Kernboodschap adviesrapport Nederland digitaal droge voeten

Nederland loopt voorop in de digitale wereld en is één van de meest ICT-intensieve economieën van Europa. De digitale economie groeit harder dan alle andere sectoren. We beschikken over een kwalitatief goede infrastructuur. Denk aan de AMS-IX, het grootste internetknooppunt ter wereld, en onze razendsnelle, breedbandige telecomnetwerken. Daardoor is Nederland een aantrekkelijk vestigingsland voor ICT-bedrijven en multinationals. E-commerce genereert nieuwe economische activiteiten en werkgelegenheid. Slimme digitale toepassingen dragen bij aan innovatie en vooruitgang in tal van sectoren. De digitale economie vormt inmiddels een derde mainport, naast Schiphol en de Rotterdamse haven. Een mainport die bovendien het snelst groeit.

Digitalisering biedt enorme kansen voor de samenleving en economie van de 21e eeuw, maar dan is het wel zaak te zorgen dat de digitale wereld veilig en vertrouwd blijft. Of het nu gaat om innovatie, bestrijding van criminaliteit, het beschermen van bedrijfsgevoelige informatie, privacy of onze nationale veiligheid: cybersecurity is een basisvoorwaarde voor een welvarende en veilige samenleving. Feit is dat de cyberdreigingen fors toe nemen, dat blijkt onder andere uit het Nationaal Cyber Security Beeld Nederland. Criminaliteit, (bedrijfs)spionage en terrorisme vormen online net zo'n bedreiging als 'op straat'.
Wanneer onze digitale infrastructuur bedreigd wordt dan kan dit leiden tot maatschappelijke ontwrichting. De digitale infrastructuur is voor 80% in handen van de private sector, dus de overheid kan het niet alleen. Maar het bedrijfsleven kan het ook niet alleen, Nederlandse veiligheidsdiensten spelen een cruciale rol. Er is maar één manier om de cybersecurity op orde te brengen: samenwerken. Het is dringend noodzakelijk om de cybersecurity in Nederland te versterken.

We vinden het allemaal vanzelfsprekend dat er regels, stoplichten en rotondes zijn om het verkeer veilig te houden. En dat bedrijven betrouwbare, veilige apparaten en voedsel en drinkwater leveren aan consumenten. De veiligheid van de digitale wereld moet net zo belangrijk worden als de veiligheid van de fysieke wereld om ons heen. De burger moet veilig en vertrouwd kunnen blijven leven in een digitale wereld, het bedrijfsleven moet goed zaken kunnen doen en de overheid zorgt voor de randvoorwaarden om dat mogelijk te maken. Op alle drie de fronten is werk aan de winkel.
Op verzoek van de Cyber Security Raad (CSR) heb ik in oktober 2016 het rapport ´De economische en maatschappelijke noodzaak van meer cyber security, Nederland digitaal droge voeten´ uitgebracht. De adviezen in deze gespreksnotitie heb ik in dat rapport ook opgenomen. Gezien het aantal cyberincidenten en de toegenomen dreiging sinds oktober 2016, zijn mijn adviezen ook in 2018 helaas nog onverminderd van kracht.
De € 95 miljoen die het Kabinet heeft vrijgemaakt voor cybersecurity is een eerste stap in de goede richting.Cybersecurity vraagt om structurele aandacht van regering, politici, beleidsmakers, bestuurders, toezichthouders, bedrijven en burgers.

1. Welke stappen moet de overheid nemen?

Om de cybersecurity te versterken en de digitale weerbaarheid te vergroten is een meerjarig actieprogramma inclusief investeringsagenda noodzakelijk. Dit programma zou door het kabinet in samenwerking met het bedrijfsleven en decentrale overheden opgesteld
moeten worden. Voor de uitvoering van dit actieprogramma zou een hoge publieke functionaris moeten worden benoemd, die onder directe verantwoordelijkheid van het kabinet opereert.

In het actieprogramma moet een aantal concrete zaken worden geadresseerd:

- De overheid moet het goede voorbeeld geven door veiligheid en privacy bescherming een speerpunt te maken in de eigen digitale bedrijfsvoering, voor zowel de rijksoverheid, alsook voor lagere overheden.
- De bevoegdheden van de Nederlandse opsporings-, Inlichtingen- en Veiligheidsdiensten moeten worden gemoderniseerd. Zorg dat hun mogelijkheden in de pas lopen met de ernstig toenemende mate van de complexiteit en omvang van cyberdreigingen. Ik ben dus blij dat de WIV en de Wet Computer Criminaliteit III, inclusief de checks & balances daarbij, door de Eerste en Tweede Kamer zijn goedgekeurd.
- De overheid heeft een rol in het stimuleren en zo nodig afdwingen van de eigen verantwoordelijkheid bij de private sector: zorg dat zij zaken op orde hebben en voldoen aan randvoorwaarden voor cybersecurity.
- Invulling moet worden gegeven aan de wettelijke zorgplicht van ICT-producten en -diensten. Zoals dat geldt voor ieder ander product. Cyberdreigingen ontstaan omdat er onveilige producten en diensten op de markt beschikbaar komen, vanwege gebrek aan eisen en de druk van 'time to market'. De overheid heeft een sturende rol om dit marktfalen te verhelpen.
- Ook het introduceren van een accreditatie- of certificeringssystematiek verhoogt de veiligheid van ICT-producten en – diensten en doet de dreiging daarmee afnemen.
- Introduceer en stimuleer als overheid de zogenaamde 'ketenverantwoordelijkheid' tussen bedrijven onderling, waarvan een deel 'vitale aanbieders' betreft (zie onderstaand 2 een nadere toelichting).
- Zorg ervoor dat regelgeving sneller kan worden aangepast aan de razendsnelle ontwikkelingen binnen het digitale domein. Kortom, maak regelgeving meer flexibel.

Zowel de overheid als bedrijfsleven moeten ongeveer 10% van het jaarlijkse ICT budget te besteden aan specifieke cybersecurity maatregelen.

2. Welke stappen moet het bedrijfsleven nemen?

Niet alleen de overheid is aan zet, maar elk bedrijf of organisatie heeft primair zelf een verantwoordelijkheid. Wanneer bedrijven niet investeren in hun cybersecurity brengt dat op den duur hun bedrijfsprocessen en daarmee de eigen concurrentiepositie ontegenzeggelijk in gevaar. Security als randvoorwaarde of *license to operate* in het productieproces moet een vanzelfsprekend onderdeel van de *corporate governance code* zijn.
Het installeren van beveiligingssoftware, encryptie van de eigen informatie, tijdig installeren van software-updates zijn basismaatregelen die iedere ondernemer zelf moet kunnen nemen. Het is belangrijk dat bedrijven hun eigen netwerken beschermen en zich weerbaar maken tegen cyberaanvallen.

In de private sector zijn grote ondernemingen veelal voldoende cyber aware en wordt cyber security binnen deze bedrijven al gezien als een randvoorwaarde voor het voortbestaan van de onderneming. Dat geldt in veel mindere mate voor de kleine(re) ondernemingen. Vanwege de toenemende connectiviteit en ketenafhankelijkheid zorgt dat voor een risico in de gehele keten. Daarom moet in nauwe samenspraak tussen overheid en privaat nadere invulling worden gegeven aan ketenverantwoordelijkheid. Bijvoorbeeld kan een grote onderneming, met veel kennis en expertise in huis, de kleine onderneming in de keten helpt om meer secure te worden, bijvoorbeeld door kennis beschikbaar te stellen ('groot helpt klein'). Dat is niet alleen een advies dat ik geef, maar zelf, in mijn rol van CEO van Post NL, ook actief bezig.
De zwakste schakel in de digitalisering is de factor 'mens'. Daarom is het noodzakelijk dat elke onderneming zijn eigen mensen weerbaar en bewust maakt van cyberrisico's. Door herhaaldelijk hierover te communiceren en het personeel te trainen op cyberveilig gedrag.

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

Onderwijs en (wetenschappelijk) onderzoek zijn cruciaal: om de eigen kennispositie van Nederland te bewaken, Nederland is immers een kenniseconomie. Er is een dreigend te kort aan cyber security experts waar we tijdig en doeltreffend op in moeten spelen. We moeten ervoor waken dat we in de toekomst afhankelijk zijn van experts en kennis uit landen om ons heen. Dat zou ons in potentie kwetsbaar maken. Ik geloof ook in het inzetten van white hat hackers, die bij uitstek van buiten naar binnen kijken op digitale beveiliging. Dat doe ik ook binnen mijn eigen onderneming en dat levert waardevolle informatie op. Uiteraard horen daar heldere kaders bij die de belangen van beide partijen goed behartigen.

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

Mijn belangrijkste boodschap op dit punt is: Maak Nederland digitaal vaardig! Op het moment dat de Nederlandse burger digitaal vaardiger is, begrijpt hij hoe digitalisering ons leven beïnvloedt. Dan is het logisch om te beseffen dat dat naast talloze kansen ook nieuwe bedreigingen met zich meebrengt. En dan snapt iedereen dat je maatregelen kunt of moet nemen die je beschermen tegen die dreigingen. Dat begint vanaf de jongste leeftijd wat mij betreft. Digitale vaardigheden zijn inmiddels net zo belangrijk als lezen, schrijven en rekenen. Digitale geletterdheid en cyber security, moeten versneld worden opgenomen als basisonderdeel in het onderwijscurriculum in de gehele keten van basis- tot beroepsonderwijs. Om de weg op te mogen, moet men beschikken over een rijbewijs, om de digitale weg op te gaan, is ‘cyberwijs’ net zo noodzakelijk.

De inzet van doelgerichte voorlichtingscampagnes over cybersecurity voor specifieke doelgroepen (waaronder mkb-bedrijven) en het brede publiek is nodig om de groepen te bereiken die niet (meer) via onderwijs leren over digitalisering en cyber veiligheid.