FME POWERED BY DUTCH TECHNOLOGY

POSITION PAPER CYBERSECURITY

Cybersecurity zowel een kans als een kwetsbaarheid

De technologische industrie is als hoogproductieve exporterende sector de drijvende kracht van de Nederlandse economie. De snelle integratie van ICT in de productie maakt het mogelijk internationaal concurrerend te opereren en nieuwe banen in Nederland te creëren. Digitalisering van de technologische industrie verdient topprioriteit. Om de kansen die digitalisering biedt blijvend te kunnen blijven benutten, is het noodzakelijk dat we ons veilig in de digitale wereld kunnen bewegen.

We leven in een steeds sneller veranderende wereld. Een van de meest ingrijpende veranderingen in onze maatschappij is de exponentiële ontwikkeling van digitale technologie en Smart Industry. Deze revolutie biedt veel kansen om doeltreffender en doelmatiger te werken, maar levert tegelijkertijd niet te veronachtzamen risico's voor het ongestoord functioneren van de maatschappij, bedrijven en de nationale veiligheid.

Om de kansen die dit digitale tijdperk biedt en als technologische sector voorop te blijven lopen en digitale dreigingen als digitale spionage en cybercriminaliteit het hoofd te bieden, moeten de krachten gebundeld worden.

Onze hoogtechnologische industrie is aantrekkelijk voor economische spionage door buitenlandse bedrijven en andere landen. Cyberspionage gaat direct ten koste van het Nederlandse verdienmodel. Dat gebeurt niet alleen bij grote bedrijven. Ook MKI'ers en start-ups, die innovatieve ideeën ontwikkelen, zijn regelmatig doelwit van cybercriminelen en statelijke actoren die intellectuele eigendommen willen stelen. Dit is des te schadelijker als we ons realiseren dat ons bedrijfsleven en onze export zeer kennisintensief zijn, waarvan de technologische industrie de aanjager is met 57 miljard aan exportomzet.

Het economisch belang en de veiligheidsnoodzaak rechtvaardigen en vragen om een eenduidige politieke sturing inzake de digitaliseringsagenda van de Nederlandse overheid. Daarom roept FME het volgende kabinet op om hiervoor een ministerieel Topteam voor Digitalisering in te stellen met daarbinnen ook nadrukkelijke aandacht voor cybersecurity. Hiervoor zou een functionaris moeten worden benoemd die een meerjarig cybersecurity-actieprogramma opstelt in publiek-private samenwerking. Het actieprogramma brengt ambities, bevoegdheden en middelen samen om de cybersecurity in Nederland structureel te verbeteren en de economische kansen die cybersecurity biedt te versterken.

Ministerieel Topteam voor Digitalisering

In het ministeriële Topteam voor Digitalisering ziet FME voor onderstaande ministeries de volgende uitdagingen om vorm te kunnen geven aan een meerjarig cybersecurity-actieprogramma:

Ministerie van Economische Zaken

Missie: Het ministerie van Economische Zaken staat voor een duurzaam, ondernemend Nederland. EZ zet zich in voor een uitstekend ondernemersklimaat en een sterke internationale concurrentie-positie.

Het verdienmodel van Nederland staat onder druk door cybercriminaliteit en (economische) spionage. De internationale concurrentiepositie zal onder druk komen te staan wanneer de kansen die cybersecurity biedt, niet optimaal worden benut. Daarom vraagt FME:

- ✓ Meer sturing en regie op het beleid waarin de kansen van digitalisering - met daarbij de essentiële randvoorwaarden van cybersecurity - worden gewaarborgd.
- ✓ Meer aandacht voor de digitale bescherming en versterking van technologische industrie en aanpalende sectoren.
- ✓ Regie, sturing en coherent beleid, vanuit de strategische positie die EZ inneemt, in de kansen van digitalisering en als hoeder van de digitale infrastructuur.
- ✓ Meer specifiek vraagt FME aandacht voor de kwetsbaarheid van electriciteitsnetwerken die door digitalisering steeds smarter worden (Smart Grids).

Ministerie van Veiligheid en Justitie

Missie: Het ministerie van Veiligheid en Justitie zorgt voor de rechtsstaat in Nederland, zodat mensen in vrijheid kunnen samenleven, ongeacht hun levensstijl of opvattingen.

Het Nationaal Cyber Security Centrum, als onderdeel binnen het ministerie van Veiligheid en Justitie, heeft zich de laatste jaren ontwikkeld tot hét expertisecentrum op cybersecurity vraagstukken. Het NCSC is opgericht om primair de Rijksoverheid en de vitale sectoren te adviseren. FME vindt deze beleidsopvatting te nauw omdat zowel de veiligheid van digitale systemen, als het economische verdienmodel onder druk staan door cybercriminaliteit en (economische) spionage. FME roept daarom op om ook:

- ✓ De technologische industrie en aanpalende sectoren te bedienen van concrete adviezen die de digitale weerbaarheid vergroten en daarmee het verdienmodel van Nederland te beschermen.

Ministerie van Defensie

Missie: Defensie beschermt wat ons dierbaar is. Militairen verdedigen Nederland, de (economische) belangen en bevriende landen.

Omdat cybercriminaliteit en (economische) spionage door statelijke actoren de maatschappij ontwrichten, is FME zeer content met de ingezette samenwerking tussen het Cyber Commando en de technologische industrie op het terrein van kennis-uitwisseling in de brede zin van het woord. FME ziet kansen om:

- ✓ Met Defensie het gesprek aan te gaan over de eventuele mogelijkheden om het beschermde netwerk van Defensie in te zetten ten behoeve van de bescherming van de technologische industrie en aanpalende sectoren.

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (AIVD)

Missie: Het ministerie van BZK borgt de kernwaarden van de democratie.

De AIVD heeft in haar jaarverslag 2015 onderkend dat niet alleen de dreiging van digitale aanvallen tegen elektronische netwerken in ons land groot is, maar ook dat het aantal aanvallen zal toenemen. Ook staat in het jaarverslag dat buitenlandse inlichtingenofficieren, onder meer uit China, belangstelling tonen voor de Nederlandse technologische sector en aanpalende sectoren. Daarom roept FME op om:

- ✓ Zorg te dragen voor betere kennisdeling van de AIVD met de (hoog)technologische industrie en aanpalende sectoren om het verdienmodel in Nederland in stand te houden.

Ministerie van Onderwijs, Cultuur en Wetenschap

Missie: Het ministerie van OCW werkt aan een slim, vaardig en creatief Nederland. OCW wil dat iedereen goed onderwijs volgt en zich voorbereidt op zelf-standigheid en verantwoordelijkheid.

Nederland heeft een vooraanstaande positie op het terrein van digitalisering en behoort tot de top 10 van meest concurrerende kenniseconomieën in de wereld. Wil ons land deze positie blijven behouden, dan moeten we zorgen voor een open, veilige en economisch kansrijke digitale samenleving. De digitale toekomst van Nederland moet veilig worden gesteld, daarom roept FME het ministerie op om vanuit hun rol te zorgen voor:

- ✓ Het opleiden van ICT-technologen met kennis van cybersecurity. Om te beschikken over voldoende cybersecurityprofessionals zijn ook flexibele onderwijsprogramma's noodzakelijk voor werkenden.
- ✓ De Nederlandse jeugd in het basis en middelbare onderwijs voor te bereiden op de digitale toekomst. Leren coderen wordt een kerndoel op alle scholen.

Ministerie van Buitenlandse Zaken

Missie: Het ministerie van Buitenlandse Zaken behartigt de internationale betrekkingen, vanuit Den Haag en via een netwerk van ruim 150 posten over de hele wereld.

Het ministerie van Buitenlandse zaken en in het bijzonder de Nederlandse ambassades en consulaten hebben een belangrijke taak daar waar het economische diplomatie betreft. Omdat Nederland zichzelf als een 'safe place to do business' presenteert en omdat cybersecurity niet stopt bij landsgrenzen roept FME het ministerie op om cyberdiplomatie te bevorderen zodat:

- ✓ Het Nederlandse vestigingsklimaat wordt verstevigd;
- ✓ Nederlandse bedrijven veilig zaken kunnen blijven doen in het buitenland.

Overige beleidsterreinen

Naast de rol en uitdagingen die we zien voor bovenstaande ministeries is het ook goed om op diverse beleidsterreinen het belang van cybersecurity te onderstrepen.
Twee voorbeelden brengen we daarbij graag onder de aandacht:

Ministerie van Infrastructuur en Milieu

FME ondersteunt de proeftuin-ambitie van het ministerie van Infrastructuur en Milieu voor onder meer zelfrijdende auto's. FME vraagt daarbij aandacht voor de randvoorwaardelijke risico's zoals cybersecurity.

Ministerie van Volksgezondheid, Wetenschap en Sport

De zorgsector wordt steeds smarter onder andere door de inzet van medische technologie. Door deze inzet wordt de zorg ook beter, betaalbaarder en bemensbaar. FME vraagt daarbij aandacht voor de randvoorwaardelijke risico's zoals cybersecurity.

De overheid heeft een cruciale rol in de digitale wereld, zoals hierboven ook blijkt. Coördinatie en sturing is noodzakelijk vanwege de versnippering over een groot aantal ministeries. Daarom pleit FME voor een ministerieel Topteam Digitalisering met hierin ook aandacht voor cybersecurity. De uitdagingen waar Nederland voor staat en de kansen die Smart Industry bieden, vragen hierom.

Meer informatie

www.fme.nl/cybersecurity

Of neem contact op met:

- Liesbeth Holterman
  Beleidsadviseur
  E liesbeth.holterman@fme.nl
- Tara Kolk
  Adviseur Public Affairs
  E tara.kolk@fme.nl