B.J.S.A.A.F. (Brenno) de Winter
brenno@dewinter.com - @brenno
0653536508

Gespreksnotitie ter voorbereiding op
De Tweede Kamer Hoorzitting
7 februari 2018

Inleiding

De vaste commissie voor Justitie en Veiligheid organiseert de hoorzitting rond vier deelvragen:

- Deelvraag 1: Welke stappen moet de overheid nemen op het gebied van wetgeving, certificering, standaarden en beleid, en voor het beveiligen van de vitale infrastructuur?
- Deelvraag 2: Welke stappen moet het bedrijfsleven nemen? Is er bij het bedrijfsleven voldoende aandacht voor cyberveiligheid en het tegengaan van bedrijfsspionage? Wat moeten bedrijven beter doen?
- Deelvraag 3: Welke rol spelen onderzoekers en (ethische) hackers bij het vergroten van de cyberveiligheid en zijn zij voldoende beschermd in hun werk?
- Deelvraag 4: Wat zijn aangrijpingspunten voor burgers om het bewustzijn van cybercrime te vergroten, om vervolgens door middel van preventie cybercrime te voorkomen?

De stand van zaken

Wij hebben als land een hoge mate van digitalisering. Veel van ons geld is niet meer contant, maar een getal in een computer, systemen als de OV-chipkaart, betalingen met een chip, mobiele telefoon of contactloos, zakelijke financiële hebben een vaste plaats in onze samenleving. 97,1 procent van de Nederlandse bevolking heeft toegang tot internet en in de leeftijdsgroepen tot 65 jaar ligt dat cijfer zelfs boven de 99 procent. Wereldwijd heeft ongeveer de helft van de mensen toegang tot internet. Meer dan 85 procent van de Nederlanders heeft een smartphone. Wij behoren – dankzij vrijheden en goede infrastructuur – ook tot de digitale voorhoede. Dat is goed nieuws in een internetwereld waar de snoeiharde regel is ‘The Winner Takes It All’.

Inmiddels begint zich duidelijk af te tekenen dat de digitalisering ook grote veranderingen in de samenleving onvermijdelijk maakt. Bijvoorbeeld met het afdwingen van fysieke veiligheid met een zelfsturende auto. Jaarlijks komen wereldwijd maar dan 1,2 miljoen mensen in het verkeer om het leven. In Europa zijn dat er zo’n 26.000. Zelfsturende auto’s kunnen die statistieken, zelfs met de huidige, gebrekkige stand van de techniek, drastisch veranderen. De politieke vraag of we zelf nog wel op de weg moeten rijden, zal zich onvermijdelijk opdringen. Voorwaarde is wel dat zo’n auto niet wordt gehackt door kwaadwillende mensen om het voertuig een mensenmassa in te sturen. Naast de botsproeven zullen we ook de software moeten toetsen.

Vertrouwen in het ecosysteem

Veilige digitalisering is een randvoorwaarde voor vertrouwen in ons bancaire systeem, onze dagelijkse processen en de vooruitgang die nog volgt. Daarbij is het niet meer zo dat we nog kunnen kijken naar enkele systemen. Wanneer een DDoS-aanval de toegang tot een bank blokkeert dan merkt de iDeal-accepterende webwinkel dat. Een digitale kraak op een medische instelling raakt de onschuldige patiënt die rekende op zorg. Een Internet of Things-apparaat is op zichzelf niet zo interessant, maar als onderdeel van een groter netwerk met groeiende bandbreedte om een volledige niet gerelateerde partij lam te leggen wel. Internet is een ecosysteem. Wanneer we spreken over de vitale infrastructuur en die aansluiten op internet dan is het onderdeel van het ecosysteem. Een kwetsbaarheid in niet-vitale infrastructuur kan de vitale infrastructuur treffen.

B.J.S.A.A.F. (Brenno) de Winter
brenno@dewinter.com - @brenno
0653536508

Gespreksnotitie ter voorbereiding op
De Tweede Kamer Hoorzitting
7 februari 2018

Bij digitale veiligheid gaat het niet alleen om de stand van de techniek in Nederland, maar om de stand van het ecosysteem. Zijn onderdelen kwetsbaar dan zijn wij per definitie kwetsbaar. Inlichtingendiensten vinden zwakheden in Microsoft Windows en delen ze niet. Dan is het een kwestie van tijd voor andere partijen die zwakheden ook vinden. We kopen dan dus inherent onveilige producten zonder dit te weten en overheden faciliteren dit. Daarbij moet wel worden erkend dat bij de inkoop de veiligheid slechts soms een thema is. Veel aanbestedingen roeren het thema niet aan en ook in het bedrijfsleven is dat mondjesmaat een thema. De mentaliteit is meer dat we dat 'later' wel regelen.

Dat geeft leveranciers niet echt een thema het beter te doen. Daarbij hebben zij zeer beperkt verantwoordelijkheden of aansprakelijkheid. Bij gebrek aan bindende normen, matige vraag en aansprakelijkheid is veiligheid minder belangrijk. Neem een leverancier van consumentenproducten. Als een apparaat maar een paar cent duurder is dan de concurrent gaat er een markt verloren. Dat zorgt voor honderdduizenden, zo niet miljoenen, Internet of Things-apparaten met kwetsbaarheden. Een walhalla voor aanvallers.

We hebben wel oplossingen onder handbereik. Zo heeft het Centrum voor Informatiebeveiliging en Privacybescherming meerdere goed doorwrochte methodieken ontwikkeld voor bijvoorbeeld veilige softwareontwikkeling in samenwerking met relevante marktpartijen en overheden. Internationaal worden deze opgepikt, maar Nederland neemt niet het voortouw dit tot bindende norm voor bijvoorbeeld de overheid te maken.

Fouten herhalen

In mijn carrière heb ik meer dan 2.000 datalekken onderzocht. De grote gemene deler is herhalen van dezelfde fouten. Er is sprake van een slechte digitale hygiëne. Als een softwareleverancier verbeteringen maakt dan blijven deze vaak liggen. Zo wordt het mogelijk om op basis van bekende zwakheden in te breken. Dat zagen we bijvoorbeeld in 2011 bij DigiNotar (liepen 16 updates van Windows achter), KPN in 2012 (bepaalde updates waren zes jaar niet gedaan), enzovoort. Het Wannacry-gijzelvirus kon goed verspreiden om dat veel Windows-systemen een cruciale update niet hadden doorgevoerd. Na deze laatste realisatie brak het 'Non Petya'-virus uit dat in een aantal varianten precies hetzelfde Windows-lek misbruikte. Opnieuw was Windows niet bijgewerkt. Het Amerikaanse Equifax moest de CEO-opofferen, omdat een hack mogelijk was als gevolg van slecht update beleid. Een paar voorbeelden van de honderdduizenden hacks met vergelijkbare kenmerken. Om dan in te breken is dan ook nauwelijks kennis nodig. Met standaard software is klikken de noodzakelijke skillset om in staat te zijn een database leeg te halen, een systeem over te nemen of spionage software te verspreiden.

Een ander voorbeeld is slechte toegangsbeheersing tot systemen. Wie zich iets verdiept weet dat al jaren dat een wachtwoord alleen onvoldoende is. Eigenlijk hoort er iets bij een code in een SMS, app om toestemming te geven, etc. Dat is niet de norm. Bij DigiD is het niet overal verplicht, in de Tweede Kamer was het tot voor kort niet verplicht. Een wachtwoord in de verkeerde handen is dan meteen een probleem. Dat ontdekte Henk Krol toen hij inbrak bij een bloedlab in Eindhoven in 2012. Maar het maakte volgens The Guardian ook de hack op Deloitte mogelijk. Wie eerlijk weet en erkent dat bepaalde wachtwoorden op veel plaatsen worden gebruikt. Dus als het wachtwoord één keer lekt dan is er breed toegang tot

veel informatie. Inmiddels weten we dat wachtwoorden massaal lekken. Soms met miljarden tegelijkertijd. En zelfs bij taxicentrale Uber bleek na een configuratiefout de broncode voor software toegankelijk met daarin een wachtwoord om alle klantgegevens op te halen. Lang verhaal kort: we zien bij herhaling dat hetzelfde type fouten wel erg vaak voorkomt. Ethische hackers tonen hetzelfde probleem dan ook bij herhaling aan bij veel instellingen.

Het herhalen van fouten is een logisch gevolg van ons eigen handelen. Op geen moment trekken we openlijk lering van incidenten. Er zijn weinig partijen die na een veiligheidsincident over de lessons learned durven te praten, omdat het niet in de cultuur zit. Zo worden rapporten over simpele incidenten worden bij lokale overheden onder de Gemeentewet geheim verklaard, terwijl buurgemeenten, andere bedrijven of instellingen met exact dezelfde software exacte dezelfde risico's lopen. Er rust een taboe op het feit dat we kwetsbaar zijn, waardoor er ruimte ontstaat voor de onderwereld om dezelfde truc bij verschillende organisaties toe te passen. In 2017 werd dat taboe goed zichtbaar toen Uber daadwerkelijk 100.000 dollar bleek te betalen om een incident stil te houden. Bij Uber ging het om persoonsgegevens, maar waarom zou dit gedrag bij zwakheden in een zelfrijdende auto niet hetzelfde zijn. Volkswagen is een duister voorbeeld dat het moeilijk is om duidelijk te krijgen dat verborgen software daadwerkelijk doet wat het moet doen.

Pre-Titanic

Er zijn nogal wat producten die we op ons ecosysteem aansluiten met veel veiligheidsrisico's. Organisaties en personen stapelen fout op fout die de kwetsbaarheden vergroten. Dat grappenmakers, oplichters, spionnen, overheden en andere partijen deze fouten misbruiken om hen moverende redenen kan daarom nauwelijks tot verbazing leiden. Daar komt ook bij dat technologie ook kan helpen de pakkans te verkleinen. En als iemand in beeld komt dan is er de vraag of jurisdictie geen probleem vormt om daadwerkelijk actie te ondernemen (zowel strafrechtelijk als civielrechtelijk). Toch de focus sterk op gericht op 'cyber crime' ofwel het verhaal *na* de digitale ramp. Ofschoon opsporing belangrijk is, zou het logisch zijn wat van die aandacht ook te geven aan het voorkomen van incidenten en het bestrijden van de gevolgen.

Hoe dat moet, is geen nieuw vraagstuk. Het denken over fysieke veiligheid is gekanteld na de ondergang van de Titanic. In aanloop naar die ramp waren honderdduizenden doden gevallen met scheepsrampen in stormen en later met stoomschepen. Er ontstond een roep om regels om de kans op incidenten te verkleinen en de overlevingskans te vergroten. Wereldwijd was die draagkracht er onvoldoende. Na de ramp kwam het SOLAS-verdrag (Safety of Life At Sea). Het kader gaf regels voor de bouw van schepen, uitrusting voor noodsituaties, infrastructuur om rampen te bestrijden, verplichte training van mensen en het onderzoeken en leren van incidenten. Digitaal is veiligheid niet heel anders. We zien de incidenten, de dreiging, maar ervaren weerstand bij het neerleggen van nieuwe, wereldwijde normen voor de digitale bouw van veiligere schepen, regels voor gebruik van deze schepen en vooral de reddingsmiddelen als het toch misgaat.

In de scheepvaart heeft Nederland een leidende rol gekozen. Begin 19de eeuw zocht het naar regels voor bijvoorbeeld de Rijnvaart. Digitaal gaat de Algemene Verordening Gegevensbescherming zo'n rol spelen. We zetten stappen op beveiligingsgebied, maar een

bredere verbetering van het ecosysteem is het niet. SOLAS gaat over basis hygiëneregels om veel ellende te voorkomen. Ook digitaal moeten we die basisregels krijgen. Daarna komen de meer geavanceerdere aanvallen pas in beeld. Waarom zou een inlichtingendienst gaan hacken op ingenieuze wijze als het heel simpel kan zonder je in de kaart te laten kijken?

Normen, goed gedrag en basale eisen zijn onvermijdelijk. We zullen de gebruiker – net als bij fysieke veiligheid – van uitleg moeten voorzien wat te doen en hoe te handelen. Dat betekent intensiever werken aan bewustwording, voorbeelden van goed gedrag tonen en mensen helpen juiste keuzes te maken. Nederland loopt voor op diverse landen op informatieveiligheidsgebied, maar is geen natuurlijk leider. We hebben de unieke positie dat ze veiligheid kunnen aangrijpen om leiderschap te tonen. Het is zaak de ICT-industrie van pre-Titanic gedrag naar post-Titanic gedrag te krijgen. Fingerend beleid kan daar een rol spelen.

- Deelvraag 1: Welke stappen moet de overheid nemen op het gebied van wetgeving, certificering, standaarden en beleid, en voor het beveiligen van de vitale infrastructuur?

Voor de digitale infrastructuur is dat onvermijdelijk voor het ecosysteem. Verstandiger is het nog om bredere normen neer te leggen. Een veiligere vitale sector is kansloos als de rest van het ecosysteem onder aanval ligt. Dat betekent ook publiek onderzoek plegen naar grotere incidenten. Dat is bij Diginotar gebeurd, maar daarna niet meer.

- Deelvraag 2: Welke stappen moet het bedrijfsleven nemen? Is er bij het bedrijfsleven voldoende aandacht voor cyberveiligheid en het tegengaan van bedrijfsspionage? Wat moeten bedrijven beter doen?

Veel basale hygiëne op orde krijgen, risico gebaseerd digitaliseren en vooral kennis uitwisselen. Veiligheid hoort in de cultuur ingebed te zijn. Er is aandacht voor de problematiek. De aandacht kan absoluut beter, maar veel belangrijker is dat op basis van leiderschap dit tot cultuur wordt verheven.

- Deelvraag 3: Welke rol spelen onderzoekers en (ethische) hackers bij het vergroten van de cyberveiligheid en zijn zij voldoende beschermd in hun werk?

Door het veel herhalen van dezelfde fouten worden onderzoekers in de positie gebracht dat zij soms organisaties wijzen op zwakheden. Sommigen hebben honderden keren lekken gemeld, sommigen zelfs duizenden keren. In de meeste gevallen zijn dat dezelfde fouten. Als zij dat doen dan zijn zij soms civielrechtelijk beschermd door het responsible disclosure beleid. Strafrechtelijk biedt dat beleid nauwelijks of zeer beperkt zekerheden. Het beleid helpt, maar nog altijd zijn er (Nederlandse) bedrijven die dwang gebruiken om geheimhouding af te dwingen (bijvoorbeeld een bank), meldingen onmogelijk maken (een Frans-Nederlandse luchtvaartcombinatie), zoeken naar redenen om te zeggen dat het geen responsible disclosure is (banken). Kortom: dit kan beter.

- Deelvraag 4: Wat zijn aangrijpingspunten voor burgers om het bewustzijn van cybercrime te vergroten, om vervolgens door middel van preventie cybercrime te voorkomen?

Basale hygiëne aanleren op basis van goede voorlichting. Dat gaat over basale zaken zoals het omgaan met wachtwoorden, inloginstellingen, bijwerken van systemen, herkennen van oplichtersmails, verstandig gedrag online, anonimisering, gebruik van antivirussoftware, het delen van gegevens, gebruik van smartphones, waar data op te slaan, hoe veilig in te kopen, enzovoort.