Inleiding Ronald Prins, Fox-IT

Hartelijk dank voor uw uitnodiging.

U heeft hij mij ter voorbereiding van deze sessie drie deelvragen gegeven. Laat ik ook de vrijheid nemen om een tweetal andere belangrijke thema's onder het kopje bedrijfsspionage te bespreken. Deze zijn:

- Hoe groot is het probleem van bedrijfsspionage in Nederland?
- Zijn bedrijven zelfstandig in staat zich daar voldoende tegen te wapenen, en wat voor rol zou de overheid daar bij kunnen spelen?

Maar eerst uw vragen:

- Is het toelaatbaar dat onder druk van inlichtingendiensten bij bedrijfsnetwerken en providers/softwareleveranciers achterdeurtjes worden gecreëerd?

Ik snap uw vraag vanuit de onthullingen van Edward Snowden. Het creëren van achterdeurtjes is alleen zinvol voor die landen waar een eigen serieuze software of hardware industrie aanwezig is. In Nederland wordt heel weinig software ontwikkeld dat breed verspreid wordt. Ik kan me dus niet voorstellen dat Nederlandse diensten zich hier mee bezighouden.

Achterdeurtjes lijken misschien handig maar zijn niet ook per se essentieel om een succesvolle cyberint operatie uit te voeren. Als het criminele hackers al lukt om 10 duizenden computers in Nederland te hacken, dan moet het de AIVD ook wel lukken om daar succesvol in te zijn, zonder van te voren achterdeurtjes te creëren.

- Leidt dit tot een onverantwoorde verzwakking van de IT-infrastructuur?

IT-infrastructuur is vanuit zichzelf al zwak. Dat hebben we kunnen zien uit het HeartBleed incident van vorige week. De standaard software die onder andere het slotje in uw browser laat zien, bleek een enorm lek te hebben dat er al twee jaar in zat. Theoretisch benaderd zal elke extra achterdeur leiden tot een verdere verzwakking van infrastructuur. Mocht bijvoorbeeld een andere inlichtingendienst ontdekken hoe de achterdeur in elkaar steekt, dan zou het voor die dienst makkelijker kunnen worden om massaal in te breken. Maar nogmaals, het pad van de achterdeurtjes is voor Nederlandse diensten niet interessant. We produceren hier nauwelijks software die over de wereld verspreid wordt.

- In welke mate verspreiden inlichtingendiensten malware, en is dat toelaatbaar?

Wij worden regelmatig geconfronteerd met malware van buitenlandse inlichtingendiensten. En nee dat is niet toelaatbaar, het is immers strafbaar computer vredebreuk in Nederland te plegen. Maar ik denk dat uw vraag zich vooral richt op de Nederlandse diensten. Ik heb daar geen idee van. Vanuit Nederlands oogpunt biedt in ieder geval de WIV wel de mogelijkheid.

- Hoe groot is het probleem van bedrijfsspionage in Nederland

Zoals u ook in het jaarverslag van de AIVD heeft kunnen lezen is spionage bij bedrijven een toenemend probleem. Dat is ook niet zo vreemd gezien dat het voor de aanvaller relatief goedkope en risicoloze operaties zijn.

De geraffineerdheid van dit soort aanvallen maakt dat het een zeer complexe operatie is om dit soort aanvallen te onderkennen in netwerken.

Wij helpen regelmatig bedrijven die een externe aanleiding hebben om dit te onderzoeken. Met een stofkam ontdekken we het dan ook wel uiteindelijk. Vaak zelfs meerdere campagnes tegelijk die soms ook al meerdere jaren bezig zijn en nog nooit eerder onderkend zijn.

De aanvallen die we onderkend hebben in Nederland en andere landen in de EU geven al voldoende aanleiding om ons zorgen te maken. Maar al deze aanvallen komen naar boven, niet om dat er structureel naar gezocht wordt, maar om dat er een externe aanleiding is om te gaan zoeken. We hebben bijvoorbeeld onderzoeken gedaan omdat uit de Snowden papers bleek dat er waarschijnlijk ingebroken was. De wijze hoe nu de spionage-incidenten aan het licht komen, rechtvaardigen volgens mij de conclusie dat we nu slechts het topje van de ijsberg zien.

- Zijn bedrijven zelfstandig in staat spionage te onderkennen, en wat zou de rol van de overheid hierin kunnen zijn

Ik denk dat we slechts een handvol organisaties in Nederland op dit moment zelfstandig in staat zijn spionage operaties in hun netwerken te onderkennen en daarmee te stoppen. Maar zelfs de beste in dit spel redeneert vanuit de zienswijze: ”De Chinezen zitten in ons netwerk, en we gaan er vanuit de onze gevoelige informatie bij hun bekend is”.

Ik zie hier nadrukkelijk een rol voor onze veiligheidsdienst. Net zoals de AIVD in het fysieke domein inlichtingen operaties van andere landen onderkent door rond te ‘kijken’ en te ‘praten’ zouden ze dit ook in het digitale domein moeten doen. Het ontbreekt hun echter nu aan een essentiële bevoegdheid daarvoor, namelijk kabelgebonden interceptie. Alleen door mee te kijken op grote knooppunten kan in kaart gebracht worden wat andere landen in de netwerken van onze bedrijven uitspoken. Ik pleit hier nadrukkelijk voor deze bevoegdheid vanuit een verdedigend standpunt en niet om onze diensten hiermee ook een massale surveillance bevoegdheid te geven. Dat is een hele andere discussie die apart gevoerd dient te worden.