VPRAŠANJA

Na tehnološkem portalu Slo-Tech so danes objavili izčrpen prispevek, kako je mogoče brez večjega truda, finančnega vložka ali časa pošiljati sporočila SMS s poljubnim pošiljateljem ali celo opravljati "ponarejene" telefonske klice (s poljubno vrednostjo klicočega).

http://slo-tech.com/novice/t511312#crta

Med drugim navajajo predstavnike operaterjev, ki so zagotovili, da tovrstne identitetne "ponaredbe" v njihovih omrežjih tehnično niso mogoče, ali - nasprotno - da v resnici ne obstajajo načini, s katerimi bi lahko zanesljivo ugotavljali identiteto klicateljev.

Zato me zanima naslednje:

- So ponaredbe identitete v resnici tehnično nemogoče ali obstajajo načini, ki jih ne morete ugotoviti, zabeležiti ali preprečiti?
- Koliko zahtev po dostopu do prometnih podatkov ste imeli leta 2011?
- Ste predstavnikom policije, tožilstva ali pripravljalcem zakona o elektronskih komunikacijah kdaj omenili, da elektronskim podatkom ni mogoče stoodstotno zaupati?

***

MOBITEL

- So ponaredbe identitete v resnici tehnično nemogoče ali obstajajo načini, ki jih ne morete ugotoviti, zabeležiti ali preprečiti?

- Koliko zahtev po dostopu do prometnih podatkov ste imeli leta 2011?

Mobitelovo omrežje je visoko kakovostno, zmogljivo in skladno z regulativo upravljano mobilno omrežje, ki uporabnikom mobilnih komunikacij v Sloveniji nudi najbolj tehnično dovršeno in varno uporabo sodobnih mobilnih storitev. To potrjujejo tudi zakonite kontrole državnih organov. Varnostne funkcionalnosti mobilnega omrežja so stalno aktivne, saj brez njih uporaba storitev mobilnega omrežja ni mogoča. Z vrsto varnostnih mehanizmov, sistemsko vgrajenih v naše mobilno omrežje, neprestano skrbimo za varnost komunikacij naših uporabnikov. V sklopu tega tudi preprečujemo vdor v naš sistem telefonskih povezav, na osnovi katerega bi prišlo do zlorabe prikaza kličoče številke (CLI - Calling Line Identification).

Varnostna politika in tehnična implementacija varnostnih sistemov na ravni omrežja so odvisni od posameznega operaterja, a na svetovni ravni ni enotne rešitve, ki bi neizpodbitno zagotovila, da v Mobitelovo omrežje pride klic s pravo in nepopačeno identifikacijo. Tako ne moremo zagotoviti, da operaterji po vsem svetu uporabljajo enako zahtevne varnostne mehanizme z enako doslednostjo, kot jo zagotavljamo v našem mobilnem omrežju.

Kot javno telefonsko omrežje smo obvezani sprejeti (zaključevati) klice na številke uporabnikov v našem omrežju vseh operaterjev, ki za to izrazijo interes. Torej, čim govorimo o prometu med različnimi operaterji (domačimi in tujimi), govorimo o globalni problematiki. Če reševanja le-te ne bo potekalo tudi v sklopu regulative, ne bo dovolj učinkovite rešitve, saj morajo pravila igre biti jasno določena, kršitve pa sankcionirano. Takšno mnenje smo že večkrat izrazili, tudi uradno v sklopu javne obravnave oziroma zbiranja pripomb s strani državnih organov, ki pripravljajo zakonodajo na našem področju. Pri našem delovanju med

drugim upoštevamo tudi priporočila ECC (http://www.erodocdb.dk/docs/doc98/official/pdf/Rec1102.pdf) oziroma si od njih obetamo krepitev reda in varnosti na tem področju, na osnovi prispevka vseh deležnikov, vendar še enkrat poudarjamo, da je potrebno zagotavljati integriteto kličoče številke CLI na celotni verigi od izvora, preko tranzitnih omrežij do omrežja, ki klic na ciljni številki zaključi. Slednje pa je pogosto težko, saj se telekomunikacije v regulatorno-pravnem pogledu v različnih državah sveta močno razlikujejo.

Vzemimo na primer klic, ki ga sproži nek slovenski turist iz hotela v Keniji in kliče uporabnika slovenskega omrežja y. Slovensko omrežje y mora tak klic zaključiti (uporabniki upravičeno pričakujejo, da so dosegljivi za klice z vsega sveta), do omrežja y pa pripotuje preko verige mednarodnih omrežij, nad katerimi nima učinkovite kontrole. Pri sedanji zasnovi omrežij omrežje y iz namišljenega primera nima mehanizma, na osnovi katerega bi v realnem času sistemi verificirali verodostojnost identifikacije kličočega. Podobno oziroma recipročno velja za omrežje x. Žal trenutno na svetu ni učinkovite regulacije, ki bi regulirala identifikacijo izvornega klica na celi poti in so določeni taki potencialni primeri prepuščeni sistemu reševanja reklamacij, pri katerem pa – v kolikor je reklamacija pravočasna – obstajajo vse možnosti za odkritje morebitnih zlorab. Vendar takih primerov praktično ne beležimo.

Poleg tega pa v svetu obstajajo tudi razne internetne aplikacije, ki omogočajo določene scenarije generiranja klicev in SMS-ov, gostujejo pa lahko na nekem »eksotičnem« omrežju kjerkoli v svetu in skozenj pridejo do katerekoli lokacije v svetu. Pri tem ni kontrole, kdo uporablja te aplikacije in s kakšno identiteto inicira klice – ali to dela imetnik številke prostovoljno ali pa ne. V omrežju Mobitel imamo vzpostavljene mehanizme kontrole takega prometa, vendar so ti mehanizmi dodatno kompleksni zaradi prenosljivosti številk. Za odkrivanje in saniranje takih primerov nam vedno ostane mehanizem reklamacij in ta pomeni za uporabnike tisto dodatno varovalko, ki verjetnost zlorab zmanjša na najmanjšo možno raven.

- Ste predstavnikom policije, tožilstva ali pripravljalcem zakona o elektronskih komunikacijah kdaj omenili, da elektronskim podatkom ni mogoče stoodstotno zaupati?

V Telekomu Slovenije smo pristojne opozorili, da bi po našem mnenju moral novi zakon definirati več možnosti za kontrolo in zavarovanje pred zlorabami uporabe naročniške identitete, ki je dodeljena operaterjem, a jih različni ponudniki storitev na internetu uporabljajo kot element identitete.

SIMOBIL

1. **So ponaredbe identitete v resnici tehnično nemogoče ali obstajajo načini, ki jih ne morete ugotoviti, zabeležiti ali preprečiti?**

Možnosti ponaredbe identitete so omejene in tehnično kompleksne, saj navadno terjajo poglobljena znanja tako s TK kot IT področij. Izkušnje kažejo, da je pri zlorabah žal še vedno največkrat kriv t.i. človeški faktor (posoja ali kraja telefona oz. uporabniškega imena in gesla).

Prikaz lažne identitete pošiljatelja kratkega sporočila je tehnično manj kompleksen, obstaja celo nekaj ponudnikov, ki to ponujajo kot svoj poslovni model. V Si.mobilu takšne storitve ne ponujamo, ponudnike, ki to storitev ponujajo pa poskušamo čim bolj omejiti. Prikaz lažne identitete kličočega pa je tehnično bistveno bolj kompleksna in od storilca terja tehnično opremo in obilico znanja s področja informacijskih in telekomunikacijskih tehnologij.

Odkritje poneverb je možno post-festum, s primerjavo klicev tistega, ki naj bi klic opravil

(tistega, ki so mu identiteto ukradli) in tistega, ki je klic prejel.

2. **Koliko zahtev po dostopu do prometnih podatkov ste imeli leta 2011?**

Zakon definira dva tipa zahtevkov po dostopu do prometnih podatkov: od organov oblasti (informacije o številu zahtev v skladu z zakonodajo ne smemo razkrivati), ter od naših naročnikov. Slednji lahko podatke zahtevajo le za svoje klice (to zahtevo lahko opravi samo naročnik za samo njegove prometne podatke, ji jih na koncu posredujemo samo njemu).

3. **Ste predstavnikom policije, tožilstva ali pripravljavcem zakona o elektronskih komunikacijah kdaj omenili, da elektronskim podatkom ni mogoče stoodstotno zaupati?**

Konec lanskega oktobra je bila na spletni strani MVZT objavljena Javna obravnava osnutka predloga Zakona o elektronskih komunikacijah, v katerem je Direktorat za informacijsko družbo zainteresirano javnost pozval, naj poda svoje pripombe in predloge na zakonski osnutek, kar smo v Si.mobilu tudi naredili. Pri tem je poleg verodostojnosti potrebno opozoriti predvsem na visoke stroške vzpostavitve in vzdrževanje sistema, ki je potreben za zbiranje in hranjenje.

Odgovor je pripravil:
Andraž Zmajšek,
vodja informacijske varnosti

T-2

- So ponaredbe identitete v resnici tehnično nemogoče ali obstajajo načini, ki jih ne morete ugotoviti, zabeležiti ali preprečiti?

V sodobnih telekomunikacijah so poskusi goljufij, zlorab in napadov, med katerimi so tudi zlorabe identitet, vedno pogostejši. Zato je ključna naloga ponudnikov telekomunikacijskih storitev varnost in preprečevanje možnosti, da bi do tovrstnih zlorab prišlo. Potencialne goljufije, zlorabe in napade tudi v T-2 omejujemo s pomočjo pripravljene stroge varnostne politike, prav tako pa razvijamo in imamo razvite številne mehanizme varovanja, ki preprečujejo možnosti, da bi do zlorab prišlo. Temeljna varnostna načela in mehanizmi proti zlorabam, goljufijam in napadom, ki jih moramo v T-2 upoštevati, so opredeljeni direktivah EU, slovenski zakonodaji in internih dokumentih. Za svojo elektronsko varnost pa morajo poskrbeti tudi uporabniki sami.

- Koliko zahtev po dostopu do prometnih podatkov ste imeli leta 2011?

T-2 omogoča prestrezanje storitvenega prometa uporabnikov v skladu z zakonodajo. Podrobnejših podatkov vam na žalost ne moremo posredovati.

- Ste predstavnikom policije, tožilstva ali pripravljalcem zakona o elektronskih komunikacijah

kdaj omenili, da elektronskim podatkom ni mogoče stoodstotno zaupati?

V T-2 smo menja, da zanesljivost podatkov ne ustvarja dvomov, o katerih sprašujete.

TUŠMOBIL

»Pri Tušmobilu nismo zasledili nikakršnih zlorab v sisteme naših storitev, kot jih navajate. Vseskozi smo izjemno pozorni na zagotavljanje najvišjih varnostnih standardov, kar nam omogoča permanentno nadgrajevanje varnostnih rešitev. Za pošiljanje sporočil SMS prek aplikacije (storitev SMS Kurir) vsakemu uporabniku izdamo certifikat, ki aktivno ščiti sistem pred morebitnimi vdori in takšne poskuse, ob poskusu izvedbe, tudi zazna in prepreči.«