Tweede Kamer der Staten-Generaal
t.a.v. de leden van de vaste commissie voor Economische Zaken & Klimaat
Postbus 20018
2500 EA 'S-GRAVENHAGE

DATUM 30 maart 2022
KENMERK 2022/AA/cv/008
ONDERWERP Online veiligheid en cybersecurity

Geachte leden van de vaste commissie voor Digitale Zaken,

Op donderdag 7 april spreekt u met elkaar over online veiligheid en cybersecurity. Op de agenda staan veilige hard- en software, benodigde investeringen in cybersecurity en het Digital Trust Center (DTC). Deze onderwerpen zijn even relevant als urgent. Onderzoek van IBM toont aan dat de technologische industrie in 2021 voor het eerst meer werd aangevallen dan enige andere sector. De onderzoekers rapporteerde bovendien een toename van het aantal gerapporteerde kwetsbaarheden in industriele controlesystemen (ICS) met 50 procent.[1] Dit maakt cybercriminaliteit het belangrijkste risico voor de bedrijfscontinuïteit en een veroorzaker van grote economische en maatschappelijke schade.

Extra aandacht voor en investeringen in cybersecurity zijn daarom bittere noodzaak. De ambities van het nieuwe kabinet op het gebied van cyberweerbaarheid zijn terecht hoger dan ooit. We moeten echter constateren dat de verdeling van gereserveerde middelen niet in evenwicht is. Er wordt te weinig gedaan aan de bescherming en ondersteuning van (kleine) ondernemers tegen digitale dreigingen. Om die reden vraagt FME voor uw voorbereiding aandacht voor de volgende punten:

- Creëer een **integrale aanpak van cyberweerbaarheid**.
- Investeer meer in de slagkracht van het **Digital Trust Center**
- Investeer in de verspreiding van kennis over de beveiliging van **Operationele Technologie (OT)**
- Betrek de technologische industrie bij de totstandkoming van Europese regelgeving voor de veiligheid van ICT-producten zoals geformuleerd in de ***Cyber Resilience Act (CRA)***

Over FME

FME is de ondernemersorganisatie voor de technologische industrie. Onze 2.200 leden zijn technostarters, handelsbedrijven, middelgrote en kleine industrie (MKI) en grote industrie/multinationals die actief zijn in de sectoren metaal, elektronica, elektrotechniek en kunststof. Er werken bij onze leden 220.000 medewerkers. De gezamenlijke omzet van de FME-leden bedraagt € 108 miljard en zij exporteren voor € 51 miljard. Daarmee realiseren de FME-leden een zesde van wat Nederland in totaal met export verdient.

[1] IBM Security X-Force Threat Intelligence Index 2022

Integrale aanpak van cyberweerbaarheid

De technologische industrie ambieert het snelst lerende, meest flexibele en beste digitaal verbonden productienetwerk van Europa tot stand te brengen in 2025. Digitale incidenten hebben de potentie maatschappelijke ontwrichting en grote economische schade te veroorzaken. Denk aan de nevenschade die ontstond door de ransomware-aanval op *Colonial Pipeline* of in de Rotterdamse haven vanwege NotPetya. Ransomware vormt een dusdanig groot probleem dat de economische veiligheid in gevaar brengt. De aangekondigde Nederlandse Cybersecuritystrategie (NLCS) komt dan ook geen moment te laat.

De Cyber Security Raad concludeerde dat voor de integrale aanpak van cyberweerbaarheid een investering van € 833 miljoen nodig is.[2] Met deze investering kan tevens concrete invulling gegeven worden aan het verstevigen van de (digitale) strategische autonomie. De huidige aanzet voor de aanpak van cyberweerbaarheid is ontoereikend. Met de gereserveerde financiële middelen (300 mln.) kan de overheid slechts een gedeelte van de nodige ambitie realiseren met haar aangekondigde NCS. Om tot een evenwichtige verdeling van de gereserveerde middelen te komen moet er meer geïnvesteerd worden in de weerbaarheid van het bedrijfsleven. Het Digital Trust Center en haar capaciteit moet worden uitgebreid, meer dan nu gepland is. Daarnaast moet er geïnvesteerd worden in de verspreiding van kennis over de beveiliging van industriële processen.

- *FME pleit daarom voor de creatie van een Integrale aanpak van cyberweerbaarheid.*

Digital Trust Center

Het kabinet concentreert haar inzet op de bescherming van de vitale (digitale) infrastructuur en haar processen. Hierdoor wordt onvoldoende geanticipeerd op de kwetsbaarheid van de niet-vitale technologische industrie, die voor een groot deel uit kleine en middelgrote bedrijven bestaat. Kleinere bedrijven nemen minder vaak cybersecuritymaatregelen.[3] In de technologische industrie zijn kleine ondernemingen vaak onderdeel van leverancierskeetens die verbonden zijn met genoemde vitale processen. De kwetsbaarheid van het niet-vitale bedrijfsleven doet afbreuk aan de cyberweerbaarheid van de vitale sector.

Ondernemers kunnen meer investeren in cyberweerbaarheid. Tegelijkertijd stellen we vast dat het borgen van digitale veiligheid een maatschappelijke opgave is waar de Rijksoverheid stelselverantwoordelijkheid voor draagt. De huidige ambitie van de minister van Economische Zaken en Klimaat genereert onvoldoende impact. Het DTC deelt informatie en stimuleert de samenwerking tussen en binnen sectoren maar op een te kleine schaal.

- *FME pleit daarom, overeenkomstig met het adviesrapport van de Cyber Security Raad Integrale aanpak cyberweerbaarheid, voor:*
  - *Structurele investeringen à € 8 miljoen extra per jaar in de verbetering van informatiedelingscapaciteit en ondersteuning van het MKB door het DTC.*
  - *Structurele investeringen à € 12 miljoen extra per jaar in weerbaarheidsadviezen voor organisaties binnen en buiten de vitale infrastructuur.*

[2] CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid'
[3] ING-thema update Industry 2022

Operationele Technologie

De technologische industrie zet vol in op digitalisering. Hierdoor krijgen verschillende productiestappen een digitale koppeling. Voorheen werden productieprocessen enkel aangestuurd door operationele technologie (OT) of industriële controlesystemen (ICS). De voor hackers toegankelijke IT-systemen raken door digitalisering steeds meer vervlochten met deze productieprocessen. Om die reden wordt de beveiliging van OT-systemen steeds belangrijker.

De complexiteit van productieprocessen en de benodigde machines maakt dat het updaten (*patchen)* van OT-systemen niet altijd mogelijk is zonder apparatuur te vervangen. Dit maakt het *patchen* van kwetsbaarheden in OT-systemen zeer kostbaar in financieel economische zin. In algemene zin geldt dat het *patchen* van OT-systemen lastiger is dan voor IT-systemen. Overeenkomstig met het adviesrapport van de Cyber Security Raad *Integrale aanpak cyberweerbaarheid* wil FME aandacht vestigen op het gebrek aan handelingsperspectief voor beheerders van OT-systemen.

- *FME pleit daarom, overeenkomstig met het adviesrapport van de Cyber Security Raad Integrale aanpak cyberweerbaarheid, voor de ondersteuning van de beheerders van OT-systemen met de inrichting van een (virtueel) steunpunt OT dat is aangesloten op het Landelijk Dekkend Stelsel van informatieknooppunten. Doelstelling daarbij is begeleiding van inkoopprocessen en het verzamelen/delen van meldingen over kwetsbaarheden van leveranciers en beheerders.*

Cyber Resilience Act

Met het werkprogramma voor 2022 neemt de Europese Commissie het initiatief om de cybersecurity van producten te reguleren. Een snelgroeiend aantal producten heeft een IT-component. IT legt de basis voor belangrijke innovatieve ontwikkelingen die onze toekomst vormgeven. Denk hierbij aan *smart Industry, smart mobility* of *smart farming.* De aangekondigde verordening heeft daarom veel impact op de gemeenschappelijke markt en haar concurrentievermogen.

- *FME vraagt de Tweede Kamer er bij de minister op aan te dringen de volgende zaken in te brengen bij de werkgroepen van de Europese Commissie:*
  - *De CRA moet rechtszekerheid scheppen ten aanzien van bestaande productregelgeving.*
  - *Vereisten moeten neutraal geformuleerd worden, zodat toekomstige innovatie niet belemmerd wordt.*
  - *Europese normalisatie-instellingen kunnen het best de vereiste technische details beschrijven.*
  - *DE CRA moet de verantwoordelijkheid van de fabrikant duidelijk identificeren door er evenwichtige grenzen aan te stellen.*
  - *De CRA moet de verantwoordelijkheid van de fabrikant voor producten na het op de markt brengen duidelijk omschrijven.*
  - *De lidstaten moeten investeren in effectief want competent toezicht.*

Tot slot vragen wij uw aandacht voor specifieke uitdagingen op gebied van Russische software. Ondernemers uit de technologische industrie wegen de continuïteit, integriteit en vertrouwelijkheid van softwareleveranciers voortdurend af. Zij zijn daarbij niet goed geholpen door de Nederlandse overheid wanneer deze inconsistente boodschappen publiceert over hetzelfde onderwerp. Vitale sectoren en de Rijksoverheid wordt geadviseerd geen gebruik te maken van Kaspersky antivirussoftware.

Dit advies geldt niet voor lagere overheden en de rest van het Nederlandse bedrijfsleven. Hierin wijkt het standpunt van het NCSC af van andere Europese overheden als Duitsland, Italië en Frankrijk. Dit beleid is slecht uitlegbaar en roept veel vragen op bij ondernemers uit de technologische industrie. Hierop hebben bedrijven meer houvast en duidelijkheid nodig.

FME is uiteraard graag bereid om het bovenstaande schriftelijk of mondeling nader toe te lichten. Daarvoor kunt u contact opnemen met Adriaan Andringa, Public Affairs adviseur (adriaan.andringa@fme.nl of 06-281 652 59).

Met vriendelijke groet,

Geert Huizinga
Directeur belangenbehartiging FME