Poštnina plačana pri pošti 1102 Ljubljana

glas gospodarstva

VARNOST IN ZAŠČITA

Foto: Depositphotos

panožna številka, oktober 2020

Pozornost podnevi in ponoči – za varnost in konkurenčnost
Kibernetska varnost

Strnjene vrste vseh sil tudi v primeru epidemij
Zaščita in reševanje

Slovensko obrambno industrijo bi vključili v zakon
Obramba

S-TMM Sistemi

Supporting limits

CELOVITE REŠITVE KI USTVARJAJO DODANO VREDNOST

Naše reference;
Ministrstvo za obrambo, Kontrole zračnega prometa-letališča, Policija, Agencije za nadzor frekvenčnega spektra.

Podjetje se prvenstveno ukvarja z izgradnjo, integracijo in vzdrževanjem radijskih komunikacij za profesionalno rabo. To našim strankam omogoča doseganje najboljših rezultatov.

Za potrebe naših strank izvajamo inštalacije in meritve radio komunikacijskih sistemov, tako mobilnih kot tudi stacionarnih sistemov.

Radio komunikacijski sistem za kontrolo zračnega prometa

Vozilo opremljeno s taktičnimi zvezami

Vozila za nadzor frekvenčnega spektra

MORS-URSZR - Vozilo za zveze, enote za hitre intervencije Civilne zaščite republike Slovenije za delo na terenu

S-TMM Sistemi d.o.o. ▪ Zabrv 120 ▪ SI-1292 Ig ▪ Slovenija ▪ www.s-tmm.si ▪ info@s-tmm.si ▪ Tel: +386 1 420 24 90

Gostujoči komentar

Razmere na področju varnostnih groženj pri poslovanju

Svet v novem tisočletju doživlja spremembe brez primere, ki povzročajo vse večjo negotovost ter nestabilnost vlad in gospodarstev. Dogodki, ki zaznamujejo generacije, na primer trenutna pandemija COVID-19, določajo »novo normalnost« našega vsakodnevnega življenja in poslovanja. Globalna geopolitična pokrajina se je polarizirala in zarisale so se nove politične meje, ki so države, kot so Iran, Severna Koreja, Rusija, Venezuela, Kuba in zdaj Kitajska, oddaljile od Zahoda. Vojna prek posrednikov, ki trenutno poteka med Iranom in Savdsko Arabijo, je privedla do regionalne nestabilnosti na Bližnjem vzhodu ter povzročila naraščanje svetovnih cen nafte in plina. Geopolitična pokrajina se še naprej spreminja, zato so podjetja izpostavljena novim varnostnim izzivom. Pri grožnjah, ki se pojavljajo v gospodarstvu, ne gre več le za varovanje rezultatov poslovanja. V novih razmerah so grožnje poslovanju na novo opredeljene in vključujejo tveganja za lastnino, ugled in tudi posameznike.

Globalna konkurenca je zabrisala meje med gospodarskimi in državnimi subjekti, s čimer se je začelo novo obdobje državno sponzoriranega gospodarskega vohunstva in obsežnih kraj intelektualne lastnine. Podjetja z lestvice Fortune 500 so postala redne tarče kibernetskih napadov, kar je privedlo do senzacionalističnih poročil o odtekanju informacij in milijardnih izgubah. Zavedanje o pomembnosti kibernetske varnosti se je okrepilo, vendar pa so podjetja še vedno izpostavljena asimetričnim kibernetskim grožnjam. Namesto klasičnih, neposrednih napadov na močno zavarovane strežnike podjetij so akterji ogrožanja danes izurjeni v prepoznavanju šibkih členov vrednostnih verig. Napadi se osredotočajo na manjše tarče, na primer ponudnike z manj strogimi varnostnimi standardi, ki omogočajo prikrit dostop do večjih tarč. Precejšnje varnostne vrzeli so nastale tudi zaradi trenutno razširjenih protokolov dela od doma, saj so zaposleni zunaj svojih delovnih mest navadno manj vestni pri upoštevanju strogih varnostnih standardov. Posledično so asimetrične grožnje po vsem svetu postale običajna oblika gospodarskega boja, obstoječi varnostni standardi pa se temu niso ustrezno prilagodili. Za učinkovito zaščito pred asimetričnimi grožnjami je treba vzdolž celotne vrednostne verige skrbeti za ozaveščanje o varnosti in izvajati protokole aktivnega spremljanja groženj.

Izjemno se je povečalo tudi povpraševanje po osebnem varovanju, saj so vplivni izvršni direktorji in njihove družine postali potencialne tarče ugrabitev. Zasebne varnostne službe so postale bistvenega pomena tudi za varovanje nepremičnin in ključnih zaposlenih po vsem svetu. To velja zlasti za industrije, ki delujejo v državah z visokim tveganjem, od katerih mnoge zaposlujejo več zasebnih varnostnikov kot policistov. Naraščajoča politična nestabilnost je na teh trgih spodbudila povpraševanje po visoko usposobljenih operativcih, izurjenih v specialnih silah, ki so zmožni evakuirati zaposlene iz sovražnega okolja, na primer med terorističnim napadom ali družbenimi nemiri.

Z razvojem tehnologije in nenehnimi inovacijami se grožnje poslovanju še naprej povečujejo. Zato se morajo razvijati tudi varnostne rešitve, da bodo podjetja krepila ozaveščenost in kar najbolj zmanjšala tveganja. gg

Foto: Kraftart

Pri grožnjah, ki se pojavljajo v gospodarstvu, ne gre več le za varovanje rezultatov poslovanja. V novih razmerah so grožnje poslovanju na novo opredeljene in vključujejo tveganja za lastnino, ugled in tudi posameznike.
Andrej Bastar, soustanovitelj in izvršni direktor, Brasidas Group AG

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

glas gospodarstva
VARNOST IN ZAŠČITA
oktober 2020

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

ogg

Izdajatelj:
Gospodarska zbornica Slovenije
Dimičeva 13, 1504 Ljubljana

Gospodarska zbornica Slovenije

Odgovorni urednik:
Samo Hribar Milič

Izvršna urednica:
Ana Vučina Vršnak

Oblikovna podoba:
Samo Grčman

Oblikovanje:
Nenad Bebić

Uredniški odbor:
Grit Ackermann, Antonija Božič Cerar, Marko Djinović, Ariana Grobelnik, Bojan Ivanc, Tomaž Kordiš, Tajda Pelicon, Petra Prebil Bašin, Matej Rogelj, Igor Zorko

Uredništvo:
Dimičeva 13, 1504 Ljubljana
01 5898 000
gg.plus@gzs.si

Trženje oglasnega prostora:
Dašis, d. o. o.
gg.trzenje@gzs.si
01 5130 824

Obramba **58**
Širok spekter slovenskih proizvodov in storitev na področjih obrambe, varnosti in zaščite

Varnost pri delu **76**
Delodajalec mora zaposlene ščititi in spodbujati k zdravemu načinu življenja

Bančništvo **74**
Banke: Največja težava ostajajo spletne in kartične prevare

Tisk: Present, d. o. o.

Datum natisa: 30. 10. 2020

Distribucija: Pošta Slovenije

ISSN 13183672

Revijo Glas Gospodarstva prejmejo člani GZS brezplačno (1 izvod).

Letna naročnina za dodatni izvod je: 80,00 evrov z vključenim DDV.

Poštnina za tujino se zaračuna posebej.

Medij Glas gospodarstva izdajatelja Gospodarske zbornice Slovenije, s sedežem v Ljubljani, Dimičeva 13, je vpisan v razvid medijev, ki ga vodi Ministrstvo za izobraževanje, znanost in šport, pod zaporedno številko 516.

Notranjost revije je natisnjena na recikliranem papirju Viprint papirnice VIPAP VIDEM KRŠKO, d. d., ki je za vse papirje pridobila certifikat FSC®, za nekatere papirje iz grafičnega programa pa tudi certifikat Ecolabel (okoljska marjetica).

Pri tiskanju smo uporabili okolju prijazne barve na rastlinski osnovi.

Pomagajo skrbeti za informacijsko varnost v energetiki

Družba Informatika, d. d., se že več let ukvarja z varovanjem programske in strojne opreme, omrežij in podatkov v lastnem okviru ter tudi v dejavnosti energetike. S katerimi izzivi se pri tem soočajo danes in kje je pri tem mesto kibernetske varnosti, nam je zaupal njen direktor, mag. Andrej Stajič.

Kakšno vlogo in pomen ima kibernetska varnost v družbi?

Da sta razvoj družbe in tehnologije neločljivo povezana, je še posebej opazno v današnjih časih, ko sta delovanje in obstoj družbe, kot jo poznamo, močno odvisna od delovanja tehnologije. Varovanje tehnoloških rešitev je torej izjemno pomembno, saj z njim varujemo družbo, ljudi, njihove pravice in lastnino. Vzporedno z razvojem družbe in tehnologije se spreminjajo tudi paradigme varovanja. Kibernetska varnost je eno od področji informacijske varnosti, ki se prekriva z drugimi vidiki varnosti, kot so fizična, požarna, digitalna, računalniška varnost itd. Kljub delitvi varnosti na področja je nujen holističen pristop, saj v praksi vektorji napada niso omejeni zgolj na eno področje. Tak pristop v svoji naravi tudi ni egoističen, saj temelji na sodelovanju z namenom varovanja vseh deležnikov; poleg varnosti posameznega podjetja je smiselno zagotoviti varnost vseh podjetij v verigi. Za doseganje zadovoljive ravni varnosti je treba spreminjati tudi družbo, zakonodajo, miselnost, poslovne modele, vzorce in običaje.

Kakšno težo dajete kibernetski varnosti v svojem podjetju?

Za nas je kibernetska varnost bistvenega pomena, saj delujemo v okviru energetskega sektorja, enega ključnih sektorjev kritične infrastrukture. Zaradi tega si prizadevamo za razvoj kibernetske varnosti tako v podjetju kot tudi v širšem okolju. Tako se že nekaj desetletij kontinuirano in uspešno ukvarjamo tudi z varovanjem programske in strojne opreme, omrežij in podatkov. Večkrat smo že spreminjali, prilagajali in izboljševali oblike in metode varovanja v skladu z aktualnimi modeli poslovanja ter standardi informacijsko-komunikacijske tehnologije in informacijske varnosti, saj si nenehno prizadevamo za ohranitev varnega okolja za svoje stranke, partnerje, dobavitelje in zaposlene. Kibernetsko varnost na podlagi lastnih dolgoletnih izkušenj pojmujemo kot pomemben korak v evolucijskem procesu razvoja metodologij varovanja.

Na kakšen način zagotavljate kibernetsko varnost za svoje stranke?

Klasične varnostne rešitve za varovanje računalniških sistemov in informacijskih storitev niso več zadostne, saj smo soočeni z novimi grožnjami in tveganji, ki so se pojavili zaradi hitrega razvoja tehnologije in razširjenosti njene uporabe, posledično pa tudi zaradi spremenjenih vzorcev delovanja poslovnih in organizacijskih sistemov ter celotne družbe. V ta namen intenzivno delamo na vzpostavitvi varnostnega operativnega centra (VOC), ki bi zagotavljal varnostne storitve v okviru energetske panoge. Prepričani smo, da brez operativnih centrov, ki med seboj učinkovito sodelujejo, zelo kmalu ne bo mogoče zagotavljati zadostne stopnje varnosti. Trenutno imamo vzpostavljen delujoči VOC, ki v okviru preverjanja konceptov že spremlja varnostne dogodke za več podjetji iz energetskega sektorja. Na podlagi tega se dela triaža in analiza incidentov ter izdelava rednih in izrednih poročil.

Kaj boste na področju kibernetske varnosti razvijali v prihodnje?

Strategijo, procese in storitve kibernetske varnosti v okviru VOC bomo neprenehoma in smiselno nadgrajevali in širili v skladu z rastjo potreb poslovnega okolja in sistemov, ki jih varujemo, kakor tudi v skladu z uveljavljenimi standardi ter najaktualnejšimi naprednimi in inteligentnimi tehnologijami za proaktivno zagotavljanje kibernetske varnosti. Na ta način bomo kontinuirano dvigovali zrelostno raven kibernetske varnosti in delovanja VOC ter stremeli k izpolnjevanju cilja, da postanemo verodostojen in vodilen člen ter partner pri udejanjanju celostne kibernetske varnosti v nacionalnem sistemu kritične infrastrukture za sektor energetike in širše.

»Intenzivno delamo na vzpostavitvi varnostnega operativnega centra (VOC), ki bi zagotavljal varnostne storitve v okviru energetske panoge,« pravi mag. Andrej Stajič, direktor Informatike, d. d.

PROMO

INFORMACIJSKE STORITVE IN INŽENIRING, D.D.
INFORMATIKA

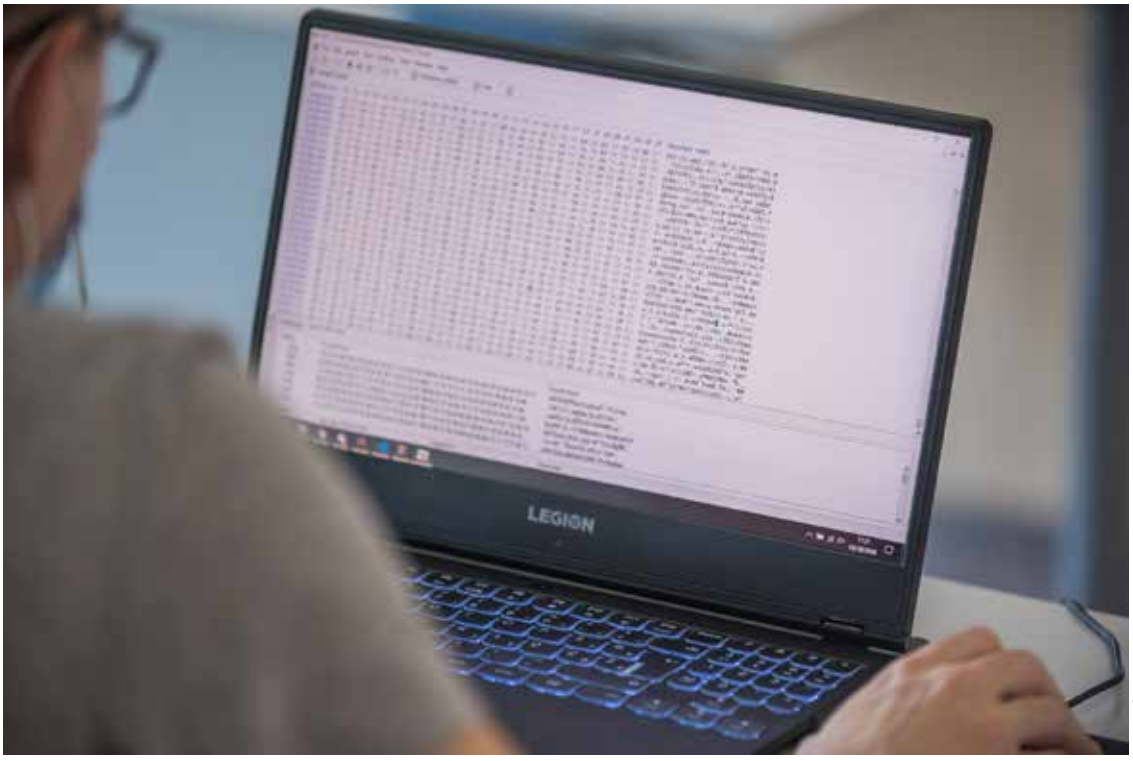


Foto: KrafiART

IKT horizontalna mreža

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Kibernetska varnost

Slovenija mora bolje povezati svoje zmogljivosti za zagotavljanje informacijske varnosti

V oktobru, ki je mesec kibernetske varnosti, je na Gospodarski zbornici Slovenije (GZS) potekala konferenca o kibernetski varnosti podjetij z naslovom »24/7/365: Kibernetska (ne)varnost nikoli ne počiva. Kaj se dogaja, ko spimo?«.

Maruša Boh, Združenje za informatiko in telekomunikacije (ZIT), GZS

DIHS je za večjo osveščenost objavil Vodnik za prve korake k varnejšemu poslovanju

Celodnevni dogodek je bil priložnost za poglobljeno razpravo o tem, kako zagotavljati učinkovito kibernetsko varnost 24 ur na dan, vsak dan v tednu in vse dni v letu.

Dr. Uroš Svete, direktor Uprave RS za informacijsko varnost, je poudaril, da varnost ni enkraten dogodek, temveč gre za stalni proces. Slovenija mora po njegovem v prihodnje svoje zmogljivosti za zagotavljanje informacijske varnosti bolje povezati, predvsem pa okrepiti. Pri tem bo zelo pomembno sodelovanje vseh deležnikov, torej sodelovanje z gospodarstvom in znanstveno-raziskovalno sfero, predvsem v povezavi z zagotavljanjem novih kadrov.

Kot pravi, si je treba prizadevati za popularizacijo področja informacijske varnosti med mladimi ter za primerne izobraževalne programe v slovenskih izobraževalnih ustanovah, ki bodo ves čas sledili spremembam in napredku na tem področju. Le na ta način in ob sodelovanju vseh deležnikov bo mogoče resnično okrepiti celoten sistem, da bo ta sposoben zagotavljanja informacijske varnosti za vse, je jasen Svete.

Zagotavljanje varnosti ni nekaj, kar traja od 8h do 16h, ampak je proces, ki zahteva nenehno pozornost.

Več kot polovica napadov na MSP

Čeprav Slovenija na videz ni med najbolj zanimivimi državami za kibernetske napade, to ne pomeni, da smo popolnoma varni in da se na področju kibernetske varnosti ne more zgoditi nič. Kriza COVID-19 situacije ni poslabšala, je pa dejstvo, da se je s pospešeno digitalizacijo povečal tudi prenos podatkov na internetnih omrežjih, kar je povečalo tudi število kibernetskih napadov. Pri tem velja izpostaviti, da

Foto: KraftART

Treba si je prizadevati za popularizacijo področja informacijske varnosti med mladimi.

Kriza je zaradi novega koronavirusa povzročila izjemno hitre spremembe v načinu dela in v uvajanju digitalnih orodij. Bili smo prisiljeni hitro reagirati in se prilagoditi novi situaciji. Bolj kot se družba digitalizira, več je prostora za napade, večja so tveganja in večje so posledice napadov. Zagotavljanje varnosti zato zahteva nenehno pozornost.

S pospešeno digitalizacijo med pandemijo se je povečal tudi prenos podatkov na internetnih omrežjih, kar je povečalo obseg kibernetskih napadov.

je bila več kot polovica vseh kibernetskih napadov usmerjena na mala in srednja podjetja (MSP). Bolj usmerjene napade je bilo zaznati tudi na komitente bank, epidemijo pa se je izkoriščalo tudi za poskuse okoriščanja z različnimi prijemi družbenega inženiringa, smo slišali na konferenci.

Gorazd Božič, vodja Nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, je predstavil lekcije, ki so jih v SI-CERT identificirali v tem letu. Ali se bomo od njih uspeli tudi kaj naučiti in naučeno uveljavili v praksi? Pravi, da se manjša in srednja podjetja še vedno premalo zavedajo vseh nevarnosti in groženj, ki jim pretijo.

»Zadnja leta se veliko posvečamo trudu, da bi vodstva MSP prepričali, da bi se ukvarjali z ozaveščanjem zaposlenih o tem, kakšne so možnosti tveganja in kako jih prepoznati, kajti človeški faktor je tisti, ki je pogosto kriv, da v podjetje pride izsiljevalski virus,« je povedal Božič in dodal, da »žal večina MPS kibernetsko varnost tradicionalno razume kot strošek, dokler se ne zgodi nekaj neprijetnega«.

Foto: KraftART

Pomen informacijsko varnostne kulture in pomanjkanje kadra

Dvig informacijsko varnostne kulture postaja pomemben za kibernetsko varnost družbe. Ljudje bodo morali bolj odgovorno uporabljati pametne tehnologije, saj bodo le tako zmanjšali tveganje v prihodnje. »S svojim vedenjem, ozaveščenostjo in pristopom lahko bistveno zmanjšamo možnosti za zlorabo in s tem dvignemo raven informacijske varnosti – tako v zasebnem, kot tudi poslovnem okolju,« je povedal Božič.

Milan Gabor je certificirani etični heker, ki podjetjem in organizacijam pomaga dvigati raven informacijske varnosti, na dogodku pa je o etičnemu hekerju govoril v luči poklica prihodnosti. Ponudil je vpogled v stanje glede kadrov na področju informacijske varnosti, ki ni preveč rožnato. Nekatere napovedi kažejo, da bo v Evropi do leta 2022 primanjkovalo veliko kadra s tega področja, po nekaterih napovedih do 350.000 strokovnjakov.

Da je kibernetska varnost z razvojem digitalizacije še kako pomembna in da izobraževanje in ozaveščanje ljudi lahko poskrbita za varnejšo družbo in delovanje podjetij, je izpostavila Katja Mohar Bastar, direktorica Digitalnega inovacijskega stičišča Slovenije (DIHS). Povedala je, da so spodbude v obliki vavčerja za kibernetsko varnost, ki MSP omogoča sofinanciranje sistemskega varnostnega pregleda in penetracijskega testiranja, le ena oblika pomoči, kako povečati odpornost na kibernetske grožnje. Ob tej priložnosti je DIHS objavil Vodnik za prve korake k varnejšemu poslovanju kot del aktivnosti osveščanja. gg

Sistema, ki bi zagotavljal 100 % varnost podjetja, ni. Lahko pa povečamo odpornost na kibernetske napade. Odsotnost varnostnih kontrol, pomanjkanje kadra in vedno bolj napredni hekerji so tisti indikatorji tveganja, ki lahko povzročijo hude motne v poslovanju, vključno s finančno škodo in škodo ugleda. Pred napadi se moramo ustrezno zavarovati, zato je dvig ravni informacijske in kibernetske varnosti v celotni družbi izrednega pomena.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Sistemizirani digitalni varnostniki

Mag. Matevž Mesojednik, Vodja varnostno operativnega centra, NIL

Kibernetska varnost je danes izjemno širok in prepleten pojem, ki ga pogosto, še bolj pa krivično, povezujemo izključno z informacijsko tehnologijo. Učinkovita strategija kibernetske obrambe na drugi strani v enaki meri naslavlja tudi druga povezana področja, kot so ekonomija, pravo in kriminal. Kadar – in pravilno je, da – razmišljamo o kibernetski varnosti na ravni vodstva organizacije, je bistveno razumevanje, kaj nam takšna varnost nudi. Očitno ne gre za tipično naložbo, katere vložena sredstva nadejano rezultirajo v njeno plemenitenje. V procesu uresničevanja strategije kibernetske obrambe prvenstveno vlagamo v zaščito svojih ključnih dobrin. Te so praviloma specifične posameznim organizacijam ali panogam. In vendar je obojim danes skupno eno: dobrine so svojim lastnikom in uporabnikom vse pogosteje dostopne tudi v digitalni obliki.

S kibernetsko zaščito v resnici najamemo in sistemiziramo digitalnega varnostnika. Torej nekoga, ki nadzoruje in ščiti naše dobrine, podobno kot to v banki počne varnostnik. Dobro ali malo manj dobro. Vodstva organizacij morajo imeti za opravičevanje digitalnih varnostnikov jasno opredeljena in ovrednotena korporativna tveganja. Ta je treba ustrezno zaščititi, kar je hkrati tudi vzvod za preudarno in utemeljeno investiranje v kibernetsko varnost.

Povedano je temelj procesa upravljanja informacijskih tveganj. Enako temeljno je zavedanje, da kibernetski kriminalci, z izjemo tistih bolje organiziranih, zares ne razmišljajo o velikosti ali premoženju svojih žrtev. Hipotezo pojasnimo na banalnem primeru roparja. Ta enako ne okleva pred vlomom v prazno trgovinico z na stežaj odprtimi vrati in izpostavljeno blagajno, za nameček pa brez varnostnika in video nadzorne kamere. Namesto zanj pogumnega/pogubnega poskusa vdora v strogo varovano banko bo nepridiprav svojo priložnost verjetneje iskal v taisti trgovinici. Ta zelo verjetno ni edina, hkrati pa nepridiprav pri tem ne bo izpostavljal sebe.

Zato le imejmo v procesih pojmovanja kibernetske varnosti pred sabo karikaturi strogo varovane banke in izpostavljene trgovinice. Ne bodimo lahkomiselni in izogibajmo se prehitrim zaključkom, da nismo zanimiva tarča kibernetskih napadov. Dovolj zgovorne so globalne statistike, ki pričajo o dobri tretjini [1/3] manjših in srednje velikih podjetij, ki so že bila tarča uničujočih napadov z izsiljevalskim virusom (angl. ransomware). Med prizadetimi podjetji je morala kar petina [1/5] vsaj za nekaj dni ustaviti svojo osrednjo dejavnost, večina oz. slabe tri četrtine [3/4] pa se je v izogib nenadejanemu izpadu poslovanja odločila za plačilo odkupnine. Ob zapisanem spomnimo, da so v kibernetskem svetu geografske meje zabrisane, naše digitalne dobrine bližje končnim uporabnikom, enako pa tudi motiviranim in vse bolj spretnim napadalcem.

Pogosto šibko kibernetsko odpornost podjetij si lahko razlagamo z več dejavniki. V največji meri se tu odraža pomanjkanje obrambnih zmogljivosti informacijskih sistemov, ki so bili ciljno zasnovani za podporo in digitalizacijo poslovnih procesov, manj pa za sposobnost branjena pred kibernetskimi kriminalci. Rešitev za lastnike informacijskih sistemov, ne nazadnje pa tudi za podjetne ponudnike informacijskih rešitev, se je že v zgodnjih 90. letih prejšnjega stoletja ponudila v prej omenjenih digitalnih varnostnikih. Med te uvrščamo protivirusne zaščite, požarne pregrade, varnostne prehode in druge preventivno naravnane tehnične ukrepe. Gre za nekakšne obliže, ki slabo oskrbovane rane (beri: šibko varnostno utrjene informacijske sisteme), vsaj na odprtih delih ali vsaj na videz zakrijejo. Brazgotine pa, vsaj tiste nepravilno oskrbovane, ostanejo.

V NIL-ovem varnostno operativnem centru (NIL SOC) si nalagamo odgovornost rednega izboljševanja kibernetske odpornosti uporabnikom naših storitev. Zakoreninjene zmogljivosti tradicionalnih informacijskih sistemov, ki pogosto temeljijo izključno na preventivi in krpanju šibko oskrbovanih ran, bogatimo z nujno potrebno ekspertizo zaznavanja in odzivanja na pomenljive varnostne dogodke. V ta namen smo sistemizirali vrhunske NIL-ove strokovnjake za digitalno varnost, ki bdijo nad varnostno neidealnimi informacijskimi okolji in odvračajo pozornost kibernetskih kriminalcev.

Zagotovite si odpornost na kibernetske grožnje

BMA PARTNERJI

Skoraj vsako podjetje lahko označimo kot tehnološko, kot tako pa je izpostavljeno tudi kibernetskim tveganjem. Kibernetski vdori lahko povzročijo prekinitve v poslovanju in dobavni verigi, težave z izdelki in še več. To lahko vpliva tudi na zunanje deležnike, kot so stranke, pacienti, gostje ali dobavitelji. Čeprav gre za eno glavnih poslovnih tveganj, s katerimi se soočajo organizacije, večina ni primerno pripravljena na kibernetske vdore oziroma druge varnostne dogodke.

Statistika na tem področju je strašljiva, saj analitiki predvidevajo, da bodo do leta 2021 letne škode zaradi kibernetskih vdorov po vsem svetu dosegle kar 6 bilijonov USD1. Vlaganje v kibernetsko varnost pa bo v štiriletnem obdobju do leta 2021 preseglo 1 bilijon USD2. Uprave organizacij se teh groženj zavedajo, ampak ali so nanje tudi dobro pripravljene? Imajo pripravljena orodja za obravnavo kibernetskih napadov takoj, ko se zgodijo? Kibernetski vdor (incident), ne glede na vrsto ali javno razkritje, lahko katastrofalno vpliva na poslovne izide organizacij.

Kako začeti?

Za začetek vzpostavljanja kibernetske odpornosti je treba upoštevati nekaj pomembnih korakov:

1. **Prepoznavanje** (razumeti morate svoje okolje in splošno kibernetsko tveganje),
2. **Zaščita** (izvesti morate primerne varovalne ukrepe za zamejitev škode ob kibernetskem vdoru ali drugem varnostnem dogodku),
3. **Zaznavanje** (vzdrževati morate preglednost svojega omrežja, da lahko zaznate vdore),
4. **Odzivanje** (predpostaviti morate, da bo prišlo do vdora, in pripraviti ustrezen načrt) in
5. **Reševanje** (največje tveganje je prekinitev poslovanja; obrnite se na strokovnjake, ki vam bodo pomagali hitro rešiti situacijo).

Izvedite oceno kibernetskih tveganj

Zelo učinkovit in celosten način izvedbe teh korakov je izvedba ocene kibernetskih tveganj po metodologiji samostojnega sprotnega vrednotenja kibernetske izpostavljenosti Cyber Quotient (CyQu) družbe Aon, ki uporablja vodilno podatkovno analitiko za vrednotenje izpostavljenosti organizacije kibernetskim tveganjem, odkrivanje najbolj ranljivih točk in poenostavljanje strategij za zmanjšanje tveganj. Rezultat je ocena zrelosti na področju kibernetskih tveganj, primerjalni rezultat glede na podobne organizacije in jasna pot do ocenjevanja ter razumevanja izvedljivih popravnih strategij.

CyQu vam lahko pomaga prepoznati ranljivosti – razumeti, kakšna je vaša izpostavljenost v devetih kritičnih domenah: varovanje podatkov, nadzor dostopa, končne točke in sistemi, varnost omrežij, fizična varnost, varnost aplikacij, drugi deležniki, odpornost poslovanja in delo na daljavo.

Ta nagrajena metodologija vam zagotovi avtomatizirano oceno in pregled zrelosti družbe na področju kibernetskih tveganj in izpostavljenosti v (najmanj) devetih varnostnih domenah, označi ranljiva območja in določi potencialna kibernetska tveganja za organizacijo. Vašo organizacijo primerja s podobnimi organizacijami v vaši panogi po vsem svetu.

Zavarovalnice že nudijo rešitve za zavarovanja kibernetskih tveganj. Postopek sklenitve takega zavarovanja je lahko precej zapleten, saj zahtevajo kakovostne podatke in je lahko s tem povezana izpostavljenost zelo visoka, vse to pa vpliva na postopek pravilnega vrednotenja stroškov zavarovanja. Če torej načrtujete prenos tega tveganja na zavarovalnico, lahko to orodje uporabite kot pomoč sebi in zavarovalnici pri zagotavljanju boljšega pregleda in razumevanja svojega položaja in izpostavljenosti.

Za več informacij smo vam na voljo na naslovu: bma.partnerji@bmap.si

PROMO

[1,2] *Cybersecurity Facts, Figures, Predictions, And Statistics For 2019 To 2021, Sausalito, Calif, 2019*

Foto: Depositphotos

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Kibernetska varnost

Pozornost podnevi in ponoči – za varnost in konkurenčnost

Digitalna preobrazba prinaša nove rešitve s še večjo odvisnostjo od digitalnih tehnologij in zagotavljanja kibernetske varnosti. Med vodilnimi vse bolj prevladuje prepričanje, da je uveljavljanje ukrepov kibernetske varnosti del obvladovanja tveganj, ki podjetjem zagotavljanja konkurenčno prednost.

Mihael Nagelj, predsednik Sekcije za kibernetsko varnost, Združenje za informatiko in telekomunikacije (ZIT), GZS

Živimo v obdobju stalnih in hitrih sprememb, ki stalno pospešujejo digitalno preobrazbo vseh področij delovanja družbe. Stanje zaradi COVID-19 je spremenilo način delovanja podjetij in marsikje še pospešilo digitalno preobrazbo. A žal je prineslo tudi nove oblike ogrožanja.

Zapostavljeni varnostni ukrepi v podjetjih so dobro opremljenim in motiviranim napadalcem odprli dodatne možnosti za lažje vdore v pogojih dela od doma. V tej situaciji so se podjetja in varnostni strokovnjaki v Sloveniji dobro odzvali, brez večjih posledic vdorov.

Za večjo gospodarsko rast

Poleg skrbi za delovanje v obstoječih pogojih številna podjetja že načrtujejo delovanje v fazi prehoda po obdobju COVID-19 za obdobje gospodarske rasti, kot jo po strmem padcu dejavnosti v letu 2020 napovedujejo poslovni analitiki. Digitalna preobrazba prinaša nove rešitve in še večjo odvisnost od digitalnih tehnologij, te pa bodo zahtevale tudi ustrezno raven varnosti.

Vse bolj med vodilnimi v podjetjih prevladuje prepričanje, da je uveljavljanje ukrepov kibernetske varnosti del obvladovanja tveganj v podjetjih, ki jim prinaša konkurenčno prednost, saj z zmanjšanjem tveganj lahko zanesljiveje oskrbujejo svoje

Ukrepi kibernetske varnosti niso enkraten dogodek, so stalna skrb vodilnih, zaposlenih in strokovnjakov kibernetske varnosti.

Dogodek 24/7/365 je bil priložnost, da so podjetja v sektorju kibernetske varnosti in predstavniki države spregovorili o odprtih vprašanjih kibernetske varnosti v podjetjih in tudi s praktičnimi primeri dobre prakse predstavili možnosti za izboljšanje stanja. To je nujno, če bodo podjetja želela uspešno izvajati svojo digitalno preobrazbo.

odjemalce, zmanjšujejo nepotrebne stroške in zagotavljajo svoj ugled na trgu.

Z zmanjšanjem tveganj lahko zanesljiveje oskrbujemo svoje odjemalce, zmanjšujemo nepotrebne stroške in zagotavljamo ugled na trgu.

Analizi kibernetskih tveganj o uresničevanju poslovnih ciljev podjetja morajo slediti ukrepi, ki se nanašajo na zmanjševanje ranljivosti v omrežjih, na ozaveščanje o grožnjah, izobraževanje pri uporabi storitev informacijskih in komunikacijskih tehnologij ter uveljavljanje ukrepov varnosti v dnevni praksi. Za optimalno uresničevanje ukrepov kibernetske varnosti je nujno uravnotežiti poslovna tveganja in ukrepe kibernetske varnosti, kar pa je mogoče uresničiti le ob tesnem sodelovanju vodstva podjetja in specialistov kibernetske varnosti. Nujna je tudi povezanost podjetja z ostalimi dejavniki kibernetske varnosti v družbi. Šele z aktivnim delovanjem vodstev podjetij, organov države, posameznikov in strokovnjakov bomo lahko dosegali ustrezno raven odpornosti podjetij in družbe v celoti.

Nacionalna strategija kibernetske varnosti je načrt ukrepov, namenjen izboljšanju varnosti in odpornosti nacionalnih infrastruktur in storitev.

Širša družbena odgovornost

Večkrat slišimo o nujnosti širše družbene odgovornosti za kibernetsko varnost. Prepletenost telekomunikacijskih in informacijskih tehnologij in njihova skokovita rast zahtevata angažiranost vseh, tako uporabnikov storitev, ponudnikov storitev in specialistov. V zadnjih letih Republika Slovenija zmanjšuje zaostajanje, ki pa ga v kratkem času ni mogoče odpraviti, saj je področje zelo kompleksno. Potrebni bodo nadaljnji koraki za zmanjšanje zaostankov. Eden od teh je sprejetje nacionalne strategije kibernetske varnosti, ki bo skupaj z akcijskim načrtom podlaga za hitrejši razvoj področja.

Nacionalna strategija kibernetske varnosti je načrt ukrepov, namenjen izboljšanju varnosti in odpornosti nacionalnih infrastruktur in storitev. To je pristop, ki na visoki ravni določa vrsto nacionalnih ciljev in prednostnih nalog, ki jih je treba uresničiti v določenem časovnem obdobju za odpravljanje tveganj v kibernetskem prostoru, ki bi lahko ogrozila ekonomske in socialne koristi. S Strategijo kibernetske varnosti iz leta 2016 je Slovenija okrepila sistem zagotavljanja kibernetske varnosti, vzpostavila nove rešitve in istočasno odprla pot nadaljnjim izboljšavam. S stanjem v podjetjih ne moremo biti zadovoljni, saj o tem pričajo pokazatelji v raziskavi SURS Kibernetska varnost v podjetjih z vsaj 10 zaposlenimi (vir: https://www.stat.si/StatWeb/News/Index/8421). O nujnosti sprememb je letos tekla razprava na številnih srečanjih strokovnjakov kibernetske varnosti, vse pogosteje pa se v razpravo vključujejo tudi vodilni iz podjetij, ki jih k zagotavljanju varnosti zavezuje tudi zakonodaja. Prevladujoča mala in srednja podjetja (MSP) so v specifični situaciji zaradi še večjega pomanjkanja virov, se pa varnostni dogodki teh podjetij ne izognejo.

Ne pozabimo na izobraževanje pri uporabi storitev informacijskih in komunikacijskih tehnologij!

Prihajajoče spremembe Strategije kibernetske varnosti in akcijskega načrta za njeno uresničevanje predstavljajo priložnost za podjetja, da v krovnem dokumentu kibernetske varnosti države in še posebej v akcijskem načrtu predlagajo umestitev ustreznih rešitev za izzive prihodnosti, ki se nanašajo na vključevanje novih tehnologij, raziskav in razvoja, razvoj novih produktov, javno zasebnega partnerstva, vključevanja v mednarodne trge, specifičnosti MSP ali zagotavljanja potrebnih specialističnih kadrov. Razvoj in zadrževanje specialističnega kadra postajata vse bolj kritična in zahtevata drugačne rešitve na strateški ravni. Specifičen je položaj MSP v sektorju kibernetske varnosti, ki je zasnovan predvsem na vrhunskem znanju posameznikov. V okviru projekta CYBER pod okriljem programa Interreg Europe se deležniki na GZS posebej ukvarjajo z vprašanji sprememb ekosistema za delovanje MSP, ki delujejo v sektorju kibernetske varnosti. Skupaj s partnerji v evropskih regijah na podlagi izmenjave dobrih praks in izkušenj projektna skupina pripravlja predloge, ki bodo izboljšali ekosistem delovanja MSP v sektorju kibernetske varnosti, zagotovili njihov razvoj in tudi tako prispevali k razvoju odpornosti družbe.

Foto: Depositphotos

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Vse bolj rafinirane metode napadalcev

Iz letnega poročila SI-CERT je razvidno, da je v letu 2019 prišlo do velikega porasta »phishing« prijav (t. i. internetno ribarjenje oziroma lažno predstavljanje podjetja), saj uporabniška gesla odpirajo vrata nadaljnjim zlorabam. Še naprej se kaže trend ciljanja na podjetja, kjer je povzročena finančna škoda še višja kot pretekla leta. Ta trend se v tem letu še krepi. Rast »phishinga« je znašala v letošnjem septembru celo 65 % glede na enako obdobje lani.

Metode napadalcev so vedno bolj rafinirane in se prilagajajo specifični situaciji uporabnikov. Če uporabnik ni previden, lahko hitro napadalcu omogoči vnos škodljive kode. Ta pristop je za napadalce najbolj učinkovit in jim omogoča nadaljnje aktivnosti v internem omrežju. Znani so primeri, kako z lahkoto posamezniki pridejo do sredstev ogrožanja varnosti, da ne omenjam organiziranega kriminala, ki razpolaga z znatnimi viri in stalno prednostjo pred obrambo.

Najbolj prepoznavne posledice so šifriranje virov podatkov podjetja (angl. ransomware) ob uničevanju varnostnih kopij in dodatno izsiljevanje z objavo podatkov v javnih medijih. Izrednega pomena je, da podjetja posredujejo informacije o takšnih dogodkih nacionalnemu odzivnemu centru za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team), saj s tem omogočijo ukrepe za preprečevanja nadaljnje širitve napadov in vzpostavitev ustreznih preventivnih ukrepov.

Podjetjem so na voljo številne storitve, s katerimi si lahko pri obvladovanju kibernetskih tveganj pomagajo pri implementaciji varnostnih standardov, kot je denimo standard ISO/IEC 27001, pri izvajanju preventivnih ukrepov ali v primerih varnostnega incidenta. Vendar pa je treba poudariti, da se podjetje lahko in tudi mora organizirati na način, da se koncepti kibernetske varnosti uveljavljajo v vseh delih organizacije. Tako obvladovanje kibernetskih tveganj postane dnevna praksa, ki omogoča učinkovito odkrivanje in ukrepanje ob poizkusih vdorov. gg

65 % je letos septembra znašala rast pojava »phishinga« v primerjavi z enakim obdobjem lani.

Če uporabnik ni previden, lahko napadalcu omogoči vnos škodljive kode.

Operativni center kibernetske varnosti je bistveni člen kibernetske zaščite

Telekom Slovenije podjetjem v svojem najsodobnejšem operativnem centru kibernetske varnosti v Sloveniji nudi varnostne rešitve, ki so posebej prilagojene potrebam malih in srednje velikih podjetij.

Hitro in natančno odkrivanje ter odpravljanje groženj

Vsako podjetje, ne glede na velikost ali panogo, v kateri deluje, potrebuje celovito rešitev, s katero lahko zagotavlja ustrezno raven kibernetske varnosti in hkrati celostno obvladuje vse ravni varnosti – od varnostne politike in ozaveščenosti zaposlenih do opreme, ki zajema vse omrežne elemente (tj. računalnike, strežnike in omrežje kot celoto). Pri tem je treba zagotavljati hitro in natančno odkrivanje in odpravljanje kibernetskih varnostnih tveganj, in sicer ne glede na to, na kateri končni točki bi lahko do njih prišlo. Za to podjetja potrebujejo strokovno specializirano ekipo, vrhunsko opremo in zanesljive sistemske rešitve. Vse to podjetjem vseh velikosti zagotavlja Operativni center kibernetske varnosti Telekoma Slovenije.

Najbolj zmogljiv operativni center v državi

Operativni center kibernetske varnosti predstavlja jedro operativnih zmogljivosti tako za Telekom Slovenije kot druge organizacije, javne ustanove in podjetja. Je najbolj zmogljiv tovrstni center v Sloveniji in zagotavlja učinkovito zaščito pred varnostnimi tveganji v skladu z najvišjimi mednarodnimi standardi informacijske in kibernetske varnosti. Podjetjem in organizacijam nudi vrhunsko podporo in rešitve, s katerimi lahko učinkovito zaščitijo svoje poslovno okolje ter gradijo zaupanje svojih partnerjev in uporabnikov.

V Operativnem centru kibernetske varnosti Telekoma Slovenije vrhunski strokovnjaki s specifičnimi znanji z različnih področij varnosti storitev in infrastrukture obvladujejo varnostne dogodke s pomočjo nadzornih in analitičnih orodij 24 ur na dan, vse dni v letu. V nenehni pripravljenosti aktivno spremljajo varnostne dogodke v IKT-sistemih na različnih omrežnih elementih in jih v realnem času ocenjujejo glede na vsebino in kontekst, tako da se lahko ob podpori najsodobnejše tehnologije takoj ustrezno odzovejo, kadar je to potrebno. Ob tem izvajajo tudi testiranja, s pomočjo katerih odkrivajo morebitne ranljivosti IKT-sistemov in internih procesov ter jih odpravljajo. Posebna pozornost je namenjena varnosti in zasebnosti komunikacije, storitve, ki jih zagotavljajo strokovnjaki v Operativnem centru kibernetske varnosti, pa izvajajo skladno z najstrožjimi merili glede ravni storitve. Vsi procesi so podprti z mednarodnima standardoma ISO 22301:2012 za sistem upravljanja neprekinjenega poslovanja in ISO/IEC 27001:2013 za sistem vodenja in varovanja informacij.

Storitve se prilagodijo glede na velikost in potrebe vsakega podjetja

Strokovnjaki Operativnega centra Telekoma Slovenije pri obravnavi večjih podjetij upoštevajo tudi tehnologije, s katerimi že razpolagajo, in nadgradijo obstoječe interne procese kibernetske varnosti. Za mala in srednje velika podjetja pa je na voljo zanje prilagojena, učinkovita in cenovno ugodna storitev, s katero je poslovanje odpornejše na kibernetska varnostna tveganja. To še posebej velja tudi v primeru, ko podjetja sama nimajo zaposlenih strokovnjakov za kibernetsko varnost.

Operativni center kibernetske varnosti Telekoma Slovenije je prejel nagrado za najbolj inovativno varnostno rešitev v Sloveniji. Po mnenju Instituta za korporativne varnostne študije, ki nagrado podeljuje v sodelovanju s Slovenskim združenjem korporativne varnosti, gre za informacijsko-varnostno rešitev, ki predstavlja pomembno dodano vrednost na področju zagotavljanja kibernetske varnosti v Republiki Sloveniji. Ob tem je Operativni center kibernetske varnosti Telekoma Slovenije prejel tudi nagrado Varnostni produkt leta.

Več informacij: http://ts.si/OCKV

Svetovalci Telekoma Slovenije so vam na voljo na e-naslovu poslovni@telekom.si oz. številki 080 70 70.

TelekomSlovenije

Foto: Depositphotos

Zagotavljanje dobre varnostne drže postaja v današnjem času res velik izziv.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Kibernetska varnost

Z avtomatizacijo do obvladovanja kibernetsko-varnostnih tveganj

Organizacije posedujejo informacijska sredstva v obliki podatkov, ki so večinoma shranjeni na računalniških sistemih. Ti sistemi pa so bolj ali manj ranljivi. Vendar je dobra novica ta, da je danes na voljo popolnoma avtonomno računalniško gnano penetracijsko testiranje, s katerim lahko podjetja sproti korigirajo morebitne ugotovljene slabosti v kibernetski obrambi.

Matjaž Kosem, Carbonsec

Danes skorajda ne mine dan, ko na spletu ne preberemo novice o kakšnem hekerskem vdoru in preštevanju poslovne škode, o kakšni novi ranljivosti v sistemih, ki so prisotni v skoraj vsakem podjetju, ali pa o spet novih inovativnih tehnikah socialnega inženiringa, pa tudi o bajnih zaslužkih, do katerih določeni posamezniki pridejo s pomočjo hekerskega izsiljevanja … Zagotavljanje dobre varnostne drže postaja v današnjem času res velik izziv, zato ni čudno, da si marsikateri vodja informacijske varnosti (angl. Chief Information Security Officer – CISO) zastavlja vprašanje, kako naprej oz. kako zares učinkovito obvladovati varnostna tveganja.

Kaj vse vpliva na kibernetsko-varnostna tveganja in kako jih učinkovito obvladovati? Glavna skrb pri varovanju informacijskih sredstev je, da bodo ta vedno na razpolago tistim, ki imajo za njihov dostop pravico, in to v točno takšni obliki, kot morajo biti. Organizacije posedujejo informacijska sredstva v obliki podatkov, ki so večinoma shranjeni na računalniških sistemih. Ti sistemi imajo manjšo ali večjo mero ranljivosti, ki jo lahko izkoristi heker – slednje poenostavljeno imenujemo grožnja. In ker si seveda želimo, da bi bila verjetnost realizacije grožnje čim manjša, bomo naredili vse, da bi to preprečili.

Ker si želimo, da bi bila verjetnost realizacije grožnje čim manjša, bomo naredili vse, da bi to preprečili.

Foto: Depositphotos

Ranljivosti se ves čas spreminjajo. In tudi grožnje se nenehno spreminjajo.

Tveganja, da bi do uresničitve groženj prišlo, lahko praviloma zmanjšujemo na tri načine:

1. Sredstva varujemo z varnostnimi napravami in rešitvami: od relativno majhnega nabora osnovnih zaščit, kot so klasične požarne pregrade in protivirusni programi, več kot desetletje nazaj, se danes v organizaciji lahko najde tudi več kot 100 različnih varnostnih rešitev.
2. Pomagamo si s sistemi za upravljanje z ranljivostjo: na ta način ves čas vemo, kateri sistemi nimajo nameščenih varnostnih popravkov ter katere popravke bi bilo bolj nujno namestiti kot druge.
3. Grožnje spremljamo s pomočjo naprednih orodij za varnostne grožnje, t. i. TI (angl. Threat Intelligence): namen je, da dovolj zgodaj izvemo, ali se nekje dogajajo napadi, specifični za določeno industrijo, ki pa se lahko zgodijo tudi nam.

Že od nastanka računalnikov je obstajala ideja o umetni inteligenci, ki bi človeštvu močno olajševala napredek.

Ker je informacijski sistem »živ organizem«, pomeni, da se vse troje neprestano spreminja. Dodajanje novih sistemov, prenavljanje delov omrežij, povezovanje z oblačnimi storitvami, vpeljevanje novih storitev – ranljivosti se ves čas spreminjajo. Že samo pogled v podatkovno bazo ranljivosti CVE (angl. Common Vulnerabilities and Exposures) razkrije, da se ta neprestano povečuje. Tudi grožnje se spreminjajo, pa naj gre za nove hekerske skupine ali pa nove kampanje s še nikoli videnimi tehnikami napada.

Preverjen, a časovno zamuden način

Eden izmed najboljših načinov preverjanja, kje dejansko smo, je stari dobri vdorni test. Kljub priljubljenosti pa imajo tovrstna testiranja varnosti vendarle nekaj pomanjkljivosti. Test traja vsaj dva tedna, lahko pa tudi precej več, in je zaradi pomanjkanja ekspertov relativno drag. Rezultati so praviloma odvisni od izkušenosti in talenta »pentesterja«, včasih celo dnevne forme ali počutja. Zaradi omenjenega se vdorna testiranja največkrat izvajajo enkrat letno in imajo pravo vrednost le na dan zaključka (»rok trajanja« velja torej do prve spremembe sistema).

Kakšna bi bila možna rešitev?

V idealnem svetu bi bil vdorni test hitrejši, cenejši in popolnejši, torej neodvisen od ekspertize posameznika. Če se nekoliko pošalim, lahko rečem, da bi potemtakem potrebovali 1.000 popolnih pentesterjev v eni škatli in vedno na voljo, po možnosti s pritiskom na gumb. Na srečo je tehnologija, ki lahko popolnoma nadomesti pentesterja v notranjem delu omrežja, danes že na voljo. Že od nastanka računalnikov je obstajala ideja o umetni inteligenci, ki bi človeštvu močno olajševala napredek. Tako je bil slavni šahist Gari Kasparov prvič v zgodovini s strani računalnika premagan že leta 1996. Slavni Stephen Hawking se je umetne inteligence celo bal, saj naj bi po njegovem pomenila tveganje za obstoj človeštva, kar samo pomeni, kakšen velikanski potencial dejansko ima. Razvoj tehnologije je tako prišel tudi do tistih, ki so se zavedali potrebe po vsakodnevnem preverjanju kibernetske varnosti.

Popolnoma avtonomno računalniško gnano penetracijsko testiranje je danes tu in omogoča podjetjem, da vsakodnevno testirajo svojo kibernetsko varnostno držo ter sproti korigirajo morebitne ugotovljene slabosti v kibernetski obrambi.

Danes v kibernetiki ni stalnic. Podjetja, ki se že poslužujejo tovrstne obravnave svoje varnosti, so tako veliko bolj odporna na morebitni vdor, ki lahko močno omaja ugled in stabilnost poslovanja. gg

Informacijskega kriminala tudi v Sloveniji vedno več

»Pri vzpostavljanju varnostnih rešitev je potrebno zavedanje, da bo prej ali slej tudi naše podjetje doživelo varnostni incident. Ko se ta zgodi, je izredno pomembno, da ga čim prej zaznamo, omejimo in nato začnemo z odpravo njegovih posledic oziroma vzpostavitvijo normalnega delovanja,« pravi Jure Pečar, prodajni svetovalec za omrežja in varnost v družbi S&T Slovenija.

Katere ključne nevarnosti pretijo podjetjem na področju IT?

Informacijskega kriminala je tudi v Sloveniji vse več in podjetja se soočajo z najrazličnejšimi poskusi vdorov. Velik porast je bilo zaznati tudi v koronskem obdobju. V okviru našega varnostno operativnega centra (SOC), ki v S&T Slovenija deluje že tri leta, skrbimo za varnost več kot 45.000 uporabnikov, kar je daleč največja SOC operacija v Sloveniji in to nam daje dober vsakodnevni vpogled v dogajanje. Kot najbolj pogoste oblike napadov zaznavamo različne poskuse vdorov z ribarjenjem (t. i. Phishing) – tako množične, ki naslavljajo veliko uporabnikov, kot tudi zelo ozko usmerjene (Spear Phishing) na izpostavljene posameznike, denimo direktorje, vodje financ itd. Opazili smo tudi precej DDOS napadov (Distributed Denial of Service) in poskuse spreminjanja spletnih strani (Defacement).

V zadnjega pol leta smo se ukvarjali tudi z dvema primeroma vrivanja v poslovno komunikacijo (BEC – Business Email Compromise), ko so napadalci na precej enostaven način oškodovali dve slovenski podjetji. Vsako je utrpelo več kot četrt milijona evrov škode in vprašanje je, ali jim jih bo uspelo povrniti.

Kako se je mogoče pred njimi zavarovati, vzpostaviti kakovostno informacijsko varnost?

Tradicionalni obrambni mehanizmi, kot so požarni zidovi, antivirusni programi in podobno kljub nenehnemu razvoju ne morejo več zagotoviti ravni varnosti, ki je potrebna za nemoteno poslovanje, in vse bolj prevzemajo vlogo osnovnega higienika pri zagotavljanju informacijske varnosti. Pri vzpostavljanju varnostnih rešitev se je treba zavedati, da bo prej ali slej tudi naše podjetje doživelo varnostni incident. Ko se ta zgodi, je izredno pomembno, da ga čim prej zaznamo, omejimo in nato začnemo z odpravo njegovih posledic oziroma vzpostavitvijo normalnega delovanja. Tu nam sicer v določeni meri lahko pomaga tehnologija, npr. napredni sistemi za zaznavanje anomalij na osnovi umetne inteligence in strojnega učenja, vendar pa samo tehnologija ni odgovor na vse izzive. Ključno je tudi, da imamo ustrezno sposobne kadre ali pa si jih zagotovimo preko zunanjega izvajanja. Tretji, zelo pomemben, a največkrat prezrt člen, pa so ustrezne varnostne politike, urejeni poslovni procesi in zapisane procedure. V S&T pri vseh naših aktivnostih – od načrtovanja, vzpostavitve in nato rednega izvajanja – pazimo, da uravnotežimo vse te tri komponente uspešne obrambe proti kibernetski napadom – torej ustrezno tehnologijo, urejene procese in strokovne zaposlene. Pokaže se, da v praksi podjetja ne morejo zagotoviti tehnoloških in človeških virov, zato je navezava na kompetentnega partnerja edina možna rešitev za nemoteno poslovanje.

Kaj je treba najprej narediti, ko ugotovimo, da smo napadeni? Kako voditi obrambo?

Izjemno pomemben je hiter in kakovosten odziv. Če nimamo izkušenj, brskanje po Googlu ne bo dalo rezultata, ampak vam bo ukradlo dragocene minute za odziv. In če kdaj, tu res velja pregovor: »Čas je denar«. Povežite se s kompetentnimi strokovnjaki, ki morajo od vas dobiti vse potrebne informacije, brez prikrivanja morebitnih storjenih napak. Za lažje ravnanje v izjemno stresni situaciji, ki nastane takoj, ko odkrijemo, da so nas napadli, smo v S&T Slovenija vzpostavili storitev 'SOC line', ki je tako rekoč klic v sili za varnostne incidente. Telefon je na voljo vsem podjetjem, ki so v stiski zaradi varnostnega incidenta, tudi tistim, ki prej niso sodelovala s S&T Slovenija.

Prvi korak je vsekakor zavarovanje dokazov in analiza stanja prizadetega sistema (zajem različnih datotek, log sporočil itd.), ki naj bi povedala, kaj se nam je zgodilo, kakšen je obseg incidenta. Iz tega lahko potem pripravimo načrt akcij za povrnitev v delujoče stanje. V tem delu se velikokrat pokažejo težave v neurejenih okoljih, kjer npr. ni ažurnih arhivskih kopij podatkov ali pa so tudi te prizadete. Nemalokrat je zaradi kompleksnosti napada potrebna popolna restavracija sistema, in če nimamo na razpolago kopij podatkov, ima to lahko za posledico veliko škodo. Vsekakor pa je treba tudi po vzpostavitvi delujočega stanja preveriti, ali smo res odstranili vse vzroke in ali smo zakrpali vse ranljivosti.

Kaj je treba narediti, da iz takšnega napada izidemo (še) močnejši? Kako se iz njega učiti, nova spoznanja vgraditi v informacijski varnostni sistem?

Ko smo preživeli napad in vzpostavili stanje, je nujna analiza, zakaj se nam je incident zgodil, nato pa se moramo v miru pripraviti na naslednjo bitko. Optimizirajmo mehanizme za zaznavo incidentov, da bomo v prihodnje incident zaznali prej in se bo morda manj razširil in povzročil manjšo škodo. Prav tako preverimo, ali naši postopki za obnovo sistema v primeru katastrofe res delujejo. In ne nazadnje – ključno je nenehno osveščanje oziroma izobraževanje uporabnikov o informacijski (ne)varnosti.

Digitalna evolucija prinaša nove varnostne izzive

Z razvojem mobilnih omrežij bodo vse stvari postale povezane in konstantno na spletu. V obdobju 5G bo omogočenih več kot milijon povezav na kvadratni kilometer. Vsak predmet, s katerimi se srečamo v osebnem in poklicnem življenju, bo povezan v omrežje. S 5G bo odzivni čas omrežja tudi 50-krat hitrejši kot s 4G tehnologijami, zamik med delovanjem in reakcijo pa bo izjemno nizka. To bo omogočilo številne aplikacije v realnem času, ki danes preprosto še ne obstajajo.

Množični podatki in uporaba umetne intelligence (AI) bosta prizore iz znanstvene fantastike spremenila v resničnost: strojno učenje, strojni vid, diagnostični pomočniki itd. V zdravstveni industriji na primer bomo uporabljali DNK teste, ki jih bodo izvajali drobni čipi z uporabo tehnologije AI, ter hkrati ogromne navidezne medicinske možgane, ki bodo sposobni obdelave milijonov hkratnih testov. Potencialna vrednost velikih podatkov in AI se bo končno začela realizirati, kar bo prineslo številne koristi za vse človeštvo.

Uporaba tehnologije v oblaku bo prav tako postala veliko bolj razširjena, stroški tehnologije pa bodo upadli. V naslednjih 10 letih se bo skoraj 100 % podjetij povezovalo s storitvami v oblaku. 85 % aplikacij se bo selilo v oblak. Zato se bo učinkovitost podjetij močno povečala. V oblaku bomo lahko razvijali in lansirali novo programsko opremo, oblak pa bo postal t. i. digitalni možgani.

Pa vendar obstajata dve strani vsakega kovanca. Mobilna omrežja in senzorji bodo ustvarili bolj povezan svet; vendar bo hkrati tudi ranljivost IKT sistemov eksponentno naraščala. AI in množični podatki bodo omogočili globoko rudarjenje podatkov; vendar se bo tveganje za zlorabo podatkov prav tako povečalo. Oblačne tehnologije bodo omogočile izmenjavo virov in odprle zaprte sisteme; vendar to pomeni, da bodo tudi tradicionalno branljive meje zaščite podatkov postale zamegljene.

V družbi Huawei menimo, da novi izzivi ne smejo biti izgovor za neaktivnost. Izzivi so del tehnološkega napredka in družbenega napredka in se jih ne smemo izogibati.

Varnost, vgrajena v inovacijski proces

Kot ponudnik tehnologije v digitalni dobi je ena prvih nalog za Huawei iskanje inovativnih načinov za izgradnjo varnosti v naše inovativne tehnologije. Tu je nekaj naših ključnih pobud:

- varnost kot steber korporativnega upravljanja,
- aktivno raziskovanje nove tehnologije in
- novi varnostni koncepti.

Poglobljena analiza za ustrezno zaščito potrebuje tehnologijo množičnih podatkov za primerjavo trenutnih sistemskih podatkov z znanimi zlonamernimi vedenji. Prav tako zahteva uporabo AI za oceno, katere postopke bi bilo treba dovoliti, da se nadaljujejo, in katere bi bilo treba premestiti v izolirano okolje in podrobno pregledati. Varnostne politike je treba sprotno posodabljati, da bi preprečili nadaljnje širjenje morebitnih zlonamernih kod in tako v celoti izkoreniniti grožnje.

Za izgradnjo teh varnostnih konceptov v Huaweieve izdelke in rešitve je Huawei od leta 2012 sprejel naslednje varnostne prakse, kot so Varnost v razvoji, Varnost po načrtu (Security by design) in neodvisno varnostno preverjanje v Huaweiev varnostni okvir.

Varnost dobavne verige od začetka do konca

Raziskave, proizvodnja, dobava in uporaba izdelkov IKT so močno odvisni od globalizirane dobavne verige. Zato morajo naše varnostne prakse zajemati tudi celotno oskrbovalno verigo. Interno to pomeni vsako fazo proizvodnje, dostave in storitve izdelka, navzven pa vključuje upravljanje dobaviteljev. Celovita end-to-end varnost je zapletena in zahteva zelo sistematičen pristop z zavezanostjo vseh zainteresiranih strani. Posebej pomembna so naslednja vprašanja:

Sledljivost strojne in programske opreme

Kompleksne tehnologije vključujejo na tisoče komponent in milijone vrstic kode. Zagotoviti moramo, da je vsak sestavni del vsakega izdelka sledljiv in prepoznan. Huawei lahko sledi vsem zamenljivim komponentam do ravni enega kondenzatorja ali diode. Za programsko opremo imamo hitro sledljivost na ravni izvorne kode.

Varno uvajanje in vzdrževanje

Varnost med uvajanjem in vzdrževanjem izdelkov neposredno vpliva na varnost in stabilnost omrežij strank in tudi na storitve, ki se na njih izvajajo. Huawei usklajuje svoje dostavne procese s svojimi strankami in strogo izpolnjuje lokalno zakonodajo ter zahteve stranke glede kibernetske varnosti, tako za delovanje v procesnem okolju kot tudi za vzdrževanje na daljavo. Huaweijeva notranja programska oprema in orodja težijo k popolni skladnosti procesov na vsakem koraku.

Upravljanje dobaviteljev

Če tehnologija ali procesi dobavitelja niso varni, ogrožajo varnost proizvodov in storitev, ki se dobavljajo končnim strankam. Huawei je bilo prvo podjetje v komunikacijski industriji, ki je s svojimi dobavitelji podpisalo sporazum o kibernetski varnosti, ki jim bo pomagal okrepiti varnost svojih izdelkov in storitev. Pri izbiri in reviziji dobaviteljev Huawei ocenjuje in preizkuša njihove sisteme kibernetske varnosti in kakovost njihovih varnostnih nadzorov. Samo dobavitelji, ki opravijo te revizije, lahko postanejo Huaweievi partnerji.

Kibernetska varnost mora biti del kulture podjetja

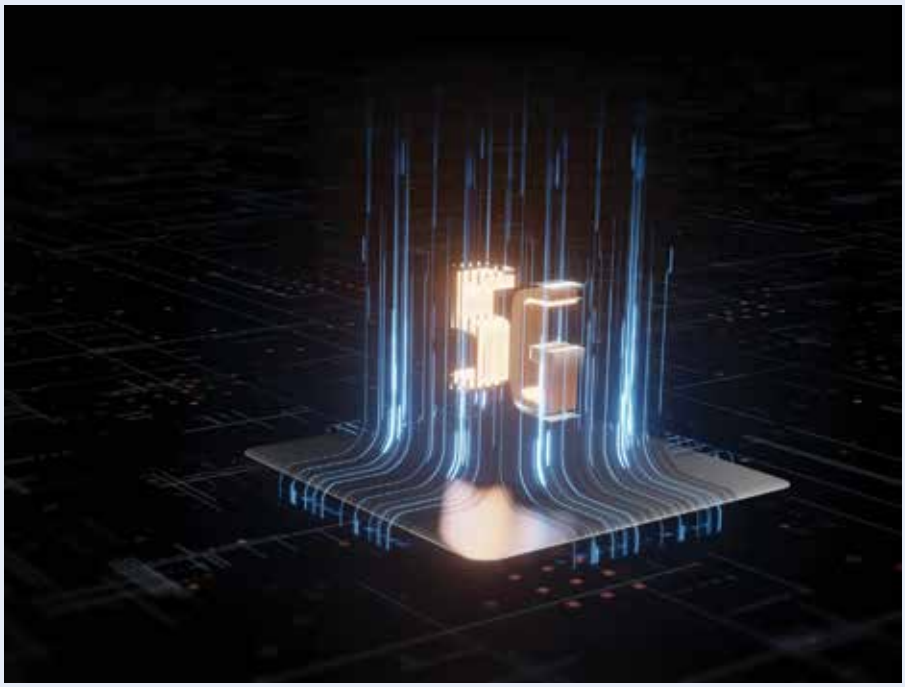
Kibernetske varnost ni le vprašanje tehnologije, temveč tudi ljudi. To bi moral biti pomemben poudarek pri zaposlovanju, usposabljanju in motivaciji zaposlenih. Huawei deluje v več kot 170 državah in regijah ter redno izvaja izobraževanje in usposabljanje o kibernetski varnosti svojim 180.000 zaposlenim. Vsi zaposleni v Huaweiju morajo opraviti test iz kibernetske varnosti in podpisati Huaweieva navodila za poslovno ravnanje, ki vključujejo poglavje o kibernetskem varovanju. Kibernetska varnost je ključna kompetenca v Huaweievem sistemu notranjega ocenjevanja spretnosti in predstavlja obvezno usposobljenost za številne položaje.

Varnost s sodelovanjem

Današnja omrežja so raznolika in obsežna. Ponudniki tehnologije ne morejo biti samo arhitekti varnosti. Zgraditi morajo skupno ozaveščenost o kibernetski varnosti s celotnim ekosistemom. Aktivno sodelovanje bo tako ključnega pomena za učinkovito upravljanje kibernetske varnosti.

HUAWEI

Več: https://carrier.huawei.com/



PROMO

Foto: KraftART

Etično hekanje pomeni izvajanje varnostnih pregledov, penetracijskih testov ali varnostnih analiz z vednostjo naročnika in v kontroliranem okolju.

CYBER
Interreg Europe
European Union
European Regional
Development Fund

Kibernetska varnost

CYBER Night: S hekanjem do novih kadrov

Etično hekanje ni samo obrt, ampak tudi miselna naravnanost.

Željka Kelkedi, Služba za razvoj kadrov in izobraževanje, GZS

Ustrezne kadre, ki bi zagotavljali manjšo ranljivost podjetij, je težko pridobiti.

V Evropi in Sloveniji v zadnjih letih podjetja poročajo o pomanjkanju kvalificiranih kadrov na področju kibernetske varnosti. Ob tem pa obseg groženj in napadov na podjetja, še posebej na mala in srednja, skokovito narašča. Ustrezne kadre, ki bi zagotavljali manjšo ranljivost podjetij, je težko pridobiti, in sicer ne le zaradi pomanjkanja specializiranega študijskega programa, ampak tudi zaradi same narave poklica, ki je zelo praktično usmerjen. Etično hekanje, ena izmed metod zagotavljanja informacijske varnosti tako kritične infrastrukture kot podjetij, pri kateri etični hekerji izvajajo varnostne preglede, penetracijske teste ali varnostne analize z vednostjo naročnika in v kontroliranem okolju, še najboljše ponazori slednjo trditev. Da etično hekanje ni samo obrt, ampak tudi miselna naravnanost, priča skupina etičnih hekerjev v Sloveniji, ki z različnimi aktivnostmi prispeva k opolnomočenju kadrov na področju kibernetske varnosti.

Pogovor z udeleženci CYBER Nighta je razkril, da etični hekerji pogrešajo praktično usposabljanje in mentorstvo s strani strokovnjakov iz podjetij.

V okviru projekta CYBER (ki spada v program Interreg Europe), katerega partner je tudi Gospodarska zbornica Slovenije (GZS), smo na GZS v sodelovanju s skupnostjo etičnih hekerjev oktobra letos organizirali prvi CYBER Night – hekersko tekmovanje, t. i. Capture the Flag. Tekmovalci se v takem načinu tekmovanja soočajo z najrazličnejšimi izzivi na področju iskanja ranljivosti sistemov ter vdiranja v sisteme, pridobivanja zaupnih podatkov in premagovanja varnostnih ovir, testirajoč tako svoje znanje iz računalniških omrežij, sistemov, programiranja kot tudi kriptografije idr. Med reševanjem izzivov hekerji pobirajo »zastave«, od tod tudi ime tekmovanja.

Pogovor z udeleženci CYBER Nighta je razkril, da še bolj kot to, da v Sloveniji pogrešajo specializirani študijski program informacijske oz. kibernetske varnosti, pogrešajo praktično usposabljanje in mentorstvo s strani strokovnjakov iz podjetij. Namreč, pri etičnem hekanju štejejo predvsem praktične izkušnje ter hekerska miselna naravnanost. Hekatoni, kot denimo CYBER Night, tako po eni strani predstavljajo priložnost za izobraževanje novih etičnih hekerjev, po drugi strani pa za podjetja s stalno naraščajočimi in spreminjajočimi se potrebami na področju kibernetske varnosti predstavljajo enega od načinov iskanja talentov in pridobivanja kadrov. gg

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Za zagotavljanje kibernetske varnosti je ključen nenehen nadzor

Vsa podjetja, ne glede na to, s čim se ukvarjajo, so izpostavljena različnim varnostnim tveganjem, napadi pa postajajo vse pogostejši.

»Kot podjetje, ki nudi telekomunikacijske storitve, smo za napade zanimivi iz dveh različnih zornih kotov,« pravi Bojan Brodar, direktor informacijske varnosti v družbi Telemach. Tako so lahko napadi usmerjeni neposredno v podjetje in njegovo poslovanje, lahko pa z napadom vplivajo oziroma napadejo njihove naročnike. To se lahko na primer zgodi preko tako imenovanega zvabljanja oziroma phishing napadov, socialnega inženiringa, škodljive kode in izsiljevalskega programja. »Cilj takih napadov je priti do informacij, dostopov do podatkov ali v primeru izsiljevalskega programja zaklep podatkov in izsiljevanje podjetij ali posameznikov, da plačajo za ključ, ki podatke znova odklene,« pojasni direktor. Doda, da so kot ponudnik storitev bolj izpostavljeni DDOS napadom in napadom na imenske (DNS) strežnike, kjer je cilj motnja ali prekinitev zagotavljanja oziroma delovanja storitev.

Vse bolj privlačni osebni podatki

Na to, koliko je katero podjetje zanimivo napadalcem, vplivajo različne stvari. Pri telekomunikacijskih podjetjih so npr. zanimivi osebni podatki, ki jih je veliko, zato bi njihova kraja ali izbris oziroma kakršna koli manipulacija z njimi naredila precej škode – neposredne pri poslovanju ali posredno z razkritjem in postopki ter kaznimi, ki bi sledile. Na drugi strani pa bi posreden napad na naročnike z DDOS napadom ali DNS napadom, ki bi vplival na delovanje storitev, lahko močno in negativno vplival zelo široko – na delovanje podjetij, državnih ustanov, šol itd. »Ravno v današnjem času, ko je delo in šolanje od doma aktualnejše, bi tak napad že pri naročnikih povzročil veliko nejevolje, kaj šele pri vseh podjetjih, državnih ustanovah itd. Slednje bi lahko potencialno ohromilo delovanje države,« pove Brodar in doda, da lahko v obeh primerih nastane neposredna finančna škoda, veliko škodo pa utrpi tudi ugled podjetja, ki ima lahko dolgoročne negativne posledice.

Nadzor izvajajo s pomočjo nadzornega centra

V Telemachu zagotavljajo kibernetsko varnost z vidika več varnostnih plasti in z različnimi ukrepi. »Ključen je nenehen nadzor, ki ga opravljamo s pomočjo nadzornega centra, ki spremlja dogodke 24/7, v ozadju pa imamo tako organizacijske kot tehnične ukrepe, ki zagotavljajo neprekinjeno delovanje podjetja in storitev našim naročnikom,« pove Brodar. Doda, da sistem varovanja informacij sloni na standardu ISO 27001, ki so ga tudi certificirali. »Če naštejem nekatere od ukrepov, so to: segmentacija in omejevanje dostopov do omrežja in sistemov, redne varnostne posodobitve sistemov, napredna orodja za zaznavo odstopanj v internem omrežju in e-pošti, požarni zidovi, orodja za omejevanje DDOS napadov itd.,« pove sogovornik.

Za poslovne uporabnike v pripravi nova ponudba

Poudari, da za področje poslovne prodaje, kjer so naročniki bolj izpostavljeni, že pripravljajo ponudbo za izboljšanje kibernetske varnosti. Poleg tega bodo še naprej veliko vlagali v to področje. Na njem vsako leto izvajajo posodobitve in nadgradnje obstoječih rešitev ter dodajajo nove plasti in nove rešitve, ki pripomorejo k varnemu in neprekinjenemu poslovanju podjetja in zagotavljanju storitev.

telemach

Kibernetska varnost v času korone

Ali sploh znamo pravilno komunicirati?

Odnos do spletnih prevar in napadov preko spleta je večplasten: del javnosti zadeva sploh ne zanima, delu javnosti je vseeno (dokler sami ne postanejo žrtve), drugi pa menijo, da so prevare pravzaprav »vseprisotne« in jih je pretirano strah. Ključno je seveda informiranje in ozaveščanje, da bomo vedeli, kaj je res in kaj ne.

dr. David Modic in dr. Mojca Ciglarič, Fakulteta za računalništvo in informatiko, Univerza v Ljubljani

Imajo prevaranti v času korone več časa? Verjetno ne. Že prej so delali »na polno« in tudi sedaj je tako.

Ta prispevek piševa od doma. Tako kot marsikdo drug hodiva v službo in po opravkih le takrat, ko res morava. Morda se je prav v teh nenavadnih koronskih časih še bolj jasno pokazalo, da imamo tisti, ki se ukvarjamo z varnostjo in prevarami na spletu, težavo z jasnim komuniciranjem. Poglejmo, zakaj.

Koliko je v resnici incidentov?

Marsikdo meni, da bi kot strokovnjaka za kibernetsko varnost morala biti v tem času, torej v času koronavirusa, do vratu v delu – po njihovem je napadov in prevar preko spleta vedno več. Poročila nacionalnega odzivnega centra za kibernetsko varnost SI-CERT pa ne kažejo kakega bistvenega porasta incidentov; prejemajo sicer bistveno več prijav kot običajno, ampak večinoma gre za večkratne prijave istega incidenta. Vprašajmo se, zakaj bi bilo napadov in prevar v času korone več. Imajo prevaranti več časa? Verjetno ne. Že prej so delali »na polno« in tudi sedaj je tako.

Po eni strani nekatere večje organizacije zaznajo poskus vdora vsakih 5 minut, 24 ur na dan, vsak dan v letu, po drugi strani pa filtri neželene pošte zaustavijo milijone prevar vsak mesec, mi pa to opredelimo »le« kot neželeno pošto.

Od ignorance oziroma indiference do pretiranega strahu

Vemo, da spletne prevare in napadi del javnosti zanimajo, delu javnosti pa je vseeno – to se njih ne tiče, dokler se jih čez noč ne »dotakne«, ko namreč tudi sami postanejo žrtve spletnih prevarantov. Po drugi strani je veliko ljudi prepričanih, da so prevare vseprisotne in da se izgube v gospodarstvu in družbi na letni ravni merijo v dvomestnih številkah v obliki odstotka bruto domačega proizvoda (BDP).

Do tako različnih mnenj prihaja zato, ker poznamo različne zgodbe. Ena je ta, da je poskusov vdorov in prevarantskih pisem kar precej. Podatki, ki jih imamo za neko večjo organizacijo, kažejo, da zaznajo poskus vdora vsakih 5 minut, 24 ur na dan, vsak dan v letu. Ampak tu leži zagata. Druga zgodba je namreč ta, da filtri neželene pošte zaustavijo milijone prevar vsak mesec, mi pa to opredelimo »le« kot neželeno pošto.

Raziskave kažejo, da so resnične žrtve redke. Zakaj torej tak strah? Morda zato, ker so izgube, ko do njih pride, precejšnje. Morda zato, ker smo ljudje taki, da nas bolj strašijo stvari, ki jih ne razumemo. Morda tudi zato, ker gre za vdor v prostor, kjer se načeloma počutimo varne – na primer doma, če izgubo utrpimo iz domačega naslanjača, ali pa v službi, če podjetje, kjer smo zaposleni, kar naenkrat izgubi stranke in posel ter začne odpuščati.

Foto: Depositphotos

Način komuniciranja se je spremenil – primer aplikacije Zoom

V času omejitev zaradi COVID-19 se je spremenil predvsem način komuniciranja. Mnogo več je uporabe telekonferenčnih sistemov, število dnevnih uporabnikov aplikacije Zoom je denimo naraslo iz predkoronskih 10 na sedanjih 300 milijonov uporabnikov. Vprašanje je, ali se uporabniki zavedamo, kakšnim grožnjam zasebnosti se izpostavljamo pri uporabi takšnih sistemov? Aplikacija sama morda ni nič bolj varna ali nevarna, kot so še mnoge druge, ki jih pogosto uporabljamo, kljub temu pa je prav, da se z vsako novo aplikacijo zavedamo tudi tveganja, ki ga prinaša njena uporaba.

Že v letošnjem aprilu, zelo kmalu po začetku pandemije, so se začeli na medmrežju pojavljati zapisi, ki so opozarjali na težave z varnostjo in zasebnostjo Zooma. Vsak uporabnik je pred začetkom uporabe aplikacije potrdil izjavo, s katero je aplikaciji dovolil početi z njegovimi podatki (to vključuje tudi posnetke sestankov in pogovorov) skoraj karkoli. Ključni podatki niso bili šifrirani, varnost sistema je bila na zelo osnovni ravni. Mobilna aplikacija je pošiljala podatke Facebooku celo, če uporabnik tam sploh ni imel računa. Nekatera podjetja in šole so uporabo omenjene aplikacije prepovedala, drugi so jo uporabljali naprej, ampak takrat so vsaj že vedeli, kakšno tveganje s tem prevzemajo. Ko so kritike postale dovolj glasne, je Zoom večino očitanih težav odpravil. Naj poudariva, da primera ne opisujeva zato, da bi se opredeljevala za ali proti omenjeni aplikaciji, temveč zato, da pokaževa, kako pomembno je, da smo kot uporabniki dobro informirani! To je ključno! Uporabnik mora vedeti, kakšna so tveganja. Če smo hudomušni, lahko uporabimo druge besede: pogosto nam manjka domišljije, na kakšne načine lahko nekdo drug uporabi naše podatke. Za vsako aplikacijo moramo vedeti, ali prinaša tudi morebitne nevarnosti, te pa je dobro tehtati z njenimi koristmi.

Podcenjevanje vs zastraševanje

Težava strokovnjakov na področju informacijske varnosti je, da ne znamo in včasih tudi nočemo hoditi po tanki črti med podcenjevanjem objektivne stiske posameznika in neosnovanim zastraševanjem širnega sveta. Resnica je dovolj učinkovita: vdori in prevare pogosto niso uspešni. Kadar pa so, je to za posameznika lahko katastrofa.

Bodite pripravljeni!

Ni potrebe po tem, da bi bili panični, je pa dobro, če ste pripravljeni. Podobno kot v primeru, ko dobimo kot novopečeni vozniki avtomobila v roke vozniški izpit: neizkušeni voznik bo za volanom bistveno bolj napet in prestrašen kot pa izkušeni voznik. Nihče od njiju sicer ne pričakuje nesreče, oba pa imata v prtljažniku škatlo prve pomoči. Tako je tudi glede kibernetske varnosti dobro biti informiran in pripravljen, ni pa nobene potrebe po strahu ali celo paniki. gg

Raziskave kažejo, da so resnične žrtve redke. Zakaj torej tak strah? Morda zato, ker so izgube, ko do njih pride, precejšnje.

Vprašanje je, ali se uporabniki zavedamo, kakšnim grožnjam zasebnosti se izpostavljamo pri uporabi različnih video komunikacijskih sistemov?

Akademija FRI

Na Fakulteti za računalništvo in informatiko v okviru Akademije FRI potekajo različne delavnice in tečaji, ki približajo varnost sleherniku. Fakulteta izvaja osnovna varnostna ozaveščanja za splošno populacijo, pa tudi tečaje s podrobnejšo in bolj poglobljeno vsebino, ki jo lahko oblikujemo tudi v dogovoru z naročnikom.

Epidemija v Sloveniji

Ponovno razglašena epidemija COVID-19

Vlada RS je pozno zvečer v nedeljo, 18. oktobra, na podlagi Zakona o nalezljivih boleznih izdala Odlok o razglasitvi epidemije nalezljive bolezni COVID-19 na območju celotne države. Razglasitev epidemije velja 30 dni.

Ana Vučina Vršnak

Poveljnik Civilne zaščite Srečko Šestan je drugi dan po razglasitvi epidemije, torej v ponedeljek, 19. oktobra, zjutraj, izdal sklep o aktiviranju državnega načrta zaščite in reševanja.

V Sloveniji se glede na uradne podatke o številu okuženih soočamo z drugim valom epidemije nalezljive bolezni COVID-19, je sporočila Vlada. »Priča smo njenemu hitremu in eksponentnemu širjenju med populacijo, ki močno presega normalno obolevnost oziroma incidenco. Aktualne epidemiološke razmere v zvezi s širjenjem okužbe z virusom SARS-Cov-2 zahtevajo takojšnjo razglasitev epidemije na celotnem območju Republike Slovenije, saj vse statistične regije dosegajo oziroma presegajo stopnjo incidence, ki zahteva razglasitev epidemije,« je navedla Vlada.

Poveljnik Civilne zaščite Srečko Šestan je drugi dan po razglasitvi epidemije, torej v ponedeljek, 19. oktobra, zjutraj, izdal sklep o aktiviranju državnega načrta zaščite in reševanja. Ta omogoča, da poleg zdravstvenih in drugih služb država uporabi tudi sile in sredstva za zaščito, reševanje in pomoč.

Posamezniki, ki bi želeli pomagati, se lahko obrnejo na občinske odbore Civilne zaščite.

Foto: Depositphotos

Kot so sporočili iz uprave za zaščito in reševanje, bo Ministrstvo za zdravje RS izdajalo strokovna priporočila in o njih tekoče obveščalo poveljnika Civilne zaščite, ta pa bo zagotovila potrebno število strokovnih sodelavcev, ki bodo zagotavljali ustrezen operativni odziv glede na razvoj razmer in potrebe po zaščiti, reševanju in pomoči ter podporo poveljnikom in štabom Civilne zaščite.

Vsi organi, ki so določeni v državnem načrtu zaščite in reševanja ob pojavu epidemije nalezljive bolezni pri ljudeh, so v skladu z omenjenim načrtom dolžni izvajati aktivnosti ter upravi za zaščito in reševanje vsak dan do 17. ure posredovati poročilo o razmerah, aktivnostih in izvedenih ukrepih.

Z aktiviranjem državnega načrta zaščite in reševanja ob pojavu epidemije nalezljive bolezni pri ljudeh so aktivirani tudi načrti zaščite in reševanja na ravni regij in občin, izpostave in regijski štabi pa izvajajo naloge v regijah ter morajo o tem prav tako dnevno poročati vodstvu uprave.

Vključitev prostovoljcev

Srečko Šestan je javnosti predstavil glavna področja nalog, ki jim jih nalaga državni načrt ob razglasitvi epidemije. Gre za nudenje storitev dveh mobilnih laboratorijev, za ekipe reševalcev in ekipo gasilcev, ki izvajajo dezinfekcijo in dekontaminacijo objektov. Civilna zaščita opravlja tudi vlogo razdeljevanja zaščitne opreme.

Civilna zaščita je na voljo tudi sistemu zdravstva, v tem trenutku je to pomoč pri postavljanju mobilnih enot za vstopne kontrolne točke testiranj.

Posamezniki, ki bi želeli pomagati obstoječim ekipam, se lahko obrnejo na občinske odbore, kjer jih bodo predvsem vključili v naloge razdeljevanja pomoči posameznikom, ki bodo pomoč potrebovali.

Dodati velja še, da je vodja strokovne skupine za zajezitev in obvladovanje epidemije COVID-19 pri Ministrstvu za zdravje RS Bojana Beović v ponedeljek, 19. oktobra, predstavila podatek, da je okuženih okoli en odstotek vseh prebivalcev države – to je preračunano 20.000 oseb, kar je več kot uradno 7.103 aktivnih primerov. gg

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Foto: arhiv URSZR

Civilna zaščita se je pri operativi prvič srečala z nevarnostjo v obliki virusa, ki je stalno prisoten, vendar neviden. »To je neka druga zgodba, ki se ne more primerjati z ničimer, kar so nas učili,« pravi Sandi Curk.

Zaščita in reševanje

Strnjene vrste vseh sil tudi v primeru epidemij

Sile za zaščito, reševanje in pomoč so razpoložljive zmogljivosti države, lokalnih skupnosti, podjetij, zavodov in vseh ostalih za pomoč ob naravnih ali drugih nesrečah, seveda tudi v primeru epidemij. Med drugim so tu enote in službe Civilne zaščite, Policije, Slovenske vojske.

Samo Hribar Milič, Ana Vučina Vršnak

V siceršnjih, sedaj bi jim morda celo lahko rekli »normalnih« razmerah, se Uprava Republike Slovenije za zaščito in reševanje (URSZR) z različnimi silami za zaščito, reševanje in pomoč (med njimi je Civilna zaščita) ukvarja predvsem z naravnimi nesrečami. A koronavirus je zadevo spremenil. »Pri izvajanju operativnih nalog smo se prvič srečali z nevarnostjo v obliki virusa, ki je med nami stalno prisoten, vendar neviden. To je neka druga zgodba, ki se ne more primerjati z ničimer, kar so nas učili.« Tako je svoj vtis in doživljanje dogajanja zaradi koronavirusa opisal Sandi Curk, poveljnik regijskega štaba za civilno zaščito za Notranjsko in Kras. Sredi julija letos je URSZR v sodelovanju z Nacionalnim inštitutom za javno zdravje (NIJZ) ter drugimi ministrstvi in vladnimi službami objavila Državni načrt zaščite in reševanja ob pojavu epidemije oziroma pandemije nalezljive bolezni pri ljudeh, verzija 2.0, ki je nadgradnja verzije 1.0 z izkušnjami, ki jih je država pridobila v času epidemije COVID-19 od marca do maja 2020.

Varstvo pred naravnimi in drugimi nesrečami sicer zajema varstvo ljudi, živali, premoženja, kulturne dediščine in okolja pred naravnimi in drugimi nesrečami, da se zmanjša število nesreč, ter prepreči oziroma zmanjša število žrtev in drugih posledic. Ta celovit sistem organizirajo država, občine in druge lokalne skupnosti. Curk, ki je bil med drugim priča dogajanju v Perutnini Pivka (več o tem na strani XXX) – to je bil namreč eden večjih žarišč v »njegovi« regiji, ki so ga uspeli obvladati, poudarja prav to skupno delo gospodarstva, strokovnih ustanov in lokalne samouprave: sodelovanje vodstva družbe, NIJZ, tudi župana občine Pivka, ki je ob pomoči Občinskega štaba za civilno zaščito sprejel omejitvene ukrepe na celotnem območju občine. »Vsi ukrepi pa ne bi zadostovali, če ne bi s svojim pozitivnim odnosom sodelovali tudi občani,« je prepričan Curk.

»Bili smo prva linija, ki je pričela s šivanjem zaščitnih mask. V dveh tednih smo dosegli, da je prebivalstvo in gospodarstvo prejelo potrebno količino.

Najstarejša gospa, ki je prostovoljno šivala maske, je imela čez 90 let.

Moram poudariti, da so se maske šivale po vaseh in društvih. Pri šivanju so sodelovale poklicne in ljubiteljske šivilje. Najstarejša gospa, ki je prostovoljno kot nekdanja profesionalna šivilja pristopila k šivanju, je imela čez 90 let,« razlaga Curk.

Od nas samih je odvisno, ali bo prihod koronavirusa zaustavil delovni proces in normalni potek življenja.

Da prihod koronavirusa ne bi zaustavil delovnega procesa

Podjetnikom in gospodarstvenikom pravi: »Od nas samih je odvisno, ali bo prihod koronavirusa zaustavil delovni proces in normalni potek življenja. Ni dovolj, da samo poskrbimo za ukrepe in jih začnemo izvajati, pomembno je, da zaposleni razumejo, zakaj in kako se morajo obnašati.« Takojšnje ukrepanje, predvsem pa vsakodnevno izvajanje ukrepov, je največje zagotovilo, da bo delovni proces deloval naprej, s tem pa zadovoljstvo tako vseh zaposlenih kot celotne družbe, pravi Curk, ki je prepričan, da si Slovenija »ne more privoščiti vnovičnega zapiranja gospodarstva«.

COVID-19 je tako v Sloveniji kot v Evropi v porastu. Širjenju pomagajo tudi vremenski pogoji, pred nami pa je še sezona gripe. Curk ocenjuje, da Vlada RS ob veliki pomoči strokovnjakov in NIJZ zagotavlja vse ukrepe za zajezitev virusa. »Od te točke naprej smo mi tisti, na katerih temelji ta zaustavitev,« je prepričan.

Ne želimo se zavedati, da lahko en sam primer okuženega v podjetju privede do situacije, ko moramo zapreti cel proizvodni proces.

»V kolikor se ne bomo zbudili in pričeli slediti navodilom stroke in dosledno uporabljali edino, kar imamo na razpolago (zaščitne maske, razkuževanje rok, varnostna razdalja), nam ni pomoči. Kljub stalnim opozarjanjem stroke in sporočil Vlade RS se še vedno izvajajo srečanja in zabave, tako v zasebnih krogih kot javnih ustanovah. Ne želimo se zavedati, da lahko en sam primer okuženega v podjetju privede do situacije, ko moramo zapreti cel proizvodni proces,« opozarja. Posledic koronavirusa se ne boji, zelo pa se boji zaustavitve gospodarskega sistema, ki bi lahko pripeljal do izgube delovnih mest, velikih osebnih stisk in na koncu lahko tudi do lakote.

So podjetja in predstavniki oblasti dovolj pozorni in skrbni v pripravah vsega potrebnega za spoprijemanje z temi razmerami? Curk pravi, da so »predstavniki gospodarstva v regiji svoje poslanstvo izvedli odgovorno«,

Foto: Civilna zaščita

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Foto: UN Photo/OCHA/Mark Garten

13. oktobra obeležujemo mednarodni dan zmanjševanja tveganj nesreč

Generalna skupščina Združenih narodov je z namenom spodbujanja globalne kulture zmanjšanja tveganj nesreč 13. oktober razglasila za mednarodni dan zmanjšanja tveganj nesreč (angl. International Day for Disaster Risk Reduction).

Ta dan predstavlja priložnost za ocenjevanje napredka pri zmanjševanju tveganja nesreč in njegovem vplivu na izgube življenj, premoženja in zdravja v skladu s Sendajskim okvirom za zmanjšanje tveganja nesreč 2015–2030, sprejetim na tretji svetovni konferenci Združenih narodov o zmanjšanju tveganja nesreč marca 2015 na Japonskem, so pojasnili na Upravi RS za zaščito in reševanje.

Leta 2016 je generalni sekretar OZN spodbudil začetek kampanje »Sendai Seven Campaign«, ki se osredotoča na promocijo vsakega od sedmih sendajskih ciljev v naslednjih sedmih letih. Cilj za leto 2020 je cilj E: »Znatno povečati število držav z nacionalnimi in lokalnimi strategijami za zmanjšanje tveganja nesreč do leta 2020«, ki postavlja temelje za izvajanje Sendajskega okvira in je tesno povezan s prednostno nalogo 2: »Krepitev upravljanja za obvladovanje tveganj nesreč«.

V skladu s poudarkom letošnjega mednarodnega dneva za zmanjšanje tveganj nesreč o vplivu nesreč na življenje in počutje ljudi je letošnja tema namenjena posredovanju sporočila, da se je mogoče številnim nesrečam izogniti ali jih preprečiti, če obstajajo strategije za zmanjševanje in obvladovanje tveganja nesreč.

Slovenija aktivnosti zmanjševanja in obvladovanja tveganj nesreč uveljavlja skozi Resolucijo o nacionalnem programu varstva pred naravnimi in drugimi nesrečami v letih od 2016 do 2022, strategijo trajnostnega razvoja pa v okviru Strategije razvoja Slovenije do leta 2030. Uprava RS za zaščito in reševanje kot nacionalna kontaktna točka za Sendajski okvir se aktivno vključuje v vsa področja zmanjšanja tveganja nesreč, v zadnjem obdobju predvsem v povezavi s podporo državi pri odzivu na pandemijo COVID-19.

tako da je Notranjska s Krasom »ena od vzornih regij«. Poleg vseh ukrepov za zaščito dnevno potekajo informativni pogovori z zaposlenimi, tako da lahko iz delovnega procesa napotijo po zdravstveno pomoč vsakega delavca z najmanjšimi simptomi bolezni. Ker so pred nami najbolj kritični meseci, je po njegovi oceni »takojšnje ukrepanje, predvsem pa vsakodnevno izvajanje ukrepov, največje zagotovilo, da bo delovni proces tekel naprej«.

Foto: arhiv URSZR

Za opremo precej sredstev

Civilna zaščita za doseganje svoje visoke ravni usposobljenosti temelji na rednem izobraževanju in nujni opremi za zaščito in reševanje. Večino tehnične opreme zagotavljajo občine same in zanjo namenjajo zelo velika sredstva, pravi Curk. Vendar pa se je treba v razmerah širjenja koronavirusa kljub pomoči države in vseh javnih služb še dodatno znajti. Sogovornik poudari, da je večina podjetij v regiji pristopila k izdelavi zaščitnih vezirjev s pomočjo 3D tiskalnika, v nekaterih podjetjih pa so delavke pričele s šivanjem zaščitnih mask. »Zaščitne opreme in sredstev imamo v tem trenutku dovolj, imamo pa premalo odgovornosti in skrbi za svoje lastno zdravje. Sledimo ukrepom in priporočilom stroke,« še izpostavi regijski poveljnik Civilne zaščite za Notranjsko in področje Krasa Sandi Curk. gg

Foto: arhiv URSZR

Foto: arhiv URSZR

Civilna zaščita za doseganje svoje visoke ravni usposobljenosti temelji na rednem izobraževanju in nujni opremi za zaščito in reševanje.

Uprava RS za zaščito in reševanje (URSZR) opravlja upravne in strokovne naloge organiziranja, priprav in izvajanja varstva pred naravnimi in drugimi nesrečami in je organ v sestavi Ministrstva za obrambo RS. Sile za zaščito, reševanje in pomoč so razpoložljive zmogljivosti države, lokalnih skupnosti, gospodarskih družb, zavodov ali drugih organizacij za zaščito, reševanje in pomoč ob naravnih ali drugih nesrečah. Glede na način vključevanja in sodelovanja državljanov se delijo na prostovoljne, poklicne in dolžnostne. Posamezne enote in službe se lahko organizirajo tudi v kombinaciji poklicnih in prostovoljnih članov. Prostovoljne enote in reševalne službe so organizirane pri nevladnih, predvsem humanitarnih organizacijah. Njihovo delovanje je dopolnjeno s poklicnimi reševalnimi službami. Poklicne enote in službe za zaščito, reševanje in pomoč so samostojne enote oziroma službe, ki delujejo tudi na področju zaščite in reševanja, ko je potrebno. Dolžnostne enote in službe za zaščito, reševanje in pomoč so organizirane kot enote in službe Civilne zaščite na podlagi državljanske dolžnosti. Naloge zaščite, reševanja in pomoči izvajajo:

- Enote, službe in drugi operativni sestavi društev in organizacij, ki opravljajo naloge zaščite, reševanja in pomoči oziroma javno službo na podlagi odločitve državnega organa ali pristojnega organa lokalne skupnosti. Sem spadajo gasilske enote, enote ter službe društev in nevladnih organizacij.
- Gospodarske družbe, zavodi in druge organizacije, ki organizirajo reševalne enote in službe na podlagi odločitve pristojnega organa lokalne skupnosti ali državnega organa in glede na tveganje v dejavnosti, ki jo opravljajo.
- Enote in službe Civilne zaščite, ki so organizirane na podlagi državljanske dolžnosti kot dopolnilne sile za zaščito, reševanje in pomoč. Organizirajo jih država, lokalne skupnosti in gospodarske družbe, zavodi ter druge organizacije, skladno z merili za organiziranje, opremljanje in usposabljanje sil za zaščito, reševanje in pomoč.
- Policija, ki zagotavlja varnost, javni red in mir ter sodeluje v reševalnih akcijah s helikopterji, skladno z razpoložljivostjo svojih sil.
- Slovenska vojska z letalsko enoto, enoto za jedrsko, kemijsko in biološko obrambo, inženirsko enoto in zdravstveno službo, pa tudi z drugimi enotami, če niso udeležene pri obrambnih nalogah.

Tiskano na papirju Vyprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Podjetje z več kot 28-letnimi izkušnjami na področju radiokomunikacijskih rešitev in visoko strokovno usposobljenim kadrom.

S pridobljenimi mednarodnimi certifikati sledimo in zagotavljamo zanesljivo, kakovostno (ISO9001:2015) in transparentno (TRACE - ID TC4172-6213) poslovanje.

KOMPAS telekomunikacije

Sodobne rešitve proizvajalca taktične opreme

L3HARRIS™
FAST. FORWARD.

FALCON III AN/PCR-160(V) širokopasovni HF/VHF taktični radijski sistem

KLJUČNE PREDNOSTI:

- prvi in edini Type 1 taktični radijski sistem, ki ustreza najsodobnejšim NSA kripto zahtevam
- najmanjša, najlažja in najhitrejša HF naprava
- prenos podatkov do 10-krat hitrejši od danes dostopnih radijskih postaj
- zagotavlja združljivost med vojaškimi enotami ZDA, kolicijskimi silami in partnerstvi za mir
- podpira neposredno zamenjavo L3HARRIS opreme za obstoječe mobilne in stacionarne radijske postaje

AN/PRC-163 večkanalna ročna radijska postaja

KLJUČNE PREDNOSTI:

- prenos skupne operativne slike vključno z videom ISR
- podpora bližnjih zračnih sil
- ognjena podpora
- omogočena komunikacija zunaj vidnega polja
- valovne oblike za taktično uporabo na mejnih področjih

... za zanesljivo in varno radijsko zvezo v vseh pogojih delovanja

Ostali partnerji: **MOTOROLA Solutions** - radiokomunikacijske rešitve, **ASC Technologies** - profesionalne snemalne naprave in programi za nadzor kakovosti, **ELBIT Systems of America** - nočnogledi, **CEOTRONICS** - audio video oprema, **VIDICODE** - rešitve za snemanje klicev, **SENSEAR** - glušniki, **ROLATUBE** - prenosljivi stolpi, **AMPHENOL PROCOM** - antene, **VICTRON ENERGY** - inverterji, polnilci, pretvorniki, **INTESO** - IT rešitve **in drugi**

Pot k sejmišču 30, 1231 Ljubljana-Črnuče | t: +386-1-5303110 | e: info@kompas-telekom.com | w: kompas-telekom.com

Zaščita in reševanje

Pomen razkuževanja

Civilna zaščita občine Kamnik ima imenovano ekipo za potrebe razkuževanja in dekontaminacije tudi ob pojavu epidemije oziroma pandemije nalezljive bolezni pri ljudeh.

Ana Vučina Vršnak

Pri razkuževanju opreme se uporabljajo predpisana sredstva za dezinfekcijo in razkuževanje, ki imajo dokazan učinek na mikroorganizm in so učinkovito sredstvo za obvladovanje širjenj pandemije.

Za potrebe razkuževanja vozil in opreme ekip uporablja smernice in priporočila Uprave RS za zaščito in reševanje, ob tem pa vso potrebno osebno varovalno opremo.z

Za potrebe razkuževanja in dekontaminacije se uporabljajo zaščitni ukrepi in naloge za zaščito, reševanje in pomoč, so nam povedali v kamniški Civilni zaščiti. Dodali so, da so potrebe glede razkuževanja povezane s prostori, opremo in vozili.

Na vprašanje, kakšna dezinfekcijska sredstva potrebujejo in katerim kriterijem morajo ustrezati, so dejali, da se pri razkuževanju opreme uporabljajo predpisana sredstva za dezinfekcijo in razkuževanje, ki imajo dokazan učinek na mikroorganizme in so učinkovito sredstvo za obvladovanje širjenja pandemije in zagotavljajo ustreznost ter varnost za uporabnika.

»Glede na uporabljeno napravo se ekipa že pogovarja o nakupu močnejše naprave z ULV dezinfekcijo,« pojasnjujejo. Za vsakodnevne potrebe razkuževanja uporabljajo ročne pršilke megle ValSept Medical v priročni 185 ml embalaži. Ekipa za dezinfekcijo prostorov in opreme uporablja naprave Fogger z možnostjo razkuževanja z ULV, pravijo.

Za potrebe razkuževanja vozil in opreme ekipa uporablja smernice in priporočila Uprave RS za zaščito in reševanje, ob tem pa vso potrebno osebno varovalno opremo.

Za dezinfekcijo, ki jo kot sredstvo za obvladovanje širjenja pandemije priporočajo strokovne institucije, so primerni izključno biocidni proizvodi, ki so kot taki registrirani pri Uradu RS za kemikalije in uvrščeni v register biocidnih proizvodov.

»Pri vsem tem je treba poudariti, da se ob vsakem izvajanju nalog razkuževanja izvajajo vsi predpisani postopki razkuževanja, uporaba naprave Fogger skladno z navodili proizvajalca in pravilno sestavo razkužila, saj le tako dosegamo učinkovito razkuževanje. To pa izvajalcem nalog tudi zagotavlja stopnjo zahtevane varnosti in zaščite,« so še povedali v Civilni zaščiti občine Kamnik. gg

Foto: PGD Kamnik

Foto: Depositphotos

Predlog je, da bi z zakonom določili prenos deleža stroškov reševanja v gorah tistim, ki ne bi bili ustrezno zavarovani.

Zavarovalnice bi lahko pripravile paket, ki bi pokrival klasično gorsko in helikoptersko gorsko reševanje.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Zaščita in reševanje

Kdo bo plačal reševanje v gorah?

Nedavno so pristojni razpravljali o tem, kako dolgoročno urediti financiranja reševanja v gorah.

Ana Vučina Vršnak

Septembra so se sešli minister za obrambo Matej Tonin, predstavniki Planinske zveze Slovenije, Gorske reševalne zveze Slovenije in Slovenskega zavarovalnega združenja. Tema pogovorov je bila dolgoročna ureditev financiranja reševanja v gorah.

Tonin je predstavil trenutno financiranje helikopterskega reševanja in predlog, po katerem bi zakonsko določili, da se delež stroškov reševanja v gorah tistim, ki ne bi bili ustrezno zavarovani, prenese na njih. Tako zbrana sredstva bi porabili izključno za financiranje reševanja v gorah, usposabljanja in izobraževanja. Tako Planinska zveza Slovenije kot Gorska reševalna zveza Slovenije tako rešitev podpirata, so sporočili z Ministrstva za obrambo.

Predstavniki zavarovalnic so povedali, da zavarovalnice paketa, ki bi pokrival klasično gorsko in helikoptersko gorsko reševanje, v Sloveniji še nimajo, a bi ga na podlagi statističnih podatkov iz preteklih reševanj lahko pripravili.

Za večjo odgovornost

Sogovorniki so se strinjali, da je treba dvigniti tudi družbeno odgovornost vseh, ki hodijo v gore, da se zavedajo, da se nesreče dogajajo in da se morajo tudi sami v gorah obnašati odgovorno. Sam sistem reševanja v gorah se ne bo spreminjal, saj je po ministrovih besedah eden najboljših v Evropi.

Število posredovanj v slovenskih gorah se iz leta v leto povečuje. Leta 2013 je Gorska reševalna služba opravila 393 intervencij, od tega 175 s pomočjo helikopterja, lani pa 604 intervencije. Kar 255-krat jim je na pomoč priskočil helikopter. Stroški helikopterskih intervencij v gorah so samo obrambno ministrstvo lani stali 580.000 EUR. gg

Sistem reševanja v gorah se ne bo spreminjal, saj je po ministrovih besedah eden najboljših v Evropi.

novatel

Satelitski internet

Sistem omogoča dostop do širokopasovnega interneta kjerkoli po Evropi in za delovanje ne potrebuje kabelskih priključkov, saj vsa internetna komunikacija poteka preko visoko zmogljivega satelita. Uporaba satelitskega interneta je namenjena na geografskih lokacijah, kjer druge povezave niso mogoče. Sistem se lahko uporablja kot stacionarna enota in kot prenosna enota na vozilu ali v kovčku.

STACIONARNA ANTENA
namenjena pritrditvi
na želeno lokacijo

tooway
Fast internet for everyone

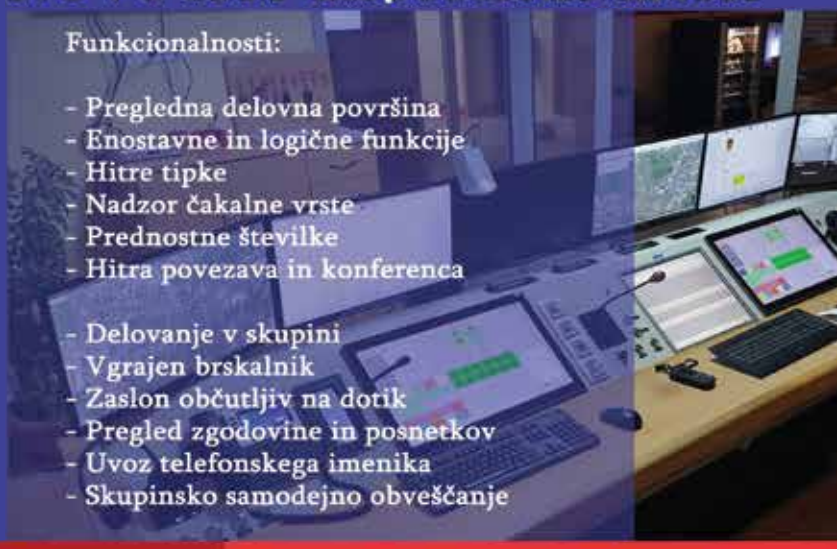
newspotter

ANTENA ZA NA VOZILO
avtomatsko iskanje
signala

ANTENA V KOVČKU
avtomatsko iskanje
signala

Upravljanje s celotno telefonsko komunikacijo preko zaslona na dotik, NOVT4000 omogoča tudi upravljanje z vrati, lučmi, zapornicami in z drugo opremo.

NOVT4000 dispečersko mesto



Funkcionalnosti:

- Pregledna delovna površina
- Enostavne in logične funkcije
- Hitre tipke
- Nadzor čakalne vrste
- Prednostne številke
- Hitra povezava in konferenca

- Delovanje v skupini
- Vgrajen brskalnik
- Zaslon občutljiv na dotik
- Pregled zgodovine in posnetkov
- Uvoz telefonskega imenika
- Skupinsko samodejno obveščanje

ASK
ALARM • SMS • KONFERENCA

Aplikacija za obveščanje, alarmiranje in dinamično komuniciranje + MONITORING

- **Za komunikacijo v zaprtih skupinah**
- Odlična storitev za **pametni telefon**
- **Naši uporabniki**: gasilci, reševalci, društva, bolnice, velika podjetja, ...

Oseba **zadolžena za proženje**, sprejme zahtevo za alarmiranje.

Oseba **opravi klic ali pošlje SMS** na odhodno številko ter preda sporočilo.

ASK **samodejno hkrati** kliče uporabnike ali pa jim **avtomatsko pošlje SMS**.

info@novatel.si **www.novatel.si** **082/800-820**

Foto: Depositphotos

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Policija

Zaradi COVID-19 ne zaznavajo večjih odstopanj pri kriminaliteti

Pri Policiji ocenjujejo, da je bila varnostna situacija v Sloveniji v času izvajanja ukrepov zaradi koronavirusa ugodna, ugodna pa je tudi danes, saj policija zagotavlja varnost ne glede na razmere. Kljub temu pa stalno spremljajo gibanje kriminalitete, da se lahko pravočasno odzovejo na morebitne težave.

Ana Vučina Vršnak

Policija, ki zagotavlja varnost, javni red in mir, je vse naloge na področju odkrivanja in preiskovanja kriminalitete v času od 13. marca (ko je bila prvič razglašena epidemija) do 31. maja 2020, torej v prvem obdobju izvajanja ukrepov zaradi epidemije koronavirusa, izvajala enako, kot jih je pred vzpostavitvijo trenutnega stanja oziroma do 18. oktobra, ko je bila ponovno razglašena epidemija. Ugotovili so, da so bila nekatera kazniva dejanja številčno v manjšem upadu, druga pa v manjšem porastu. »Ocenjujemo, da je bila varnostna situacija v Sloveniji v času izvajanja ukrepov ugodna, ugodna pa je tudi danes, saj policija zagotavlja varnost ne glede na razmere. Kljub navedenemu pa stalno spremljamo gibanje kriminalitete, da se lahko pravočasno in ustrezno odzivamo na morebiten porast kaznivih dejanj ali na morebitne nove pojavne oblike,« poudarjajo.

Premoženjska kriminaliteta

Pri vseh obravnavanih kaznivih dejanjih največji delež predstavlja premoženjska kriminaliteta (približno 65 %), ki zajema tatvine, velike tatvine, rope, roparske tatvine, avtomobilsko kriminaliteto, požige, kazniva dejanja zoper kulturno in naravno dediščino, goljufije, poškodovanje tuje stvari …, pri kateri Policija beleži v obdobju od 1. januarja do 21. septembra 2020 primerljivo število kaznivih dejanj glede na isto obdobje preteklega leta (oziroma 1,1 % upad). V tem obdobju so sicer obravnavali za 3,8 % manj tatvin, za 0,1 % manj velikih tatvin in za skoraj četrtino manj ropov.

Policija ugotavlja, da so bila nekatera kazniva dejanja v času epidemije številčno v manjšem upadu, druga pa v manjšem porastu.

Pri vseh obravnavanih kaznivih dejanjih največji delež predstavlja premoženjska kriminaliteta (približno 65 %).

1.032 kaznivih dejanj nasilja v družini, za katere je bila podana kazenska ovadba (10 % več kot lansko leto, ko jih je bilo 938), je letos (do 21. septembra) obravnavala Policija.

Minimalni upad kaznivih dejanj

Število obravnavanih kaznivih dejanj v letu 2020 (do 21. septembra 2020), za katera je bila podana kazenska ovadba, je po podatkih policije primerljivo s številom kaznivih dejanj v istem obdobju preteklega leta (2 % upad; 38.427 kaznivih dejanj v 2020, 39.209 kaznivih dejanj v 2019). Pri tem je treba izpostaviti, da gre za podatke v obdobju slabih devetih mesecev, kar statistično ne zaokrožuje celega statističnega leta, zato ocenjujejo le trenutni trend. K spremembi števila kaznivih dejanj v posameznih mesecih lahko vplivajo različni dejavniki, stanje pa se praviloma proti koncu leta uravnoteži. V omenjenem obdobju je primerljiva tudi stopnja preiskanosti; policija je letos preiskala 49,8 % vseh kaznivih dejanj, lani 51,4 %, pri čemer preiskave letos storjenih kaznivih dejanj, pri katerih je storilec neznan, še potekajo.

Vlomov, ki sicer spadajo v kazniva dejanja velikih tatvin, je letos za 4,6 % več kot v enakem obdobju leta 2019, pri čemer je bilo največ vlomov izvršenih v stanovanja, stanovanjske hiše v naselju in izven naselja, in na parkiriščih, vlomi na nekaterih drugih prizoriščih pa so manj številčni oziroma so v upadu. »Pri tem poudarjamo, da smo v začetku leta prijeli dve skupini tujih storilcev, za kateri še vodimo preiskavi, saj sumimo, da sta januarja in februarja izvršili več deset vlomov v stanovanja,« pravijo na Policiji.

Če pa upoštevamo zgolj obdobje od 13. marca do konca maja letos, je stanje premoženjske kriminalitete prav tako primerljivo glede na enako obdobje leta 2019 (oziroma je zaznati 3,3 % porast). Vlomov, ki sicer sodijo v kazniva dejanja velike tatvine, je bilo v obdobju izvajanja ukrepov za 9,9 % več kot v enakem obdobju leta 2019.

Premoženjska kriminaliteta v devetih mesecih letošnjega leta je torej »v primerljivih okvirih« kot lani, pri čemer tudi čas dveh mesecev in pol, torej v času izvajanja ukrepov zaradi epidemije COVID-19, bistveno ni vplival na skupno število premoženjskih kaznivih dejanj. Pri tem je treba opozoriti, da lahko vsak posameznik, z ustreznim samozaščitnim ravnanjem, stori največ za zaščito svoje lastnine oziroma s tem odvrne storilca od izvršitve kaznivega dejanja,

zaradi česar policija svetuje upoštevanje preventivnih nasvetov, ki so dosegljivi tudi na spletni strani policije.

Na področju krvnih in spolnih deliktov v prvih devetih mesecih in pol leta 2020 ni ugotovljenih večjih odstopanj v primerjavi z enakim obdobjem leta 2019.

Nekoliko v porastu družinsko nasilje

Na podlagi trenutnih statističnih podatkov pa policija ugotavlja, da so kazniva dejanja zoper zakonsko zvezo, družino in otroke v letošnjem letu nekoliko v porastu. Letos (do 21. septembra) je policija obravnavala 1.032 kaznivih dejanj nasilja v družini, za katere je bila podana kazenska ovadba (10 % več kot lansko leto, ko jih je bilo 938). V času uveljavitve ukrepov za preprečevanje epidemije (13. marec do konca maja) pa je policija obravnavala 303 kazniva dejanja nasilja v družini, kar je za 6,3 % več kot v istem obdobju lani, ko jih je bilo 285. Policija v vseh primerih odreagira in ustrezno ukrepa, v večini primerov pa je osumljencu izrečena prepoved približevanja. Kazniva dejanja zanemarjanja mladoletne osebe in surovo ravnanje pa so v letošnjem letu glede na isto obdobje lani nekoliko v upadu.

Nevarnosti na spletu

V času omejevalnih ukrepov so se otroci in mladostniki pretežno zadrževali v hišah in stanovanjih, kjer so svoj čas pogosto preživeli z uporabo računalnika. S ciljem preprečevanja storitve kaznivih dejanj in zlorab na škodo otrok in mladostnikov v dneh povečanja uporabe interneta policija svetuje staršem, naj bodo pozorni, kaj njihovi otroci na internetu počnejo, da se z otroki pogovarjajo o pasteh interneta in da ob morebitni zaznavi kaznivega dejanja o tem obvestijo policijo.

»Otrokom in staršem svetujemo, da na internetu ne izdajajo svojih osebnih podatkov, ne objavljajo ali pošiljajo svojih osebnih fotografij ali fotografij svojih prijateljev, se ne pogovarjajo z neznanci, ki so jih spoznali preko interneta, naj ne pristanejo na pogovore z njimi preko spletne kamere in naj nikomur ne zaupajo gesel svojih računov elektronskih pošt, družbenih omrežij ... Gesla naj tudi pogosto menjajo. V primeru izsiljevanja ali objave neprimerne vsebine naj o tem obvestijo policijo,« so jasni pristojni.

Starši morajo biti pozorni, kaj njihovi otroci počnejo na internetu. Z otroki naj se pogovarjajo o pasteh interneta.

Policija oziroma Ministrstvo za notranje zadeve RS sodelujeta z različnimi domačimi podjetji pri nabavi zaščitne in varovalne opreme policistov.

Foto: Depositphotos

Večina ponudnikov je slovenskih, pri čemer pa je delež proizvodnje v Sloveniji manjši, saj poteka proizvodnja večinoma v drugih državah.

MNZ in Policija pri opremi zadovoljna s slovenskimi ponudniki

Policija, ki za potrebe varnosti sodeluje tudi v reševalnih akcijah s helikopterji, skladno z razpoložljivostjo svojih sil po potrebi pomaga tudi Upravi RS za zaščito in reševanje (URSZR). Policija namreč predstavlja tudi sile za zaščito, reševanje in pomoč – tudi v luči epidemije COVID-19, vendar pa za te namene posebej ne kupuje opreme. »Vsa oprema, ki jo kupujemo, je namenjena izvajanju zakonskih nalog Policije, kar pomeni, da opremo, ki jo kupimo, uporabljamo tudi za primere zaščite in reševanja, kot so telekomunikacijska oprema, brezpilotniki, defibrilatorji, alpinistično jamarska oprema, potapljaška oprema, oprema za reševanje s helikopterjem,« pojasnjujejo na Policiji.

Policija oziroma Ministrstvo za notranje zadeve RS sodelujeta z različnimi domačimi podjetji pri nabavi zaščitne in varovalne opreme policistov. »Še posebej se lahko v zadnjih letih pohvalimo, da smo kar nekaj novih rešitev – produktov pripravili v sodelovanju s slovenskimi podjetji,« pravijo na Policiji, kjer dodajo, da je velikokrat tudi težava premajhni trg, tako da so manj zanimivi za večje proizvajalce opreme.

Ministrstvo za notranje zadeve in Policija vso opremo nabavljata s postopki javnih naročil. Večina ponudnikov je slovenskih, pri čemer pa je delež proizvodnje v Sloveniji manjši, saj poteka proizvodnja večinoma v drugih državah. gg

ELEKTRONIKA naglič
info@naglic.si
(01)7292660

Elektronika Naglič: Do rešitve skupaj s stranko

Specifične želje strank so zanje poseben izziv, v katerega z veseljem zagrizejo in poiščejo ustrezno rešitev.

Podjetje Elektronika Naglič je Miroslav Naglič, ki je bil do takrat zaposlen v družbi Iskra, ustanovil pred 26. leti, ko se je odločil karierno pot začrtati po svoje. Manjše družinsko podjetje, ki je preraslo družino, ima danes šest redno zaposlenih, sodelujejo pa tudi z zunanjimi sodelavci.

Svojo pozornost že od prvih korakov namenjajo predvsem profesionalnim radijskim zvezam. Na tem področju so partnerji z vodilnimi blagovnimi znamkami na svetu, kot sta **Motorola Solutions** in **Yaesu**.

V Sloveniji so edini distributer znamke **Swissphone**, ki je vodilna v svetu na področju alarmiranja in **RAM Mounts** nosilcev elektronskih naprav, ki jih odlikuje doživljenjska garancija in proizvodnja izključno v ZDA.

Lasten razvoj in domača proizvodnja

Poleg zastopstva tujih blagovnih znamk gradijo svojo zgodbo tudi z lastnim razvojem in domačo proizvodnjo. Stremijo k najboljši kakovosti lastnih izdelkov in skrbno izbirajo materiale in dobavitelje vseh sestavnih delov.

Njihove izdelke zato odlikuje dolga življenjska doba in najkakovostnejši materiali. V določenih fazah proizvodnje sodelujejo tudi s slovenskimi podjetji.

»Če imajo naše stranke specifične želje, se z veseljem in zavzeto lotimo izziva pri iskanju in načrtovanju rešitev,« pravijo v podjetju in dodajo, da med njihove najbolj prodajane izdelke sodijo vmesniki za prenos podatkov (tudi preko Etherneta), prenosni komunikacijski kovčki, napajalniki radijskih postaj, oddvojena delovna mesta, DC DC pretvorniki in dispečerski sistemi.

Naredili moderen dispečerski center

Podjetje Elektronika Naglič je prvo v Sloveniji naredilo moderen dispečerski sistem, ki je v uporabi na reševalnih postajah v Ljubljani in Mariboru, na Ljubljanskem potniškem prometu in v Luki Koper.

Dispečerski sistem s sistemom sledenja, v uporabi na reševalni postaji v Ljubljani.

Slovenija je zanje premajhna, zato se trudijo biti prepoznavni tudi na globalnem trgu. »Zelo smo ponosni na to, da so naši proizvodi zanimivi tudi v tujini,« pravijo. Poudarijo, da jih odlikujejo odzivnost, zavezanost h kakovosti in cenovno dostopne servisne storitve.

Spremljate jih lahko na spletni strani www.naglic.si, na poslovnem socialnem omrežju LinkedIn in na družabnem omrežju Facebook.

Prenosni dispečerski sistem s sistemom sledenja ekipam na terenu.

Prenosni komunikacijski kovček narejen po meri za radijske postaje Motorola SL1600, v kompletu s polnilnimi enotami.

ERDI-12 je vmesnik za prenos podatkov med Motorolinimi DMR radijskimi postajami serije DM3000/DM4000 in drugimi napravami na RS232/RS485 serijskimi komunikacijami.

NP13D je klasičen analogni napajalnik, posebej konstruiran za napajanje radijskih postaj Motorola. Proizvajamo ga v dveh izvedbah, kot samostojnega in z nadgradnjo kot na fotografiji.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

780 mio EUR je predvidenih za investicije v Slovenski vojski v letih 2021–2026 v predlogu novega zakona.

Foto: Depositphotos

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Predlog novega zakona Ministrstvu za obrambo RS nalaga, da v okviru GOIS enkrat letno organizira predstavitev investicij, določenih z letnim načrtom, ki ga sprejme vlada.

Obramba

Slovensko obrambno industrijo bi vključili v zakon

Oprema, ki so jo slovenska podjetja dobavila slovenski vojski, je v veliki meri rezultat skupnega razvoja, vlaganj in dobrega sodelovanja obrambnega resorja z znanstvenoraziskovalno sfero in industrijo.

Darja Kocbek

V letih 2021–2026 bo MORS nabavljal predvsem bojna vozila, vojaška letala, transportna vozila, logistična vozila in medicinsko opremo, komunikacijske in informacijske sisteme ter opremo za kibernetsko obrambo.

Obstoj in nadaljnji razvoj obrambne industrije je za Republiko Slovenijo ključnega pomena, tako z vidika nacionalne kot z vidika kolektivne obrambe, je minister za obrambo Matej Tonin septembra letos dejal na strokovnem srečanju s predstavniki Gospodarskega interesnega združenja Grozd obrambne industrije Slovenije (GOIS), direktorji podjetij obrambne industrije ter predstavniki Banke Slovenije, Združenja slovenskih bank in komercialnih bank. Povedal je, da je v predlogu novega zakona o zagotavljanju sredstev za investicije v Slovenski vojski v letih 2021–2026 predvidenih 780 mio EUR za investicije.

V predlog tega zakona, ki čaka na tretjo obravnavo v Državnem zboru RS, je vključena tudi slovenska obrambna industrija. Minister Tonin je izpostavil 6. člen, ki Ministrstvu za obrambo RS (MORS) nalaga, da gospodarskim subjektom s sedežem v naši državi enkrat letno v okviru GOIS organizira predstavitev investicij, določenih z letnim načrtom, ki ga sprejme vlada. To bo po ministrovih besedah gospodarskim subjektom omogočilo boljše predvidevanje tržnega razvoja ter morebitno sodelovanje v investicijskih projektih in naročilih.

Kot članica EU se je Slovenija pridružila Stalnemu strukturnemu sodelovanju (Permanent Structured Cooperation – PESCO), ki je okvir za poglobitev sodelovanja na področju obrambe med državami EU. Državam članicam naj bi pomagal skupaj razvijati obrambne zmogljivosti, vlagati v skupne projekte ter krepiti operativno pripravljenost in prispevek svojih obrambnih sil.

Na ravni EU deluje tudi Evropska obrambna agencija (EDA), ki državam članicam pomaga, da se pri določanju prednostnih nalog EU lahko bolj osredotočijo na razvoj obrambne zmogljivosti in obrambnih raziskav, ki jih bo obravnavala Evropska komisija. Tonin je povedal, da je v sklepni fazi izbor projektov s področja obrambnih raziskav v skupnem znesku 500 mio EUR. Te projekte v celoti financira EU. Pri tem so

Podjetje DAT - CON je ponudnik specializiranih mobilnih in stacionarnih rešitev za opazovanje in nadzor večinoma obalnih in kopenskih meja. Ponuja tudi sistemsko integracijo, razvoj elektronskih aplikacij, namenske elektronike in posebne merilne opreme. Podjetje je bilo ustanovljeno leta 1992 in je s sklepanjem partnerstev z vodilnimi podjetji na področju termovizije, optike, merilnih naprav in komunikacijske opreme uspešno zaključilo vrsto projektov po celotnem svetu. Z odličnimi in učinkovitimi sistemi, ki jih uporabljajo kriminalistične ter državne varnostne službe za vzdrževanje pravnega reda v državah in za preprečevanje kriminalne dejavnosti je podjetje uspešno prodrlo na evropske in tuje trge.

E: sales@dat-con.com **T: +386 (0) 3 70 335 44** **S: www.dat-con.com**

Sistem za neiznvazivno skeniranje telesne temperature SCR/BT

Rešitev na ključ, ki operaterju kritične javne infrastrukture (letališča, železniške postaje, šole...) omogoča, da množice ali posameznike neinvazivno skenira za povišano telesno temperaturo, ki bi lahko bila prenašalec nalezljive bolezni.

DAT - CON SCR / BT lahko uporablja več načinov delovanja, odvisno od aplikacije:

- skeniranje ene osebe z referenco z zaznavanjem absolutne telesne temperature
- več oseb s skeniranjem množice in zaznavanjem ljudi z višjo telesno temperaturo.

Termične kamere so pasivne naprave, ki ne oddajajo sevanja, temveč za oddajanje slik v visoki ločljivosti brez potrebe po dodatni osvetlitvi uporabljajo infrardeče sevanje. Operater potrebuje samo računalnik z operacijskim sistemom Windows 7, 10 ali Pro. Izvedba je lahko fiksna ali prenosna. Zaznavanje najmanj 100 oseb v minuti, ki prehajajo merilno območje in jim izmeri telesno temperaturo.

SPACE STERILIZER – Sterilizator prostora s patentirano tehnologijo

Edinstven zračni sterilizator, ki s patentirano tehnologijo iz zraka odstranjuje bakterije ter tiho in varno sterilizira okolico, s čimer zagotavlja zaščito pred virusi, kot so SARS, MERS-CoV in koronavirus. V primerjavi z ostalimi čistilci zraka, ki po filtriranju v napravi sesajo in pihajo zrak, pa Space Sterilizer z ustvarjanjem in oddajanjem aktivnih ionov v okolico ter z neposrednim hlapenjem učinkovito uniči vse patogene organizme v zraku ali na kateri koli trdi površini. Vsi modeli so zasnovani kot samostojne in prenosljive enote, ki se uspešno borijo proti virusom in bakterijam v katerih koli zaprtih prostorih s površino do 330 kvadratnih metrov. So enostavni za uporabo in za svoje delovanje ne potrebujejo nobene dodatne ali nadomestne opreme. Primerni so za čakalnice, sejne sobe, vrtce, šole in ostale prostore, v katerih se zbira, zadržuje ali menja veliko število ljudi.

uspešni tudi slovenski konzorciji podjetij in znanstveno-raziskovalnih ustanov.

500 mio EUR je vreden izbor projektov s področja obrambnih raziskav, ki jih v celoti financira EU.

Kupili bodo opremo, ki je bila predvidena že pred rebalansom proračuna

Ker se MORS-u na podlagi rebalansa proračuna za leto 2020 finančna sredstva ne bodo povečala, bodo v letu 2020 izvedena naročila vojaške opreme, ki so bila predvidena v že sprejetem proračunu za leto 2020. Za potrebe Slovenske vojske bodo med drugim kupili terenska vozila 4x4, opremo bojevnika, opremo za specialne sile in inženirsko opremo, opremo za usmerjanje letalske podpore, potapljaško opremo, tovorna vozila s priklopnikom za avtošolo, letališko logistično opremo, strelivo različnih kalibrov, taktične zaščitne jopiče …, so nam pojasnili na obrambnem ministrstvu.

Foto: Depositphotos

V letih 2021–2026 nameravajo skladno s sprejetim splošnim dolgoročnim programom razvoja in opremljanja Slovenske vojske ter srednjeročnim obrambnim programom nabavljati predvsem bojna vozila, vojaška letala, transportna vozila, logistična vozila in medicinsko opremo, komunikacijske in informacijske sisteme ter opremo za kibernetsko obrambo. Vlagati nameravajo tudi v infrastrukturo, raketne sisteme, pehotno orožje in opremo.

Obrambno sodelovanje na ravni EU oziroma zavezništva Nato pa je mogoče predvsem v okviru Evropske obrambne agencije (EDA), Organizacije vzajemnega sodelovanja na področju oborožitve (OCCAR) in Natove agencije za podporo in nabave (NSPA), so še povedali na ministrstvu.

Na podlagi izvedenih postopkov javnih naročil na MORS ugotavljajo, da pri dobavi bojnih in službenih uniform, zaščitnih jopičev ter opreme za nošenje in bivanje na terenu praviloma sodelujejo proizvajalci in dobavitelji, ki so slovenska mala in srednja podjetja. »Ocenjujemo, da je proizvodov slovenskega porekla trenutno med 70 in 75 %. Razlog za tako visok delež

Evropska komisija je junija 2018 predlagala ustanovitev Evropskega obrambnega sklada s ciljem spodbujati konkurenčnost, učinkovitost in inovacije evropske obrambne industrije ter sodelovanje med podjetji obrambne industrije in znanstvenimi ustanovami ter med državami članicami. Sredstva za projekte, ki jih bo financiral ta sklad, bodo na voljo v okviru novega dolgoročnega proračuna EU za obdobje 2021-2027. Do takrat EU sredstva za obrambo namenja prek pilotnih programov Pripravljalni ukrep za raziskave na področju obrambe (PADR) in Evropski program za razvoj obrambne industrije (EDIDP).

Podjetje C-ASTRAL izdelalo že več kot 400 brezpilotnih sistemov

Leta 2004 so izdelali prve prototipe in leta 2005 je v Ajdovščini poletel prvi slovenski brezpilotni sistem, Spectral System.

C-ASTRAL je eno od vodilnih svetovnih podjetij na področju raziskav in razvoja, projektiranja, proizvodnje in integracije t. i. malih brezpilotnih sistemov (ang. small Unmanned Aircraft System – sUAS) in pripadajoče strojne, komunikacijske in programske opreme. Ustanovljeno je bilo leta 2007 v Ajdovščini, njegovi ustanovitelji pa so bili aktivni na področju letalskih in vesoljskih tehnologij in njihovih aplikacij že od 90. let naprej. Leta 2004 so izdelali prve prototipe in leta 2005 je v Ajdovščini poletel prvi slovenski brezpilotni sistem, Spectral System. Več kot 400 sistemov, ki jih je podjetje izdelalo od svoje ustanovitve, leti nad vsemi kontinenti v 70 državah sveta, uporabljajo pa jih tako komercialni kot tudi institucionalni operaterji. S sistemi je bilo opravljenih tudi več neuradnih rekordov, kot so operacije na visokih nadmorskih višinah (nad 4500 m ASL), operacije na Arktiki in Antarktiki ter t. i. BVLOS (beyond visual line of sight) operacije.

Izdelujejo štiri tipe brezpilotnih zrakoplovov

Trenutno C-ASTRAL izdeluje in integrira štiri tipe brezpilotnih zrakoplovov. Trije so izvedenka sistema BRAMOR (ppX, ki je namenjen natančnemu kartiranju, C4EYE, ki je namenjen sočasnemu opazovanju Zemlje s pomočjo videa in elektrooptike, ter sAR, ki je namenjen zaščiti in reševanju s pomočjo lokalizacije telefonskih oddajnikov). V letu 2020 pa je podjetje lansiralo na trg tudi sistem ATLAS (Advanced Technology Light Acquisition System). Gre za manjši modularen sistem, ki je povsem kompatibilien s C-ASTRAL-ovim zemeljskih segmentom, omogoča pa večino funkcionalnosti sistema BRAMOR na manjšem zrakoplovu, ki pa še vedno leti uro in pol.

Podjetje od leta 2012 razvija tudi svojo programsko opremo in okolje C3P (Command Control Communications and Planning), ki je po mnenju poznavalcev v industriji eno najbolj ergonomskih in uporabniku prijaznih programskih okolij in vmesnikov za nadzorovanje brezpilotnih zrakoplovov. V sisteme so integrirani elektrooptični, komunikacijski in aerofotogrametrični senzorski paketi, pa tudi spektrometri. Programsko okolje C-ASTRAL C3P je tudi popolnoma interoperabilno s t.i. BMS (Battle Management Systems) ter prilagodljivo do te mere, da ga je s pomočjo odprtih protokolov mogoče povezati v raznolike sisteme poveljevanja, kontrole kot tudi agregacije senzorskih podatkov. C-ASTRAL veliko sistemov v posebnih konfiguracijah izdeluje tudi po naročilu za znane stranke.

Uporabniki aktivni na različnih področjih

Uporabniki sistemov C-ASTRAL so aktivni na raznolikih področjih – od zaščite in reševanja, obalne straže, nadzora nad požari, nadzora meje na kopnem, zaščite lastnih sil v operacijah NATA in Združenih Narodov, ekološkega monitoringa s strani nevladnih organizacij, protiterorističnem delovanju, na vseh področjih geodezije, nadzora infrastrukture, daljinskega zaznavanja ter kartiranja neeksplodiranih ubojnih sredstev. C-ASTRAL-ovi sistemi npr. letijo in kartirajo rudnike v Avstraliji, Južni Ameriki ter opravljajo monitorig rečnih strug v Panami, Avstriji ter ZDA, pomagajo pa tudi pri izgradnji cestne infrastrukture v Afganistanu in nadzorovanju varnosti plinovodov v Turčiji, Kanadi, Teksasu in Mehiki.

V redni uporabi vojske in policije

Na obrambnem področju so sistemi v redni uporabi v štirih državah NATA, pa tudi v policijskih in vojaških silah osmih drugih držav. S pomočjo komercialnega partnerstva C-ASTRAL z japonskim podjetjem TERRA DRONE CORPORATION se sistemi zdaj aktivno prodajajo na svetovnih komercialnih trgih.

C-ASTRAL je aktiven tudi v raziskovalnih in razvojnih projektih, ki jih podpirata tako Evropska komisija kot tudi Evropska obrambna agencija. Eden izmed prodornejših in naprednejših projektov je povezan z upravljanjem in manevriranjem 'jate' brezpilotnikov, drugi pa je povezan z radiološko, biološko in kemično obrambo.

PROMO

Obrambno sodelovanje na ravni EU in zveze Nato je mogoče predvsem v okviru Evropske obrambne agencije (EDA), Organizacije vzajemnega sodelovanja na področju oboroževanja (OCCAR) in Natove agencije za podporo in nabave (NSPA).

je mogoče iskati predvsem v smotrnem oblikovanju javnih naročil in delitvi javnega naročila na posamezne manjše sklope, ki omogočajo tudi udeležbo malih in srednjih podjetij,« so nam pojasnili na ministrstvu.

V zadnjih letih so slovenska podjetja Slovenski vojski med drugim dobavila tudi brezpilotne letalnike, taktične pištole, manevrsko strelivo različnih kalibrov, inženirske stroje, simulatorje in trenažerje za protioklepne oborožitvene sisteme, zložljive turne smuči itd. »Ta oprema je v veliki meri rezultat skupnega razvoja, vlaganj in dobrega sodelovanja obrambnega resorja z znanstvenoraziskovalno sfero in industrijo«, še pojasnjujejo na ministrstvu.

Slovenija se je pridružila Stalnemu strukturnemu sodelovanju (Permanent Structured Cooperation – PESCO), ki je okvir za poglobitev sodelovanja na področju obrambe med državami EU.

Mil Sistemika lahko konkurira tudi največjim svetovnim podjetjem

Tomaž Grad iz Mil Sistemike nam je pojasnil, da je njihov sistem poveljevanja in kontrole C4I namenjen uporabi v oboroženih silah, mogoče pa ga je uporabiti tudi v okviru civilne zaščite in reševanja. Sistem je razvit skladno s standardi zavezništva Nato in ponuja neprekinjeno linijo poveljevanja od najvišje ravni, načrtovanja operacij do najnižje ravni, torej do posameznega človeka na terenu.

»Zaradi svoje tehnične odličnosti, domenskega znanja in položaja na trgu lahko Mil Sistemika v sodelovanju s partnerji s svojimi proizvodi konkurira tudi največjim svetovnim podjetjem na področju sistemov poveljevanja in kontrole oziroma sistema kriznega odzivanja v civilni sferi,« pravi Grad.

V kriznih razmerah (nesreče, poplave, potresi) je po njegovih besedah bistveno usklajeno ukrepanje države in lokalne skupnosti, torej civilne zaščite, reševalcev, policistov, vojakov, gasilcev, ki na terenu izvajajo naloge reševanja in pridobivajo informacije o stanju. Če nimajo podatkov o obsegu nevarnosti oziroma katastrofe, ne morejo optimalno ukrepati, zaradi česar so lahko ogrožena tudi življenja. Reševalci so po nepotrebnem izpostavljeni nevarnosti in dragoceni viri niso učinkovito izrabljeni.

Proizvodi, ki omogočajo komuniciranje v kriznih pogojih

»Mil Sistemika proizvaja vrsto proizvodov, ki omogočajo komuniciranje v kriznih pogojih, spremljanje razmer na terenu in učinkovito upravljanje z viri,« nam je povedal Tomaž Grad.

Programski paket IHTA je namenjen operativnemu centru oziroma poveljstvu. Z njegovo pomočjo ter z zbranimi informacijami operater pripravi načrt delovanja oziroma povelje. Sistem pa tudi zagotavlja povezljivost različnih radijskih sistemov, izmenjavo podatkov in informacij ter sprotno spremljanje doga-

Foto: Depositphotos

Si EnE

Slovensko partnerstvo za energijo in okolje na obrambnem področju

- Energetski in okoljski izzivi na obrambnem področju
- Raziskovalno razvojno in tehnološko sodelovanje v obrambnih programih
- Vključevanje slovenskih partnerjev v globalne obrambne verige vrednosti

Julija 2020 ustanovljeno partnerstvo SiEnE predstavlja **strateški in celovit pristop** naslavljanja **energetskih in okoljskih izzivov na obrambnem področju** pod okriljem TECES in Ministrstva za obrambo Republike Slovenije (MORS).

Strateško **povezovanje obrambnih in civilnih deležnikov** v okviru SiEnE omogoča **učinkovitejše vključevanje slovenskih partnerjev** v mednarodne obrambne programe ter globalne obrambne verige vrednosti.

Pristopite v partnerstvo na SiEnE.teces.si

Vzpostavljeno pod okriljem

teces
Where linking creates synergy

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Foto: Depositphotos

janja. Opravlja naloge na področju upravljanja zvez ter naloge zbiranja, obdelave in hrambe podatkov. Njegove glavne funkcije so: priprava in posredovanje ukrepov, spremljanje izvajanja in poročanje, spremljanje razmer na terenu, posredovanje podatkov iz avtomatskih sistemov (brezpilotnih letal ipd.).

Programski paket BES je prilagojen uporabniškim vmesnikom. Z robustnostjo delovanja je prilagojen tudi za delo v vozilih ali na terenu. Aplikacija PES pa je namenjena vojakom ali reševalcem za lažje opravljanje nalog na terenu. Skupaj pokrivata segment celotnega izvršnega dela sistema kriznega upravljanja in sta povezljiva s senzorskimi in drugimi merilnimi sistemi. Poleg integracije ponujata tudi zmogljivo kartografsko podlago (GIS) in omogočata sledenje lastnim enotam in izmenjavo skupne situacijske slike z drugimi podobnimi sistemi.

Celoten sistem pa povezuje sodobna in inovativna komunikacijska platforma COMMS2, namenjena podatkovnemu komuniciranju prek fiksnega, radijskega ali satelitskega omrežja. Omogoča usmerjanje prometa, avtomatsko retranslacijo in podpira množico radijskih naprav, tako starejših, analognih, s serijskim modemom kot tudi novejših s podporo IP prometu (LTE, DMR TETRA ipd.).

»Brez zanesljivih sredstev zvez in informacijsko-komunikacijske podpore je težko uspešno in predvsem

Andrej Orožen, soustanovitelj in predsednik uprave Dewesofta

Foto: Dewesoft

varno posredovati na terenu. Radijska naprava ima z vidika varnosti za gasilca oziroma reševalca enak pomen, kot ga ima zaščitna obleka ali čelada,« nam je razložil Grad.

Dewesoft že nekaj let odlično sodeluje z Evropsko vesoljsko agencijo (ESA)

Dewesoft razvija in izdeluje inštrumente za merjenje in zajem podatkov, krmiljenje ter regulacijo, ki jih uporabljajo razvojniki v najnaprednejših laboratorijih po vsem svetu. Njihove naprave pri razvoju novih tehnoloških rešitev uporabljajo praktično vse industrije, od avtomobilske, vesoljske, letalske do gradbene, transportne, kot tudi energetika. Tako so nepogrešljivi na primer pri razvoju raket in satelitov, ki zagotavljajo hitro komunikacijo, pri razvoju novih varnejših vozil in vozil z manj izpusti, varnejših mostov in viaduktov, sistemov za zeleno energijo ter drugih izdelkov, ki izboljšujejo naše vsakdanje življenje, pojasnjujejo v podjetju.

Podjetje izvozi 99 % svojih izdelkov. Do konca letošnjega septembra so v Dewesoftu ustvarili dobrih 22 mio EUR prihodkov, kar je 21 % več kot v enakem obdobju lani.

Dewesoft v programih Evropske obrambne agencije (EDA) že sodeluje preko hčerinskih podjetij in sistemskih integratorjev, ki gradijo sisteme in rešitve za EDA, nam je pojasnil soustanovitelj in predsednik uprave Dewesofta Andrej Orožen. S članstvom v Grozdu obrambne industrije Slovenije (GOIS) se po njegovih besedah možnosti sodelovanja in dostopa do drugih dobaviteljev v EDA povečujejo.

Mora pa imeti podjetje, ki želi projekte neposredno prijaviti na razpise EDA, urejene ocene klasifikacije področja dela ter biti prepoznan kot proizvajalec in ponudnik v EDA. Dewesoftu je pri tem na pomoč priskočilo Ministrstvo za obrambo RS in jih podučilo o potrebnih postopkih, jih pri tem opremilo z vsemi

V zadnjih letih so slovenska podjetja Slovenski vojski med drugim dobavila tudi brezpilotne letalnike, taktične pištole, manevrsko strelivo različnih kalibrov, inženirske stroje, simulatorje in trenažerje za protioklepne oborožitvene sisteme, zložljive turne smuči itd.

potrebnimi dokazili, dokumenti in pristopnimi kodami tako za EDA kot tudi za zavezništvo Nato. »S predstavniki obrambnega ministrstva smo res konstruktivno sodelovali,« poudari Orožen.

Zaradi svoje tehnične odličnosti, domenskega znanja in položaja na trgu lahko Mil Sistemika konkurira največjim svetovnim podjetjem na področju sistemov poveljevanja in kontrole.

Vedno so veseli novih izzivov

EDA ima po lastnih zagotovilih pomembno vlogo na področju inovacij, raziskav in razvoja za srednja in majhna podjetja. V Dewesoftu po Orožnovih besedah te podpore EDA do sedaj niso koristili. »Dewesoft je namreč odlično in zelo agilno podjetje, ki se dokazuje s svojimi inovativnimi produkti in rešitvami. In kot takega nas prepoznavata tako EDA kot zavezništvo Nato, pa tudi podjetja, ki delujejo na področju vesoljske industrije,« razlaga Orožen.

Vedno pa so veseli novih izzivov in dela z drugimi razvojnimi oddelki, saj jim to daje možnost izboljšanja produktov. »Kadar dobimo priložnost, da se predstavimo, imamo običajno tudi možnost korektno ponuditi svoje izdelke in rešitve. Na nas pa je, da smo v igri tehničnih argumentov najbolj prepričljivi, da bi tako posel tudi pridobili,« pojasnjuje sogovornik.

Medtem ko Dewesoft že nekaj let odlično sodeluje z Evropsko vesoljsko agencijo (ESA), so v podjetju sedaj osredotočeni še na neposredno sodelovanje z EDA. Naslednji korak pa bo najverjetneje povezovanje z razvojnimi oddelki in dobavitelji zavezništva Nato. »Tega smo v Dewesoftu sposobni in verjamemo, da bo razvoj z uporabo naše opreme hitrejši in boljši. Nedavno smo na trg dali dve novi družini inštrumentov ter novosti v programski opremi Dewesoft X,« pravi Andrej Orožen.

Petre šotori – hale lahko ponudi svoje šotore, ponjave

Ministrstvo za obrambo lahko na razpisih za izvedbo investicij v okviru GOIS na podlagi dolgoletnega dobrega sodelovanja pričakuje ponudbe podjetja Petre šotori – hale, predvsem šotore, ponjave. V podjetju so nam pojasnili, da bi pomoč Evropske obrambne agencije (EDA) na področju inovacij, raziskav in razvoja za mala in srednja podjetja lahko izkoristili pri razvoju in raziskavi vojaških šotorov, nadstreškov in ponjav.

»Sodelovanje z zavezništvom Nato je za nas aktualno v primeru vojaških vaj za vzpostavitev infrastrukture. Seveda smo zainteresirani in pripravljeni za njih tudi kaj proizvajati, zlasti začasne nadstreške, skladiščne šotore in drugo opremo,« so nam pojasnili glede sodelovanja z zavezništvom Nato. gg

DEWESoft® v vesoljski industriji

Dewesoft kar četrtino prihodkov ustvari v sodelovanju z vesoljsko industrijo. Odskočna deska je bilo sodelovanje z NASO, po katerem se je Dewesoft začel pojavljati tudi v Evropskih, Ruskih, Kitajskih in nazadnje še Indijskih vesoljskih projektih.

DEWESOFT IN NASA

Leta 2003 je NASA pričela projekt posodobitve opreme za zajem podatkov pri izstrelitvi Space Shuttla. Po testiranju več proizvajalcev so se odločili za opremo podjetja Dewetron. Glede na to, da pa je bilo potrebno že razpoložljivim signalom dodati še meritev podatkov, ki jih je plovilo pošiljalo na zemljo (telemetrija) pa so zahtevali direktno sodelovanje z Dewesoft ekipo, ki je zgradila programski paket, ki so ga videli na testirani opremi. Po nekoliko zapletenem začetku je bilo sodelovanje več kot uspešno in še danes je oprema nameščena tudi v sobi za vodenje izstrelitev.

Eden izmed Dewesoftovih novejših projektov z NASO je bila zamenjava zastarele merilne opreme na njihovem vozilu (crawler-transporter) za transport prenosnega izstrelišča (Mobile Launcher 1 platform). Dewesoft je poleg programske opreme za ta projekt zagotovil tudi svoje merilne inštrumente. S pomočjo teh NASA zajema podatke o vibracijah, temperaturi in tlaku, na podlagi katerih lahko zagotavlja varen transport rakete do dejanskega izstrelišča.

SIRIUS R8RT
Merilni sistem z velikim številom analognih kanalov vključuje visoko kakovostno pretvorbo signalov, zmogljiv računalnik s hitrim SSD diskom in omogoča hitro preslikavo podatkov na EtherCAT vodilo, s tem pa kompatibilnost s tujimi "real-time" kontrolerji.

DEWESOFT IN EVROPSKA VESOLJSKA AGENCIJA

Osnovna misija ESE (European Space Agency) je zagotavljanje neodvisnega dostopa v vesolje Evropskim državam. ARIANE 6, s predvidenim prvim poletom v 2021, pa bo njena najnovejša generacija izstrelitvenega plovila.

Dewesoft bo s svojo opremo prisoten na samem izstrelišču, že zdaj pa je zagotavljal zajem podatkov na treh uspešnih testiranjih glavnega motorja. Motor z imenom P120C, dolg 13.5 m s premerom 3.4 m je napolnjen s 142 ton goriva in ustvari silo potiska okoli 4650 kN. Sam zagonski test traja le 135 sekund, pri njem pa Dewesoft zajema več kot 600 različnih parametrov s hitrostmi do 200 tisoč podatkov na sekundo.

DEWESOFT V INDIJI

Indijska vlada je za namen IPRC (Indian space research organization) financirala izgradnjo objekta za strukturne preizkuse (STF -Structural Test Facility), prvega takšnega v okviru propulzijskega raziskovalnega kompleksa indijskega inštituta za vesoljske raziskave v Mahendragiriju v državi Tamil Nadu v Indiji. Dewesoftov sistem zbira podatke o ključnih parametrih, kot so temperatura, pritisk, premiki, napetost...

V kabelski terminalski sobi (CTR), ki je skoraj 400 metrov od nadzorne sobe, so nameščeni Dewesoftovi moduli, medtem ko je kontrolna soba opremljena s strežniki in prikazovalnimi računalniki. Sistem v prvi vrsti skrbi za simuliranje in preslikavo zanesljivosti parametrov med stabilizacijo leta, v fazah ločevanja in med dinamičnim dogajanjem v orbiti. Podatke zajema simultano, iz preko 2000 analognih kanalov, kar je za Dewesoft največji sistem do danes.

DEWESOFT V BRAZILIJI

Dewesoftova ekipa se je pred dobrim letom mudila v Braziliji na DCTA, državni ustanovi za razvoj znanosti in letalsko-vesoljskih tehnologij, ki je v vojaški bazi blizu mesta São José dos Campos.

Dewesoft Sine processing merilni sistem je preko namenskega COLA signala sinhroniziran z vzbujevalnim sistemom, ki preko stresalnika sinusno vzbuja strukturo. Vzbujanje med testom potuje po frekvenčnem območju od 25 do 1000Hz.
Z uporabo frekvenčne detekcije po metodi preč-

kanja ničle ali z uporabo Hilbertove transformacije Dewesoft programska oprema zaznava frekvenco vzbujanja skozi celoten potek testa. Preko relativnega ali fiksnega sledilnega filtra nato sistem odstrani motnje in zagotovi, da se preračun izvaja le na trenutni frekvenci vzbujanja.

Slovenska obrambna industrija je usmerjena v visokotehnološki razvoj

Slovenska podjetja poslujejo predvsem v visokotehnološkem delu obrambne industrije, dosegajo odlične rezultate in so uspešni izvozniki. V Sloveniji so neprepoznavna predvsem zaradi odnosa Slovencev do vojaškega sveta. Predstavniki podjetij Panna Plus in Guardiaris so nam zaupali svoj pogled na dejavnost, ki v sklopu njihovih podjetij zaposluje 50 visoko izobraženih mladih ljudi z visoko dodano vrednostjo.

Družba Panna Plus je dobavitelj in predstavnik velikih svetovnih vojaških korporacij, kot so Rafael, Nexter Group, Northrop Grumman, SAAB na celotnem območju nekdanje Jugoslavije, predvsem držav članic NATO. Svojo dodano vrednost že leta podjetje usmerja v spin-off podjetje Guardiaris, v sklopu katerega deluje že 40 ljudi. V Sloveniji namreč vse do danes ni bilo na voljo finančnih instrumentov za področje razvoja obrambne industrije. Guardiaris je sicer v svetu obrambne industrije mikropodjetje, a že danes lastne proizvode več kot uspešno prodaja po celem svetu.

V Sloveniji je sicer večina podjetij, ki delujejo na področju obrambne industrije, združena v GOIS (Grozd obrambne industrije Slovenije). Člani grozda so lani ustvarili za 500 milijonov evrov prihodkov, od tega 75 odstotkov v izvozu. Največ so izvozili v države EU. Dodana vrednost na zaposlenega je v letu 2019 znašala 57.000 evrov.

Svoje vojske ne spoštujemo

Kljub uspešnemu poslovanju pa imajo tovrstna podjetja kar precej težav. Slovenci smo 50 let živeli pod jugoslovansko vojsko, ki je v resnici nikoli nismo prepoznali kot lastne, nismo je spoštovali in to je čutiti še danes. »Ne zavedamo se namreč pomena domače vojske, še manj domače vojaške industrije. Poleg tega pa so ugled obojih še dodatno spodkopavale afere, vezane na vojaški sektor. A raziskava Voice of People iz leta 2006 je pokazala, da se je vojska v svetu po koruptivnosti veliko bolje odrezala kot politiki, parlamentarci, poslovneži; da je torej korupcije po svetu v vojski bistveno manj, kot so sliko ustvarili določeni mediji.«

Prepričali kupce iz 14 držav

Podjetje Guardiaris danes posluje v 14 državah po celem svetu. Njegova največja stranka je Švicarska vojska, kjer ima družba odlično referenco na področju simulatorjev, nedavno pa so podpisali tudi pogodbo z avstrijsko vojsko, ki jih je prepoznala kot unikum v simulacijski tehnologiji oborožitvenih sil. Kot poudarjajo, tako Guardiaris kot druga slovenska podjetja iz obrambne industrije ogromno vlagajo v tehnologijo predstavitve, v patente, design, saj je prednost svetovnih gigantov na tem področju skoraj neulovljiva. Istočasno pa večino družb iz tega področja deluje po principu 'lastni poslovni angeli', a so – kot je to družba Panna Plus – v medijih izpostavljene kot veliki dobičkarji. Niso preprodajalci in niso vojni dobičkarji, to so podjetja, specializirana na področju obrambne industrije, ki večino sredstev vlagajo v znanje in razvoj.

Pogrešajo razumevanje bank

Ena od večjih težav, s katero se soočajo podjetja iz obrambne industrije, je pomanjkanje razumevanja domačih bank, ki obrambnih produktov ne prepoznajo kot perspektivne in zato s temi podjetji ne želijo sodelovati. »Kako naj potem financiramo svoje posle? V svetu ni namenskih skladov, ki bi financirali vojaško industrijo, banke v Sloveniji pa nam ne stojijo ob strani. Tudi mi smo del gospodarstva, tudi mi ustvarjamo dodano vrednost in pomemben delež izvoza,« še povedo. Ravno zato so v septembru v okviru GOIZ organizirali posvet z bankami in jih na to opozorili.

V svetu tovrstna podjetja izvajajo milijardne posle, zato so banke njihov zvesti podporniki. Zavedajo se namreč, da domača obrambna industrija pomeni varnost. Ni namreč toliko pomembno, kako velika je država in kako veliko vojsko ima; že to, da je sposobna izdelati določeno tehnologijo, ki v svetu nekaj pomeni, pri drugih državah vzbuja strahospoštovanje.

Dodajo, da ima Švica sicer močno domačo vojsko, v katero veliko vlaga, a praktično nikoli ni bila v vojni. »Vsi se zavedajo, da se te države ne splača napadati, da bi bilo to predrago. Bolj se jim splača vanjo vlagati denar,« ponazorijo. V Sloveniji pa je po njihovem mnenju vojska stigmatizirana. To se odraža tudi v obrambni industriji, saj podjetja res skoraj nemogoče pridejo do sredstev, pa čeprav poslujejo dobro in imajo zagotovljene dolgoročne posle.

Pet let od prvega stika do podpisa pogodbe

Obrambna industrija običajno deluje tako, da naredi občasno večji, dobro plačan posel, potem pa mora s temi sredstvi preživeti do naslednjega posla. »Poglejte primerjavo – trgovina v centru Ljubljane na primer ustvari dnevno 1.000 evrov dobička, na leto torej okroglih 250.000 evrov. V petih letih, kolikor v obrambni industriji običajno traja cikel – od prvega stika do podpisa pogodbe – ta trgovina ustvari več kot milijon evrov dobička. To se nikomur ne zdi nič posebnega, ko pa vojaško podjetje zasluži milijon evrov, vsi govorijo o zelo visokem dobičku in t. i. vojnem dobičkarstvu. Vsi pa pozabljajo, da bo moralo s tem denarjem pet let financirati zaposlene in razvoj še naslednjih nekaj let,« opozorijo.

Da so slovenska podjetja, ki poslujejo v obrambni industriji, zelo usmerjena v visokotehnološki razvoj, je namreč naša edina možnost, da se lahko enakovredno borijo na svetovnem trgu, saj z velikimi igralci iz še večjih dežel, ki za razvoj vojaške tehnologije namenjajo milijarde, enostavno drugače ne morejo tekmovati. Lahko pa trgu ponudijo nekaj drugačnega, nekaj, česar veliki že zaradi velikosti niso sposobni proizvesti. Zaradi tega jih opazijo tudi veliki tekmeci in jih zaradi slovenske inovativnosti vabijo v svoje projekte,« pojasnijo.

Sodelujejo z obrambnim ministrstvom in znanstvenimi institucijami

Sogovorniki potrdijo, da je v zadnjih letih sodelovanje obrambnih podjetij z Ministrstvom za obrambo in Slovensko vojsko postalo zgledno. »Za nas in v našem imenu testirajo naše izdelke, v zameno pa jih lahko kupijo pod veliko boljšimi pogoji kot ostali kupci po svetu. Pomagajo nam ugotoviti, ali pravilno razmišljamo, ali gre naš razvoj v pravo smer,« pravijo in dodajo, da jih ministrstvo podpira tudi pri pridobivanju poslov v tujini. »Tako je na primer neformalno pomagalo, ko so se potegovali za posel v sosednji Avstriji, in jih neformalno pohvalilo kot dobrega in zanesljivega dobavitelja Slovenske vojske. To velikokrat več pomeni kot vsi uradni postopki,« pojasnijo sogovorniki, a dodajo, da njihovi projekti niso tako veliki, da bi pritegnili zanimanje politikov in bi jih ti pomagali prodajati, kot se to na primer dogaja v Franciji ali ZDA.

Simulatorji uporabni tudi za gradnjo cest

Podjetja iz obrambne industrije pa ne izdelujejo le orožja in sredstev za uničevanje, kot številni zmotno mislijo. Zelo aktivna so tudi pri projektih, ki nam olajšajo vsakodnevno življenje. Tako je na primer družba Panna Plus leta 2014 uspešno pridobila evropska sredstva in z njihovo pomočjo razvila simulator, ki se uporablja za zagotavljanje varnosti v cestnem prometu. Vrednost projekta je znašala okoli 400 tisoč evrov, od tega je 280.000 v obliki projektne subvencije prispevala država. »Simulator, proizveden in v celoti sprogramiran v Sloveniji, omogoča opazovanje odzivov voznika na določeno akcijo na cestišču ali v avtu,« povedo sogovorniki. Dodajo, da danes izsledke in rezultate te tehnologije uporabljajo tudi pri simulatorjih za vojaško uporabo, na njeni osnovi pa so razvili tudi nov simulator, s pomočjo katerega so zmagali na razpisu družbe DARS in s katerim danes soustvarjajo prihodnje slovenske ceste. »Tako se lahko na primer s pomočjo simulatorja zapeljete po tretjem pasu še nezgrajene avtoceste, odločevalci pa lahko na ta način ugotovijo, zakaj na primer določen znak ne bi smel biti na tistem mestu, kamor so ga sprva postavili, in ali je izhod z avtoceste morda prekratek ali pa kako vreme vpliva na stanje na cesti in podobno,« ponazorijo sogovorniki. Dodajo, da sodelujejo tudi z Univerzo v Ljubljani in da se za sodelovanje z njimi zanima vse več znanstvenih ustanov. Upajo, da bo počasi tudi ta, morda za nekatere ljudi sicer tehnologija z druge strani, našla pot tudi v naš vsakdanjik. Ne nazadnje – človek ni stopil na Luno, ker je želel, ampak ker se je tako odločil. Raketa pa je bila razvita v vojaške namene, kajne?

Iskra®

WORLD OF INNOVATIONS

- 70 let tradicije
- 7 proizvodnih obratov
- 1200 zaposlenih
- 3 R&D oddelki
- ISO standardi
- Laboratorij za kalibracijo

PROMET

V Iskri se z avtomatizacijo cestnega prometa ukvarjamo že od leta 1962. Danes so slovenske ceste in avtoceste opremljene in nadzorovane z Iskrino opremo ter nadgrajeno na sodobne standarde

TELEKOMUNIKACIJE

Rešitev za 5G omrežje, mikrovalovni prenos, optične povezave za elektrodistribucijska omrežja, IP omrežja, Metro / MPLS omrežje in varnost IP omrežij

ENERGETIKA

Nudimo rešitev za nadzor distribucijskih pametnih omrežij, rešitve nadzora porabe energije, avtomatizacija v energetiki in industriji, zaščita in vodenje elektroenergetskih sistemov in kompenzacija jalove energije

AVTOMATIZACIJA ŽELEZNIŠKEGA PROMETA

Naši strokovnjaki na podlagi svojega strokovnega znanja in izkušenj ter sodobnih razpoložljivih tehnologij dajejo odgovore na najzahtevnejša vprašanja, povezana z varnostjo sodobnega železniškega prometa.

ELEKTROTEHNIČNE KOMPONENTE

Globalno priznan ponudnik inteligentnih industrijskih rešitev in vrhunskih elektro-tehničnih izdelkov

TRAJNOST

Varujmo naše okolje in poskrbimo za nove generacije. Dajemo velik poudarek energetski učinkovitosti, predvsem prihrankom energije

ISKRA SHIPYARD

Vodilno ladjedelništvo na vzhodni obali Jadranskega morja

TEHNOLOGIJE FILTRIRANJA VODE

Sistemi ki zagotavljajo pitno vodo iz praktično vsakega vodnega vira

Iskra d.o.o.
Headquarters : Stegne 21, 1000 Ljubljana, Slovenia

www.iskra.eu
E-mail : info@iskra.eu

Phone : +386 1 513 10 00
Fax : +386 1 511 15 32

Foto: Arex

Intervju

V času konflikta se lahko hitro zgodi, da ti prijatelji obrnejo hrbet

Država bi morala imeti interes, da je na področju obrambe samooskrbna. Kajti, ko pride do kritične situacije ali konflikta, se lahko hitro zgodi, da ti prijatelji obrnejo hrbet, pravi dolenjski podjetnik Ivan Kralj, direktor podjetja Arex, ki je tudi prejemnik Nagrade GZS za izjemne gospodarske in podjetniške dosežke za leto 2017.

Nina Šprohar

Slovenija velja za razmeroma varno državo. Se vi, kot strokovnjak na tem področju, s to trditvijo strinjate?
Varnost je zelo širok pojem, trenutno je najbolj pomembna varnost pred terorističnimi in drugimi napadi. Dokler se nič ne zgodi, smatram, da smo varni. A nas po drugi strani to ne sme uspavati, saj se čez noč lahko vse spremeni. Če se predstavljamo kot varna država in s tem privabljamo vse mogoče ljudi, je to lahko dvorezen meč. Priložnost dela tatu, pravijo, in s preveč liberalnim pristopom torej damo priložnost tudi tistim, ki nam hočejo slabo.

Smo pripravljeni tudi na primer napada?
Mislim, da smo. Verjamem, da tudi naše obveščevalne institucije delajo tako, kot morajo, in skrbijo za varnost, tudi usposobljenost ljudi je zagotovo na dovolj visokem nivoju, vprašanje je le oprema.

V sodobnih, tehnoloških časih, se kot pereč dejavnik varnostnih groženj pojavljajo tudi kibernetski napadi. Kako dobro smo zaščiteni na tem področju?
Kibernetske napade je izkusil že skoraj vsaj podjetnik in državljan. Osebno menim, da je na tem področju večina podjetij šibkih. Tudi naši poslovni partnerji so doživeli napad, njihov denar se je nakazal na neznan

Varnost je zelo širok pojem, trenutno je najbolj pomembna varnost pred terorističnimi in drugimi napadi.

račun in še vedno ga niso dobili nazaj. Tudi nobena država ni kibernetsko varna, tu Slovenija ni nobena izjema. Še veliko bo treba postoriti, da to stopnjo varnosti dosežemo.

Kaj pa je sicer za podjetje najbolj dragoceno, kaj je tisto, kar se najbolj splača zaščititi?
Podjetje je bogato, če ima dobre delavce, tehnologije in izdelke. Vse našteto se splača zavarovati, čuvati, da ti omenjenega drugi ne ukradejo. Tudi intelektualna lastnina je izrednega pomena, nanjo vedno prežijo tisti, ki se jim ne da izgubljati časa z razvojem in želijo do rešitev priti po krajši poti, torej po bližnjici.

Dokler se nič ne zgodi, smatram, da smo varni. A nas po drugi strani to ne sme uspavati, saj se čez noč lahko vse spremeni.

Najbrž je vaše podjetje še bolj zaščiteno, glede na to, da proizvajate orožje ...
Da, varnost je izrednega pomena, saj so naši izdelki zanimivi tudi za tiste, ki ne razmišljajo le obrambno. Zato imamo varnostne službe, delujemo samozaščitno, pazimo tudi pri komunikaciji, prenosu skic novih izdelkov in podobno.

Je slovenska obrambna industrija v dobri kondiciji?
Proizvajalci – približno 40 nas je –, smo združeni v grozdu, nekateri imajo bolj podporno funkcijo, v splošnem pa skoraj nobeno podjetje ni usmerjeno samo v obrambo, temveč proizvajajo tudi izdelke, namenjene za civiliste. Podobno smo tudi Arex pred časom razdelili na dva dela – na obrambni in na civilni program.

Kibernetske napade je izkusil že skoraj vsaj podjetnik in državljan. Osebno menim, da je na tem področju večina podjetij šibkih.

Kako prijazno za obrambno industrijo je sicer slovensko tržišče? Je povpraševanja dovolj ali se pogosteje obračate na tuje trge?
V šali pravim, da kar Slovenija potrebuje, lahko mi izdelamo v enem dnevu. (smeh) Tisti, ki se za preživetje zanaša na domači trg, je po mojih izkušnjah velik optimist. To zagotovo ni mogoče, saj je slovensko tržišče premajhno. Bi pa država morala imeti interes tudi za našo industrijo, da smo samooskrbni. Ko pride do kritične situacije, konflikta, se lahko hitro zgodi, da ti prijatelji obrnejo hrbet.

Država bi morala imeti interes tudi za našo industrijo, da smo samooskrbni. V Sloveniji domači proizvajalci namreč nimajo prednosti kot ponekod drugod, kjer so lahko domači proizvajalci tudi do 20 % dražji od tuje konkurence.

Vendar smo člani zveze NATO in Evropske unije, najbrž se nanje lahko zanesemo?
Tisti, ki mislijo, da bo zveza NATO rešila vse, se motijo. Dober prikaz tega so Ciper, Grčija, Turčija, zdaj tudi Armenija in Azerbajdžan. NATO nima čarobne paličice, čeprav skušajo ukrepati. Kar je prvi ukrep, je embargo. V Armenijo in Azerbajdžan se od sedaj ne sme več prodajati orožja. Mi lahko torej uspešno delamo le v času miru, takoj, ko nastanejo konflikti, je posla konec. Takrat so vsi deležniki odvisni od domačega trga.

Podjetje je bogato, če ima dobre delavce, tehnologije in izdelke. Vse našteto se splača zavarovati, čuvati, da ti omenjenega drugi ne ukradejo.

Pravite torej, da je obrambne izdelke smiselno proizvajati doma ...
Da, to so pokazale že izkušnje leta 1991. Če tega nimaš, je vse na trhlih tleh. Zagovarjam kakovosten zdravstveni, šolski sistem, a ne smemo pozabiti, da lahko nekoč pride tudi do konflikta in na tej točki je pametno imeti razvito obrambno industrijo.

Očitno tudi naša država razmišlja podobno, saj Ministrstvo za obrambo Republike Slovenije (MORS) načrtuje nabavo vojaške opreme v vrednosti kar 780 mio EUR.
Meni se to ne zdi tako visok znesek, v primerjavi z ostalimi evropskimi državami vlagamo v obrambo precej nižji odstotek proračuna. Dejstvo je, da na trgu za 780 mio EUR ne dobiš tako veliko, poleg tega se tovrstni izdelki hitro starajo – včasih postanejo zastareli že po petih letih.

Zakaj?
Podobno kot na drugih področjih – včasih so avtomobile delali za 40 let, zdaj jih za 10, največ 20 let. Potrošniška mrzlica nas vse sili, da neprestano razvijamo, posodabljamo izdelke. Tudi sodobni materiali niso več tako odporni, spodnji del orožja je večinoma iz polimerov, ki so bolj podvrženi staranju in razpadanju. Življenjska doba orožja je omejena tudi s številom strelov. Konec koncev pa velja omeniti, da ima tudi strelivo omejen rok trajanja, saj po približno 20 letih razpade in lahko pride do samoeksplozije. Ni torej tako, da bi recimo danes vojsko opremili in bi to pomenilo, da je sedaj opremljena za vedno. S časom je treba opremo obnoviti oziroma zamenjati.

Najbrž hitro napreduje tudi tehnologija, ki je vkomponirana v orožje.
Da, izredno hitro. Optične naprave na orožju so podvržene velikim obremenitvam, tresljajem in vibracijam. Po približno 10.000 strelih te naprave odpovedo. Podobnim obremenitvam so izpostavljeni tudi daljinomeri, nočne kamere.

Kam pa gre razvoj tehnoloških dodatkov?
Cilj je predvsem zmanjševanje velikosti ter čim nižja poraba energije.

Se boste tudi vi potegovali za prej omenjeno javno naročilo MORS?
Odvisno, kaj točno bodo kupovali – če bomo želeno imeli na zalogi in če bomo konkurenčni, potem se bomo. V Sloveniji domači proizvajalci namreč nimajo prednosti kot ponekod drugod, kjer so lahko domači proizvajalci tudi do 20 % dražji od tuje konkurence.

Kaj pa sicer proizvajate v podjetju?
Razvitih imamo veliko družin izdelkov, to so strelivo za usposabljanje, pištole, linke za strelivo, specialne stroje za obrambno industrijo, tekstilne izdelke,

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

VALHALLA

Engineering & **Knowledge** matters.

Family of **superior remote control weapon stations**

Specialized in the **design** & **development**
of Remote Controlled Weapon Station.

www.valhalla-turrets.com

izdelke za čelade, za partnerska podjetja pa proizvajamo tudi razne sestavne dele. Prav zadnji sklop predstavlja približno 30 % našega poslovanja. Ne proizvajamo le izdelkov za vojsko in policijo, temveč tudi za civilno družbo.

Zagovarjam kakovosten zdravstveni, šolski sistem, a ne smemo pozabiti, da lahko nekoč pride tudi do konflikta in na tej točki je pametno imeti razvito obrambno industrijo.

A je pri nas zakonodaja glede posedovanja orožja stroga?
Niti ne, imamo različne vrste dovoljenj, recimo za športno rabo, za lov, ne izdajamo pa dovoljenja za lastno varnost. Poleg usposabljanja je treba prestati tudi teste, kjer lahko takoj padeš, če imaš težave z drogami in alkoholom, tudi nekatere bolezni so nezdružljive z rabo orožja. A edina prava in tudi največja težava pri nas je orožje s črnega trga.

Ga je res tako veliko?
Točne številke nihče ne pozna, a vsakič, ko pride do kakšnega neljubega dogodka, vidimo, da je storilec posedoval ilegalno orožje. Ljudje, ki imamo za posedovanje orožja dovoljenje, smo običajno zelo osveščeni, ga imamo radi in se zavedamo, da nam ga lahko policija vzame takoj, ko pride do kakšnega konflikta. Slednje stoodstotno podpiram.

V naši branži se namreč poslov na daljavo ne sklepa, ker se pred prodajo vedno opravi prevzemni test, tega pa na daljavo ni mogoče opraviti.

Koliko je v obrambni industriji dodane vrednosti? Kakšen kader potrebujete v podjetjih?
Potrebujemo predvsem tehnično podkovan kader, a se zavedam, da v šoli vsega znanja ni moč dobiti. Tam lahko mladi dobijo tehnično znanje, usmeritev, potem pa morajo na delovnem mestu pridobiti še praktične izkušnje in specifično znanje, povezano z balistiko, mehaniko, eksplozivi ... Verjamem, da moraš dobrega delavca »narediti« sam.

Kako ste preživeli čas epidemije in kako ste pripravljeni na novo poslabšanje stanja?
V prvem valu smo imeli naročil dovolj, trudili smo se, da ni prišlo do okužb znotraj podjetja in smo v resnici delali še več kot običajno. A kaj kmalu smo prišli do »blokade«, povezane z omejitvijo transporta. Sodelujemo namreč z državnimi ustanovami po celem svetu, do zdaj bi morali biti že na obisku v Braziliji, ZDA in na Filipinih. V naši branži se namreč poslov na daljavo ne sklepa, ker se pred prodajo vedno opravi prevzemni test, tega pa na daljavo ni mogoče opraviti. Tudi sejemske aktivnosti so popolnoma zamrle. Zato lahko pričakujemo, da bomo morali še kar nekaj časa živeti na lovorikah preteklosti in obujati prejšnje kontakte – novih namreč ne moremo vzpostaviti. Je pa tudi dejstvo, da ko opraviš posel v eni državi, potem te 10 let ne potrebujejo več.

Kako boste torej preživeli to težavno obdobje?
Upajmo, da bo šlo, a se zapletamo v težave z bankami. Te so prepričane, da ko pride do vojne, mi že služimo. Pa je to daleč od resnice. Vsak spopad, vsaka vojna za nas predstavlja težavo. Obrambno industrijo pa so namesto tega vrgli v en koš, kot da mi podpiramo teroriste, zato nas banke zelo slabo podpirajo. Evropa že organizira evropsko vojsko, vlaga milijarde v razvoj raznih varnostnih naprav. Če se tudi pri nas ne bo v kratkem kaj spremenilo, bodo določena podjetja propadla, druga pa se bodo preselila v tujino, ker pač ne bodo mogla pridobivati evropskih sredstev s področja obrambne industrije. gg

Banke so prepričane, da ko pride do vojne, mi že služimo. Pa je to daleč od resnice. Vsak spopad, vsaka vojna za nas predstavlja težavo.

Foto: Arex

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

LAHKOTNOST UDOBNOST VARNOST

Kolekcija zaščitne obutve PLANIKA PROTECT sledi sodobnim trendom v obutveni industriji. Lahkotnost, novitete pri uporabi tehnoloških rešitev, udobnost in varnost so osnova pri razvoju modelov. Z dolgoletnimi izkušnjami in lastnim znanjem smo za izdelke iz kolekcije PLANIKA PROTECT razvili udobna in prilagodljiva kopita za zelo širok segment uporabnikov. Vsi modeli iz kolekcije PLANIKA PROTECT zagotavljajo vodotestnost (AIR TEX membrana) ne glede na vremenske razmere. Vse to dosežemo z upoštevanjem najstrožjih meril pri izbiri materialov in pri vgradnji le teh. Vsi sestavni deli ustrezajo strogim proizvodnim standardom, združeni tvorijo celovit izdelek, ki vam skupaj s tradicijo Planike zagotavlja udoben in varen korak v vseh vremenskih pogojih.

S pomočjo dragocenih povratnih informacij ,tako od profesionalnih uporabnikov kot tudi od vsakodnevnih kupcev, razvijamo popolne izdelke, ki ustrezajo vsem zahtevam pri različnih pogojih uporabe.

Razvito in izdelano v Sloveniji.

Planika Turnišče d.o.o., Prešernova ulica 4, Turnišče 9224 tel: +386 2 572 38 65 mail: info@planika-t.si www.planika.si facebook.com/PlanikaTrekking

Investicije v Slovensko vojsko – odlična priložnost za slovensko obrambno industrijo

Sprejem Zakona o zagotavljanju sredstev za investicije v Slovenski vojski v letih 2021–2026 bo za Ministrstvo za obrambo velik premik na bolje glede izgradnje ključnih zmogljivosti. Pred nami bo tudi pomemben izziv, da v te projekte učinkovito in trajnostno vključujemo slovensko industrijo. Ministrstvo za obrambo bo zato, skladno z veljavno zakonodajo, pri nakupu oborožitve in vojaške opreme upoštevalo primerno razmerje med tehničnimi in taktičnimi zahtevami ter podporo slovenski obrambni industriji. Na podlagi tega upravičeno pričakujemo gospodarsko korist za Republiko Slovenijo.


Brezpilotni letalnik

Vključevanje slovenske obrambne industrije bo predvsem odvisno od tehnologije, kakovosti in uspešnosti posameznih podjetij ter gospodarske konkurenčnosti. Poleg možnosti neposrednega vključevanja slovenske industrije za dobave oborožitve in vojaške opreme je še pomembnejše dolgoročno sodelovanje tudi pri drugih projektih v okviru večjih koncernov, predvsem pa vključevanje slovenske industrije in znanosti v nove raziskovalno-razvojne projekte, ki se financirajo iz evropskih obrambnih skladov.

Investicije v Slovensko vojsko

Zakon o zagotavljanju sredstev za investicije v Slovenski vojski v letih 2021–2026 bo zagotovil nujno potrebna sredstva za nabavo glavne opreme na področjih:

- vojaškega letalstva – predvidena je nabava taktičnega transportnega letala in dveh helikopterjev za podporo specialnim silam;
- opremljanja srednje bataljonske bojne skupine – predvidena je nabava kolesnih oklepnih vozil na platformi 8x8, oboroženih z daljinsko vodenimi oborožitvenimi postajami 30 mm, in lahkih kolesnih oklepnih vozil na platformi 4x4 za različne namene;
- zagotovitve delovanja srednje bataljonske bojne skupine – predvidena je nabava taktičnih transportnih vozil, logistične opreme za namestitev in bivanje ter medicinske opreme;
- sistema poveljevanja in kontrole – predvidena je nabava opreme, ki bo zagotovila varen, dinamičen in premestljiv sistem za prenos informacij, sinhronizacijo orožij, povezovanje različnih rodov, visoko raven kibernetske obrambe in izmenjavo informacij z zavezniki v primeru delovanja v mednarodnem okolju, vse skladno s standardi zavezništva;
- zračne obrambe in protioklepnega boja – predvidena je dopolnitev zaloge protioklepnih raket ter nabava ali dopolnitev raketnega sistema zračne obrambe kratkega dosega;
- pehotne oborožitve in opreme za opazovanje – predviden je dokup lahke pehotne oborožitve, ročnih protioklepnih orožij, minometov in optoelektronskih sredstev z možnostjo detekcije ciljev, za opazovanje in namerjanje ter delovanje v vseh pogojih;
- vlaganja v vojaško infrastrukturo za zagotovitev primernih pogojev za delovanje – ob zagotovitvi novih oborožitvenih sistemih bo prilagojena vojaška infrastruktura, izgrajeni bodo novi in posodobljeni stari logistični objekti (garaže, skladišča, delavnice) ter infrastruktura za usposabljanje (simulatorji, strelišča, poligoni).

Dobra praksa vključevanja slovenske industrije in znanosti pri nakupu ali razvoju obrambnih proizvodov

Slovenska obrambna industrija je organizirana v Gospodarsko interesnem združenju – Grozdu obrambne industrije Slovenije (v nadaljevanju: GOIS). V GOIS je trenutno vključenih 40 slovenskih podjetij z letnim prometom več kot 500 milijonov evrov. Od tega izvoz predstavlja 75 odstotkov letne proizvodnje z dodano vrednostjo na zaposlenega 57.000 evrov, kar je za 25 odstotkov več od slovenskega povprečja. Temu je treba dodati, da ima 60 slovenskih podjetij soglasje za proizvodnjo vojaškega orožja ali opreme.

Razvoj slovenske obrambne industrije je odvisen od obrambnega sistema. V času izvajanja temeljnih razvojnih programov, pred več kot desetletjem, so bila Slovenski vojski zagotovljena sredstva za izgradnjo zmogljivosti ter izvajanja ciljnih raziskovalnih programov (CRP) in izvajanja razvojno-tehnoloških projektov (TP-MIR), ki so sledili razvojnim ciljem in zagotavljanju

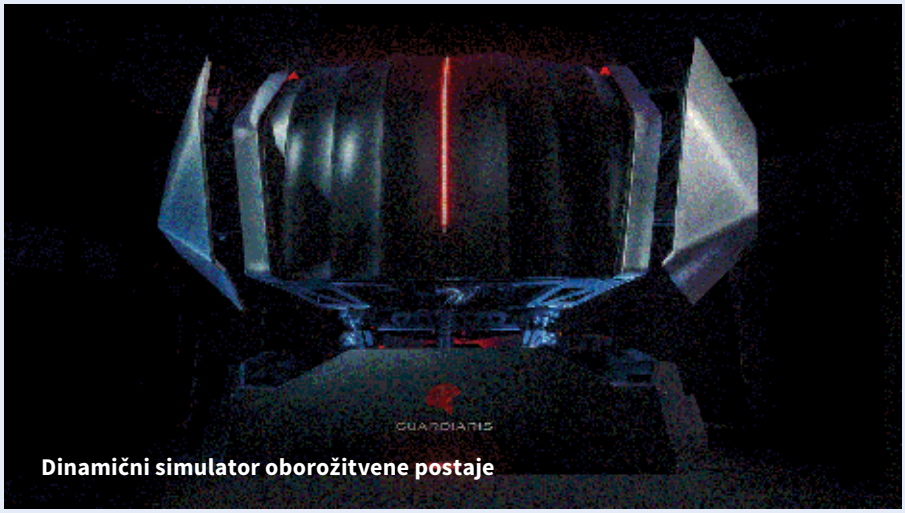
razvoja zmogljivosti Slovenske vojske. Povezano s tem so nastala nova slovenska podjetja, nekatera obstoječa podjetja pa so začela postopno preusmeritev na obrambno industrijo. Podlaga za sodelovanje je bila določba v obeh zakonih, da se pri nakupih oborožitvenih sistemov in opreme v pogodbe vključi zahteva po izvajanju programa protidobav. Iz vseh treh navedenih področij imamo nekaj zelo uspešnih podjetij tudi v svetovnem merilu, na primer na področju izdelave linkov za strelivo, lahkih brezpilotnih letalnikov za različne namene, zložljivih turnih smuči za vojaške namene ter različnih simulacijskih in trenažnih sistemov za oborožitvene sisteme.

Na Ministrstvu za obrambo tako ugotavljamo, da imamo v Republiki Sloveniji vrhunske znanstvene ustanove, pa tudi podjetja, ki lahko razvijajo in proizvajajo različne tehnološko zahtevne sisteme, uporabne na obrambnem področju ter na področju zaščite in reševanja. Naj pri tem omenimo razvoj prvega slovenskega satelita, ki sta ga razvili slovenski znanost in industrija. V tem projektu sicer naše ministrstvo ni sodelovalo, vendar ocenjujemo, da je to znanje izrednega pomena za razvoj novih vojaških zmogljivosti.

Podlaga za sodelovanje Ministrstva za obrambo z industrijo je Program sodelovanja, podpisan leta 2010, ki natančneje opredeljuje sodelovanje med podjetji obrambne industrije, vključenimi v GOIS, in ministrstvom, in sicer predvsem pri:

- informiranju in možnem vključevanju slovenske obrambne industrije pri nakupih novih oborožitvenih sistemov,
- povečanju obsega razvojnih projektov, ki bodo vodili do novih obrambnih proizvodov ter posledično večje konkurenčnosti slovenske obrambne industrije,
- podpori industriji in znanosti pri oblikovanju in izvajanju mednarodnih raziskovalno- razvojnih projektov,
- skupinskih nastopih na sejmih oborožitve in vojaške opreme ter sodelovanju pri drugih promocijskih dogodkih,
- zagotavljanju vojaških standardov in kodifikaciji sredstev preskrbe ter zagotavljanju kakovosti skladno z zahtevami Nata.

V preteklih letih se je sodelovanje med ministrstvom in industrijo poglobilo predvsem pri preizkušanju novih obrambnih proizvodov, razvitih v slovenski industriji. To sodelovanje se je izrazilo predvsem pri izvozu obrambnih proizvodov, ki se je v zadnjih letih



Dinamični simulator oborožitvene postaje

povečal za desetkrat oziroma se je v obdobju izvajanja programa protidobav glede na najboljša leta v preteklosti podvojil.

Nadaljnji razvoj slovenske obrambne industrije

Novi nakupi oborožitve in vojaške opreme za Slovensko vojsko so izziv in priložnost za slovensko industrijo. Temu smo se zavezali tudi s pristopom Republike Slovenije k sodelovanju PESCO (Stalno strukturno sodelovanje na področju obrambe EU – Permanent Structure Cooperation), s čimer sledimo cilju okrepitve nacionalne obrambe ter skupne zunanje in varnostne politike EU.

Investicije v Slovensko vojsko ter vlaganja v raziskave in razvoj na obrambnem področju bodo pripomogli k integraciji slovenske obrambne industrije in znanosti v širše evropske povezave, kar bo pripomoglo k rasti slovenske in evropske obrambne industrijske baze.

Pri izvajanju postopkov naročil oborožitve in vojaške opreme se bomo srečevali z zaščito bistvenih interesov varnosti države članice, kar je opredeljeno v 346. členu Pogodbe o delovanju EU. V tem je podlaga za vključevanje slovenske obrambne industrije pri dobavi, vzdrževanju ter poznejših nadgradnjah oborožitve in vojaške opreme.

Z Zakonom o zagotavljanju sredstev za investicije v Slovenski vojski v letih 2021–2026 se ureja poraba sredstev v višini 780 milijonov evrov za investicije v Slovenski vojski. Glede na trenutno dobro prakso, vključevanje slovenske obrambne industrije v različne projekte, tudi mednarodne raziskovalno-razvojne projekte, in stopnjo tehnološke razvitosti ocenjujemo, da bo večino vloženih sredstev v razvoj


Taktična pištola

zmogljivosti Slovenske vojske mogoče povrniti z izvozom novih obrambnih proizvodov v desetletnem obdobju. Primer dveh slovenskih podjetij govori v prid tej trditvi. Pred enim mesecem sta podpisali pogodbi za razvoj daljinsko vodene oborožitvene postaje z nemškim obrambnim ministrstvom ter za razvoj in dobavo taktičnih simulacijskih centrov za pehotno orožje z avstrijskim obrambnim ministrstvom. Slovensko podjetje v tem trenutku končuje vse priprave za zagon proizvodnje pištol v Braziliji. Glede vlaganja v vojaško infrastrukturo je mogoče že zdaj predvideti, da bodo gradbena dela praviloma izvajala slovenska gradbena podjetja. Tako je bilo tudi v primeru posodobitve vojaškega letališča v Cerkljah ob Krki, kjer je vložek Natovih sredstev 40 milijonov evrov, pri čemer so praviloma vsa dela izvajala slovenska podjetja.

Pomembo vlogo pri vključevanju slovenske obrambne industrije v nove nakupe bo prevzel tudi GOIS, predvsem s pripravo in izvedbo strokovnih tematskih srečanj med ponudniki oborožitve in vojaške opreme ter slovensko obrambno industrijo.

Na ravni EU poteka povezovanje nacionalnih obrambnih agencij in grozdov, grozd pričakuje nove priložnosti za slovensko obrambno industrijo.

Obramba

Širok spekter slovenskih proizvodov in storitev na področjih obrambe, varnosti in zaščite

Gospodarsko interesno združenje Grozd obrambne industrije Slovenije – GIZ GOIS služi kot glavna organizacijska ter informacijska povezovalna točka med slovensko industrijo, znanstveno-raziskovalnimi organizacijami in državo.

Ana Vučina Vršnak

3.000 delavcev zaposluje 40 članov GIZ GOIS.

Člani Gospodarskega interesnega združenja Grozd obrambne industrije Slovenije (GIZ GOIS) – trenutno jih je 40 in zaposlujejo več kot 3.000 delavcev – ponujajo zelo širok spekter proizvodov in storitev. »Njihova prednost je, da so s svojim proizvodnim in storitvenim programom v absolutni večini del obrambnega in hkrati civilnega sektorja. Posledično je temu primerno tudi upravljanje z riziki in fleksibilnost pri izvrševanju že dogovorjenih poslov ali pridobivanju novih,« pojasnjuje Ante Milevoj, direktor GIZ GOIS.

57.000 EUR znaša dodana vrednost na zaposlenega v podjetjih članih grozda.

Pol milijarde prometa

Omenjeni grozd je prostovoljno in samostojno interesno združenje ponudnikov proizvodov in storitev na področju obrambe, varnosti in zaščite. Podjetja, ki so povezana v grozd, beležijo okoli 500 mio EUR letnega prometa, 75 % od tega predstavlja izvoz. Dodana vrednost na zaposlenega med člani je 57.000 EUR, kar je 25 % več od slovenskega poprečja, poudari Milevoj.

GOIS služi kot glavna organizacijska in informacijska povezovalna točka med slovensko industrijo, znanstveno-raziskovalnimi organizacijami in državo. Hkrati je vključen tudi v mednarodne povezave, za svoje člane opravlja naloge poslovnega razvoja trgov, mreženja, organizira sejme in kreira poslovne priložnosti.

Nove priložnosti ob povezovanju nacionalnih obrambnih agencij in grozdov

Glede na trenutno stanje, »novo realnost«, želijo po besedah Milevoja v čim večji meri speljati letni program dela. Sejemske aktivnosti so v veliki meri odpadle ali pa so prestavljene na naslednje leto. »V tem letu krepimo delo s člani, kjer to lahko naredimo z uporabo virtualnih orodij, na tematskih seminarjih, individualnih mreženjih s tujimi sogovorniki, vključevanjem v evropske projekte v okviru Evropske obrambne agencije. Na ravni EU poteka tudi povezo-

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

SeanTech
process engineering

SeanTech procesni inženiring, reševanje sodobnih tehnoloških izzivov po meri kupca

SeanTech process engineering, solving modern technological challenges

SeanTech, procesni inženiring, d.o.o. je slovensko podjetje z blagovno znamko Gostol procesna oprema, ki se osredotoča na razvoj in implementacijo celovitih rešitev procesne opreme, prilagojene tehnologiji kupcev, skladno z direktivo ATEX za implementacijo opreme v potencialno eksplozijsko ogrožena okolja, GAMP, 21 CFR Part 11 in standardi EU.

Kupcem ponuja odgovor na njihove tehnološko-tehnične izzive z razvojem in proizvodnjo prilagojene procesne opreme, njeno implementacijo v proizvodnjo kupca, zagonom in izobraževanjem osebja ter s poprodajnimi aktivnostmi servisiranja in zagotavljanja rezervnih delov.

Prodajni program obsega lastne rešitve za stroje ter avtomatizirane industrijske, pilotne ali laboratorijske linije v Ex-industrijah in drugih industrijah. Sestavljajo ga najrazličnejše vrste mešalnikov, gnetilnikov, hidravličnih stiskalnic, dvovaljnikov, ekstruderjev, škarij, mlinov, rezalnikov-drobilnikov, granulatorjev, navijalnikov cevi GRP in drugih rešitev za gumarsko, livarsko, farmacevtsko, prehrambno, kemično, namensko industrijo, proizvodnjo kompozitnih cevi GRP, tehnične keramike in drugih izdelkov. Kupcem ponujajo učinkovite, avtomatizirane in nadzorovane procese mešanja, gnetenja, homogeniziranja, iztiskanja, valjanja, ekstruzije, sekanja, mletja, rezanja, sušenja, granuliranja, sejanja, oblaganja, navijanja in druge.

SeanTech, procesni inženiring, d.o.o.

Phone: + 386 (0)5 33 11 700, Fax: + 386 (0)5 33 11 709
e-mail: info@seantech.eu, website: www.seantech.eu
Headq.: Mekinčeva ul. 15, SI-1000 Ljubljana
Branch: Prvomajska ul. 37, SI-5000 Nova Gorica
Office: Kidričeva ulica 9a, SI-5000 Nova Gorica, Slovenia, EU

process equipment
gostol
YEARS OF TRADITION

Člani grozda so imeli sredi septembra priložnost svoje rešitve predstaviti tujim veleposlanikom iz držav članic NATO.

vanje nacionalnih obrambnih agencij in grozdov. Tudi od tega pričakujemo nove priložnosti za slovensko obrambno industrijo,« pravi Milevoj.

Prihodnje leto na sejme

Veliko pričakovanja je med člani glede obrambnega sejma IDEX (International Defence Exhibition), ki bo v Abu Dhabiju predvidoma potekal med 21. in 25. februarjem 2021, in ki je poleg sejma Eurosatory v Parizu verjetno najbolj reprezentativni sejem na področju obrambe. »Tudi člani GOIS bodo tam – tako v okviru skupinske stojnice v organizaciji agencije SPIRIT Slovenija, kot tudi s samostojnimi stojnicami,« pravi Milevoj in dodaja, da bo večina podjetij obrambne industrije po načrtih prav tako sodelovala na mednarodnem sejmu obrambe, varnosti, zaščite in reševanja (SOBRA) v Gornji Radgoni med 23. in 25. septembrom 2021. Ker bo sejem potekal v času predsedovanja Slovenije Evropski uniji, si po besedah Milevoja člani GOIS obetajo dodatne sinergične učinke od nastopanja na sejmu in spremljevalnem programu.

Predstavitev veleposlanikom

Sredi septembra so se člani GIZ GOIS srečali z ministrom za zunanje zadeve Anžetom Logarjem in tujimi veleposlaniki. Člani grozda so imeli priložnost svoje rešitve predstaviti tujim veleposlanikom iz držav članic NATO.

Na sliki od leve: Ante Milevoj, Matej Tonin in Ivan Kralj.

Vljudnostni obisk pri ministru Toninu

Prav tako pa je GIZ GOIS septembra obiskal še obrambnega ministra Mateja Tonina. Kot je povedal Milevoj, je bilo srečanje vljudnostne narave. Predstavili so aktivnosti grozda ter se dotaknili skupnih projektov. gg

»Z aprilom 2020 se je upokojil prvi direktor GIZ GOIS Jože Renar. Za njegovo več kot desetletje dolgo in predano delo v korist slovenske obrambne industrije se mu lepo zahvaljujemo in mu želimo prijetno nadaljevanje v novem poglavju. Dolžnost direktorja je prevzel Ante Milevoj, ki mu želimo uspešno delovanje v tej vlogi.«
Ivan Kralj, predsednik NS GIZ GOIS

alpos alu

Serijski in projektni proizvajalec izdelkov iz aluminija

Tradicija in znanje – naše bistvene prednosti.

ALPOS ALU aluminijasti izdelki so proizvedeni v skladu z evropskimi standardi, kar potrjujejo in redno preverjajo pooblaščene evropske ustanove. Proizvodi blagovne znamke "alpos alu" so prepoznavni kot sinonim kakovosti in zadovoljstva kupcev.

ALPOS ALU d.o.o.
Cesta Kozjanskega odreda 29b
SI-3230 Šentjur
SLOVENIJA

T: +386 3 74 62 750
F: +386 3 74 62 770
E: info@alpos.si
www.alpos.si

PIO FLASH - uparjalni sistem, ki z uporabo sredstva na bazi vodikovega peroksida Izaeffect zagotavlja najboljše rezultate

Vsi se soočamo z nevarnostjo širitve epidemije COVID-19 in z ukrepi, ki so nam spremenili vsakdan. Podjetja in organizacije iščemo rešitve, kako s svojim znanjem in izkušnjami pomagati pri nastali situaciji. Tako je v času korone prišlo do sodelovanja med podjetjem Iskra Pio, ki je visoko tehnološko podjetje, ter podjetjem Iza, ki se že več let celovito specializira za dezinfekcijo na področju izdelave dezinfekcijskih sredstev Izaeffect po lastni formuli. Vsa sredstva so pred lansiranjem na trg testirana in priglašena na Uradu za kemikalije. So biorazgradljiva in niso nevarna za uporabo.

Združili znanje in tehnologijo

Iskra Pio že od leta 1991 projektira in izdeluje opreme za čisto in čistilno tehnologijo za farmacevtska podjetja, medicinske ustanove, lekarne ter raziskovalne institute doma in v tujini. Z intenzivnim zaposlovanjem visoko strokovnega kadra v vseh letih se nenehno povečuje asortima in obseg proizvodnje ter zvišuje raven kakovosti izdelkov. Eden izmed programov podjetja Iskra PIO so tudi dekontaminacijske naprave, ki so nujno potrebne za zagotavljanje sterilnih pogojev pri izdelavi zdravil. Kot najučinkovitejša bio-dekontaminacija se je po več kot 25-letnih izkušnjah izkazal PIO FLASH uparjalni sistem, ki z uporabo sredstva na bazi vodikovega peroksida – Izaeffect zagotavlja najboljše rezultate. Sistem deluje na principu kombinacije uparjalne faze in zelo drobnih kapljic suhe megle vodikovega peroksida; tako združuje več različnih stanj vodikovega peroksida, ki ima zaradi svoje kompleksnosti odlične rezultate mikrobiološke dekontaminacije.

Razvili mobilne dekontaminacijske naprave DECON

Znanje in tehnologijo smo združili s strokovnim znanjem, ki ga ima na področju dezinfekcijskih sredstev družba Iza, in tako na podlagi znanja in potreb trga razvili mobilne dekontaminacijske naprave DECON. To so samostojne ergonomsko oblikovane naprave, ki preko distribucijskega sistema generirajo dezinfekcijski aerosol. Ta služi razkuževanju prostora, v katerem je.

Zaradi svoje enostavnosti in majhnosti so naprave DECON primerne za dekontaminacijo prostorov v farmaciji in zdravstvu, pa tudi v hotelih, gostinskih lokalih, domovih za ostarele, šolah, vrcih, poslovnih stavbah, avtomobilih, vlakih, letalih in drugih prostorih, kjer je treba zagotavljati ustrezno mikrobiološko raven čistosti.

V zadnjem obdobju smo z dodatnimi testi z dezinfekcijskim sredstvom Izaeffect dobili odlične rezultate aerosolnega razkuževanja, ki učinkovito uniči bakterije, plesni, glive in viruse, za njim pa ne ostane nobene sledi, saj razpade na kisik in vodo. Vsi rezultati so dokazani s potrebnimi testi učinkovitosti.

IZA EFFECT® BIO RAZGRADLJIVO RAZKUŽEVANJE

p:o Clean visions.

Foto: TKK

V podjetju TKK ves čas posodabljajo obstoječi sistem aktivne požarne zaščite.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Požarna varnost

Požarna varnost je del celovite politike varnosti

Požarna preventiva sodi med najpomembnejše organizacijske ukrepe v Heliosu, v TKK so v ta namen v petih letih investirali skoraj pol milijona evrov, v Kemisu 1,5 milijona evrov.

Darja Kocbek, Ana Vučina Vršnak

Na Heliosovi lokaciji na Količevem je Center za zaščito in reševanje, kjer pogodbeno sodelujejo s poklicnimi gasilci – ti opravljajo redne preventivne obhode ter izvajajo požarne straže.

Podjetja, ki se zavedajo, kako veliko škodo in posledično stroške jim lahko povzroči požar, ne izpolnjujejo le minimalnih zahtev za požarno varnost, ki jih predpisuje zakonodaja. Za ta podjetja je požarna varnost del celovite politike varnosti in ves čas investirajo v ukrepe za izboljšanje požarne varnosti.

V Heliosu so razvili lasten program usposabljanja »Gasilec za prvo intervencijo«

V podjetju Helios TBLUS požarna preventiva sodi med najpomembnejše organizacijske ukrepe, ki jih izvajajo na vseh lokacijah podjetja. Na lokaciji na Količevem je Center za zaščito in reševanje v neposredni bližini podjetja. Na tej lokaciji pogodbeno sodelujejo s poklicnimi gasilci, ki v Heliosu opravljajo redne preventivne obhode ter izvajajo požarne straže. V sklopu podjetja v Preski pri Medvodah deluje poklicna gasilska enota, kjer je zaposlenih 10 poklicnih gasilcev. Gasilci so na lokaciji prisotni 24 ur dnevno, vse dni v letu. Poleg tega je skoraj 350 zaposlenih članov Prostovoljnega industrijskega gasilskega društva Helios, razvili pa so tudi edinstven lasten program usposabljanja »Gasilec za prvo intervencijo«. Prostovoljno industrijsko gasilsko društvo Belinka pa deluje v sklopu podjetja na lokaciji

Kdor za požarno varnost poskrbi, je v prostem času brez skrbi

Oktobra obeležujemo mesec požarne varnosti. Letošnja tema projekta, v katerem sodelujejo Uprava za zaščito in reševanje, Gasilska zveza Slovenije in Slovensko združenje za požarno varstvo, je požarna varnost v prostem času in poteka pod sloganom Kdor za požarno varnost poskrbi, je v prostem času brez skrbi.

Namen letošnjega projekta je opozoriti prebivalce, da tudi med preživljanjem prostega časa obstaja veliko nevarnosti, ki lahko povzročijo požar. Ne glede na to, kje preživljamo prosti čas, ne smemo pozabiti, da lahko kadarkoli zagori. Da bo prosti čas minil brezskrbno in veselo, je pomembno, da poznamo preventivne ukrepe, s katerimi lahko preprečimo nastanek požara.

Foto: Helios

V podjetju Helios TBLUS požarna preventiva sodi med najpomembnejše organizacijske ukrepe, ki jih izvajajo na vseh lokacijah podjetja.

Zasavska cesta. Na tej lokaciji obenem sodelujejo še s poklicnimi gasilci Gasilske brigade Ljubljana.

»Na vseh lokacijah podjetja z načrtnimi vlaganji sistematično vzdržujemo visok nivo požarne varnosti. V preteklih treh letih smo obnovili in na novo namestili sisteme šprinkler za javljanje in gašenje požara v več objektih na lokacijah podjetja Helios TBLUS na Količevem in v Preski,« pojasnjuje Maša Bantan Marot, vodja korporativnega komuniciranja. S tem namenom so leta 2015 na lokaciji podjetja v Preski dogradili požarni bazen z več kot 1.000 m3 vode, ki je omogočil tudi dograditev lastne hidrantne mreže. »V obdobju 2018-2019 smo na tej lokaciji obnovili kombinirano gasilsko vozilo, v letošnjem letu pa smo začeli z obnovo požarnih redov in načrtov evakuacije,« je še povedala Bantan Marotova.

Na vseh lokacijah izvajajo redna izobraževanja zaposlenih na temo požarne varnosti v obliki predavanj, praktičnih usposabljanj ter gasilskih in evakuacijskih vaj. Prav tako ves čas vlagajo v projekte za izboljšanje zdravja, varnosti pri delu in okolja.

Za ločevanje dveh požarnih sektorjev so med objektom tesnilnih mas in poliuretanskih pen oziroma prekritjem med halama namestili tri požarne zavese.

V TKK so v zadnjih petih letih sprejeli pet večjih ukrepov

V podjetju TKK ves čas posodabljajo obstoječi sistem aktivne požarne zaščite. »V zadnjih petih letih smo veliko naredili v smeri povečane požarne varnosti. Sprejeli smo pet večjih ukrepov, uvedli številne posodobitve in v nadgradnjo požarne varnosti investirali skoraj pol milijona evrov, natančneje 455.500 EUR,« nam je pojasnila vodja marketinga Katja De Kimpe.

Za ločevanje dveh požarnih sektorjev so med objektom tesnilnih mas in poliuretanskih pen oziroma prekritjem med halama namestili tri požarne zavese. V mešalnici pod stropom so namestili razvod cevi šprinkler, kamor so pritrjene šobe šprinkler »ampoule«. Šobe delujejo tako, da pri povišani temperaturi okolja (nad 70 °C) počijo, iz njih pa začne škropiti mešanica vode s penilom – gasilo.

»Tudi v novem visokem regalnem skladišču je nameščen sistem šprinkler. Vodo zanj črpamo z dizelsko črpalko iz požarnega bazena velikosti 1.050 m3 , ki se nahaja pod skladiščem,« razlaga Katja De Kimpe. Za ločevanje požarnih sektorjev so skladno z izdelano požarno študijo na prehodih skladišča namestili požarna vrata, ki se ob sprožitvi požarnega alarma avtomatsko zaprejo.

Na prehodu iz proizvodnje v skladišče je nameščena požarna zapornica z namenom preprečevanja onesnaževanja okolja s požarno vodo. Voda od sistema šprinkler se ulovi za zapornico v skladiščni hali, ki je zgrajena kot lovilna posoda za zajem razlitih kemikalij in požarne vode.

Kurilnico so v TKK opremili z gasilnim sistemom B-12 BONPET in javljalci požara. V primeru, da se sproži javljalec požara, se izklopi delovanje gorilnikov in ustavi dotok goriva v kurilnico.

Požarno centralo so posodobili s sistemom alarmiranja Prostovoljne industrijske gasilske enote (PIGE). Z vklopom oz. pritiskom na gumb ročnega javljalca požara kjerkoli v podjetju centrala pošlje sporočilo (SMS pozivnik) vsem članom PIGE. »V podjetju TKK ves čas posodabljamo obstoječi sistem aktivne požarne zaščite. Tako smo letos razširili šprinkler sistem tudi v proizvodnjo tesnilnih mas, v garderobe in v naše nove laboratorije,« nam je še pojasnila Katja De Kimpe.

Kemis je v petih letih v izboljšanje požarne varnosti vložil približno 1,5 milijona evrov

Veliko pozornost požarni varnosti namenjajo tudi v Kemisu. Sprejete imajo ukrepe za zagotavljanje požarne varnosti na tehnični in organizacijski ravni. Tehnična raven se nanaša na opremljenost prostorov in na opremo za pasivno in aktivno požarno varnost. Objekt podjetja je tako razdeljen na 33 požarnih sektorjev, ki imajo javljalnike požarov in so povezani z avtomatskim sistemom javljanja požara. Požarni sektorji so razdeljeni s stenami, ki so odporne na ogenj. Celoten skladiščni in manipulativni prostor je pokrit s kamerami in dogajanje spremlja varnostnik, ki je prisoten 24 ur vse dni v tednu.

Nad celotnim območjem objekta je nameščen avtomatski gasilni sistem, ki sproži gašenje le na lokaciji požara in deluje neodvisno od električne energije iz omrežja ter ima lasten bazen vode za gašenje. Objekt ima tudi hidrantno omrežje, ki se napaja iz javnega vodovoda in prek 100 ročnih gasilnih aparatov. Imajo tudi IR kamero, s katero vsak dan kontrolirajo temperaturo skladiščenih odpadkov.

»Na organizacijski ravni požarno varnost zagotavljamo z opremljenostjo in usposobljenostjo zaposlenih za preventivno delovanje in ukrepanje. V

Varno ravnanje z odpadki, še posebej nevarnimi, je nepogrešljiv del infrastrukture sodobne družbe. GZS že leta opozarja na pomanjkljivo infrastrukturo in moteno delovanje sistema ravnanja z odpadki, zaradi česar prihaja do nezaželenega kopičenja različnih vrst odpadkov po vsej Sloveniji, kar povzroča vrsto težav, tudi zelo nevarnih. Odločba inšpekcije, ki enemu od dveh podjetij, ki v Sloveniji zagotavljata varno obdelavo nevarnih odpadkov, prepoveduje sprejemanje le-teh, je v nasprotju s širšimi interesi javnosti v državi, kjer imamo že zdaj omejene zmogljivosti za varno, sprotno in brezhibno ravnanje z odpadki, ki jih ustvarimo. Zato GZS nasprotuje taki nerazumni in škodljivi odločbi, ki je bila sprejeta še pred zaključkom postopkov za legalizacijo posodobljenih objektov.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

sklopu načrta zaščite in reševanja imamo opredeljene vse postopke v primeru različnih nesreč, zaposlene izobražujemo in izvajamo različne vaje. Imamo osem prostovoljnih gasilcev, ki imajo na lokaciji Kemisa vso potrebno opremo v posebnem zabojniku in so člani PGD Sinja Gorica,« pojasnjujejo v Kemisu.

Za zagotavljanje požarne varnosti sodelujejo tudi z gasilci na območju Vrhnike. Že več kot 10 let odlično sodelujejo z GZ Vrhnika ter bližnjimi prostovoljnimi gasilskimi društvi. »Naši prostovoljni gasilci se udeležujejo izobraževanj z drugimi prostovoljnimi gasilci, ki tudi izobražujejo naše zaposlene in enkrat letno skupaj izvedemo tudi praktično vajo gašenja. Občasno pa skupaj z GZ in prostovoljnimi gasilskimi društvi izvedejo širšo vajo ukrepanja ob nesreči v Kemisu,« so nam razložili.

V sklopu zaščite in reševanja Kemis redno letno donira določena sredstva za nakup opreme za prostovoljna gasilska društva na območju GZ Vrhnika. »V zadnjih petih letih smo v izboljšanje požarne varnosti vložili približno 1,5 milijona evrov. Z rednim osveščanjem glede preventivnega delovanja in z usposabljanjem se zavzemamo za nenehno izboljševanje požarne varnosti v podjetju,« so nam še povedali. gg

Regijski natečaj – Požarna varnost in prosti čas

Uprava RS za zaščito in reševanje v šolskem letu 2020/2021 razpisuje natečaj »Naravne in druge nesreče na temo Požarna varnost in prosti čas!« za predšolsko in šolsko mladino. Predmet natečaja je izdelava likovnih in literarnih izdelkov ter filmov na temo požarna varnost in prosti čas. Rok za oddajo izdelkov je 14. februar 2021.

»Z natečajem Naravne in druge nesreče želimo mlade, posredno pa tudi njihove starše, vzgojitelje in učitelje ozavestiti oziroma informirati, da s preventivnim znanjem in ravnanjem lahko nekatere naravne in druge nesreče preprečijo, pri nekaterih nesrečah pa pripomorejo k zmanjšanju škode oziroma sebi ali komu drugemu rešijo življenje,« so dejali v Upravi za zaščito in reševanje.

Mlade so pozvali, naj pišejo, rišejo ali posnamejo film o tem, kako jim je preventivno znanje in ravnanje pomagalo preprečiti nastanek požara ali pa jim je pomagalo, da so ob požaru v prostem času pravilno ravnali in s tem pripomogli k zmanjšanju škode oziroma so sebi ali nekomu drugemu lahko rešili življenje.

Nad celotnim območjem objekta je nameščen avtomatski gasilni sistem, ki sproži gašenje le na lokaciji požara in deluje neodvisno od električne energije iz omrežja ter ima lasten bazen vode za gašenje.

Foto: Depositphotos

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Kako podjetja skrbijo za varnost

Pomembno je slediti trendom in dobrim praksam

Hiter razvoj informacijsko-komunikacijskih tehnologij (IKT), digitalizacija in podnebne spremembe so za podjetja nove grožnje, proti katerim je treba zagotoviti ustrezno varovanje.

Darja Kocbek

V Petrolu zatrjujejo, da tehnično varovanje zagotavljajo po zadnjih standardih s področja tehnične zaščite.

Razvoj novih tehnologij in znanj podjetjem omogoča, da svoje premoženje in ljudi lahko vse učinkoviteje zavarujejo pred škodo. Istočasno pa so zlasti hiter razvoj IKT, digitalizacija in podnebne spremembe nove grožnje, proti katerim je treba zagotoviti ustrezno varovanje. Poskrbeti morajo za ustrezno kombinacijo fizičnega in tehničnega varovanja ter varovanje pred kibernetskimi napadi. Slednjih je vse več. Nacionalni odzivni center za kibernetsko varnost SI-CERT je lani zabeležil 2.733 napadov, leta 2015 jih je bilo 1925, leta 2010 pa 478.

Petrol ves čas investira v tehnično varovanje

Petrol kot energetska družba sodi med zavezance iz naslova uredbe o obveznem organiziranju varovanja. V podjetju so nam pojasnili, da fizično varovanje na varovanih območjih izvajajo v skladu z veljavno zakonodajo kot obliko zagotavljanja varovanja ljudi in premoženja. Ostalih oblik fizičnega varovanja se poslužujejo glede na oceno ogroženosti.

Prav tako ima Petrol vse objekte, ki jih ima v lasti, tehnično varovane. V podjetju zatrjujejo, da tehnično varovanje zagotavljajo po zadnjih standardih s področja tehnične zaščite. V to področje tudi ves

čas investirajo in tako sledijo trendom in dobrim praksam.

Varnost pred kibernetskimi vdori v Petrolu zagotavljajo »z ekipo strokovnjakov, ki z uporabo sodobnih varnostnih mehanizmov, tehnologij in rešitev zagotavljajo visoko raven varnosti s preprečevanjem, zaznavanjem in omejevanjem vdorov«. Pri zagotavljanju kibernetske varnosti sodelujejo tudi z zunanjimi strokovnjaki, ki imajo ustrezna znanja in reference za to področje dela.

»Penetracijske teste izvajamo redno. Izvajalce posameznih testiranj vedno izberemo med kompetentnimi izvajalci tovrstnih aktivnosti. Gre za načrtovane penetracijske teste, fokusirane na določena področja. Po potrebi izvajamo penetracijske teste ob vpeljavah novih rešitev zaradi dodatnega preverjanja varnosti,« so nam še pojasnili v Petrolu.

Plinovodi širijo sistem videonadzora

V družbi Plinovodi, ki je operater prenosnega sistema zemeljskega plina, prav tako pravijo, da zagotavljajo visoko raven fizičnega in tehničnega varovanja svojih objektov in sistemov. V družbi imajo sistem tehničnega varovanja, v katerega so integrirani sistemi protipožarnega varovanja, protivlomnega varovanja, video-nadzorni sistem in sistem kontrole pristopa.

Nacionalni odzivni center za kibernetsko varnost SI-CERT je v letu 2019 zabeležil 2.733 kibernetskih napadov, kar je 12 % več kot leta 2018. Povprečno oškodovanje z vrivanjem v poslovno komunikacijo je doseglo 65.000 EUR. Največje posamično oškodovanje z vrivanjem v poslovno komunikacijo je zneslo 200.000 EUR, najvišje oškodovanje v direktorski prevari 35.000 EUR. Največja znana ocenjena škoda pri napadu izsiljevalskega virusa je lani bila 2,4 mio EUR. V poslovnem okolju so predvsem zaskrbljujoči trendi okužb z izsiljevalskimi virusi (ransomware), v poročilu navaja SI-CERT. Napadalci so v zadnjih letih prešli iz množičnega širjenja virusov vsem uporabnikom v bolj usmerjene kampanje, kjer iščejo omrežja podjetij in javnih ustanov, ki niso povsem dobro zaščitena. Odkupnine, ki jih zahtevajo, so med 10.000 in 100.000 EUR. Vstopne metode niso novost: najbolj uporabljena vstopna točka so bili slabo zaščiteni oddaljeni dostopi – dejstvo, ki mora upravljavce omrežij še posebej skrbeti v današnjem času epidemije in povečanega dela od doma, opozarjajo na centru SI-CERT.

Izveden imajo prenos požarnih in protivlomnih signalov v varnostno-nadzorni center. Na centralni lokaciji izvajajo tudi fizično varovanje s stalno prisotnostjo varnostnikov.

»Na področju informacijske varnosti razpolagamo z moderno tehnološko opremo, ki zagotavlja varovanje vseh komunikacij z internetom in zaščito vseh končnih točk na strani uporabnikov. V obratovanju imamo centralni sistem za nadzor delovanja strežnikov, komunikacij in požarnih zidov,« so nam razložili v Plinovodih. Pri razvoju in upravljanju informacijskih sistemov sledijo najnovejšim varnostnim smernicam in dobrim praksam na področju informacijske varnosti.

Uvedli so sistem za upravljanje varnostnih dogodkov in tveganj v realnem času (Security Information and Event Management – SIEM) in vzpostavili Sistem Upravljanja Varovanja Informacij (SUVI) ter Sistem Upravljanja Neprekinjenega Poslovanja (SUNP). »Izvajamo periodične varnostne preglede informacijskega sistema s strani priznanih zunanjih izvajalcev ter skrbimo za usposabljanje kadrov za obvladovanje informacijske varnosti,« razlagajo.

Zadnji investiciji, ki jih v družbi Plinovodi izvajajo na področju varovanja, sta širjenje sistema videonadzora na področju tehničnega varovanja in uvedba novih informacijsko varnostnih sistemov v procesnem delu informacijskega sistema.

Nova KBM uporablja model treh linij obrambe

Da nenehno nadgrajujejo in dodelujejo procese in orodja za zaznavanje varnostnih dogodkov in za odziv nanje, zagotavljajo tudi v Novi KBM. »V zadnjem času je v središču naše pozornosti sistem zagotavljanja neprekinjenega poslovanja, pri čemer se posvečamo tudi zagotavljanju neprekinjenosti storitev, ki jih za nas opravljajo zunanji izvajalci. Banka obvladuje tveganja v skladu z modelom treh linij obrambe,« so nam pojasnili v Novi KBM.

To pomeni, da so odgovornosti pri zagotavljanju varnosti razdeljene med lastnike posameznih procesov in storitev, strokovnjake, zaposlene na področju upravljanja tveganj ter notranjo revizijo.

V Novi KBM že več let opažajo trend povečanja tveganj na področju kibernetske varnosti, posledično povečujejo vire za izvajanje ukrepov na tem področju. »V zadnjem času je še posebno izpostavljeno in aktualno področje zagotavljanja odpornosti za primere različnih vrst nesreč in napadov,« pravijo. gg

V Novi KBM je v zadnjem času v središču pozornosti sistem zagotavljanja neprekinjenega poslovanja.

V Plinovodih imajo sistem tehničnega varovanja, v katerega so integrirani sistemi protipožarnega varovanja, protivlomnega varovanja, video-nadzorni sistem in sistem kontrole pristopa.

Zavarovalnice

Za boljšo varnost ves čas sledijo novim tehnologijam

Kako zavarovalnice v ponudbo vključujejo najsodobnejše tehnologije in kako stranke spodbujajo k njihovi uporabi? Kako dopolnjujejo ponudbo z novimi riziki, ki so posledica digitalizacije, podnebnih sprememb?

Darja Kocbek

V zadnjih letih opažamo več ekstremnih vremenskih pojavov. Ker spodbujamo varno in samozaščitno ravnanje, smo razvili aplikacijo Triglav Vreme.

Celo najbolj zahtevne procese, kot sta sklepanje življenjskih zavarovanj ali ogled škode, imajo sedaj stranke Zavarovalnice Sava možnost opraviti na daljavo.

Zavarovalnica Triglav

»V svoje poslovanje že več let vpeljujemo napredne tehnologije za optimizacijo poslovnih procesov, s čimer obenem spodbujamo transparentnost in enostavnost. Digitalno okolje nam tudi omogoča, da nenehno izboljšujemo naše storitve. Pri tem uporabljamo rešitve, ki smo jih v zadnjih letih vzpostavili v strateško-razvojnih procesih, predvsem uvajanje vsekanalnega prodajnega pristopa do strank in digitalne rešitve za oddaljeno in brezpapirno poslovanje, ki so v teh izrednih razmerah zaradi izbruha koronavirusa dobile dodaten zagon.

Sodobno tehnologijo vidimo tudi kot orodje, ki nam lahko pomaga pri ozaveščanju strank in širše javnosti o pomenu preventivnega ravnanja ter varnosti. Z namenom spodbude varne vožnje smo tako javnosti pred leti predstavili mobilno aplikacijo Drajv. Zavedamo se, da digitalizacija in tehnološki razvoj poleg številnih prednosti prinašata tudi nekatere nevarnosti, tako za posameznike kot tudi za podjetja. Zato smo pred časom razvili zaščito pred kibernetskimi tveganji. Ta je posameznikom na voljo v sklopu paketnega zavarovanja osebne zaščite.

Zaradi vse večjega obsega digitalizacije (delovnih) procesov in regulativ na področju varstva osebnih podatkov je kibernetska varnost vse pomembnejša tudi za podjetja. Spletni goljufi iščejo vse bolj usmerjene in prefinjene načine, da vstopijo v digitalna okolja. Pri tem so ranljiva predvsem majhna in srednja podjetja, saj imajo na voljo manj virov in namenjajo manj sredstev za kibernetsko varnost. Zato v Zavarovalnici Triglav zavarovanja kibernetske zaščite nudimo tudi podjetjem.

V zadnjih letih opažamo več ekstremnih vremenskih pojavov. Ker spodbujamo varno in samozaščitno ravnanje, smo razvili aplikacijo Triglav Vreme. V njej lahko uporabnik aktivira potisna sporočila, ki opozarjajo na različne vremenske dogodke, med drugim tudi na nevarnost toče. Vse meteorološke podatke in opozorila na nevarnosti aplikacija pridobiva od Agencije RS za okolje (ARSO).«

Zavarovalnica Sava

»V zadnjem letu nam je uspelo celoten proces poslovanja in vse točke stika z zavarovanci organizirati tako, da lahko nemoteno potekajo na daljavo. Celo najbolj zahtevne procese, kot sta sklepanje življenjskih zavarovanj ali ogled škode, imajo sedaj stranke možnost opraviti na daljavo. Z uporabo novih tehnologij tako omogočamo podpis na daljavo, video identifikacijo na daljavo in ogled škode na daljavo. V praksi to pomeni, da je mogoče novo zavarovalno polico skleniti in uveljavljati svoje pravice brez fizičnega stika z agentom.

Zavedamo se, da je fizičen stik za določene stranke še vedno ključen, zato ohranjamo tudi to pot, a hkrati ugotavljamo, da smo Slovenci vse bolj pripravljeni na novosti, ki jih omogoča poslovanje na daljavo. Zelo pomembno se nam zdi, da strankam – preden se prvič srečajo z našimi storitvami na daljavo – podrobno razložimo celoten proces, bodisi z opisom in video predstavitvijo na spletni strani, z navodili

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

naših agentov ali podporo v klicnem centru.

Nova tehnologija omogoča preventivo tako na področju varovanja zdravja kot premoženja. V Zavarovalnici Sava na primer uporabljamo telemetrijo, ki zavarovancem omogoča popoln nadzor. Motoristično zavarovanje Vigo, ki je kombinacija tehnologije in zavarovanja, omogoča SOS klic – v primeru nesreče samodejno pokliče pomoč ter lahko pomaga pri preprečitvi kraje motorja. Dodana vrednost za zavarovance je tudi možnost, da lahko spremljajo svojo vožnjo, imajo na voljo oceno svojih voženj, lahko iščejo navdih za poti in postanejo del virtualne Vigo skupnosti.

Vsekakor pa tehnologija posega tudi na področje zdravja in osebnih zavarovanj. V luči trenutnih razmer, ko je težko priti do zdravnika, našim zavarovancem dodatnega zdravstvenega zavarovanje Zdravje omogočamo video posvet s specialistom. S porastom in dostopnostjo novih tehnologij, ki so predvsem pri mlajši generaciji v nenehni rabi, razvijamo nova kritja in zavarovanja, ki bodo odgovarjala potrebam in zahtevam mlajših generacij.«

Zavarovalnica Generali

»V zavarovalnici Generali sta preventiva in izboljšanje varovanja oseb ter premoženja zelo pomembna tako z vidika preprečevanja nesreč kot z vidika izboljševanja izkušnje zavarovancev na vseh stičnih točkah z zavarovalnico. Strankam svetujemo, jih spodbujamo in nagrajujemo za uporabo sodobnih tehnologij, ki prispevajo k večji varnosti. Spodbujamo jih na primer, da se odločajo za vgradnjo naprav GPS za sledenje v primeru kraje, alarmov v domovih, uporabo protivlomnih vrat, sodobnih sefov in uporabo varnih gradbenih materialov ter elementov.

Strankam že dolgo nudimo izkušnjo elektronskega podpisa, od začetka letošnjega leta ponujamo tudi možnost oddaljenega podpisa ter videoidentifikacije stranke, kar v razmerah COVID-19 omogoča varno sklenitev zavarovanje na daljavo z Generalijevim zavarovalnim zastopnikom. Pri uporabi tovrstnih rešitev beležimo visoko rast.

Na zavarovalniškem trgu smo prvi vzpostavili neposredno sklepanje avtomobilskih zavarovanj prek spleta. Pri tem smo razvili blagovni znamki WIZ in G24. V okviru spletnega poslovanja ponujamo precej vrst zavarovanj. Poleg tega strankam nudimo uporabo mobilnih aplikacij in portalov, kjer dobijo informacije o zavarovanjih, plačilih, reševanju škodnih dogodkov ... Smo tudi v koraku z novostmi na področju zdravstvenih zavarovanj (nudimo na primer telefonske in video posvete z zdravniki specialisti, psihologi, fizioterapevti …).

Digitalni razvoj, v katerega veliko vlagamo, je eden glavnih stebrov strategije Generalija. Ena od glavnih usmeritev zavarovalnice je tudi razvoj asistenčnih storitev za stranke, pri čemer je poleg klasičnih storitev vedno bolj pomembno varovanje zdravja v okviru zdravstvenih storitev, razvijamo oziroma načrtujemo tudi »cyber« zavarovanje in »pametni dom« (smart home).« gg

Digitalni razvoj, v katerega veliko vlagamo, je eden glavnih stebrov strategije Generalija. Ena od glavnih usmeritev zavarovalnice je tudi razvoj asistenčnih storitev za stranke.

Uporabljajo opremo z večjo dodano vrednostjo

Rešitev Captis, ki je produkt družbe HSI, uporabniku olajša, pohitri in poceni upravljanje parkirišč in vhodov v podjetja, pri tem pa omogoča zelo natančno beleženje vstopov in izstopov. Uporablja se lahko kjer koli, kjer imamo opravka z vozili ali parkirišči.

HSI, ki deluje od leta 2005, je razvojno usmerjeno podjetje na področju varnosti in varnostnih sistemov, velik poudarek pa dajejo sodobnim tehnologijam. Zastopajo različne proizvajalce opreme varnostnih rešitev, namenjene tehničnemu varovanju objektov, hkrati pa razvijajo lastne rešitve. Te dodajo manjkajoče dele mozaika in tako strankam omogočijo, da so korak pred konkurenco, saj uporabljajo opremo in rešitve z večjo dodano vrednostjo. V HSI so osredotočeni na zastopanje tujih proizvajalcev v smislu trženja B2B, svetovanja in izvedbe integralnih varnostnih rešitev tako poslovnim kot zasebnim uporabnikom, razvijajo pa tudi lastne programske rešitve, ki se uporabljajo za namene varnosti in učinkovitosti varnostnih tveganj. Velik poudarek dajejo rešitvam za potrebe na objektih kritične infrastrukture.

Prilagodijo se naročnikom

Ena od rešitev, ki se lahko uporablja v logistiki, na parkiriščih, na cesti, na bencinskih servisih, skratka povsod tam, kjer imamo opravka z vozili ali parkirišči, je tudi Captis, ki jo v HSI tudi prilagodijo individualnim naročnikom. »Captis je rešitev, ki uporabniku olajša, pohitri in poceni upravljanje parkirišč in vhodov v podjetja, pri tem pa omogoča zelo natančno beleženje vstopov in izstopov. Lahko deluje samostojno brez potrebe prisotnosti osebe na vhodu. S pomočjo podpore različnim tehnologijam zaznave vozil se Captis lahko hkrati uporablja za potrebe ureditve parkirišč za zaposlene in goste ter tudi za potrebe podpore logistiki, ki z najavami vozil doseže večjo prepustnost na vhodih, manjše čakalne vrste, s tem pa nižje izpuste in obremenitev okolja,« povedo v HSI.

Velik poudarek varnosti delovanja

Za dosego cilja uporabljajo različne tehnologije kot npr. RFID (Radio-frequency identification) in LPR (License plate recognition), ki delujejo kot enoten sistem, v katerem lahko končni uporabnik s poljubnimi pravili prilagodi delovanje sistema na način, ki rešuje njegov izziv. Rešitev teče v spletnem brskalniku, kar omogoča enostavno uporabo tudi dobaviteljem in kupcem, ki lahko upravljajo najave preko ločene prijave. Captis lahko povežejo in integrirajo z obstoječimi ERP in logističnimi aplikacijami, ki jih uporablja podjetje, s čimer poenostavijo uporabo celotnega procesa. V okviru delovanja Captisa je zelo velik poudarek na varnosti delovanja rešitve in tudi na skladnosti z GDPR.

Pridobiva nove funkcionalnosti

»Rešitve na trgu navadno uporabljajo eno tehnologijo, na primer LPR ali pa RFID. Že kombinacija različnih tehnologij priča o fleksibilnosti Captisa,« prednosti naštejejo v HSI in dodajo, da so zelo fleksibilni pri iskanju rešitve in prilagajanju. Ravno prilagodljivost vidijo kot ključno konkurenčno prednost. »Klasične rešitve so na trgu v smislu out-of-the-box – imaš to, kar si kupil, nato pa iščeš vmesne rešitve za prilagoditev podjetja. Tak način je danes nesprejemljiv,« zatrdijo v HSI.

Dodajo, da Captis nenehno pridobiva nove funkcionalnosti. Kmalu bodo npr. integrirali možnost avtentikacije z mobilnim telefonom, kar pomeni, da bodo lahko uporabniki ob npr. izrednih dogodkih z ustreznimi pravicami neposredno in v realnem času vplivali na delovanje sistema. Druga funkcionalnost bo uporaba time-slot rezervacij za napovedovanje vozil. To se uporablja predvsem v logistiki za zmanjšanje vrst na vhodih in za tekoče delo na nakladalnih rampah.

Foto: Depositphotos

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Zasebno varovanje

Ključno je hitro prilagajanje novim razmeram

Če se po eni strani beleži povečano povpraševanje po varovanju v trgovinah in zdravstvenih ustanovah, pa potrebe drugod nihajo, v nekaterih primerih celo upadajo. Treba je sprejeti pogoje nove realnosti, v prihodnosti pa bodo sodobne tehnološke rešitve zmanjšale potrebe po fizični prisotnosti varnostnega osebja.

Darja Kocbek

Epidemija je pokazala, kako resno je treba razumeti ter sprejemati spreminjajoče se dejavnike v okolju.

Od podjetij, ki se ukvarjajo z zasebnim varovanjem, ob hitrih tehnoloških spremembah letos prilagoditve in razvoj zahteva tudi epidemija novega koronavirusa. »Epidemija nam je pokazala, kako resno je treba razumeti ter sprejemati spreminjajoče se dejavnike v okolju zasebnega varovanja ter načrtovanje človeških virov,« so nam pojasnili v podjetju Aktiva varovanje. V Sintalu poleg ažurnega seznanjanja z vladnimi ukrepi varnostnike usposabljajo tudi za opravljanje novih nalog, kot je na primer merjenje temperature.

Varnostnike usposabljajo tudi za opravljanje novih nalog, kot je na primer merjenje temperature.

V Aktivi varovanje se zavedajo pomena tehnoloških sprememb

Ker odgovornost do zagotavljanja varnostnih storitev naročnikom ob skrbnem načrtovanju izvedbe zahteva tudi upoštevanje nepredvidenih okoliščin, bo v prihodnje treba sprejeti pogoje nove realnosti, ki so posledica epidemije. Tako bo treba ustrezno zagotoviti pogoje za nemoteno izvajanje del, tudi s primernimi rezervami, pravijo v Aktivi varovanje.

Sicer pa eksponentna rast tehnologij nasploh terja spremljanje in prilagajanje novostim. »V naši družbi se zavedamo pomena tehnoloških sprememb in zanje nenehno iščemo ustrezne razvojne rešitve,« razlagajo.

Za varnostne sisteme je razvoj tehnologij ključen, saj ima velik vpliv za projektiranje sodobnih varnostnih rešitev. V Aktivi varovanje v prihodnosti pričakujejo bistveno povečanje tehničnih oblik varovanja, v katerih bodo sodobne tehnološke rešitve uporabnikom nudile nove dimenzije nadzora in s tem zmanjšanje potreb po fizični prisotnosti varnostnega osebja.

Za varnostne sisteme je razvoj tehnologij ključen, saj ima velik vpliv za projektiranje sodobnih varnostnih rešitev.

»Čeprav bo človek tudi v prihodnosti še vedno ključ za upravljanje sistemov tehničnega varovanja in prav tako še vedno pomemben del sistemov varovanja, je jasno, da bo prihodnost vse bolj pripadala

Foto: Depositphotos

V Aktivi varovanje v prihodnosti pričakujejo bistveno povečanje tehničnih oblik varovanja.

strojem in umetni inteligenci,« so nam razložili v Aktivi varovanje.

V Sintalu imajo lastni razvojni oddelek

Odkar smo priča epidemiji COVID-19, v Sintalu beležijo povečano povpraševanje po varovanju v trgovinah in zdravstvenih ustanovah. Potrebe nekaterih drugih naročnikov pa precej nihajo, saj je vlada z odlokom prepovedala opravljanje nekaterih dejavnosti v času epidemije, določene delovne obrate je treba zaradi karantene začasno zapreti, obseg poslovanja se je zmanjšal tudi zaradi upada naročil in podobno.

»Še naprej se bomo trudili hitro prilagajati omenjenim spremembam, kar seveda povzroča dodatne stroške, vendar nam hkrati zagotavlja, da obseg poslovanja ostaja v okvirih prejšnjega leta,« nam je pojasnila Sanda Zakrajšek, ki v Sintalu skrbi za marketing in odnose z javnostmi.

V Sintalu imajo lastni razvojni oddelek, ki neprestano uvaja tehnološke novosti. V času epidemije so med drugim naročnikom ponudili tehnološko napredno mobilno aplikacijo Sintal Alarm, s katero lahko na telefonu spremljajo stanje svojega alarmnega sistema.

»Letos smo razvili in dali v uporabo tudi digitalnega govornega robota, ki razbremenjuje delo zaposlenih v našem varnostno-nadzornem centru,« med novostmi izpostavlja Zakrajškova. Napredek gre v smeri digitalizacije in iskanja novih tehnoloških rešitev. V Sintalu velik del rešitev razvijejo sami, nekatere rešitve pa iščejo na trgu. V prihodnjih letih po njenih besedah v podjetju pričakujejo vse hitrejši

Po tridesetletnem razvoju sodobnega zasebnega varstva v Sloveniji lahko ugotovimo, da sta tako zasebno varovanje kot detektivska dejavnost po mednarodnih standardih dobro razvita, v članku Profesionalizacija zasebnega varstva v Sloveniji navajata dr. Miha Dvojmoč in dr. Andrej Sotlar s Fakultete za varnostne vede Univerze v Mariboru. Po podatkih Ministrstva za notranje zadeve RS se je leta 2018 z dejavnostjo zasebnega varovanja v Sloveniji ukvarjalo 145 podjetij. Največ licenc je bilo izdanih za varovanje ljudi in premoženja (95), za izvajanje sistemov tehničnega varovanja (94) in varovanje javnih zbiranj (75).

razvoj, »na katerega pa z lastnimi naprednimi tehnološkimi rešitvami v veliki meri vplivamo tudi mi«.

V Protectu skupina strokovnjakov spremlja razvoj

V družbi Protect priznani strokovnjaki s področja zasebno varnostnih storitev, licenčni projektanti elektronike, energetike, računalništva, informatike ter drugih eksaktnih znanj tvorijo skupino, ki spremlja razvoj tehničnih in drugih varnostnih elementov oziroma oblik.

Naložba v varovanje je dolgoročna naložba, pravijo v Varnosti Vič

»Danes je uporaba tehničnega varovanja skoraj nujno potrebna, če želimo zagotoviti večjo varnost in boljši pregled nad dogodki. Naložba v varovanje je dolgoročna naložba,« navajajo v podjetju Varnost Vič, ki izhaja iz bivše DO Varnost, torej iz organizacije z dolgoletnimi izkušnjami na področju fizičnega in tehničnega varovanja.

V GVS opozarjajo, da varovanje doma ni več prestiž

Varovanje doma danes ni več prestiž, temveč nuja. Nobena tehnična in mehanska zaščita hiše ali stanovanja pa ne more stoodstotno preprečiti vloma. »Kadar nas obiščejo nepridipravi, je najbolje biti povezan z intervencijsko službo varnostnega podjetja, saj bo operater na teren nemudoma poslal intervencijsko ekipo z licenco, ki je usposobljena za prijetje kriminalcev,« razlagajo v podjetju GVS – Globalno varnostni servis. gg

V času epidemije je Sintal naročnikom ponudil tehnološko napredno mobilno aplikacijo Sintal Alarm.

Foto: Depositphotos

Novim nevarnostim in grožnjam se prilagaja tudi zagotavljanje varnosti v bančnih institucijah.

Bančništvo

Banke: Največja težava ostajajo spletne in kartične prevare

Trendi na področju varovanja, ki so jih ali jih uvajajo banke, so največkrat usmerjeni v prepoznavanje obnašanja strank z namenom prepoznave anomalij, ki lahko nakazujejo na poskus prevare.

Andreja Šalamun

Razvoj novih metod zagotavljanja varnosti je usmerjen predvsem v ažurno prepoznavanje sumljivih primerov in v izpopolnjevanje večfaktorske prepoznave.

Globalizirani in digitalizirani svet prinaša nove nevarnosti in grožnje, zato se tem trendom prilagaja tudi zagotavljanje varnosti v bančnih institucijah. Iz fizične se seli tudi v druge sfere. Kot pravijo v NLB, so letos znova v ospredju kibernetske goljufije, ki so se s pandemijo koronavirusa še pomnožile. To ugotavlja tudi SICert, ki tako kot posamezne banke veliko pozornost namenja programu ozaveščanja prebivalstva o varnosti na internetu, ozaveščanju o različnih spletnih goljufijah oz. najpogostejših prevarah.

Kot pravijo v banki Intesa Sanpaolo, so trendi na področju varovanja, ki so jih ali jih uvajajo banke, največkrat usmerjeni v prepoznavanje obnašanja strank z namenom prepoznave anomalij, ki lahko nakazujejo na poskus prevare. »Pri tem je treba izpostaviti, da smo banke zelo omejene zaradi zakonodaje, ki pokriva področje varstva osebnih podatkov in njihove avtomatske obdelave,« izpostavijo.

Najšibkejši člen smo ljudje

V Novi KBM že več let opažajo trend povečanja tveganj na področju kibernetske varnosti, v Gorenjski banki pa ob tem poudarjajo, da poskusi zlorab z leti postajajo vse bolj prefinjeni, hkrati pa opozarjajo, da smo najšibkejši člen v tej zgodbi ljudje in da je nujno izobraževanje. Predvidevajo, da bo razvoj novih metod zagotavljanja varnosti usmerjen predvsem v ažurno prepoznavanje sumljivih primerov in v izpopolnjevanje večfaktorske prepoznave.

Žrtve prevar tudi podjetja

V bankah priznavajo, da so v zadnjem času zaznali kar nekaj poskusov zlorab, ne razkrivajo pa točne številke. »Imeli smo nekaj dogodkov s področja fizične varnosti (ropi, tatvine), ki so razmeroma dobro preiskani. V elektronskem bančništvu smo zaznali neuspešne poskuse zavajanja komitentov z lažnimi sporočili in ponarejenimi spletnimi stranmi banke (phishing), žrtev različnih prevar pa je bilo tudi več podjetij

Tiskano na papirju Vyprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

(direktorska prevara, vrivanje v poslovno komunikacijo),« pravijo v Novi KBM. Poudarjajo, da njihovi ukrepi za zamejitev zlorab poleg tehničnih rešitev zajemajo tudi ozaveščanje zaposlenih in strank.

»Hkrati s povečevanjem varnostih tveganj se zaostrujejo tudi zahteve regulatorjev, banke pa so v procesu digitalizacije in prestrukturiranja. Vse te spremembe zahtevajo intenzivno vključenost strokovnjakov za varnost, kar je, glede na omejeno število kadrov, težko zagotoviti,« priznavajo v Novi KBM.

Kar nekaj primerov poskusov zlorab so lani zaznali tudi v Gorenjski banki, povezani pa so bili z direktorskimi prevarami, lažnimi spremembami računov podjetij, lažnimi spletnimi stranmi za prodajo različnih izdelkov in goljufivimi obljubami pri nakazilih sredstev v lažne sklade. »Proti takšnim primerom se borimo s preventivnim preverjanjem sumljivih transakcij in ozaveščanjem strank in zaposlenih,« poudarijo.

Rast prevar pri spletnih nakupih

V NLB pravijo, da v primeru zagotavljanja varnosti spletnih storitev implementirajo ukrepe, kot jih predpisuje regulativa, pri tem pa skrbijo tudi za ozaveščanje uporabnikov o pomembnosti varnega poslovanja. Pravijo, da so lani zaznali rast prevar pri spletnih nakupih, pri čemer so posamezniki »nasedli« navidezno ugodni ponudbi prodajalca. Opozarjajo tudi na pomen izobraževanja zaposlenih. Neprevidnost pri prejemanju elektronske pošte in odpiranju različnih priponk ter povezav ima lahko negativne posledice, opozarjajo v NLB.

Uporabniki premalo poučeni o varni rabi spleta

V banki Intesa Sanpaolo navajajo, da stalno spremljajo zlorabe na vseh področjih in da imajo v ta namen vzpostavljene sisteme nadzora. »Iz teh izhaja, da so še vedno največja težava spletne in kartične prevare,« pravijo. Tudi oni ugotavljajo, da so uporabniki premalo poučeni o varni rabi spleta. Pravijo, da so pozorni na vse elemente varovanja, ker so ti soodvisni, njihov cilj pa je zagotavljanje takšne ravni varnosti, kot je potrebna za zaščito podatkov in premoženja strank ter zdravja zaposlenih. Zaradi širjenja okužb v zadnjem času banka namreč veliko pozornosti namenja tudi varovanju zdravja zaposlenih in s tem zagotavljanja kontinuitete nemotenega delovanja.

Pokriti želijo vsa tveganja in izboljšati sisteme

Fizična varnost predstavlja samo delček pri zagotavljanju varovanja zaposlenih, strank in podatkov, ki jih banka hrani. V banki Intesa Sanpaolo velik del tega izvajajo v sklopu informacijske varnosti, v katero je vključenih več orodij in služb, ki skrbijo vsaka za svoje področje varovanja, nadzora, analize in poročanja z namenom, da pokrijejo vsa tveganja in iščejo izboljšave v sistemih, ki jih uporabljajo.

Z informacijsko varnostjo se ukvarjajo strokovnjaki

V Novi KBM obvladujejo tveganja v skladu z modelom treh linij obrambe. To pomeni, da so odgovornosti razdeljene med lastnike posameznih procesov in storitev, strokovnjake, zaposlene na področju upravljanja tveganj ter notranjo revizijo. V dveh organizacijskih enotah banke je zaposlenih več strokovnjakov, ki se primarno ukvarjajo s področjem informacijske varnosti. Pravijo, da je v zadnjem času v središču njihove pozornosti sistem zagotavljanja neprekinjenega poslovanja, pri čemer se posvečajo tudi zagotavljanju neprekinjenosti storitev, ki jih zanje opravljajo zunanji izvajalci.

Upoštevajo priporočila Evropskega parlamenta

Medtem pa v Gorenjski banki v zadnjem času največ pozornosti posvečajo uvajanju priporočil Evropskega parlamenta na področju uporabe in dostopa do sodobnih plačilnih poti. »Slednja so bila, poleg zasledovanja strateške usmeritve vpeljave digitalizacije v procese in rešitve, ena izmed pomembnih vzvodov za vpeljavo novega postopka prijave v spletno banko Link,« poudarijo. Dodajo, da s pomočjo neodvisnih družb, ki zanje izvajajo preizkuse ranljivosti spletnih aplikacij in vitalnih komponent omrežij banke, redno preverjajo varnost vseh sistemov, ki so vezani na splet. Hkrati si, kot tudi nekatere druge banke, redno izmenjujejo informacije s SI-CERT-om, nacionalnim odzivnim centrom za kibernetsko varnost, in se medsebojno obveščajo o morebitnih sumljivih praksah. gg

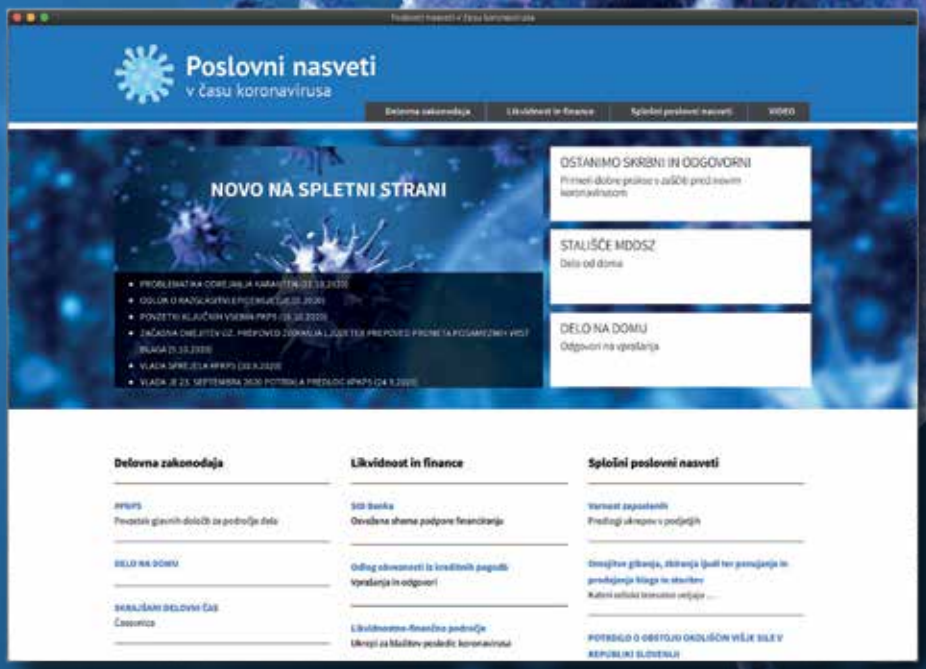
Več podjetij je bilo žrtev različnih prevar, vključno z direktorsko prevaro, vrivanjem v poslovno komunikacijo ipd., pravijo v Novi KBM.

V NLB so lani zaznali rast prevar pri spletnih nakupih, pri čemer so posamezniki »nasedli« navidezno ugodni ponudbi prodajalca.

V banki Intesa Sanpaolo ugotavljajo, da so uporabniki premalo poučeni o varni rabi spleta.

Foto: Depositphotos

Poslovni nasveti
v času koronavirusa



**Bodite na tekočem o ukrepih na področju delovne zakonodaje, financ in likvidnosti.
Oglejte si aktualne poslovne informacije, koristne napotke glede preventive ...**

www.gzs.si/koronavirus

Naročite se na poslovni tednik
in prejemajte ažurne informacije v svoj e-poštni nabiralnik

Poslovni tednik

https://www.gzs.si/pt

Foto: Depositphotos

Preventivno testiranje vseh zaposlenih je bilo ključno za zaustavitev okužb v podjetju.

Promocija zdravja na delovnem mestu

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Varnost pri delu

Delodajalec mora zaposlene ščititi in spodbujati k zdravemu načinu življenja

Širjenje virusa SARS-CoV-2 občutno vpliva na zagotavljanje varnosti in zdravja pri delu. Delodajalci so zdaj, še bolj kot v preteklosti, pod drobnogledom, od njih pa se pričakuje dosledno upoštevanje vseh priporočil za omejevanje širjenja omenjenega virusa.

Andreja Šalamun

V javnosti še vedno odmeva primer družbe Pivka perutninarstvo, ki se je septembra soočila s prvo množično okužbo z virusom SARS-CoV-2, ki se je širila znotraj podjetja. S hitro reakcijo, poostritvijo ukrepov in napotitvijo zaposlenih in poslovnih partnerjev na testiranje jim je širjenje virusa uspelo hitro zamejiti. Kljub vsemu pa je ta, vsaj za nekaj časa, precej otežil njihovo poslovanje.

»Od prve okužbe do zajezitve je preteklo le dober teden,« pravi Janez Rebec, predsednik uprave Pivka in direktor družbe Delamaris. Pojasni, da so že prej imeli ustanovljen krizni tim, ki se je nemudoma sestal, obvestili so Civilno zaščito, občino Pivka in koprsko območno enoto Nacionalnega inštituta za javno zdravje (NIJZ) ter lokalno enoto za medicino dela. »Sami smo predlagali prva testiranja, ki so se izkazala za upravičena. Na osnovi posvetovanja z NIJZ in direktorjem Milanom Krekom ter z namenom, da bi pridobili presek stanja in ugotovili morebitne žariščne cone ter ustavili val okužb, smo za dokončno zajezitev izvedli tudi preventivno testiranje vseh zaposlenih na lokaciji Kal, kar je bilo ključno za zaustavitev okužb v podjetju,« pove Rebec.

Vodili so evidence oseb v karanteni, uvedli merjenje temperature pred prihodom na delu in ob odhodu z dela ter tudi dnevno spremljanje bolezenskih znakov vsakega od zaposlenih.

Še dodatno zaostrili ukrepe

Kot pove Janez Rebec, so ukrepe, ki so jih že prej uvedli, še dodatno zaostrili. Poleg obvezne maske, varnostne razdalje, razkuževanja, omejitve sestankov in srečevanj med enotami ter spremenjenega urnika malic (po oddelkih), varnostne razdalje med posamezniki tudi v času malice in drugih rednih preventivnih ukrepov so prepovedali še zadrževanje v skupnih prostorih in organizirali delo od doma, kjer je to mogoče. Vodili so evidence oseb v karanteni, uvedli merjenje temperature pred prihodom na delu in ob odhodu z dela ter tudi dnevno spremljanje bolezenskih znakov vsakega od zaposlenih.

»V trenutku, ko je bilo v podjetju 46 odsotnih, smo organizirali testiranje vseh zaposlenih na lokaciji Kal. Takrat smo ugotovili, da ima še 32 oseb virus, čeprav

»Zdaj poslovanje poteka po ustaljenih tirnicah, seveda pa bo ostalo zavedanje, kako realna je grožnja virusa, ki lahko udari kogarkoli in kadarkoli,« opozarja Rebec.

večina ni imela nobenih simptomov. Zaradi okužbe ali preventivne izolacije oz. karantene je bilo v tistem času odsotnih sto zaposlenih. Po testiranju (18. 9.), ki smo ga izvedli na priporočilo NIJZ ter v sodelovanju s Civilno zaščito, so se okužbe zaustavile,« pove sogovornik in doda, da so se delavci po 14 dneh postopoma vračali na delovna mesta. »Zdaj poslovanje poteka po ustaljenih tirnicah, seveda pa bo ostalo zavedanje, kako realna je grožnja virusa, ki lahko udari kogarkoli in kadarkoli,« opozarja Rebec.

Poleg tega, da so želeli čim prej zaustaviti širjenje virusa, so skušali zagotoviti tudi nemoteno delo.

V proizvodnjo tudi delavci iz režije

Kako pa je veliko število pozitivnih testov in posledično odrejenih karanten vplivalo na delo podjetja? Poleg tega, da so želeli čim prej zaustaviti širjenje virusa, so skušali zagotoviti tudi nemoteno delo. V podjetju Pivka perutninarstvo je treba namreč zaradi načina proizvodnje (načrtovana reja, zagotavljanje dnevno svežega mesa) zagotavljati neprekinjen potek proizvodnje, v posameznih dneh pa je bilo odsotnih tudi 100 delavcev. »V času, ko je bila v proizvodnji odsotnost delavcev največja, so te nadomestili delavci iz drugih oddelkov in režije,« pove Rebec, ki je ponosen na to, da jim je uspelo izpolniti skoraj vsa naročila in obveznosti do kupcev. Ker so javnost seznanili, da izdelki ne predstavljajo tveganja za potrošnika – to sta potrdila tudi NIJZ in Evropska agencija za varno hrano (EFSA) –, povpraševanje ni upadlo.

Ker so javnost seznanili, da izdelki ne predstavljajo tveganja za potrošnika – to sta potrdila tudi NIJZ in Evropska agencija za varno hrano (EFSA) –, povpraševanje ni upadlo.

Ključno je bilo testiranje

Kot pravi Rebec, varnost, kakovost in sledljivost procesov v podjetju zagotavljajo že več kot 60 let. »Obvezni ukrepi so zagotavljanje ločenih poti gibanja, dnevno razkuževanje prostorov, umivanje in razkuževanje rok. Maske je treba nositi tudi na hodnikih, umivanje in razkuževanje rok je še pogostejše,« našteje in doda, da bodo to vzdrževali tudi v prihodnosti. Prav tako zaposlenim še naprej merijo temperaturo in vodijo evidence bolezenskih znakov vseh zaposlenih. »Pri tem se posvetujemo s strokovnjaki, NIJZ, Civilno zaščito in medicino dela,« pove Rebec.

Poudari, da je bilo v njihovem podjetju za zajezitev širjenja virusa ključno testiranje vseh zaposlenih. S tem so odkrili, da so bile mnoge osebe, ki so imele virus, povsem brez simptomov bolezni in jih na drugačen način ne bi mogli odkriti.

Podjetja torej v času širjenja koronavirusa vse več pozornosti posvečajo zagotavljanju varnosti in zdravja svojih zaposlenih.

Pripravili smernice za promocijo zdravja na delovnem mestu

Podjetja torej v času širjenja virusa SARS-CoV-2 vse več pozornosti posvečajo zagotavljanju varnosti in zdravja svojih zaposlenih. Zakon o varnosti in zdravju pri delu, ki določa pravne temelje za ureditev tega področja, pravi, da mora namreč delodajalec ne le poskrbeti za varnost na delovnem mestu, ampak tudi načrtovati in izvajati promocijo zdravja na delovnem mestu za svoje zaposlene, hkrati pa zagotoviti potrebna sredstva in način spremljanja izvajanja. Določene ukrepe in aktivnosti mora torej delodajalec izvajati zato, da bi ohranjal in krepil telesno in duševno zdravje delavcev. Delodajalec mora načrtovati promocijo zdravja na delovnem mestu tudi v izjavi o varnosti z oceno tveganja. Za pomoč pri uresničevanju te zahteve je Ministrstvo za zdravje RS izdelalo Smernice za promocijo zdravja na delovnem mestu, ki so javno dosegljive na spletu. V smernicah predlagajo delodajalcem, naj oblikujejo lasten načrt promocije, ki upošteva značilnosti podjetja, delovnega procesa in pričakovanj zaposlenih.

Z usklajenimi interesi do večjega uspeha

Podjetja se tega lotevajo na različne načine, saj so delovni procesi, ki v njih potekajo, zalo različni. Kot poudarjajo na Ministrstvu za zdravje, je pomembno, da delodajalec in zaposleni uskladijo interese, saj je tako končni uspeh zagotovo večji. Običajno podjetja zaposlene k zdravemu življenjskemu slogu spodbujajo na različne načine – spodbujajo jih na primer k aktivnemu prihodu na delovno mesto, da namesto dvigala uporabljajo stopnice, da čim več hodijo, kolesarijo ali se kako drugače gibajo. Mnoga podjetja organizirajo dnevno dostavo sadja in zelenjave za svoje zaposlene, organizirajo različne rekreativne prireditve, jih na delavnicah in izobraževanjih ozaveščajo o zdravi prehrani, pomenu fizične aktivnosti, zdravem načinu življenja, o tem, kako obvladovati stres ipd.

Kot poudarjajo na NIJZ, lahko na tak način zaposlenim omogočijo bolj kakovostno življenje in manj kroničnih nenalezljivih bolezni, ki se pojavljajo s staranjem in katere trenutno rastejo tako v Sloveniji kot drugod po svetu. Gre predvsem za kronične srčno-žilne bolezni, kronična dihalna obolenja, sladkorna bolezen tipa 2 ter bolezni kostno-mišičnega sistema. gg

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Koristi certifikata Excellent SME Slovenia

- mednarodno prepoznavna kredibilnost podjetja, ki jo potrjuje Gospodarska zbornica Slovenije,
- dnevno aktualna odličnost podjetja,
- lastno bonitetno poročilo za vaše stranke (v slovenskem, angleškem ali nemškem jeziku),
- QR koda Excellent SME za vaša tiskana gradiva, e-pošto ali kot stenski plakat
- 24-urno nadzorovanje delovanja spletne strani,
- dnevna poročila o poskusih kopiranja spletne strani,
- verificirana spletna stran (tudi za podjetja brez svoje spletne strani),
- uvrstitev na referenčno listo na spletni strani GZS excellent-sme.gzs.si

coface FOR TRADE

Gospodarska zbornica Slovenije

SAFE Signed

TEHNOLOGIJA, KI REŠUJE ŽIVLJENJA

SISTEMI ZA KRIZNO UPRAVLJANJE

NAVIGACIJA IN SLEDENJE

TAKTIČNE KOMUNIKACIJE

INTEROPERABILNOST

INTEGRACIJE SENZORJEV IN OROŽJA

PAMETNA SENZORSKA OMREŽJA

USPOSABLJANJE IN SIMULACIJE

MIL SISTEMIKA

NAREJENO V SLOVENIJI