

Telekom Slovenije zagotavlja varnost komunikacij svojih uporabnikov skladno s slovenskimi predpisi in najvišjimi mednarodnimi standardi. V družbi odgovarjamo na očitke, ki so se v zadnjem času začeli pojavljati v javnosti, pri tem pa opozarjamo, da gre za kompleksno temo, ki poleg tehnične naprednosti zahteva celosten pristop, spoštovanje zakonodaje ter sodelovanje operaterjev, proizvajalcev in različnih inštitucij.

V Telekomu Slovenije smo kot odziv na različne javne objave prejeli nekatera vprašanja glede varnosti Mobitelovega omrežja GSM. Zato odgovarjamo na očitane pomanjkljivosti s pojasnilom, s katerim želimo podati celovite in korektne informacije.

V omrežju Mobitel se pri obeh sistemih, tako v GSM kot UMTS, uporabljajo različni mehanizmi varnosti, ki ustrezajo visokim domačim in mednarodnim standardom. Vendar jih v Telekomu Slovenije zaradi zagotavljanja varnosti svojih omrežij skupaj s tehničnimi podrobnostmi javno ne moremo podrobneje razkrivati. Pri tem posebej opozarjamo, da pri navedbah, ki so sprožile različna ugibanja, prihaja do nekaterih nesporedov oziroma mešanij pojmov, saj se v teh objavah hote ali nehoti mešata dva elementa varnosti GSM-omrežij: prvi se nanaša na zaščito vsebine komunikacije na radijskem vmesniku med mobilnim telefonom in bazno postajo, drugi pa na zaščito identitete uporabnikov. Oba sta seveda pomembna elementa varnosti, toda stanje in značilnosti enega in drugega v GSM-sistemu sta ločeni temi.

Zaščita vsebine komunikacije

V tem primeru gre za potencialno možnost zlorabe komunikacijske zaupnosti na radijskih vmesnikih (t. j. komunikacija med mobilnim terminalom in bazno postajo). Ti zaradi tehnoloških danosti, na katere operater nima vpliva, predstavljajo največjo potencialno ranljivost vsakega omrežja GSM. Zato tudi obstajajo različni zakonski predpisi, ki tovrstno zaupnost varujejo in v ta namen regulirajo delovanje tako posameznikov kot organizacij. S tega vidika noben sistem GSM na svetu ni popolnoma in brezpogojno odporen na zlorabe in nezakonite posege v zasebnost komunikacij, saj je v tem primeru spoštovanje slednje pogojeno s spoštovanjem zakonodaje.

Pri tem lahko operaterji zagotovijo ustrezno zaščito svojih omrežij, vendar se velikokrat pozablja, da je prav tako pomembna in potrebna ustrezna zaščita tudi na ravni mobilnih naprav, ki jih v medsebojni komunikaciji uporabljata oba sogovornika. Če torej uporabniki ne uporabljajo ustrezne opreme na obeh koncih komunikacije (obeh terminalih, ki sta v zvezi), noben GSM-operater na svetu ne more trdno zagotavljati, da je nemogoče, da bi »tretje osebe z ustrezno opremo in znanjem nezakonito prestrezale pogovore in SMS-sporočila«. Hkrati kot že omenjeno velja, da je vsako tovrstno dejanje nezakonito in je skladno z domačo in mednarodno zakonodajo kaznivo dejanje, za katerega lahko posameznik/organizacija kazensko odgovarja.

Zloraba identitete

Za drugi del očitkov, ki se nanašajo na zlorabo identitete uporabnika mobilnega omrežja, pa velja, da je to v Mobitelovem omrežju preprečeno z vrsto standardnih in nadstandardnih varnostnih mehanizmov. Vendar lahko Telekom Slovenije absolutno varnost tovrstnih posegov zagotavlja le v svojem omrežju. V Telekomu Slovenije smo tako že večkrat opozarjali, tudi pristojne institucije, da ne moremo preprečiti, da bi bila identiteta uporabnikov, ki kličejo ali pošiljajo sporočila SMS Mobitelovim uporabnikom iz ostalih domačih ali mednarodnih omrežij, potencialno zlorabljena. Tu bi si želeli ustreznih dodatnih zakonodajnih ukrepov tako naše države kot tudi evropske skupnosti. Pri tem še enkrat odločno poudarjamo, da trditve, da je do zlorabe identitet uporabnikov prišlo v omrežju Telekoma Slovenije, niso resnične. Kljub temu pa kot odgovoren operater ne podcenjujemo nobenih takih ali podobnih varnostnih groženj, zato z nenehnimi operativnimi ukrepi zagotavljamo maksimalno možno varnost uporabnikov in njihovih komunikacij. Pri tem je velika prednost Telekoma Slovenije v tem, da je kot največji in nacionalni operater ustrezno tehnično opremljen, vprašanja varnosti obravnavamo resno in profesionalno, imamo najboljšo ekipo in mednarodne izkušnje, pri načrtovanju in upravljanju omrežja pa smo avtonomni. Celotno omrežje upravljamo sami, vsi elementi omrežja in podpornih sistemov so pod našo odgovornostjo in kontrolo, na račun varnosti, zakonodajnih zahtev ali kakovosti pa ne sklepamo kompromisov v škodo uporabnikov. Kot nacionalni operater pa je Telekom Slovenije še bolj podvržen strogi kontroli različnih državnih organov v različnih časih in je kot tak referenca za vprašanja komunikacijske varnosti, saj jih obravnavamo izjemno strokovno.

Torej, kar se tiče zlorabe zaupnosti komunikacij, obstaja zakonito in potencialno tudi nezakonito prestrazanje komunikacij. Nobeno od njiju pa seveda ni v pristojnosti nobenega operaterja. Zakonito prestrazanje morajo sicer vsi operaterji omogočati pristojnim organom, kar je zakonsko predpisano in strogo nadzorovano, nezakonito prestrazanje komunikacij pa se preprečuje z različnimi mehanizmi, skladno s tehničnimi možnostmi. Seveda gre pri zagotavljanju vseh elementov varnosti za uporabo standardiziranih varnostnih mehanizmov, ki pa so v omrežju posameznih operaterjev različni, zato so tudi omrežja (vključno z uporabljenimi terminali/mobilniki) v splošnem različno ranljiva na varnostna tveganja. V Telekomu Slovenije neprestano spremljamo razvoj in vlagamo v nove tehnologije sodobnih telekomunikacij, napredne rešitve pa uvajamo v najkrajšem možnem času. Tako bo tudi v prihodnje, vendar je treba spomniti, da je mobilna telefonija ekosistem, v katerem igrajo pomembno vlogo ne le omrežja, temveč tudi mobilniki - slednji morajo prav tako podpirati napredne oblike šifriranja. Zagotavljanje varnosti na ravni posameznega operaterja, kot je Telekom Slovenije, namreč ne zadostuje, v kolikor visokim varnostnim zahtevam ne ustrezajo tudi druga omrežja in oprema, ki je uporabnikom na voljo.

Kodirni (šifrirni) sistemi in GSM

Kar se tiče samega sistema GSM in kodirnih protokolov, opozarjamo, da je GSM-sistem že od samega začetka, torej leta 1991, tarča potencialnih zlorab, zato se varnostni mehanizmi stalno razvijajo in posodablajo – po svetu in tudi v omrežju Mobitel. Upoštevati je treba, da je GSM vzpostavljen v okoli 219 državah in ga uporablja preko tri milijarde uporabnikov. Pri tem Mobitelovo omrežje niti najmanj ne zaostaja za razvitim svetom, ki se sooča z enakimi varnostnimi izzivi. Naprednejši protokol A5/3 namreč tudi globalno glede zagotavljanja ustrezne opreme omrežij in mobilnikov še ni v celoti nadomestil A5/1, saj proizvajalci komunikacijske opreme šele v zadnjem času zagotavljajo ustrezno podporo in interoperabilnost, ki bi to omogočila. Na trgu je še vedno zelo veliko mobilnikov, ki sodobnejšega protokola A5/3 ne podpirajo ali pa podpora ni ustrezna.

Zato v Telekomu Slovenije v GSM-sistemu uporabljamo oba kodirna protokola, poleg A5/1 tudi naprednejši protokol A5/3, pa tudi druge varnostne mehanizme, kar je primerljivo z vodilnimi operaterji po svetu. Za sistem GSM je sicer že v pripravi novejši algoritem in vpeljavo slednjega kot nadgradnjo baznih postaj GSM načrtujemo že v naslednjem letu. Seveda pa bo tudi uporaba slednjega pogojena ne le z nadgradnjo omrežja, temveč tudi z mobilniki, ki podpirajo takšna napredna šifriranja. Pri tem velja, da so UMTS-omrežja naprednejša tudi v smislu višjega nivoja varnosti, zato je komunikacija v omrežju Mobitel UMTS vsekakor najbolj varna.

Varnost komunikacij in zaupnost na prvem mestu

V Telekomu Slovenije pozdravljamo vsako pobudo, ki lahko prispeva k ozaveščanju javnosti o pomenu komunikacijske varnosti in ki lahko spodbuja h kakršnim koli izboljšavam na tem področju. Varnostne vidike, na katere se opozarja, jemljemo resno in zavzeto, vendar se v različne javne razprave s tega področja ne moremo vključevati, saj lahko s tem ogrozimo varnostne mehanizme, ki jih uporabljamo. Zagotavljanje varnosti omrežij in uporabnikov ter zaupnosti njihovih komunikacij je namreč temeljno poslanstvo Telekoma Slovenije. Zato so uporabniki največjega slovenskega operaterja lahko z gotovostjo prepričani, da v Telekomu Slovenije s svojim znanjem, vrhunsko tehnologijo in skrbnostjo zagotavljamo najvišjo možno stopnjo varnosti njihovih komunikacij.