Varnost v kibernetskem prostoru – poročilo s konference RISK 2016[1]

9. in 10. marca 2016 je v Laškem potekala konferenca »*RISK 2016 – 11th Adriatic Security, Networking and IT Optimization Cenference*« v organizaciji podjetja Real Security. Gre za tradicionalni mednarodni dogodek, ki povezuje vodilne strokovnjake s področja kibernetske varnosti in optimizacije sistemov s predstavniki organizacij, državnih institucij in kritične infrastrukture. Namen letošnje konference je bil zagotoviti obveščenost udeležencev o razvoju varnostnih groženj, predstaviti najnovejše varnostne pristope oz. storitve (angl. *SaaS – security as a service*) in dobre prakse, prav tako pa omogočiti druženje med strokovnjaki za varnost in predstavniki različnih, državnih ter zasebnih organizacij. Cilj RISK konference je udeležencem omogočiti vpogled v aktualne rešitve, strategije, taktike in produkte preprečevanja informacijskih groženj.

Na konferenci je sodelovalo več kot 350 udeležencev, skupno pa je bilo izvedenih 29 enournih predavanj. Svoje poglede na razvojne trende so predstavili predavatelji iz različnih uglednih organizacij (npr. NIST, ISACA, Intel Security, Hewlett-Packard Enterprise (HP), FireEye, Dell, Qualys, ADD idr.). Predavanja so pripravili tudi nekateri predavatelji iz Slovenije, med njimi SIQ, SRC, S&T Slovenija in Fakulteta za varnostne vede. Predavanja so potekala v angleškem in slovenskem jeziku.

Udeležence je ob otvoritvi nagovoril CEO Real Security Rento Uhl, ki je ob zahvali obiskovalcem in predavateljem izpostavil aktualen trend v varnostni industriji – kljub finančnim rezom in varčevanju se na varnostnem področju še vedno odvija neverjeten tehnološki razvoj. Nagovoru sta sledili dve panelni predstavitvi v izvedbi predstavnikov organizacij FireEye – Yogi Chandiraman in HP – Steve Lamb.

Yogi Chandiraman je konferenco otvoril z opozorilom vsem organizacijam, da informacijski incidenti in vdori niso več vprašanje, saj je vsaka organizacija, ne glede na velikost, industrijo ali geografski položaj, tarča storilcev. Vdori v informacijske sisteme so postali nekaj običajnega, problem, ki ga opažajo, je, da so (informacijske) varnostne službe v organizacijah še vedno v defenzivnem položaju, posebej v javnem sektorju. Grožnje organizacijskim informacijskim sistemom drastično naraščajo, storilci imajo pred žrtvami asimetrično prednost (lažje je odkriti eno ranljivost, kot zaščititi vse), zaradi česar se količina napadov podvoji vsake pol leta. Težava je v tem, da so detekcijski in odzivni časi občutno predolgi: v povprečju čas odkritja vdora v informacijski sistem podjetja traja več kot 150 dni, vdorov pa v več kot polovici primerov ne odkrijejo organizacije same.

1 *Pri pisanju vsebinskega poročila s konference RISK 2016 so sodelovali študenti FVV Marko Mlaker, Ida Majerle, Suzana Kužnik, Gašper Mlakar, Kristijan Kovač, Robert Furman, Peter Makovšek, Jaka Žužek, Frančišek Vid Kek, Robert Kujavec in Sašo Volčjak. Za pomoč se jim avtorja iskreno zahvaljujeva.*

Pregled trenutnega stanja informacijskih groženj kaže, da storilci spreminjajo svoj namen – njihov cilj ni več samo kraja podatkov, ampak tudi destrukcija organizacij oz. poslovnih procesov (t. i. *disruptive attacks*), kar je vidno v drastičnem porastu izsiljevalskih (zlonamernih) programov (t. i. *ransomware*), ki resno ogrožajo neprekinjeno poslovanje podjetij. Zato bi si morale organizacije zastaviti naslednja vprašanja: (a) kdaj se bo napad zgodil, (b) kako je/bo to vplivalo na poslovanje in (c) kako zmanjšati škodo oz. posledice. Zaradi spremenjene narave groženj sicer ni na voljo popolnoma zanesljive prevencijske tehnologije, kar od stroke zahteva spremenjene poglede na varnost. Učinkovit odziv na te izzive organizacija HP vidi v razvoju integriranih avtomatiziranih rešitev, forenzike omrežnega prometa in opolnomočenju usposobljenih strokovnjakov, ki razumejo sodobno varnostno IT okolje. Pri razvoju informacijske varnosti priporočajo uporabo metodologije CMSC (angl. *Cyber security maturity curve*), ki organizacijam skozi tri razvojne faze v grafični podobi prikaže, katere tehnične ukrepe je treba razvijati glede na stanje trenutne informacijske zrelosti podjetja.

Tudi Steve Lamb je opozoril na asimetrično problematiko v varnostni stroki, saj so kljub izboljšanju investicij v razvoj varnosti varnostne grožnje vedno bolj uspešne. Predstavil je ugotovitve raziskave *HP Cyber Risk Report.* Najpomembnejša ugotovitev te raziskave je drastičen porast ranljivosti in groženj na področju aplikacij za mobilne telefone, s poudarkom na operacijskem sistemu Android. Lamb je poudaril tudi problem, da se v praksi ali preveč ali pa nepravilno ukvarjamo z vprašanjem preprečevanja informacijskih tveganj. V povprečju organizacije uporabljajo več kot 60 varnostnih tehnologij, razlog za tako veliko število pa je iskati v tem, da podjetja iščejo univerzalno rešitev (t. i. *silver bullet*), s katero bi rešile vse varnostne težave. Takšna zasičenost z varnostnimi rešitvami vodi v situacijo, ko nekatere ukrepe ali področja razvijajo preveč, druga pa premalo. Lamb je poudaril še eno težavo: pomanjkanje strokovno usposobljenega kadra oz. nekvalitetni izobraževalni programi, ki ne spodbujajo inovativnega razmišljanja pri mlajših generacijah. Trenutno razvijamo kadre, ki varnostne probleme rešujejo po principu zahtevanega minimuma, logično pa na ta način ni mogoče konkurirati visoko usposobljenim in motiviranim storilcem.

V nadaljevanju je Kurt Schoenmaekers (Intel Security) izpostavil štiri tehnologije in uporabniške storitve, ki trenutno v stroki predstavljajo varnostni izziv: mobilne naprave, internet stvari (IoT), računalništvo v oblaku in vnos osebnih naprav v organizacijsko okolje. Slednje je povezano s konceptom uporabe sive tehnologije – s strani organizacije neodobrene tehnologije (t. i. *shadow IT*). Schoenmaekers je postavil vprašanja, s katerimi se trenutno ukvarjajo varnostni menedžerji in IT strokovnjaki: vlagati v razvoj znanja/talenta ali v avtomatizirane rešitve; uporabljati prosto dostopne ali plačljive programe; razvijati lastne rešitve ali zaupati obstoječim ponudnikom; in ali je merjenje stanja informacijske varnosti sploh smiselno? Praksa kaže, da so organizacije naklonjene plačljivim programom, razvoju talenta in lastnih rešitev, hkrati pa podpirajo merjenje informacijske varnosti. V nadaljevanju je predstavil smernice učinkovitega načrtovanja informacijske varnosti, ki priporočajo analiziranje informacijskih tveganj, avtomatiziran nadzor, povezovanje s subjekti v poslovnem ekosistemu in sodelovanje z neodvisnimi specializiranimi organizacijami.

Kot primer detekcije napadov na informacijske sisteme je predstavil rešitev McAfee Threat Intelligence Exchange (TIE), ki v kombinaciji z McAfee Data Exchange Layer (DxL) odkrije grožnjo v obliki detekcije sprememb v sistemu. S to rešitvijo je organizacijam omogočena reakcija na anomalije v realnem odzivnem času.

Problem prenasičenosti trga z varnostnimi rešitvami na eni strani in pomanjkanja strokovno usposobljenega kadra na drugi je izpostavil tudi Alexander Raczynski (Forcepoint). Ponovno je poudaril že znano ugotovitev, da je trg delovne sile na IT varnostnem področju močno podhranjen, saj je globalno nezapolnjenih več kot milijon delovnih mest (angl. *talent-gap*). Obstoječi produkti na področju IT varnosti pa so po ugotovitvah raziskave Cisco RSAC Survey 2015 za večino (62 %) vodij informacijske varnosti prekompleksni in neuporabni. Zaradi kombinacije različnih težav je odzivanje organizacij na grožnje neuspešno; čas kompromitacije informacijskega sistema (t. i. *dwell-time*), sestavljen iz časa, ki ga organizacije potrebujejo za odkritje grožnje in okrevanja, v povprečju traja 275 dni. Za uspešnejše soočanje z grožnjami Raczynski predlaga uporabo univerzalnih hibridnih platform, ki omogočajo obnavljanje podatkov, zaščito oblakov in omrežno forenziko – gre za 4D (angl. *defend, detect, decide, defeat*) univerzalno rešitev.

O težavah upravljanja informacijske varnosti je razpravljal Ramsés Gallego, predstavnik organizacij ISACA in Dell ter nosilec številnih mednarodnih certifikatov s področja upravljanja informacijskih sistemov. V dinamičnem in energičnem predavanju je opozoril, da se svet spreminja s svetlobno hitrostjo, največji razvoj pa je mogoče opaziti na področju informacijske tehnologije. Udeležencem je demonstriral uporabo elektronske zapestnice, ki posname mišično mimiko posameznika in omogoča brezžično izvajanje ukazov na elektronskih napravah. Prav tako je prikazal uporabo 3D krmilnika gibanja, ki bo v prihodnosti potencialno nadomestil klasično miško in tipkovnico, uporabnost tovrstne tehnologije pa je vidna predvsem v medicini. Meni, da glavne težave, s katerimi se soočamo, niso v tehnologiji, saj je ta zelo kvalitetna, razvojni potencial pa z vidika obstoječih idej velik. Problem je predvsem v ljudeh, njihovi (ne) pripravljenosti sprejemati novosti in ustrezno upravljati z varnostnimi tveganji. Gallego poudarja, da je uspeh organizacij v prihodnosti odvisen od tega, kaj počnejo danes, pomembno pa je, da so odgovorni kadri sposobni postavljati (a) prava vprašanja, (b) v pravem trenutku in (c) pravim osebam. Pri tem navaja znane besede Gandhija, ki nazorno opišejo trenutno poslovno situacijo: »*The future depends on what we do today*.« Gallego pripisuje menedžerjem podjetij ključno vlogo pri doseganju učinkovitega upravljanja informacijske varnosti, medtem ko je IT kader odgovoren, da je menedžerjem varnostna problematika predstavljena na pravi in razumljiv način. Pri tem je pomembno, kako fleksibilna je organizacija v kontekstu sodobnih sprememb na področju tehnologije in groženj. Med te spremembe uvršča porast v številu motiviranih storilcev (omeni npr. obstoj t. i. mesta Hackerville, od koder izvira veliko hekerjev) in idejo o računalništvu v vesolju (angl. *space computing*), kjer ne obstajajo zakonske omejitve. Gallego poudari, da vedno več držav uradno priznava kibernetski prostor kot prostor izvajanja pete domene vojne (za zemljo, vodo, zrakom in vesoljem), zato se morajo tudi organizacije čim hitreje zavedati, da je virtualnost današnja resničnost.

Tisti, ki menijo, da je virtualnost nasprotje realnosti, se motijo; virtualnost je zelo realna, v semantiki pa je virtualno nasprotje fizičnega.

Boštjan Špehonja (Unistar) je v svojem nastopu predstavil in demonstriral delovanje trenutno enega izmed najbolj aktualnih zlonamernih programov Cryptolocker. Gre za izsiljevalski program, ki se navadno širi preko okuženih priponk v elektronski pošti. Ob naložitvi na sistem zakriptira vse datoteke na računalniku in nato od žrtve zahteva plačilo določene vsote denarja za pridobitev šifrirnega ključa. Na praktičnem primeru je pokazal tudi phishing prevaro, ki jih je nasploh zaradi sofisticiranosti vse težje ločiti od avtentičnih elektronskih sporočil. Špehonja je predstavil tudi program izobraževanja za zaposlene v organizacijah (angl. *Astec security awareness program*), s katerim uporabnike ozaveščajo o aktualnih grožnjah.

Miha Petrač (ADD) in Grega Zupanek (ElitAvia) sta predstavila primer, kako je podjetje v želji po izboljšanju razpoložljivosti in mobilnosti preneslo poslovne storitve v oblak. Zasebno letalsko podjetje je imelo v preteklosti težave s počasnim delovanjem sistemov in občasnimi izpadi storitev. V ta namen so izvedli prenovo: izbrali so dva ponudnika interneta hkrati, za varnost poskrbeli s požarnim zidom nove generacije, ki omogoča zaščito pred naprednejšimi grožnjami (NGFW – angl. *Next Generation Firewall*), hkrati pa so uvedli pametno brezžično omrežje. Njegova značilnost je, da ima eno glavno dostopno točko, prek katere se izvaja vsa konfiguracija in nadzor, preostale dostopne točke pa se ob primeru uporabe oz. dostopa avtomatsko povežejo na glavno točko, od katere pridobijo podatke o varnostnih omejitvah in konfiguracijah. S pomočjo teh informacijskih rešitev so prenovili obstoječo IT infrastrukturo in tako okrepili mobilnost uporabnikov s hitrejšim ter zanesljivejšim delovanjem sistemov in močnejšim nadzorom omrežja.

Roman Cupka (Flowmon networks) je predstavil inteligentno varnostno rešitev za spremljanje in nadziranje omrežnega prometa. Hitro, zanesljivo in dobro varovano omrežje je namreč za sodobne organizacije ključnega pomena, vendar zaradi razvoja groženj, obstoječe SNMP tehnike (ang. Simple Network Management Protocol), s katerimi se izvaja osnoven nadzor, klasična statistika nad obsegom prometa in uporabo pomnilnikov, ne zadostuje več. S predstavljeno rešitvijo lahko organizacije izboljšajo neprekinjeno poslovanje, saj je z njihovo platformo mogoče odkrivati anomalije na ravni omrežja in aplikacij, preprečevati napredne grožnje in diagnosticirati težave z natančno statistiko omrežnega prometa.

V nadaljevanju sta Samo Gaberšček in Simon Simčič (SRC) predstavila študijo primera – implementacijo varnostne rešitve SIEM, namenjene varovanju osebnih podatkov in spremljanju uporabe sistemov. Rešitev vključuje vèdenje o tem, kdo je dostopal do podatkov, kdaj in s kakšnim namenom. Predavatelja sta prikazala analitiko dostopov do podatkov. V grafičnem uporabniškem vmesniku se lahko za vsako stranko preveri, kdo je dostopal do njenih podatkov. Nato se lahko ugotavlja, kaj so počeli s podatki in če morda obstaja sum, da so prekoračili svoja pooblastila. Orodje omogoča spremljanje najbolj aktivnih uporabnikov in najbolj priljubljene dokumente. Naročnik ima tako nenehno vpogled v to, kaj zaposleni počnejo z osebnimi podatki drugih in kako jih uporabljajo. Na ta način je strankam lažje zagotoviti zasebnost, hkrati pa je možna izdelava profilov uporabnikov, kar bi se lahko uporabilo tudi pri behavioristični analizah.

Predavanje na temo socialnega inženiringa je izvedel Grega Prešeren (S&T Slovenija). Na začetku je poudaril, da največjo grožnjo informacijski varnosti predstavljajo ljudje – uporabniki, zato varnostne tehnologije niso vedno ali izključno učinkovite pri preprečevanju groženj. Veliko groženj prihaja z interneta, kjer se uporabniki pogosto nahajamo, približno 30–50 % groženj pa nam pri tem ni poznanih. Med zelo uporabne medije, ki jih storilci pogosto izkoriščajo, sodijo socialna omrežja, kjer pridobivajo podatke o profilu žrtev, s katerimi nato lažje navežejo stik. V drugem delu predavanja je predstavil realne prevare, s katerimi storilci dosežejo, da uporabniki škodljive kode naložijo na sistem. Med najpogostejše in hkrati najbolj uspešne uvrščamo: phishing prevare preko elektronske pošte z okuženimi priponkami, nigerijska pisma, uporabo zasebne elektronske pošte na službenih napravah, lažne telefonske klice s strani tehnične pomoči, ponarejene oglase na legitimnih straneh itd. Predstavljena je bila tudi prevara s pomočjo brezžičnega omrežja (t. i. *ewil twin wireless network*), iz česar je bilo zelo dobro razvidno, da je lahko zloraba brezžičnih povezav usodna za varnost organizacij, ne glede na vse varnostne tehnologije v podjetju.

Tamas Barna (Intel Security) je predstavil programsko opremo, o kateri je razpravljal tudi Schoenmaekers, namenjeno hitremu obveščanju strank o grožnjah in posodabljanju varnosti. Gre za zbiranje informacij o najnovejših grožnjah, s poudarkom na ciljanih napadih in naprednejših oblikah zlonamernih programskih kod. Preko platforme se podatki o grožnjah vnesejo v obstoječe oz. nameščene varnostne tehnologije v naročniški organizaciji, kar ji omogoča, da je njen varnostni sistem stalno aktualen in posodobljen.

Andrzej P. Kleśnicki (Qualys) je na začetku predavanja najprej razpravljal o količini informacijskih ranljivosti, ki smo jim izpostavljeni sodobni uporabniki. Število kritičnih ali zelo nevarnih ranljivosti je visoko, kar je potrdil s statističnimi podatki različnih poročil in raziskav. Opisal je tudi nekaj odmevnih primerov ranljivosti preteklega leta: npr. ranljivosti na požarnih zidovih Juniper Networks, Cisco napravah, OpenSSH protokolu in na Linux operacijskem sistemu. Glede na tvegano okolje, v katerem poslujejo organizacije, je v zaključku podal nekaj priporočil, kako se izogniti uresničenim grožnjam. Seveda je v prvi vrsta potrebna stalna pripravljenost v smislu aktivnega posodabljanja obstoječe tehnologije, velik pomen pa pripisuje tudi klasifikaciji lastniških podatkov ter močni zaščiti podatkov v oblakih. Kleśnicki poudarja, da je treba analizirati varnostne potrebe, postavljati racionalne varnostne cilje in biti previden pri izbiri novih tehnologij.

Aaron Boyd (Silent Circle) je razpravljal o problematiki zasebnosti, ki je danes zelo okrnjena in ogrožena. Tisti uporabniki, ki jim v sodobnem času uspe obvarovati lastno zasebnost, imajo veliko moč in prednost pred drugimi. Izzivi za varovanje zasebnosti izhajajo tudi iz dejstva, da trenutno obstaja veliko nezavarovanih oblik komunikacijskih sistemov in zlorab elektronskih komunikacij. Boyd je opozoril na pomembnost šifriranja podatkov in komunikacijskih kanalov, kar je po njegovem mnenju ključen element varnosti in zasebnosti uporabnikov mobilnih naprav. Poudaril je, da države pogosto zahtevajo, da jim telekomunikacijska podjetja omogočijo možnost nadzora in vpogleda v komunikacije na uporabniških napravah. Kadar se to zgodi, v napravah uporabnikov nastanejo »odprta vrata«, ki jo lahko izkoristijo tudi zlonamerneži in njihova škodljiva programska oprema, kar še dodatno povečuje tveganja na že tako ranljivih mobilnih napravah.

V predstavitvi je predstavil pametni telefon in operacijski sistem, ki v kombinaciji omogočata varno komunikacijo in prenos podatkov, s pomočjo »*peer-to-peer encryption*« komunikacijskega sistema. Na ta način je uporabniku v največji možni meri zagotovljena tako varnost na eni kot zasebnost osebnih podatkov na drugi strani.

Alexander Tomik (Riverbed) je predstavil rešitev za nadziranje, preverjanje in upravljanje aplikacij v organizacijskem okolju (APM – angl. *Aplication Performance Management*). Gre za celovit programski paket za diagnosticiranje napak, težav ali odstopanj na omrežnem in aplikacijskem nivoju. Poudarek je na testiranju in preverjanju aplikacij, njihovo analiziranje pa poteka globinsko: na ravni uporabe s strani uporabnika, na omrežni in internetni ravni, na podatkovni ravni in na nivoju izvorne kode ter programskega jezika. S takšnim pristopom je mogoče hitrejše odkrivanje in reševanje napak, ki upočasnjujejo delovanje sistemov, prav tako je s tem produktom mogoče identificirati (ne)odgovorne uporabnike.

Sandra Hilt (Centrify) je razpravljala o neustreznih predstavah, ki jih imamo ljudje glede informacijskih tveganj. Opozorila je, da smo ljudje manj občutljivi na kibernetske kot fizične grožnje, saj nam abstraktnost virtualnega okolja daje lažen občutek varnosti. Večina uporabnikov uporablja osnovne programske kontrole, ki pa so pogosto neučinkovite, saj jih napredne grožnje in storilci dobro poznajo in jih lahko zelo enostavno tudi zaobidejo. V nadaljevanju predavanja je predstavila varnostno rešitev – centralno SSO (angl. *single-sign-on*) platformo, v kateri so shranjene osebne ali službene aplikacije, vanjo pa uporabnik vstopi s pomočjo večnivojske avtentifikacije. Prvotna avtentifikacija uporabnika se izvede s pomočjo elektronskega naslova in gesla, za vpis pa je potreben še vnos kode, ki jo uporabnik prejme na mobilno napravo. V platformo oz. sistem lahko vključimo tudi naprave in s tem olajšamo sledenje aktivnostim, povezanih z uporabo teh naprav. S tem se poveča funkcionalnost uporabnika v smislu hitrejšega dostopa do uporabniških računov in aplikacij, prav tako pa se izboljša varnost. Uporabnik se izogne poplavi gesel, ki ga sili v oblikovanje nevarnih – enostavnih ali podobnih dostopnih kod. V primeru uporabe predstavljene platforme ima uporabnik eno, izredno močno geslo, ki je dodatno avtentificirano, z geslom, prejetim na mobilni napravi.

Raj Samani (Intel Security) je govoril o najnevarnejših grožnjah, ki smo jim uporabniki izpostavljeni pri uporabi spleta. Bolj konkretno se je, tako kot nekateri drugi predavatelji, osredotočil na problem razširjenosti izsiljevalske programske opreme (angl. *ransomware*). Opozoril je, da se je ta pojavila tudi za operacijske sisteme OS X, ki so do nedavno veljali za varne pred tovrstnim izsiljevanjem. Težava, ki jo opaža, je tudi v tem, da se tehnike storilcev in zlonamerni programi zelo hitro spreminjajo; nekateri izmed virusov dnevno spremenijo svojo kodo in podpis več kot tridesetkrat, zaradi česar jih antivirusni programi težko zaznajo. Eden izmed trenutno najbolj problematičnih izsiljevalskih programov je CryptoWall 3.0, s katerim so storilci zaslužili že več kot 300 milijonov ameriških dolarjev. Na koncu je poudaril, da tako kot strokovnjaki za varnost, tudi storilci uporabljajo analitične tehnike, s katerimi poskušajo povečati uspešnost svojih napadov. Profiliranje se dogaja predvsem na ravni phishing prevar, preko katerih se širijo najnevarnejši virusi. Samani je izpostavil, da uporabniki odgovornosti za

varnost ne smemo prelagati na tretje subjekte, saj je to izključno naša naloga, ki pa je seveda lažje uresničena v sodelovanju z IT strokovnjaki.

Hamut Pascha (SimpliVity) je razpravljal o problematiki varnega in hkrati hitrega dostopa do podatkov v oblakih, ki so v organizacijskem okolju zelo razširjeni. Kar 51 % aplikacij v poslovni rabi je trenutno povezanih z oblačno arhitekturo, medtem ko se do oddaljenih platform povezuje več kot 80 % zaposlenih. Ker infrastrukture oblakov postajajo vse bolj obsežne in kompleksne, sploh pa, kadar jih organizacije izvajajo v lastni režiji, je vse bolj očitna potreba po avtomatiziranem upravljanju in poenostavitvi arhitekture sistemov. V rešitvah, ki jih ponujajo, so združeni strežniški sistemi z vsemi potrebnimi vmesniki, sistemski administratorji pa lahko celoten sistem upravljajo na enem mestu.

Branko Lobnikar, Kaja Prislan in Blaž Markelj (Fakulteta za varnostne vede) so opozorili, da je treba pri uvajanju, sicer zelo učinkovitih varnostnih tehnologij, spoštovati zasebnost uporabnikov na delovnem mestu. Težava, ki jo vidijo, je v kontradiktorni situaciji, saj se z novimi rešitvami zaostruje in olajšuje nadzor, ki ga izvaja vodstvo v želji po varovanju lastnine in podatkov. To nemalokrat vodi do kršitev ustavno zavarovane pravice do zasebnosti. Avtorji so predstavili ugotovitve raziskave, izvedene med zaposlenimi v Sloveniji, glede odnosa do informacijskega in komunikacijskega nadzora, ki ga izvajajo njihove organizacije. Anketiranci so izrazili mnenje, da je nadzor presegel meje sorazmernosti in da se tehnike ne uporabljajo v prave namene. Ocenjujejo, da je glavni namen varnostnih rešitev predvsem nadzor nad zaposlenimi in ne dejansko v varovanju, kar naj bi bil primarni namen informacijskega in komunikacijskega nadzorovanja. Nadzor jih sicer ne moti, nimajo pa pozitivnega odnosa do namenov delodajalcev. Avtorji ugotavljajo, da obstoječe nadzorne tehnike ne vplivajo na poštenost ali produktivnost, veliko je takšnih zaposlenih, ki se tem kontrolam poskušajo izogniti. Pri tem opozarjajo, da lahko pretiran nadzor vodi v negativen odnos do varnosti in kršenje pravil, v primeru kršitve pravic pa je organizacija celo kazensko odgovorna. Avtorji zato priporočajo preudarno izbiro novih tehnologij, ki je pravilno pojasnjena uporabnikom, njihova zasebnost pa je upoštevana pri sami implementaciji (koncept vgrajene zasebnosti). Po mnenju Lobnikarja, Prislanove in Marklja določeno mero odgovornosti nosijo tudi ponudniki storitev, ki bi lahko pomagali pri informiranju naročnikov glede možnih pravnih in moralnih dilem, v primeru uporabe novih tehnologij.

Moni Stern (Checkmarx), Marko Šmid in Grega Prešern so predstavili varnostno rešitev CxSAST. Z njo se pregleduje, analizira oz. skenira ter popravlja izvorne kode statičnih aplikacij, ki so pogosto ranljive in zato predmet kompromitacije. Program lahko izvorno kodo pregleda v 18 različnih programskih jezikih, uporaben pa je predvsem v fazi razvijanja in testiranja aplikacij. Omogoča testiranje in pregled celotnih kod ali pa samo posameznih delov, s čimer razvijalci prihranijo veliko časa. Z njim lahko pred samo distribucijo aplikacije odpravimo napake in ranljivosti, saj je sposoben zaznati več kot sto najbolj kritičnih oz. pogostih napak, ki jih izkoriščajo spletni napadalci.

Sergej Pirh in Peter Stavanja (SRC) sta predstavila primer implementacije rešitve za nadzor zunanjih izvajalcev in študijo primera konkretne finančne ustanove. V uvodu sta opozorila, da največjo grožnjo organizacijam predstavljajo

lastni uporabniki (zaposleni, privilegirani uporabniki in zunanji izvajalci), saj imajo uporabniške pravice, s katerimi pri svojem delu dostopajo do podatkov, ki so za organizacije vitalnega pomena. Zaposleni pogosto z malomarno ali nevedno uporabo sistemov omogočajo izvedbo ali uresničitev zunanjih groženj. Predstavila sta delovanje programske opreme ObserveIT, ki služi kot programsko orodje za upravljanje notranjih tveganj, v smislu detekcije internih groženj in analitike uporabniškega vedenja. Njegova naloga je spremljanje in beleženje vseh aktivnosti, ki jih uporabnik izvaja v informacijskem sistemu, ter alarmiranje upravljavcev, če so aktivnosti v nasprotju z varnostno politiko organizacije. Po funkciji je takšna rešitev primerljiva z videonadzorom prostorov, le da se v tem primeru nadzor izvaja v informacijskem sistemu.

Robert Zelazo (Fireye) in Jure Šimundić (PBZ) sta predstavila potek prenove informacijskega sistema na primeru bančne institucije. Zahteve (med njimi tudi zlonamerne) v omrežje navadno prihajajo v ločenih paketih, težava pa je, da jih klasični varnostni sistemi (angl. *sandbox*) sicer analizirajo, vendar paketov medsebojno ne povežejo v morebiten sum zlonamernega programa. Zato je treba z medsebojnim povezovanjem paketov prepoznati in ovrednotiti škodljiv program, pred njegovo odstranitvijo oziroma onemogočanjem pa se preveri, katere podatke je zlorabil, kaj je z njimi počel in kakšno škodo je to povzročilo organizaciji. V nadaljevanju predavanj je predstavnik bančne institucije opisal potek prenove njihove informacijske strukture. V prvi fazi so naredili kontrolo in analizo omrežnega prometa in elektronske pošte, temu je sledila implementacija omrežnih varnostnih kontrol proti naprednim grožnjam, uvedba sistema upravljanja elektronske pošte, varovanja povezav med internetom in poštnim strežnikom ter preverjanje in izboljševanje kriptografskih protokolov. Kasnejša analiza varnostnega stanja je pokazala, da je bila pred implementacijo projekta banka ogrožena pred spletnimi napadi, grožnjami preko elektronske pošte in socialnim inženiringom, ranljivosti pa je bilo treba odpraviti tudi na ravni požarnega zidu, mobilnih naprav in strežnikov. Po uporabi takšnega varnostnega protokola se je varnost banke in njenih uporabnikov močno izboljšala.

Gerd Büttgen (VXL) je predstavil centralno platformo za upravljanje elektronskih naprav v organizacijskem omrežju (UDM – angl. *Universal Device Management*). V platformo je mogoče vključiti vse omrežne komponente, stacionarne, mobilne in podporne naprave. Platforma, nameščena na infrastrukturi ponudnika, omogoča spremljanje in nadziranje v nadzorni sistem vključenih naprav (stacionarni in prenosni računalniki, mobilne naprave, tiskalniki, strežniki, usmerjevalniki ipd.), oddaljeno upravljanje in posodabljanje, z različnimi možnostmi kriptiranja pa je poskrbljeno tudi za varnost. S platformo je mogoče na enem mestu nadzirati in upravljati informacijsko infrastrukturo organizacije.

Tim Grance (National Institute of Standards and Technology, ZDA) je uvodoma izpostavil štiri temeljne upravljavske izzive z vidika informacijske varnosti: (a) računalništvo v oblaku, (b) veliki podatki (angl. *big data*), (c) socialni mediji in (d) internet stvari (IoT). V nadaljevanju se je osredotočil na IoT trend, vse bolj prisoten tudi v organizacijskem okolju. Opozarja, da je področje zelo obsežno in kompleksno, z razvojem tehnologije pa se ta heterogenost še povečuje. Grance je koncept definiral kot medmrežno prepoznavanje in komuniciranje med napravami, kar zagotavlja prenos in dostop do velikih količin podatkov, hkrati pa

tudi oddaljeno upravljanje drugih naprav. Povezovanje poteka s pomočjo aplikacij in brezžičnega omrežja, lahko pa tudi preko klasičnega mobilnega omrežja. Med IoT naprave uvrščamo vse, kar je »pametno«, od bele tehnike, avtomobilske industrije, mobilnih naprav, strojev v proizvodnji do elektronskih naprav v zdravstvu itd. Kot največji (varnostni) problem Grance opredeljuje povezovanje kritične infrastrukture v internet, saj lahko zloraba teh povezav vodi v prevzem kontrole in potencialno do katastrofalnih posledic. Težave vidi tudi v zasebnosti uporabnikov in varnosti osebnih podatkov. V zaključku je predstavil prosto dostopne smernice in standarde, ki jih razvija organizacija NIST. Z njimi si lahko uporabniki in organizacije pomagajo pri razumevanju, ozaveščanju ali načrtovanju varnosti. Trenutno je v javni obravnavi osnutek priročnika, ki je namenjen upravljanju IoT področja. K podajanju predlogov je povabil vse zainteresirane subjekte, saj NIST spodbuja vključevanje javnosti v razvoj priporočil.

Neil Foxley (Entrust) je predstavil priporočila za učinkovito zaščito spletnih strani. Na začetku predavanj je povedal, da je varnost spletnih storitev in spletnih strani ključnega pomena za ugled organizacije, saj gre za glavne komunikacijske kanale, s katerimi podjetje sodeluje s strankami. Pri uporabi varnostnega protokola SSL, ki je zelo razširjen v praksi, se pojavlja mnogo ranljivosti, zaradi katerih je kompromitiranih veliko spletnih strani in uresničenih veliko spletnih vdorov. Foxley je predstavil načine zaščite spletnih in aplikacijskih strežnikov, ki trenutno sodijo med najbolj napadane komponente organizacijske infrastrukture. Poudarek teh rešitev je na uporabi ustreznih kriptirnih algoritmov v kombinaciji z digitalnimi potrdili, varnostnimi protokoli, varnostnimi tehnologijami na vstopnih točkah in spletnih strežnikih ter certifikatih na spletnih domenah.

Graham Wallace (Senetas) je predstavil rešitve na področju kriptiranja podatkov. Predstavljen je bil razvoj varnostnih tehnik za potrebe optičnih omrežij. Z razširitvijo optike se je pojavilo prepričanje, da je enkripcija na tovrstnem mediju nepotrebna, njim pa je s pomočjo diagnostičnih orodij in testiranj optičnih mrež avstralskih organizacij uspelo prebiti varnostno zaščito in vdreti v podatkovni tok optičnih mrež. S tem so dokazali, da je kriptiranje podatkov na tem področju prav tako pomembno. Vsebinskemu delu predavanja je sledil praktičen prikaz vohunjenja in kraje podatkov na optični povezavi – uspešno je prestregel videoposnetek v prenosu in na ta način udeležencem konference prikazal nevarnost zanemarjanja uporabe kriptografije na optičnih vodilih.

Andrej Rakar in Andrej Gornik (Slovenski inštitut za kakovost – SIQ) sta s tehničnega in praktičnega vidika predstavila aktualne hekerske napade. Poudarila sta različne primere groženj, predstavila sta že omenjeni Crypto virus, nato pa nadaljevala z vohunskimi programi za mobilne naprave, ki se širijo preko sistemskih posodobitev. Predstavila sta tudi napade z dešifriranjem varnostnih protokolov SSL/TSL, namenjenih kriptiranju komunikacij. Menita, da se bodo kibernetske grožnje razvijale še naprej, prihodnje trende pa bodo označevale predvsem informacijske sabotaže, izsiljevanje, dolgotrajno izkoriščanje informacijskih sistemov s pomočjo stranskih vrat (angl. *backdoor*), potenciali pa se kažejo tudi v t. i. *mousejack* napadih na brezžične miške in tipkovnice.

Siniša Popović (Interface Masters Technologies) je predstavil pristope, ki se ukvarjajo z razvijanjem inovativnih rešitev na področju omrežnih analitik. Podjetje (Niagara Networks) ponuja različne rešitve za optimizacijo in nadzor omrežnega prometa, v obliki zunanjih obhodnih »*switchov*« - posrednikov pri

prenosu podatkovnih paketov, aktivnega in pasivnega vsebinskega nadzora prometa, preprečevanja vohunjenja oz. kopiranja in časovnega žigosanja.

Andrej Žabkar in Simon Simčič (SRC) sta predstavila zagotavljanje neprekinjenega poslovanja podjetja na primeru storitve eRecepti Nacionalnega inštituta za javno zdravje (NIJZ). V ta namen je treba izdelati načrt okrevanja, ki zajema opis postopkov za čim hitrejše normaliziranje stanja in vzpostavljanja ponovne razpoložljivosti v primeru izpada sistema. Operativne sposobnosti okrevanja se navadno razvijejo skozi šest korakov: (1) preverjanje primernosti kapacitet sistema, (2) identificiranje kritičnih točk sistema, (3) ocena najhitrejše vključitve rezervne lokacije v sistem, (4) definiranje postopkov okrevanja za storitve, (5) periodična testiranja sistema za izboljšanje delovanja ob najvišjih obremenitvah, (6) preverjanje obnovitvenega procesa z visoko stopnjo avtomatizacije. V virtualnem okolju sta predavatelja demonstrirala preklapljanje med strežniki v Mariboru in Ljubljani v primeru izpada, prikazanih pa je bilo tudi nekaj preizkušenih testnih scenarijev izpada. S testiranjem so ugotovili, da se je čas okrevanja zmanjšal z 8 ur na 2 uri. Z načrtom neprekinjenega poslovanja se je povečala robustnost sistemske infrastrukture in izboljšala pripravljenost na nepričakovane katastrofalne dogodke. Ključne pridobitve podjetja pri izdelavi takšnega načrta neprekinjenega poslovanja so nižji stroški v primeru izpadov, preventivni ukrepi znižujejo tveganje motenj v poslovanju, ne nazadnje pa je čas okrevanja veliko hitrejši.

Rolf Schroeder (Wacom) je predstavil poslovne rešitve za hitrejše poslovanje. Poudarek storitev, ki jih ponujajo, je na elektronskem poslovanju, podpisovanju, finančnih transakcijah, upravljanju računov in izpolnjevanju dokumentacije. Ponujajo elektronsko tablico, ki na enostaven način omogoča izvedbo vseh teh aktivnosti, s čimer se organizacija izogne ali občutno zmanjša papirno poslovanje.

Rdeča nit konference, ki so jo poudarjali predstavniki organizacij in predavatelji, je bila vezana na hiter tempo razvoja varnostnih ranljivosti na področjih, kot so oblak, internet stvari, socialni mediji in mobilne naprave. Veliko poudarka je bilo tudi na predstavitvi in demonstracijah delovanja novodobnih groženj, predvsem phishing napadov, na katere so zaposleni v organizacijah zelo ranljivi, in izsiljevalskih programov, ki organizacijam onemogočajo neprekinjeno poslovanje. Dodatne težave, s katerimi se soočajo organizacije, se kažejo v varčevanju na varnostnem področju in pomanjkanju strokovnega kadra, kar je posredna posledica nekvalitetnih izobraževalnih programov. Pomanjkanje talenta na varnostnem področju je pereč problem, ki postaja vse bolj očiten, saj storilcem daje še večjo prednost, medtem ko v organizacijah zavira razvoj. Razpravljavci na konferenci so se strinjali s potrebo po izboljšanju usposobljenosti kadrov in racionalni izbiri obstoječih rešitev. Ker količinski in kvalitativni razvoj kibernetskih groženj glede na napovedi ne bo stagniral, je izvajanje takšnih in podobnih izobraževalnih dogodkov v slovenskem prostoru nujno potrebno tudi v prihodnosti.

Konferenca se je zaključila z dobrodelno dražbo, namenjeno zbiranju denarja za slovensko društvo Rdeči noski. S tem je organizator (Risk Security) jasno poudaril potrebo po pomoči, medsebojnem povezovanju in solidarnosti varnostne stroke, ki ima možnost in sposobnost izboljšati svet, ne samo na poslovnem, temveč tudi drugih področjih.

Kaja Prislan, Branko Lobnikar