Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2016, marec • št. 11



Podelitev nagrad »Slovenian Grand Security Award 2016«

Razvoj novih tehnologij postavlja pomembne izzive za varovanje zasebnosti

Mojca Prelesnik, Informacijska pooblaščenka

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

Prvim desetim strankam, ki se bodo javile na elektronski naslov: *info@novapanorama.si* ponujamo brezplačno uro varnostnega svetovanja na temo kako optimizirati investicije v varnostni sistem in tekoče stroške financiranja varnostnega sistema?

IZVIRNA MISEL

Profesionalni in celovit varnostni sistem v podjetju odločilno prispeva k povečanju pozitivnih poslovnih izidov ter k dvigu kulture, konkurenčnih prednosti in ugledu podjetja (M. Vršec).

PRAVA IZBIRA

Nova Panorama, d. o. o. je ob sodelovanju vrhunskih varnostnih strokovnjakov usposobljena izvajati varnostni inženiring, to je varnost od A do Ž oziroma t. i. "varnost na ključ". Gre za vzpostavljanje integralnih varnostnih sistemov na projektni način, z integracijo varovanja v sisteme vodenja kakovosti z uvajanjem varnostnih standardov ter z upoštevanjem dobre prakse. Konkretni projektni proizvod je izdelava in implementacija varnostnega elaborata.

Storitve in produkti Nova Panorama, d. o. o. naročniku oziroma uporabniku zagotavljajo uvedbo varnostno in ekonomsko upravičenega varnostnega sistema, ki vzpostavlja ustrezno preventivo, opozorilni sistem in proces obvladovanja ranljivosti, ogroženosti, sprememb, tveganj in izrednih dogodkov.

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

- Načini (oblike) svetovanja
- Posnetek in analiza stanja
- Intervjuji in vprašalniki
- Ocene ogroženosti
- Varnostni elaborati
- Pravilniki, načrti, navodila

Integralni varnostni sistemi (celovito varovanje)

- Varnostna funkcija
- Varnostna politika
- Varnostna strategija
- Pravna podlaga
- Organiziranost in status varovanja
- Področja varnosti
- Civilna zaščita
- Varnostni menedžment
- Varnostni režim
- Alarmni in odzivni sistem
- Strokovni nadzor
- Portfelj zavarovanj

Varovanje oseb in premoženja

- Varovanje ljudi premoženja
- Prevoz in varovanje denarja ter drugih vrednostnih pošiljk
- Varovanje javnih zbiranj

10 LET ODLIČNOSTI

- Izvajanje sistemov tehničnega varovanja

Kakovost in varnost

- Integracija varovanja v ISO 9000:2000
- Varnostni standardi
- Presojevalci kakovosti varovanja

Krizno vodenje (krizni menedžment)

- Objektivna potreba po načrtovanju kriznega vodenja
- Poslovanje na rezervni lokaciji

IZOBRAŽEVANJE

Varnostni menedžment

- Obvladovanje poslovnih in varnostnih tveganj ("risk management")
- Usposabljenje kriznega štaba
- Varnostna služba – usposobljenost varnostnikov za naloge varovanja podjetja
- Varnostna kultura in poslovna etika
- Usposabljanje za nadzornike
- Scenariji obvladovanja izrednih dogodkov



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
izr. prof. dr. Denis Čaleta

Trženje:
ICS-Ljubljana
info@ics-institut.si
Aljoša Kandžič
aljosa.kan@ics-institut.si

Oblikovanje in DTP:
ICS-Ljubljana

Tisk:
Schwarz print d.o.o.

Datum izida
marec 2016

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

Objavljeni prispevki in njihova vsebina odražajo mnenja in stališča avtorjev ter predstavljajo v celoti njihovo odgovornost.

Tradicionalna konferenca »Dnevi korporativne varnosti 2016« je tisti najpomembnejši dogodek na področju korporativne varnosti, ki s seboj vedno prinese odlično priložnost za izdajo posebne številke revije. Vsebina te številke je zelo tesno povezana s perečimi konferenčnimi temami in predstavitvijo dobrih praks različnih strokovnjakov in podjetij. Interdisciplinarnost področja korporativne varnosti se kaže tudi v vsebinskem obsegu revije. Tematike, ki jih predstavljamo so z različnih zornih kotov neposredno povezane s področjem korporativne varnosti oz. imajo na njo pomemben vpliv. Posebej velja poudariti pomen prenosa dobrih praks, ki širokemu krogu bralcev in strokovni javnosti pomaga iskati odgovore na probleme in izzive s katerimi se srečujejo v svojih poslovnih okoljih. Podjetja, ki v tokratni številki revije predstavljajo posamezne primere svojih rešitev, ne smemo ocenjevati samo z vidika promocije za njihove dobre prakse in tehnološke rešitve, temveč je potrebno razumeti to kvaliteto skozi prizmo resnega zavedanja pomena procesa korporativne varnosti in s tem tudi njegove podpore.

Posebej smo v pričujoči številki namenili prostor najboljšemu med enakimi in sicer korporativno varnostnemu managerju leta 2015 ter z njim opravili intervju, ki bo bralcem približal ozadnje dejavnikov, kateri so vplivali na doseg tega prestižnega priznanja. Naslednjo pomembno mesto pa je tokrat namenjeno Informacijskemu pooblaščencu Republike Slovenije, ki je eden izmed najbolj vidnih korporativnih članov Slovenskega združenja korporativne varnosti. Z Informacijsko pooblaščenko smo pripravili intervju ob 10. obletnici te pomembne institucije. Življenje v informacijski družbi logično pomeni, da je tematika s tega področja izredno aktualna. Zaradi navedenega v vsebinskem obsegu tokratne številke temu področju ponovno namenjamo pomembno mesto. V tem delu je potrebno prikazati dobro rešitev pri varnemu komuniciranju preko mobilne telefonije in seveda pred nevarnostmi, ki jih prinaša uporaba interneta in socialnih omrežij. Nikakor pa se nismo želeli izogniti tudi aktualnim izzivom, ki jih prinašajo trenutni dogodki v družbenem okolju. Poglobljeno odpiramo vsebine povezane z nevarnostmi, ki jih prinaša prekomerna normiranost določenih poročij. V trenutnem primeru je to nova tobačna zakonodaja in zadevo osvetljujemo tudi z varnostnega stališča. Seveda pa nismo mogli mimo varnosti na avtocestah, kjer smo bili pred kratkim ponovno priča tragični nesreči. Z zanimivim pogledom na situacijo lahko lažje razumemo kompleksnost zagotavljanja varnosti na avtocestah. Ostali zanimivi prispevki so vezani na aktualna področja video-nadzornih sistemov, arhiviranja in obvladovanja dokumentarnega ter arhivskega gradiva, odkrivanje prevar na zavarovalniškem področju in zelo zanimivega področja vezanega na varovanje kulturne dediščine z ustreznim sistemskim pristopom pri uporabi tehničnih sistemov varovanja. Sedma jubilejna konferenca Dnevi korporativne varnosti pa je tako pravi trenutek, da naredimo kratko analizo stanja na področju korporativne varnosti in njenega sistemskega razvoja.

V uredništvu revije smo prepričani, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji.

izr. prof. dr. Denis Čaleta
Glavni urednik



KOLUMNA
izr. prof. dr. Denis Čaleta, ICS-Ljubljana

SISTEMSKI PRISTOPI NA PODROČJU KORPORATIVNE VARNOSTI

9



INTELIGENTNI IP VIDEO NADZORNI SISTEM IN VARNA IT INFRASTRUKTURA

Video nadzorni sistemi so integralni del upravljanja varnostnih tveganj, ki so v današnjem času zelo intenzivna in se tudi zelo dinamično spreminjajo. Zato je potrebno temu delu pri obvladovanju tveganj posvetiti večjo pozornost, predvsem pri načrtovanju in izbiri sistema, ki ga nameravamo uporabiti.

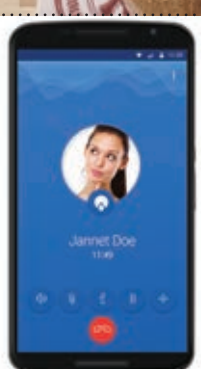
18



NEUSKLAJEN PRISTOP K TVEGANJEM POMENI SPREJEM GOTOVEGA PORAZA

Sodobno varnostno okolje je, za razliko od preteklosti, ko so bile osnovne grožnje posameznim državam povezane predvsem z vojnami, postalo bistveno bolj zapleteno. Spekter groženj in tveganj se je razširil na vse segmente družbe in procesov, ki potekajo v njej. Prav tako so tudi posledice groženj in tveganj razpršene po celotni družbi in vplivajo na vse področja od nacionalne varnosti, gospodarstva, zdravstva, informacijskih omrežij in drugo.

22



NAIVNOST PRI UPORABI SPLETNIH KOMUNIKACIJSKIH PROGRAMOV

Ko je govora o varnosti, je najpogostejša prva misel fizično varovanje, v primeru informacijskih tehnologij pa antivirusni programi, požarni zidovi, najrazličnejši sistemi za zaznavanje vdorov in tako naprej. Seveda je za zaščito podjetja zgoraj omenjen pristop pravilen in v skladu z dobrimi praksami. Kljub temu pa v podjetjih še vedno obstajajo varnostne vrzeli.

36



SOCIALNA OMREŽJA KOT VIR PRIDOBIVANJA PODATKOV

Število uporabnikov socialnih omrežji vse bolj narašča. Njihova uporabnost se je od fizičnih oseb razširila tudi na podjetja, organizacije in druge ustanove. Tako tudi socialna omrežja vse bolj postajajo odličen vir različnih podatkov in s tem tudi tarča kibernetskih kriminalcev.

43

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
mag. Boris Kankaraš, korporativno varnostni manager
Vodja Pristaniške varnosti Luke Koper d.d.

KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE NEPREKINJENOSTI DELOVANJA ORGANIZACIJE

V današnjem poslovnem svetu korporativna varnost predstavlja enega izmed bistvenih procesov za zagotavljanje neprekinjenosti delovanja. V primeru kritične infrastrukture, med katere vsekakor umeščamo tudi Luko Koper d.d., je to še posebej pomembno.

Svoje delo izvajate kot korporativno varnostni manager oz. vodja Področja pristaniške varnosti Luke Koper d.d.. Nam lahko poveste katera so ključna področja vaših pristojnosti?

Področje pristaniške varnosti je danes organizirano tako, da ima v svoji organizacijski strukturi zaposlene varnostne managerje in varnostno osebje, poklicne gasilce in strokovne delavce, ki smo pristojni za fizično in tehnično varovanje Luke Koper d.d., njeno požarno in okoljsko varnost, civilno obrambo v širšem smislu besede (obrambno načrtovanje, kritično infrastrukturo, krizno odzivanje...) ter varovanje tajnih podatkov in poslovnih skrivnosti.

Luka Koper predstavlja del vitalne kritične infrastrukture nacionalnega in mednarodnega pomena. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Koprsko pristanišče je »vmesnik« med morskimi in kopenskimi transportnimi potmi globalne logistične verige. Velikost pristanišča (morje in kopno), veliko število notranjih in zunanjih deležnikov, izredno visoka dinamika izvajanja dejavnosti ter vplivi različnih dejavnikov na osnovno dejavnost pristanišča so pomembnejši faktorji, ki jih je potrebno upoštevati in spremljati, pri zagotavljanju varnosti ljudi in infrastrukture. Takšno okolje zahteva veliko usklajevanja in koordinacije z vsemi deležniki, ki sodelujejo v procesu in nenehno prilagajanje in revidiranje načrtov odzivanja, ki jih ima Luka Koper d.d. izdelane ter seveda ustrezno usposabljanje, izobraževanje in vaje tistih, ki so v te aktivnosti vključeni.

g. Boris Kankaraš je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2015«

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

*avtor je član Slovenskega združenja korporativne varnosti



Če na vprašanje odgovorim s pozitivnim predznakom ugotavljam, da imamo v Sloveniji kar nekaj podjetij v katerih je vodstvo prepoznalo pomen in vlogo korporativne varnosti. Vprašanje, ki se mi ob tem poraja pa je ali so ti strateški managerji implementirali korporativno varnost zato, ker je del korporativnega upravljanja ali zato, ker se zavedajo kompleksnosti varnostnih tveganj?

Kako so po vašem mnenju pomembne ključne informacije korporacije v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču. Ali temu področju v Luki Koper namenjate veliko pozornost?

Nedvomno so informacije s tega vidika ključne, sploh če so točne in pravočasne. Luka Koper d.d. je v okviru svoje organizacijske strukture na tem področju aktivna, še vedno pa obstajajo določene rezerve.

Kako pristopate k preprečevanju terorističnih tveganj, katerim ste v vaši dejavnosti zelo izpostavljeni?

Koprsko pristanišče je »vmesnik« med morskimi in kopenskimi transportnimi potmi globalne logistične verige. Velikost pristanišča (morje in kopno), veliko število notranjih in zunanjih deležnikov, izredno visoka dinamika izvajanja dejavnosti ter vplivi različnih dejavnikov na osnovno dejavnost pristanišča so pomembnejši faktorji, ki jih je potrebno upoštevati in spremljati, pri zagotavljanju varnosti ljudi in infrastrukture.

Ob dejstvu, da je pristanišče zanimiva tarča, temu tveganju posvečamo veliko pozornosti. Izvajamo vse aktivnosti, ki so na razpolago v okviru slovenskega pravnega reda. Posebno pozornost posvečamo izmenjavi informacij med deležniki s pristojnostmi na področju varnosti, notranjimi deležniki, ki sodelujejo v izvajanju pristaniških dejavnosti ter seveda izvajamo aktivnosti odvračalno/preprečevalne narave, ki se izvajajo v okviru Področja pristaniške varnosti.

Kakšno je vaše sodelovanje z državnimi organi, ki so tudi posredno vpeti v zagotavljanje celovite varnosti v Luki Koper?

Odlično! Ob upoštevanju stanja v državnih organih, ki so pristojni za varnost pristanišča je sodelovanje odlično. Pri tem moram pripomniti, da določeno težavo predstavlja slaba harmonizacija predpisov, ki urejajo varnost in pristojnosti državnih organov pri zagotavljanju varnosti pristanišča.

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

Brez dvoma. Osebno menim, da je to ključna kvaliteta. Nenazadnje je nevednost in nepoznavanje tisto, kar zelo močno vpliva ne samo na varnostno kulturo ampak tudi na odnos do varnosti. Izredno velik vpliv ima tako na samo varnost podjetja in posledično na njegovo uspešnost.

V tem študijskem letu se je začel izvajati podiplomski magistrski program »management korporativne varnosti«, ki ga v soorganizaciji pripravljata Institut za korporativne varnostne študije – ICS in GEA College - Fakulteta za podjetništvo. Menite, da je to prava pot za uveljavljanje stroke in predvsem za izobraževanje strokovnjakov s področja korporativne varnosti v Republiki Sloveniji?

Brez dvoma bo izvajanje programa in pridobivanje novih strokovnjakov pomembno vplivalo na pogled na stroko. Menim pa, da to ne bo dovolj z vidika uveljavljanja stroke in odnosa do varnosti v Republiki Sloveniji. Glede na okolje v katerem živimo, spremembe tveganj in njihov vpliv v globalnem svetu, pa v Sloveniji živimo v iluziji, da smo varna država. Smo, če gledamo statistiko. Žal pa je kar nekaj sivih polj in žal samo do prvega večjega varnostnega incidenta (bodisi z vidika posledic ali narave incidenta).

> Kot član združenja vidim in verjamem v poslanstvo Slovenskega združenja korporativne varnosti, ki predstavlja in prinaša dodatno kvaliteto v slovenski prostor.

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

Vsekakor. Že prej sem dejal, da je uvedba podiplomskega magistrskega programa »management korporativne varnosti«, dodana vrednost k prepoznavanju in uveljavljanju stroke, da pa to ni dovolj. Kot član združenja vidim in verjamem v poslanstvo Slovenskega združenja korporativne varnosti, ki predstavlja in prinaša dodatno kvaliteto v slovenski prostor. Izmenjava znanj in izkušenj, nova spoznanja na področju korporativne varnosti, jasna, razumljiva in strokovna sporočila strokovni in širši javnosti so pomemben dejavnik uveljavljanju stroke...

Na letošnji otvoritvi mednarodnega dogodka Dnevi korporativne varnosti boste prejeli prestižno nagrado »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2015«, ki ga vsako leto podeljuje Slovensko združenje korporativne varnosti in Institut za korporativno varnostne študije-ICS. Kaj vam osebno pomeni ta laskavi naziv?

Najprej veliko čast in hkrati potrditev tega, da delam prav. A nagrado sprejemam hkrati kot obvezo in spodbudo za svoje nadaljnje delo. ■



Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah. **SKUPAJ SMO MOČNEJŠI!**

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

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih strokovnih srečanjih;
- popusti pri nakupu izdanih publikacij ICS - Ljubljana;
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS - Ljubljana;
- popusti pri članarinah za zaposlene, ki prihajajo iz vrst včlanjenih organizacij;
- brezplačna naročnina na revijo Korporativna varnost;
- popusti pri oglaševanjih in postavitev logotipa na spletno stran ICS - Ljubljana.

www.ics-institut.si

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



KOLUMNA
denis.caleta@ics-institut.si

SISTEMSKI PRISTOPI NA PODROČJU KORPORATIVNE VARNOSTI

Dinamično varnostno okolje vsak dan pred organizacije postavlja zahtevna tveganja in grožnje, ki jih je potrebno obvladovati, da lahko osnovni poslovni procesi nemoteno potekajo.

Grožnje kot so terorizem, migracije, informacijska tveganja in vdori v informacijske sisteme, ropi in ostala tveganja pri strateškem managementu podjetij počasi dvigujejo raven zavedanja o potrebnosti obvladovanja tveganj in zagotavljanju neprekinjenosti delovanja njihovih organizacij. Spoznanje, da tudi Slovenija ni imuna na ta tveganja se počasi krepi v širši družbeni skupnosti. Zavedanje o tem pe je še posebej izrazito v tistih podjetjih, ki poslujejo v mednarodnem okolju in so zato še dodatno izpostavljeni določenemu nizu tveganj pri poslovanju. Počasi, vendar vztrajno se pri slovenskih podjetjih povečujejo potrebe po profilu strokovnjaka korporativne varnosti. V mednarodnem okolju je ta potreba jasen standard, ki ga podjetja zasledujejo, če želijo biti v svojem delovanju uspešnejša. Z gotovostjo lahko ocenimo, da v Sloveniji v tej potrebi močno zaostajamo, tudi za nam primerljivimi državami v regiji. Zaradi odsotnosti vključevanja korporativno varnostne stroke pri zagotavljanju podpore glavnih poslovnih procesov je velik odstotek podjetij doživel škodne dogodke, ki so v nekaterih primerih pomenili tudi propad podjetja. Danes pa huda konkurenčna tekma na globalnem tržišču ne dopušča več delovanja po principu sreče, saj je samo vprašanje časa kdaj se podjetje znajde v situaciji, kjer je izpostavljeno posamezni ali celemu nizu groženj. Če v tem trenutku ni ustrezno delujočega sistema korporativne varnosti, ki skozi različne dejavnosti že v osnovi zagotavlja preprečevanje ranljivosti v organizaciji, potem je delovanje podjetja resno ogroženo.

Počasi, vendar vztrajno se pri slovenskih podjetjih povečujejo potrebe po profilu strokovnjaka korporativne varnosti. V mednarodnem okolju je ta potreba jasen standard, ki ga podjetja zasledujejo, če želijo biti v svojem delovanju uspešnejša.

Kljub temu, da se je strateški management počasi začel zavedati potrebe po uvajanju korporativne varnosti v procese delovanja podjetij, pa je problem v tem, da je to nemogoče izvesti v zelo kratkem časovnem obdobju. Korporativna varnost zaradi svoje interdisciplinarnosti vpliva praktično na vse ostale procese v organizaciji s katerimi se dopolnjuje ali je v razmerju soodvisnosti. Ravno ta kompleksnost pa onemogoča njeno implementacijo samo na podlagi trenutne odločitve vodstva.

Na to dejstvo vpliva več pomembnih dejavnikov, ki v implementaciji te zahteve igrajo ključno vlogo. Prva in najpomembnejša je vsekakor strateška odločitev vodstva podjetja, da se resno loti potrebe po celovitem obvladovanju varnostnih in drugih s tem povezanih tveganj. Ta odločitev za seboj potegne potrebo po zagotavljanju ustreznih virov, ki jih lahko opredelimo v okviru finančnih, kadrovskih in nenazadnje tehničnih virov. Če bi lahko ocenili, da je z ustrezno odločitvijo in namero strateških vodstev lažje zagotoviti finančne in tehnološke vire, je na področju kadrovskega potenciala to zelo zahtevna naloga, ki jo je zelo težko izvesti v kratkem obdobju. Razlogov

*avtor je član Slovenskega združenja korporativne varnosti



Korporativna varnost zaradi svoje interdisciplinarnosti vpliva praktično na vse ostale procese v organizaciji s katerimi se dopolnjuje ali je v razmerju soodvisnosti. Ravno ta kompleksnost pa onemogoča njeno implementacijo samo na podlagi trenutne odločitve vodstva.

za to je več. In sicer, kot najpomembnejšega lahko navedemo, da se je korporativna varnost kot profesija začela razvijati šele pred kratkim. To pomeni, da odsotnost tradicije, ustreznih oblik izobraževanja in do nedavnega zelo podcenjene vrednosti tega kadra, nekako ni predstavljalo ustreznega okolja za razvoj profesije korporativne varnosti. To je na področju kadrovske ponudbe in povpraševanja po kadru s področja korporativne varnosti pomenilo slabo kvaliteto in zelo omejen obseg kadrov. Kvalitetni kadri so svoje profesionalno okolje nadgrajevali v mednarodnem okolju, kjer so slovenski strokovnjaki izredno cenjeni. Strokovnjaki, ki pa so delovali v slovenskem okolju so bili v zelo omejenem številu razpršeni v tistih redkih podjetjih, kjer je strateško vodstvo pravilno razumelo spremembe v kompleksnem in dinamičnem poslovnem okolju in nujno potrebo za delovanje korporativne varnosti v njihovih organizacijskih sredinah. V ostalih organizacijah pa so se v večini primerov nahajali nekompetentni strokovnjaki, ki so bili nesposobni in ne dovolj prodorni, da bi proces korporativne varnosti pravilno pozicionirali v njihovih organizacijah. To se je seveda odražalo tako, da se je korporativna varnost v organizacijskem smislu pojavljala na petem ali šestem nivoju odločanja v organizaciji, z nikakršnim vplivom in ugledom, kar je imelo za posledico tudi izredno slabo finančno vrednost teh delovnih mest. Vsa ta dejstva nam kažejo realno sliko in odgovor, zakaj danes na kadrovskem tržišču, kljub pripravljenosti strateških vodstev, da za zaposlitev kadra korporativne varnosti namenijo ustrezne finančne vire, le teh ni možno najti. Profesija se namreč izgradi šele skozi utrezen sistem izobraževanja, ki ga v zadnjem obdobju predstavlja magistrski program »Management korporativne varnosti« in seveda vse strokovne oblike usposabljanj in izobraževanj, ki se izvajajo v okviru Instituta za korporativne varnostne študije, ICS--Ljubljana. Poleg navedenega pa je seveda nujna potreba po močnem stanovskem združenju, ki se je v zadnjih petih letih razvilo v okviru Slovenskega združenja korporativne varnosti. To so tisti nujni okviri, ki so pomembni, da se bo profesija korporativne varnosti krepila v širšem družbenem okolju in da bo ta njena moč izhajala ravno iz ustreznih kompetenčnih kadrov, ki bodo sposobni s svojimi interdisciplinarnimi znanji ustrezno odgovarjati na vse oblike tveganj in groženj katerim so izpostavljena slovenska podjetja. Pozitiven proces, ki ga lahko zaznamo je tudi prehod določenih izkušenih strateških strokovnjakov s področij nacionalne varnosti, tehničnih

Profesija se namreč izgradi šele skozi utrezen sistem izobraževanja, ki ga v zadnjem obdobju predstavlja magistrski program »Management korporativne varnosti« in seveda vse strokovne oblike usposabljanj in izobraževanj, ki se izvajajo v okviru Instituta za korporativne varnostne študije, ICS-Ljubljana. Poleg navedenega pa je seveda nujna potreba po močnem stanovskem združenju, ki se je v zadnjih petih letih razvilo v okviru Slovenskega združenja korporativne varnosti.

področij in seveda poslovnih področij, na področja korporativne varnosti. Ob predpogoju, da so ob prehodu na področje korporativne varnosti pripravljeni nadgraditi svoje znanje z nujnimi vsebinami korporativne varnosti in razumevanje poslovnega procesa, lahko to smatramo kot tisti nujen korak, ki bo to profesijo dolgoročno še krepil in ji dal ustrezne interdisciplinarne nastavke v smeri višje kvalitete.

Naslednji pomemben dejavnik pa je pomembno razumeti v potrebi postavitve ustreznega sistema za obvladovanje tveganj in zagotavljanja neprekinjenosti poslovanja znotraj poslovnih organizacij. Nemogoče je namreč samo na podlagi odločitve vodstva izvesti in postaviti tak sistem korporativne varnosti znotraj podjetja. Prvič je izkušnje ali predvsem organizacijske rešitve nemogoče nekritično prekopirati in prenesti v določeno organizacijo. Vsaka organizacija ima določene svojstvene specifike, ki so odvisne od portfelja poslovnih dejavnosti, okolja v katerem deluje, stopnje organizacijske in varnostne kulture in še bi lahko naštevali. Zaradi navedenega je potrebno sistem korporativne varnosti v podjetjih postavljati postopoma in zelo premišljeno. Pomen teh procesov mora spoznati tudi srednji management in ga vzeti kot podporo pri lažjem obvladovanju tveganj na njihovi ravni poslovanja in seveda preko tega tudi bolj učinkovito in lažje zagotavljanje postavljenih ciljev na svojem nivoju organizacije. Seveda pa je ključen dejavnik pri postavljanju tega sistema in sodelovanja z vsemi ostalimi deležniki v podjetju, ravno visoko strokovno podkovan korporativno varnostni manager, ki bo s svojo strokovno avtoriteto in interdisciplinarnim znanjem utrjeval pomen korporativne varnosti in seveda nizal tudi rezultate na področju obvladovanja tveganj ter zagotavljanju uspešnosti organizacije. Zavedati se je namreč potrebno, da strateško vodstvo podjetja največkrat razume samo poslovno-finančni okvir ocenjevanja uspešnosti vsakega posameznega procesa. Zaradi tega je ključno, da direktor korporativne varnosti v podjetju zna delovanje procesa korporativne varnosti predstaviti tudi skozi poslovne vidike in prihranke ali uspehe poslovanja, ki so med drugim nastali zaradi učinkovitejšega preprečevanja določenih ogroženosti ali tveganj. Pri strateškem managementu mora priti do uveljavitve zavedanja, da je vložek v obvladovanje tveganj investicija v učinkovitejše delovanje podjetja in ne strošek.

Vsa navedena dejstva strateški management postavljajo v situacijo v kateri je potrebno razumeti razmerja in stanje na področju korporativne varnosti. To pomeni, da morajo biti pri angažiranju ustreznih strokovnjakov s področja korporativne varnosti potrpežljivi, smeli in seveda v določenem delu tudi pripravljeni tvegati z mlajšim kadrom, ki še nima vseh potrebnih izkušenj, ima pa neizmerno energijo za strokovno uveljavljanje. Seveda je v teh zadnjih primerih najboljše zagotavljanje razmerja starejših in izkušenih kadrov ter mlajših, na katere se v določenem časovnem obdobju prenaša nujno potrebne izkušenje. Seveda izkušnje največkrat pridejo ravno skozi neposredno lastno izvajanje aktivnosti. Pri izbiri kadra pa mora biti kljub upoštevanju in razumevanju vseh dejavnikov tudi kanček srečne izbire korporativno varnostnih kadrov. V organizacijah in posameznikih so določene specifike, ki se morajo dopolnjevati do te ravni, da lahko rečemo, da je posameznik res prava izbira za določeno organizacijo.

Vse napisano nam kaže na osnovno zahtevo, ki sem jo zapisal v naslovu te kolumne in sicer, da se lahko korporativne varnosti lotimo samo z ustreznimi sistemskimi koraki. Smo v Sloveniji pri tem uspešni? Odgovor je, ne še povsem. Se je pa v zadnjem obdobju stanje le začelo spreminjati v pozitivno smer, kar nas lahko navdaja z določeno stopnjo upanja in pričakovanja, da bomo v prihodnosti, tudi v Sloveniji, imeli na tem področju ustrezno uveljavljeno profesijo korporativne varnosti, ki bo poskrbela za sistemsko delovanje znotraj poslovnih in drugih organizacijskih sredin. ■





Elesovi ambasadorji vrednot so: Jakov Fak, kolesarke ekipe BTC City, Miha Podgornik, Atletska zveza Slovenije, Benjamin Savšek in Marin Medak.

PRENAŠAMO ENERGIJO. PRENAŠAMO VREDNOTE.

Energija teče, skupaj z nami. Ker kot sistemski operater slovenskega elektroenergetskega prenosnega omrežja skrbimo za njen varen, zanesljiv in neprekinjen prenos 24 ur na dan. Smo strokovnjaki z znanjem in izkušnjami, ki sogradimo energetsko prihodnost Slovenije na skrbno zastavljenih temeljih: odgovornosti , zavzetosti, znanju, zanesljivosti, sodelovanju in vztrajnosti. Strateško in trajnostno načrtujemo, gradimo in vzdržujemo prenosno omrežje Republike Slovenije. Za električno energijo na dosegu vaše roke.

www.eles.si

ELES

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
Mojca Prelesnik
Informacijska pooblaščenka Republike Slovenije

RAZVOJ NOVIH TEHNOLOGIJ POSTAVLJA POMEMBNE IZZIVE ZA VAROVANJE ZASEBNOSTI

Živimo v kompleksnem in dinamičnem svetu, kjer je na informacijah temelječa družba prežeta z razvojem novih tehnologij. Ravno ta hiter razvoj pred nas postavlja pomembne izzive, ko govorimo o zagotavljanju varovanja zasebnosti.

Kompleksno varnostno okolje je povezano z razvojem novih tehnologij. Kako uspe institut informacijskega pooblaščenca spremljati tako nagle spremembe v tej dinamični informacijski družbi?

Kot nadzorni organ za varstvo osebnih podatkov skušamo preko izobraževanja zaposlenih, vključevanja in sodelovanja z ustreznimi profili strokovnjakov slediti trendom razvoja in poznavanja novih tehnologij. Po drugi strani pa s pripravo različnih smernic, mnenj in tudi s podajanjem pripomb v okviru priprav novih zakonov skušamo izobraževati upravljavce iz javnega in zasebnega sektorja, da bi na vse vidike varovanja zasebnosti mislili v največji možni meri že ob uvajanju novih tehnologij, ki pomenijo nove oblike obdelave osebnih podatkov. To pomeni razmišljanje o varovanju zasebnosti vnaprej, ne šele takrat ko do škode oziroma posega v zasebnost že pride.

Največji izziv, s katerim se srečujemo dnevno, tako mi pri Informacijskem pooblaščencu kot naši kolegi po svetu je, kako zakone, ki v marsičem težko sledijo hitremu razvoju tehnologije, uporabiti v zvezi z novimi tehnologijami. Prav zaradi razvoja novih tehnologij je varstvo osebnih podatkov danes pred povsem drugačnimi izzivi, kot recimo pred 20 leti in več, ko sta bila sprejeta za evropski prostor ključna dokumenta, ki opredeljujeta temeljne standarde varstva osebnih podatkov, to sta Konvencija 108 Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov in Direktiva 95/46/ES o varstvu osebnih podatkov. Predvsem to je tudi eden od ključnih razlogov za prenovo sistema varstva osebnih podatkov okviru EU, ki je z dosego političnega soglasja konec lanskega leta prešlo v sklepno fazo. Varstvo osebnih podatkov je namreč tako z vidika možnih načinov in oblik obdelave osebnih podatkov, kot tudi s tem povezanih izzivov in potreb, predvsem glede zavarovanja osebnih podatkov, neposredno in življenjsko povezano oziroma odvisno od informacijskih tehnologij.

Največji izziv, s katerim se srečujemo dnevno, tako mi pri Informacijskem pooblaščencu kot naši kolegi po svetu je, kako zakone, ki v marsičem težko sledijo hitremu razvoju tehnologije, uporabiti v zvezi z novimi tehnologijami.

Veliko pozornosti posvečate regulaciji brezpilotnih letalnikov. Je uporaba te tehnologije z vašega vidika zelo problematična?

Razmah uporabe brezpilotnih letalnikov terja široko družbeno in strokovno razpravo ter sodelovanje vseh deležnikov pri pripravi normativnih aktov in vzpostavitvi pogojev za izkoristek številnih prednosti, ki jih prinašajo. Brezpilotni letalnik kot tak, brez sistemov za opravljanje nalog, v osnovi ne pred-

*avtor je član Slovenskega združenja korporativne varnosti

stavlja posega v temeljne človekovega pravice – podobno kot ga ne predstavlja helikopter sam. Najpomembnejša tveganja v povezavi z varovanjem človekovih pravic izvirajo predvsem iz sistemov za opravljanje nalog in zajem podatkov ter iz tega kdo in s kakšnimi nameni uporablja tovrstne sisteme, ki lahko vključujejo: oborožitvene sisteme, sisteme za nadzor in zajem podatkov (fotografiranje, video snemanje, naprave za nočno opazovanje, toplotne kamere...). Gre torej za najrazličnejše senzorje, ki jih ti brezpilotniki ali pogovorno droni, nosijo. In nabor teh je, že skoraj enako kot domišljija, neomejen.

Študija Evropske komisije na temo tveganj pri uporabi brezpilotnikov jasno izpostavlja, da so tveganja pri uporabi brezpilotnih letalnikov s strani organov odkrivanja in pregona kaznivih dejanj glede posegov v zasebnost visoka (»*high risk*«), zlasti v primerjavi z uporabo na nekaterih drugih področjih, in sicer gre za možnost: diskriminacije, učinka zastraševanja glede svobodnega uveljavljanja človekovih pravic (angl. chilling effect), dehumanizacije nadzorovanih, javnega nezadovoljstva in odpora proti nadzoru, pojava zlorabe podatkov za druge namene (angl. function creep).

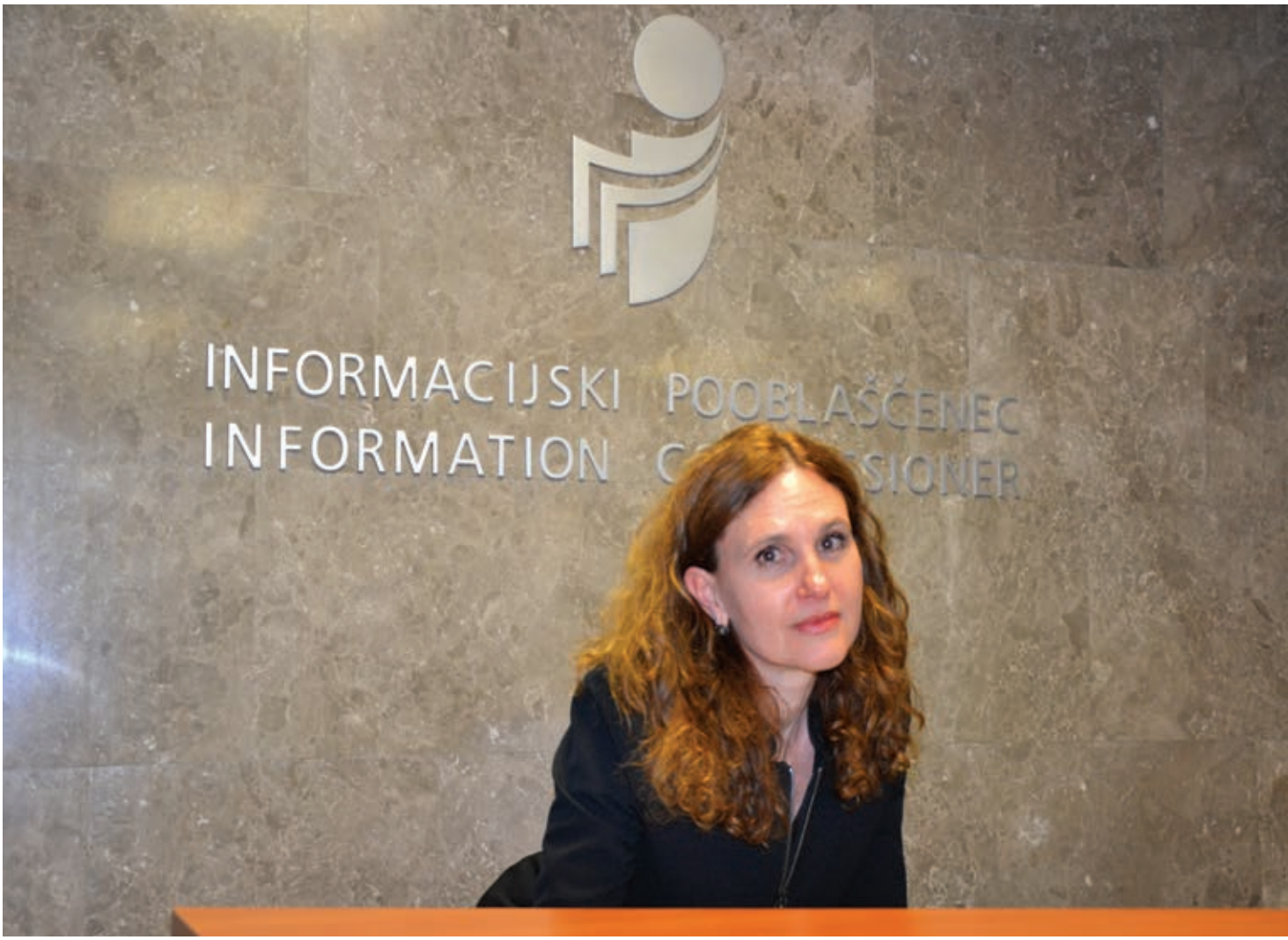
IP želi s svojimi aktivnostmi predvsem prispevati k javni razpravi in normativni ureditvi, zato smo že večkrat pozvali tako resorno ministrstvo kot agencijo za civilno letalstvo, da morajo to področje čimprej normativno urediti. Tu Slovenija zelo zaostaja za drugimi državami članicami Evropske unije. Prav zato smo izdali tudi poročilo, v katerem opozarjamo na tveganja, ki jih uporaba brezpilotnih letalnikov predstavlja za pravico do informacijske zasebnosti in podajamo priporočila tako zakonodajalcu, kot organom pregona, upravljavcem in posameznikom.

Pred kratkim ste praznovali 10. obletnico obstoja Urada Informacijskega pooblaščenca. Kateri so po vašem mnenju tisti glavni dosežki tega obdobja?

Brez dvoma je osrednji dosežek, da danes najbrž ni več posameznika, državne institucije ali podjetja, ki še ne bi slišal za obe ustavni pravici, katerih varuh smo, tako pravico do dostopa do informacij javnega značaja kot tudi pravico do varstva osebnih podatkov. Ob deseti oble-

Brez dvoma je osrednji dosežek, da danes najbrž ni več posameznika, državne institucije ali podjetja, ki še ne bi slišal za obe ustavni pravici, katerih varuh smo, tako pravico do dostopa do informacij javnega značaja kot tudi pravico do varstva osebnih podatkov.





tnici smo tudi presegli dosedanje rekorde glede obsega dela in na obeh pravnih področjih rešili največ zadev. Velikokrat rečemo, da enostavnih primerov, ki jih rešujemo praktično ni več, po vsebini so namreč postali zelo kompleksni. Prav zato je med primeri, ki jih obravnavamo težko izpostaviti zgolj nekaj primerov. Mogoče bi na področju varstva osebnih podatkov vseeno kot pomembne dosežke izpostavila številne smernice, za vsa pomembna področja obveznosti upravljavcev, pa nekatere odločitve Ustavnega sodišča RS, ki so rezultat naših pobud npr. glede (ne)zakonitosti hrambe prometnih podatkov elektronskih komunikacij. Enako prelomne so bile številne odločitve v zvezi s pritožbami glede dostopa do informacij javnega značaja. Na tem pravnem področju je potrebno biti pozoren, ker predlagatelji zakonov zelo radi, sicer povsem nesistemsko, dodatne izjeme od prostega dostopa do informacij javnega značaja, uzakonjajo v področnih zakonih. Take nesistemske »rešitve« pa so za transparentnost nevarne in zahrbtne. Predvsem je pomembno, kot kaže praksa, da po 10. letih na obeh področjih tako z vidika zavezancev kot tudi posameznikov spoštovanje in izvajanje nekaterih bistvenih pravic in obveznosti postaja vodilo.

S pravnimi normami je nemogoče v popolnosti opredeliti vse situacije v realnem življenju. Predvidevam, da je ravno pravna praksa skozi vaša mnenja tisto pomembno orodje, ki ga uporabljate pri opredelitvi nenavadnih situacij?

Res je, življenje je preveč pisano, da bi ga lahko v celoti zajeli v zakonih. Bistveno pa je, da znamo na vsako življenjsko situacijo z ustrezno uporabo zakonov primerno odgovoriti. Zato so nenazadnje pomembni tudi primeri, ko je sproženo sodno varstvo zoper naše odločbe in se oblikuje dragocena sodna praksa glede dopustnosti posegov v zasebnost. Aktivno seveda spremljamo tudi delo evropskih sodišč - predvsem Sodišča EU in Evropskega sodišča za človekove pravice. Veliko energije prav s ciljem pojasnjevanja primerov iz prakse posvetimo pripravi smernic in mnenj – teh napišemo letno preko 2000. Z njimi skušamo tako posameznikom kot upravljavcem osebnih podatkov, pomagati z zelo praktičnimi nasveti, kako zakonito in pravilno uporabljati predpise, vse seveda predvsem s ciljem ustreznega varstva in zavarovanja osebnih podatkov.

Kakšen pomen namenjate procesom izobraževanja in usposabljanja? Je to iz vaše perspektive učinkovit vzvod za dvigovanje splošnega zavedanja?

Dvig splošnega zavedanja o katerikoli novi pravici ni možen brez usposabljanj, tako tistih, ki jih izvajamo pri IP kot tudi seveda vseh nadaljnjih, ki jih za svoje zaposlene in druge izvajajo sami upravljavci. Prav slednji tudi nosijo glavni del odgovornosti za zakonito obdelavo osebnih podatkov v okviru svojega dela. Prav zato zaposleni na IP redno nastopamo na konferencah, strokovnih združenjih in drugih dogodkih, kjer zelo različnim ciljnim publikam približujemo temeljne vsebine pravic, ki jih varujemo.

Sodobne tehnologije omogočajo obsežen in invaziven nadzor nad zaposlenimi, ki pa je lahko pretiran in posega v pravice zaposlenih.

Kateri so tisti primeri v praksi, kjer zaznavate največ kršitev s področja zlorabe osebnih podatkov?

Zelo veliko težav je še vedno na področju razmerij med delodajalci in zaposlenimi. Sodobne tehnologije omogočajo obsežen in invaziven nadzor nad zaposlenimi, ki pa je lahko pretiran in posega v pravice zaposlenih. Ukvarjali smo se s primeri nadzora uporabe spletnih strani, nadzora uporabe e-pošte in telefonov, vse pogosteje se nesorazmerno uvajajo tudi GPS naprave. Kršitve se dogajajo tudi na področju informacijske varnosti, ko upravljavci ali njihovi pogodbeni obdelovalci ne izpolnijo vseh dolžnosti glede varnosti podatkov – pogosto se pretirano zanašajo na tehnične ukrepe in zanemarijo organizacijske ukrepe, kot je izobraževanje. Vsako leto znova pa ugotavljamo tudi porast primerov nezakonitega izvajanja videonadzora - vsi bi snemali vse in vsakogar.

V zadnjem obdobju se napoveduje pomembne spremembe na področju regulative EU s področij, ki jih pokrivate. Nam lahko postrežete s kakšnimi bolj konkretnimi podatki.

Že več let smo priče razprav o potrebi po novem sistemu varstva osebnih podatkov na ravni EU, ki bi ustrezal izzivom, ki smo jim priča, predvsem z vidika novih tehnologij. Zdaj smo prišli v tem procesu do pomembne prelomnice. Decembra lani sta namreč Evropski parlament in Svet EU dosegla dogovor na politični ravni o novi splošni uredbi EU o varstvu osebnih podatkov, ki bo nadomestila direktivo 95/46/ES. Med pomembnimi novostmi, ki jih uredba prinaša bodo: uporaba uredbe za EU podjetja, kot tudi podjetja, ki niso iz EU, a nudijo storitve evropskim potrošnikom. Gre za t.i. načelo enega glavnega nadzornega organa (ang. *One Stop Shop principle*), ki bo omogočalo, da evropska podjetja vse rešujejo samo z enim »glavnim« nadzornim organom za varstvo osebnih podatkov. Pomembna je tudi uvedba potrebne privolitve starša oziroma nosilca roditeljske pravice za veljavno soglasje za obdelavo osebnih podatkov v kontekstu ponujanja t.i. storitev informacijske družbe mlajšim od 16 let. Prihajajo tudi zelo visoke kazni za kršitelje - največ 2% letnega prometa oz. 20 mio. EUR, pa dolžnost obveznega obveščanja o varnostnih incidentih oz. kršitvah zavarovanja osebnih podatkov (ang. *Notification of personal data breach. V*zpostavlja se Evropski odbor za varstvo osebnih podatkov (ang. *European data protection Board*) in mehanizem doslednosti (ang. *Consistency mechanism*), pa tudi možnost zastopanja posameznikov s strani nevladnih organizacij ali, če bodo članice to omogočale tudi možnost samostojne sprožitve pravnih postopkov. Zelo pomembna je tudi uvedba izdelave presoj vplivov na zasebnost (ang. *Data protection impact assesment*), ki bo v določenih primerih celo obvezna, pa tudi imenovanje uradnih oseb za varstvo osebnih podatkov (ang. *Data protection officer*), ki bodo pri posameznih upravljavcih osebnih podatkov bdeli nad področjem varstva osebnih podatkov.

Še v začetku leta se je v strokovnih krogih pričakovalo, da bo uredba dokončno potrjena v prvi polovici letošnjega leta, zdaj pa se vse bolj sliši, da bo to šele v drugi polovici leta 2016. To pomeni, da se bo predvidoma najverjetneje začela uporabljati v drugi polovici 2018. Določen je namreč dveletni »vacatio legis«.

V okviru magistrskega študija »Management korporativne varnosti«, ki se izvaja na Fakulteti za podjetništvo/GEA College so v sodelovanju z vami razvili študijsko vsebino opredeljeno kot »Sistemski pristopi obvladovanja ključnih podatkov poslovnih organizacij«. Menite, da so lahko kadri, ki bodo končali ta magistrski program ustrezen potencial za podjetja, katera bodo na podlagi evropskih direktiv morala imeti zaposlenega pooblaščenca za varovanje osebnih podatkov?

Vzpostavitev sistema, ko bodo morali upravljavci v javnem sektorju in tudi številni upravljavci v zasebnem sektorju določiti t.i. uradno osebo za varstvo osebnih podatkov, ki nas čaka kot rečeno v letu 2018, bo po eni strani pomenila pomemben korak v smeri zagotovitve ustrezne pozornosti področju varstva osebnih podatkov tudi v obliki kadrovskih virov, po drugi strani pa seveda izziv usposabljanja le-teh za novo nalogo. Številni veliki upravljavci ta sistem v praksi že izvajajo, vsekakor pa so dobrodošla vsa prizadevanja na ravni sistema visokega izobraževanja za zagotavljanje zadostnega nabora ustrezno usposobljenih kadrov za tovrstne naloge. Korporacijska varnost je izrazito interdisciplinaren pojem in interdisciplinarni bodo morali biti tudi kadri.

Urad Informacijske pooblaščenke je med drugim tudi korporativni član Slovenskega združenja korporativne varnosti. Bi lahko tako sodelovanje opredelila kot primer dobre prakse, ki bo v bodoče postal standard tudi za druge državne organe pri prenosu idej v različna družbena okolja?

Absolutno je to primer zelo dobre prakse ali kot dostikrat rečemo, »posebno javno-zasebno partnerstvo«. Vsak državni organ mora biti na svojem področju odprt za sodelovanje s stroko in njene predloge, sicer se izgubi dragocena vez. Državni organi nikakor ne smemo biti predvsem sami sebi namen, ampak smo tukaj zato, da uveljavimo določene pravice in s tem povezane standarde, od katerih imajo potem koristi konkretni ljudje. Zato moramo slediti dogajanju v praksi. To je mogoče doseči na različne načine in sodelovanje v tovrstnih združenjih, predvsem seveda v okviru naših svetovalnih pristojnosti, je ena od dobrih poti.

Kako gledate na napore Slovenskega združenja za korporativno varnost, da v slovenskem okolju dvigne splošno zavedanje o potrebi celovitih pristopov do obvladovanja tveganj? Lahko v tem okviru najdete tudi povezavo z učinkovitejšim zavedanjem o varovanju osebnih podatkov?

V sodelovanju s Slovenskim združenjem za korporativno varnost smo organizirali nekaj dogodkov, ki so bili zelo uspešni in so pomembno prispevali k dvigu ozaveščenosti, javnemu diskurzu ter izmenjavi informacij. Tu bi zlasti rada izpostavila posvet, ki je na temo brezpilotnikov potekal lansko leto v Državnem svetu. Odličen posvet, ki je povezal strokovnjake in deležnike z različnih področij – tako kot pri obravnavani temi mora biti in edino tako rodi sadove. Sodelovanje in povezovanje strokovnjakov s področja varnosti na srečanjih združenja, pa omogoča izmenjavo strokovnih znanj z različnih področij, ki tudi našim sodelavcem nudijo nova znanja in izkušnje. ■

7. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 16.—17. marec 2016



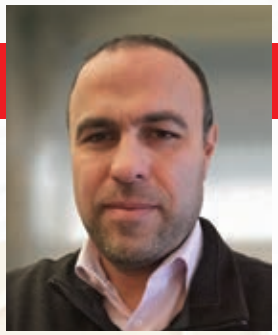
PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

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

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

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

Avtor: Aleš Polajnko, ORG. TEND d.o.o.



INTELIGENTNI IP VIDEO NADZORNI SISTEM IN VARNA IT INFRASTRUKTURA

Video nadzorni sistemi so integralni del upravljanja varnostnih tveganj, ki so v današnjem času zelo intenzivna in se tudi zelo dinamično spreminjajo. Zato je potrebno temu delu pri obvladovanju tveganj posvetiti večjo pozornost, predvsem pri načrtovanju in izbiri sistema, ki ga nameravamo uporabiti.

Glede na to, da so današnji IP video nadzorni sistemi zelo »inteligentni«, nam omogočajo, da z njimi izvajamo preventivne ukrepe, nadziramo in tudi konkretno reagiramo v primeru varnostnih incidentov. Zato moramo poleg izbora samih lokacij in funkcij nadzora na lokaciji precej pozornosti posvetiti tudi samemu načrtovanju varne infrastrukture za takšen sistem. Zatrdimo lahko, da je mogoče s takšnimi inteligentnimi IP video nadzornimi sistemi v določenih situacijah nadomestiti tudi precej drugih senzorjev, ker to funkcijo izvajamo vzporedno z video nadzorom, prav tako pa tudi zmanjšujejo potrebo po fizičnem posegu na varovani lokaciji (»virtual guard«). Takšni sistemi nam na široko odpirajo možnosti, da z njimi nadziramo in upravljamo tudi druge preventivne in aktivne varnostne ukrepe na lokacijah. Da bi to lahko dosegli, mora biti inteligentni video nadzorni sistem že v osnovi takšen, da preprečuje kakršnekoli manipulacije s kamerami, medtem ko mora komunikacija med kamero in nadzornim sistemom oz. podatkovnim skladiščem vsebovati vse potrebne varnostne elemente, ki to preprečujejo. V primeru incidenta nam mora sistem omogočiti predvsem visoko kakovost samega posnetka incidenta, hitro iskanje incidenta ter verodostojnost posnetka (vsaka slika-frame mora biti podpisana z digitalnim certifikatom). Vse to pa v eni napravi združuje in ponuja MOBOTIX.

Video analiza in iskanje dogodkov se izvaja v sami kameri, ki za to ne potrebuje dodatne procesorske moči in zna sama upravljati video »ring buffer« na NAS-u ali strežniku. Rezultat tega je, da so MOBOTIX video nadzorni sistemi zelo zanesljivi, potrebujejo manj strežnikov, manj delovnih postaj in manj omrežne infrastrukture. To pa zmanjša celoten strošek sistema, kot tudi skupni račun za energijo. Programska oprema na IP kamerah, vse nadgradnje in VMS so brezplačni.

TEND varnostne rešitve IT in MOBOTIX video nadzorni sistemi

Podjetje ORG. TEND d.o.o. je na trgu prisotno od leta 1999, njegova glavna dejavnost je sistemska integracija IT (informacijskih tehnologij). 30 strokovnjakov z različnih področij IT načrtuje, implementira in vzdržuje sisteme IT, ki naročnikom nudijo podporo poslovnim procesom, pogoje in infrastrukturo za delovanje IT sistemov, skrbijo za ključne podporne procese, kot so sistemi za varno in neprekinjeno komunikacijo med vsemi deležniki poslovanja ter varne, zanesljive in šifrirane rešitve za shranjevanje podatkov. Ekipa s svojimi izkušnjami in znanjem skupaj z rešitvami vodilnih svetovnih proizvajalcev IT opreme poskrbi za vse preventivne ukrepe, ki podjetje ščitijo tako pred zunanjimi kot notranjimi varnostnimi tveganji s področja informacijske tehnologije. Mnoge zgoraj naštete rešitve pa so tudi osnova za varen, učinkovit in dolgoročno-razvojno usmerjen IP video nadzorni sistem. TEND na tem področju predstavlja vezni člen med podjetji, ki so strokovnjaki za tehnično varovanje in te sisteme implementirajo. Za dobro izveden IP video nadzorni sistem je potrebno vzpostaviti dobro, varno in učinkovito IT infrastrukturo. Odličen primer je uporaba video nadzornih sistemov podjetja MOBOTIX, s katerim sodelujemo že 15 let.

MOBOTIX – profesionalni VMS in Smart IP kamere od leta 2000

MOBOTIX je podjetje za razvoj programskih rešitev z lastnimi IP kamerami (Made in Germany). Leta 2005 je MOBOTIX predstavil svoji prvi profesionalni sistem za upravljanje videa, ki je še vedno v uporabi v tisočih napravah po vsem svetu. Mobotix VMS rešitve se uporabljajo tudi v mnogih varnostno zahtevnih aplikacijah, kot so zapori, letališča ali nogometni stadioni. Že od leta 2000 so MOBOTIX IP kamere znane po svojih visokokakovostnih video zmogljivostih, zanesljivosti (9,5 let za TBF) in majhne porabe pasovne širine, predvsem zaradi svoje »decentralizirane arhitekture«. Video analiza in iskanje dogodkov se izvaja v sami kameri, ki za to ne potrebuje dodatne procesorske moči in zna sama upravljati video »ring buffer« na NAS-u ali strežniku. Rezultat tega je, da so MOBOTIX video nadzorni sistemi zelo zanesljivi, potrebujejo manj strežnikov, manj delovnih postaj in manj omrežne infrastrukture. To pa zmanjša celoten strošek sistema, kot tudi skupni račun za energijo. Programska oprema na IP kamerah, vse nadgradnje in VMS so brezplačni.

Nova generacija 6MP notranjih IP kamer

MOBOTIX ponuja dovolj široko paleto različnih modelov IP kamer s 6MP resolucijo, ki vključujejo tako imenovano »moonlight« tehnologijo.

Nove 6MP notranje IP kamere (Indoor line) so zelo konkurenčne in obenem podpirajo vse druge funkcije, ki jih najdemo v vseh obstoječih zunanjih MOBOTIX IP kamerah (IP 66). Za zelo dostopno ceno dobi uporabnik popolnoma samostojen sistem za video nadzor, vključno s kartico SD in napredno funkcijo snemanja na oddaljen »snemalnik« oz. NAS. Na NAS shranjujemo dogodke in alarme. Za nadzor in pregled uporabljamo profesionalni video menedžment sistem (VMS), ki nam ponuja funkcije za video analizo, kot sta npr. toplotni zemljevid (Heat map) ter statistika za objekte, ki jih nadziramo. Poleg tega je v kamerah integrirana hemisferična tehnologija, na voljo so različne možnosti objektivov-leč, kjer velja omeniti tudi novo 103 ° lečo. Le-ta nam omogoča npr. pokritje sobe brez mrtvega kota. V programsko opremo kamere sta vključena tudi modul »MxActivitySensor«, s katerim drastično zmanjšamo lažne alarme, in zelo zanimiva funkcionalnost, ki nam omogoča samodejno vedenjsko detekcijo objekta (v modelu C25). Vsi modeli notranjih kamer lahko opcijsko vključujejo tudi popolni dvosmerni avdio (osnovne nastavitve imajo to funkcionalnost izklopljeno), vključno z mikrofonom in zvočnikom. Lahko rečem, da so opisane funkcionalnosti kot nalašč za majhne pisarne in trgovine, saj je sistem mogoče enostavno razširiti brez stroška licenčnin in z brezplačnimi nadgradnjami (»lifetime free«) tako za programsko opremo kamere kot za video nadzorni sistem - VMS.

Modele kamer C25 in p25 z 6MP je mogoče preprosto namestiti v samo nekaj minutah npr. v pisarnah s spuščenimi stropi. Poleg hemisferične tehnologije ima model p25 na voljo vse možnosti za objektive-leče in senzorske opcije. S tem lahko zagotovimo izvedbo popolne rešitve za različna okolja varovanja. Vsi notranji modeli kamer MOBOTIX so podprti z »On-Wall« nastavki, kar nam omogoča enostavno montažo na različne površine.



6MP dvojna termična IP kamera

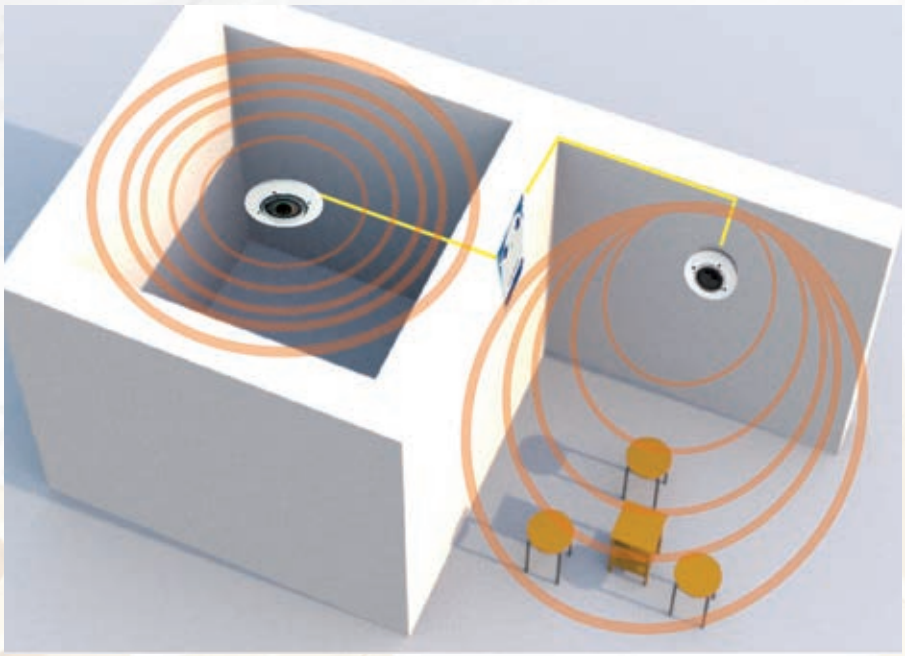
Zanesljivo tudi za uporabo pri daljših razdaljah

Termične/toplotne kamere zaznajo toplotno sevanje ali temperaturni profil predmetov, zato lahko odlično delujejo tudi v popolni temi. MOBOTIX uporablja industrijski razred senzorjev z zelo visoko toplotno ločljivostjo 50 mK, kar je enako 1/20 °C. Takšne karakteristike nam omogočajo zaznavanje (termovizijo) ljudi ali drugih objektov, ki oddajajo toploto na zelo velikih razdaljah v razponu do 400 m. Uporaba integrirane programske opreme v kameri »MxActivitySensor« pa nam omogoča preprosto zaznavanje premikanja objektov, ki je zelo zanesljivo tudi v popolni temi.

MOBOTIX toplotna kamera podpira vse funkcije in možnosti, ki jih imajo drugi modeli MOBOTIX kamer, vključno z možnostjo avtomatskega snemanja ali uporabo sporočil (massaging system), ki jih lahko sprožijo različni tipi dogodkov. Ohišje modelov kamer M15 ali S15 je vodoodporno in v skladu s standardom IP66. Hkrati lahko tem modelom kamer poleg toplotne kamere dodamo optični barvni 6MP senzor. Tako dobimo hkrati dvojen pogled s toplotno sliko in kakovosten video s 6MP resolucijo. Takšna konfiguracija v vodoodporni IP kameri dramatično poveča možnosti uporabe in apliciranja. Uporaba standarda za napajanje PoE in zelo nizka poraba energije, ki tudi s termičnim senzorjem dosega le 6W in je najnižja na trgu, nam omogoča uporabo in delovanje termične kamere MOBOTIX v vsaki situaciji.

Potrebujemo samo eno termično MOBOTIX kamero, da lahko nadzorujemo velik zunanji prostor brez potrebe po dodatni osvetlitvi. Kombinacija termičnega senzorja in optičnega video senzorja ter inteligentna programska oprema, ki temelji na zaznavanju gibanja »MxActivitySensor«, popolnoma ustrezajo uporabi v situaciji, kjer moramo pokrivati širok »perimeter« varovanja. Tako lahko učinkovito in brez sekundarne opreme, kot so npr. IR reflektorji ali dodatni senzorji gibanja in kamere, zaznamo vse pomembne dogodke tudi v popolni temi.

Z uporabo termične kamere lahko zagotovimo popolno zasebnost pri nadzoru na javnih mestih ali npr. varovanju objektov, kjer se stikata zasebno in javno. Toplotna slika, ki se shrani, ne pokaže dovolj, da bi omogočila identifikacijo osebe. V primerih, kjer idetifikacijo potrebujemo, dodamo optični barvni senzor. Ta funkcionalnost in rezultat nam bosta močno v pomoč pri večanju sprejetosti video nadzora v javnosti in uporabe video nadzora v občutljivih situacijah oz. na lokacijah, kot so npr. javne površine mesta, bazeni, gostinski in športni objekti, kjer je danes to zelo občutljiva tema, zaradi česar velikokrat precej znižamo proaktivno delovanje varovanja.



Kamera MOBOTIX z dvojnim senzorjem lahko samodejno izvede preklop snemanja oz. pogleda iz toplotnega senzorja v pogled z optičnim barvnim senzorjem, ki posname sliko z visoko resolucijo, če se objekt pojavi v preddefiniranem območju kamere, kjer je to dovoljeno. Ta edinstvena lastnost MOBOTIX sistema združuje dva pomembna vidika: zagotovitev zasebnosti med normalnim nadzorom in popoln dostop do posnetka-slike visoke resolucije v primeru kritičnih dogodkov, z upoštevanjem cone zasebnosti, če je ta definirana.

Toplotna radiometrija - termovizja za avtomatsko zaznavanje temperature

MOBOTIX je v kameri »Mx Activity Sensor« odlično združil tehnologije toplotnega in optičnega senzorja s funkcionalnostjo. To sistemu omogoča samodejno odkrivanje predmetov in oseb v popolni temi na razdalji nekaj sto metrov. Brezplačna nadgradnja programske opreme v kameri pa nam omogoča tudi tako imenovani »Spot Metering«, ki se izvaja v sredini slike. To nam omogoča merjenje temperature v območju od -40°C do + 550 °C, z značilno natančnostjo ±10°C. Takšna rešitev še poveča možnosti uporabe ene kamere za več namenov in njeno namestitev v še kakšno drugo okolje.

MOBOTIX ponuja tudi dodatno vrsto senzorjev (v modelih M15, S15, S15 PT Mount), kjer je senzor umerjen po celotnem zajemu slike s toplotno radiometrijo (TR senzor). Po zaslugi te lastnosti lahko takšen sistem uporabimo-nasta-

Kamera MOBOTIX z dvojnim senzorjem lahko samodejno izvede preklop snemanja oz. pogleda iz toplotnega senzorja v pogled z optičnim barvnim senzorjem, ki posname sliko z visoko resolucijo, če se objekt pojavi v preddefiniranem območju kamere, kjer je to dovoljeno.

vimo za ustvarjanje samodejnih alarmov, ki jih definiramo s temperaturnimi omejitvami ali s temperaturnimi območji na sliki. Tak senzor je odlična rešitev npr. za zaznavanje ognja na varovanem območju ali drugih virov toplote, ki presegajo nastavljene vrednosti. Nastavimo lahko do 20 različnih temperaturnih sprožilcev in v tem primeru je celotna slika uporabna z značilno natančnostjo ± 10 ° C. Tak sistem z MOBOTIX z dvojno toplotno(TR) kamero lahko uporabimo tudi za hot spot vizualizacijo pri nadzoru. Omogoča nam, da preventivno reagiramo, lokaliziramo premočan vir toplote ter po zaslugi tega preprečimo večjo škodo.

Video nadzorni sistem - VMS – Mx management Center

Leta 2015 je Mobotix razvil nov profesionalni video nadzorni sistem VMS »Mx Management Center«. Glede na koncept lahko rečemo, da gre za nov mejnik v profesionalni VMS industriji. Koncept uporabniškega vmesnika temelji na gestah, kot so povleci in spusti, zaradi česar je zelo intuitiven za uporabo. Nov Mx Management Center (MxMC) nima omejitev sistema in je sposoben upravljati več sto kamer ter uporabnikov. VMS dopušča hkratno uporabo kamer drugih proizvajalcev z uporabo protokola ONVIF ter njihovo vključitev v sistem. MxMC lahko sočasno upravlja več monitorjev in prikazov na video stenah. Izjemno hitro predvajanje in post-video iskanje sta implementirana, prav tako tudi vmesnik POS (Point-of sale) za VMS v trgovinah. Ponovno je treba poudariti, da je programska oprema brezplačna. MxMC v povezavi z MOBOTIX kamerami popolnoma podpira decentralizirano arhitekturo. Scenariji dostopa do posnetkov so lahko glede na podporno infrastrukturo in varnostne zahteve različni. V primeru, ko komunikacija s kamero ni najhitrejša ali so zahteve glede varnosti in občutljivosti podatkov zelo visoke, nam neposreden dostop do posnetkov preko kamere zagotavlja zaščiteno in šifrirano end-to-end povezavo, ne da bi morali zagotoviti izmenjavo datotek s prenosom podatkov prek širokopasovnih omrežij (kamera je v tem primeru odličen požarni zid). Neposreden dostop do posnetkov-podatkov od MxMC do NAS omogoča najhitrejše predvajanje video podatkov in je tipičen primer uporabe sistema, kjer je vključena tudi večja nadzorna soba.

Upravljanje s pasovno širino, ki je na voljo MOBOTIX kamera odvisno od razpoložljive pasovne širine med prikazom slike upravlja s hitrostjo snemanja in ločljivostjo slike (na interno SD kartico vedno shranjuje podatke v nastavljeni resoluciji in nastavljeno hitrostjo snemanja). Vendar lahko na kameri med snemanjem istočasno pregledujete in po potrebi približujete sliko (zoom za področje interesa), ne da bi zato potrebovali prenos celotne slike v visoki resoluciji. Ta funkcija optimizira in zagotovi najboljšo kakovost slike ob trenutno razpoložljivi pasovni širini. Prav tako se s tem izognemo situaciji ene same točke odpovedi (single point of failure) in imamo omogočeno kakovostno predvajanje tudi preko omejenih podatkovnih povezav.



Statistični podatki o dejavnostih in POS

MxMC ponuja tudi odlično orodje za upravljanje s posnetki, saj imamo zagotovljen hiter pregled nad vsemi dejavnostmi v okviru dogodkov s funkcionalnostjo »histogram«. Ta grafični pregled nam omogoča, da istočasno v neki časovni dimenziji pregledamo hkratno vse posnetke kamer v sistemu. Statistiko dogodkov enostavno analiziramo v kateremkoli časovnem obdobju, obsegu ali z izbiro drugih pogojev za pregled situacije v grafični obliki. VMS ponuja tudi možnost enostavnega pregleda in iskanja posnetih dogodkov, povezanih s transakcijami blagajn. Ta funkcija je idealna za majhne aplikacije, kjer lahko analiziramo vedenje kupcev ali iščemo dogodke, povezane s transakcijami. Nov POS (Point-of-Sale) vmesnik prikazuje celoten račun s sliko pri blagajni, omogoča iskanje artiklov po imenu ali ceni ter nato analizira podatke iz vseh kamer v sistemu, kjer se iskani niz pojavi.

Mx Analytics - Statistika in zaznavanje vedenjskih vzorcev

Hemisferične MOBOTIX kamere so zelo primerne za nadzor trgovin in drugih okolij, kjer je na prvem mestu spremljanje kupca. V vseh modelih kamer MOBOTIX z enim senzorjem, je vključena video analiza, ki nam omogoča izdelavo tako imenovanih toplotnih zemljevidov in beleženje statistike za objekte v preddefiniranih uporabniško določenih koridorjih s samodejnim poročanjem. Modeli kamer, kot sta denimo C25 in Q25, ki jih montiramo na strop, lahko analizirajo tudi obnašanje premikajočih se predmetov, s čimer pridobimo dodatne samodejne alarme, npr. če se ti predmeti ustavijo, obrnejo ali se premikajo v nedovoljeni smeri. Za vse naštete video analize ni potrebna delovna postaja, prav tako pa z njimi ne obremenjujemo komunikacijskega omrežja, saj se te analize izvajajo in obdelujejo v vsaki kameri posebej. To seveda povečuje zanesljivost in varnost ter seveda precej znižuje strošek celotnega sistema. ■

Avtor: prof.dr.Iztok Podbregar / Fakulteta za organizacijske vede, UM



NEUSKLAJEN PRISTOP K TVEGANJEM POMENI SPREJEM GOTOVEGA PORAZA

Sodobno varnostno okolje je, za razliko od preteklosti, ko so bile osnovne grožnje posameznim državam povezane predvsem z vojnami, postalo bistveno bolj zapleteno. Spekter groženj in tveganj se je razširil na vse segmente družbe in procesov, ki potekajo v njej. Prav tako so tudi posledice groženj in tveganj razpršene po celotni družbi in vplivajo na vsa področja od nacionalne varnosti, gospodarstva, zdravstva, informacijskih omrežij in drugo.

Republika Slovenija se nahaja na križišču zaključka Balkanske poti in prehoda med Panonsko in Padsko nižino in je zaradi tega še bolj izpostavljena nepričakovanim dogodkom, med katerimi so tudi posledice netransparentnih groženj.

To dejstvo postavlja vse deležnike v procesu ocenjevanja groženj in tveganj ter sprejemanja ustreznih protiukrepov v povsem novo situacijo. Ta zahteva kvalitetno in tekoče medsebojno sodelovanje pri sprejemanju učinkovitih ukrepov, ki bi dejansko zagotovili zmanjševanje ogroženosti v celoti. Brez tega sodelovanja in usklajevanja, bi ukrepi povečali varnost zgolj določenega segmenta družbe, istočasno pa bi na drugem segmentu, povzročili poslabšanje. To zahteva od vseh, ki sprejemajo odločitve v okviru svojih pristojnosti, interdisciplinarni pristop in stalno preverjanje celovitosti vseh sprejetih ukrepov.

Države in njihove Vlade imajo veliko odgovornost, da v relativno kratkem času sprejmejo povsem usklajene, odmerjene odločitve, ki predstavljajo celovito rešitev in dejansko zmanjšujejo tveganja celotnega niza groženj. Državni organi Republike Slovenije so dolžni vsak predlog predpisa, vsako odločitev, pa naj se zdi še tako nepomembna, celovito pripravljati, usklajevati in sprejeti tako, da ne povzroči izboljšanja enega področja, hkrati pa izrazito poslabšati drugega področja groženj.

Državni organi Republike Slovenije so dolžni vsak predlog predpisa, vsako odločitev, pa naj se zdi še tako nepomembna, celovito pripravljati, usklajevati in sprejeti tako, da ne povzroči izboljšanja enega področja, hkrati pa izrazito poslabšati drugega področja groženj.

Poseben fenomen predstavlja priprava predpisov, ki zahtevajo sodelovanje dveh ali več državnih organov. Vsak teži k temu, da ureja samo svoj segment (npr. organiziran kriminal), odsotnost komunikacije, koordinacije in neobčutljivost ter včasih popolno nepoznavanje drugih povezanih področij, vodi v izrazito povečano tveganje in grožnje na področju, ki so ga želeli urediti.

V Slovenski družbi je prisoten fenomen, da je percepcija grožnje in distance do realnosti nekega tveganja zelo velika, ob tem pa posamezni resorji Vlade RS ne čutijo nujne potrebe po usklajevanju in iskanju skupnih rešitev. Razkorak med percepcijo in realnostjo nekega tveganja, povzroča dodatno tveganje, ki ga je možno rešiti z interdisciplinarnim pristopom.

V zadnjih letih smo priča zelo (ne)posrečenemu delovanju državnih organov, ki se kaže v tem, da vidi potrebo po posvetovanju in usklajevanju posameznih rešitev v Svetu za nacionalno varnost Republike Slovenije samo ob izjemnih dogodkih. Hkrati pa Vlada Republike Slovenije skozi predloge različnih resorjev, zelo nekritično sprejema predpise, ki povzročajo prikrita tveganja ter nevarnosti. Le te v praksi potem rešujemo z zamikom in velikim presenečenjem, ker so se zgodila. To je še posebej nerazumljivo zato, ker imamo dokaj solidne procedure usklajevanja in dobro informacijsko podporo Vlade RS. Enostavno se nam je zgodil fenomen birokratske zaprtosti posameznih resorjev in nerazumna samozavest posameznih disciplin znanja v resorjih, ki ne čutijo nobene potrebe po sodelovanju z ostalimi resorji in disciplinami znanja.

Poznavalci bi pričakovali, da bo Svet za nacionalno varnost Republike Sloveni-

je, oz. operativci, ki pripravljajo rešitve za odločevalce, opravljali svojo funkcijo usklajevanja vsaj pri tistih predlogih predpisov, ki pomenijo implementacijo različnih predpisov EU v Slovensko okolje. Pri implementaciji predpisov EU je potrebno biti še posebej previden vsaj iz dveh razlogov. Prvi razlog je v tem, da jih implementiramo tako, da z nacionalnim predpisom sebično uredimo naš nacionalni prostor, hkrati pa porušimo ravnovesje v naši regiji in s tem posredno izjemno povečamo tveganja in grožnje celotne regije. Drugi razlog je v tem, da predpise EU nekritično, prehitro ali nesorazmerno implementiramo v našo prakso in s tem povzročimo neracionalno porabo sredstev, pa naj bo to nehote ali zaradi nepoznavanja obravnavanega področja. Zato bi pričakovali, da Svet za nacionalno varnost bolj redno spremlja in se vključuje tudi v sprejemanje posameznih predpisov in zakonov z namenom doseganja zadostne in potrebne celovitosti predpisov. Na ta način bi dosegli zgodnje preventivno delovanje in s tem tudi racionalno uporabo subjektov nacionalne varnosti v kasnejši implementaciji prej omenjenih predpisov.

Država ima poglavitno vlogo pri ocenjevanju ogroženosti in tveganj ter sprejemanju ukrepov za njihovo zmanjševanje, saj kot zakonodajalec določa pravne okvire ter zagotavlja profesionalne subjekte na obveščevalno varnostnem področju. Ti s svojim delovanjem zagotavljajo potrebne informacije, ki služijo za sprejemanje ukrepov. Ob tem pa ne sme zanemariti ostalih segmentov družbe, predvsem gospodarstva, ki za svoje uspešno delovanje potrebuje stabilno okolje, v katerem je čim manj ovir, ki bi jih lahko povzročile parcialne in ne dovolj premišljene odločitve. Gospodarstvo je vpeto v širše mednarodno okolje, v katerem je potrebno biti konkurenčen in imeti čim bolj prost pretok blaga in storitev. Država mora s svojimi ukrepi poskrbeti za čim višjo stopnjo varnosti države in državljanov in istočasno zagotavljati spodbudno poslovno okolje, v katerem so vsi zakonodajni ukrepi primerno odmerjeni.

> V Slovenski družbi je prisoten fenomen, da je percepcija grožnje in distance do realnosti nekega tveganja zelo velika, ob tem pa posamezni resorji Vlade RS ne čutijo nujne potrebe po usklajevanju in iskanju skupnih rešitev.

> Nekateri konkretni primeri, ki kažejo na potrebo po zagotavljanju sinergije pri sprejemanju zakonodajnih in drugih sistemskih ukrepov.

V tem delu želimo predstaviti nekaj konkretnih primerov, ki dobro osvetljujejo pomen zagotavljanja sinergije pri sprejemanju zakonodajnih in drugih sistemskih ukrepov. Ob teh primerih ne želimo ustvarjati vtisa, da gre za zagovarjanje ali nasprotovanje določenim spremembam, temveč z dejstvi predstaviti pomen premišljenega, z vsemi deležniki usklajenega ukrepanja in sprejemanja odločitev. Samo tak način namreč zagotavlja sinergijo, ki vodi k odmerjenim





ukrepom, katerih pozitivni učinki bodo razpršeni na področjih vseh deležnikov. Ti konkretni primeri se nanašajo na trenutno zelo pereče spreminjanje tobačne zakonodaje in spreminjanje zakonodaje glede orožja.

Spreminjanje tobačne zakonodaje

V praksi po svetu, obstaja mnogo primerov, ko so posamezne države uredile tobačno zakonodajo premišljeno, z upoštevanjem mnenj in stališč vseh deležnikov, ki so kakor koli povezani s to problematiko, ter tako zagotovile sinergijski učinek. Tam, kjer takega pristopa ni bilo, so nastale negativne posledice, ki so te države v zelo kratkem času prisilile v iskanje novih rešitev, saj tako sprejeti ukrepi niso prinesli pričakovanih rezultatov. Tak je primer Kanade in Švedske. Kanada v letu 1994, in Švedska v letu 1998, sta dvignili davek na tobak, pri čemer nista upoštevali vseh morebitnih negativnih posledic očitno ne dovolj domišljene in z vsemi deležniki usklajene rešitve. Dvig davka v teh dveh državah je povzročil porast problema tihotapljenja, ki je bil tako velik, da so davke znova znižali. Slovenija prav tako spreminja tobačno zakonodajo, v katero vključuje direktive EU ter dodaja še niz nacionalnih ukrepov. Temeljni poudarki sprememb se nanašajo na uvajanje licenc in licenčnine za prodajo tobaka, večjo obdavčitev tobaka, prepoved oglaševanja in prikazovanja na prodajnih mestih in standardizirano embalažo.

Žal več dejstev glede trenutnega spreminjanja tobačne zakonodaje v Sloveniji kaže na to, da tudi Slovenija ni izbrala načina iskanja sinergijskega učinka, temveč bolj kot ne, načrtuje in predlaga neusklajene ukrepe in s tem povečuje nevarnost, da se na določenih drugih področjih povzroči določena tveganja in grožnje. V ponazoritev navajamo nekaj konkretnih dejstev:

- Ministrstvo za zdravje v novem predlogu tobačne zakonodaje predlaga uvedbo licenc za prodajalce cigaret, a ni pojasnilo kakšen je postopek pridobitve licence, kolikšna bo višina licenčnin, kam se bo denar iztekal in kdo ga bo upravljal. Primeri iz Madžarske in Irske kažejo, da lahko uvedba licenčnin celo poveča delež nezakonite trgovine s tobačnimi izdelki in vodi do korupcije pri podeljevanju licenc.
- Eden od argumentov Ministrstva za zdravje v predlogu sprememb zakonodaje je, da se delež kadilcev v zadnji letih povečuje, po podatkih, ki jih zbira finančna uprava RS, pa delež prodanih cigaret zadnja leta pada, kar je izključujoče.
- Večja obdavčitev tobaka pogosto ne vodi v zmanjševanje števila kadilcev ampak v povečan obseg nezakonite trgovine s tobačnimi izdelki. Na račun vse večje obdavčitve in trenutne gospodarske klime, kjer je brezposelnost še vedno visoka, iščejo kadilci cenejše alternative legalnemu tobaku in cigaretam. Po podatkih KPMG nezakonita trgovina s cigaretami v Sloveniji narašča že četrto leto zapovrstjo, letni davčni izpad zaradi tihotapljenja cigaret znaša kar 31 milijonov evrov. Poleg vpliva na izpad prihodkov države in negativnega vpliva na javno zdravje, nezakonita prodaja cigaret ogroža tudi nacionalno varnost. Po poročilu o nelegalni trgovini (WCO Illicit Trade Report 2012) naj bi bilo prekupčevanje s cigareti, poleg prekupčevanja z drogo, eden izmed glavnih virov financiranja terorističnih aktivnosti.
- Da zgolj prepoved oglaševanja in prikazovanja na prodajnih mestih ne prinaša želenih rezultatov, nazorno kaže primer Nemčije, kjer je oglaševanje dovoljeno, kljub temu pa ima nizko stopnjo kajenja med mladimi, saj veliko namenijo preventivi in izobraževanju, zakonodaja pa je veliko manj restriktivna kot v nekaterih drugih državah z naraščajočimi deleži kadilcev. Nemčija je tudi primer države, ki se problematike kajenja med mladimi loteva z učinkovitimi izobraževalnimi programi, ki nagovarjajo bistvene vzroke za začetek kajenja med mladimi, kot so uporništvo, pritisk sovrstnikov, zgledovanje po starših ter nizka samopodoba.

Glede na način spreminjanja tobačne zakonodaje v Sloveniji, se nam na podlagi trenutnega stanja postopka, upravičeno poraja bojazen, da bo tudi na tem področju prišlo do sprejemanja nedorečenih, neusklajenih in s tem tudi problematičnih rešitev, ki tako kot v zgoraj omenjenih primerih, ne bodo rešile te problematike, temveč bolj kot to, ustvarile dodatne probleme in stopnjevale nekatere od oblik ogrožanja.

- Domnevo, da bo standardizirana embalaža učinkovita, v določeni meri negirajo zadnje raziskave v Avstraliji, ki je prva uvedla standardizirano embalažo leta 2012. Rezultati namreč kažejo, da ni dokaza, da bi standardizirana embalaža vplivala na zmanjševanje kajenja, saj se je po uvedbi ukrepa delež kadilcev med mladimi povečal, ravno tako pa se je povečal tudi obseg nezakonite trgovine s tobačnimi izdelki.

Glede na način spreminjanja tobačne zakonodaje v Sloveniji, se nam na podlagi trenutnega stanja postopka, upravičeno poraja bojazen, da bo tudi na tem področju prišlo do sprejemanja nedorečenih, neusklajenih in s tem tudi problematičnih rešitev, ki tako kot v zgoraj omenjenih primerih, ne bodo rešile te problematike, temveč bolj kot to, ustvarile dodatne probleme in stopnjevale nekatere od oblik ogrožanja. Vsa zgoraj našteta dejstva več kot nazorno kažejo na to, da spreminajnje tako kompleksega področja, ne more in ne sme biti stvar Ministrstva za zdravje, temveč morajo pri tem sodelovati tudi ostali deležniki, od izobraževanja, financ, gospodarstva in nenazadnje nacionalno varnostnega sistema.

Spreminjanje zakonodaje glede orožja

Podoben primer ne dovolj premišljenih in neusklajenih predlogov sprememb zakonodaje, trenutno poteka v procesu spreminjanja predpisov na področju orožja v Sloveniji. Nesporno je, da orožje predstavlja določen varnostni problem, da je z njim mogoče storiti najhujša kazniva dejanja, ter bi omejevanje dostopnosti gotovo pripomoglo tudi k zmanjševanju ogroženosti in kriminalitete. Vendar se je tudi k reševanju tega problema pristopilo enostransko, nepremišljeno, brez upoštevanja mnenj ostalih deležnikov (strelska društva, lovci..) ter njihovega aktivnega vključevanja v iskanje primernih in celovitih rešitev. Predlogi sprememb so usmerjeni zgolj v legalni trg in lastnike posameznih vrst orožja, za katerega imajo vsa ustrezna dovoljenja. Predlogi ne zajemajo ukrepov, ki bi omejili črni trg in tihotapljenje orožja, kljub dejstvu, da je velika večina kaznivih dejanj, vključno s terorizmom, storjena z orožjem s črnega trga. Ukrepi bodo tako prizadeli zgolj trgovce in imetnike legalnega orožja, ki so že do sedaj pod nadzorom, nikakor pa ne bodo rešili izvirnega problema, orožja in njegove dostopnosti na črnem trgu.

Zaključek

Na podlagi analize ugotovljenih virov ogrožanja v globalnem, regionalnem in nacionalnem okolju, lahko ocenimo, da so varnostne razmere zaenkrat ugodne in obvladljive ter, da je stopnja ogroženosti Republike Slovenije nizka. Obstajajo pa nekateri indikatorji, da se lahko, na določenih področjih tako stanje zelo hitro poslabša.

Upravljanje oziroma obvladovanje različnih groženj je potrebno obravnavati s sistemskim in z logističnim pristopom. Sistemsko razmišljanje brez pretiranega poenostavljanja, ter poudarjanjem nujnosti upoštevanja etike soodvisnosti in interdisciplinarnega sodelovanja zagotavlja, da bo spregledov pomembnih dejavnikov čim manj, s tem pa bo tudi zagotovljena uravnoteženost in zadostnost sprejetih ukrepov. Na ta način dosežemo potrebno sinergijo različnih področij, usmerjenih k istemu cilju.

Pri načrtovanju ukrepov za obvladovanje groženj in tveganj, se je potrebno izogibati prekomernim ukrepom, saj ti spreminjajo sprejemljiva sorazmerja med koristmi in posledicami. Prav tako



lahko izzovejo negativne vplive v regiji, kar samo po sebi pomeni pojav nove varnostne grožnje. Odgovor na te dileme se ponuja v takem načinu delovanja, da na trenutne realne in dejanske grožnje odgovori nacionalno varnostni sistem s svojimi specializiranimi službami. Sistemsko in normativno urejanje področja obvladovanja tveganj in groženj pa je potrebno obravnavati interdisciplinarno, premišljeno, s sodelovanjem vseh deležnikov na katere se grožnje ali ukrepi za njihovo obvladovanje nanašajo ali na njih kakorkoli vplivajo.

Menimo, da bi poleg rednih odborov Vlade Republike Slovenije, Svet za nacionalno varnost moral obravnavati in usklajevati vse predpise, ki se dotikajo tveganj in groženj na področju organiziranega kriminala, tihotapstva, zdravja, farmacije, transporta itd. Skratka, poleg ostalih koordinacij v Vladi RS, je potrebno tudi »on line« delovanje Sveta za nacionalno varnost. Poleg tega je potrebno izboljšati tudi komunikacijo z nevladnim sektorjem in gospodarstvom, ki večkrat neposredno prej začuti posledice nekoordiniranega delovanja.

Viri:

- Cooper, A.; Witt, D. (2008). The linkage between tax burden and illicit trade of excisable products: the example of tobacco, World Customs Journal, http://www.worldcustomsjournal.org/media/wcj/-2012/2/Cooper_Witt.pdf
- Davidson, S. (2016). Does nobody ever check the numbers?, http://catallaxyfiles.com/2016/01/29/does-nobody-ever-check-the-numbers/
- Illicit Trade Report 2012, World Customs Organization, https://www.google.si/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=WCO+Illicit+Trade+Report+2012
- Letno poročilo KPMG 2015; http://kpmg.co.uk/creategraphics/2015/06_2015/CRT026736/index.html
- Drogen und Suchtbericht 2015, www.drogenbeauftragte.de)
- Obdavčitev tobaka in nezakonita trgovina (2012). Projekt »TobTaxy – Making Tobacco Tax Trendy«
- http://sfp.tttp.eu/sites/sfp.tttp.eu/files/SFP%20KIT_SL_v1.pdf
- Savona, E. et all. (2015). European Outlook on the Illicit Trade in Tobacco Products, Joint Research Centre on Transnational Crime, Università Cattolica del Sacro Cuore di Milano – Università degli Studi di Trento. http://www.transcrime.it/pubblicazioni/european-outlook/
- Smuggling and cross-border shopping of tobacco products in the European Union, a report for the Health Education Authority, London, http://www.ash.org.uk/files/documents/ASH_256.pdf. ■



Avtorja: Kristina Preininger, Muzejska svetovalka – Narodna galerija
Samo R. Zorko, Varnostni manager – Zarja Elektronika





VAROVANJE UMETNIŠKE IN KULTURNE DEDIŠČINE ZAHTEVA ZELO ODGOVOREN PRISTOP

Narodna galerija je osrednja nacionalna ustanova za starejšo umetnost v Sloveniji, ki hrani največjo zbirko likovnih del na slovenskem ozemlju od visokega srednjega veka do 20. stoletja. Začetki Narodne galerije segajo nekaj manj kot 100 let nazaj, ko je bilo ustanovljeno društvo Narodne galerije.

Pred obnovo je imela Narodna galerija na voljo razstavne prostore v Narodnem domu (stalna zbirka in galerija Narodni dom), v t.i. Ravnikarjevem krilu (stalna zbirka in razstavišče za občasne razstave) in v vhodni avli (razstavišče za kiparske in oblikovalske razstave). Po nedavni otvoritvi obnovljenega Narodnega doma pa so vzpostavljene nove razstavne površine v bivših prostorih telovadnega društva (za stalno zbirko in za občasne razstave), novi prostori za izobraževalne dejavnosti (Galova kamra, ustvarjalna delavnica, grafični atelje in predavalnica), nove restavratorske delavnice in novi servisni prostori.
Poleg zdajšnje zaključene modernizacije vseh prostorov v stari palači, je bilo za Narodno galerijo leto 2001 morda najpomembnejše prelomno leto, saj se je takrat končala gradnja nove vhodne avle, delo avtorjev Sadar Vuga Arhitekti. S trenutno modernizacijo prostorov v stari palači je Slovenija dobila sodoben muzej, ki ustreza visokim standardom za predstavljanje umetnostnega gradiva. Tako je te dni Narodna galerija odprla nove naloge in oblike posredovanja kulturne dediščine v svetu spreminjajočih se razmerij med gledalstvom in muzejskimi ustanovami katero bo – tako kot vsem nacionalnim galerijam po svetu – določil in izoblikoval le čas. Pridobljene so nove gmotne možnosti za izvajanje temeljne, davnega leta 1918 zastavljene naloge: varovati umetniško dediščino slovenskega naroda in jo na vrhunski strokovni ravni posredovati javnosti.

Diskretno, a nič manj zanesljivo

Pri obnovi najstarejšega objekta Narodne galerije, Narodnega doma, je sodelovalo tudi kamniško podjetje ZARJA Elektronika. Podjetje ima veliko izkušenj in znanj pri obnovi zgodovinskih, kulturnih, umetnostnih in sakralnih objektov. Svoje sisteme tehničnega varovanja je vgradilo v številne cerkve, muzeje, spominske sobe pa tudi v zasebne zbirke različnih umetniških del.

Kot zanimivost velja omeniti, da je bil Narodni dom prva javna stavba v Ljubljani z električno osvetljavo, drugim je v tistem času svetlobo še vedno zagotavljal plin. Prav tako pa je bila ta palača tudi prva javna zgradba s samo slovenskim napisom.

Pri obstoječih stavbah ne moremo vplivati na požarne lastnosti gradbenih materialov in oblog, požarno odpornost konstrukcij, odmike od sosednjih stavb, obliko in velikost dovoznih poti, intervencijskih površin ... Če stavbo uporabljamo kot muzej ali knjižnico, ji dodamo tudi vlogo skladišča premične materialne dediščine. To pa seveda pomeni tudi večjo požarno obremenitev in večje tveganje.

Eden izmed referenčnih objektov podjetja je tudi hiša znamenitega arhitekta Jožeta Plečnika v Ljubljani. Vgradnja tehničnih rešitev v objekte umetniškega in kulturnega pomena zahteva posebne spretnosti in veščine, saj so objekti navadno starejšega datuma, gradbeni materiali so bolj krhki in se hitreje poškodujejo. Takšna dela so nemalokrat že na meji z restavratorstvom. Zelo pomemben je tudi estetski vidik vgrajenih komponent, ki morajo biti v »ozadju«, v ospredju je umetnost in kulturna dediščina, kljub temu pa morajo v primeru grožnje (požar, vlom, poplavitev ...) brezhibno opravljati svojo primarno nalogo. Številni proizvajalci komponent tehničnega varovanja (Tecnoalarm - Pininfarina, Apollo – Soteria ...) zato sodelujejo z znanimi industrijskimi oblikovalci, da barvno in oblikovno zadovoljivo tudi najbolj petične uporabnike in njihove okuse. Tudi v Narodnem domu je bilo potrebno izgledu in namestitvi vgrajenih kompo-



nent nameniti posebno pozornost, saj so morali biti diskretno in nevsiljivo nameščeni v arhitekturno in umetniško dovršene sobane Narodne galerije. Nameščeni sistemi tehničnega varovanja ZARJE Elektronike v omenjenem objektu so videonadzor, sistem zaznavanja, javljanja, alarmiranja in gašenja požara, protivlomno varovanje, pristopna kontrola ter registracija delovnega časa. Avtomatsko gašenje je izvedeno v prostorih, kjer je požarna ogroženost večja. To so prostori v kleti: depo papirni fond, karantena za zaplinjevanje in lakirnica. Za gašenje je uporabljeno »čisto« gasilo Novec, ki ob gašenju ne povzroči nobene škode, prijazno pa je tudi do okolja (ODP – »Ozone Depletion Potential = 0«), kar pomeni, da nima škodljivega učinka na ozonski plašč stratosfere.

Poleg vseh omenjenih tehničnih sistemov, je vgrajeno tudi posebno varovanje, ki zaznava premike oziroma odstranitev vsakega posameznega eksponata (slike, kipa, skulpture). Takšnih tipal je nekaj manj kot 700, nameščena so diskretno. Hkrati morajo biti dovolj robustna, da jih ne sproži mimohod obiskovalca (skupine) in občutljiva, da učinkovito, pravočasno in zanesljivo zaznajo vsak »sumljiv« poseg v razstavni prostor posameznega eksponata.

Vgrajen požarni sistem NJP-400A je rezultat lastnega razvoja in proizvodnje, zaradi združljivosti pa je bila zamenjana tudi obstoječa požarna centrala v novem delu, NJVP-300A. V celotnem kompleksu Narodne galerije so tri Zarjine centrale, ki so med seboj povezane z redundančno mrežo ZarjaNet. Vse informacije v zvezi s požarnim javljanjem so tako poenotene in prikazane na vseh treh centralah. Apollo javljalniki v novem delu so ostali isti in so se le prenaslovili v skladu z novim sistemom NJP-400A. Angleški Apollo je Zarjin dolgoletni parter, saj so njegovi požarni javljalniki zanesljivi, robustni in uporabni v zelo širokem spektru aplikacij. »Prepričani moramo biti mi, predvsem pa naši uporabniki, da komponenta ne bo odpovedala v najbolj kritičnih situacijah«, pravijo v ZARJI Elektroniki. »To za proizvajalca Apollo vsekakor lahko trdimo, pomembna pa je tudi njegova vsestranska tehnična pomoč in podpora«, še dodajajo.

Posebno vlogo in pomen na objektu ima AMS – Alarm Management Sistem, ki vse sisteme integrira in poveže v celoto. Vsa varnost celotnega objekta je tako skoncentrirana na en zaslon, kar je bil cilj na začetku projekta. Tak pristop ima številne prednosti glede enostavnosti upravljanja, vzdrževanja in seveda stroškovne učinkovitosti.

Posebno vlogo in pomen na objektu ima AMS – Alarm Management Sistem, ki vse sisteme integrira in poveže v celoto. Vsa varnost celotnega objekta je tako skoncentrirana na en zaslon, kar je bil cilj na začetku projekta. Tak pristop ima številne prednosti glede enostavnosti upravljanja, vzdrževanja in seveda stroškovne učinkovitosti. Zelo pomembno je tudi dejstvo, da je AMS lasten produkt podjetja, kar pomeni hitro, prilagodljivo in učinkovito implementacijo uporabnikovih želja v delovanje sistema. Alarmni signal se prenaša na Policijo in v Varnostno nadzorni center.

AMS uporabniška izkušnja

AMS (angl. Alarm Management System) omogoča nadzor različnih sistemov (npr. požarni, vlomni, video, kontrola dostopa, registracija delovnega časa, varovanje eksponatov ...) preko grafičnega uporabniškega vmesnika (angl. Graphical User Interface - GUI), ki uporabniku zagotavlja večjo preglednost, boljši nadzor in hitrejše reagiranje. Preko GUI uporabnik lahko spremlja dogajanje na sistemih v realnem času na zelo pregleden način, zaledna logika AMS pa zagotavlja, da je uporabnik v nekem trenutku osredotočen na trenutno najpomembnejše dogodke in uporabnika usmerja v pravilno ravnanje, tako da lahko s tem prepreči marsikatero neprijetno situacijo. Poleg spremljanja dogajanja pa je v realnem času možno tudi upravljanje s sistemi, tako da lahko uporabniki v dani situaciji reagirajo hitreje tudi v primeru, če se sistemi nahajajo na različno oddaljenih lokacijah oziroma da do sistemov nimajo fizičnega dostopa. Pri razvoju AMS so razvojni arhitekti podjetja sledili najsodobnejšim trendom razvoja programske opreme, saj je bila aplikacija razvita s strani inženirjev z bogatimi izkušnjami na področju razvoja sistemskih rešitev. AMS je zasnovana kot spletna (ang. Web) aplikacija, kar prinaša še boljšo uporabniško izkušnjo in preprostejšo uporabo, saj lahko uporabnik do aplikacije dostopa kar preko spletnega brskalnika (angl. Web Browser) na računalniku, tablici, mobilnem telefonu itd. kjerkoli in kadarkoli. Ker je aplikacija nameščena na spletnem strežniku (angl. Web Server), uporabnikom aplikacije ni potrebno posebej nameščati, sama uporaba aplikacije je neodvisna od operacijskega sistema, naenkrat pa do aplikacije dostopa (teoretično) neomejeno število različnih uporabnikov, ki imajo vnaprej določena pooblastila (prijava poteka na osnovi uporabniškega imena in gesla). Dostop do aplikacije je možen preko lokalnega omrežja (LAN) znotraj objektov na isti lokalni mreži kot tudi globalnega omrežja (WAN), če se naročniku to zdi potrebno in smiselno. Zaledna komunikacija s sistemi poteka po različnih protokolih (npr. Modbus TCP), ki omogočajo nemoteno in zanesljivo delovanje. Tudi sama izgradnja dejanskega stanja različnih sistemov v nekem prostoru poteka preko spletne aplikacije in omogoča zelo hitro delo, saj so bila pri razvoju upoštevana vsa mnenja in predlogi za izboljšave ostalih podobnih aplikacij s strani uporabnikov, ki se s tem ukvarjajo že mnogo let. Seveda pa aplikacija omogoča tudi pregled arhiva dogodkov, sledenje uporabnikovim akcijam, iskanje elementov, različne stopnje obveščanja preko elektronske pošte ali SMS sporočil itd. Pri nadaljnjem razvoju aplikacije je primarni cilj podpreti še več različnih sistemov, s tem postati še bolj prilagodljivi in v prihodnosti vodilni na področju upravljanja s sistemi preko grafičnega nadzornega centra.

Obseg in potek del v Narodnem domu

ZARJA Elektronika se je z nameščanjem tehničnih rešitev v objekt vključila proti koncu leta 2014, ko je bila končana glavnina restavratorskih del in je bil tehničnemu osebju omogočen dostop za vgradnjo oziroma nadgradnjo žičnih povezav. Projekt je moral biti dokončan v rokih, saj je bil datum odprtja Narodnega doma določen in znan vnaprej. Tehničnih izzivov je bilo več, največji so bili zastarele instalacije, ki niso ustrezale standardom, menjava sistema in





koordinacija z ostalimi izvajalci – restavratorji. Da je bilo pravočasno končano, so dela potekala tudi med vikendi in ponoči. Podjetje je v objektu Narodne galerije prisotno že več kot 30 let, od osemdesetih prejšnjega stoletja, s svojo tretjo generacijo požarnih central lastnega razvoja pa je prepoznano kot zanesljiv in zaupanja vreden partner. Izbor izvajalcev je potekal preko razpisa, ki je potekal v več fazah. Zadnji večji tehnični poseg na objektu je ZARJA Elektronika opravila leta 2009, ko je v manj kot dveh mesecih nadgradila protivlomni sistem, saj je postalo zakonsko določeno, da morajo imeti javne zgradbe izrednega državnega pomena stopnjo protivlomnega varovanja vsaj 3 (»Grade 3«) ali več. Pri zadnji obnovi Narodnega doma se je dograditev povezala z obstoječim sistemom in integrirala v celovito rešitev protivlomnega varovanja, ki ustreza zakonskim zahtevam, mednarodnim standardom in smernicam dobrih praks. Narodni dom je bil med obnovo zaprt, ostali deli Narodne galerije pa so obratovali normalno.

Dobre prakse so pokazale, da je stopnja zaščite sorazmerna z dobrim upravljanjem s stavbo. To vsekakor vključuje organizacijo varstva pred požarom (sistem avtomatskega zaznavanja, javljanja in alarmiranja in morebitno avtomatsko gašenje) in varovanje pred nepooblaščenim vstopom v objekt. Sistem varovanja se mora stalno vzdrževati, preverjati in nadgrajevati, za kar pa pogosto ni volje in sredstev. Obvezen je požarni načrt in navodila za ukrepanje ob nastopu kritične situacije. Posebno pozornost zahtevajo razne prireditve, povečano število obiskovalcev (turistična sezona), preurejanje prostorov in menjava razstav. Tudi v teh objektih ostajajo vroča dela (vzdrževanje, prenove) najpogostejši vzrok požarov.

Prenova stavb, kar se je zgodilo tudi v primeru Narodnega doma, je dobra priložnost za izboljšanje – nadgradnjo vgrajene požarne in tehnične zaščite. Sodelovanje strokovnjakov s področja varstva kulturne dediščine in varstva pred požari lahko pripelje do dobrih rezultatov in Narodni dom je takšen primer dobre prakse. ■

Zarja Elektronika je vodilno slovensko podjetje na področju tehničnega varovanja z delovanjem v širši regiji. Podjetje ima reference v številnih prepoznavnih slovenskih podjetjih, pa tudi v širši regiji. Eden največjih in tehnološko najzahtevnejših projektov v zadnjih letih je bil sistem gašenja z vodno meglo (angl. »water mist«) za potrebe letališča Jožeta Pučnika. Vsi projekti imajo skupni imenovalec, da je potrebno zelo veliko znanja in praktičnih izkušenj.

Varno v nov dan



Avtor: Klemen Radetič / višji strokovni sodelavec za analize prevar, Zavarovalnica Triglav, d.d.*



SODOBNI PRISTOPI PRI PREISKOVANJU PREVAR V SKUPINI TRIGLAV

O zavarovalniški prevari govorimo, kadar nekdo zavarovalnici posreduje neresnične ali napačne informacije, kadar namerno poškoduje ali uničuje stvari, kadar predloži lažne dokumente ali sklene zavarovanje po škodnem dogodku. Vse to z namenom, da bi od zavarovalnice prejel določeno odškodnino, ki je sicer ne bi dobil, če bi navajal resnične podatke.

O zavarovalniških prevarah

Ob besedi »kriminalec« večina ljudi pomisli na nekoga, ki je kradel v trgovini, vlamljal v stanovanja, oropal pošto... Vse prevečkrat pa pozabimo, da so tudi prevare v zavarovalništvu kriminalna dejanja, ki povzročajo veliko škodo. Raziskava Zavarovalnice Triglav, d.d. iz leta 2012 je pokazala, da se pravzaprav večina tega sploh ne zaveda. Pri upravičevanju je izgovor posameznika pogosto: »Saj to vsi počnejo!« in »Zavarovalnica nam mora nekaj denarja tudi vrniti!« V javnosti prevladuje mnenje, da so zavarovalniške prevare »zločin brez žrtev« in da zahtevki, ki jih vložijo goljufi, škodujejo le zavarovalnici, ne zavedajo pa se, da si ob sklenitvi zavarovalne police na nek način kupijo varnost. Glavna posledica je, da zaradi zavarovalniških prevar vsi zavarovanci plačujemo višje premije.

Association of Certified Fraud Examiners (ACFE) v svojem poročilu iz leta 2014 ugotavlja, da povprečna organizacija na račun prevar izgubi približno 5 odstotkov svojih prihodkov na leto. To predstavlja skupno več kot 3,7 trilijona dolarjev izgub na leto. Zanimiv je tudi podatek, da si skoraj polovica organizacij ni nikoli povrnila morebitnih izgub, ki so jih utrpele zaradi prevar. Po podatkih ACFE so prevare običajno ugotovljene prek namigov. Večino namigov o sumu prevare posredujejo zaposleni v organizaciji, ki je žrtev prevare. Prevare v zavarovalništvu se pojavljajo v vseh oblikah in velikostih. Lahko gre za preprosto dejanje, ki vključuje zgolj eno osebo, ali pa za kompleksno združbo, ki vključuje večje število ljudi tako znotraj kot zunaj zavarovalnice.

V Sloveniji je za zavarovalniške goljufe zagrožena kazen do enega leta zapora, če je bilo dejanje načrtovano in še ni bilo izvedeno. Če je do goljufije že prišlo, je lahko storilec kaznovan z do tremi leti zapora. Če je bila zavarovalniška goljufija storjena v okviru organizirane skupine, je kazen za posameznika še višja. V kazenskem zakoniku (KZ-1, 211.člen) je zavarovalniška goljufija kazniva, če storilec ob sklenitvi pogodbe navede lažne ali zamolči pomembne podatke, sklene prepovedano dvojno zavarovanje ali sklene zavarovalno pogodbo po nastanku zavarovalnega ali škodnega primera.

Obvladovanje prevar v Skupini Triglav

Znotraj Zavarovalnice Triglav, d.d. deluje posebna Služba za preprečevanje, odkrivanje in raziskovanje prevar (SPORP). S tem se zgledujemo po uspešnih praksah sodobnih globalnih podjetij, ki delujejo v skladu s smernicami svetovnih organizacij, kot sta ACFE in International Association of Insurance Supervisors (IAIS). Na enak način je raziskovanje zavarovalniških prevar organizirano tudi v drugih zavarovalniških družbah Skupine Triglav v Srbiji, Makedoniji, Bosni in Hercegovini, Črni gori ter na Hrvaškem. Poleg ustanovitve specializiranega oddelka smo v Zavarovalnici Triglav v zadnjih letih uvedli številne ukrepe, usmerjene v preprečevanje in odkrivanje zavarovalniških goljufij. Prva obrambna linija v boju proti prevaram so zaposleni v zavarovalnici, ki jih stalno izobražujemo o pomenu prepoznavanja

Association of Certified Fraud Examiners (ACFE) v svojem poročilu iz leta 2014 ugotavlja, da povprečna organizacija na račun prevar izgubi približno 5 odstotkov svojih prihodkov na leto. To predstavlja skupno več kot 3,7 trilijona dolarjev izgub na leto.

* Korporacijski član Slovenskega združenja korporativne varnosti

zavarovalniških prevar. V Sloveniji je v program vključenih več kot 1.500 zaposlenih na področju sklepanja zavarovanj in likvidacije škod. Izobraževanje je bistvenega pomena za osveščanje zaposlenih o negativnih posledicah goljufij in za vzpostavljanje ter negovanje kulture, v kateri zavarovalniške goljufije niso sprejemljive. Vzpostavili smo tudi t.i. Linijo za sporočanje prevar, ki je namenjena zaposlenim in eksterni javnosti za prijavo sumov prevar.

Zavarovalnica dnevno obravnava veliko število škodnih zahtevkov, vendar pa strokovnjaki za prevare ne morejo preveriti vsakega od njih, saj bi bilo to neekonomično s časovnega, stroškovnega in tržnega vidika. Na bolj razvitih zavarovalniških trgih obstajajo številne napredne rešitve, ki smo jih v Zavarovalnici Triglav že pred časom začeli prenašati v svoje delovanje. Na področju preprečevanja, odkrivanja in raziskovanja zavarovalniških goljufij smo v zadnjih letih uvedli številne novosti, s katerimi lahko hitro zaznavamo kompleksne goljufije z več udeleženci, ki se izvajajo v daljšem časovnem obdobju. Takšnih goljufij tudi zelo izkušeni cenilec ponavadi ne more zaznati. Za učinkovit boj proti zavarovalniškim goljufijam smo implementirali napredno računalniško rešitev, programsko orodje »POP modul«, ki samodejno zaznava različne sume prevar. Z IT podprtim zaznavanjem lahko analitik pregledno razporedi posamezne sumljive primere po enem ali več ključnih indikatorjih prevar, številih točk sumljivosti, vrstah zavarovanj, vrednostih ipd. Z uporabo sistemsko razvitih indikatorjev lahko že ob sklepanju posamezne zavarovalne police zaznamo povečano tveganje goljufije. Kasneje ob nastanku škodnega dogodka pa ključni indikatorji prevar omogočajo neodvisnost od prijav ali namigov cenilcev, drugih zaposlenih ali zunanje javnosti. S tem smo pridobili dodaten kanal za avtomatsko identifikacijo sumljivih škodnih primerov in omogočili njihovo pravočasno zaznavo. Preiskovalci tako lahko sami proaktivno iščemo sumljive primere in se odločamo za preiskave sumljivih primerov. Izkušnje kažejo, da se učinkovitost uspešno raziskanih primerov povečuje, če je raziskovanje usmerjeno na podlagi kompleksnih analiz množice podatkov s katerimi razpolaga organizacija. Tehnologija, ki smo jo vzpostavili, nam daje tudi usmeritve za ustrezno vzpostavljanje ključnih notranjih kontrol za preprečevanje in odkrivanje morebitnih prevar, hkrati pa omogoča tudi meriti uspešnost delovanja organizacije pri preprečevanju zavarovalniških prevar.

Pri analizi zaznanih sumov prevar se srečujemo z veliko količino podatkov, s čimer pomen pridobiva uporaba različnih računalniških orodij in analitičnega pristopa k raziskavi. Gradniki sistema »POP Modul« so različna analitična orodja, ki so standardni izdelki v globalnih industrijskih sektorjih, uporablja pa jih več kot 4500 organizacij po svetu (zavarovalne družbe, banke, obveščevalne službe, policija, vojska, uradi za preprečevanje pranja denarja itn.). Gre za orodja, ki omogočajo rudarjenje med podatki, iskanje in vizualizacijo povezav ter druge analize podatkov. Analitik z njihovo pomočjo v zelo kratkem času dobi celostno podobo o preteklem škodnem dogajanju udeleženih oseb, povezave med različnimi udeleženci škodnih dogodkov ter možnost identifikacije drugih povezanih sumljivih primerov. Ta orodja imajo poseben pomen predvsem pri razkrivanju mrež goljufov in združb, ki se načrtno ukvarjajo z zavarovalniškimi prevarami.

S spremembami navad zavarovancev ter uporabo novih tehnologij, svoj pomen izgubljajo klasični načini odkrivanja in preiskovanja prevar. Poleg podatkov s katerimi razpolaga zavarovalnica, so velike količine podatkov in sledi na voljo tudi preko javno dostopnih virov. Anali-



Na področju preprečevanja, odkrivanja in raziskovanja zavarovalniških goljufij smo v zadnjih letih uvedli številne novosti, s katerimi lahko hitro zaznavamo kompleksne goljufije z več udeleženci, ki se izvajajo v daljšem časovnem obdobju. Takšnih goljufij tudi zelo izkušeni cenilec ponavadi ne more zaznati.

za podatkov na spletu marsikdaj razkrije številne dokaze s katerimi potrdimo sum prevare.

Največ zavarovalniških prevar odkrijemo na področju avtomobilskih zavarovanj. Ravno v tem segmentu se največkrat srečamo z iznajdljivimi goljufi, ki izbirajo nove pristope lažnega prikazovanja škodnih dogodkov in fingiranja prometnih nesreč. Na srečo računalniki in tehnologija v sodobnih vozilih hranijo veliko podatkov o vozilu, napakah ki se pojavijo ob trkih, načinu vožnje in podobno. Pred kratkim smo zato pričeli z uporabo naprednega računalniškega forenzičnega orodja za odčitavanje podatkov iz vozil. Pridobljene podatke nato analiziramo in primerjamo s podatki o škodnem dogodku, kar nam pogosto pomaga pri dokazovanju suma prevare. Pozitivne izkušnje z uporabo tega orodja ima tudi nizozemska prometna policija, ki si z njim pomaga pri rekonstrukciji hujših prometnih nesreč.

S prej predstavljenimi orodji in pa analitičnim pristopom nam je uspelo identificirati tudi večje število organiziranih skupin, ki so se ukvarjale z namernim povzročanjem prometnih nesreč. Pri vsakem škodnem dogodku so se sicer pojavljale različne osebe, ki niso imele preteklega škodnega dogajanja in s tega vidika tudi niso bile sumljive. V večini primerov je šlo za mlajše udeležence (stare do 20 let), vse prometne nesreče so se zgodile v večernem času, udeležena so bila starejša in manj vredna vozila, ki so bila zavarovana mesec ali dva pred nesrečo. S pomočjo indikatorjev prevar smo hitro zaznali več podobnih primerov z istim modusom. Z nadaljnjo analizo smo identificirali organizatorje nesreč, ki so udeležencem plačali manjše zneske za sodelovanje v prevari. Medsebojne povezave in vloge so bile ugotovljene tudi z analizo številnih podatkov dostopnih na svetovnem spletu.

Pogosta shema prevar, ki jo zaznamo s pomočjo IT orodij in indikatorjev prevar so tudi namerna poškodovanja vozil. V teh primerih gre za nameščanje ukradenih delov na vozila ali uvoz že poškodovanih vozil. Goljufi nato zavarovalnici lažno prikažejo prometno nesrečo in dobijo odškodnino za nov in originalen del. Na tak način so preko trkov »legalizirali« ukradene dele vozil. To je le nekaj najpogostejših primerov s katerimi se srečujemo in kjer so nam sodobne tehnologije zaznavanja prevar in analiz podatkov v veliko pomoč. Omogočajo nam namreč, da hitro zaznamo sumljive primere, kjer se pojavlja isti modus operandi. Z analitičnim delom in zbiranjem podatkov iz naših baz ter odprtih virov (open source inteligence) in z zbiranjem podatkov na terenu pa te združbe identificiramo. S takšnim načinom dela smo izboljšali učinkovitost, resurse strokovnjakov za preiskave prevar pa usmerjamo v primere goljufij, ki so najbolj škodljivi za zavarovalnico (in zavarovance).

Zaradi dobrih rezultatov v matični družbi v Sloveniji, smo z implementacijo podobnih sistemov avtomatskega zaznavanja prevar začeli tudi v odvisnih zavarovalniških družbah na tujih trgih. Goljufi pa seveda ne počivajo. Pri svojem delu so iznajdljivi in iščejo vedno nove načine kako priti do denarja, zavarovalnice pa so pred stalnim izzivom kako odkriti čim več goljufivih odškodninskih zahtevkov. Sistem indikatorjev prevar je tako potrebno redno posodabljati na podlagi izkušenj iz preiskav in ga prilagajati novim pristopom goljufov. ■



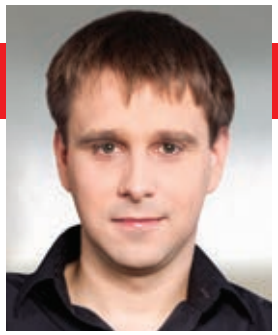


Skupina Triglav

triglav

Vse bo v redu.
www.triglav.eu

Avtor: Gregor Spagnolo, Biokoda d.o.o.



NAIVNOST PRI UPORABI SPLETNIH KOMUNIKACIJSKIH PROGRAMOV

Ko je govora o varnosti, je najpogostejša prva misel fizično varovanje, v primeru informacijskih tehnologij pa antivirusni programi, požarni zidovi, najrazličnejši sistemi za zaznavanje vdorov in tako naprej. Seveda je za zaščito podjetja zgoraj omenjen pristop pravilen in v skladu z dobrimi praksami. Kljub temu pa v podjetjih še vedno obstajajo varnostne vrzeli.

Pri pogovorih z varnostnimi inženirji zmeraj pridemo do zaključka, da je glavna težava pri varovanju sistemov in informacij ravno človek, saj preko zaposlenih v podjetjih uhaja največ informacij. Seveda se tega sploh ne zavedajo in podatki najpogosteje uhajajo preko komunikacijskih medijev, kot so elektronska pošta, telefonski pogovori, oziroma programi za komunikacijo, na primer Skype, Whats app in podobni.

Dandanes se večina ljudi zaveda, da se telefonskim pogovorom prisluškuje in je potrebno poiskati alternativne sisteme za komunikacijo. Tudi to je eden izmed razlogov, da se vse seli na splet, zaradi česar je število in uporaba spletnih komunikacijskih orodij v zadnjih letih skokovito narasla.

Sama uporaba spletnih komunikacijskih programov je postala priljubljena predvsem zato, ker je komunikacija tako rekoč brezplačna. Vse kar je potrebno je le, da imajo uporabniki povezavo do interneta. Vendar pa na žalost pri večini tovrstnih orodij obstajajo zanke, ki jih večina ne pozna.

Vzemimo za primer prisluškovalno afero, ki je v slovenskih medijih odmevala ne dolgo nazaj. Uporabnika sta uporabljala brezplačno aplikacijo za komunikacijo, ki pa ni šifrirala vsebine pogovorov. Zakaj sta uporabljala aplikacijo, ki ne nudi nobene stopnje varnosti, je jasna. Bila je enostavna za uporabo.

Ali varna aplikacija omogoča tudi zasebnost?

Kako je do tega pravzaprav lahko prišlo, če sta uporabljala program, ki naj bi zagotavljal varnost? Že, res, da pogovorni program, ki sta ga uporabljala zagotavlja varnost, vendar pa varnost ne pomeni zmeraj tudi zasebnosti. Varnost namreč predstavlja zaščito pred morebitnimi napadalci, ne pa tudi zasebnosti pred obveščevalnimi službami in raznimi drugimi organi, ki nam načeloma ne želijo povzročiti škode, kljub temu pa beležijo naše pogovore.

Meja med varnostjo in zasebnostjo je namreč tanka ter težko ločljiva. Nekateri za dovolj varno in zasebno smatrajo že komunikacijo preko SSL povezave. Seveda je taka zaščita povsem dovolj za varen in zaseben dostop do spletnih omrežij, vendar ne predstavlja nikakršne zaščite pred raznimi vladnimi organi ali industrijskim vohunjenjem.

Kaj pa je dovolj varno? Kako ta način uhajanja informacij preprečiti? Večina podjetij se zaveda, da v primerih, ko govorimo o vladah ali velikih korporacijah, zlonamerne kode niso namenjene kraji denarja, temveč pridobivanju informacij. Pomembno je torej najti način, kako zaščititi informacije, poleg tega pa tudi kako zaščititi našo intelektualno lastnino. V Ameriki se na ta račun že vrstijo tožbe proti Kitajskim podjetjem, ki so ukradla različne pomembne informacije, kot so

Dandanes se večina ljudi zaveda, da se telefonskim pogovorom prisluškuje in je potrebno poiskati alternativne sisteme za komunikacijo.

sama programska koda ali celo načrti za izdelavo določenih izdelkov. Vzemimo za primer podjetje AMSC. Podjetje, ki izdeluje vetrne elektrarne, se je znašlo na robu stečaja, pri čemer so bili primorani odpustiti več tisoč delavcev samo zato, ker jim je Kitajsko podjetje Sinovel ukradlo celotno programsko kodo. Ampak ali problem predstavljajo zgolj Kitajci in njihovo t.i. industrijsko vohunjenje? Še zdaleč ne. Enako počnejo tudi druge velike države kot je Amerika. Bistven porast zavedanja o razsežnostih trgovanja z informacijami je povzročil Edward Snowden, ki je javnosti razkril s koliko in katerimi informacijami razpolaga NASA in kako z njimi trguje. Z njegovim razkritjem je bila širša javnost seznanjena s tem, da se ne trguje samo z informacijami, ki so pomembne ‚zgolj' za državno varnost, temveč segajo tudi na teritorije velikih podjetij in korporacij.

Zapletena zaščita, ki je velik finančni zalogaj.

Ob omembi zaščite programov, pomislimo na kompleksne sisteme, zapletene za uporabo, ter grafične vmesnike, ki so daleč od pozitivne uporabniške izkušnje, če sploh obstajajo. Sistem za zaščiteno komunikacijo, kot je PGP, je za povprečnega uporabnika zapleten. Predstavljajte si, da vse svoje zaposlene peljete skozi postopek učenja PGP-ja. Ob tem pa ne smemo pozabiti, da je potrebno v enak sistem vpeljati tudi vse poslovne partnerje vašega podjetja. Po že omenjenem razkritju Snowdena, so se razmahnili Cryptu Party dogodki, na katerih ljudi osveščajo in učijo, kako varno uporabljati telefone, elektronsko pošto in druge komunikacijske kanale. Vendar z Biokodo takšno učenje ni potrebno, kajti v našem podjetju smo naredili produkt, ki uporablja trenutno najvišjo kriptografsko priznano in overjeno stopnjo zaščite in kar je najpomembneje, uporabniku prijazen grafični vmesnik. Biokoda omogoča stopnjo varnosti komunikacije, ki je do zdaj bila mogoča samo na najvišjih nivojih določenih držav. Podjetja in vlade želijo lastno gostovanje Produkt Biokoda je zasnovan tako, da omogoča on-premise in oblačne postavitve. Podjetje lahko samo gostuje, strežnik skrbi za administracijo in zadrži vse podatke pri sebi. Vsa podjetja, ki uporabljajo Biokoda sistem, se lahko povežejo med seboj, če to želijo. Zaposleni v enem podjetju lahko vzpostavijo kontakt z zaposlenimi drugega podjetja. Biokoda sistem vsakega podjetja bo zase zadržal vse podatke in ne bo razkril niti IP naslova klicatelja drugega podjetja. Vsako podjetje se lahko odloči, če želi dovoliti komunikacijo z Biokoda javnim oblakom. Tako se lahko uporablja varna Biokoda komunikacija tudi z osebami, ki nimajo lastne namestitve. Uporaba globalnega Biokoda oblaka je brezplačna za individualne uporabnike.

Poglejmo še na področje vladnih institucij. Varna komunikacija med vladnimi organi je na zelo nizkem nivoju, saj se uporablja zgolj v določenih primerih. Določeni segmenti vlade imajo sicer svoje varnostne rešitve, vendar pa so se nekatere izkazale za neprimerne in drage. S sistemom Biokoda, ki deluje na že obstoječi infrastrukturi, lahko določena vladna institucija varno interno komunicira, prav tako pa je poskrbljeno za varno komunikacijo z drugimi institucijami. Če vzamemo za primer begunsko krizo, bi lahko z Biokoda aplikacijo, policija, vojska in gasilske enote komunicirali popolnoma varno, brez možnosti prisluškovanja.

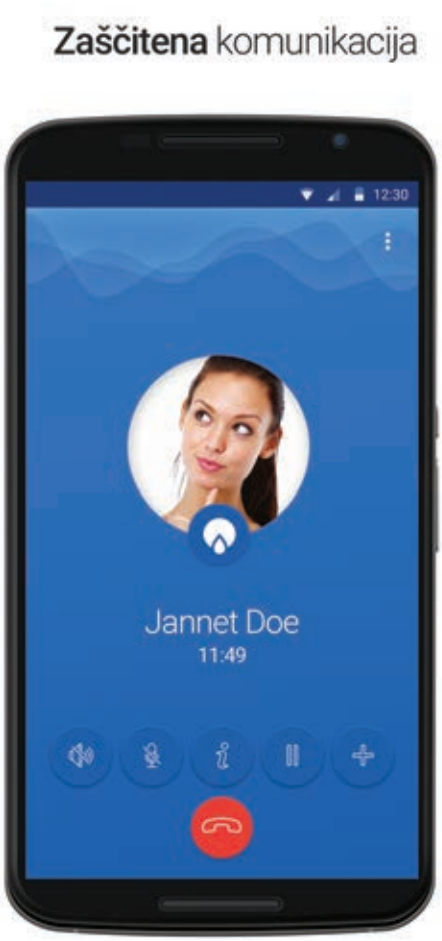
Jedro Biokode temelji na šifrirnem protokolu, ki ob vsaki akciji pošiljanja in prejemanja spreminja trenutno stanje ključev šifrirnega kanala.

Vzpostavitev šifriranega kanala temelji na izmenjavi večih javnih delov eliptičnih šifrirnih ključev in uporabi psevdo-naključnih funkcij za izpeljevanje šifrirnih ključev. Vsak paket, poslan po mreži, uporablja nov izpeljan šifrirni ključ, ki izhaja iz trenutnega stanja šifrirnih ključev za izpeljevanje. Ob prejemu paketa, se le-ta odšifrira in pripravi stanje šifrirnega kanala tako, da se ob naslednjem poslanem sporočilu s strani prejemnika pripravijo novi ključi za izpeljevanje šifrirnega ključa.

Biokoda ob vseh naprednih šifrirnih mehanizmih uporablja tudi najbolj napredni zvočni kodek, ki je visoko-toleranten na izgube paketov na omrežju. Zvočni kodek je bil dodatno nadgrajen s samodejnim zaznavanjem kvalitete podatkovne povezave. Tako odjemalec samodejno prilagodi izhodno količino podatkov ter kvaliteto zvoka glede na razmere na omrežju.

Biokoda (Biocoded) aplikacija je na voljo za Android in Apple mobilne naprave. Sama namestitev in uporaba sta brezplačni. ■

Biokoda omogoča stopnjo varnosti komunikacije, ki je do zdaj bila mogoča samo na najvišjih nivojih določenih držav.



BIOKODA





— 1. —

Šifrirano sporočanje

- Tekstovna sporočila
- Glasovna sporočila
- Slike
- Deljenje datotek



— 2. —

Šifrirani glasovni klici

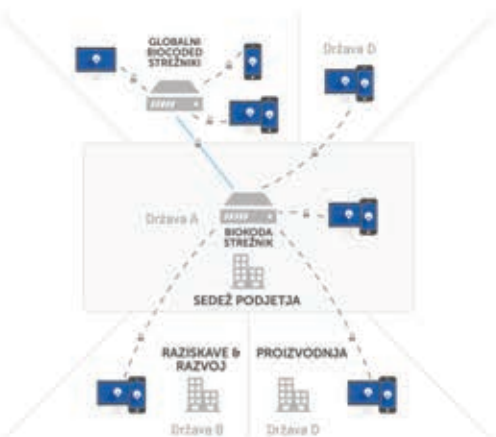
- Wi-Fi
- 3G/4G/LTE
- Nizka poraba podatkov



— 3. —

Napredne možnosti komuniciranja

- Samouničljiva sporočila po preteku časa
- Integrirana kamera za zajem slik
- Identifikacija šifrirnih ključev glasovnega klica



— 4. —

Namestitev na **vaši infrastrukturi**

- Povezljiva z drugimi namestitvami
- Povezljiva z globalnim Biocoded oblakom
- Namestitev pod vašo varnostno politiko

Prenesi aplikacijo

https://www.biocoded.com/get/kv

biokoda®

Avtor: Rok Novak / Reisswolf Slovenija*



OPTIMIZACIJA PROCESOV UPRAVLJANJA Z DOKUMENTACIJO IN ARHIVSKIM GRADIVOM

Pri vzpostavljanju sistema upravljanja z dokumentacijo in arhivskim gradivom v arhivih je poleg zakonodaje, standardov in varnostnih zahtev, ki smo jih predstavili že v prejšnji številki revije Korporativna varnost, velik poudarek potrebno posvečati tudi ekonomskemu vidiku upravljanja.

Dejstvo je namreč, da se v večini organizacij temu vprašanju še vedno posveča bistveno premalo pozornosti, zato upravljanje z dokumentacijo in arhivi praviloma ni učinkovito in organizacijam povzroča bistveno previsoke stroške. Zakaj je temu tako? Razlogi za to se po naših izkušnjah kažejo predvsem v nezainteresiranosti lastnikov in poslovodstev za celovito urejanje področja upravljanja z dokumentacijo in arhivi, zaradi njihovega nepoznavanja stroke in možnih rešitev in predvsem tudi zaradi prikritih stroškov upravljanja z dokumentacijo in arhivi. Lastniki in poslovodstva enostavno ne prepoznajo dodane vrednosti, ki jim jo lahko za organizacijo prinaša urejen sistem upravljanja z dokumentacijo in arhivi. Gre za ustvarjanje dodane vrednosti iz različnih vidikov upravljanja kot npr.: vidik zakonitosti upravljanja z dokumentacijo in arhivi, vidik celovitosti, ki zagotavlja celovito in sistemsko upravljanje z dokumentacijo na vseh nivojih delovanja organizacije, varnostni vidik, ki organizacijam zagotavlja varno upravljanje z dokumentacijo, časovni vidik, ki organizacijam skrajšuje in poenostavlja postopke upravljanja z dokumentacijo ter nenazadnje ekonomski vidik, ki organizacijam zmanjšuje stroške upravljanja z dokumentacijo in povečuje dobiček na dolgi rok. Torej, kot smo že dejali, lahko celovito upravljanje z dokumentacijo in arhivskim gradivom v arhivih, organizacijam bistveno povečuje učinkovitost delovanja ne tem področju in posledično zmanjšuje stroške poslovanja na tem področju tudi za več kot 50%.

Lastniki in poslovodstva enostavno ne prepoznajo dodane vrednosti, ki jim jo lahko za organizacijo prinaša urejen sistem upravljanja z dokumentacijo in arhivi.

Ko govorimo o celovitem upravljanju z dokumentacijo in arhivskim gradivom v arhivih razmišljamo o celovitem procesu upravljanja z dokumentacijo od njenega nastanka, arhiviranja pa vse do varnega uničenja. V osnovi govorimo o treh stebrih upravljanja in sicer: tekočem uničevanju dokumentacije in čiščenju arhivov (izločanju arhivskega gradiva za uničenje), tekočem upravljanju z dokumentacijo in upravljanju z arhivi dokumentacije v fizični obliki ter upravljanju z dokumentacijo v elektronski obliki.

Pomembno je, da se uporabnikom zagotavlja vse tri omenjene stebre upravljanja z dokumentacijo in arhivi in jim na ta način omogočamo doseganje dodanih vrednosti prav na vseh področjih upravljana z dokumentacijo in arhivi. Zavedati se je potrebno sodobnih trendov in potreb uporabnikov zato je ključna ciljna naravnanost in fleksibilnost pri zagotavljanju njihovih še tako specifičnih potreb in zahtev. Dejstvo je namreč, da moderno elektronsko poslovanje narekuje nove pristope pri upravljanju z dokumentacijo in arhivi, pa vendar se hkrati tudi zavedamo, da se kljub napovedim še vedno posluje z dokumenti v klasični

* Korporacijski član Slovenskega združenja korporativne varnosti



(fizični) obliki. Celo nasprotno, beleži se namreč porast števila dokumentov v papirni obliki, saj jih je z računalniki lažje kreirati. Po nekaterih napovedih naj bi v Evropi poraba belega papirja še nekaj let rasla. Povprečni zaposleni še vedno ustvari 20.000 dokumentov v enem letu in za upravljanje z njimi porabi tudi do polovico svojega delovnega časa.

Profesionalno upravljanje dokumentov in arhivov ter njihovo varno uničevanje, lahko organizacijam prihrani veliko časa in denarja. Pri tem je izjemnega pomena tudi ekološki vidik (1 tona recikliranega papirja reši 7 manjših dreves) takega poslovanja, saj so dokumenti organizirani in takoj dostopni, kar ima za posledico generiranje občutno manjšega števila kopij dokumentov. Na drugi strani pa je pomembno zavedanje o zagotavljanju reciklaže uničene dokumentacije.

Varno uničevanje dokumentacije in arhivskega gradiva

Pomemben segment upravljanja z dokumentacijo in arhivi je varen proces uničenja nastale dokumentacije in tudi drugih podatkovnih nosilcev. Konkretne rešitve in tehnologija omogoča uporabnikom odgovorno in zakonito ravnanje s poslovno dokumentacijo in podatkovnimi nosilci v procesu uničevanja. Zakonodaja vse organizacije zavezuje k varnemu uničenju podatkov na podatkovnih nosilcih, torej tudi na dokumentih v fizični obliki. Pomembno je spremljanje in dokumentiranje vseh faz postopka uničevanja in po zaključenem postopku uničenja dokumentacije in podati potrdilo o varnem uničenju. Ob tem je potrebno poudariti, da v večini primerov tehnologija procesa omogoča ponovno uporabo materialov. To pomeni, da se skoraj vsi materiali reciklirajo in ponovno uporabijo v življenjskem ciklusu izdelka. Ključno je zagotavljanje rešitev uničevanja dokumentacije in podatkovnih nosilcev z varnostnimi zabojniki, ki so zaščiteni pred nepooblaščenim dostopom in opremljeni z varnostnimi ključavnicami. Za prevoz dokumentov in podatkovnih nosilcev je potrebno uporabiti samo vozila s čvrsto nadgradnjo. Varnostni zabojniki se izpraznijo v zaprtih in po najsodobnejših varnostnih standardih varovanih in nadzorovanih prostorih. Vsi podatkovni nosilci so nato razvrščeni glede na vrsto in se uničijo v skladu z evropskimi standardi, za dodatno varnost pa je poskrbljeno s kontrolo pristopa vsega osebja.

Po nekaterih napovedih naj bi v Evropi poraba belega papirja še nekaj let rasla. Povprečni zaposleni še vedno ustvari 20.000 dokumentov v enem letu in za upravljanje z njimi porabi tudi do polovico svojega delovnega časa.

Varno upravljanje in arhiviranje dokumentacije in arhivskega gradiva

Reisswolf s svojo rešitvijo RMS (records management solutions) omogoča dokumentiran proces upravljanja z dokumentacijo v fizični in elektronski

obliki. Ta rešitev zagotavlja storitve upravljanja z dokumentacijo in arhivi z najsodobnejšo tehnologijo, ki omogoča tako arhiviranje dokumentov za daljše obdobje kakor tudi arhiviranje in stalen dostop do dokumentov, ki so pogosto v uporabi. Poseben poudarek je posvečen varnosti in sledljivosti procesa, kar nam omogoča najsodobnejša in uporabniku prijazna programska oprema. V paleti možnosti, ki jih omogoča RMS lahko najdemo naslednje rešitve:

- Prevzem dokumentacije pri uporabniku in varna dostava v lastne arhivske prostore s kombiniranimi in tovornimi vozili ter vozili prirejenimi za prevoz vrednosti,
- Celovita obdelava prevzete dokumentacije, označevanje in vnos dokumentacije v bazo podatkov,
- Sistemsko upravljanje z arhivirano dokumentacijo v najsodobnejših logistično, klimatsko in varnostno urejenih arhivskih prostorih,
- Dostava arhivirane dokumentacije po naročilu uporabnika na lokacijo uporabnika (storitve na klic),
- Odbiranje arhivirane dokumentacije za uničenje in varno uničenje le-te po predhodni odobritvi uporabnika,
- Digitalno upravljanje dokumentacije.

Ključno prednost za uporabnike navedenih rešitev predstavlja medsebojna in navzkrižna prepletenost posameznih rešitev, ki tako tvorijo homogeno celoto rešitve in zagotavljajo spremljanje dokumentacije skozi njen celoten življenjski cikel vse od nastanka pa do njenega končnega uničenja oziroma trajnega arhiviranja.

Z Reisswolf rešitvami prihranimo čas in denar

S spletom združevanja različnih rešitev ustvarja Reisswolf Slovenija storitve z visoko dodano vrednostjo in sicer:

1. Naročnikom zagotovimo varno in sledljivo hrambo, obdelavo in uničenje podatkovnih nosilcev.
2. Naročnikom skozi proces priprave (odbira) dokumentacije in ostalih podatkovnih nosilcev za hrambo izločimo podatkovne nosilce s pretečenim rokom hrambe in s tem zmanjšamo porabo arhivskega prostora.
3. Naročnikom zagotovimo zakonito hrambo in uničevanje podatkovnih nosilcev.
4. Naročnikom zagotovimo sledljiv proces hrambe in uničenja podatkovnih nosilcev.
5. Naročnikom lahko omogočimo upravljanje arhivov z našo programsko opremo tudi na njihovem naslovu.
6. Naročnikom znižujemo stroške upravljanja s podatkovnimi nosilci.
7. Uničene podatkovne nosilce skozi procese predelave vračamo v njihovo ponovno uporabo (reciklaža).

Primeri dobrih praks iz celotne poslovne skupine Reisswolf potrjujejo domnevo, da se s celovitim pristopom pri upravljanju z dokumentacijo in arhivi uporabnikom dejansko prihrani veliko stroškov, kar nenezadnje kažejo tudi poslovni rezultati podjetij v skupini, ki v povprečju izkazujejo stalno preko 20% rast prihodkov od prodaje. ■





REISSWOLF®
secret. service.

REISSWOLF D.O.O., Pod gabri 15, 1218 Komenda, Slovenija, EU;
Kontakti: 01 541 22 66, 041 401 650, info@reisswolf.si , www.reisswolf.si

Avtorica: dr. Nataša Klenovšek Arh, univ. dipl. ing. rač. in inf., mag. dr. inf.*



SOCIALNA OMREŽJA KOT VIR PRIDOBIVANJA PODATKOV

Število uporabnikov socialnih omrežji vse bolj narašča. Njihova uporabnost se je od fizičnih oseb razširila tudi na podjetja, organizacije in druge ustanove. Tako tudi socialna omrežja vse bolj postajajo odličen vir različnih podatkov in s tem tudi tarča kibernetskih kriminalcev.

Socialni mediji so postali prevladujoča metoda za uporabo interneta, ki so infiltrirali in spremenili način komunikacije in interakcije milijonov ljudi po svetu. Med vsemi je najbolj priljubljeno socialno mreženje, kjer lahko za primer navedemo Facebook, ki ima več kot milijardo uporabnikov, obstaja pa še milijarda drugih uporabniških računov, odprtih pri več kot tisočih socialnih omrežjih na internetu. Tako je socialni splet postal vir različnih informacij in podatkov, ki jih lahko pridobimo iz blogov, deljenih povezav uporabnikov, komentarjev, forumov in socialnih omrežij.

Socialna omrežja so komunikacijski kanal z ogromnim številom uporabnikov, ki so namenjena zasebni ali poslovni rabi, saj se vedno več podjetij poslužuje socialnih omrežij za promocijo različnih storitev ali izdelkov, ter tudi povezavo z drugimi poslovnimi partnerji. Zato niso samo fizične osebe tiste, ki so žrtve različnih kibernetskih napadov. Ker vedno več podjetij temelji na spletnih tehnologijah, s pomočjo česar lahko povečajo svojo učinkovitost ter prihranijo na času in denarju, pa so le-ta vse pogosteje tarče različnih kibernetskih zločinov.

Globalna dostopnost je prednost socialnih omrežij, zaradi česar so le-ta zanimiva za uporabnike, kar pa pomeni, da so socialna omrežja tudi odličen vir pridobivanja različnih (osebnih) podatkov, kar vzbudi zanimanje pri kibernetskih kriminalcih. Velika večina kibernetskih zločinov sestavljajo kraja identitete, goljufije, spletno ribarjenje (»phishing«) in podatkovno rudarjenje. Pri vseh omenjenih zlonamernih dejanjih pa je »najslabše« to, da najpogosteje uporabnik niti ne ve, da se je nad njegovimi podatki zgodilo kriminalno dejanje, saj kibernetski kriminalci izkoriščajo naivnost uporabnikov socialnih omrežij, kar kibernetskim kriminalcem delo še bolj poenostavi, zato uporabniki zaradi neprevidnosti hitro postanejo žrtve.

Vsekakor je napačno razmišljanje, da je uporabnik, ki je avtor teh informacij, tudi njihov lastnik, saj se podatki, ki jih objavite na socialnih omrežjih obravnavajo kot javno dostopni, zato se z njimi ravna podobno kot s katerim koli drugim javnim podatkom.

Kako do podatkov?

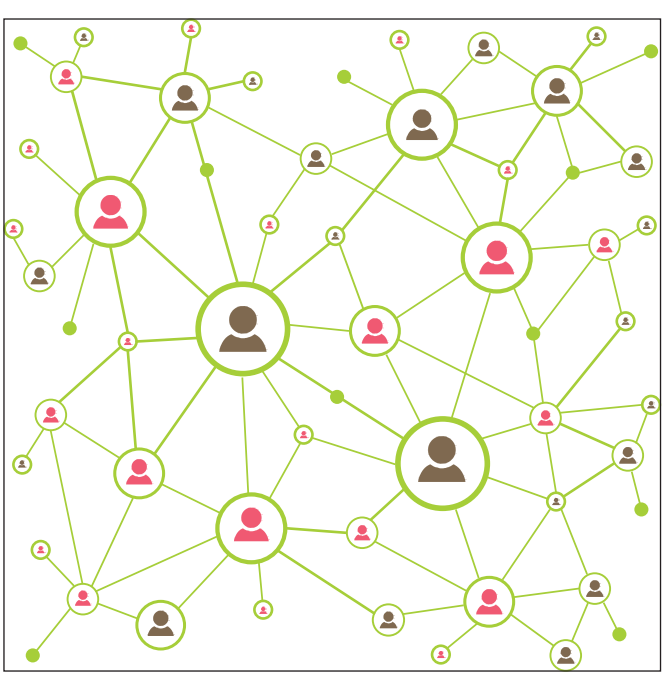
Objava na blogu predstavlja nov način pisanja dnevnika, pisanje na prijateljev virtualni zid je kot pošiljanje elektronske pošte, ter ustvarjanje novega dogodka, ki se lahko opravi le v nekaj minutah, vključno s pošiljanjem vabil vsem povabljencem. Socialna omrežja smo sprejeli z odprtimi rokami in nimamo težav z njimi deliti svojih osebnih podatkov. Ta gmota informacij pa tvori bogato družbeno sfero, ki omogoča pametno ponovno uporabo teh informacij za različne namene. Pri tem, pa si je potrebno zastaviti vprašaje, kdo je lastnik vseh teh informacij? Vsekakor je napačno razmišljanje, da je uporabnik, ki je avtor teh informacij, tudi njihov lastnik, saj se podatki, ki jih objavite na socialnih omrežjih obravnavajo kot javno dostopni, zato se z njimi ravna podobno kot s katerim koli drugim javnim podatkom.

Podatke iz socialnega omrežja kot je na primer Facebook, lahko danes pridobimo s pomočjo tako imenovanih ontologij. Ontologija predstavlja izraz, ki obravnava splošne lastnosti strukture obravnavanega problema. Ena izmed takšnih onto-

*avtorica je članica Slovenskega združenja korporativne varnosti



logij je tudi prijatelji prijatelja (FOAF - friend of a friend), s pomočjo katere lahko zajamemo socialni graf osebe, kar pomeni celotno mrežo prijateljev.

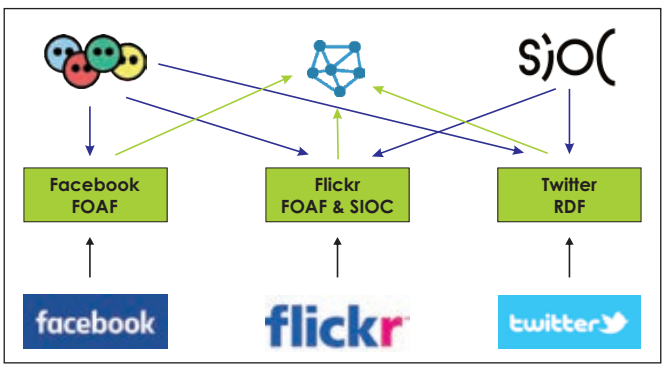


Tako lahko dobimo podatke s kom se družite, na kakšen način ste med seboj povezani, kakšni so interesi in aktivnosti. Tako je FOAF, gledano v tehničnem smislu, zelo preprosta tekstovna struktura, ki temelji na jeziku XML (Extensible Markup Language), katero računalniki zelo enostavno berejo, saj je dokaj preprosto napisati aplikacijo, ki bi takšno strukturo lahko prebrala in jo zapisala v človeku bolj berljivo obliko. FOAF zapis lahko vključuje informacije kot so ime, spol, naziv, vzdevek, družinsko ime, elektronska pošta, telefonska številka, povezave na spletno stran ali vaš blog, vsebuje pa tudi podobne podatke vseh vaših kontaktov oziroma prijateljev v socialni mreži.

```
<foaf:Person rdf:ID="nka">
   <foaf:name>Natasa Klenovsek Arh</foaf:name>
   <foaf:title>Mrs</foaf:title>
   <foaf:givenname>Natasa</foaf:givenname>
   <foaf:family_name>Klenovsek</foaf:family_name>
   <foaf:nick>natasak</foaf:nick>
   <foaf:mbox rdf:resource="mailto:natasa@mail.com"/>
   <foaf:phone rdf:resource="tel:148777554"/>
   <foaf:knows>
      <foaf:Person>
         <foaf:name>Janez Novak</foaf:name>
         <foaf:mbox rdf:resource="mailto:janez.novak@e-posta.si"/>
      </foaf:Person>
   </foaf:knows>
</foaf:Person>
```

Razvoj socialnih omrežij je uporabnikom odprl pot v virtualni svet, kjer lahko izrazijo svoje mnenje, pridobijo povratne informacije, ter se družijo s posamezniki, ki imajo podobne interese in prepričanje. Večina sodobnih uporabnikov na vsaj en način sodeluje v spletni skupnosti, naj si bo to v socialnih omrežjih, forumih, klepetalnicah ali novičarskih skupinah. S pomočjo ontologije SIOC (semantično povezane spletne skupnosti - Semantically-Interlinked Online Communities),

ki je nekako razširitev ontologije FOAF in zagotavlja metode za povezovanje razprav iz blogov, forumov in socialnih omrežij, lahko pridobimo šest glavnih razredov podatkov: spletna stran, forum, objava, vloga, uporabnik in uporabniška skupina. SIOC omogoča zajem interakcije med posamezniki in lahko izraža vloge, ki jih ti posamezniki predstavljajo v spletnem družabnem prostoru.



Tako pridobljene podatke, lahko vsakdo uporabi za različne namene. Seveda je poznavanje tovrstnih ontologij in z njimi povezanih tehnologij vsekakor prednost, ni pa ravno pogoj, da bi lahko prišli do omenjenih podatkov, ki bi jih nato izkoristili tudi za namene kriminalnih dejanj.

Kako lahko zmanjšamo tveganja

Tveganja, da bi nekdo s pomočjo omenjenih ontologij, prišel do podatkov ne moremo zatreti, lahko pa upoštevamo varnostne napotke, saj je pomembno, da smo uporabniki socialnih omrežij seznanjeni z nevarnostmi, ki jih prinaša uporaba in vključenost v socialna omrežja. Da se lahko vključimo v socialno omrežje, je prvi korak odprtje uporabniškega računa oziroma svojega profila. Pri tem je potrebno navesti svoje osebne podatke kot so ime, priimek, starost in elektronski naslov. Se pa začetni vnos osebnih podatkov med socialnimi omrežji nekoliko razlikuje. Po uspešnem odprtju profila, lahko le-temu dodamo še mnogo drugih osebnih podatkov kot so kraj bivanja, izobrazba, hobiji, zaposlitev in še mnogo več. Vsak uporabnik se lahko sam odloči katere podatke bo delil z drugimi, vendar je najbolj priporočljivo, da vaš profil omogočite samo prijateljem, ki jih poznate in jim zaupate. Vsekakor je najbolje, da javnosti razkrijete čim manj osebnih podatkov.

Tveganja, da bi nekdo s pomočjo omenjenih ontologij, prišel do podatkov ne moremo zatreti, lahko pa upoštevamo varnostne napotke, saj je pomembno, da smo uporabniki socialnih omrežij seznanjeni z nevarnostmi, ki jih prinaša uporaba in vključenost v socialna omrežja.





Objave na socialnih omrežjih

Bodite previdni s svojimi objavami na socialnih omrežjih, saj lahko le-te privedejo do različnih kaznivih dejanj, katerih boste najverjetneje žrtev sami. Že s samo objavo, da greste na počitnice, podate sum na to, da bo vaš dom takrat sameval in bo predstavljal odlično priložnost za nepridiprave. Da bi nekdo ugotovil vaš naslov, telefonsko številko, ime, priimek in še veliko več, pa v današnjih časih ne potrebuješ prav veliko znanja. Že sam vpogled v vaš Facebook profil lahko pove ogromno o vas. V primeru, da ste vaš profil »zaklenili« oziroma omejili javni prikaz vaših podatkov, pa obstajajo metode (tudi že omenjene ontologije) s katerimi se do vaših podatkov vseeno lahko dostopa. Z uporabo spletnih aplikacij, kot je Google Street View, se vizualno lahko hitro oceni približno vrednost vaše nepremičnine, ter tako zanimanje za vaš prazen dom še bolj povečate.

Mobilne aplikacije za Facebook, Twitter, Instagram, Foursquare vse uporabljajo tako imenovane »geotags« (geografske oznake), s čimer razkrijete lokacijo na kateri se nahajate, zato je zelo priporočljivo, da funkcijo za »geotagging« vsaj pri aplikacijah za socialna omrežja, ne uporabljate.

Prav tako pazite na objave vaši prijateljev in znancev, še posebno takšne, ki se povezujejo na neznano spletno stran. Ko zasledite objavo, ki naj bi jo objavil vaš »socialni« prijatelj, pred klikom na to objavo preverite kaj je namen povezave na katero boste kliknili. Če boste neprevidni, lahko zelo hitro pride do nezaželenih viroz tudi na vašem računalniku.

Pazite pri objavi slik na socialnih omrežjih, saj ko enkrat sliko objavite, zelo težko sledite kje vse bo ta vaša slika končala. Vsekakor pa enkrat objavljena slika ostane na spletu za vedno. Zato naj bo previdnost pri objavi slik še toliko bolj večja. Digitalna revolucija pa je povzročila tudi porast otroške pornografije, ki je postala vse bolj dostopna. Vsak starš je vsekakor ponosen na svojega otroka in to želi deliti s širšo javnostjo. Vendar previdno! Vsaka slika z otroki lahko hitro konča na nezaželenih spletnih straneh in na koncu se lahko v težavah znajde tudi oseba, ki je sliko objavila.

Zato vam »napačna« objava, naj bo tekstovna ali slikovna, lahko povzroči nemalo nevšečnosti v službi, družini, pri prijateljih, nenazadnje lahko tudi pri organih pregona.

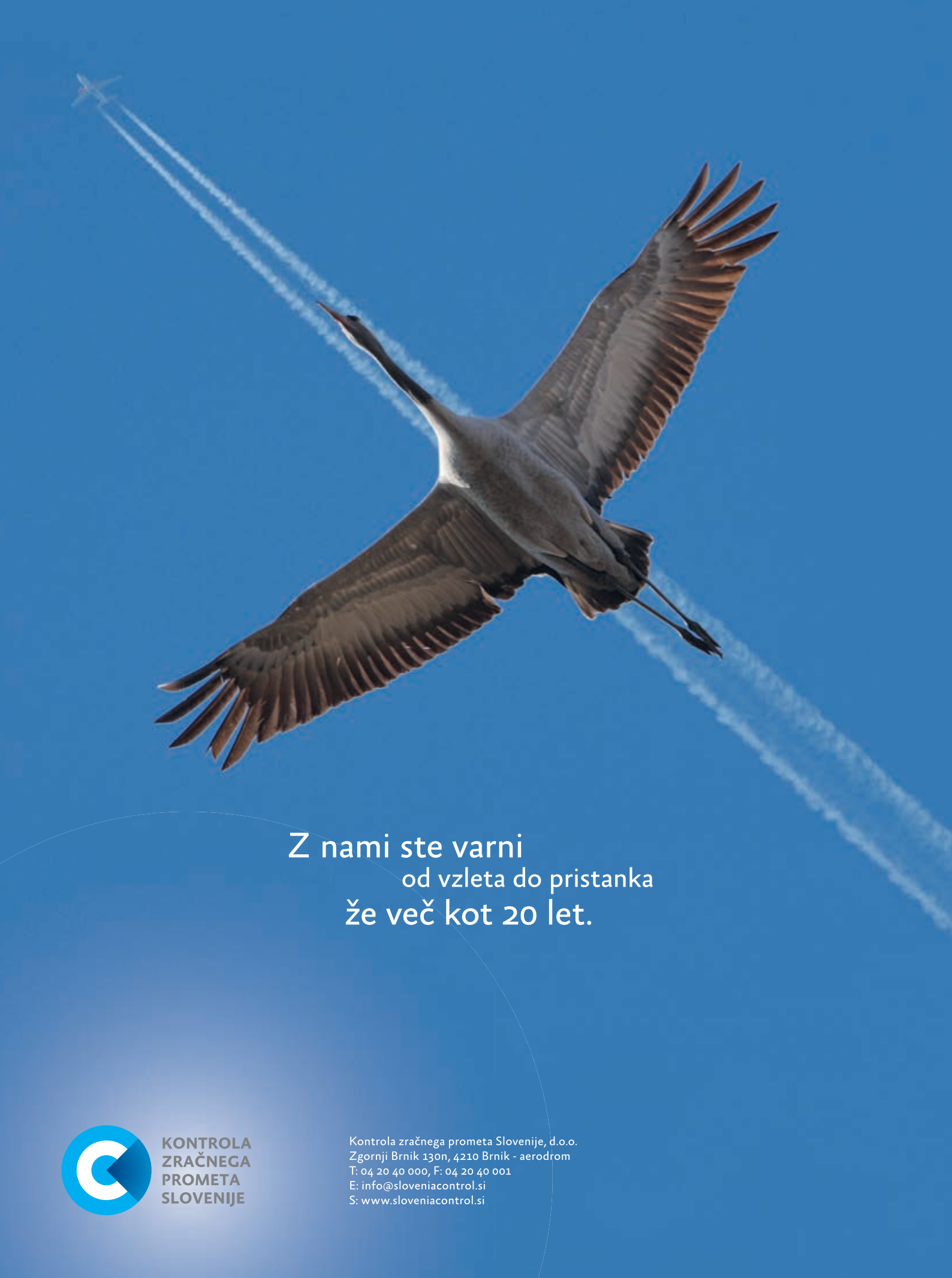
USTAVITE SE. POMISLITE. OBJAVITE.

Nekaj napotkov, ki ste jih zagotovo že slišali ali prebrali in vam lahko koristijo pri »varni« uporabi socialnih omrežij:

- skrbite za posodobljeno različico protivirusnega programa in operacijskega sistema;
- omejite prikaz vaših osebnih podatkov in uporabite varnostne nastavitve, ki jih nudijo socialna omrežja;
- za dostop do socialnega omrežja uporabite močna gesla (daljša kombinacija malih in velikih črk, številk in simbolov), ki naj ne bodo enaka geslom, ki jih uporabljate za dostope do katerih drugih aplikacij. Če ste opazili, da se iz vašega socialnega omrežja objavljajo nezaželene objave, geslo nemudoma spremenite;
- ko ste v dvomih, rajši spreglejte in ne klikajte povezav v elektronski pošti, tweetu ali objavi, četudi poznate izvor, a vendar zgleda sumljivo, je najbolje da izbrišete ali označite kot nezaželeno (spam);
- o drugih objavljajte le toliko, kot želite, da drugi objavijo o vas.

Dejstvo je, da imajo socialna omrežja velik vpliv na okolje v katerem živimo. Združujejo skupnosti, kjer se izmenjujejo različne informacije, delijo doživetja, strokovna mnenja in še mnogo več. Uporabljajo jih podjetja, tržni oddelki, za pridobivanje informacij, oglaševanje in »lovljenje« novih potencialnih kupcev njihovih proizvodov ali storitev.

Uporabite diskretnost in zdravo pamet, ko objavljate kakršne koli podatke na socialnih omrežjih. Imejte v mislih, da ne morete slediti kje končajo vaše objave, sporočila ter slike in kdo vse do njih dostopa. Četudi zbrišete objavo iz vašega socialnega omrežja, to še ne pomeni, da je izbrisana za vedno in se do nje ne more več dostopati. Ne objavljajte stvari, ki bi vzbudila zanimanja spletnih kriminalcev in ne objavljajte grozečih sporočil, četudi so ta le samo za šalo. ■



KONTROLA ZRAČNEGA PROMETA SLOVENIJE

Kontrola zračnega prometa Slovenije, d.o.o.
Zgornji Brnik 130n, 4210 Brnik - aerodrom
T: 04 20 40 000, F: 04 20 40 001
E: info@sloveniacontrol.si
S: www.sloveniacontrol.si

Avtor: Boštjan Špehonja / Etični hacker*



(NE) ANONIMNOST NA SVETOVNEM SPLETU

Ste kdaj pomislili na to, da obstajajo podjetja, ki lahko o vas vedo skoraj vse? Vedo s čim se ukvarjate, kje živite, kakšni so vaši interesi, politična usmerjenost, kakšno je vaše zdravstveno stanje, kakšne so vaše prehrambene navade, kje nakupujete, počitnikujete in še marsikaj drugega.

Verjetno se je vsakemu izmed nas kdaj zgodilo, da je iskal določene podatke preko določene spletne strani, nato pa so se mu podobni rezultati iskanja v obliki oglasov prikazovali tudi na drugih spletnih straneh. Recimo iskanje lokacije za počitnice, iskanje spletnega gostovanja, nakup avtomobila itd. Tehnologijo, s katero kreatorji spleta to dosežejo lahko imenujemo preprosto piškotki.

Piškotki so majhne datoteke, ki se shranijo na našo elektronsko napravo s katero obiščemo spletno stran. Vsebujejo različne informacije, ki jih spletna stran prebere, ko jo ponovno obiščete. Piškotke lahko razdelimo v več kategorij. Prvi so tako imenovani lastni piškotki, kateri vsebujejo podatke kot so seje, artikli v košarici, uporabniško ime, nastavitev jezika na spletni strani in podobno. V kolikor ti ne bi obstajali, bi recimo morali na Facebooku pri vsakem kliku na kakršno koli vsebino ponovno vpisovati geslo. Zato so lastni piškotki pomembni za normalno delovanje strani, in nam izboljšajo uporabniško izkušnjo. Drugi piškotki vsebujejo podatke, ki so namenjeni predvsem administratorjem ter lastnikom spletnih strani. S temi piškotki se vodi statistika, koliko obiska ima spletna stran, katere novice in članki se na strani najbolj prebirajo, kako se giblje tok klikanja uporabnikov itd. Tretja kategorija piškotkov pa so tisti, ki beležijo podatke o aktivnostih na spletu, jih obdelajo, in pošljejo tretjim subjektom, v veliki večini so to spletni oglaševalci. Te so tako imenovani "third part cookies", ki v določeni meji lahko posegajo v uporabnikovo zasebnost. Doubleclick, Quantserve, Scorecard Research, AddThis, Adnxs, Yieldmanager so le nekatera podjetja, ki se ukvarjajo s spletnim oglaševanjem, in uporabljajo omenjene piškotke. Za njih marsikdo sploh slišal ni, lahko pa rečemo, da vedo o nas veliko več, kot bi pričakovali. Poglejmo si primer storitve DoubleClick, ki je, tako kot AdSense, AdWords, ter Google-Analytics v lasti spletnega velikana Googla. Vsaka spletna stran, katera vsebuje to storitev, na naših elektronskih napravah pušča prav sledljive piškotke. Po podatkih spletne strani internetlivestats.com je bilo leta 2014 vseh spletnih strani 968,882,453. Od tega je storitev DoubleClick po statistiki na spletni strani trends.builtwith.com uporabljalo 1,751,885 spletnih strani. Vsakič, ko obiščemo eno izmed teh spletnih strani, katere uporabljajo omenjeno storitev, se v brskalnik naložijo različni piškotki.

Piškotki so majhne datoteke, ki se shranijo na našo elektronsko napravo s katero obiščemo spletno stran. Vsebujejo različne informacije, ki jih spletna stran prebere, ko jo ponovno obiščete.

Primer vsebine:

time: 01/Dec/2015 12:01:32
ad_placement_id: 105
ad_id: 1003
userid: 100000000000001
client_ip: 123.45.67.89
referral_url:
http://youtube.com/categories/

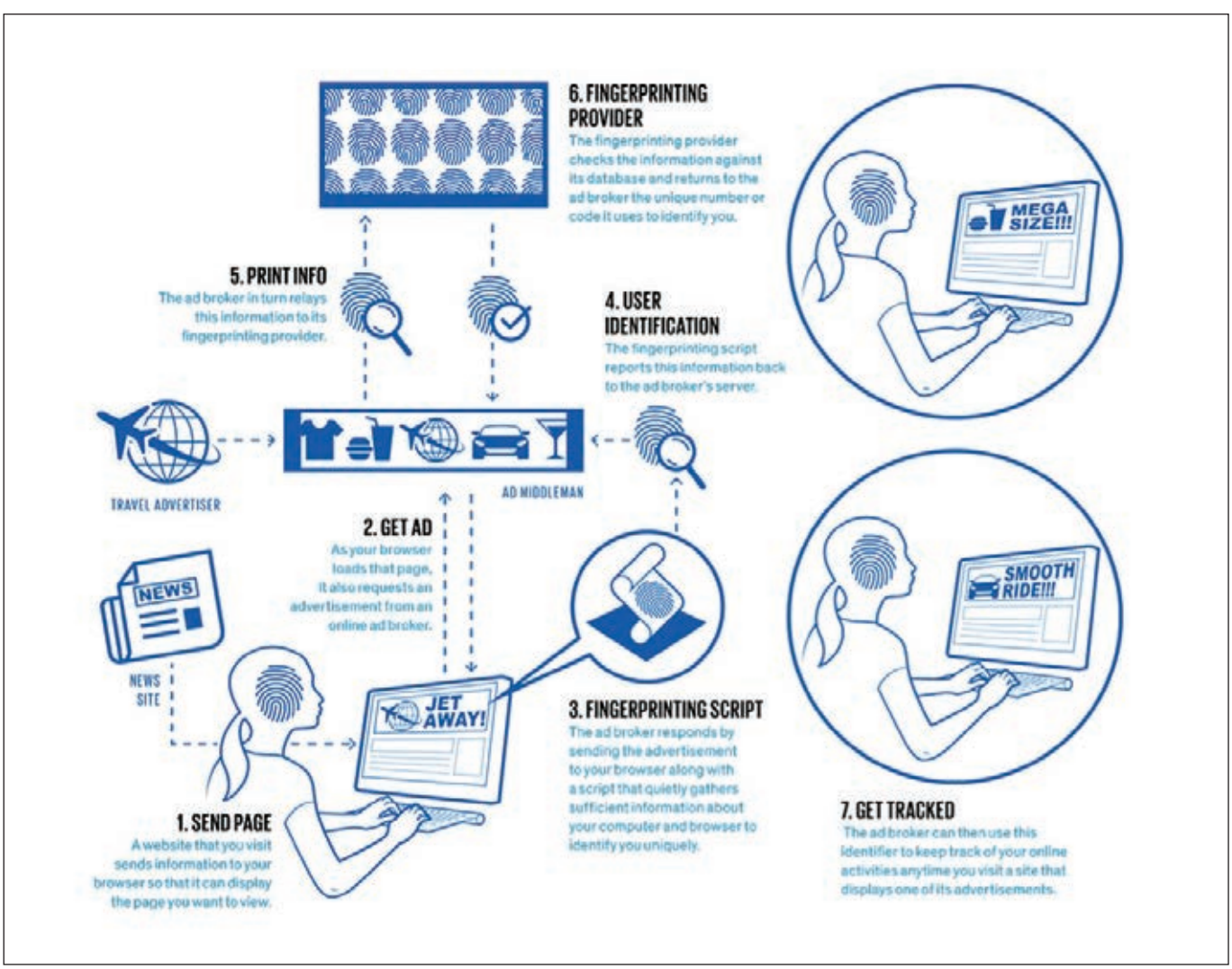
Parameter time pove čas in datum kdaj se je določen oglas prikazal. Userid je unikatna ID številka piškotka, ki je bila dodeljena vašemu brskalniku. Ad_id je številka oglasa ki se nam je prikazal na strani, ad_placement_id je oznaka, ki nam pove kje na spletni strani se je oglas prikazal, referral_url pa na kateri strani ste bili, ko ste oglas videli. Preko IP naslova lahko ugotovijo v kateri državi se uporabnik nahaja ter približno lokacijo. Če je zgornji piškotek nastavljen na spletni strani, ki uporablja omenjeno storitev, za tem pa brskate po drugi spletni strani, ki uporablja isto storitev, se informacije združijo in evidentirajo. DoubleClick storitev uporabljajo tudi nekatere slovenske medijske hiše na njihovih spletnih straneh. Če recimo brskate po njih in poleg aktualnih novic klikate tudi na novice iz področja računalništva, in ta vzorec pogosto ponavljate tudi na drugih spletnih straneh, je s tem vaš brskalnik pristal v segmentu "računalništva". Na ta način oglaševalcem omogočate izbiro kateri ciljni oglasi se vam bodo prikazovali. V pravkar omenjenem primeru ni načeloma nič spornega. Pomisleki glede zasebnosti pa se pojavljajo, če brskate po vsebini z zdravjem in se tako sledi vašim klikom, preko katerih lahko

*avtor je član Slovenskega združenja korporativne varnosti

ugotovijo vaše zdravstveno stanje. Brskanje po političnih straneh lahko izda vašo politično usmerjenost, podobno velja za pornografske strani. Podobne tehnologije in podoben način zbiranja uporabljajo tudi prej omenjena podjetja za katere marsikdo sploh ne ve, da obstajajo. Na ta način nastajajo velike baze podatkov ki se obdelujejo, segmentirajo in uporabljajo za razvoj ter izboljšanje obstoječih storitev. Verjetno ni potrebno posebej omenjati, da Google, poleg omenjenega, na razne načine o vas zbira še lokacije, z algoritmi skenira vašo elektronsko pošto, shranjuje zgodovino ogledanih posnetkov na Youtubu, shranjuje vašo zgodovino iskanja, preko aplikacij na pametnih telefonih pa ima dostop do vaših kontaktov, gibanja, ter drugih podatkov. Zato je priporočljivo kdaj obiskati googlovo nadzorno ploščo ter omejiti oz. vsaj pregledati podatke, ki se hranijo o vas.

Piškotke, ki so vezani na brskalnike lahko s preprostimi nastavitvami omejimo ter izbrišemo. V celoti pa jih omejiti ne moremo, saj je večina spletnih strani narejena tako, da piškotke uporabljajo za normalno delovanje strani.

Piškotke, ki so vezani na brskalnike lahko s preprostimi nastavitvami omejimo ter izbrišemo. V celoti pa jih omejiti ne moremo, saj je večina spletnih strani narejena tako, da piškotke uporabljajo za normalno delovanje strani. V ta namen so na spletnih straneh opozorila o uporabi piškotkov. Nekoliko bolj sporni pa so tako imenovani "Super cookies" ali "Flash cookies" katerih pa ni mogoče odstraniti na tako enostaven način. Shranjeni so v naši elektronski napravi s katero brskamo po spletu in so popolnoma neodvisni od spletnega brskalnika. Uporablja jih Flash Player. Vsakič, ko obiščemo spletno stran, ki uporablja Flash Player, se podatki iz piškotkov nekontrolirano pretakajo in uhajajo iz našega računalnika. Piškotki so namenjeni identificiranju spletnega brskalnika, vendar bomo pri naslednjem primeru videli, da se preko tega z veliko gotovostjo identificira tudi spletnega uporabnika. Navadni piškotki imajo velikost po standardu omejeno na 4kb, super piškotki pa lahko vsebujejo kar 100kb podatkov.



VIR: http://spectrum.ieee.org/img/taking-your-print-1405517867866.jpg

Recimo, da prvič obiščemo spletno stran, ki uporablja oglaševalske storitve. Poleg vsebine spletne strani, se uporabniku na spletni strani prikažejo tudi oglasi. Preden se oglasi prikažejo, se v ozadju izvede nekaj skript, ki pobere prstne odtise našega brskalnika. S temi prstnimi odtisi nas skripta skoraj enoznačno določi. Po statistiki je mogoče unikatno določiti 85% brskalnikov. Identifikacijo brskalnika pošlje v svojo bazo in jo preišče. V kolikor nas v bazi ni, se nam dodeli unikatna ID številka za sledenje, ki se preko super piškotkov zabeleži kot datoteka na našem računalniku, in je, kot rečeno, popolnoma neodvisna od spletnih brskalnikov. To so datoteke s končnico *.sol, razporejene pa so navadno na večih mestih pod datotekami Flash Player-ja. Pobiranje prstnih odtisov brskalnika se navadno pobira z java skripto, iz brskalnika pa dobimo informacije kot so User-Agent, ki nam pove kakšen operacijski sistem uporabljamo, kakšen brskalnik ter njegovo verzijo. Poleg tega nam brskalnik našteje vse pisave, ki jih imamo nameščene na operacijskem sistemu, podrobnosti dodatkov (pluginov), ki so nameščeni na brskalniku, dimenzije zaslona, v kakšni časovni coni se nahajamo, ali imamo omogočene piškotke, HTTP_ACCEPT Headers kateri nam pove jezik brskalnika ter nekatere druge parametre.

Ali podjetja, ki upravljajo s piškotki poznajo naše osebne podatke?

V veliki večini DA, še posebej tista, ki so povezana s socialnimi omrežji. Tudi ta uporabljajo podobne sisteme sledenja. Unikatnost posameznega brskalnika se računa z entropijo. Ta je merilo za količino informacije, ki jo dobimo s spoznavanjem vrednsti slučajne spremenljivke. Vprašamo se, koliko bitov entropije potrebujemo, da enoznačno določimo brskalnik? Vzemimo, da je na zemlji 7 milijard ljudi in od tega zračunamo entropijo za enega prebivalca: E = log2 (1 oseba/7miliard oseb)=32,7, torej potrebujemo 33 bitov za enoznačno določitev uporabnika. V povprečju samo brskalnik posreduje 10.5 bita entropije, kar pomeni da ima vsaka 2^10,5=1449 oseba isti brskalnik. (podatke o tem koliko bitov entropije je mogoče pridobiti iz vašega brskalnika lahko preverite na https://panopticlick.eff.org/). Na socialnem omrežju ustvarite profil in označite, da živite v Novi Gorici. Ta ima po podatkih statističnega urada 13.491 prebivalcev. Po izračunani entropiji – log2(13491/7milijard)=23,11 bita entropije. Če na neki tretji strani, ki v ozadju uporablja iste mehanizme za sledenje, podate svoj rojstni dan, izdate še dodatnih -log2(1/365) =8,51 bitov informacije. Po statistiki sta spol, pošta in datum rojstva unikatna za 87% ljudi. Veliko vlogo pri zbiranju podatkov ima tudi referral url, kateri se pretaka preko http zahtevkov in nam pove iz katere spletne strani smo obiskali neko drugo spletno stran. Preprosto povedano, če na našem profilu socialnega omrežja kliknemo na neko tretjo povezavo, se bo preko http zahtevka skozi parameter "referral" posredovala tudi povezava do našega profila. https://www.facebook.com/profile.php?id=200008916360982. V tem primeru je id 200008916360982 unikatna številka facebook profila in oglaševalska podjetja skenirajo vaš javni profil socialnega omrežja ter tako o vas izvejo še dodatne informacije. To je le en, poenostavljen primer, na kakšen način se podatki uporabnikov zbirajo preko interneta. Glede na omenjeno lahko trdim, da anonimnosti v tem primeru na internetu vsekakor ni, saj se dobro beleži vsak naš premik na spletu. Mogoče bo kdo hitro pomislil na to, da obstajajo mehanizmi za anonimnost na spletu s čimer se strinjam, vendar velika večina uporabnikov spleta takih mehanizmov ne uporablja.



Kako se izogniti sledenju?

Odgovor na to vprašanje je zelo enostaven – težko. V kolikor bi se želeli v popolnosti zakriti, bi potrebovali proxy strežnike oz. VPN povezave preko katerih bi si spremenili IP naslov, socialna omrežja ter tako kakršna koli storitev, pri kateri se izdajamo z imenom, odpade. Potrebno bi bilo odstraniti Flash Player, blokirati java scripte, z raznimi dodatki brskalnikov onemogočiti skripte, v brskalniku omogočiti brskanje brez beleženja zgodovine ter nadzirati vse piškotke, ki se naložijo na našo elektronsko napravo bodisi preko brskalnika oz. odstranjevati piškotke, ki so naloženi na naši elektronski napravi. Poenostavljeno pa bi svetoval, da se vsaj piškotki in zgodovina brskalnika večkrat na mesec izbriše. To naredite preprosto tako, da odprete brskalnik, in skupaj pritisnete tipke ctrl+shift+delete. Izberite obdobje brisanja, označite piškotke (cookie) ter izbriši. ■

Avtor: Boris Milič, mag. ing. prom.*



PROMETNA VARNOST MED ELEKTROTEHNIKO IN PROMETNO STROKO

Z množično uporabo avtomobila je pričelo naraščati tudi število prometnih nesreč in žrtev. Vedno višje hitrosti, »različno« usposobljeni šoferji, neprimerna cestna infrastruktura, strmo naraščanje prometa in podobno, predstavlja diametralno nasprotje zagona avtomobilske industrije in je povod za slabo prometno varnost. Ali to zveni znano?

Množična uporaba avtomobilov je skrajšala (časovno) razdalje med kraji in mesti, na krajših (srednjih) razdaljah je avtomobil prehitel železniški potniški promet, razvoj avtomobilske industrije je odpiral nova delovna mesta, množična proizvodnja je omogočila sprejemljive cene avtomobilov, nizke cene goriv pa so razcvet avtomobilizma le še spodbujale.

Prometna varnost danes

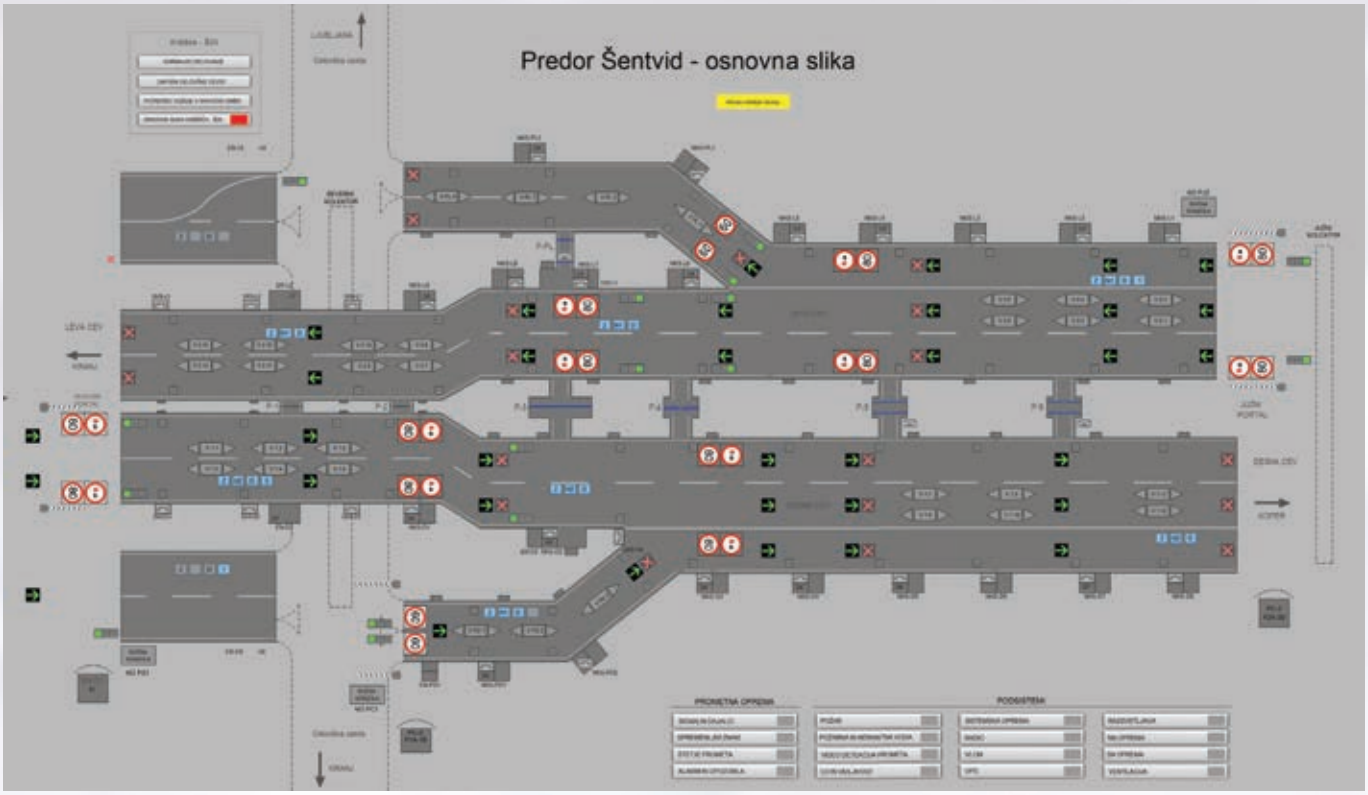
Kdo je torej kriv za slabo stanje prometne varnosti danes? (Pre)slabo usposobljeni novi vozniki, slaba cestna infrastruktura, nerazumljiva, nedosledna in prepogosta cestna signalizacija, neusposobljeni upravljalci infrastrukture, neučinkovita in prezahtevna varnostna oprema avtomobilov, utrujeni in nezbrani vozniki, neustrezni predpisi in zakoni, zavajujoče in nepopolne informacije medijev, avtomobilske zavarovalnice?

Verjetno kombinacija vsega naštetega, vendar pa je zagotovo na prvem mestu človek. Iz zgoraj naštetega je mogoče povleči vzporednico z današnjim življenjem. V vseh segmentih prometa (cestnega) danes prevladuje bliskovit razvoj elektrotehnične stroke, ki ostale (prometno, gradbeno, logistično, pravno, medicinsko...) pušča daleč zadaj. Mogoče je trditi, da razkorak med elektrotehnično stroko (s svojimi izpeljankami, kot so računalništvo, elektronika, energetika, robotika, umetna inteligenca...) in ostalimi, predstavlja ročno zavoro celostnega razvoja prometa. Razkorak in neusklajenost delovanja preprečujeta učinkovito in optimalno uvajanje sodobnih varnostnih sistemov v cestna vozila in infrastrukturo. Dober primer tega je razvoj samovozečih cestnih vozil, ki jih razvijajo mnoga podjetja. Problem je v tem, da vsako od podjetij razvija svojo unikatno verzijo vozila, ki je v večini primerov nezdružljiva z vozili ostalih proizvajalcev. Če bi obstajal enoten, ter med različnimi strokami usklajen koncept (standard) razvoja in uvajanja samovozečih cestnih vozil, bi ta vozila že opravljala svojo funkcijo v cestnem prometu.

Zaradi nepoznavanja delovanja, razvoja in možnosti uporabe (elektro) tehničnih sistemov v prometni infrastrukturi, je razvoj le te še vedno usmerjen v izgradnjo klasične cestne infrastrukture, brez primarno vgrajenih tipal, senzorjev, predpripravljenih napajalnih točk in podobno.

Lokomotiva razvoja cestnega prometa je dejansko elektrotehnična stroka, vse ostale stroke, vključno s prometno, pa so vključene bolj ali manj pavšalno. Premalo širine in pomanjkanje tehničnega znanja je verjetno glavni razlog, da razvoj cestnega prometa ne vodi prometna stroka. Ravno to dejstvo predstavlja prej opisano zavoro razvoja sodobnega cestnega prometa. Večji vpliv prometne (in gradbene stroke) je viden pri usmerjanju razvoja cestne infrastrukture, vendar pogosto žal v napačno smer. Zaradi nepoznavanja delovanja, razvoja in možnosti uporabe (elektro) tehničnih sistemov v prometni infrastrukturi, je razvoj le te še vedno usmerjen v izgradnjo klasične cestne infrastrukture, brez primarno vgrajenih tipal, senzorjev, predpripravljenih napajalnih točk in podobno. Brez izdatnih finančnih vložkov, takšne klasične cestne infrastrukture nikoli ne bo mogoče vključiti v sodoben cestni promet, saj takšna ne bo omogočala niti osnovne dvosmerne komunikacije z vozili.

*avtor je član Slovenskega združenja korporativne varnosti



SCADA predora Šentvid. Vir: avtor, 2012

(Avto) cestni predori

Manjši, vendar z vidika prometne varnosti zelo pomemben del cestne infrastrukture predstavljajo avtocestni predori. Avtocestni predori se uvrščajo med kritično infrastrukturo, največjo nevarnost pa tako za predore, kot njihove uporabnike, predstavljajo požari. Predor namreč v primeru požara predstavlja dimnik, z idealnimi pogoji za gorenje; dober vlek in neomejen dotok svežega zraka. Za uporabnike predora, ki se v času požara nahajajo v predoru, predstavljajo smrtonosno kletko; še posebej enocevni, kjer je zagotavljanje požarne varnosti za udeležence izredno težavno. Požari v predorih so najpogosteje posledica prometnih nesreč oziroma okvar na vozilih.

Zaradi zagotavljanja požarne varnosti, so se že pred leti pričele v cestne predore vgrajevati razne požarno-varnostne naprave. Poudariti je potrebno, da morebitni požari v avtocestnih predorih niso pomembni in nevarni le za prometne udeležence, ki se v času požara nahajajo v njih. V kolikor pride do močnejših požarov, moči preko 10 MW, pa ti požari lahko močno poškodujejo tudi sam predor. Za močnejše poškodbe predora je mogoče šteti sesutje betonske obloge in podobno, kar v praksi pomeni zaprtje predora in več mesecev obnove, ter popravil. Ekonomska škoda zaradi takšnega dogodka je lahko ogromna.

Posledično takšen način zahteva nenehno rast števila zaposlenih in nenazadnje, tudi števila nadzornih centrov.

Nadaljnji korak v razvoju predorske varnosti je omogočila elektrotehnika, ki je opremila predore z avtomatskimi, daljinsko vodenimi in nadzorovanimi sistemi, ter botrovala uvedbi predorskih Nadzornih centrov, opremljenih z računalniškimi aplikacijami za daljinsko upravljanje sistemov in naprav SCADA (**S**can, **C**ontrol, **A**larm and **D**ata **A**cquisition). V predorskih Nadzornih centrih so praviloma s SCADO upravljali operaterji, ki so kot strokovnjaki posameznih elektrotehničnih področij vgrajene sisteme ne le poznali, ampak tudi razumeli njihovo delovanje. Dodatna tehnična znanja so pridobivali z rednim vključevanjem v delo elektrovzdrževanja. V zadnjih letih so se predorski Nadzorni centri pričeli spreminjati v centre za tako imenovano »prometno vodenje«. Operaterje, ki so praviloma prihajali iz elektrotehnične stroke, je pričela izrivati prometna stroka. Prevladala je misel, da za upravljanje s predorsko elektro-strojno opremo ni potrebno elektrotehnično znanje, strokovno poznavanje vgrajenih sistemov in njihovega delovanja, temveč zadošča že poznavanje osnov prometa. Poleg zaposlenih, so se tudi Nadzorni centri za nadzor predorov počasi preobrazili v Nadzorne centre za prometno vodenje. Zaposleni operaterji v nadzornih centrih so dobili nove prioritete. Intenzivna rast števila nadzornih kamer in števila raznih »prometnih« sistemov, so pričeli »dušiti« osnovno poslanstvo nadzornih centrov. Posledično takšen način zahteva nenehno rast števila zaposlenih in nenazadnje, tudi števila nadzornih centrov. Področni, Regionalni, Glavni in Nacionalni nadzorni centri so rezultat takšne strategije... Zaposleni v vseh teh centrih se ukvarjajo z množicami informacij, ki jih pridobivajo s pomočjo video nadzora in raznih senzorjev v cestni infrastrukturi. In kako lahko s pridobljenimi informacijami dejansko vplivajo na prometno varnost?

Na dva načina; s telefonskim obveščanjem in z uporabo vgrajenih signalnih sistemov. Telefonsko obveščajo policiste, gasilce, reševalce, vzdrževalce avtocest in podobno. Z uporabo vgrajenih signalnih sistemov lahko daljinsko vklopijo rdečo

luč na semaforju pred in v predoru, vključijo omejitev hitrosti na elektronskem znaku spremenljive vsebine in podobno. V današnjem času je računalniški program, ki bo namesto operaterjev opravljal vse te omenjene funkcije, sposoben izdelati praktično vsak študent informatike!

Asfinag

Da je takšna smer razvoja zgrešena, se je že pred leti zavedel Avstrijski Asfinag. Reševanja prej omenjene problematike se je lotil z združevanjem vodenja in upravljanja predorskih sistemov iz enega mesta. Dober primer takšne strategije je nadzorni center v Celovcu, ki vodi in upravlja 24 zahtevnih predorskih sistemov na Avstrijskem Štajerskem, med katerimi so tudi predor Karavanke (7864 m), Oswaldiberg (4307 m) in Ehrentalerbergtunnel (3345 m). Asfinag je v teh predorih praktično vse podsisteme že avtomatiziral, trenutno izvajajo še manjkajoče poenotenje SCADA sistemov. Osnova za izvedbo teh del je strokovno izdelan Projekt integracije predorskih sistemov v centralni SCADA sistem. Asfinag je v teh 24 predorih uspel izvesti avtomatizacijo zahtevnih predorskih podsistemov in s tem dosegel nivo, ki za delovanje praktično ne potrebuje ljudi in postavlja dežurna operaterja v nadzornem centru Celovec v vlogo opazovalca. Kdaj bo center deloval samostojno, je le še vprašanje časa in seveda politike vodstva...

Hkrati z zgoraj opisanimi ukrepi, pa Asfinag postopoma v upravljanje predorskih (in ostalih) sistemov vključuje tehnično podkovano strokovno osebje v službah elektrovzdrževanja. Tehnično podkovanem strokovnem osebju, preko SCADA aplikacij, omogoča vzdrževalne posege, spreminjanje nastavitev in kontrolo raznih zahtevnih podsistemov. Tako njihovi, tehnično podkovani zaposleni, postopoma prevzemajo dela, ki so bila še do pred kratkim domena izvajalcev sistema in tehnično podkovanih operaterjev.

Elektrotehnika danes

Razvoj cestne infrastrukture, voznih sredstev in njihove opreme gre medtem bliskovito naprej. Elektrotehniki ne čakajo prometnikov, ampak razvijajo in uvajajo, za različne posamezne naročnike (avtomobilske koncerne, graditelje infrastrukture ipd), unikatne in po večini žal med sabo nekompatibilne sisteme. Dober primer nesodelovanja prometne in elektrotehnične stroke so novi avtocestni predori. Že nekaj časa velja trend, da je zaradi zagotavljanja prometne varnosti potrebno predore opremljati z množico, za večino voznikov neznanih, signalno-varnostnih sistemov in naprav. Tako vas danes ob vstopu v predor pričaka ambient, podoben adventno okrašenemu glavnemu trgu v večjem mestu. Bela, rumena, rdeča, modra, zelena in oranžna so le nekatere izmed barv v predoru, ki večini voznikov le odvračajo pozornost od vožnje, namesto obratno. Koliko od vas ve, da so z zeleno označeni prečni prehodi v sosednjo cev? Zakaj so svetleče talne oznake na levi bele in na desni rdeče? Kaj za vas kot voznika pomeni, če svetleče talne oznake utripajo? In najnovejši dosežek, modre talne oznake – ali poznate njihov pomen?

Če ste na večino vprašanj odgovorili z ne, ni z vami nič narobe. Tako bo odgovorila večina! Vendar ni vse tako črno, kot je videti na prvi pogled. Na predlog elektrotehnične stroke

> Glede na lani sprejete EU standarde komunikacije med vozili (car to car) in med vozili ter infrastrukturo, je cilj »0 mrtvih in huje poškodovanih« v cestnem prometu končno postal realen in dosegljiv. Vendar le s popolno in med sabo odvisno avtomatizacijo cestnega prometa.

je EU sprejela enotne standarde komunikacije za inteligentne transportne sisteme (http://www.etsi.org/news-events/news/851-2014-12-press-etsi-publishes-european-standards-for-intelligent-transport-systems), ki omogočajo poenotenje komunikacije med prevoznimi sredstvi, ter med prevoznimi sredstvi in infrastrukturo. To sprejetje bo (je) omogočilo pričetek enotnega razvoja avtomatskih signalno-varnostnih sistemov, od avtomatskega zagotavljanja varnostne razdalje med različnimi vozili, pa vse do samovozečih vozil, ki z današnjega vidika predstavljajo najvišji varnostni standard.

Danes razvoj avtomobilov (in na splošno vseh voznih sredstev) močno prehiteva izobraževanje in usposabljanje novih voznikov. Inštruktorji v avtošolah kandidate usposabljajo po nekih utirjenih pravilih, pri tem pa ne uspejo slediti času in novostim, ki jih avtomobilska industrija prinaša praktično vsakodnevno. Praktične vožnje avtomobila vas danes avtošole učijo na enak način in z enakimi vajami, kot ste se jih učili pred 30 in več leti. In to kljub temu, da so danes vozna sredstva opremljena z nepreglednim številom sistemov aktivne zaščite, ki popravljajo voznikove napake pri vožnji in katerih pomen ter delovanje večina voznikov sploh ne pozna. Ravno tako večina voznikov ne pozna namena kopice signalno-varnostnih sistemov, vgrajenih v cestno infrastrukturo, del tega je bil opisan že v prejšnjih poglavjih. Na vseh nivojih cestnega prometa je mogoče ugotoviti, da je najšibkejši člen pri zagotavljanju varnosti v cestnem prometu človek. O tem govori tudi Resolucija Republike Slovenije o nacionalnem programu varnosti cestnega prometa za obdobje od 2013 do 2022 (Uradni list RS, št 39/2013), kjer je zapisano:

»na nastanek prometnih nesreč vpliva več dejavnikov, poglavitni pa so udeleženci v cestnem prometu, cestna infrastruktura, motorna vozila in prometno okolje. Pri vseh teh dejavnikih ima človek najpomembnejšo vlogo, saj je kot voznik v vlogi uporabnika motornega vozila in cest, kot načrtovalec pa je zelo pomemben člen pri gradnji cest. Varnost cestnega prometa je odvisna od odgovornega ravnanja posameznika, vzgojno izobraževalnih in preventivnih institucij, medijev, represivnih in pravosodnih organov, civilne družbe, gospodarskih družb, vodstev samoupravnih lokalnih skupnosti in ne nazadnje državnih organov«.

Kot lahko vsak razbere iz (črne) statistike prometnih nesreč, se cilju Evropske unije »0 mrtvih in huje poškodovanih v prometnih nesrečah«, ne približujemo. Ravno nasprotno; če se število žrtev prometnih nesreč eno ali dve leti niža, se naslednje leto zopet zviša. Na tisoče prometnih strokovnjakov dnevno ponuja rešitve na področju prometne varnosti. Razni

modeli prometnega vodenja, spremembe cestne infrastrukture, novi načini izobraževanja in usposabljanja voznikov, raziskovalne naloge, ki dokazujejo neverjetne uspehe na področju prometne varnosti s področja prometne varnosti so le del tega, vendar so v realnosti uspehi zelo daleč od želenih. Kljub mnogim različnim pogledom na stanje v cestnem prometu, ugotovitvam in zaključkom, je večina strokovnjakov poenotena le v enem dejstvu – glavni krivec za slabo prometno varnost je človek, oziroma človeški vpliv.

Zaključek

Upravljanje cestnega prometa je zelo zahtevno in pogosto nepredvidljivo, saj nanj vplivajo mnoge spremenljivke in neznanke. Še pred leti se je zdelo, da bo le vrhunsko usposobljen človek (operater) sposoben učinkovito upravljati in nadzirati inteligentne transportne sisteme, spremenljivo cestno signalizacijo, ter predore in njihovo tehnološko zapleteno opremo. Danes je mogoče z zanesljivostjo trditi, da temu ni tako. Glede na lani sprejete EU standarde komunikacije med vozili (car to car) in med vozili ter infrastrukturo, je cilj »0 mrtvih in huje poškodovanih« v cestnem prometu končno postal realen in dosegljiv. Vendar le s popolno in med sabo odvisno avtomatizacijo cestnega prometa.

Le s popolnoma samodejnim delovanjem elektrotehničnih sistemov v cestni infrastrukturi in v voznih sredstvih, je mogoče doseči tisto stopnjo prometne varnosti, ki si jo vsi želimo. ■



Posledice požara v predoru Mont Blanc, Marec 1999. Vir: http://news.bbc.co.uk/2/hi/europe/388904.stm

Avtor: Gregor Kovač, mag / sodni izvedenec*



UPORABA SODOBNIH FORENZIČNIH METOD PRI ANALIZI VIDEOPOSNETKOV

Z namenom varovanja ljudi in premoženja se za sistematično snemanje, prenos in shranjevanje t. i. žive slike šteje vsaka uporaba videonadzornega sistema (ang. CCTV – Closed Circuit TV). Velik del družbenega življenja tako v javnem kot tudi v zasebnem sektorju s pomočjo tehnologij za zagotavljanje varnosti v sodobni družbi zagotavljajo prav videonadzorni sistemi.

Nikakor ne smemo zanemariti dejstva, da se videonadzorni sistemi uporabljajo tudi v raziskovalne namene (npr. analiziranje vedenja in kupnih navad). Videonadzorni sistemi so prisotni pri nadzoru bankomatov, v prostorih posameznih podjetij, v šolah, vrtcih, športnih objektih, pri nadzoru prometa, parkirišč, trgovin, bencinskih servisov, igralnic, letališč, itd. Videonadzor ima z vidika odvračanja potencialnih storilcev kaznivih dejanj in prekrškov prvenstveno preventivno-psihološki učinek, kasneje pa lahko omogoča odkrivanje posnetih odklonskih (deviantnih) ravnanj, ki jih celotna družba šteje za nenormalne oziroma škodljive.

Prve pametne videonadzorne aplikacije je uvedla Agencija za obrambo in napredne raziskave (ang. DARPA Defence Advanced Research Project Agency) v ZDA leta 1997. Z uporabo videonadzornih kamer pa so kot pionirji na tem področju pričeli Nemci. Najbolj znano je njihovo snemanje lansiranja raket med drugo svetovno vojno. V tistem času so bile kamere bistveno manj zmogljive od sedanjih, saj so snemale v črno-beli tehniki s slabo ločljivostjo in ostrino slike.

V sodobnem času tako večji sistemi videonadzorov kot tudi snemalne naprave v lasti posameznika vsakodnevno posnamejo ogromno količino digitalnega slikovnega materiala, ki imajo kot t. i. slikovni dokazi vedno večjo vlogo pri interpretaciji različnih kaznivih dejanj in prekrškov na sodišču. V sodnih ali v upravnih postopkih je za ugotovitev ali za razjasnitev kakšnega dejstva potrebno strokovno znanje, s katerim sodišče ne razpolaga.

Pri reševanju tovrstnih vprašanj si sodišče pomaga s sodnim izvedencem za področje kriminalistično tehničnih preiskav in podpodročjem preiskav fotografij ter posnetkov varnostnih kamer. Sodni izvedenec mora tako na podlagi svojega specifičnega znanja in strokovnosti podati izvid in mnenje s kate-



*avtor je član Slovenskega združenja korporativne varnosti

Naloge sodnega izvedenca, ki mu sodišče z odredbo naloži različna vprašanja, so obsežnejše kot zgolj uporaba avtomatskega sistema za prepoznavo obrazov in podajanje izvida zgolj na podlagi zaključkov algoritma sodobnih biometričnih sistemov.

rim ugotovi in/ali razjasni dejstva, ki so potrebna, da lahko sodišče ali upravni organ lažje odloča. Z vidika procesnih določb je izvedenčevo mnenje ali izvid eden od dokazov v postopku, ki ga mora sodnik ocenjevati v skladu z načelom proste presoje dokazov. Tako je v Sloveniji od 8. 1. 2015 mogoča tudi izdelava izvedenskega mnenja in izvida (na poziv sodišča, fizične ali pravne osebe) o primerjavi osebe in njegovih predmetov na sporni in primerjalni fotografiji ali video posnetku ter fotografiji zajeti iz video nadzornega sistema. Analiza se opravi s pomočjo strokovnega znanja, uporabe sodobnih forenzičnih metod, analize morfoloških karakteristik obraza (fizična antropologija), pregleda in analize predmetov, antropometrijskega merjenja osebe, merjenja in primerjave višine osebe in uporabe posebnih preiskovalnih metod v skladu z normativi in pravili znanosti, ki veljajo v predmetni stroki.

Pri tem je potrebno biti kot sodni izvedenec vedno zavezan pravilom, ki veljajo v predmetni znanosti in v stroki. Izvedensko mnenje ima namreč dokazni pomen, torej bistveno vpliva na izid v sodnem postopku.

Naloge sodnega izvedenca, ki mu sodišče z odredbo naloži različna vprašanja, so obsežnejše kot zgolj uporaba avtomatskega sistema za prepoznavo obrazov in podajanje izvida zgolj na podlagi zaključkov algoritma sodobnih biometričnih sistemov. Za kvalitetno analizo je potrebna celovita analiza tako spornega, kot tudi primerjalnega slikovnega materiala. Pred katerokoli uporabljeno forenzično metodo je potrebna osnovna slikovna obdelava. Sporni slikovni material je navadno zajet pod različnimi pogoji, ki niso vedno najboljši, zato je potrebno tak material ustrezno obdelati in pri tem izvesti številne postopke za njihovo izboljšavo (odprava šuma, stabilizacija, kontrast, popravek osvetlitve).



Obvezno je, da sodni izvedenec pri svojem delu uporablja tudi sodobne forenzične metode in pri tem, poleg lastne zaznave biometričnih značilnosti na obrazu in telesu osebe, upošteva tudi rezultate naprednih biometričnih orodij, ki so v zadnjem času še kako prisotna tudi v moderni družbi.



V kolikor identifikacija obraza storilca ni izvedljiva, lahko sodni izvedenec uporabi tudi druge uporabne forenzične metode, s katerimi lahko:

- Izmeri in primerja višino storilca in obdolženca.
- Ugotavlja specifične značilnosti na obrazu in konstituciji storilca in jih primerja z značilnostmi na obdolžencu.
- Primerja levi ali desni profil obraza storilca in ga primerja z obraznim profilom obdolženega.
- Primerja predmete, ki jih je storilec uporabljal v času izvršitve kaznivega dejanja, s predmeti, ki so bili zaseženi v fazi predkazenskega postopka.
- Uporablja sisteme za avtomatsko iskanje obrazov.
- Uporablja sisteme za ugotavljanje podobnosti v gibanju človeškega telesa.
- Z analizo digitalne fotografije ugotovi morebitno ponarejanje, prenarejanje.
- Z uporabo programske opreme zajame (skenira) obraz in ga pretvori v 3D model.
- Ugotavlja časovno usklajenost.

V forenzični praksi preiskovanja videoposnetkov mora biti izvedensko mnenje z izvidom tako samo v domeni sodnega izvedenca za področje primerjave oseb na videoposnetkih in fotografijah zajetih iz posameznih videonadzornih sistemov. Obvezno je, da sodni izvedenec pri svojem delu uporablja tudi sodobne forenzične metode in pri tem, poleg lastne zaznave biometričnih značilnosti na obrazu in telesu osebe, upošteva tudi rezultate naprednih biometričnih orodij, ki so v zadnjem času še kako prisotna tudi v moderni družbi. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Management korporativne varnosti

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

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

Zakaj **Management korporativne varnosti**?

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

Komu je študij namenjen?

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



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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



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

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

Predmetnik

I. LETNIK

Skupni obvezni predmeti

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

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

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

Smer Korporativni varnostni manager – podjetnik

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

Izbirni predmeti (študent izbere dva):

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

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

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

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

CENTER VIŠJIH ŠOL

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

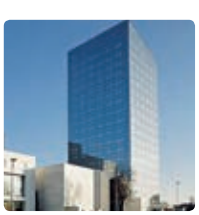
FAKULTETA ZA PODJETNIŠTVO

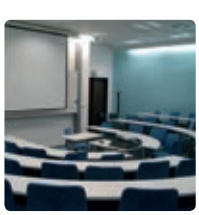
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

POSLOVNO-IZOBRAŽEVALNI CENTER

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





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

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo

Dvojna 6MP termična kamera

Zaznavanje gibanja v popolni temi • "Moonlight technology"



MOBOTIX Management Center
VMS - za Windows / Mac
brez stroškov / brez omejitve

M15 dvojna termična kamera, kombinacija toplotnega in optičnega senzorja - vključen MxActivitySenzor

Thermal resolution *Equivalent to 0.05 °C, range -40 to +550 °C*

Video sensor *MxActivitySensor reducing false alarms*

Event Recording *Onboard (SD card) & direct to NAS*

Detection *Up to 400 meters in complete darkness*

Communication *Two-way audio included*

Power *Lowest energy bill, < 6W, Standard PoE*

Extreme *Weatherproof, IP66, -30 to +60 °C*

tend

MOBOTIX



M15 Dual
Thermal & Optic



S15 Dual
Thermal & Optic



S15 Dual
World First Dual Thermal



S15
PTMount Thermal Black



S15
PTMount Thermal White

Distribucija: ORG. TEND d.o.o., Kraljeviča Marka ulica 19, 2000 Maribor, E: mobotix@tend.si, T: 02 250 57 50, W: www.mobotix.si