Allereerst wil ik bij deze uw commissie hartelijk danken voor de uitnodiging om namens AMS-IX, de Amsterdam Internet Exchange, deel te nemen aan een rondetafelgesprek over het op 24 januari jl. bij de Tweede Kamer ingediende wetsvoorstel computercriminaliteit III. Het is al weer enige tijd geleden dat het oorspronkelijke voorstel ter consultatie werd gepubliceerd, dat was in mei 2013, en het is daarom opmerkelijk dat de definitieve versie door het kabinet is aangekondigd als onderdeel van een urgent actieprogramma "Integrale aanpak jihadisme".

Zoals u wellicht weet bestaat het internet uit tienduizenden onafhankelijk van elkaar gemanagede IP-netwerken. De rol van AMS-IX is het faciliteren van interconnectiviteit tussen dergelijke netwerken. Daartoe beheren we een gedistribueerd platform in de Amsterdamse regio, welke bestaat uit volledig redundant met elkaar verbonden apparatuur in 11 verschillende datacenters. Partijen als ISP's en contentleveranciers kunnen daarop aansluiten om met elkaar verkeer uit te wisselen wanneer dat in beider belang is. Als zodanig is het AMS-IX platform een belangrijk, weliswaar enigszins verborgen, onderdeel van de technische internetinfrastructuur.

AMS-IX is een vereniging zonder winstoogmerk, en inmiddels zijn meer dan 750 netwerken aangesloten waarvan driekwart uit het buitenland afkomstig is. De laatsten komen specifiek naar Nederland om hier onderling zaken te doen, en met recht kun je dus spreken van een internationaal internetknooppunt: in termen van aangesloten partijen is AMS-IX wereldwijd zelfs de grootste in haar soort. Het is het hart van de Nederlandse digitale infrastructuur, door uw Kamer vorig jaar erkend als de 'derde mainport'. De focus van beleidsmakers op een open, neutraal, veilig en vrij internet, waarbij rechten van eindgebruikers, eerlijke concurrentie en innovatie voorop stonden, heeft mede bijgedragen aan dit succes. De economische belangen voor Nederland zijn onmiskenbaar, en het vertrouwen, zowel voor bedrijven als eindgebruikers, in de diensten die via het internet geleverd worden, is essentieel om onze internationale koppositie te behouden en ook om in de toekomst de vruchten te plukken van de kansen die de sector te bieden heeft. We zijn dan ook blij dat dit de insteek is van het Ministerie van Economische Zaken, naast het werk dat het Ministerie van Buitenlandse Zaken verricht om andere staten te overtuigen van het belang van een vrij, veilig en open internet.

AMS-IX is een neutrale, geheel onafhankelijke facilitator, en fungeert niet als spreekbuis namens de bij haar aangesloten partijen. Zoals uit het hieraan voorafgaande mag blijken, zijn de economische belangen echter zodanig groot en sector overstijgend, dat wij u ondanks onze neutrale positie graag van input voorzien. Als deelnemer in de stichting Digitale Infrastructuur Nederland (DINL) hebben we samen met een groot aantal andere betrokkenen uit de sector in mei 2015 onze zorgen geuit met betrekking tot de voornemens zoals omschreven in het indertijd ter consultatie geformuleerde voorstel. We zijn content met een aantal aanpassingen die in de laatste versie zijn terechtgekomen, zoals het enkel medewerking moeten verlenen aan een decryptiebevel bij verdenking van bepaalde zeer ernstige strafbare feiten en het strafbaarstellen van heling in computergegevens. In de kern zijn onze zorgen echter ongewijzigd.

Drie punten die ik hier wil aankaarten zijn: wat is eigenlijk de nut en noodzaak van de 'hackbevoegdheid' voor opsporing, oftewel is deze proportioneel? Hoe verhoudt de mogelijke inzet ervan zich tot andere wettelijke verplichtingen voor marktpartijen? En tot slot het essentiële punt dat het gebruik van zwakheden ten behoeve van het heimelijk binnentreden in geautomatiseerde werken het internet minder veilig maakt.

1. Overwegingen in de bij het wetsvoorstel horende Memorie van Toelichting (MvT) om de nieuwe bevoegdheid met betrekking tot het heimelijk binnendringen van een geautomatiseerd werk te motiveren, zijn vooral praktisch van aard:
   - internationale rechtshulpverzoeken zouden te traag verlopen;
   - wanneer data versleuteld is dan levert een tap niets op;

- nieuwe spelers in het veld vallen niet onder de Telecomwet en hoeven niet aan de tapplicht te voldoen;
- het gebruik van clouddiensten levert complicaties op voor opsporing;
- het uitzetten van een tap bij een openbare aanbieder is weinig effectief wanneer een verdachte (vaak) wisselt van (draadloos) netwerk.

Natuurlijk is er alom begrip, ook binnen onze sector, voor een veranderde omgeving en de uitdagingen waar opsporingsdiensten heden ten dage voor staan. Maar wat ons betreft is dit onvoldoende om de noodzakelijkheid en proportionaliteit van de nieuwe 'hackbevoegdheid' te onderbouwen. Potentiële negatieve gevolgen zijn immers verstrekkend: zowel in termen van de inbreuk op fundamentele rechten alsook als het gaat om de economische schade vanwege het schenden van vertrouwen. Het kan toch niet een kwestie zijn van: hacken in zowel binnen- als buitenland door onze opsporingsdiensten is technisch mogelijk, het werkt sneller en is relatief goedkoop, het maakt het leven voor de diensten makkelijker, en dus moeten we het kunnen en willen doen.

2. Partijen in de sector worden reeds aan een wettelijke zorgplicht onderworpen, en bestaande wet- en regelgeving wordt aangepast om tevens nieuwe spelers die buiten de traditionele wettelijke telecom-kaders vallen te reguleren. Het borgen van de veiligheid en integriteit van informatiesystemen, alsmede de daarmee samenhangende continuïteit van dienstverlening, ook vanwege vitale Nederlandse belangen, staan in deze context voorop. Tegelijkertijd zitten we nu aan tafel om de mogelijkheid te bespreken voor opsporingsdiensten om heimelijk toe te treden tot automatische werken die veelal beheerd worden door dezelfde private sector. Diensten zullen dus baat hebben bij het bestaan van kwetsbaarheden en onveiligheden, terwijl markpartijen er gelijktijdig alles aan moeten doen deze te vermijden en daarover dienen te rapporteren. Deze twee conflicterende overheidsmotieven zijn wat AMS-IX betreft niet met elkaar te rijmen.

3. Om heimelijk binnen te komen in een geautomatiseerd werk zijn per definitie zwakheden nodig. Zodra deze lekken zijn verholpen is dat binnentreden namelijk niet meer mogelijk. Wil een opsporingsambtenaar kunnen hacken in een systeem dan zijn zogenaamde 'zero-day vulnerabilities' nodig, ofwel andere kwetsbaarheden die nog niet publiek bekend zijn en nog niet door een leverancier zijn gerepareerd. Niet alleen zal men op zoek moeten gaan naar dergelijke lekken om ze te kunnen gebruiken, bijvoorbeeld door kennis daarover aan te schaffen, al dan niet via een derde. Ernstiger is dat de kwetsbaarheden voor iedereen beschikbaar zijn en blijven. Niet alleen voor onze opsporingsdiensten, maar ook voor twijfelachtige buitenlandse regimes, criminelen en organisaties die bedrijfsspionage willen plegen. En niet alleen de verdachte in kwestie, maar iedereen die gebruik maakt van betreffende (lekke) software is en blijft kwetsbaar. Bovendien kun je, wanneer Nederland het zelf ook doet, buitenlandse mogendheden er niet op aanspreken als zij, buiten hun eigen landsgrenzen, in Nederland heimelijk in geautomatiseerde werken binnentreden. Al met al wordt op deze manier een structurele bijdrage geleverd aan een onveiliger internet, en dat is wat AMS-IX betreft zeer ongewenst.

Bedrijven als Hacking Team leveren forensische tools om in te kunnen breken op systemen, en uit op wikileaks gelekte correspondentie[1] blijkt dat de Nederlandse politie daarover in contact is geweest met deze buitenlandse leverancier. Die overigens zelf recentelijk gehackt is. Als Nederland besluit tot aanschaf van dergelijke tools over te gaan, dan betekent het dat onze overheid financieel bijdraagt en indirect verantwoordelijk is voor het in standhouden van een ecosysteem dat handelt in software-kwetsbaarheden. Dit moeten we niet willen.

[1] https://wikileaks.org/hackingteam/emails/emailid/11256

Staatssecretaris Dijkhoff heeft na het AO met uw commissie op 20 januari jl. toegezegd om met een brief te komen namens het kabinet over het gebruik en het mogelijke aanschaffen van 'zero day exploits' door verschillende diensten. Ik ben zeer benieuwd waar het kabinet mee komt, en met name of dan ook verwezen gaat worden naar de eventuele aanschaf van tools bij derde partijen. In strikte zin zou met gebruik van een dergelijke tool de overheid zich namelijk niet zelf begeven op de markt voor 'zero day exploits' en andere kwetsbaarheden, maar het resultaat, ook in moreel opzicht, is natuurlijk hetzelfde: een industrie wordt in stand gehouden met als gevolg het minder snel dichten van lekken met een bijkomende onveiligheid op het internet.

U heeft ongetwijfeld kennisgenomen van het in april 2015 verschenen rapport van de WRR 'De publieke kern van het internet'. Het wachten is nog op een formele kabinetsreactie met betrekking tot deze studie, maar momenteel werkt het Ministerie van Buitenlandse Zaken aan een diplomatieke internetstrategie waarin de belangrijkste aanbevelingen van de WRR lijken te worden overgenomen. Ook stuurt men de belangrijkste auteur van het rapport alvast proactief op pad om in het buitenland de belangrijkste conclusies te promoten: namelijk dat Nederland ervoor moet pleiten dat er een zogenaamde kern van internetprotocollen en -infrastructuur is, welke te beschouwen moet worden als een publiek goed. En omdat voor Nederland het internet een grote sociaaleconomische betekenis heeft, is het van belang het functioneren en de integriteit van die publieke kern van het internet veilig te stellen en deze te beschermen tegen oneigenlijke interventies door staten en andere partijen. Een diplomatieke boodschap, aldus de WRR, die zich niet lijkt te verhouden tot de hackbevoegdheid voor opsporingsdiensten die nu voorgesteld wordt. Daar is AMS-IX het mee eens.

Ook al betreft het volgens de MvT een 'introduceren van een nieuwe bevoegdheid om, onder strikte voorwaarden, een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk te kunnen binnen dringen in het kader van de opsporing van ernstige strafbare feiten', feit blijft dat bij inzet van die bevoegdheid van zwakheden gebruikt zal moeten worden, en dat er dus een prikkel gecreëerd wordt om deze daadwerkelijk te gebruiken, ze te laten bestaan, ze niet publiek te maken, zodat ze niet worden gerepareerd. Deze houding lijkt haaks te staan op de rol die Nederland voor zichzelf ziet als aanjager van cyberdiplomatie. Als gastheer van de Global Conference on Cyber Space toonde Nederland zich vorig jaar een groot voorstander van internationale samenwerking bij de bestrijding van cybercrime. Dat is ook de lijn op dit moment van Nederland als voorzitter van de Europese Unie. Laten we vooral die lijn vasthouden en ons richten op een gezamenlijke aanpak: zowel met het bedrijfsleven, dat wil zeggen de sector, als met het buitenland. En in dat laatste geval valt er heel wat te winnen met het beter delen van informatie en het versnellen van procedures als rechtshulpverzoeken.

Bastiaan Goslings, AMS-IX regulatory officer

bastiaan.goslings@ams-ix.net