje rizika koji mogu izazvati ranjivost kritičnih infrastruktura te jačanje njihove otpornosti.", rekla je ravnateljica Uprave unutarnje plovidbe te dodala kako se naglašava i važnost razmjene podataka između državnih tijela i agencija te operatora kritične infrastrukture o prijetnjama i rizicima.

Novi Zakon

„Ova konferencija predstavlja upravo jedan od oblika korisne razmjene iskustava, znanja i informacija. No, ne treba zaboraviti da se iskustva dijele i izvan granica Hrvatske, prvenstveno u sklopu NATO saveza i Europske unije", istaknula je ravnateljica Kunštek. U tom kontekstu,

spomenuto je i da s europske razine dolaze nove inicijative za poboljšanje regulative, a riječ je o Direktivi Europskog parlamenta i Vijeća o otpornosti kritičnih subjekata, kojom bi se revidirao dosadašnji pristup kritičnoj infrastrukturi. Govorila je i o sve većem značaju kibernetičke sigurnosti.

Kunštek se osvrnula i na temu samih ulaganja u prometnu infrastrukturu, gdje je predstavila primjer dobre prakse javno-privatnog partnerstva na projektu Zračne luke Zagreb te je spomenula i nekoliko projekata sufinanciranih iz sredstava EU, među njima i projekt uređenja vodnog puta Dunava kod Sotina. Realizacijom ovog projekta će se, uz najkritičniju dionicu za plovidbu, spriječiti i urušavanje obale uz koju se nalazi naselje Sotin. Ravnateljica Uprave unutarnje plovidbe istaknula je podršku Ministarstva ovakvim projektima te izrazila želju da konferencija pridonese daljnjem jačanju sigurnosti svih industrijskih sektora i povezane infrastrukture.

Državni tajnik u MORH-u Zdravko Jakop istaknuo je da je obrambenu perspektivu na području zaštite industrije i kritične infrastrukture kao jednu od temeljnih zadaće Hrvatske vojske. Civilnim institucijama je vojska potpora u situacijama u kojima je primjereno upotrebiti vojsku. „Vojska ima veliku ulogu u mirnodopskim uvjetima, a jedna od tih uloga je civilno-vojna suradnja i po pitanju kritične infrastrukture, a odnosi se na hitni medicinski prijevoz, zaštitu i spašavanje, poplave, potrese... Tijekom 2020. posebno je to došlo do izražaja za vrijeme pandemije i potresa kada je Hrvatska vojska imala ulogu u podizanju logističkih kampova za borbu protiv pandemije, a bili smo altivno uključeni i u otklanjanju razornih posljedica zagrebačkog i petrinjskoj potresa, ali i snimanje kritičnih infrastruktura i otklanjanje šteta. Zaštita infrastrukture nije primarna zadaće HV-a, ali je itekako prepoznata posebno kada je riječ o kibernetičkim i hibridnim prijetnjama", rekao je Jakop.

Izlaganje na temu Ususret novom Zakonu o kritičnoj infrastrukturi održala je voditeljica Odjela za kritičnu infrastrukturu i kulturnu baštinu Ivana Cesarec. Osvrnula se na KI u RH od 2013. do 2019. i Zakon o KI (2013.) te podzakonske akte i Direktivu Vijeća 2008/114/EZ. Rekla je da su uočeni određeni izazovi u provedbi (složenost; dinamika; koordinacija); da je došlo do institucionalnih promjena (MUP RCZ 2019. uspostava Odjela za KI i KB); ali i novih sigurnosnih prijetnji (kibernetičke prijetnje – NIS Direktiva);

U lipnju ove godine je finaliziran Prijedlog Zakona o KI. Riječ je o novim podzakonskim aktima, odnosno četiri Pravilnika: poslovi sigurnosnog koordinatora za KI; metodologija za izradu analize rizika poslovanja KI; klasificiranje podataka i kriteriji za određivanje stupnja tajnosti za podatke iz područja ZKI).

Svrha Zakona iz 2013. bila je uspostava normativnog okvira za izgradnju učinkovitog sustava ZKI koji osigurava odgovarajuću razinu zaštite; kontinuitet poslovanja; ograničava učinke prekida ili poremećaja u radu KI (na sigurnost, imovinu i okoliš, ekonomsku stabilnost, neprekidno funkcioniranje vlasti…). Svrha novog Zakona iz 2021. je potreba za usklađivanjem prema novim operativnim i zakonodavnim okolnostima i općenito promjenama u predmetnom području nakon sedam godina, „priprema" za daljnje faze na nacionalnoj razini nakon donošenja Popisa NKI, omogućavanje boljeg razumijevanja propisa, razmatranje mogućih izazova implementacije Izmjena. Upravo zbog većeg broja izmjena donosi se novi prijedlog Zakona, a ne Izmjene i dopune postojećeg.

RH uspješno usklađuje svoje zakonodavstvo s EU legislativom

Denis Čaleta iz instituta za korporativne sigurnosne studije je govorio o ključnim suvremenim izazovima u jačanju otpornosti zaštite kritične infrastrukture rekavši da je put koji se odnosi na stratešku razinu dugačak i pun nerazumijevanja. Osvrnuo se na primjer EU financiranih projekata na temu zaštite kritične infrastrukture. Naglasio je da je najveći problem kod stvaranja otpornosti prije svega u različitim razinama razumijevanja. Hrvoje Sagrak i Slavko Vidović iz tvrtke Infopdom govorili su o poslovnoj agilnosti naglasivši da je otpornost ovisna o razini poslovne agilnosti, a sama poslovna agilnost je programabilna kroz menedžerske mehanizme. Istaknuli su da je Udruga za promicanje pametnih industrija (Cro SI) koju je osnovao Infodom zajedno s pet fakulteta (FER, FOI, FSB, EFZG, EFDU) razvila pripadajuće modele i mehanizme otpornosti. „Upravljanje podacima je postalo sastavni dio menadžmenta organizacije. Zamislite banku gdje okolina prestaje vjerovati u nju, ona je gotova u jednom danu. Ako povjerenje nestaje, sve je prazno", rekao je Vidović

Dražen Ljubić iz Zavoda za informacijsku sigirnost govorio je o razvoju nacionalnih sposobnosti kroz usklađivanje nacionalne i EU legislative EU NIS Direktive, a čiji je cilj osigurati zajedničku razinu sigurnosti mrežnih i informacijskih sustava čije bi neispravno funkcioniranje uslijed sigurnosnih incidenata moglo imati snažne posljedice na društvo i/ili nacionalnu ekonomiju. Transpozicija NIS direktive u hrvatsko zakonodavstvo činjena je kroz Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga u srpnju 2018.

„RH uspješno usklađuje svoje zakonodavstvo s EU legislativom i svoje sposobnosti s novim zahtjevima. Primjena EU NIS

direktive u RH dala je dobre rezultate, a u transpoziciji EU NIS2 direktive treba koristiti do sada stečena iskustva", rekao je.

Upravljanje i digitalizacija kritične infrastrukture bila je tema predavanja Ivana Jurasa iz tvrtke GDi, globalnog izvoznika softvera i računalnih usluga „u oblaku" za geoinformacijska rješenja i upravljanje poslovnim procesima u javnoj upravi, industriji, komercijalnim tvrtkama i telekomunikacijama. GDi je i ovlašteni distributer vodeće svjetske tvrtke za GIS – Esri iz SAD-a – čiju ArcGIS platformu koristi velik broj ministarstava, agencija, javnih i privatnih poduzeća u RH. Prijetnje kritičnoj infrastrukturi su razne: prirodne nepogode, terorizam, kriminalne aktivnosti, nesreće koje uključuju opasne tvari i sl. Neke se prijetnje ne mogu predvidjeti, a smanjivanje svih mogućih rizika na najmanju mjeru nije uvijek ekonomski isplativo. Zbog toga se sve veći fokus stavlja na procjenu ranjivosti i izgradnju otpornosti kako bi se osigurao kontinuitet pružanja usluga ili neometana opskrba energijom, osobito nakon nepredviđenih destruktivnih događanja. Samo integrativni pristup omogućuje bolje razumijevanje i pravovremenu akciju.

Rješenje Juras vidi u digitalizaciji kritične infrastrukture jer smatra da je jedan od ključnih razloga za digitalizaciju kritične infrastrukture i upravljanje njome činjenica da nedostatak informacija o njoj ukoliko nešto pođe po zlu može nanijeti veliku štetu. Ključno je znati gdje se kritična infrastruktura nalazi, u kakvom je stanju, koji su procesi nad njome obavljeni ili će se tek obaviti a kada je to sve moguće u realnom vremenu to omogućava bolju upravljivost i osiguranje otpornosti. Nabrojao je primjere uspješnih implementacija koje je GDI obavio navevši ključne klijenti u mrežnim i energetskim industrijamana: INA, Janaf i Plinacro.

XDR - sigurnosno rješenje budućnosti predstavio je Nino Talian, iz KIng ICT-a. XDR je napredna i proaktivna tehnika otkrivanja prijetnji i odgovora koja omogućuje vidljivost podataka na krajnjoj točki, mreži i komponentama sustava u kombinaciji s analitikom i automatizacijom. Ovaj pristup omogućuje sigurnosnim timovima da identificiraju prijetnje koje su složene ili skrivene, pomaže u poboljšanju brzine otkrivanja prijetnji, a također ima sposobnost pratiti prijetnje kroz više komponenti sustava. XDR rješenja objedinjuju različite alate, omogućujući učinkovitije odgovore na prijetnje.

Kibernetske prijetnje i otpornost elektroenergetske infrastrukture kroz primjer Colonial Pipeline pokazao je Krešimir Kristić iz HEP-a, a na taj cyber napa se osvrnuo i Fred Streefland iz tvrtke Hikvision. Cyber-napadi na infrastrukturne usluge su u porastu, a hakeri iskorištavaju Internet stvari (IoT) koji stvara milijune novih ranjivosti u kritičnoj infrastrukturi. Više od 60 posto napada ransomwarea usmjereno je na industrije s kritičnom infrastrukturom, predvođene zdravstvom, komunalnim uslugama i proizvodnjom. Potrebna nam je suradnja javnog i privatnog sektora za izgradnju većeg konsenzusa o sigurnosnim standardima IoT-a i povjerenja u sigurnost u cijeloj kritičnoj infrastrukturi. Cybersigurnost je neophodna u današnjem složenom svijetu. Zaštita kritične infrastrukture je izazovna, ali ostvariva. Za osiguranje IT-a, OT-a i IoT-a potreban je holistički pristup i potpuna vidljivost okruženja.

Obzor Europa - nove prilike u području civilne sigurnosti

„Ma, tko će nas..." naziv je predavanja Vlatka Košturjaka iz tvrtke Diverto koji je rekao da je upravo ta rečenica standardni renesansni početak gotovo svakog epskog incidenta. I još Neće nas nitko…, Nemamo mi ništa zanimljivo…, Ne mogu oni nas naći na karti… Organizacije su izloženije kibernetičkim napadima što je posljedica rada od kuće i u ovoj godini, upozorili su još proljetos iz Diverta u svom izvještaju. Diverto je jedan od pionira u cyber sigurnosti i među vodećima u ovom dijelu svijeta, a njihovi stručnjaci pružaju usluge informacijske sigurnosti za više od 100 velikih organizacija.

Zorana Barišić iz Ministarstva znanosti i obrazovanja i Goran Sačić iz Agencije za mobilnost i programe EU predstavili su Obzor Europa - nove prilike u području civilne sigurnosti za društvo (2021. - 2027.), a riječ je o najvećem programu EU za financiranje istraživanja i inovacija. Programom se doprinosi i postizanju ciljeva održivog razvoja te se potiču konkurentnost i rast. Pomoću proračuna od 95,5 milijardi eura, uključujući 5,4 milijarde eura iz instrumenta Next Generation EU, programom se nadopunjuju nacionalno i regionalno financiranje u području istraživanja i inovacija. Obzor Europa nastavak je prethodnog EU-ova programa Obzor 2020.

Kako izgleda zaštita objekata kritične infrastrukture pojasnila je Renata Dončević iz tvrtke Alarm automatika. Prvi korak u zaštiti KI je prosudba ugroženosti i analiza rizika. Slijedi projektiranje s više zona zaštite, a uz to je potrebna oprema s visokim stupnjem zaštite i certifikatima. Za velike sustave kao što je KI - industrijski objekt s više sustava zaštite upravljanje može biti kompleksno stopga je nužna integracija svih sustava zaštite i povezivanje na jedno programsko sučelje s grafičkim mapama objekta i okoline, jednostavna detekcija lokacije alarma i upravljanje svim sustavima, brža reakcija operatera/zaštitara, moguća kasnija analiza događaja i reakcija operatera te automatsko povezivanje događaja. Iz tog je razloga ključno jasno definirati tko može raditi prosudbu ugroženosti i projekt. Jelena Levak iz tvrtke RiniGARD predstavila je Praetorian projekt i pojasnila kako izgleda zaštita kritične infrastrukture

Zaštita kritične infrastrukture na primjeru KB Sv. Duh

Direktor prodaje Eccosa, Ivan Bilać, je na primjeru projekta rekonstrukcije bolničkog kompleksa KB Sveti Duh, dogradnje dnevne bolnice uz rješavanje parkirališnih potreba bolnice predstavio nova rješenja zaštite kritične infrastrukture. Eccos je implementirao i integrirao u vlastitu središnju nadzornu aplikaciju Epsimax sustave tehničke zaštite: sustav videonadzora, kontrole pristupa, protuprovale, evidencije radnog vremena te sustave vatrodojave, plinodojave i odimljavanja, bolnički komunikacijski sustav i sustav bolničke signalizacije, sustav satova te instalirao sustav nadzora parkirališnih mjesta i usmjeravanja te naplate parkinga unutar novoizgrađene garaže na četiri etaže.
Cilj projekta bio je podizanje razine sigurnosti i kvalitete pružanja bolničkih usluga kroz objedinjeno upravljanje i administriranje, interakcijom među sustavima što omogućava pravodobno i točno djelovanje prilikom pojave alarma iz raznih sustava, lakšom i točnom naknadnom rekonstrukcijom pojedinog događaja, administriranjem prava korisnika u svim integriranim sustavima kroz jedinstveno sučelje te grafičkim prikazom statusa svih priključenih komponenti s mogućnošću direktnog upravljanja. Vrijednost projekta od preko 200 milijuna kuna i osvojena Hrvatska Velika Nagrada Sigurnosti 2021. u kategoriji najreprezentativniji projekt sustava sigurnosti potvrđuju veličinu i uspješnost projekta.

od naprednih kombiniranih cyber i fizičkih prijetnji. Projekt je prijavljen krajem kolovoza 2020. godine pod pozivom H2020-SU-INFRA-2020 (*Protecting the infrastructure of Europe and the people in the European smart cities*). Strateški cilj projekta je povećati sigurnost i otpornost europskih kritičnih infrastruktura, olakšavajući koordiniranu zaštitu međusobno povezanih kritičnih infrastruktura od kombiniranih fizičkih i kiber prijetnji. U tu svrhu projekt će pružiti višedimenzionalni (ekonomski, tehnološki, politički, društveni), a ipak specifični set alata. Takav set alata podržat će sigurnosne menadžere kritičnih infrastruktura (KI) u donošenju njihovih odluka kako bi predvidjeli i izdržali potencijalne kiber, fizičke ili kombinirane sigurnosne prijetnje vlastitoj infrastrukturi i drugim međusobno povezanim kritičnim infrastrukturama, a koje bi mogle imati ozbiljan utjecaj na njihov rad i/ili sigurnost stanovništva u njihovoj blizini.

Praetorian će se posebno pozabaviti (tj. spriječiti, otkriti, odgovoriti i, u slučaju objavljenog napada, ublažiti) kiber i fizičke napade koje su stvorili ljudi ili prirodne katastrofe koje utječu na kritičnu infrastrukturu. Također će se pozabaviti načinom na koji napad ili incident u određenoj KI može ugroziti normalan rad drugih susjednih / međusobno povezanih KI-a i kako sve njih učiniti otpornijima, predviđanjem kaskadnih učinaka i predlaganjem jedinstvenog odgovora među KI-ima. PRAETORIAN je projekt vođen od strane predstavnika KI-a, koji će svoje rezultate prikazati u tri međunarodna pilota, koji uključuju 9 izvanrednih kritičnih infrastruktura: 2 međunarodne zračne luke, 2 luke, 3 bolnice i 2 elektrane.

Prvog dana konferencije održane su i dvije panel rasprave koje je moderirao Robert Mikac, izvanredni profesor na Fakultetu političkih znanosti u Zagrebu. Drugi dan konferencije koja je okupila vrhunske stručnjake iz Republike Hrvatske i inozemstva, s ciljem pružanja kvalitetne platforme za raspravu o ključnim sigurnosnim izazovima u industriji i zaštiti kritičnih infrastruktura započeo je panel raspravom „Ulaganja u infrastrukturu". Industrija i kritične infrastrukture su izuzetno povezane i međuovisne, što itekako potvrđuje i industrija nuklearne energije. Industrija svakodnevno razvija koncepte i rješenja bitne za učinkovito funkcioniranje KI, ključnih i digitalnih usluga. Stoga je jasno kako se KI ne mogu održavati i unaprjeđivati bez snažne potpore iz različitih segmenata industrije.

Na panelu su sudjelovali direktor Fonda za financiranje razgradnje NEK, dr. Hrvoje Prpić koji je govorio o budućem Centru za zbrinjavanje radioaktivnog otpada. Infrastruktura kakva je Centar za zbrinjavanje radioaktivnog otpada zahtjeva sustavnu organizaciju zaštite. Najveća prijetnja je neovlašteni pristup radioaktivnom otpadu, te njegovo iznošenje u nekontrolirane okolnosti. Prednosti preferentne lokacije su svakako izoliranost i nepristupačnost, a nužna je fizička i tehnička zaštita objekata i lokacije. Uz Prpića, u panel raspravi su sudjelovali i Josip Turkalj iz AKD zaštite i Robert Bernat iz Instituta Ruđer Bošković.

U nastavku konferencije su izneseni regionalni primjeri zaštite Ki, a održana je i radionica Cyber ugroze u videonadzoru o čemu ćete moći čitati u idućem broju Zaštite. Konferenciju su sponzorski podržali HEP, Hikvision, Infodom, Alarm automatika, Diverto, Eccos, GDI, Rinigard, Tehnozavod Marušić, KING ICT, AKD zaštita i HGK. ■