Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Tanja Muha
direktorica Agencije za komunikacijska omrežja in storitve Republike Slovenije*

VARNOSTNI IZZIVI POSTAVLJAJO NEPREKINJENOST DELOVANJA ELEKTRONSKIH OMREŽIJ V POSEBEN POLOŽAJ

Moderno in dinamično varnostno okolje pred nas prinaša vedno nova tveganja in izzive, na drugi strani pa tehnologija napreduje z nesluteno hitrostjo. Če v ta okvir dodamo še vedno pogostejše pojavljanje različnih kibernetskih tveganj, lahko z gotovostjo potrdimo, da je to področje trenutno podvrženo velikim izzivom, ki jih je potrebno ustrezno uravnavati. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Tanjo Muha.

Vodite Agencijo za komunikacijska omrežja in storitve Republike Slovenije, ki ima zelo obširen nabor pristojnosti. Nam lahko na kratko opišete na katerih področjih vse ima AKOS pomembno vlogo.

Agencija kot regulatorni organ obstaja že vse od leta 2001, ko je bila primarno pristojna na področjih telekomunikacij, pošte in upravljanja z radiofrekvenčnim spektrom. Danes bi lahko pristojnosti agencije razdelili na pet glavnih področij, to so: elektronske komunikacije, pošta, elektronski mediji, železniški promet in upravljanje z radiofrekvenčnim spektrom. Znotraj teh sektorjev, pa ima agencija več pristojnosti, med drugim tudi na področju zagotavljanja celovitosti in varnosti telekomunikacijskih omrežij in storitev, ter varstva končnih uporabnikov.

> Operaterji morajo skladno z zakonodajo sprejeti ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj omrežij in storitev, prav tako pa tudi ukrepe za zagotavljanje celovitosti omrežij, da se zagotovi neprekinjeno izvajanje storitev.

Izredno aktivno sodelujete v okviru mednarodnih organov EU. Nam lahko kratko predstavite te aktivnosti agencije.

Agencija je članica združenj evropskih regulatorjev na vseh področjih njenega dela in pristojnosti, v okviru katerih aktivno sodeluje pri pripravi dokumentov, in s tem sooblikuje regulatorne politike na evropskem nivoju. Predstavniki agencije se redno udeležujejo sestankov ekspertnih delovnih skupin ter plenarnih zasedanj. Agencija pa redno sodeluje tudi z Evropsko komisijo in Agencijo evropske unije za varnost omrežij in informacij - ENISO. V letošnjem letu je agencija na tem področju še posebej aktivna, saj sem sama podpredsednica združenja evropskih regulatorjev za elektronske komunikacije BEREC, vodja sektorja na agenciji Katja Kmet Vrčko

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

pa je sopredsednica ekspertne delovne skupine, ki se ukvarja z vprašanjem kibernetske varnosti v 5G omrežjih.

Kibernetska varnost postaja eden od najpomembnejših izzivov modernega varnostnega okolja. Kako v tem okviru zagotavljati ustrezno varno in neprekinjeno delovanje telekomunikacijskih operaterjev?

Prvi pogoj za to je zakonodaja, ki zavezuje operaterje k določenim ravnanjem. Drugi pogoj pa je dejansko izvajanje zakonodaje v praksi. Obveznosti operaterjev na tem področju določa Zakon o elektronskih komunikacijah. Operaterji morajo skladno z zakonodajo sprejeti ustrezne tehnične in organizacijske ukrepe za obvladovanje tveganj omrežij in storitev, prav tako pa tudi ukrepe za zagotavljanje celovitosti omrežij, da se zagotovi neprekinjeno izvajanje storitev. Operaterji morajo tudi redno obveščati agencijo v primerih kršitev varnosti ali celovitosti, če so te pomembno vplivale na delovanje omrežij ali izvajanje storitev. Agencija lahko zahteva revizijo varnosti in sprejem ter izvajanje varnostnega načrta, v kolikor se to izkaže za potrebno. Agencija pa je pripravila in sprejela tudi Splošni akt o varnosti omrežij in storitev, ki podrobneje določa način vzpostavitve sistema upravljanja varovanja informacij (SUVI) in sistem upravljanja neprekinjenega poslovanja (SUNP). V zakonu so predpisani tudi ukrepi v primeru izjemnih stanj. Agencija izvaja nadzor nad spoštovanjem teh zahtev na strani operaterjev in v primeru nespoštovanja tudi ustrezno sankcionira kršitelja. Se pa agencija zaveda, da je mogoče marsikaj rešiti še preden agencija uvede nadzorne postopke. Z namenom, da operaterji spoštujejo zakonodajo, agencija tako z operaterji redno sodeluje in jim nudi podporo pri ustrezni implementaciji zahtev zakonodaje. Pomembno je tudi seznanjanje operaterjev z novostmi oziroma dogajanjem na teh področjih, tako da si bo agencija tudi v prihodnje prizadevala tudi za preventivno delovanje in ustrezno informiranje, ter izmenjavo znanja z operaterji in tudi drugimi pristojnimi institucijami in organi.

Pred nami stoji še zahtevna implementacija določil Zakona o informacijski varnosti, kot posledica evropske NIS direktive. Kako sodelujete z nosilno institucijo za uveljavitev omenjenega zakona in predvsem procesov kibernetske varnosti?

Pristojnosti agencije na področju zagotavljanja varnosti in celovitosti omrežij in storitev segajo že skoraj 10 let nazaj. V tem času je agencija pridobila veliko dragocenih izkušenj na tem področju, ki so sedaj dobrodošle pri sami implementaciji NIS direktive. Že v preteklosti je agencija z vsemi ostalimi resornimi organi na področju zagotavljanja varnosti imela vzpostavljeno zgledno sodelovanje, ki se sedaj nadaljuje z vključitvijo novih organov. Agencija ima vzpostavljeno redno sodelovanje tudi z Upravo za informacijsko varnost, ki je bila ustanovljena letos. Tako je bila agencija vključena v delovno skupino za pripravo Zakona o informacijski varnosti, ki jo je vodilo pristojno ministrstvo, skupaj pa smo pripravljali tudi oceno tveganj 5G omrežja z vidika kibernetske varnosti v Republiki Sloveniji, ki jo je zahtevalo Priporočilo Evropske komisije o kibernetski varnosti 5G omrežij. Kaže se, da je agencija pomemben člen pri oblikovanju pristopov in politik na teh področjih, ravno zaradi večletnih izkušenj, aktivnega delovanja in nekaterih že vzpostavljenih pristopov. Tako namerava agencija tudi v prihodnje sodelovati in nuditi podporo s svojim strokovnim znanjem, v kolikor bo k sodelovanju povabljena s strani pristojnih organov.

Kako bi ocenili izzive, ki jih prinašajo geopolitične napetosti med glavnimi svetovnimi velesilami in Evropo? Veliko je bilo napisanega o prepovedi kitajskih ponudnikov tehnologije 5G. V katero smer bodo po vaših izkušnjah in informacijah šle evropske države, med njimi tudi Slovenija?

To je zelo kompleksno vprašanje, ki buri dogajanje tako na nacionalnem, evropskem, kot tudi svetovnem nivoju, in vključuje več vidikov preučevanja, med drugim varnostni, ekonomski in zunanjepolitični. In temu primerno je potrebnega tudi več časa za iskanje ustreznega enotnega odgovora. 5G omrežje bo preoblikovalo našo družbo in gospodarstvo ter odprlo nove priložnosti za ljudi in posel. Je pa zato nujno potrebna vzpostavitev ustrezne oblike mehanizma zagotavljanja varnosti. Evropska komisija se je tega lotila na način, da je sprejela Priporočilo o kibernetski varnosti 5G omrežij, na podlagi katerega so države članice morale do konca meseca junija pripraviti svoje ocene tveganj 5G omrežij z vidika kibernetske varnosti. Trenutno pa, v sodelovanju z Evropsko komisijo in ENISO, BEREC v okviru delovne skupine, kateri naša agencija sopredseduje, pripravlja usklajeno oceno tveganj držav članic, ter na podlagi tega orodje za definiranje nabora ustreznih, učinkovitih in sorazmernih možnih ukrepov za obvladovanje tveganj pri 5G omrežju. V tem času so nekatere države članice že sprejele individualne odločitve glede uporabe opreme kitajskega proizvajalca opreme Huawei. Tako se je na primer Nemčija odločila, da ne bo prepovedala Huaweijeve opreme pri gradnji omrežij 5G. Za sodelovanje pri gradnji omrežja 5G s Huawei pa se dogovarja tudi Italija. Francija je trenutno edina država, ki je uzakonila možnost podaje veta na uporabo določene vrste opreme. Končne odločitve glede tega v Sloveniji še ni, je pa dejstvo, da so že obstoječa mobilna omrežja v Sloveniji grajena z opremo Huawei. Zato je potrebno o morebitnih prepovedih resno razmisliti, saj bi to lahko imelo resne posledice na vračanje že investiranih sredstev in tudi višino bodočih investicij operaterjev.

Kje vidite glavne varnostne izzive, ki jih prinaša pričakovana uveljavitev tehnologije 5G?

Kot že rečeno bo 5G omrežje preoblikovalo našo družbo in gospodarstvo ter odprlo nove priložnosti za ljudi in nove poslovne priložnosti. Zaradi tehničnih karakteristik 5G omrežij in posledično možnosti njegove uporabe se bo to

omrežje uporabljalo na vseh segmentih družbe in na sektorjih, ki se sedaj v to zgodbo še niso vključevali. Govorimo o pametni industriji 4.0, širjenju obsega e-storitev na področju zdravja, izobraževanja, poslovanja, povezovanja pametnih naprav M2M in internetu stvari, pametnih omrežjih (smart grid), upo-

Kot že rečeno bo 5G omrežje preoblikovalo našo družbo in gospodarstvo ter, odprlo nove priložnosti za ljudi in nove poslovne priložnosti. Zaradi tehničnih karakteristik 5G omrežij in posledično možnosti njegove uporabe se bo to omrežje uporabljalo na vseh segmentih družbe in na sektorjih, ki se sedaj v to zgodbo še niso vključevali.

rabi dronov in samovozečih vozil, in nenazadnje o možnostih uporabe za javno varnost, ter zaščito in reševanje (PPDR). S povezovanjem velikega števila sistemov in naprav, ter posledičnega zbiranja ogromnega števila podatkov, se veča tudi možnost različnih zlorab. In zlorabe se v takem okolju lahko dogajajo tako na strani naprav pri končnih uporabnikih, kot tudi na samem omrežju. Zato je potrebno poleg mehanizmov in zakonodaje, ki skrbijo za varstvo osebnih podatkov in zasebnosti, poskrbeti tudi za ustrezne mehanizme in zakonodajo, za zagotavljanje informacijske in kibernetske varnosti, ter varnosti samih omrežij. Še vedno velik del tveganj pa predstavljajo uporabniki storitev sami, ki se ne zavedajo svojega dela odgovornosti v tem okolju. Treba je osveščati tudi uporabnike.

Kakšen pomen v AKOS namenjate procesom izobraževanja in usposabljanja? Je to z vaše perspektive učinkovit vzvod za dvigovanje splošnega zavedanja, posebej med operaterji?

Kot zelo pomemben dopolnilni del k sami regulaciji vidimo tudi samoregulacijo, pri spodbujanju katere pa veliko lahko pripomore ozaveščenost končnih uporabnikov, ki se posledično bolj zavedajo svojih pravic in obveznosti. Zato agencija veliko pozornost namenja tudi opismenjevanju na področju varnosti na svojem novem portalu za medijsko in informacijsko pismenost – MIPI, pri čemer se je dogovorila za sodelovanje tudi z drugimi organi, ki se ukvarjajo s tovrstnimi vprašanji. V kolikor se izkažejo potrebe, agencija organizira tudi različne delavnice za operaterje, kar se je prav tako izkazalo za koristno.

Ste tudi inšpekcijski organ, ki predvsem skrbi za uveljavitev in izpolnjevanje določil Zakona o elektronskih komunikacijah (Zekom). Kakšni so vaši generalni občutki in ocena glede stanja v praksi med operaterji? Je to zavedanje po ustrezni implementaciji varnostnih zahtev na dovolj visokem nivoju?

Vsi operaterji morajo na podlagi nacionalne zakonodaje sprejeti takšne varnostne ukrepe, ki so primerni predvidenemu tveganju oz. izhajajo iz analize tveganj, pri čemer morajo upoštevati značilnosti svojega poslovanja, velikosti organizacije, pomembnosti funkcij in storitev, ki jih zagotavljajo. Zavedanje

Združenje omogoča, da se srečujejo na enem mestu strokovnjaki s področja zagotavljanja varnosti, ki izmenjujejo dobre prakse, tako da lahko vsi člani pridobimo z vključenostjo v to združenje. Pri tem ni nezanemarljivo, da združenje povezuje tako deležnike iz različnih panog privatnega sektorja, kot tudi javnega sektorja.

potrebnih varnostnih zahtev je pogojeno tudi z zrelostjo operaterja. Večji operaterji so za svojo usposobljenost začeli pridobivati certifikate, kot so za sistem upravljanja neprekinjenega poslovanja (ISO 22301) ali za sistem vodenja varovanja informacij (ISO 27001). Nadalje so nekateri že vzpostavili operativne varnostne centre, ki bdijo nad dogajanjem v omrežju in imajo vzpostavljene procese ravnanja v primeru določenih varnostnih incidentov, ali v primeru napak ali okvar v omrežju. Izvajajo redne ocene tveganja, ter posodabljajo svojo varnostno politiko in politiko neprekinjenega poslovanja glede na tveganja s katerimi se soočajo oz. so jih prepoznali v okviru svojih analiz. Pri manjših operaterjih je to zavedanje na nižjem nivoju oziroma so razpoložljiva finančna sredstva za zagotavljanje visoke varnostne ravni bistveno manjša. Vseeno pa lahko pri tem do določene mere upoštevamo tudi dejstvo, da posamezen negativni dogodek pri manjših operaterjih vseeno nima tako velikega vpliva oz. prizadene manjše število uporabnikov, storitve, ki jih zagotavljajo ti operaterji, pa niso kritične za državo in njene funkcije.

Predstavniki AKOS so izredno aktivni pri delovanju v okviru Slovenskega združenja korporativne varnosti. Kakšne so vaše izkušnje z delovanjem v omenjenem združenju?

Združenje omogoča, da se srečujejo na enem mestu strokovnjaki s področja zagotavljanja varnosti, ki izmenjujejo dobre prakse, tako da lahko vsi člani pridobimo z vključenostjo v to združenje. Pri tem ni nezanemarljivo, da združenje povezuje tako deležnike iz različnih panog privatnega sektorja, kot tudi javnega sektorja.

Menite, da je združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti lahko odgovor na obvladovanje zahtevne varnostne situacije, in ali so lahko taka združenja ustrezen partner državnim institucijam, kot je AKOS, pri zagotavljanju njenega osnovnega poslanstva?

Ko se pogovarjamo o informacijski in kibernetski varnosti v luči digitalizacije družbe in vpeljave 5G omrežja, se obseg vključenih deležnikov zelo poveča. Prihaja do prepletanja sektorjev, ki so se do sedaj bolj redko srečevala, mnoga med njimi pa tudi še niso posvečala potrebne pozornosti zagotavljanju varnosti. Zato je po mojem osebnem mnenju ključno povezovanje in izmenjevanje znanj, izkušenj in dobrih praks, ter seveda ozaveščanje vseh vpletenih. Združenje korporativne varnosti je primer dobrega načina povezovanja, ki zagotovo lahko pripomore k kvalitetnejši razpravi in skupnemu doseganju zastavljenih ciljev.

Agencija bo še naprej proaktivno sodelovala z drugimi pristojnimi organi na področju zagotavljanja varnosti, pri tem pa si bo prizadevala za vzpostavitev enotnega informacijskega orodja za poročanje o incidentih, kar bi poenostavilo tako delo organom, kot tudi zavezancem za poročanje.

Za konec bi vas prosili, da kratko ocenite izzive, ki stojijo pred agencijo v prihodnosti.

V prihajajočih mesecih bo agencija imela zagotovo še veliko dela pri pripravi ustreznih podlag v okviru vodenja delovne skupine v BEREC in pri sodelovanju z Ministrstvom za javno upravo pri implementaciji prenovljenega evropskega zakonika na področju elektronskih komunikacij, ki tudi na področju varnosti omrežij in storitev prinaša kar nekaj novosti. V prihodnje bo zagotovo treba oblikovati ustrezne obveznosti dobaviteljev opreme in posodobiti obstoječe varnostne zahteve za operaterje omrežij na nacioalnem in evrospkem nivoju. Agencija se pripravlja na javni razpis z javno dražbo frekvenc za javne mobilne storitve, med drugim tudi za 5G omrežje. Na podlagi ugotovljenih tveganj bo verjetno treba vključiti pogoje za zagotavljanje varnosti javnih omrežij tudi pri dodeljevanju pravic uporabe teh frekvenc. Veliko bo treba narediti tudi na ozaveščenosti končnih uporabnikov. Tako je agencija v letošnjem letu vzpostavila portal za medijsko in informacijsko pismenost – MIPI. Namenjen je opismenjevanju uporabnikov in posledično njihovemu odgovornejšemu obnašanju. Preko portala želi agencija na poljuden in prijazen način svetovati, uporabnikom dati konkretne napotke, ter opozarjati na novosti, aktualne teme in kakovostne vsebine. Na portalu bo agencija tudi v prihodnje objavljala novičke iz različnih področij svojega delovanja, tako tudi v povezavi z vprašanji povezanimi z zagotavljanjem varnosti. Agencija bo še naprej proaktivno sodelovala z drugimi pristojnimi organi na področju zagotavljanja varnosti, pri tem pa si bo prizadevala za vzpostavitev enotnega informacijskega orodja za poročanje o incidentih, kar bi poenostavilo delo, tako organom, kot tudi zavezancem za poročanje. ■