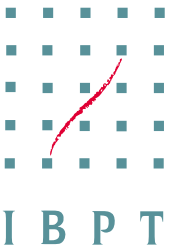

BELGISCH INSTITUUT VOOR POSTDIENSTEN EN TELECOMMUNICATIE

MEDEDELING VAN DE RAAD VAN HET BIPT VAN 30 APRIL 2013 BETREFFENDE DE MOGELIJKE RISICO'S VOOR SCHENDING VAN DE VEILIGHEID VAN DE NETWERKEN EN DIENSTEN VOOR MOBIELE TELEFONIE IN HET KADER VAN DE 2G- EN 2,5G-TECHNOLOGIE.

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipse Building - Gebouw C - Koning Albert II-laan 35, 1030 Brussel
Tel. 02 226 88 88 Fax: 02 226 88 77 http://www.bipt.be

Inhoudsopgave

1. DOEL VAN DE MEDEDELING

Op 17 februari 2012 heeft het BIPT aan de heer Johan Vande Lanotte, Vice-eersteminister en minister van Economie, Consumenten en Noordzee, een advies overgezonden betreffende de mogelijke veiligheidsrisico's voor de netwerken en diensten voor mobiele telefonie in het kader van de 2G- en 2,5G-technologie (hierna "mobiele 2G- en 2,5G-netwerken" genoemd). Op 7 juli 2012 heeft het BIPT op zijn website van zijn advies aan de minister een versie gepubliceerd die voor het publiek bestemd is.

Overeenkomstig de conclusies van het voormelde advies en het werkplan 2013[1] van het BIPT, is er een nieuwe studie verricht over de veiligheid van de mobiele 2G- en 2,5G-netwerken.

Deze studie is in essentie gebaseerd op een enquête gehouden onder de voornaamste Belgische aanbieders van mobiele-telefoniediensten van de types GSM, GPRS en EDGE in verband met de potentiële risico's voor de schending van de veiligheid van hun mobiele netwerken. Deze enquête onderzoekt de huidige en toekomstige maatregelen die de Belgische operatoren hebben genomen of zullen nemen om de integriteit en de vertrouwelijkheid van hun GSM-, GPRS- en EDGE-diensten te garanderen. Er is ook bijzondere aandacht besteed aan de veiligheid van voicemail.

In de laatste vier maanden van 2012 heeft het BIPT dus de voornaamste leveranciers van 2G- en 2,5G-mobieletelefoniediensten bevraagd, in casu Belgacom, Mobistar en KPN Group Belgium, waarbij hun een vragenlijst is voorgelegd over het huidige en toekomstige beheer van de veiligheid van hun mobiele netwerk en over de risico's voor schending ervan.

2. JURIDISCH KADER

Op grond van de artikelen 113, 113/1, 113/2, 114, 114/1 en 114/2 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna de WEC) beschikt het BIPT over bevoegdheden met betrekking tot de kwaliteit en veiligheid van de openbare netwerken en diensten voor elektronische communicatie.

Artikel 114, § 1, van de WEC schrijft het volgende voor:

> *"Ondernemingen die openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten aanbieden, treffen de passende technische en organisatorische maatregelen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen, eventueel samen wat de veiligheid van het netwerk betreft. Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen. Er worden met name maatregelen genomen om de impact van veiligheidsincidenten op gebruikers en onderling verbonden netwerken zo laag mogelijk te houden."*

Artikel 114/2, § 2, van de WEC schrijft onder andere het volgende voor:

> *De ondernemingen die openbare communicatienetwerken of openbare elektronische-communicatiediensten aanbieden leveren het Instituut, op zijn verzoek, alle informatie die nodig is om de veiligheid of de integriteit of beide, van hun diensten en netwerken te beoordelen, met inbegrip van de stukken met betrekking tot hun veiligheidsbeleid. […]"*

[1] Fiche "*RE-ER/7/2013/03: Enquête over de veiligheid van mobiele netwerken*" van het werkplan 2013 van het BIPT, februari 2013.

Bovendien belast artikel 14, § 1, 3°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, de zogenaamde statuutwet, het BIPT ermee onder andere de naleving van de WEC te controleren.

De voormelde enquête werd derhalve verricht op basis van die bepalingen.

3. REIKWIJDTE VAN DE STUDIE BEPERKT TOT DE 2G- EN 2,5G-TECHNOLOGIE – UITSLUITING VAN DE 3G- EN LATERE TECHNOLOGIEËN.

Deze studie is beperkt tot de 2G- en 2,5G-mobieletelefoniediensten, in dit document "mobiele netwerken" genoemd, en spitst zich in het bijzonder toe op de veiligheid van communicatie via radiokanalen, d.w.z. tussen het eindtoestel van de gebruiker (zoals een draagbare telefoon) en de netwerkinfrastructuur.

3.1. DE 2G- EN 2,5G-TECHNOLOGIE

De essentiële vernieuwing van de GSM-, GPRS- en EDGE-netwerken ten opzichte van de voorgaande technologieën voor mobiele telefonie is de volledig digitale aard ervan. Dit brengt een onmiskenbare verbetering met zich van het prestatievermogen (beter gebruik van het spectrum en regeneratie van de informatie bijvoorbeeld) en heeft natuurlijk geleid tot het succes dat deze generatie van netwerken kent sedert 1991, dus al meer dan 20 jaar geleden. Bij het opstellen van deze normen had de veiligheid van de communicatie echter niet het belang dat er vandaag aan wordt gehecht. Het BIPT stelt daarbij vast dat deze normen gebaseerd zijn op mechanismen die ter discussie kunnen worden gesteld ten aanzien van de recente technologische vooruitgang.

Het GSM-netwerk is de tweede technologie inzake mobiele telefonie, zogenaamd "2G", die onder andere spraakoverdracht en de uitwisseling van korte tekstberichten (sms) via circuit-schakeling ondersteunt. Het GPRS-netwerk[2] is een technologie die afgeleid is van het gsm-netwerk en die de dataoverdracht via pakketschakeling invoert. Deze wordt doorgaans bestempeld als een "2,5G"-technologie. Ten slotte is het EDGE[3]-netwerk een verbetering van de voorgaande netwerken die het voornamelijk mogelijk maakt om hogere overdrachtsnelheden te halen.

3.2. 3G- EN LATERE TECHNOLOGIEËN

De derde generatie (3G) van technologieën voor mobiele telefonie en latere technologieën stellen voor om hogere snelheden te bereiken, waardoor de deur wordt opengezet voor multimediatoepassingen, zoals beeldtransmissie, videoconferentie of breedbandinternet-toegang. Bij het opstellen van de 3G-normen en van latere generaties is geprofiteerd van de opgedane ervaring, met name inzake veiligheid, zodat deze nieuwe technologieën het voordeel hebben van rijpere, meer ingewikkelde en krachtigere beschermingsmechanismen dan diegene die bij 2G en 2,5G worden gehanteerd.

---

[2] GPRS: *General Packet Radio Service – Dienst voor pakketgeschakelde dataoverdracht*

[3] EDGE: *Enhanced Data Rates for GSM Evolution* - Verhoogde datasnelheid voor de gsm-evolutie.

De voornaamste feiten die zich in Europa inzake veiligheid van de mobiele netwerken hebben voorgedaan (bijvoorbeeld het schandaal waarbij *News International* in juli 2011 de voicemail heeft gehackt of de kritiek van sommige experten over de veiligheid van de 2G- en 2,5G-mobieletelefoniediensten waarover de pers heeft bericht in december 2011) hebben overigens geen betrekking op de 3G-technologieën en hoger.

De analyse van deze netwerken valt daarom buiten het bestek van deze studie.

4. INTERNE ANALYSE

De interne analyse is het resultaat van het opzoekingswerk dat verricht is met het oog op het advies van juli 2012[4] en dat overgedaan is rekening houdende met de jongste publicaties op dat gebied. Voor zover ons bekend zijn er geen belangrijke ontwikkelingen geweest wat veiligheids-risico's betreft. Er zijn immers geen nieuwe belangrijke bressen vastgesteld en er zijn sedert de vorige oefening geen nieuwe opmerkelijke feiten gerapporteerd.

Zoals vermeld in het voormelde advies zijn de meest kritieke zwakke punten :

- Het ontbreken van wederzijdse authenticatie. Het gaat om een zwak punt dat inherent is aan de veiligheidsarchitectuur: enkel het eindtoestel moet zijn identiteit bevestigen en is dus niet in staat om na te gaan met welk netwerk het in werkelijkheid is verbonden.
- Een onderhandeling van de coderingsalgoritmen[5] (van het type A5 of GEA, respectievelijk voor de GSM- of GPRS-netwerken), terwijl de efficiëntie van deze laatste verminderd zou zijn ten opzichte van de technologische vooruitgang.

5. ANALYSE VAN DE ANTWOORDEN VAN DE OPERATOREN

Omdat de antwoorden van de operatoren op de enquête van het BIPT vertrouwelijk zijn, mogen ze in dit document niet integraal kenbaar worden gemaakt.

De analyse verricht door het BIPT is bewust beperkt tot een kwalitatieve en algemene evaluatie van het risico voor een inbreuk op de veiligheid en vormt geen kwantitatieve analyse (bijv. het aantal getroffen gebruikers). Het BIPT kan daarom het gevaar voor schending van de veiligheid niet nauwkeurig kwantificeren.

Uit de analyse blijkt echter dat de operatoren getuigen van een bijzondere aandacht voor de veiligheid van hun mobiele netwerk in termen van beheer, investeringen en technologische vernieuwing. Tijdens het jaar 2012 hebben de operatoren de veiligheid van hun mobiele netwerk laten evolueren en ze blijven nu nog nieuwe maatregelen bestuderen en plannen om het veiligheidsniveau van hun mobiele netwerk nog meer te verhogen.

In verband met de 2G-netwerken stellen wij in België een vrijwel uitsluitend gebruik van een coderingsalgoritme vast waarvan de efficiëntie zou kunnen worden beproefd ten aanzien van de laatste technologische vooruitgang. Het algemene gebruik van een algoritme dat een hoger veiligheidsniveau mogelijk maakt, wordt nu bij de operatoren bestudeerd of geëvalueerd, maar dat gebruik is momenteel niet denkbaar, hoofdzakelijk om redenen van compatibiliteit: meer

[4] Zie deel 5.1 - Advies van het BIPT bestemd voor het publiek betreffende de mogelijke risico's voor schending van de veiligheid van de netwerken en diensten voor mobiele telefonie in het kader van de 2G- en 2,5G-technologie, juli 2012

[5] Dankzij de coderingsalgoritmen kan de overgedragen informatie worden beschermd tegen ongeoorloofde onderschepping of decodering.

dan een derde van het huidige park van eindtoestellen zou zeker moeten worden vervangen. Een pragmatische benadering - die overigens met name wordt aangenomen door de mobiele operatoren - bestaat daarom erin het bestaande algoritme te versterken door een aantal recente functies van de GSM-specificaties toe te passen.

In verband met de 2,5G-netwerken gaan de mobiele operatoren uit van de hypothese dat - voor sommige transmissies - de gegevens stroomopwaarts worden beveiligd, door bijvoorbeeld de verbinding te leggen met gecertificeerde https-sites. Dit moet echter worden gerelativeerd door het daadwerkelijke gebruik van deze transmissiewijze en door het geringe aandeel van het volume van mobiele gegevens die op de 2,5G-netwerken worden uitgewisseld: ongeveer 75% van het verkeer verloopt immers via 3G- of 3,5G-netwerken.

Voicemail heeft vanwege de drie operatoren een bijzondere aandacht gekregen.

In het kader van de enquête hebben de operatoren aan het BIPT geen gevallen van een bewezen schending van de veiligheid van hun mobiele netwerk meegedeeld. Bovendien zijn er ook geen relevante problemen gerapporteerd door de gebruikers.

Ondanks deze positieve resultaten is het BIPT van oordeel dat bepaalde aspecten nog verbeterd kunnen worden en zal het de aandacht van de operatoren daarop vestigen via een bilaterale follow-up.

Heel in het algemeen moet elke verhoging van het veiligheidsniveau worden beoordeeld en moeten de repercussies in overweging worden genomen die teweeggebracht worden zowel bij de operatoren (belasting van de systemen, interoperabiliteit, investeringen, enz.) als bij de eindgebruikers (klantenervaring, tarief, dienstkwaliteit, enz.). De compatibiliteit van de eindtoestellen, zowel nationaal als bij roaming, is zeker een factor die moet worden meegeteld.

6. CONCLUSIES

In het kader van de enquête hebben de operatoren aan het BIPT geen tastbare elementen of vermoedens van een schending van de veiligheid van hun mobiele netwerk meegedeeld. Sedert de vorige enquête hebben de operatoren nieuwe maatregelen aangenomen en gepland om de veiligheid van hun mobiele netwerk te versterken.

De analyse van de antwoorden van de operatoren en de confrontatie van deze laatsten met de huidige normen, leidt tot de conclusie dat de veiligheid van hun mobiele netwerk vandaag bevredigend is, maar op verschillende niveaus nog voor verbetering vatbaar is.

Daartoe is het BIPT van plan om een dynamische uitwisseling met de mobiele operatoren op te starten om over deze kwesties van verbetering te praten en vooral pragmatische en proportionele oplossingen te vinden. Het BIPT zal ook erop toezien dat de veiligheids-maatregelen die de mobiele operatoren hebben gepland, daadwerkelijk worden toegepast. Indien nodig, zal het BIPT de mogelijkheid bestuderen om bepaalde bindende instructies op te leggen, overeenkomstig artikel 114/2, § 1, van de WEC.

In elk geval zal het BIPT zijn standpunt herbekijken naarmate er nieuwe elementen opduiken ofwel na elke nieuwe enquête.