Rathenau Instituut

Hand-out Cybersecurity

Rondetafelgesprek Tweede Kamer 7 februari 2018

Een nooit gelopen race: cybersecurity behoeft over volle breedte meer prioriteit
Het Rathenau Instituut heeft in 2017 de studie *Een nooit gelopen race* gepubliceerd. In deze studie beschrijven we de belangrijkste ontwikkelingen in cyberdreigingen en de maatregelen die kunnen worden genomen om de weerbaarheid van de Nederlandse samenleving te versterken.

De studie laat zien dat de huidige maatregelen tegen cyberdreigingen niet volstaan. De Rijksoverheid en bedrijven met hoogwaardige technologie zijn structureel doelwit van geavanceerde cyberspionage door statelijke actoren. Daarnaast staan het MKB en de burger bloot aan de steeds professionelere methoden van cybercriminelen. De opkomst van het Internet of Things vergroot de kwetsbaarheid voor cyberaanvallen.

De diverse kwetsbaarheden staan bovendien niet los van elkaar. Zo kunnen vitale infrastructuren plat worden gelegd met grootschalige DDoS-aanvallen, waarvoor gebruik wordt gemaakt van honderdduizenden of zelfs miljoenen gehackte, aan het internet gekoppelde apparaten. Versterking van cybersecurity moet dan ook over de volle breedte meer prioriteit krijgen. Dat is eens te meer van belang omdat cyberdreigingen de komende jaren alleen maar verder zullen toenemen.

Voor deze hand-out hebben we de aanbevelingen uit onze studie aangevuld met meer recente informatie.

Basisbeveiliging behoeft meer aandacht
Voor zowel burgers, bedrijven als overheden geldt dat zij hun basisbeveiliging vaak niet op orde hebben. Met relatief eenvoudige maatregelen kan dan ook al veel worden gewonnen. Denk aan het tijdig installeren van software-updates, het gebruik van sterke wachtwoorden en het maken van back-ups van belangrijke bestanden. Verdergaande maatregelen zijn het gebruik van tweefactor-authenticatie, versleuteling van belangrijke data of het monitoren van afwijkende patronen in het internetverkeer.

Maatregelen overheid
Vanwege de snelle technologische ontwikkelingen en de steeds veranderende cyberdreigingen is het belangrijk om meer gebruik te maken van ‘open’ beveiligingsnormen, die in de praktijk verder ingevuld worden, en van nieuwe vormen van *governance*:

- Laat toezichthouders actief optreden tegen onveilige ICT-producten op basis van open beveiligingsnormen in wetgeving. Ook de Cyber Security Raad (2017a) wijst hierop.

- Zie toe op naleving van zorgplichten voor veilige ICT-producten door fabrikanten en ga na of de zorgplichten en de aansprakelijkheidswetgeving hiervoor aanpassing behoeven. Dit wordt ook genoemd door de Cyber Security Raad (2017a) en in het regeerakkoord.

- Spreek vitale sectoren sterker aan op hun verantwoordelijkheid voor een veilige bedrijfsvoering, bijvoorbeeld door afspraken te maken over een jaarlijkse hacktest. De Nederlandsche Bank heeft inmiddels besloten om testaanvallen te gaan uitvoeren op Nederlandse financiële instellingen (Computable, 2017). Het kabinet heeft laten weten de digitale weerbaarheid van vitale sectoren te verhogen door implementatie van de Europese richtlijn over Netwerk en informatiebeveiliging (NIB) (Ministerie van VenJ, 2017).

- Geef als overheid het goede voorbeeld: als grote inkoper van ICT-beveiligingsproducten en -diensten kan de overheid hogere eisen stellen aan die producten en diensten, en daarmee marktpartijen aanzetten tot meer innovatie. Dat vereist dat de overheid voldoende expertise in huis heeft en intern sterker aanstuurt op adequate beveiliging. De minister van BZK heeft inmiddels een ‘Plan van Aanpak ICT-personeel Rijk’ opgesteld, ter verhoging van de digitale expertise binnen de overheid (Ministerie van BZK, 2017).

Treed sterker op tegen statelijke actoren en cybercrime

- Cyberspionage, cybersabotage en manipulatie van informatie door statelijke actoren vormen een bedreiging voor de nationale veiligheid. De AIVD moet over voldoende capaciteit beschikken om het binnendringen van statelijke actoren in ICT-netwerken te kunnen signaleren en maatregelen te (laten) nemen. Het regeerakkoord voorziet in extra investeringen in de AIVD. Maar het moet blijken of die volstaan. In 2016 schreef de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) nog dat de dienst vanwege beperkte capaciteit slechts een deel ('het topje van de ijsberg') van de spionageaanvallen waarnam (NCSC, 2016).
- Daarnaast is bij opsporingsdiensten meer aandacht nodig, ook op regionaal niveau, voor aangifte en vervolging van cybercrime. In het regeerakkoord laat het kabinet weten te investeren in de aanpak van cybercrime.

Monitor *checks and balances* verruimde bevoegdheden diensten

Om beter op te kunnen treden tegen cyberspionage en cybercrime zijn onlangs de bevoegdheden van de opsporings- en inlichtingendiensten verruimd (Wet Computercriminaliteit III, nieuwe Wet op de inlichtingen- en veiligheidsdiensten). Dat heeft veel discussie losgemaakt. De discussie spitst zich toe op het toezicht op het gebruik dat de diensten maken van hun ruimere bevoegdheden en op waarborgen voor de rechtspositie van de burger. Het is dan ook belangrijk te monitoren of de in de wetten opgenomen *checks and balances* in de praktijk afdoende zijn. Het kabinet heeft laten weten de wetten binnen twee jaar na inwerkingtreding te evalueren (Regeerakkoord).

Maatregelen bedrijfsleven

Investeer in Digital Trust Centre

Veel bedrijven hebben hun beveiliging onvoldoende op orde. Een groot deel van de bedrijven dat het doelwit is van bedrijfsspionage, is zich daarvan niet bewust. Cybercrime en bedrijfsspionage kunnen leiden tot grote economische schade. Het niet-vitale bedrijfsleven en in het bijzonder het MKB hebben grote behoefte aan onafhankelijke expertise en advies op het gebied van cybersecurity. Een Digital Trust Centre moet in deze behoefte voorzien. Ook de Cyber Security Raad (2017b) pleit hiervoor. Het kabinet heeft inmiddels laten weten te investeren in een Digital Trust Centre voor het niet-vitale bedrijfsleven (Ministerie van EZ, 2017).

Bedrijven moeten zorgplichten naleven

Bedrijven kunnen de verantwoordelijkheid voor de beveiliging van 'slimme' apparaten niet afschuiven op de consument. Ze moeten zich op de hoogte stellen van hun zorgplichten voor veilige ICT-producten, en deze naleven. Ook de Cyber Security Raad (2017c) wijst hierop. Het kabinet heeft inmiddels een 'roadmap veilige hard- en software' aangekondigd (Ministerie van JenV, 2017).

Maatregelen experts en ethische hackers

Investeer in expertise

Vanwege de toenemende cyberdreigingen zal de vraag naar cybersecurity-specialisten de komende jaren alleen maar toenemen. Nu al is er krapte op de arbeidsmarkt. Het is dan ook van groot belang dat de overheid en het bedrijfsleven meer investeren in cybersecurity-opleidingen. Ook kan meer gebruik worden gemaakt van de expertise binnen de Nederlandse hacker community.

Maatregelen burgers

Bevorder digitale vaardigheden

In het onderwijs en in voorlichtingscampagnes moet meer aandacht worden besteed aan digitale vaardigheden. Tegelijkertijd mag hier niet te veel van worden verwacht. Veel burgers hebben nu al moeite om hun computer en smartphone adequaat te beveiligen. De beveiliging van allerlei slimme apparaten is voor de meeste van hen te veel gevraagd. Het kabinet heeft inmiddels aangegeven in het onderwijs en in voorlichtingscampagnes aandacht te besteden aan een veilig gebruik van internet (Regeerakkoord).

Relevante publicaties Rathenau Instituut

Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid (2017), https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race

Extra maatregelen nodig tegen cyberdreigingen – Bericht aan het Parlement (2017), https://www.rathenau.nl/nl/publicatie/extra-maatregelen-nodig-tegen-cyberdreigingen

Literatuur

Computable (2017), ‘DNB hackt banken met cyberinitiatief Tiber’, 14 november 2017.

Cyber Security Raad (2017a), *Naar een veilig verbonden digitale samenleving*.

Cyber Security Raad (2017b), *Naar een landelijk dekkend stelsel van informatieknooppunten*.

Cyber Security Raad (2017c), *Ieder bedrijf heeft digitale zorgplichten*.

Ministerie van BZK (2017), ‘Plan van Aanpak ICT-personeel Rijk’, 18 december 2017.

Ministerie van EZ (2017), ‘Oprichting van een Digital Trust Centre’, 23 september 2017.

Ministerie van JenV (2017), ‘Antwoorden Kamervragen over de artikelen aangaande de onveiligheid van Internet of Things (IoT) in Nederland’, 24 november 2017.

Ministerie van VenJ (2017), ‘Reactie inzake cyberaanval met ransomware en voortgang moties uit Wannacry-debat’, 20 september 2017.

NCSC (2016), *Cybersecuritybeeld Nederland CSBN 2016*.

Regeerakkoord (2017), *Vertrouwen in de toekomst: Regeerakkoord 2017 – 2021*.