Fox-IT B.V.
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands
T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
info@fox-it.com
www.fox-it.com

IBAN NL57ABNA0554697041
KvK Haaglanden 27301624

Datum
February 02, 2018

Onderwerp
Gepsreksnotitie rondetafelgesprek cybersecurity Tweede Kamer op 7 februari 2018

Fox-IT loopt sinds 1999 mee in de voorhoede in het gevecht tegen criminaliteit, spionage en verstoring online. In de jaren sinds onze oprichting hebben we de problematiek in dit domein zien ontwikkelen van oorspronkelijk relatief onschuldig en kleinschalig tot de situatie die we nu kennen. Een situatie waarin aanvallen om financieel gewin, aanvallen met een geopolitieke achtergrond en aanvallen met als doel verstoring aan de orde van de dag zijn, ook in Nederland.

Wij, als gezamenlijke verdedigers, hebben in die jaren echt vooruitgang geboekt. We zijn technisch volwassener, beter georganiseerd en niet meer zo naïef. Toch is cybersecurity geen succesverhaal. Ons inziens zijn we wellicht gezamenlijk beter –digitaal weerbaarder- geworden, maar verbeteren we minder snel dan onze tegenstanders en zijn we daarmee feitelijk slechter af.

Op basis van ervaringen en observaties is vrijwel iedereen in ons werkveld het over bovenstaande eens, maar vreemd genoeg ontbreekt het ons ook anno 2018 nog aan goede kwantitatieve onderbouwing. Kwantitatieve onderbouwing, niet alleen voor wat betreft de omvang van de dreiging, maar zeker ook voor de mate waarin we zelf weerbaar zijn. En dit raakt aan de thema's die als een rode draad door onze gespreksnotitie lopen. Dit zijn de thema's meetbaarheid en transparantie, die wat ons betreft fundamenteel zijn voor het verder verbeteren van ons digitale weerbaarheid als burger, als bedrijf, als overheid en als maatschappij. Cybersecurity is uiteindelijk een van de belangrijke thema's in het dagelijks leven van ons allemaal, en meetbaarheid helpt ons ook om de risico's in dit domein af te zetten tegen andere risico's.

We hebben in onze notitie geprobeerd aanbevelingen te doen die zo concreet mogelijk zijn en die gebaseerd zijn op onze dagelijkse ervaringen, in aanvulling op initiatieven die al lopen. Ten slotte de opmerking dat voor alle aanbevelingen geldt dat optreden in EU-verband vaak vele malen effectiever is om beweging in de internationale markt te krijgen of om simpelweg van elkaar te leren.

Stappen die de overheid kan nemen
In vergelijking tot de rol die de overheid neemt voor veiligheid in het fysieke domein, is haar rol op dat vlak in het digitale domein bescheiden. Toch is digitale weerbaarheid van Nederland op de lange termijn van even groot belang als (bijvoorbeeld) onze financiële weerbaarheid. Beschouw digitale weerbaarheid voor de overheid en de maatschappij dan ook als even relevant als financiële gezondheid en richt analoog daar aan besturing in.

Onderneem daarvoor stappen om digitale weerbaarheid meetbaar te maken als ware het financiële gezondheid, in eerste instantie voor de (centrale en decentrale) overheden zelf. Overheid en vitale infrastructuur hebben veelal te maken met het hoogste dreigingsniveau (van kleinere criminaliteit tot aan goed uitgeruste statelijke actoren) en voor hen zal het meest strikte regime voor digitale weerbaarheid moeten gelden. Maak dit ook meetbaar. Adresseer daarbij het feit er mogelijk discrepanties op treden tussen de belangen van individuele organisaties en die van de overheid als het gaat om voldoen aan eisen voor digitale weerbaarheid binnen de vitale infrastructuur. Concreet: bij zware eisen aan private partijen in de vitale infrastructuur zal daar iets tegenover moeten staan vanuit de overheid. Tenslotte willen wij wijzen op kleinere organisaties met een zwaar dreigingslandschap die niet goed toegerust zijn om zich te verdedigen tegen statelijke actoren. Denk hierbij bijvoorbeeld aan klein innovatieve bedrijven en politieke partijen.

Diverse meldplichten (zoals die in het kader van de AVG of de Wmgc) hebben onder andere als doel om door middel van verhoogde transparantie organisaties er toe aan te sporen meer aandacht te besteden aan digitale weerbaarheid. Als gevolg van die meldplichten kan de overheid beschikken over unieke geaggregeerde informatie over de oorzaken en effecten van incidenten. Zorg dat een meldplicht altijd gepaard gaat met een verplichting van de overheid om kwalitatief hoogwaardige informatie terug te geven aan de maatschappij. Goede informatie uit meldplichten kan organisaties helpen om risico-afwegingen te maken op basis van feiten.

De problematiek met IoT-apparatuur van de afgelopen jaren heeft geleid tot hernieuwde aandacht voor de zorgplicht van fabrikanten en leveranciers en ideeën over eisen aan apparatuur of zelfs het verbieden van onveilige apparatuur en wij ondersteunen die ontwikkeling. IoT-apparatuur is vanwege de fysieke verschijningsvorm op de markt relatief eenvoudig te identificeren en aan te pakken, maar uiteindelijk gaat het om de veiligheid van software. De zienswijze op een veiliger ecosysteem van apparatuur zal dus, hoe ingewikkeld ook, in de toekomst over meer dan alleen IoT-apparatuur moeten gaan.

Stappen die het bedrijfsleven kan nemen
In onze optiek bevinden met name de kleinere bedrijven zich in een slechte positie: deels doordat de aard en omvang van de dreiging onderschat wordt, en deels om er slecht inzicht is in het eigen niveau van beveiliging. Zij zijn vaak dan ook slecht in staat om hun eigen weerbaarheid te verbeteren. Er is met name behoefte aan concreet uitvoerbaar advies. Enerzijds ligt hier mogelijk een rol voor grotere organisaties die vanuit een maatschappelijke rol hulp willen bieden, maar anderzijds is dit met name een verantwoordelijkheid van de betreffende bedrijven zelf. Bewegingen die bijdragen aan meer “ingebouwde weerbaarheid”, zoals die op het vlak van eisen aan IoT-apparatuur, zullen deze kleinere bedrijven dan ook extra helpen.

Ontplooi en/of ondersteun daarnaast activiteiten om transparantie in de markt van securitydienstverleners te bevorderen. Denk hierbij aan initiatieven die in het buitenland al bestaan, zoals de certificeringen onder

CREST voor pentesten en incident response in het Verenigd Koninkrijk. Zoals u weet is Fox-IT betrokken bij een initiatief in Nederland voor het opzetten van een brancheverenigging.

De rol van onderzoekers en ethisch hackers
Voor wat betreft ethisch hacken is het positief om te zien dat de markt voor bug bounties ook in Nederland volwassener lijkt te worden. Desondanks blijft het wat ons betreft noodzakelijk om in internationaal verband de Nederlandse visie en aanpak van responsible disclosure uit te blijven dragen.

Aangrijpingspunten voor burgers
Verwacht geen onrealistisch kennisniveau van burgers op het vlak van techniek. Wat ons betreft zit de meeste winst er in om burgers *street wise* te maken, al vanaf de leeftijd van de basisschool. Dit is de leeftijd waarop we kinderen ook bekend maken met de regels van het verkeer en hoe ze zich veilig kunnen gedragen. *Street wise* gaat niet primair over technische kennis, maar over kennis van de trucs die onze tegenstanders gebruiken en inzicht in hoe ons eigen gedrag bijdraagt aan (on)veiligheid.

Dit is kennis die preventief werkt en die voor mensen persoonlijk effect heeft, maar daarnaast ook effect heeft zodra deze mensen op de arbeidsmarkt komen en een positieve bijdrage leveren aan de digitale weerbaarheid van de organisaties waarvoor ze werken. Beginnen op de basisschool is een kwestie van lange adem. We zullen de effecten hiervan pas later merken, maar nog langer wachten kan echt ons inziens echt niet meer.