Consultatie van het voorontwerp voor het

Besluit onderzoek in een geautomatiseerd werk

Reactie van KPN

KPN
Contactpersoon: Drs. W.M. Hoogeveen
Postbus 30 000
2500 GA Den Haag
maurice.hoogeveen@kpn.com

Kenmerk: RG/17/U/002

29 mei 2017

Inleiding en samenvatting

Met de snelle ontwikkelingen op het gebied van ICT wordt cybercrime een steeds groter probleem. Het is daarom begrijpelijk dat de Nederlandse overheid wetgeving op het gebied van de bestrijding van cybercrime moderniseert om zo mee te gaan met de tijd. De uitbreiding van het instrumentarium van justitie en politie is in hoge mate de verantwoordelijkheid van de politiek en het bestuur. In deze consultatiereactie worden enkele aandachtspunten bij het Besluit onderzoek in een geautomatiseerd werk geplaatst, vanuit het belang van ordentelijke bedrijfsvoering van telecom- en internetproviders. Immers, van deze bedrijven wordt verwacht dat zij de continuïteit van de diensten aan het publiek garanderen en hun netwerken beveiligen tegen inbraak, sabotage en spionage.

Omdat onbekende (zero day) kwetsbaarheden in software grote schade kunnen aanrichten, zoals recentelijk met de ransomware Wannacry, is het noodzakelijk dat de informatie over deze kwetsbaarheden, naast de producent, ook wordt gedeeld met vitale infrastructuren. Daarbij zijn nadere regels nodig voor de hulpmiddelen die de Nationale Politie kan gebruiken om geautomatiseerd werk binnen te dringen en onderzoek te doen, om te voorkomen dat hacks door de politie leiden tot schade bij derden. Hier hoort passend toezicht bij.[1] Een laatste probleem is dat een technisch team geen kennis heeft van complexe infrastructuren, diensten en producten van telecom- en internproviders die zij mogelijk gaan hacken, waardoor zij mogelijk (verdergaande) schade aanrichten. Ook hier is een oplossing voor nodig.

Suggesties KPN:

- Deel informatie over onbekende kwetsbaarheden bij bekendmaking ook met partijen met vitale infrastructuur zodat zij, wanneer nodig, tijdig hun infrastructuur en bedrijfsmiddelen kunnen beveiligen;
- Wanneer bij het binnendringen van geautomatiseerd werk hulpmiddelen (software) worden gebruikt, dan dienen dezen altijd voor gebruik te worden gekeurd met als doel om schade aan derden te voorkomen;
- Hulpmiddelen voor onderzoek na het binnendringen van geautomatiseerd werk moeten altijd voor gebruik worden gekeurd met als doel om schade aan derden te voorkomen;
- Hulpmiddelen voor zowel het binnendringen van geautomatiseerd werk als onderzoek moeten beiden een logregistratie bijhouden met als doel dat de toezichthouder kan controleren of gebruik van deze hulpmiddelen verantwoord heeft plaatsgevonden en of dit gebruik heeft geleid tot schade aan derden;
- Wanneer het binnendringen en onderzoek plaatsvindt in de infrastructuur, diensten of producten van telecom- of internetproviders, dan ontvangen de providers hiervan een notificatie. Het doel hiervan is dat deze bedrijven op de hoogte zijn wat er op hun bedrijfsmiddelen gebeurt en daarmee inzicht krijgen in eventuele kwetsbaarheiden.

[1] S.J. Eskens, O.L. van Daalen en N.A.N.M. van Eijk (November 2016), Geheime surveillance en opsporing Richtsnoeren voor de inrichting van wetgeving, Instituut voor Informatierecht (IViR, Universiteit van Amsterdam).

Melden van onbekende kwetsbaarheden (zero days)

Het conceptbesluit betoogt terecht dat cyberaanvallen kunnen leiden tot ernstige economische schade en ontwrichting en vernietiging van vitale infrastructuren.[2] Schade aan vitale infrastructuren kan leiden tot maatschappelijke ontwrichting.[3] Telecombedrijven worden door de overheid beschouwd als vitale infrastructuur, zowel in beleid als in lopende wetsvoorstellen.[4] Dit komt door de aard van hun infrastructuur en hun dienstverlening (communicatie). Cyberaanvallen nemen daarbij in omvang en heftigheid toe. Recent is de wereld getroffen door de *Wannacry* ransomware. In Nederland heeft deze kwaadaardige software relatief weinig schade gemaakt, echter in andere delen van de wereld was de schade aanzienlijk en leidde besmetting door Wannacry tot chaotische taferelen.

Wannacry was echter alleen mogelijk doordat de makers hiervan gebruik maakten van gestolen hacktools van de Amerikaanse inlichtingendienst NSA. Deze hacktools werkten op basis van bij de producent onbekende (zero day) kwetsbaarheden in software van Microsoft. Pas toen de NSA was bestolen van haar hacktools hebben zij Microsoft ingelicht over deze kwetsbaarheden. Deze informatie was toen echter al beschikbaar voor kwaadwillenden.[5]

Dit incident laat zien dat het niet delen van informatie over zero day kwetsbaarheden aanzienlijke riciso's met zich meebrengt. Het amendement Recourt/Tellegen heeft dit in het aanvankelijke wetsvoorstel *Computercriminaliteit III* gerepareerd en ervoor gezorgd dat informatie over onbekende kwetsbaarheden in principe met de producent moeten worden gedeeld.[6] Echter, producenten hebben tijd nodig om oplossingen te maken voor deze kwetsbaarheden. Vervolgens moeten gebruikers hun software repareren door middel van een update. Vitale infrastructuren zijn in de tussentijd mogelijk kwetsbaar, omdat zij mogelijk dezelfde software gebruiken waarin de Nationale Politie een zero day kwetsbaarheid van gebruikt om geautomatiseerd werk binnen te dringen. Zonder transparantie over zero day kwetsbaarheden blijven beveiligingslekken bestaan en zijn software en systemen kwetsbaar.

KPN dringt er daarom op aan om informatie over onbekende kwetsbaarheden ook te delen met partijen met vitale infrastructuur zodat zij, als nodig en als mogelijk, mitigerende maatregelen kunnen nemen om hun infrastructuur te beveiligen.

Het is daarbij onduidelijk hoe zero day kwetsbaarheden moeten worden bekendgemaakt wanneer de politie gebruik maakt van software om geautomatiseerd werk binnen te dringen. De relatie tussen het amendement Recourt/Tellegen en dit soort software wordt in dit geval niet gelegd in het voorliggend conceptbesluit.

Regels voor het binnendringen van geautomatiseerd werk en gebruik van technische hulpmiddelen

De bevoegdheden van de artikelen 126nba, 126uba en 126zba, zoals die worden geïntroduceerd in Computercriminaliteit III, zijn gericht op het binnendringen op

---

[2] Consultatieversie *Besluit onderzoek in een geautomatiseerd werk*, p. 8.
[3] Besluit meldplicht cybersecurity.
[4] Brief Blok vortgang eco veiligheid, besluit meldplicht cybersecurity.
[5] https://www.nrc.nl/nieuws/2017/05/14/wannacry-kwam-bij-de-nsa-vandaan-9075218-a1558565.
[6] Kamerstuk 34372-14.

geautomatiseerde werken die ‘in gebruik zijn’ bij ‘de verdachte’ of ‘een persoon’. Dat binnendringen zal vaak gebeuren via een (openbaar) elektronisch communicatienetwerk. KPN leest de bevoegdheid aldus dat die niet ziet op het binnendringen in dat netwerk zelf – dat immers niet specifiek bij de verdachte of een persoon in gebruik is – maar alleen op met dat netwerk verbonden geautomatiseerde werken. Desalniettemin kan niet worden uitgesloten dat bij de uitoefening van deze bevoegdheden ook cruciale elementen van die netwerken zijn betrokken.

Leden van een technisch team van de Landelijke Eenheid, hoe technisch bekwaam zij ook zijn, zijn niet bekend met de zeer complexe openbare elektronische communicatienetwerken van telecombedrijven. Wanneer zij worden ingezet om de geautomatiseerde werken van klanten van telecom- en internetproviders te binnen te dringen en daar hulpmiddelen in te zetten voor onderzoek, dan kunnen zij onbedoeld schade aanrichten aan processen, diensten en infrastructuur. Het conceptbesluit voorziet niet in maatregelen om dit te voorkomen. Er zijn geen nadere regels voor het binnendringen van geautomatiseerd werk, behalve dat er een plan van aanpak moet worden gemaakt en dat er verschillende technieken kunnen worden gebruikt bij het binnendringen. [7] Voor het onderzoek met technische hulpmiddelen zijn wel regels (en een keuringsdienst), maar die zijn er vooral op gericht om te zorgen voor de ordentelijke opslag van gegevens en niet om schade aan derden te voorkomen (artikelen 8 – 20). Ook de logging is alleen gericht op het onderzoek (en niet het binnendringen van geautomatiseerd werk) en hoeft alleen zaken gerelateerd aan de opslag van gegevens te loggen.

Telecombedrijven zijn *bij wet* verplicht om hackactiviteiten in hun netwerken tegen te gaan. Wanneer hier niet aan wordt voldaan dan kan de toezichthouder een boete opleggen.[8] Er zijn daarnaast verschillende onderdelen van de dienstverlening van telecomaanbieders die mogelijk direct interessant zijn voor politieonderzoek. Het gaat dan om middelen die weliswaar niet tot het openbare elektronische communicatienetwerk van de aanbieders behoren, maar wel om middelen die worden ingezet voor dienstverlening aan het publiek en die daarmee toch een breder bereik hebben dan individuele middelen van verdachten of personen (zoals eigen devices van verdachten). Cloudopslag, routers op klantlocatie die worden uitgeleverd bij breedbandverbindingen en settopboxen voor IPTV-diensten zijn hiervan enkele voorbeelden. Het is daarom noodzakelijk dat het besluit wordt voorzien van regels en toezicht om te voorkomen dat schade aan derden wordt aangericht:

- Wanneer bij het binnendringen van geautomatiseerd werk hulpmiddelen (software) worden gebruikt, dan dienen dezen altijd voor gebruik te worden gekeurd met als doel om schade aan derden te voorkomen;
- Hulpmiddelen voor onderzoek na het binnendringen van geautomatiseerd werk moeten altijd voor gebruik worden gekeurd met als doel om schade aan derden te voorkomen;
- Hulpmiddelen voor zowel het binnendringen van geautomatiseerd werk als onderzoek moeten beiden een logregistratie bijhouden met als doel dat de

[7] Consultatieversie *Besluit onderzoek in een geautomatiseerd werk*, p. 11.
[8] Dit zijn onder andere de zorgplicht in de Telecomwet, de meldplicht datalekken en de meldplicht cybersecurity.

toezichthouder kan controleren of gebruik van deze hulpmiddelen verantwoord heeft plaatsgevonden en of dit gebruik heeft geleid tot schade aan derden;
- Wanneer het binnendringen en onderzoek plaatsvindt in de infrastructuur, diensten of producten van telecom- of internetproviders, dan ontvangen de providers hiervan een notificatie. Het doel hiervan is dat deze bedrijven op de hoogte zijn wat er op hun bedrijfsmiddelen gebeurt en daarmee inzicht krijgen in eventuele kwetsbaarheiden.

Bovenstaande punten worden niet voorzien in het conceptbesluit, maar zijn wel noodzakelijk om te voorkomen dat derden en in het bijzonder telecom- en internetproviders, worden geconfronteerd door schade en/of boetes als gevolg van het binnendringen van geautomatiseerd werk en daaropvolgend onderzoek.