Expertmeeting parlementaire werkgroep ICT-projecten bij de overheid
Algemeen en Privacy & Veiligheid

De vijf voornaamste ICT-onderwerpen die vanuit het perspectief van de overheid de aandacht zouden dienen te krijgen - door P. Hetzscholdt, Cybercrime Specialist, 20 mei 2012

1. Onderzoek naar wetgeving en andere randvoorwaarden bij tot toegang tot, opslag van en opsporing van digitale informatie en daaraan gekoppelde handhaving en sanctionering

In Nederland speelt zich een relatief unieke situatie af, waarbij vele handhavers en academici[1] een roep doen om de modernisering of zelfs invoering van van toepassing zijnde wetgeving in relatie tot digitale opsporing van (online) criminaliteit. Uniek aangezien in vele andere landen de opsporingsdiensten gewoon hun gang zouden gaan en zich niet zouden bekommeren over het feit of dat wat ze digitaal uitspoken al dan niet bij wet geregeld is. De overheid zou deze personen niet in de kou moeten laten staan en gedegen onderzoek dienen te doen naar de legitimiteit van de betreffende handelingen en het eventueel ontbreken van relevante wetgeving of overschrijden van bestaande wetgeving. Deze kwestie is even zo relevant in het licht van grensoverschrijdende commerciële digitale diensten (voor consumenten, bedrijven en overheden) waarbij data danwel de dienstenaanbieder zich in een andere jurisdictie bevindt, met alle gevolgen van dien: de effecten van mogelijk meer stringente wetgeving in het buitenland, data die ten prooi valt aan buitenlandse inlichtingendiensten en internetgebruikers die risico lopen bij het afreizen naar de landen waar hun data is opgeslagen en daarmee doorzoekbaar is voor lokale autoriteiten.

2. Onderzoek naar generieke privacybeschermende maatregelen op technisch en beleidsniveau voor aanbieders van digitale diensten

De verdere digitalisering van onze communicatie en de samenleving als geheel zet zich onverbiddelijk voort. Er is momenteel een sterke trend waarneembaar, waarbij in alle sectoren eindgebruikers zélf bepalen welke apparaten en communicatiediensten zij gebruiken om toegang te krijgen tot bedrijfs- of overheidsinformatie[2]. Hetzelfde geldt voor het verspreiden van informatie. Dit in ogenschouw nemend, is het zaak om te komen tot minimumvoorwaarden en privacyvoorschriften voor (online) dienstenaanbieders, gericht op de bescherming van eindgebruikers en hun persoonlijke gegevens of bedrijfsgegevens waaraan iedere aanbieder – ongeacht het land van herkomst – zich zal dienen te houden indien de aanbieder diensten wil aanbieden in Nederland en aan Nederlandse eindgebruikers. Deze voorschriften dienen helder en proactief te worden gecommuniceerd en dienen tevens voorstellen voor technische vereisten te bevatten, waar noodzakelijk. Dit voorkomt een situatie waarin het een aanbieder in beginsel vrij staat te doen wat het wil met gebruikers en gebruikersinformatie en waar privacybeschermers enkel in actie komen nadat het kwaad is geschied en eventuele correcties nauwelijks mogelijk zijn. Internationale rechts- en wetsvergelijking is hierbij cruciaal.

---

[1] http://webwereld.nl/opinie/109837/digitale-irt-affaire-of-nieuwe-opsporing---opinie-.html
http://webwereld.nl/nieuws/110103/-cybercops-lappen-internationale-wetten-aan-laars-.html
http://www.cyberwarzone.com/cyberwarfare/dutch-justice-department-looks-illegal-foreign-computers

[2] http://www.zdnet.com/blog/forrester/the-four-horsemen-of-the-apocalypse-for-client-management-vendors/876
http://www.zdnet.com/blog/consumerization/consumerization-the-new-colossus/104

3. De noodzaak van een structurele verbetering van de communicatie tussen de Nederlandse overheid en de hacker community, met het oog op een betere bescherming van kritieke infrastructuren

Het is al vaker gezegd[3], maar er bestaat in relatie tot specifieke ICT onderwerpen een gapend gat tussen beleid en degenen voor wie het beleid bedoeld is; ondermeer door verschillen in cultuur, een generatiekloof en het gebrek aan kennis van zaken bij sommige politici en beleidsmakers. Hoewel het een kwestie van tijd is voordat deze situatie zich zal verbeteren, kan men dit proces versnellen door meer, beter en vooral ook op meer verantwoorde wijze gebruik te maken van kennis vanuit de hacker community, bijvoorbeeld door het organiseren van ontmoetingsdagen en faciliteren van kennisuitwisseling inzake specifieke kwesties en discussies in online fora. Ook dient de overheid duidelijker te zijn in het specificeren van gedrag en activiteiten die ze in deze context als absoluut illegaal beschouwt enerzijds en activiteiten die ze juist aanmoedigt anderzijds. Denk aan penetratietests en het melden van lekken en kwetsbaarheden in systemen en software. Onderwerp van discussie is dan wat de vormgeving zou moeten zijn van procedures die garanderen dat enerzijds hackers “hun ding kunnen doen” en anderzijds de overheid zich minder druk hoeft te maken over "hackers going rogue". Nauwere samenwerking tussen hackers en de overheid vergt ook van de hacking community een aantal zaken: meer duidelijkheid over hun sponsors is daar een onderdeel van. Het kan niet zo zijn dat hackers waarmee de overheid zich inlaat, zich ook laten financieren en sturen door andere overheden ten behoeve van inlichtingenverwerving, door bedrijven om commerciële mogelijkheden uit te diepen, of door onderwereldfiguren om de informatiepositie te verbeteren. De overheid dient dergelijke zaken te onderzoeken, te bespreken met betrokkenen en inzake alle relevante kwesties een helder en vooral NATIONAAL beleid te formuleren. Dat betekent dus ook dat wanneer dit beleid vormgegeven is en bekend is gemaakt, de overheid tegengesteld beleid van andere landen zal dienen te bekritiseren. Dat laatste maakt haar in de richting van de hacker community aanzienlijk geloofwaardiger. Wanneer de basis gelegd is, kan er gesproken worden over concrete onderwerpen zoals: a) de beveiliging van SCADA-systemen of van voor Nederland belangrijke opslagplaatsen van gevoelige en kostbare informatie, netwerkverbindingen en infrastructuur, b) de beveiliging van de financiële sector en c) de versterking van sectoren zoals defensie, politie en justitie, d.m.v. kennis en expertise uit de hacker community. Natuurlijk dient ook het gezamenlijk samenstellen van de agenda zélf een aandachtspunt te zijn. Een uiterst belangrijk onderwerp is het zogenaamde crowdsourcen[4] in relatie tot opsporing van bijvoorbeeld veiligheidsproblemen, of zelfs verdachten van allerhande criminele activiteiten (al dan niet digitaal). In gezamenlijkheid zouden relevante onderwerpen voor het crowdsourcen besproken kunnen worden. Een interessant voorbeeld vindt men hier: http://www.v3.co.uk/v3-uk/news/2161876/crowdsourcing-helps-kaspersky-crack-duqu-code. De moraal van het verhaal is derhalve dat het hacking-probleem vanuit internationaal perspectief moet worden bekeken en dat beleid inzake veiligheid en hackers wel degelijk nationaal vormgegeven kan worden. Nederland kan daarbij een voorbeeldfunctie hebben. Voorgaande staat of valt echter bij het *verdedigen* van dat beleid in de internationale context op het moment dat andere landen een andere mening hebben, deze willen opdringen of een volstrekt andere aanpak voorstaan.

---

[3] http://webwereld.nl/opinie/108396/zet-hackers-in-de-frontlinie---opinie-.html
http://www.spacedaily.com/reports/Cyber-defence_slow_due_to_generation_gap_US_official_999.html
http://www.scribd.com/cybernews4987/d/38252052-Recherche-Magazine-High-Tech-Crime-Cyber-Crime

[4] http://en.wikipedia.org/wiki/Crowdsourcing

Gebeurt dit onvoldoende, dan zal de gemeenschap zich in de kou voelen staan en wordt het tegenovergestelde effect bereikt van wat men voor ogen had.

4. De zeer dringende noodzaak tot inzicht verkrijgen in en mogelijk reguleren van het gebruik van algoritmen

Algoritmen[5] bepalen in steeds grotere mate ons leven en onze wereld[6]. Zonder algoritmen zou Facebook haar diensten niet aan 800 miljoen mensen kunnen aanbieden. Ook zouden veel diensten van Google en Apple niet mogelijk zijn. Momenteel hebben deze complexe computerberekeningen invloed op de financiële markt[7], hoe er wordt gebouwd, welke informatie u te zien krijgt (of niet) op het internet, de prijzen die u betaalt in (online) winkels, de muziek die u hoort, advertenties die u te zien krijgt, (proactieve) misdaadbestrijding en beveiliging van identiteiten, informatie en communicatiekanalen. Aldus bepalen algoritmen belangrijke processen in onze samenleving. Deze algoritmen houden echter niet per definitie rekening met wetten, rechten en vrijheden die wij als samenleving hoog achten, daar zij met name geschreven zijn voor heel specifieke, vaak commerciële, doeleinden. Aldus worden er momenteel allerhande misstanden gerapporteerd zoals prijsdiscriminatie, discriminatie en uitsluiting van gebruikersgroepen, zichtbare en niet direct zichtbare censuur en het bewust niet-duurzaam bouwen. Een van de meest belangrijke kwesties betreft conflicterende algoritmen met ernstige misstanden op de financiële markten als gevolg. Algoritmen ondergraven bewust en onbewust de normen en waarden die door overheden worden vastgesteld. Fouten worden veelal pas achteraf ontdekt en soms niet eens gecorrigeerd indien dat slechts voordeel voor een kleine groep gebruikers zou inhouden. Een enkel algoritme kan het welzijn van honderden miljoenen mensen beïnvloeden[8]. De Nederlandse overheid zou zich hiervan op de hoogte dienen te stellen om te bezien of maatregelen op technisch en beleidsniveau – voor aanbieders van diensten en faciliteerders van kritieke processen waarbij van algoritmen gebruik wordt gemaakt – noodzakelijk zijn.

5. Structurele aandacht en zorg voor de juiste mensen op de juiste plaatsen, met de juiste middelen en het juiste – vooraf en aan alle betrokkenen helder gecommuniceerde – mandaat

Terugkerende elementen bij falende ICT en cyber security-projecten zijn mijns inziens:
a) het gebrek aan ter zake kundige en geschoolde experts op ministerieel/departementaal, en dan met name leidinggevend, niveau. Soortgelijke problemen doen zich ook in het bedrijfsleven voor. Het onderwerp van salariëring is in Nederland nog steeds taboe in een wereld waarin andere overheden voor de cybersecurity- en cyberdefense-vraagstukken de beste (en soms duurste) personen inhuren;
b) het gebrek aan online portals of ‘dashboards’ met key performance indicators en voortgangsrapportages die op ieder willekeurig moment kunnen worden ingezien door betrokkenen;
c) specifiek met betrekking tot veiligheidskwesties: fragmentering van het ICT-landschap. Te veel partijen met te weinig verantwoordelijkheid en slechts expertise op deelgebieden;
d) het kennisniveau en de expertise op uitvoerend niveau zijn dikwijls uitstekend. Het ontbreekt echter aan voldoende ter zake kundige en vooral geschoolde leidinggevenden op strategisch niveau die de kennis – met het juiste mandaat in de hand – kunnen en durven toepassen.

---

[5] http://nl.wikipedia.org/wiki/Algoritme
[6] http://www.forbes.com/sites/alexknapp/2011/10/13/brian-david-johnson-intels-guide-to-the-future/
[7] http://www.youtube.com/watch?v=V43a-KxLFcg
[8] http://gizmodo.com/5824983/humanity-is-owned-by-computer-algorithms-and-resistance-is-futile