Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
mag. Marko Mišmaš, direktor Agencije za komunikacijska omrežja in storitve Republike Slovenije*

NEPREKINJENOST DELOVANJA KLJUČNIH KOMUNIKACIJSKIH OMREŽIJ TUDI V PRIHODNJE POMEMBEN FOKUS DELOVANJA AKOS

Nenehen tehnološki razvoj na eni strani, na drugi strani pa vedno večja intenziteta cele vrste varnostnih izzivov, pred sektor informatike in telekomunikacij postavljata resne strokovne dileme, kako ustrojiti sistem, da bo dovolj robusten in sposoben neprekinjenega delovanja. O perečih razvojnih vidikih smo se pogovarjali z mag. Markom Mišmašem, novim direktorjem AKOS.

Najprej nam dovolite, da vam čestitamo ob imenovanju na to pomembno funkcijo. Nam lahko prosim zaupate nekaj o vaših predhodnih referencah, ki bodo vsekakor pomembne za upravljanje te odgovorne funkcije?

Najlepša hvala za čestitke! Po izobrazbi sem magister telekomunikacij, na agencijo pa prihajam iz industrije, kjer sem delal 22 let. V svoji karieri sem delal v različnih sektorjih; telekomunikacijah, energetiki in avtomobilski industriji na različnih vodstvenih funkcijah v razvoju in prodaji. Skupno vsem trem je ime Iskra; Iskratel, Iskraemeco in Iskra Mehanizmi. Agencijo pa poznam zelo dobro, saj sem bil zadnja dva mandata tudi član Sveta agencije, ki predstavlja njen nadzorni organ.

Strateški varnostni izzivi, pred katerimi stoji Slovenija kot del mednarodnega okolja, bodo imeli pomemben vpliv na delovanje AKOS-a. Kje pričakujete največje izzive, ki sledijo področjem, ki jih upravljate v vaši agenciji?

Z uveljavitvijo oz. implementacijo NIS 2 se na področju zagotavljanja varnosti za nekatere sektorje, ki so tudi v pristojnosti agencije, obetajo kar precejšnje spremembe. Kot konvergentni regulator in še zlasti regulator in nadzorni

> Kot konvergentni regulator in še zlasti regulator in nadzorni organ za varnost sektorja elektronskih komunikacij, ki so ključne za zagotavljanje številnih ostalih storitev kritične infrastrukture, čutimo na tem področju veliko odgovornost. Hkrati pa vidim odlično priložnost, da prav z izkušnjami iz sektorja elektronskih komunikacij, pri spopadanju z varnostnimi izzivi pomagamo ostalim sektorjem, ki jih agencija nadzira.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

organ za varnost sektorja elektronskih komunikacij, ki so ključne za zagotavljanje številnih ostalih storitev kritične infrastrukture, čutimo na tem področju veliko odgovornost. Hkrati pa vidim odlično priložnost, da prav z izkušnjami iz sektorja elektronskih komunikacij, pri spopadanju z varnostnimi izzivi pomagamo ostalim sektorjem, ki jih agencija nadzira. Ker postajajo strateški vidiki pri varnostnih izzivih vedno bolj pomembni, sem vesel, da imamo na tem področju vzpostavljeno (tudi zakonsko) sodelovanje z URSIV. URSIV je pristojni nacionalni organ za informacijsko varnost, enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja, preko SNAV pa je umeščen tudi v sistem nacionalne varnosti. URSIV kot del Skupine za sodelovanje NIS ter agencija smo, v okviru mednarodnih organizacij ENISE in BEREC, pomembno vpeti v mednarodno okolje, kjer se zagotavlja potreben pretok informacij. Med pristojnimi nacionalnimi organi se na mednarodnem nivoju vzpostavlja tudi nujno potrebno čezmejno sodelovanje, saj vemo, da varnostni izzivi nikakor niso prostorsko omejeni zgolj na posamezne države.

Dejanska implementacija v poslovanje in delovanje zavezancev pa bo naslednja pomembna in zahtevna faza. Tukaj sem vesel, da je agencija tudi članica Slovenskega združenja za korporativno varnost, kjer se na srečanjih članov in konferencah veliko razpravlja o dobrih praksah in resničnih primerih. V pomoč članom pa je tudi vedno močnejši Inštitut za korporativno varnost.

Krize si v zadnjem obdobju kar sledijo, s tem pa je še bolj izpostavljen pomen kritične infrastrukture, zlasti varnost in odpornost komunikacijskih sistemov. Menite, da so se operaterji informacijsko komunikacijskih storitev ustrezno odzvali na izzive teh kriz?

Operaterji se na te krize odzivajo konstantno in se pripravljajo tudi za prihodnje izzive. Je pa glede na pomembnost sektorja in odvisnost celotne družbe od teh storitev potrebno razmisliti, kako bi lahko to infrastrukturo naredili še bolj odporno in kako lahko različni deležniki, tudi država, pri tem pomagajo.

Približuje se zimsko obdobje in ob tem spet opozorila o možnem pomanjkanju določenih energentov. Ste uspeli telekomunikacijsko področje ustrezno pripraviti na te izzive in realno oceniti, katera je tista infrastruktura in procesi, ki v primeru redukcij električnega toka ne smejo ostati brez le te?

Medsebojna soodvisnost je ključno in predhodno vprašanje. Omrežja nikoli ne bodo mogla delovati brez električne energije in prekinitev napajanja bo zagotovo vedno vplivala na delovanje omrežja. Manj problematični so krajši in lokalni izpadi, za daljše in obsežnejše pa je nujno potrebno sodelovanje vsaj navedenih sektorjev. Elektronska komunikacijska omrežja so zelo razvejana. Za ilustracijo, v Sloveniji imajo trije mobilni operaterji na dostopovnem delu prek 4000 lokacij in vse bi bilo potrebno opremiti z rezervnim napajanjem. Cena tega je seveda

močno odvisna od zmogljivosti, to pa na koncu vedno plača končni uporabnik. Ker je agencija, ki poleg regulacije trga skrbi tudi za zaščito uporabnikov, skupaj z operaterji tovrstne težave že prepoznala, je aktivno pristopila k iskanju različnih načinov za čim bolj učinkovit spopad tudi z izzivom pomanjkanja električne energije zaradi izvajanja redukcij.

Pred nekaj časa je bil sprejet nov Zakon o elektronskih komunikacijah (ZEKom-2). Sedaj počasi prihaja dovolj dolg časovni okvir od sprejema, da lahko naredite prve analize o uspešnosti uveljavitve teh zakonskih dopolnil. Ste zadovoljni s hitrostjo in resnostjo implementacije določil pri vseh zavezanih subjektih?

Ker gre za precejšnje število sprememb, med njimi tudi takšnih, za katere je potrebno prilagajanje poslovanja, je ta hip to kljub vsemu še nekoliko preuranjeno. Če se recimo navežem na poglavje o varnosti, smo s pripravo podzakonskih aktov, ki so bili za agencijo najtrši oreh, trenutno v zaključni fazi. Od uveljavitve ZEKom-2 je agencija pripravila in v Uradnem listu objavila že 33 splošnih aktov. Od treh splošnih aktov, ki urejajo varnost in jih je agencija pripravila v sodelovanju z URSIV, je javno posvetovanje zaključil še zadnji, agencija pa je tudi že objavila odgovore na pripombe, prejete v tem posvetovanju. Ta zavezuje operaterje, ki storitve ponujajo kritičnim subjektom. Prihodnji zavezanci so bili kar intenzivno vpleteni v sam postopek sprejemanja navedenih predpisov. Agencija je prav zaradi vseh sprememb, ki jih ti podzakonski predpisi vpeljujejo, z operaterji organizirala tudi več delavnic, na katerih se je odvijala zelo odprta razprava. Hkrati pa je bilo potrebno za prilagoditev prihodnjim zavezancem dopustiti tudi dovolj dolgo prehodno obdobje za prilagoditev oziroma implementacijo pravil.

Kaj pomembnega se je zgodilo na ravni EU, kar bo vplivalo tudi na vaše delovanje in na splošno na delovanje sektorja telekomunikacij?

Med najpomembnejšimi akti, čeprav priporočilne narave, je bil zagotovo Nabor orodij za kibernetsko varnost 5G (t.i. 5G Toolbox). Evropska komisija bdi nad državami članicami in implementacijo vseh priporočilnih, tako tehničnih kot tudi strateških ukrepov. V juniju je Skupina za sodelovanje NIS izdala že drugo poročilo o nacionalnih implementacijah ukrepov. Vesel sem, da bo Slovenija s sprejetjem prej omenjenih splošnih aktov in po sprejemu ZEKom-2 veliko večino ukrepov uspešno implementirala v svoj pravni red. Dejanska implementacija v poslovanje in delovanje zavezancev pa bo naslednja pomembna in zahtevna faza. Tukaj sem vesel, da je agencija tudi članica Slovenskega združenja za korporativno varnost, kjer se na srečanjih članov in konferencah veliko razpravlja o dobrih praksah in resničnih primerih. V pomoč članom pa je tudi vedno močnejši Inštitut za korporativno varnost. Pred nami pa je še veliko izzivov, npr. konec leta bo v javnem posvetovanju Evropska certifikacijska shema za 5G varnost, pripravlja pa se še kar nekaj novih predpisov s področja (kibernetske) varnosti.

Pred nami so tudi pomembni koraki uveljavitve dveh pomembnih evropskih direktiv CER in NIS 2. Ste ustrezno vpeti v medsektorske načrtovalne korake za uvajanje teh dveh direktiv v naš pravni sistem?

Agencija je aktivno spremljala že sprejemanje navedenih predpisov. S sprejemom NIS-2 se je področje varnosti elektronskih komunikacij premaknilo iz okvira elektronskih komunikacij v okvir NIS. Natančneje, določila NIS-2 so razveljavila 40 in 41. člen Evropskega zakonika o elektronskih komunikacija, ki urejata varnost in poročanje incidentov. Vsebinsko se za sektor elektronskih komunikacij kljub vsemu ne spreminja zelo veliko, saj NIS-2 precej sledi obstoječi ureditvi v Zakoniku. Nekatere prilagoditve v nacionalni zakonodaji bodo verjetno potrebne in tu pričakujemo dobro in tesno sodelovanje z enotno kontaktno točko po NIS, ki je v Sloveniji URSIV. V implementaciji CER pa vidimo še kako potrebno komplementarno ureditev k NIS, kjer pa bodo kompetence in izkušnje agencije kot konvergentnega regulatorja lahko prav tako koristne.

Kibernetska varnost postaja vedno bolj pereči izziv za organizacije, državo in tudi mednarodno skupnost. Na področju kritične infrastrukture so se uveljavile določene spremembe, kjer je naloge nosilca sektorja »informacijsko komunikacijskih omrežij in sistemov« prevzel Urad RS za informacijsko varnost. Je sodelovanje z omenjenim URSIV na ustrezni ravni in prinaša potrebne rezultate za krepitev tega kompleksnega sektorja, kjer imate ravno vi

skozi resorni zakon (Zekom-2) izredno velika pooblastila vezana na telekomunikacijske operaterje?

Z URSIV dobro sodelujemo. Naša najtežja skupna naloga je bila priprava podzakonskih aktov s področja varnosti na podlagi ZEKom-2. Sodelovanje med organoma je urejeno z ZEKom-2, na njegovi podlagi agencija poroča URSIV tudi o incidentih, ki jih je prejela s strani operaterjev elektronskih komunikacij. Ker je obstoječa podlaga, torej ZEKom-2, za sodelovanje med organoma še relativno nova, kar prav tako velja za prenašanje NIS 2 v nacionalni pravni red, si oboji prizadevamo za krepitev formalnega in neformalnega sodelovanja. S tem namenom smo se odzvali tudi prijaznemu vabilu ICS za vključitev v evropski projekt ENDURANCE, ki je namenjen prav iskanju sinergij in izboljšanju sodelovanja med ključnimi akterji za delovanje kritične infrastrukture.

Na področju kibernetske varnosti bo verjetno potrebno narediti še veliko smelih korakov, še posebej na področju pridobivanja ustreznih strokovnjakov. S tem izzivom se verjetno srečujete tudi na AKOS?

S pomanjkanjem ustreznih strokovnjakov se soočajo že podjetja, tudi večja, kaj šele državni organi. Pri tem delimo zelo podobno usodo z drugimi regulatorji v Evropi. Kar nas rešuje, če smem tako reči, je, da smo dobro vpeti tako v nacionalno mrežo kot tudi v mednarodno okolje. Združenja, kot je vaše, in vedno številčnejši dogodki ter konference na nacionalnem parketu, pripomorejo k pridobivanju novih znanj in izobraževanju obstoječega kadra. Trudimo se biti precej aktivni tudi na evropskem nivoju, kjer so naši strokovnjaki člani ekspertnih delovnih skupin s področja kibernetske in informacijske varnosti v ENISI in združenju BEREC.

Ob zadnji tragični naravni nesreči se je ponovno odprla žolčna razprava o tem zakaj Slovenija zamuja z uvajanjem učinkovitega sistema javnega obveščanja in alarmiranja v primeru večjih nesreč. Kako lahko AKOS pomaga, da čimprej dobimo ta delujoč sistem, kjer bo vsak državljan, ki se nahaja na določenem ogroženem območju pravočasno obveščen o možnih grožnjah?

Agencija s svojim članom sodeluje v delovni skupini za pripravo Uredbe, ki ureja vzpostavitev tega sistema, ni pa seveda njen nosilec. Zamude zato težko komentiram. So se pa že spomladi tudi na tem področju zgodili pomembni premiki, osnutek je že bil v javnem posvetovanju in po vedenju agencije tudi na izvedbeni ravni uvedba sistema ni več tako daleč.

Kako ste zadovoljni z vašim delovanjem v okviru Slovenskega združenja korporativne varnosti? Boste tudi vi nadaljevali zagovarjanje aktivne participacije AKOS znotraj tega pomembnega združenja?

Prepričan sem, da je ICS res super okolje za izmenjavo dobrih praks, tako na mesečnih srečanjih članov Slovenskega združenja za korporativno varnost kot tudi vseh ostalih dogodkih in konferencah, ki jih organizira Institut za korporativne varnostne študije. Agencija si bo prizadevala po svojih najboljših močeh, z vsem svojim znanjem in izkušnjami, tudi v prihodnje prispevati h konstantni rasti zavedanja o pomembnosti informacijske varnosti v državi. ■