BELGISCH INSTITUUT VOOR POSTDIENSTEN
EN TELECOMMUNICATIE

ADVIES VAN DE RAAD VAN HET BIPT VAN 17 FEBRUARI 2012 AAN MINISTER VANDE LANOTTE 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

Versie bestemd voor het publiek

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

EXECUTIVE SUMMARY 3
1. CONTEXT EN VOORWERP VAN HET ADVIES 3
1.1. Recente ontwikkelingen 3
1.2. Voorwerp van het advies 4
2. JURIDISCH KADER 5
3. REIKWIJDTE VAN HET ADVIES BEPERKT TOT DE 2G- EN 2,5G-TECHNOLOGIE – UITSLUITING VAN DE 3G- EN LATERE TECHNOLOGIEËN 5
3.1. De 2G- en 2,5G-technologieën 6
3.2. 3G- en latere technologieën 6
4. STANDPUNT VAN DE OPERATOREN 6
5. INTERNE ANALYSE 7
5.1. Veiligheid van de mobiele netwerken 7
5.2. Beperkingen in verband met een verhoging van het veiligheidsniveau 8
6. ANALYSE VAN DE ANTWOORDEN VAN DE OPERATOREN 8
7. SLOTCONCLUSIES 8

EXECUTIVE SUMMARY

Minister Johan VANDE LANOTTE, vice-eersteminister en minister van Economie, Consumenten en de Noordzee, heeft aan het BIPT gevraagd om een stand van zaken op te maken over de veiligheid van de Belgische netwerken en diensten voor mobiele telefonie. Het BIPT heeft op deze vraag geantwoord in een advies van 17 februari 2012.

Het advies van het BIPT is gebaseerd op een interne analyse alsook op een enquête die het gehouden heeft bij de voornaamste aanbieders van mobiele-telefoniediensten van de types GSM, GPRS en EDGE op grond van de artikelen 113 en 114 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Deze enquête van het BIPT toont aan dat er voor alle operatoren geen tastbare elementen of vermoedens van de schending van de veiligheid konden worden bevestigd.

Het BIPT komt tot de conclusie dat de veiligheid van de netwerken en diensten vandaag toereikend is maar voor verbetering vatbaar. Door de maatregelen die al aangenomen zijn en diegene die gepland zijn, laten de operatoren een echte wil blijken om snel een hoger niveau van veiligheid te bereiken.

Ten slotte heeft het BIPT al een nieuwe algemene analyse gepland voor het vierde kwartaal van het jaar 2012. Deze algemene analyse zal een interne analyse, een nieuwe enquête onder de operatoren omvatten, alsook controles in verband met de doeltreffendheid van de veiligheid van de GSM-, GPRS- en EDGE-netwerken.

1. CONTEXT EN VOORWERP VAN HET ADVIES

1.1. Recente ontwikkelingen

Recente publicaties hebben verscheidene mogelijke zwakke punten in de diensten voor mobiele telefonie blootgelegd. Verschillende experten groepen hebben immers grote vooruitgang aangekondigd inzake cryptologie[1] en stellen ook nieuwe materiële oplossingen voor, alsook software die het mogelijk zou maken om de communicatie af te luisteren die via de mobiele netwerken verloopt.

Het meest gemediatiseerde onderzoek is dat van een Duits expert, de heer Karsten NOHL. In december 2009, hebben hij en zijn team geoptimaliseerde zoektabellen voorgesteld om het coderingsalgoritme A5/1 te doorbreken en de nakende demonstratie aangekondigd van oplossingen waarmee de bescherming van de mobiele-telefonienetwerken kan worden omzeild. In augustus 2011 heeft hij de hardware- en softwarematige middelen onthuld die volgens hem zouden volstaan om daarin te slagen en in december 2011 heeft hij een studie gepubliceerd met betrekking tot 31 mobiele-telefonieoperatoren[2]. Deze studie concludeert met name dat de Belgische operatoren niet alle maatregelen nemen om het hoogste niveau van veiligheid te garanderen. Daarbij krijgen drie veiligheidsaspecten kritiek : misbruik van identiteit, de plaatsbepaling van de gebruiker en het bespioneren van communicatie.

[1] De cryptologie is de wiskundige wetenschap die de methodes bestudeert waarmee informatie vertrouwelijk kan worden uitgewisseld.
[2] http://GSMmap.org/

Het is moeilijk om "*a priori"* zonder meer in te stemmen met werk waarvan de motiveringen, de methode en de resultaten niet duidelijk worden vermeld en die niet de transparantie hebben die vereist is voor elk wetenschappelijk bewijs.

Bovendien gaat het om een mening die uitgaat van slechts één expert. De verdienste van deze studie bestaat echter erin dat de aandacht wordt gevestigd op mogelijke zwakke punten binnen de 2G- en 2,5G-technologieën voor mobiele telefonie.

Omgekeerd verdedigt de "GSM Association" (GSMA)[3], waarin de mobiele-telefonieoperatoren en de bijbehorende ondernemingen over de hele wereld verenigd zijn, sedert december 2009 een geruststellend standpunt wat de veiligheid betreft. De vereniging antwoordt op de publicaties van het team-NOHL via het volgende persbericht :

«[…] Reports of an imminent GSM eavesdropping capability are common. The GSMA, which welcomes research designed to improve the security of communications networks, routinely monitors the work of groups in this area. […] before a practical attack could be attempted, the GSM call has to be identified and recorded from the radio interface. So far, this aspect of the methodology has not been explained in any detail and we strongly suspect that the teams attempting to develop an intercept capability have underestimated its practical complexity. A hacker would need a radio receiver system and the signal processing software necessary to process the raw radio data. The complex knowledge required to develop such software is subject to intellectual property rights, making it difficult to turn into a commercial product. […][4]»

Voor zover wij weten heeft de GSMA zich niet uitgesproken over de jongste publicaties van het team-NOHL.

1.2. Voorwerp van het advies

Op 27 december 2011 heeft minister Johan VANDE LANOTTE, vice-eersteminister en minister van Economie, Consumenten en de Noordzee, aan het BIPT gevraagd om de mogelijke risico's voor de schending van de veiligheid van de Belgische diensten voor mobiele telefonie te onderzoeken.

Het BIPT heeft dus 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 de diensten voor mobiele telefonie. Deze enquête bestond uit een dynamische uitwisseling tussen de operatoren en het BIPT over 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.
Begin 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.

[3] De opdrachten ervan bestaan hoofdzakelijk erin de ontwikkeling en de bevordering van het GSM-netwerk, alsook de technologieën die daarvan zijn afgeleid, te ondersteunen.
[4] GSMA. GSMA Statement on Media Reports Relating to the Breaking of GSM Encryption. Persbericht van 30 december 2009, http://www.GSMa.com/newsroom/.

Omdat de verzamelde informatie van vertrouwelijke aard is, mag ze in dit document niet worden onthuld.

Na het juridische kader te hebben vermeld (punt 2) en na de beperking tot de 2G- en 2,5G-technologieën te hebben gerechtvaardigd (punt 3), zet deze nota het standpunt van de operatoren uiteen (punt 4), de interne analyse van het BIPT in verband met de problematiek van de risico's voor schending van de veiligheid van de mobiele-telefonienetwerken (punt 6), de analyse van de antwoorden van de operatoren (punt 7) en geeft ten slotte conclusies (punt 8).

2. JURIDISCH KADER

Op grond van de artikelen 113 en 114 van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna de wet van 13 juni 2005 genoemd) beschikt het BIPT over bevoegdheden met betrekking tot de veiligheid van de openbare netwerken en diensten voor elektronische communicatie. Het voormelde artikel 114 schrijft onder andere het volgende voor :

> *"De aanbieder van een openbare elektronische-communicatiedienst treft passende technische en organisatorische maatregelen om de veiligheid van zijn diensten te garanderen, indien nodig in overleg met de aanbieder van het openbare communicatienetwerk wat de veiligheid van het netwerk betreft. Die maatregelen waarborgen een zo hoog mogelijk beveiligingsniveau dat in verhouding staat tot het betrokken risico, rekening houdend met de stand van de techniek en de kosten van uitvoering ervan.*
> *[…] Wanneer er een bijzonder risico bestaat voor de aantasting van de veiligheid van zijn netwerk, licht de betrokken operator de abonnees en het Instituut over dat gevaar in.*
> *[…] Wanneer hij een schending van de integriteit van zijn netwerk vaststelt, neemt de betrokken operator alle nodige maatregelen om zo snel mogelijk de betrokken overheid, operatoren en abonnees in te lichten."*

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 de naleving van de wet van 13 juni 2005 te controleren.

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

Tot slot is het op basis van artikel 14, § 1, 1°, van de voormelde statuutwet dat het BIPT het advies heeft uitgebracht aan minister Johan Vande Lanotte.

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

Dit advies is beperkt tot de 2G- en 2,5G-mobieletelefoniediensten, hierna "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-technologieën

Ter herinnering: mobiele telecommunicatie is overgegaan van netwerken die gebaseerd waren op analoge normen, zogenoemd van de "eerste generatie" - in de jaren 80, met beperkte capaciteit en onderling incompatibel – naar netwerken op basis van een GSM-norm[5].

De essentiële vernieuwing van de GSM-, GPRS- en EDGE-netwerken ten opzichte van de voorgaande technologieën voor mobiele telefonie[6] 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 en ze was gebaseerd 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 circuitschakeling ondersteunt.

Het GPRS-netwerk[7] 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[8]-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 dat die van de 2G- of 2,5G–netwerken, waardoor de deur wordt opengezet voor multimediatoepassingen, zoals beeldtransmissie, videoconferentie of breedbandinternettoegang. 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[9]. De analyse van dat netwerk valt daarom buiten het bestek van dit advies.

4. STANDPUNT VAN DE OPERATOREN

In het algemeen vinden de operatoren dat de veiligheid integraal deel uitmaakt van de ontwikkeling van hun mobiele netwerk en tonen dat aan door de aanstelling van personeel dat

[5] GSM: Global System for Mobile Communications – Globaal Systeem voor Mobiele Communicatie.

[6] De eerste generatie (1G) van mobiele telefonie berust op analoge communicatie en overkoepelt verschillende normen, met name *Nordic Mobile Telephone* (NMT), *Advanced Mobile Phone System* (AMPS), *Total Access Communication System* (TACS) of Radiocom 2000.

[7] GPRS: *General Packet Radio Service* – Dienst voor dataoverdracht via pakketschakeling.

[8] EDGE: *Enhanced Data Rates for GSM Evolution* - Verhoogde Datasnelheid voor de GSM-Evolutie.

[9] 3G-normen bieden met name sleutels van 128 bits, een wederzijdse authenticatie en een versleutelde signalisatie.

uitsluitend voor die taak wordt ingezet en door de investeringen die op dat gebied worden gedaan.

De operatoren argumenteren dat de veiligheid van hun mobiele netwerk efficiënt is maar beseffen ook dat het veiligheidsniveau zal moeten toenemen naargelang van de evolutie van de dreiging, en dankzij de nieuwe functies die voortaan beschikbaar zijn. Zij benadrukken het feit dat elke evolutie van hun systeem maar mogelijk is na doorgedreven test- en validatiefases en dat ze niet alleen de relevantie ervan, de bijbehorende kosten en de tijd die nodig is voor de toepassing ervan moeten beoordelen, maar vooral de impact van deze maatregelen op de ervaring van de gebruiker. Volgens hen komt het dus erop neer ervoor te zorgen dat hun nieuwe oplossingen compatibel zijn met de oudste eindtoestellen.

Op basis van de informatie die van de operatoren verkregen is, erkent het BIPT de inspanningen die zij geleverd hebben om een hoog niveau van veiligheid van hun mobiele netwerk te bereiken.

Door de maatregelen die al genomen zijn en die gepland zijn, getuigen de operatoren van betrokkenheid, waarbij ze een werkelijke wil tonen om de veiligheid van hun mobiele netwerk te verhogen en snel naar die doelstelling toe te werken.

5. INTERNE ANALYSE

5.1. Veiligheid van de mobiele netwerken

De interne analyse van het BIPT is gebaseerd op de “state of the art” inzake veiligheid van de mobiele netwerken. Deze “state of the art” zet de veiligheidsmechanismen uiteen en toetst ze aan de huidige standaarden vanuit het oogpunt van de zwakke punten, dreigingen en tegenmaatregelen.

De onderstaande aspecten vormen de grootste inzet inzake veiligheid van de diensten voor mobiele telefonie :

- het verkeer en de activiteiten van de gebruiker mogen niet toegankelijk zijn voor derden;
- een gebruiker moet permanent op unieke wijze kunnen worden geïdentificeerd op het netwerk van de operator ;
- enkel de gebruiker mag toegang hebben tot de diensten waarop hij ingeschreven heeft.

Het risico voor schending van de veiligheid is verbonden aan het huidige niveau van dreiging, dat stijgt door technologische vooruitgang, ten overstaan van de kwetsbaarheid van de mobiele netwerken. Als dat risico voor schending bewezen is, moeten de nodige maatregelen worden genomen om het niveau van kwetsbaarheid van de mobiele netwerken te verminderen.

De meest kritische zwakke punten van de mobiele netwerken zijn inherent aan hun veiligheidsarchitectuur en zijn dus niet nieuw. Bij het uitwerken van de GSM-specificaties bestond het essentiële doel immers erin een volledig digitaal en unaniem goedgekeurde technologie voor mobiele telefonie voor te stellen. Tegenwoordig moet het gebrek aan wederzijdse authenticatie en het gebruik van bepaalde coderingsalgoritmen die ten opzichte van de technologische vooruitgang achterhaald zijn geraakt, ter discussie worden gesteld.

De interne analyse van het BIPT toont aan dat de systematische follow-up en de inzet van de nieuwe functies, zoals die welke ingevoerd worden door de normalisatie-instellingen, het mogelijk maken om de risico's voor schending van de veiligheid van de mobiele netwerken tot een minimum te beperken.

5.2. Beperkingen in verband met een verhoging van het veiligheidsniveau

Een verhoging van het veiligheidsniveau mag niet ten koste gaan van de ervaring van de klant en van de operationele capaciteit van de operatoren. Een compromis is dus absoluut noodzakelijk. Bovendien moet de compatibiliteit van de Belgische en buitenlandse eindapparatuur worden bestudeerd alvorens een nieuwe veiligheidsmaatregel toe te passen.

6. ANALYSE VAN DE ANTWOORDEN VAN DE OPERATOREN

De antwoorden van de operatoren zijn vertrouwelijk en mogen dus niet worden meegedeeld in dit advies.

De analyse van het BIPT beperkt zich bewust tot een kwalitatieve en algemene evaluatie van het gevaar voor schending van de veiligheid. De reikwijdte van de zwakke punten en van de daaraan verbonden tegenmaatregelen is niet beschouwd in termen van impactfactoren, zoals het aantal getroffen gebruikers. Het BIPT kan daarom het gevaar voor schending van de veiligheid niet nauwkeurig kwantificeren.

De analyse wijst er echter op dat de operatoren op eigen initiatief maatregelen nemen om een hoog niveau van veiligheid van hun mobiele netwerk te garanderen. Zij bestuderen en plannen momenteel nieuwe maatregelen om het niveau van veiligheid van hun mobiele netwerk nog meer te verhogen.

Inzake veiligheid zijn de mobiele netwerken aan het veranderen en zou het niet gepast zijn om vandaag te investeren in een meer uitvoerige analyse, die morgen niet langer valabel zou zijn. Het BIPT is dus van plan om tot de laatste vier maanden van 2012 te wachten tot de veiligheid van de netwerken zich stabiliseert, alvorens een meer doorgedreven analyse te verrichten. Het BIPT zal erover blijven waken dat de vandaag aangekondigde maatregelen werkelijk worden doorgevoerd.

7. SLOTCONCLUSIES

In het kader van de enquête hebben de operatoren aan het BIPT geen elementen meegedeeld die het BIPT zouden kunnen doen concluderen tot een schending van de veiligheid van hun mobiele netwerk.

Het BIPT merkt op dat de operatoren getuigen van een bijzondere aandacht voor de veiligheid van hun mobiele netwerk in termen van beheer, investeringen en technologische vernieuwing. *A priori* is de veiligheid van hun mobiele netwerk vandaag toereikend. Ze kan echter nog worden verbeterd door met name de jongste functies toe te passen die geleverd worden door de specificaties van de GSM-, GPRS- en EDGE-normen.

Het BIPT zal een nieuwe algemene analyse verrichten in het vierde kwartaal van 2012. Deze algemene analyse zal een aanvullende interne analyse, een ruimere enquête onder de operatoren omvatten, alsook controles in verband met de doeltreffendheid van de veiligheid van de mobiele netwerken.

Axel Desmedt
Lid van de Raad

Charles Cuvelliez
Lid van de Raad

Catherine Rutten
Lid van de Raad

Luc Hindryckx
Voorzitter van de Raad