VERSLAG

SECURITY CAFÉ

INLICHTINGEN EN ONZE PRIVACY

Nederland wil opheldering over het mogelijk verzamelen van internetgegevens door Amerikaanse veiligheidsdiensten. Het zusterbedrijf van Belgacom blijkt twee jaar lang bespioneerd te zijn door de Britse geheime dienst (GCHQ) en de mobiele telefoon van Angela Merkel blijkt afgeluisterd te worden door de Amerikanen in Duitsland.

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 19 november 2013, werd bij Schuberg Philis te Schiphol-Rijk georganiseerd. In het expertpanel Alexander Blom, CEO van Budget Phone Company en bestuurslid Internet Society Nederland. Ronald Huijgens van Unisys. Erik de Jong als cybercrime lead van FOX-IT en Ricky Gevers als IT-forensic specialist van Digital Investigation. Hier volgt een impressie van de discussie aangevuld met onthullingen in het NRC over het NSA-Dossier.

Om maar met de deur in huis te vallen met de eerste vraag: Hoe kan een inlichtingendienst twee jaar lang spioneren zonder dat een telecomprovider dat door heeft en er ook geen andere alarmbellen afgaan? En als ze dan toch ontdekt worden, hoe komt het dan dat het te traceren is naar de Britse geheime dienst? Allereerst moet je van goeden huize komen om zo'n lek te ontdekken, omdat top-hackers aan de andere kant echt wel weten wat ze doen. Echter, soms worden er kleine 'foutjes' gemaakt die de identiteit van de aanvaller toch blootleggen, alsdus IT-forensic specialist Ricky Gevers. Niettemin hebben de documenten van Snowden geholpen bij het vaststellen wie de ongenode gast was, alsdus Erik de Jong.

Hoezo kan de Britse GCHQ zomaar een commercieel Belgisch bedrijf bespioneren? Er zijn toch wel wettelijke regels voor? De wereld van 'Intel' en 'diplomatie/politiek' zijn ver van elkaar verwijderd, aldus Erik de Jong. Dat is wat de huidige situatie zo gênant maakt voor veel partijen (en niet alleen de daders). Spionage is een 'geaccepteerd' middel van alle tijden, het grote verschil is hier wel de mate waarin dat wordt gedaan in deze gevallen. Het is een interessant vraagstuk, in welke mate spionage acceptabel is. Hoeveel kost het en wat levert het eigenlijk op? Aangezien elk land op dit vlak zijn eigen spelregels kan maken. Je moet jezelf afvragen of overheden boven de wet staan en de 'privacy' mogen ontnemen zonder gegronde reden.

Het lijkt alsof buitenlandse overheden gegevens opvragen/vastleggen over Nederlanders, aldus Alexander Blom. Niemand lijkt verantwoordelijk te zijn of inzicht te kunnen geven in wat er precies gebeurt. Hier moet de rechter kritisch naar kijken. Daarom steunt o.a. Internet Society Nederland het initiatief om minister Plasterk aan de klagen voor witwassen van informatie over Nederlanders. De honger naar data is niet te stillen bij inlichtingendiensten.

Gerco Kanbier is directeur van Trust in People – the information protection company.

Hij is te bereiken via gerco.kanbier@trustinpeople.com

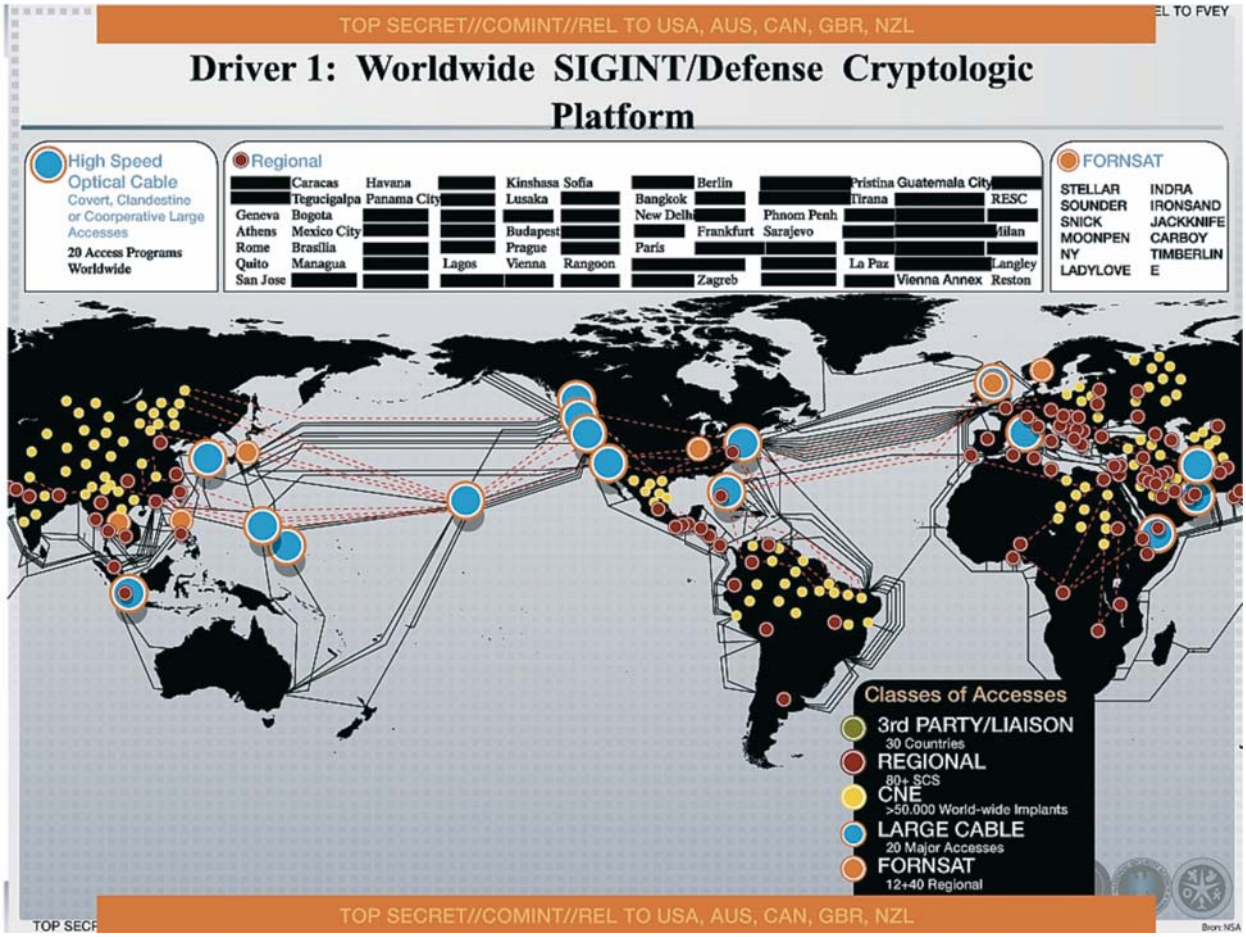
"Opinie over NRC onthullingen"

Dit Security Cafe viel nog net vóór de onthullingen van de NRC over het NSA Dossier, dat gebaseerd is op de documenten van Snowden. De 'opheldering' die minister Plasterk heeft gekregen van de Amerikaanse overheid, is dat er meta-gegevens zijn vastgelegd van 1,8 miljoen telefoongesprekken per maand. Er is in de media heel weinig over bekend of dit Nederlanders zijn die naar Amerika hebben gebeld, of dat dit de top van het Nederlandse bedrijfsleven is, of alleen mogelijke terroristen. Ik heb zelf even gekeken hoeveel ik bel per maand. Dat komt neer op grofweg 300-500 gesprekken en zou impliceren dat metagegevens van zo'n 4 tot 10.000 Nederlanders zijn vastgelegd door de NSA. Op zeer beperke schaal dus en dan alleen nog maar de metagegevens. Dan is vervolgens de vraag: Geeft Nederland deze informatie over telefoongesprekken of opereren de Amerikanen op eigen houtje? Gezien de vraag over opheldering van minister Plasterk, vermoed ik dat laatste. Danwel is het een slechte poging om de samenwerking tussen inlichtingendiensten te verhullen. Op zaterdag 23 november 2013 stond in het NRC dat de Amerikaanse inlichtingendienst NSA meer dan 50.000 computernetwerken heeft gehackt en sinds 1948 Nederland bespioneert.

In dezelfde krant staat de oprichting van het Joint Sigint Cyber Unit in 2014, een samenwerkingsverband tussen de MIVD en AIVD om actief te monitoren in cyberspace. Nu is het volgens de Wet op de Inlichten- en Veiligheidsdiensten verboden om data ongericht te analyseren van kabelgebonden-informatie. Let op, analyseren is volgens de wet iets anders dan verzamelen. Het project met de naam Argo II is bedoeld om vanaf 2014 'informatie uit communicatiemiddelen te verwerken tot inlichtingen', schreef minister Plasterk van Binnenlandse Zaken deze zomer aan de Tweede Kamer. Het systeem zal waarschijnlijk worden gebouwd door het Israëlische Nice Systems, gespecialiseerd in surveillance- en afluistersoftware, aldus een artikel in de Volkskrant. Volgens de technologiewebsite Tweakers kan dit systeem landelijk data onderscheppen, monitoren, analyseren en opslaan, en automatisch waarschuwen bij verdachte patronen. Wij Nederlanders zijn verontwaardigd dat we bespioneerd worden door onze bondgenoten, maar toch gaat Nederland nu de wet aanpassen om de burgers beter te beschermen door ongericht informatie over medelanders vast te leggen. Met welk doel? Gaat de JSCU (AIVD+MIVD) de NSA, GHCQ en de Mossad een koekje van eigen deeg geven door alle wereldburgers te bespioneren?

Wat mij ook opvalt aan deze kaart is het ontbrekende gedeelte: namelijk de 30 landen die als liaison samenwerken, waaronder Nederland. Hoe werkt Nederland dan samen met de NSA? Is dat, net zoals bij dat zusterbedrijf van Belagcom in Belgie, specifiek met één bedrijf die 'stiekem' informatie levert en daarom uit de NRC-publicatie is weggelaten? Dat kabeltje voor een aftakking naar een inlichtingendienst ga je niet vinden met een parlementair onderzoek. Hier heb je voorkennis van een 'insider' nodig, zoals Snowden. Met alle huidige publicaties rond dit onderwerp, wordt het onwaarschijnlijk dat er officieel gebruik wordt gemaakt van de aftapverplichting die alle telefonie- en internet bedrijven hebben.

Nu werden in het NRC Google, LinkedIn en Facebook ook genoemd als bronnen waar de NSA onbeperkt toegang toe zou hebben. Deze bedrijven zijn aangesloten bij het Safe Harbour convenant, waarin de verschillen in wetgeving tussen EU en de VS op gebied van Privacy en de Data Protection Act worden 'gerepareerd'. Dit houdt in dat Google, Facebook of LinkedIn jou als klant netjes horen te melden wanneer de NSA jouw gegevens heeft opgevraagd. Voor zover ik uit diverse media begreep, wordt er op zeer beperkte schaal klantdata opgevraagd o.b.v. een officiële verdenking. Echter, ik heb het vermoeden dat de NSA zich niet aan stoort officiële verdenkingen. Vanwege het staatsbelang kan de NSA gewoon meta-gegevens verzamelen op andere toegangspunten tot het internet (op tier 1 niveau). Op deze punten worden metagegevens van telefoon, e-mail, locaties en bankoverschrijvingen ontsleuteld en verzameld. Dit alles met als doel terrorismebestrijding. Of is kennis toch macht, die we ook mogen gebruiken voor politieke en commerciele doeleinden? Dit laatste is een glijdende schaal en ligt in dezelfde categorie als voorkennis van koersgevoelige informatie. Doelbinding en streng toezicht zijn een eerste vereiste. Ik verwacht dat de toezichthouders ook in deze branche de honger naar kennis nog moeten gaan beteugelen.



Hoe kan een inlichtingendienst spioneren zonder dat een telecomprovider dat door heeft?

Tot slot hadden we het in het Security Café over die politieke rel rond het afluisteren van de mobiele telefoon van Angela Merkel. Ronald Prins van Fox-IT had in Pauw en Witteman een cryptotelefoon meegebracht naar de uitzending. Zo'n telefoon is natuurlijk een oplossing, maar dan kun je niet voorkomen dat je privé-telefoontjes onderschept worden, daar beide partijen zo'n telefoon nodig hebben. Volgens Ronald Huijgens is dit ook anders op te lossen. Unisys heeft namelijk voor het ministerie van Defensie in Amerika (Department of Defence) technologie ontwikkeld die onzichtbaar is in alle communicatiekanalen (internet, WAN, wireless, 3G, 4G en satelliet) zolang het maar 'packet- switched' is. VoIP verkeer via Skype is dus prima te beveiligen. Deze beveiliging werkt echter niet zodra het circuit-switched is, zoals het geval is bij traditionele telefonie. Daarom blijft het mogelijk dat met de juiste apparatuur (zoals een mobiele zendmast op naburige ambassade) makkelijk een man-in-de-middle attack op te zetten. Alle telefoontjes in een bepaalde straal zoeken namelijk het sterkste signaal van de dichtstbijzijnde mast. Als die mast van een derde partij is, kun je alle gesprekken in een bepaalde straal opvangen en meeluisteren zonder dat men het doorheeft.

Aan het einde van de panelsessie, werd ik door een oud-MIVD-er aangesproken opdat wij wel erg naïef zijn als security professionals. Nu zijn inlichtingendiensten een wereld waar informatiebeveilging professionals zich niet dagelijks begeven. Maar voor de maatschappelijk discussie was dit café wel een wake-up call.

Links
Security Cafe: http://www.trustinpeople.com/security-cafe