Tweede Kamer der Staten-Generaal
Vaste commissie voor Justitie en Veiligheid
Postbus 20018
2500 EA DEN HAAG

Woerden, 1 februari 2018

Per mail: cie.jv@tweedekamer.nl

Betreft : inbreng rondetafelgesprek cybersecurity
Kenmerk : LdB/RC/MH

Geachte leden van de commissie Justitie en Veiligheid,

Allereerst hartelijk dank voor de uitnodiging voor dit rondetafelgesprek over cybersecurity. De centrale vraag die u ons heeft gesteld, legt wat ons betreft de vinger op de zere plek. U vraagt welke concrete stappen er gezet moeten worden om de cyberveiligheid van mensen, bedrijven en overheden te vergroten.

Laat ik in reactie daarop beginnen met het goede nieuws. Er zijn genoeg concrete stappen te zetten. De techniek om weerbaarheid van mensen, bedrijven en overheden online te vergroten is alom aanwezig. Leden van Nederland ICT, ruim 570 leveranciers van hardware, software en ICT-diensten en vele cybersecurityspecialisten werken hier dagelijks met veel passie aan.

Is ICT dan altijd veilig? Nee helaas niet. Hard- en software zullen altijd kwetsbaarheden bevatten en ook het juiste gebruik of de inzet van de beschikbare technieken blijft helaas nog te vaak achter. Als gekeken wordt naar de recente cyberveiligheid-issues is het grootste gedeelte ervan te herleiden tot het niet implementeren van beschikbare beveiligingsmaat-regelen (zoals updates van besturingssystemen, installatie van patches en versleutelde verbindingen bij e-commerce) en onwetendheid bij de gebruikers. Het kan dus een stuk veiliger! Het niet daadwerkelijk toepassen van redelijk simpele en vooral ook nu beschikbare maatregelen is helaas nog aan de orde van de dag. Is het dan allemaal de schuld van de gebruiker? Zeker niet, we zullen komende jaren nog beter samen moeten werken om van digitalisering een succes te maken.

Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
info@nederlandict.nl
www.nederlandict.nl

NL 53 ING B 0662590546
KvK 30174840

NEDERLAND ICT

Nederland ICT pleit dan ook voor meer focus op actie en op het nemen van verantwoordelijkheid als het gaat om cybersecurity. De techniek is er klaar voor, nu de samenleving nog. U heeft vooraf een viertal vragen gesteld die ik hieronder zal beantwoorden:

1) Welke stappen kan de overheid zetten?

Geef richting aan de markt. En niet voor niets leg ik hier de nadruk op de markt. In een zich zo snel ontwikkelende wereld als ICT, zowel hard- als software, is het cruciaal dat de markt werkt aan innovaties binnen een set aan spelregels zoals die door overheid en politiek worden bepaald. De Algemene Verordening Gegevensbescherming (AVG) is een goed voorbeeld hoe er op Europees niveau een beweging ten gunste van privacy en security wordt ingezet. Natuurlijk zijn er kanttekeningen te plaatsen bij de AVG, maar door het stellen van duidelijke Europese(!) kaders zijn de spelregels bepaald. De ICT-markt is een wereldwijde markt en digitale grenzen zijn relatief. Specifieke nationale eisen, gesteld aan software en hardware zijn niet alleen onwenselijk, maar passen ook niet bij de digitale werkelijkheid.

Ook vraag ik de overheid namens de sector veel vaker in de beleidsvoorbereiding en bij de totstandkoming van wetgeving in contact te treden met de sector. Terugkijkend op wetgevingstrajecten als de WIV, CCIII en de AVG constateer ik dat het beter was geweest als er al in een veel eerder stadium intensiever contact was geweest over de meer technische en operationele implicaties van dergelijke wetgeving. Duidelijkheid en werkbaarheid zijn cruciaal voor de effectiviteit. Brancheorganisatie Nederland ICT organiseert dit contact tussen overheid en bedrijfsleven graag.

2) Wat kunt u verwachten van bedrijven?

U kunt een proactieve houding verwachten van het ICT-bedrijfsleven als het gaat om privacy en security. Het is daarbij van belang voor bedrijven om inzicht te hebben in welke maatregelen voor cyberveiligheid van toepassing zijn voor welke situatie. Certificering en standaarden spelen daarbij een belangrijke rol. Bijvoorbeeld als het gaat om het maken van veilige software en hardware en het leveren van diensten. Ik wil daarbij nogmaals benadrukken dat de ICT-markt bij uitstek een sterk internationale markt is. Regulering die eisen stelt aan het ontwerp of de functionaliteit van producten kan van grote toegevoegde waarde zijn, mits deze het liefst globaal, maar tenminste op Europees niveau hetzelfde en geharmoniseerd is. Geef bedrijven de ruimte zoveel mogelijk aan te sluiten bij al bestaande internationale criteria als het gaat om standaardisatie of certificering (ISO, ISAE, NIST, etc.).U mag tevens verwachten dat ICT-bedrijven het gesprek met u en de overheid aangaan.

Ook als het gaat om ingewikkelde dossiers waar de belangen op het eerste gezicht ver uit elkaar lijken te liggen. Bedrijven, in elk geval de bedrijven die zich bij Nederland ICT hebben aangesloten, zijn zich terdege bewust van de belangrijke rol die zij vervullen in de economie en maatschappij. Ik noem hier twee voorbeelden om dat te illustreren. Nederland ICT heeft recent samen met haar leden de Data Pro Code ontwikkeld. Middels deze code leggen leden van Nederland ICT, vaak verwerkers van data, vast dat zij de privacy en veiligheid van de data van hun klanten waarborgen. We hopen dat de Autoriteit Persoonsgegevens zo snel mogelijk tijd heeft om deze code goed te keuren. Een ander initiatief waar we momenteel aan werken is een samenwerking tussen cybersecuritybedrijven, ICT-afnemers, verzekeraars en de politie. We kijken gezamenlijk of we tot een systematiek kunnen komen, ontwikkeld door het CCV (Centrum voor Criminaliteitsbestrijding en Veiligheid) waarbij bedrijven op een laagdrempelige manier het cyberrisico dat ze lopen, kunnen inschatten en vervolgens inzicht krijgen in de cybersecuritymaatregelen die ze daarvoor kunnen nemen.

3) Wat kunt u verwachten van de wetenschap/hackers?

Het belang van de wetenschap en (ethische) hackers is evident. Het is van groot belang dat er ook op fundamentele wijze onderzoek wordt gedaan naar mogelijkheden om de weerbaarheid van Nederland verder te vergroten. Nederland ICT heeft het pleidooi van enkele hoogleraren om het wetenschappelijk kennisniveau op het gebied van cybersecurity op peil te houden dan ook onderschreven. In een steeds meer digitaal wordende wereld is het van cruciaal belang dat Nederland zich kan blijven meten met andere landen als het gaat om kennis over bijvoorbeeld cryptografie en quantumcomputing. Nederland ICT werkt dan ook samen met DCYPHER (NWO) als het gaat om het samenbrengen van cybersecuritybedrijven en wetenschappers. Ook ethische hackers spelen een cruciale rol als het gaat om het aandragen van kwetsbaarheden in systemen en netwerken. Het is wel van groot belang dat dit op een veilige en vertrouwelijke wijze gebeurt en dat bedrijven een redelijke termijn krijgen om ontdekte kwetsbaarheden te herstellen. Al in 2013 hebben Nederland ICT en de aangesloten Telecombedrijven in goede samenwerking met het NCSC gewerkt aan een gedragscode om de procedures voor Responsible Disclosure verantwoord in te richten. Om het belang van ethische hackers te onderstrepen, heeft Nederland ICT het goede werk van de GDI foundation twee jaar geleden nog beloond met een prijs.

4) Wat verwachten we van de burgers?

We zijn ons er van bewust dat de technologische ontwikkelingen razendsnel gaan. Zo snel dat het voor vele burgers lastig is om bij te blijven. Nederlanders zullen zich steeds meer bewust moeten worden van het belang van goede cyber hygiëne. Gebruik goede wachtwoorden, maak gebruik van de functie om je systemen automatisch van updates te voorzien, informeer je goed over de apparaten die je koopt. Het is aan de ICT-sector burgers hierbij te ondersteunen door het leveren van duidelijke informatie over de veiligheid en privacy van hun producten en diensten. Nederland ICT zal het belang daarvan bij haar leden onder de aandacht blijven brengen. Overigens kan de overheid hier ook een rol spelen net als zij nu al doet als het gaat om de fysieke veiligheid. De spotjes tegen woninginbraak zijn al jaren op de buis. Iets dergelijks voor consumenten, zzp-ers en MKB-ers zou erg nuttig zijn. De sector ondersteunt de overheid graag als het gaat om het uitdragen van een campagneboodschap, net als we dat ook hebben gedaan bij campagnes tegen straatroof van mobiele telefoons[1] en verkeersveiligheid[2].

Tot slot nog enkele hartenkreten namens onze achterban.

- Onderwijs: investeer in de cyberprofessionals van de toekomst. Zowel als het gaat om instroom van talent als ook het stimuleren van leven lang leren.
- Helderheid: kies als overheid een richting en houd daar aan vast. Voorkom versnippering in initiatieven. Beter enkele krachtige en vooral ook concrete actielijnen in een nationale cybersecuritystrategie dan een routekaart met heel veel sporen en weinig eigenaarschap.
- Strategie voor de toekomst: we weten dat quantumcomputing grote gevolgen zal hebben voor cybersecurity, met name op het gebied van encryptie. Hier is een nationale strategie voor nodig.

Met vriendelijke groet,
Nederland ICT

Lotte de Bruijn
Directeur

---

[1] https://www.maakhetzenietemakkelijk.nl/boefproof

[2] http://www.verkeersveiligheidscoalitie.nl/