The Hague **Security Delta**

HSD Narrative:
Nationaal ‘Cyber Plan’ Investeringsprogramma

April 2016

The Hague **Security Delta**

info@thehaguesecuritydelta.com | thehaguesecuritydelta.com | @HSD_NL

Inleiding

Digitale veiligheid en veiligheid door digitale oplossingen. Dat is de kern van het toekomstig veiligheidsbeleid. Er zal geïnvesteerd moeten worden om gewenste maatschappelijke ontwikkelingen te bevorderen, maar ook om dreigende maatschappelijke ontwrichting te voorkomen. Dat gebeurt nog veel te weinig. De ontwikkelingen gaan razend snel. Daarom is urgent politieke aandacht nodig.

Naast territoriale veiligheid (Defensie), sociale veiligheid (Politie, Brandweer) en fysieke veiligheid (deltaplannen) is digitale veiligheid het onderwerp van de toekomst. Het komt niet vanzelf goed. De dreigingen in de reële wereld doen zich ook voor in de digitale wereld. Hoe eerder wij daar maatregelen nemen des te aantrekkelijker is Nederland voor vestiging van bedrijven en instellingen. Ook zorgen we er zo voor dat mensen vertrouwen houden in de overheid op het gebied van veiligheid.

De aanpak moet publiek-privaat, kan het beste in een netwerkstructuur en zal innovatief moeten zijn. De overheid is daarbij een belangrijke aanjager. Zij zal zeker op het terrein van (digitale) veiligheid in innovaties moeten investeren en gaan optreden als eerste afnemer. Deze publiek-private aanpak zal wel onder regie moeten gebeuren (NCTV) en met de benodigde middelen voor ontwikkeling en toepassing (nationaal cyberfonds). Als dat niet gebeurt zal Nederland de opgebouwde voorsprong als vestigingsplaats (economisch belang) kunnen verliezen en kan al snel maatschappelijke ontwrichting ontstaan. Investeren aan de voorkant is het advies en het mes snijdt aan meerdere kanten: digitale toepassingen veilig maken en houden, digitale netwerken en vitale infrastructuur duurzaam beter beveiligen, economische groei bevorderen en vertrouwen opbouwen.

Afhankelijkheid ICT

De Nederlandse maatschappij en economie krijgt steeds meer een digitaal karakter en is daardoor steeds afhankelijker van ICT. We gebruiken internet niet alleen meer om online nieuws te bekijken en te shoppen, ook onze bankzaken regelen we online en de verwarming thuis staat steeds vaker via onze mobiel in verbinding met het internet. Daarbij rijden we mogelijk over niet al te lange tijd ook in zelfrijdende auto's en ontvangen we pakketjes via onbemande drones.

Niet alleen onze huizen en apparaten zijn via allerlei sensoren aan internet verbonden. Dit geldt bijvoorbeeld ook voor onze leefomgeving waar stoplichten met elkaar verbonden zijn in zogenaamde slimme steden en hele industriële automatiseringssystemen van onze vitale infrastructuur op het gebied van onder andere water, energie, telecom en gezondheidszorg. Deze ontwikkeling biedt veel nieuwe mogelijkheden en economische kansen, maar brengt ook risico's met zich mee. Zeker omdat het gaat om de meest cruciale delen van onze maatschappij. Er rest ons daarom geen enkele keuze: de digitale veiligheid van onze vitale infrastructuren moet worden opgevoerd. En daar zal dus meer geld in gestoken moeten worden.

Economisch perspectief

De cijfers vanuit economische perspectief liegen er niet om: een kwart van de Nederlandse economische groei van de afgelopen 10 jaar wordt binnen de ICT-sector gerealiseerd. Dat is zo'n 22 miljard euro. De economische potentie die de digitaliseringstrend met zich meebrengt zit echter niet alleen in de IT-sector, ook de veiligheidssector lift hierop mee. Denk hierbij aan smart security, waarbij ICT wordt gebruikt voor het creëren van veiligheidsoplossingen door bijvoorbeeld de inzet van big data voor stedelijke veiligheidsvraagstukken. Of aan het beveiligen van ICT gedreven oplossingen die gemonitord kunnen worden in security operation centres.

Dit alles zie je terug in de cijfers van het onlangs gepubliceerde 'Policy Research Rapport', dat de economische potentie van de veiligheidssector in kaart bracht. Zo gaat er in deze sector een omzet van 6,6 miljard euro om, werken er een kleine 60.000 mensen en zijn 3.600 bedrijven actief. De IT security trend blijkt ook uit dit rapport: de omzet- en banengroei zit met name in cyber security en digital forensics met de afgelopen twee jaar meer dan 10% omzetgroei.

De trends van digitalisering, internet of things en 3D printing als onderdeel van de zogenaamde vierde industriële revolutie hebben echter ook een keerzijde. Diverse rapporten tonen aan dat het zorgt voor verlies van banen. Wil Nederland dit compenseren dan is een veilig internet en inspelen op de trends cruciaal.

Unieke digitale infrastructuur

We beschikken over een unieke digitale infrastructuur die hiervoor de basis legt. Zo is Nederland door de aanwezigheid van AMS-IX, NL-IX en vele datacenters het 'global centre' voor dataverkeer. We zijn dan ook de

grootste internet hub van Europa, die de meeste directe verbindingen met de VS vanuit Europa heeft. Daarbij loopt ons land voorop qua gebruik van digitale services en hebben we de hoogste bandbreedte snelheid per internetgebruiker in Europa. Door deze goede digitale voorzieningen kan Nederland ook goed mee in nieuwe trends van robotisering, internet of things en globalisering.

Vestigingsklimaat

Nederland is - onder andere vanwege deze digitale infrastructuur - aantrekkelijk voor internationale bedrijven en organisaties. Van de 2000 Forbes organisaties actief in de ICT, heeft 65% een kantoor in Nederland. Neem daarin vervolgens mee dat internationale bedrijven meer in R&D investeren dan Nederlandse bedrijven en we hebben een prachtig potentieel in handen. Echter, op de 'Doing Business Index' van de wereldbank scoort Nederland slechts een 28e positie. Streven van Nederland zou moeten zijn: een top 10 notering in deze index. Willen we onze unieke digitale infrastructuur volledig benutten voor het economische vestigingsklimaat van Nederland dan is het streven om in 2020 het veiligste internet ter wereld te hebben.

Nationaal Cyber Plan

Als we de vlieger vanuit maatschappelijk en economische perspectief op willen laten gaan, dan moeten we borgen dat onze digitale infrastructuur neutraal en veilig is. Het is daarom belangrijk een nationale digitale veiligheidsaanpak te ontwikkelen, net zoals het Deltaplan voor de fysieke vitale infrastructuur. En omdat er niet één organisatie in z'n eentje verantwoordelijk is voor de digitale beveiliging van Nederland, dient dit zowel dwars door het huis van Thorbecke als publiek- privaat georganiseerd te worden. Een aanpak die alleen werkt als er ook een meerjarig nationaal investeringsprogramma aan toegevoegd wordt. Bij elkaar gebracht in een 'Nationaal Cyber Plan'.

Nationaal Cyber Testbed

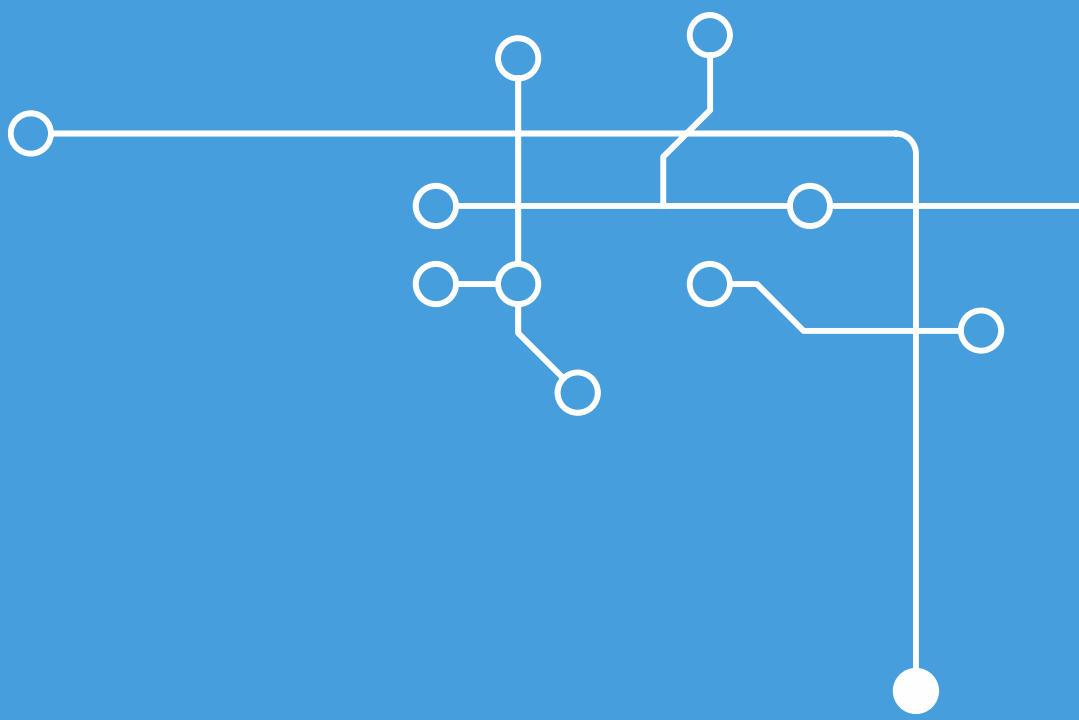
Binnen het nationale veiligheidscluster 'The Hague Security Delta' wordt hier al op voorgesorteerd. Bedrijven, kennisinstellingen en overheden werken er samen aan innovatieve oplossingen op gebied van onder andere IT security. Zo wordt momenteel gewerkt aan het opzetten van een 'Nationaal Cyber Testbed' voor de vitale infrastructuur. Het eerste cyber test- en ontwikkelingscentrum in Europa waar bijvoorbeeld datacenters, telecompartijen en energieleveranciers in een beschermde omgeving de digitale veiligheid van hun systemen kunnen testen en innovatieve veiligheidsoplossingen kunnen toetsen. Daarnaast biedt het testbed ruimte voor onderzoek door wetenschappers en onderwijs van cyber security talenten. Het opzetten van een dergelijk testbed vereist een nauwe samenwerking tussen de vitale infrastructuur sectoren én een investering van miljoenen, maar is een must om de economische potentie van onze IT en cyber security sector uit te kunnen nutten en onze kennis internationaal te vermarkten. De overheid dient dan ook op terreinen als telecom, energie en water regie te voeren en op te treden als inkoper van de geteste innovaties.

Toegankelijk innovatiebeleid

In het nationale innovatiebeleid is een terugkeer naar thema specifiek aanpak in plaats van algemeen topsectorenbeleid en algemene fiscale innovatievoorzieningen gewenst. Dit geldt in het bijzonder voor die sectoren, zoals (digitale)veiligheid, waarvoor de overheid een belangrijke afnemer en innovatie stimulator is en waarvan de verdere ontwikkeling een belangrijke maatschappelijke en economische behoefte dient. Deze aanpak sluit ook beter aan bij de aanpak van het Europese innovatieprogramma Horizon2020 en het Duitse innovatiebeleid. Echter, dit vereist een lange termijn innovatiesubsidie instrument, het inzichtelijk maken van de vraag- en investeringsagenda van de overheid en het effectiever maken van het 'Inkoop Innovatie Urgent'. Hierbij zal het percentage van het totale volume aan inkoop van de overheid van 2,5 procent naar 5 procent verhoogd moeten worden.

Tenslotte

Kortom, naarmate de digitalisering van onze samenleving steeds verder gaat, is digitale beveiliging het enige antwoord om met deze nieuwe wereld om te gaan. Daarom moeten we inzetten op een combinatie van het economisch benutten van de mogelijkheden en anderzijds het afdekken van de risico's. Een 'Nationaal Cyber Plan', inclusief investeringsprogramma is hiervoor een vereiste. Zo leggen we een essentiële basis onder het Nederlandse vestigingsklimaat en positioneert Nederland zich met recht als 'secure digital gateway to Europe'.



The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
070 204 51 80

info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL