NEDERLAND ICT

Ministerie van Economische Zaken
De heer H.G.J. Kamp
Postbus 20101
2500 EC DEN HAAG

Woerden, 17 maart 2014

Betreft : reactie Nederland ICT op wetsvoorstel IMEI-blokkade
Kenmerk : 37248/BP

Geachte heer Kamp,

Graag maakt Nederland ICT gebruik van de consultatie over het wetsvoorstel IMEI-blokkade om kritisch te reflecteren op het algehele voorstel om IMEI-blokkade in Nederland in te voeren.

Nederland ICT steunt van harte het streven van de overheid om gestolen mobieltjes op afstand onbruikbaar te maken. Wanneer dit op effectieve wijze kan, wordt de diefstal zinloos en is te verwachten dat straatroof verder zal afnemen.

De overheid ziet vooralsnog het blokkeren van IMEI-nummers van gestolen mobieltjes op de mobiele netwerken in Nederland als de aangewezen technische methode. De telecomsector deelt deze visie niet, omdat er een veel effectiever en efficiënter alternatief reeds beschikbaar is, verder beschikbaar zal komen en steeds verder ontwikkeld zal gaan worden.

De sector heeft in de afgelopen periode constructief met de overheid onderzocht hoe een systeem voor IMEI-blokkades optimaal kan werken. Dit heeft geleid tot een voorkeurscenario. Dit scenario kent desondanks belangrijke beperkingen die inherent zijn aan IMEI-blokkades:

- Het toestel zelf wordt niet onbruikbaar. Uitsluitend de toegang tot het mobiele netwerk wordt geblokkeerd.
- Het toestel blijft toegang tot Wifi hebben en blijft daarmee een aanzienlijke waarde vertegenwoordigen. Een groot aantal tablets wordt zelfs nieuw al zonder mobiele toegangsfunctionaliteit verkocht en werkt alleen op Wifi.
- IMEI-blokkade werkt in Nederland als alle aanbieders hieraan deelnemen. Dat regelt deze wet. Het toestel zal echter buiten Nederland, in landen waar niet een dergelijk systeem (met gebruik van dezelfde database) is geïmplementeerd, gewoon toegang tot het mobiele netwerk houden. Met veel criminele Oost-Europese bendes actief in Nederland zullen toestellen juist daar eindigen waar IMEI-blokkering niet is ingevoerd.
- Bij oudere toesteltypes is de IMEI-blokkade zeer eenvoudig te omzeilen door het IMEI-nummer te wijzigen. Ook blijft er bij nieuwere toestellen altijd een reële kans dat mogelijkheden worden gevonden om het IMEI-nummer te manipuleren.
- In artikel 10.12, lid 5 van het wetsvoorstel is een verbod op deze manipulatie opgenomen. Nederland ICT is blij hiermee maar zet tegelijk grote vraagtekens bij de handhaafbaarheid ervan door het Agentschap Telecom.
- Het implementeren van het IMEI blokkade proces zal minimaal negen maanden in beslag nemen.

- Met bijna 15 miljoen euro aan initiële investeringen en 3,5 miljoen euro jaarlijks terugkerende lasten zijn zeer aanzienlijke eenmalige en terugkerende kosten aan het inrichten en onderhouden van het proces verbonden.

De internationale industrie zet momenteel in op een alternatief, de 'kill switch' (nieuwe beveiligings- en blokkeringssoftware op toestellen) dat bovengenoemde beperkingen niet kent:

- Apple's iPhones, het belangrijkste doelwit, beschikken met iOS7 al over gebruiksvriendelijke en zeer effectieve software om de toestellen voor anderen dan de eigenaar volledig onbruikbaar te maken, waar deze zich ook ter wereld bevindt.
- Samsung en LG hebben eerder reeds aangekondigd met vergelijkbare oplossingen te komen.
- In de Verenigde Staten is een wetsvoorstel ingediend dat deze beveiligingssoftware verplicht op nieuwe toestellen. Hiermee wordt deze ontwikkeling extra vaart gegeven.
- De Nederlandse samenleving hoeft geen kosten te maken om van deze ontwikkeling te profiteren.

Om bovengenoemde ontwikkelingen vindt de telecomsector daarom dat de overheid haar standpunt over IMEI-blokkade moet heroverwegen. Er zijn immers alternatieven beschikbaar die nu al effectiever en gebruikersvriendelijker zijn dan IMEI na volledige implementatie kan worden. De beschikbaarheid van deze alternatieven in de nabije toekomst toenemen en de technologie zal zich snel ontwikkelen. Het is daarom niet wenselijk de industrie te verplichten in te zetten op IMEI-blokkade als technologie. Evenmin is het proportioneel richting sector om hen te verplichten hoge kosten te maken terwijl er een goed alternatief beschikbaar is.

Nederland ICT stelt daarom voor om het wetsvoorstel zo aan te passen dat de industrie tot IMEI-blokkades verplicht *kan* worden, indien blijkt dat de 'kill switch', tegen de verwachtingen in, niet van de grond blijkt te komen. Naast effectieve 'kill switches' hebben IMEI-blokkades geen toegevoegde waarde. Daarbij is de telecomsector graag bereid om samen met de overheid te werken aan intensieve voorlichting over het voorkomen van diefstal en het beveiligen van smartphones.

Voor wat betreft de verwachte effectiviteit en de bijkomende kosten stelt Nederland ICT voor een doorrekening te laten maken, waarbij de verschillende instrumenten, zoals de IMEI-blokkade, de 'kill switch' en mogelijk andere alternatieven, tegen elkaar worden afgezet.

In de bijlage heb ik de bovenstaande argumenten verder uitgewerkt en van concrete vragen voorzien. Graag is Nederland ICT bereid om deze nader toe te lichten.

Met vriendelijke groet,
Nederland ICT

Lotte de Bruijn
directeur

Bijlage

Nederland ICT heeft haar argumenten rondom de heroverweging van IMEI-blokkade hieronder puntsgewijs en in een aantal vragen uitgewerkt.

1. **Effectiviteit en proportionaliteit: hoogte van de investering niet in balans met de verwachte opbrengst**

- Het wetsvoorstel is gericht op het bestrijden van straatroof. Uit op 6 maart gepubliceerde cijfers van de politie blijkt dat het gaat om ongeveer 7.000 straatroven in 2013. Uit de cijfers blijkt dat er sprake is van een dalende trend in het aantal straatroven (daling van ongeveer 12%).
- In ongeveer 50% van de gevallen was (ook) de mobiele telefoon doelwit. De overheid verwacht dat het aantal straatroven met 20% daalt na invoering van IMEI-blokkade. Het verwachte effect is dus ongeveer 700 tot 1300 minder straatroven op jaarbasis.
- Cijfers over dalingen zijn bekend uit het Verenigd Koninkrijk en Australië (bij deze daling speelt mogelijk een rol dat beide landen eilanden zijn, waardoor gestolen toestellen het land moeilijker kunnen verlaten). Volgens korpschef Bouman (interview AD 7 maart 2014) is deze effectiviteit ook in Frankrijk en Duitsland is gemeten. Kunt u de bron van deze cijfers aangeven?
- Duitsland kent immers geen dekkend systeem van IMEI-blokkade. De meeste telecomaanbieders zijn niet overgegaan tot of zelfs gestopt met IMEI-blokkade vanwege negatieve ervaringen, onder andere door de manipuleerbaarheid van IMEI-nummers met behulp van speciale software.

- Het ontbreekt in de onderbouwing van de effectiviteit in het tegengaan van straatroof aan de motieven en daderprofielen. Dit bepaalt mede of IMEI-blokkade een effectief instrument kan zijn.
    - In 2013 werd bekend dat veel van deze diefstallen tijdens festivals zoals de Gay Pride plaatsvonden en dat vooral Oost-Europese bendes zich hieraan schuldig maakten. Bij de Gay Pride waren 41 van de 46 verdachten van Roemeense afkomst[1]. Deze bendes zullen gestolen waar snel (over land) naar andere Europese landen 'exporteren' of zullen deze gaan exporteren als toestellen in Nederland niet op het netwerk kunnen.
    - Begin van dit jaar werd bekend dat Haagse jongeren niet voor diefstal roven maar voor de kick[2]. De sector twijfelt of een IMEI-blokkade hiertegen effectief is.

- Tegen de verwachte effectiviteit staan de kosten die gemaakt moeten worden. De kosten van het systeem zijn bijna 15 miljoen euro initieel en vervolgens per jaar nog eens 3,5 miljoen euro (1,8 miljoen euro kosten en 1,7 miljoen euro nalevingskosten). In de periode van 2015 tot 2020 (6 jaar) kost het systeem de maatschappij dus bijna 36 miljoen euro. Uitgaande van de door de overheid verwachte structurele daling van 20% leidt dit in diezelfde periode tot ongeveer 8000 straatroven minder. Dit betekent een investering van 4.500 euro per voorkomen straatroof. Nederland ICT vindt dit niet proportioneel.

  Daar staat tegenover dat producenten van smartphones internationaal werken aan de zogenoemde 'kill switch', waarbij de consument het toestel op afstand geheel onbruikbaar kan maken, waar ter wereld het zich ook bevindt. De verwachting is dat op korte termijn de meeste nieuwe mobiele telefoons een 'kill switch' zullen hebben.

[1] http://nos.nl/artikel/536886-roemenen-slaan-toe-bij-gay-pride.html en http://nos.nl/op3/artikel/453892-pas-op-voor-smartphone-dieven.html
[2] http://nos.nl/artikel/593083-haagse-tieners-roven-voor-de-kick.html

2. Toestellen blijven bruikbaar na blokkering in Nederland

De verwachting lijkt te bestaan dat toestellen waarvan het IMEI-nummer wordt geblokkeerd ook onbruikbaar zijn. Dit is niet het geval. Met een IMEI-nummer kan het toestel niet meer op de Nederlandse mobiele netwerken, maar kan nog wel gebruikt worden via Wifi of in het buitenland waar het systeem niet is ingevoerd. Ook functionaliteit waar in het geheel geen internettoegang nodig is blijft werken. Korpschef Bouman vindt het belangrijk dat een toestel geblokkeerd wordt, zodat een dief er niets meer aan heeft (interview AD 7 maart 2014). Dit is echter alleen het geval bij een 'kill switch' en niet bij IMEI-blokkering.

a. Bruikbaarheid van het toestel buiten het netwerk van aanbieders om:

- Het tegengaan van straatroof heeft alleen dan maximaal effect wanneer toestellen daadwerkelijk onbruikbaar worden. Nederland ICT pleit voor een effectieve methode voor smartphoneblokkade.
- IMEI-blokkade maakt toestellen zelf niet onbruikbaar en ook data blijft op het toestel staan. Het enige dat IMEI-blokkade mogelijk maakt, is het feit dat toestellen niet meer bruikbaar zijn op het mobiele netwerk van een aanbieder in Nederland (en andere landen waar IMEI-blokkade geldt).
- Nu steeds vaker mobiel internet en communicatie via Wifi plaatsvindt (denk aan Whatsapp, Facetime, voice over IP) neemt ook de kans toe dat toestellen gebruikt blijven worden ondanks IMEI-blokkering. Het blokkeren van toestellen via Wifi is geen mogelijkheid, aangezien hierbij geen IMEI-nummer wordt geregistreerd. Een geblokkeerd toestel heeft natuurlijk minder functionaliteiten maar behoudt dus ook nog een belangrijk deel van zijn waarde.

b. Bruikbaarheid in landen waar geen IMEI-blokkering actief is:

- IMEI blokkering werkt alleen in die landen die ook IMEI blokkering hebben en aangesloten zijn op de CEIR database.
- In Europa is een aantal landen aangesloten op deze database[3] maar een groot aantal landen ook niet. Dat betekent dat wanneer een gestolen toestel naar die landen gaat, de toestellen nog altijd bruikbaar blijven. Onder meer in Duitsland is er geen sprake van een sluitend systeem van IMEI-blokkade. De meeste landen in Oost- en Zuidoost-Europa (herkomst van veel rondtrekkende criminele bendes) werken niet met IMEI-blokkering.
- Het is te verwachten dat criminelen die zich nu nog richten op de 'binnenlandse afzetmarkt' kanalen vinden om gestolen toestellen naar het buitenland te sluizen waar IMEI-blokkering niet is ingevoerd.

c. IMEI-nummers kunnen worden gemanipuleerd:

- Ondanks steeds zwaardere beveiliging van toestellen is manipulatie van IMEI-nummers nog altijd mogelijk. Beveiliging is een *ratrace* met criminelen en de aanpasbaarheid van IMEI is niet uit te sluiten. Dit feit blijkt in Duitsland een reden te zijn geweest dat telecombedrijven afzagen van IMEI-blokkering.
- Daarbij neemt de kans toe dat cybercriminelen zoeken naar manieren om beveiliging te omzeilen groter naar mate toestellen op dit onderdeel geblokkeerd gaan worden.

[3] Alleen in België, Denemarken, Estland, Finland, Frankrijk, Groot-Brittannië, Ierland, Italië, Noorwegen en Zweden is sprake van een sluitend systeem van IMEI-blokkade.

3. Vraagtekens bij handhaving verbod op manipulatie IMEI-nummers

- Artikel 10.12 lid 5 bepaalt dat het verboden is om IMEI-nummers te manipuleren. Nederland ICT is blij dat de overheid deze zorg erkent.
- Tegelijk heeft Nederland ICT vragen of de strafbaarstelling van IMEI-manipulatie via deze wet gehandhaafd kan worden:
    - In de MvT wordt duidelijk dat in het Wetboek van Strafrecht geen duidelijke wettelijke grondslag is voor het verbod. Er wordt hierbij alleen verwezen naar bestaande wetsartikelen (heling en schuldwitwassen). Dit in tegenstelling tot bijvoorbeeld Australië waar via een aparte wet een verbod op en strafbaarstelling voor IMEI-blokkade werd geïntroduceerd. Dit wordt in een Australisch overheidsrapport over IMEI-blokkade benoemd als een belangrijke maatregel die heeft gezorgd voor daling van straatroof.
    - Uit de Memorie van Toelichting wordt ook duidelijk dat het Agentschap Telecom zorgdraagt voor de handhaving. Nederland ICT vraagt zich af of het AT zowel juridisch als technisch in staat is om deze handhaving waar te maken en wat er in de praktijk aan handhaving gebeurt.

- Vragen Nederland ICT bij handhaafbaarheid:
    - Hoe luidt het advies van de toezichthouder zelf inzake de handhaafbaarheid van deze bepaling? Wordt van het AT een actieve handhaving (en opsporing van overtreders) verwacht?
    - Hoe verhoudt deze bepaling zich tot de rol van politie en het Openbaar Ministerie? Betekent dit dat het AT eerst IMEI-manipulatie moet vaststellen en vervolgens dit moet doorgeven aan het Openbaar Ministerie. Welke garanties kan de overheid geven dat de politie en het Openbaar Ministerie ook zonder verwijzing van het AT handhavend zullen optreden op basis van dit artikel in de Telecommunicatiewet? Kan in de toelichting worden aangegeven of het Openbaar Ministerie van plan is om hierop te handhaven? Wordt manipulatie van IMEI-nummers toegevoegd aan de prioriteiten van de Nationale Politie?

4. Nalevingskosten alternatieve instrumenten en impact op investeringsklimaat

- De telecomsector heeft een inventarisatie van de verwachte kosten gemaakt. Heeft de overheid ook inzicht wat de nalevingskosten zijn van alternatieven voor IMEI-blokkade? Hoe oordeelt de overheid over de verhouding tussen baten en lasten in relatie tot deze alternatieven?
- Kan de overheid een onafhankelijke instantie laten inventariseren wat de kosten-batenanalyse (effectiviteit-proportionaliteit) is van alternatieven in de strijd tegen straatroof m.b.t. smartphones?
- Is het mogelijk om een onafhankelijke instantie een inventarisatie te maken van de kosten die door de telecomsector moeten worden gemaakt omwille van overheidsbeleid? Het investeringsklimaat in de telecomsector staat onder druk. Een investering van de sector in IMEI-blokkade leidt er wederom toe dat miljoenen euro's niet besteed kunnen worden in het innoveren, uitbreiden of onderhouden van het communicatienetwerk. Kan de overheid een onderzoek laten doen wat investeringen die op aanwijzing van de overheid moeten gebeuren, betekenen voor het investeringsklimaat in de Nederlandse telecomsector?
- Hoewel niet direct in de belangensfeer van Nederland ICT, ontbreekt volgens Nederland ICT in de Memorie van Toelichting een inventarisatie van de verwachte nalevingskosten bij toezichthouders als het Agentschap Telecom en het College Bescherming Persoonsgegevens.

5. De alternatieven

a. Technologie in de smartphone: de 'kill switch'

- Diverse smartphone producten hebben in het afgelopen jaar aankondigingen gedaan dat zij in hun toestel technologie gaan implementeren die het de gebruiker mogelijk maakt om zijn toestel op afstand onbruikbaar te maken na diefstal. Deze 'kill switch' maakt een toestel geheel onbruikbaar en werkt wereldwijd (dit in tegenstelling tot IMEI-blokkade dat alleen toegang tot het netwerk blokkeert en werkt in landen met een soortgelijk systeem).
- Voorbeelden hiervan zijn:
    - Apple heeft deze technologie zomer 2013 reeds geïntroduceerd: http://support.apple.com/kb/HT5818?viewlocale=nl_NL en http://support.apple.com/kb/PH2700?viewlocale=nl_NL
    - Samsung en LG hebben in de zomer van 2013 aangekondigd dat zij deze technologie zullen introduceren: http://www.androidpit.com/kill-switch-for-samsung-and-lg-devices
- Tegelijk wordt in de VS gewerkt aan de 'smartphone theft prevention act' die producenten verplicht om een 'kill switch' in te bouwen in toestellen die nieuw op de markt komen.

b. Intensieve voorlichting over bestaande mogelijkheden

- In de media laten korpschefs zich regelmatig uit over het feit dat consumenten onvoorzichtig zijn met hun smartphone en deze opzichtig gebruiken en dat dit straatroof zou uitlokken. Hier heeft de consument een eigen verantwoordelijkheid.
- Er zijn diverse alternatieven voorhanden waarvan de consument gebruik kan maken:
    - Smartphones bieden veel beveiligingsopties maar worden vaak slecht toegepast. Consumenten kunnen hun toestel veel beter beveiligen met een (unieke) pincode of wachtwoord
    - Veel smartphones bieden de mogelijkheid om het toestel op afstand te traceren, te blokkeren en de gegevens te wissen. Dit vraagt van de consument dat zij dit tijdig instellen. Zonder toestemming van de legitieme gebruiker kan een toestel al niet gebruikt of gewist worden.
    - Daarnaast zijn diverse apps beschikbaar om het toestel te traceren, te blokkeren en gegevens te wissen. Ook enkele providers bieden hun klanten deze apps.
- De sector is graag bereid om samen met de overheid te werken aan een voorlichtings-campagne die consumenten waarschuwt om voorzichtiger met hun smartphone om te gaan en wijst op de mogelijkheden om hun smartphone te beveiligen.