TelekomSlovenije

Sektor za kadrovske, pravne in splošne zadeve
Služba za varnost

DRŽAVNI ZBOR REPUBLIKE SLOVENIJE

Prejeto: 31-07-2012	
Šifra: 200-15/12-26/4	
Povezava:	
EPA:	EU:
Sign. zn.:	
Kratica:	

Številka: 60/05-3/4
Datum: 27. 7. 2012

Republika Slovenija
DRŽAVNI ZBOR
Komisija za nadzor na delom varnostnih in obveščevalnih služb
Šubičeva 4

1000 Ljubljana

Zadeva: **Odgovor na zaprosilo za posredovanje gradiva oz. poročil operaterjev**

Zveza: Dopis številka 200-15/12-26/2 z dne 11. 7. 2012

Spoštovani,

na osnovi poziva Komisije za nadzor na delom varnostnih in obveščevalnih služb, da se izjasnimo glede varnosti in zaščite GSM omrežja, vam v nadaljevanju posredujemo zahtevana pojasnila.

Omrežje Mobitel je visoko kakovostno, zmogljivo in skladno z regulativo varno upravljano mobilno omrežje. To potrjujejo tudi zakonite kontrole državnih organov. Varnostne funkcionalnosti mobilnega omrežja so stalno aktivne, saj brez njih uporaba storitev mobilnega omrežja ni mogoča.
V omrežju Mobitel se pri obeh sistemih, tako v GSM kot UMTS, uporabljajo različni varnostni mehanizmi, ki ustrezajo izjemno visokim domačim in mednarodnim standardom. Z vrsto varnostnih mehanizmov, sistemsko vgrajenih v naše mobilno omrežje, neprestano skrbimo za varnost komunikacij naših uporabnikov. Pri tem posebej opozarjamo, da pri navedbah, ki so sprožile različna ugibanja, prihaja do nekaterih neresnic oz. vsaj nesporazumov, saj se vede ali nevede 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.

V primeru zaščite vsebine komunikacij 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. Tu operaterji niti nimamo možnosti za specifične varnostne ukrepe, ker gre za globalno standardiziran sistem, ki temelji na mednarodnem gostovanju (roaming). Zato vsa omrežja in vsi mobilni terminali na svetu trenutno podpirajo šifrirni algoritem A5/1. Določen del GSM terminalov (vse večji delež, približno polovica) pa že podpira algoritem A5/3. GSM terminal in GSM omrežje se v fazi vzpostavljanja signalizacije za klic ali SMS dogovorita za najvišji možen šifrirni algoritem – torej bodisi A5/3 bodisi A5/1. Oba algoritma sta z vidika GSMA (GSM association – mednarodno združenje GSM operaterjev) dovoljena. Le algoritma A5/2 in seveda A5/0 (brez šifriranja) sta prepovedana. Algoritem A5/1 je v uporabi praktično od začetka sistema GSM in je žal tudi od samega začetka tarča nezakonitih napadov oziroma razbijanja, dešifriranja. Najnovejše tovrstne objave žal zgolj pomenijo, da je zaradi napredka procesorske zmogljivosti računalnikov, ta nezakonitost tehnično še toliko bolj olajšana. Uvajanje algoritma A5/3 na trg omrežij in terminalov v svetu poteka izredno počasi – vsaj že 8 let. Tako je v zvezi z njim še vedno odprtih kar nekaj tehničnih vprašanj oziroma problemov. Obstajajo na primer terminali, ki skušajo od

omrežja dobiti A5/3 šifriranje, a imajo potem težave s slišnostjo in se zato pojavljajo reklamacije. Po drugi strani pa je podpora algoritma A5/3 odvisna od starosti HW opreme baznih postaj. Gre za opremo, ki se amortizira dolgoročno. Tako imamo mnogi operaterji v svetu v omrežju tudi okoli 10 let staro opremo baznih postaj GSM, ki še ni predvidevala SW podpore A5/3. Zato so tipično v svetu trenutno omrežja, ki podpirajo A5/1 ali v delu omrežja tudi A5/3. Redka so omrežja, ki v celoti podpirajo A5/3 – nenazadnje je vse manj popolnoma novih ali v celoti prenovljenih GSM omrežij. Tudi v Sloveniji je tako – poleg tega pa ostaja odprto vprašanje, kako naprej z GSM omrežji v Sloveniji po letu 2013, ko poteče (tudi Telekomu Slovenije) veljavnost sedanjih ODRF za GSM frekvence.

Tudi algoritem A5/3 je stalna tarča napadov – ni pa (še) bil v fokusu ali v dometu nedavnih objav na naših spletnih straneh, ki so vzbudile novo pozornost za to sicer vedno aktualno varnostno tematiko. 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 in je v tem primeru spoštovanje slednje pogojeno s spoštovanjem zakonodaje.

Za drugi del navedb, 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. V tem primeru gre za mehanizme overjanja med SIM karticami uporabnika našega omrežja in našim jedrnim omrežjem. Ti mehanizmi temeljijo na standardnih GSM algoritmih A3 in A8, vendar pa imamo tu operaterji možnost dodati lastne dodatne varnostne specifike navedenih algoritmov, katerih cilj je čim bolj zmanjšati verjetnost, da bi do zlorab lahko prišlo. Vendar opozarjamo, da Telekom Slovenije dodatno varnost identitete uporabnikov zagotavlja le za promet, ki izvira v lastnem 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 zakonodajnih ukrepov države in evropske skupnosti, posebej v luči tega, da je v zakonodajnem postopku novi ZEKom.

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 takšno napredno enkripcijo. Pri tem velja, da so UMTS-omrežja naprednejša tudi v smislu višjega nivoja varnosti, zato je komunikacija v omrežju Mobitel UMTS vsekakor najbolj varna.

V Telekomu Slovenije smo prepričani, da izvajamo vse potrebne zaščitne ukrepe in da spoštujemo 102. člena ZEKoma.

Letos 9. julija smo tudi Agenciji za pošto in elektronske komunikacije posredovali zahtevana pojasnila glede izpolnjevanja določil 102. člena ZEKom-a.

S spoštovanjem!

Zoran Vehovar
podpredsednik uprave

TelekomSlovenije
059 d.d.