

Inbreng verslag van een schriftelijk overleg

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen en opmerkingen voorgelegd over de initiatiefnota van het lid Verhoeven over «Het Internet der Dingen: maak apparaten veilig!» (Kamerstuk 34 613, nr. 2).

De voorzitter van de commissie,
Ypma

Adjunct-griffier van de commissie,
Verstraten

Inhoudsopgave

1.	Inleiding	2
2.	Het internet der dingen	2
3.	Risico's	3
4.	Oplossingen	3
5.	Financiële paragraaf	5

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de initiatiefnota van het lid Verhoeven (hierna: initiatiefnemer) over «Het Internet der Dingen: maak apparaten veilig!» (hierna: de initiatiefnota). De snelle ontwikkelingen op het gebied van digitalisering en de vele kansen en mogelijkheden die het Internet der Dingen biedt, vormt een kant van de medaille. De andere kant van de medaille betreft de uitdaging die er ligt- net als in de fysieke wereld – na te denken over de risico's en de veiligheidsaspecten in die digitale wereld en het veilig gebruik van apparaten in relatie tot het Internet der Dingen. Deze initiatiefnota is daar een aanzet toe. Voornoemde leden onderschrijven de noodzaak hiervan. Bovendien houdt onveiligheid van apparaten die aangesloten zijn op het internet en die vaak veel persoonlijke gegevens opslaan, verdere ontwikkeling en innovatie tegen. In de initiatiefnota wordt een zestal voorstellen gedaan. Deze leden hebben hierover een aantal vragen.

De leden van de PvdA-fractie hebben kennisgenomen van de initiatiefnota met betrekking tot voorstellen die moeten leiden tot een veiliger aanbod en gebruik van apparaten die op internet zijn aangesloten. Zij zijn het met de initiatiefnemer eens dat het tijd wordt om op een aantal vragen die rond het Internet der Dingen hangen antwoord te geven. Het gaat immers om het gebruik van, zoals de initiatiefnemer aangeeft, persoonlijke en intieme data die worden verzameld en geanalyseerd via apparaten, veelal in huis.

De leden van de SP-fractie hebben met belangstelling kennisgenomen van de initiatiefnota over de beveiliging van Internet der Dingen-apparaten. De initiatiefnemer doet hiertoe een aantal aanbevelingen, waarover de aan het woord zijnde leden nog enkele vragen hebben. Allereerst zijn zij benieuwd naar de ervaring in de Verenigde Staten met het daar ingestelde bedreigingsanalyseteam. Kan de initiatiefnemer daar meer over vertellen? Aan welk team van experts denkt hij als een dergelijk analyseteam in Nederland wordt opgericht? Wat wordt de rol van het Nationaal Cyber Security Centrum (NCSC) in het geheel?

De leden van de CDA-fractie hebben kennisgenomen van de initiatiefnota. Zij delen weliswaar niet direct alle daarin voorgestelde oplossingen maar wel de geschetste probleemanalyse omtrent apparaten die met het internet verbonden zijn. Ook deze leden achten het van groot belang niet naïef te zijn rondom de toepassingen van big data en invloed via apparatuur op onze levenswijze en de noodzaak om voor adequate consumentenbescherming te zorgen. Zij hebben nog enkele vragen aan de initiatiefnemer.

2. Het internet der dingen

De leden van de PvdA-fractie lezen dat de initiatiefnemer een aantal voorstellen doet om interactieve informatie-uitwisseling tussen apparaten die verbonden zijn met internet veilig te laten verlopen. Deze leden

hebben al aandacht gevraagd voor het beschermen van de privacy van burgers middels een voorstel voor een nieuwe datawet. In hoeverre gaan de voorstellen in de initiatiefnota verder dan de voorgestelde datawet? Zijn er nieuwe elementen? Is er overlap? Zo ja, waar?

3. Risico's

De leden van de CDA-fractie missen een reflectie op de primaire verantwoordelijkheid van de gebruiker zelf om de geschetste risico's te voorkomen. Los van de toepassing van apparatuur in bijvoorbeeld ziekenhuizen gaat het deze leden hierbij voornamelijk om apparatuur in en rondom het huis en voor persoonlijk gebruik. Deelt de initiatiefnemer de mening dat ondanks het gegeven dat internet niet meer is weg te denken uit onze samenleving, de verantwoordelijkheid voor een verantwoord gebruik wel primair bij de gebruiker ligt? Zo merkt de initiatiefnemer op dat toestemming om bepaalde informatie te delen soms diep in de gebruikersvoorwaarden zit verstopt. Dat is zo, maar deelt de initiatiefnemer de mening dat de gebruiker desalniettemin de keuze kan maken zich hierin te verdiepen en anders te beslissen over het gebruik van apparaten?

Daarnaast vragen deze leden of de initiatiefnemer de mening deelt dat in de tweede plaats de verantwoordelijkheid ligt bij de industrie en bedrijven om de betreffende apparaten veilig op de markt te brengen. Zij komen daar verder nog op terug bij de bespreking van de voorgestelde oplossingen, die vooral zien op de rol van de overheid.

Voornoemde leden vragen of de initiatiefnemer zijn stellingname kan onderbouwen dat winkels en gemeenten, bijvoorbeeld via het wifi-netwerk, proberen gegevens te verzamelen van consumenten. Op welke schaal komt dit voor? Kan de initiatiefnemer hier voorbeelden van noemen? Vindt hij dat deze handelwijze te ver gaat, ondanks de aantoonbare voordelen die het voor de betreffende ondernemer kan hebben? Zou hiervoor toestemming verleend moeten worden door de consument/burger bij het binnengaan van kantoren en gemeenten? Zo ja, op welke wijze? Hoe ziet de initiatiefnemer dat voor zich in de praktijk? Hoe denkt de initiatiefnemer over de mogelijk eenvoudige oplossing consumenten erop te attenderen hun wifi uit te zetten als zij niet het risico willen lopen dat informatie over hen wordt verzameld? Zou dit volstaan volgens de initiatiefnemer om het geschetste probleem op te lossen?

4. Oplossingen

4.1 Nederlands bedreigingsanalyseteam

De leden van de VVD-fractie vragen waar het bedreigingsanalyseteam onder moet vallen en wie dit team zal aansturen. Aan wie zou dit team moeten rapporteren?

De leden van de CDA-fractie steunen de initiatiefnemer in zijn voorstel dat de overheid over een adequate informatiepositie moet beschikken om potentiële gevaren en uitdagingen te signaleren en kritieke infrastructuur in Nederland te beschermen. Maar in hoeverre is daarvoor een aparte extra overheidsinstantie nodig zoals wordt voorgesteld? Waarom volstaat hier niet het huidige of (zoals voorgesteld) eventueel uit te breiden NCSC? Voornoemde leden vragen ook wie de kosten zouden moeten dragen voor het instellen van een dergelijk team en ook of hierin ambtenaren aan het werk moeten worden gezet die deze werkzaamheden gaan verrichten. Zou het niet beter zijn als (toonaangevende) ICT-instellingen en bedrijven in Nederland de krachten bundelen om technici bij elkaar te brengen om in de wens van de initiatiefnemer te voorzien? Wat zouden de voordelen hiervan zijn, gelet op de noodzaak van betrokkenheid van bedrijven zelf bij

de bewustwording van cybercrime? Zou de overheid hier geen voortrekkersrol maar louter een faciliterende taak in moeten hebben? Graag vernemen deze leden hierop de reactie van de initiatiefnemer. Ook vragen deze leden in hoeverre dit punt overlap vertoont en verbinding kan worden gezocht met het voorstel onder hoofdstuk 6.3 (Innovatievraag veilige Internet der Dingen-apparaten), om via een research programma startups te vragen mee te denken over cybersecurityvraagstukken.

4.2 Keurmerk en standaarden voor cyberveiligheid van apparaten

De leden van de VVD-fractie vragen of de initiatiefnemer meer kan zeggen over het voorstel om een Nederlands keurmerk te ontwikkelen. Wie of welke instantie gaat dit doen? Wie gaat de waakhond van dit keurmerk zijn? Aan welke standaarden zou dit keurmerk moeten voldoen en hoe kijken bedrijven die dit soort apparaten produceren hier tegenaan? Hoe en door wie zou het voorstel tot een EU-register moeten worden genomen? Hoe groot wordt de kans ingeschat dat het tot zo'n register gaat komen?

De leden van de SP-fractie vragen de initiatiefnemer waarom Nederland zou moeten wachten op in Europees verband vastgestelde standaarden voor cyberveiligheid van apparaten, voordat zij overgaat tot het oprichten van een keurmerk. Welke instantie zal dan het toezicht houden op naleving van het keurmerk en eventuele overtredingen van de standaarden handhaven?

De leden van de CDA-fractie vragen de initiatiefnemer naar de bestaande wet- en regelgeving, zowel nationaal, Europeesrechtelijk als internationaal ten aanzien van de veiligheid van apparaten. De initiatiefnemer doet het nu voorkomen alsof in het geheel geen geldende wet- en regelgeving omtrent de productie en het gebruik van (tal van apparaten) bestaat waarin veiligheid genormeerd is. Kan de initiatiefnemer hier wat uitgebreider op ingaan en ook aangeven ten aanzien van welke apparaten specifiek wet- en regelgeving zou ontbreken?

4.3 Innovatievraag veilige Internet der Dingen-apparaten

De leden van de VVD-fractie vragen hoe de innovatievraag zou kunnen luiden.

4.4 Software aansprakelijkheid

De leden van de VVD-fractie zijn benieuwd welke vorm van aansprakelijkheid de initiatiefnemer zelf voor ogen heeft op het gebied van software-aansprakelijkheid. Deze leden vragen of de initiatiefnemer kan aangeven wanneer (in welke situatie) een software ontwikkelaar aansprakelijk zou moeten zijn. Wat is de verhouding tot het voorgestelde keurmerk voor cyberveiligheid?

De leden van de CDA-fractie hebben eenzelfde vraag als bij hoofdstuk 4.2 ten aanzien van de aansprakelijkheid van software. Kan ook hier een overzicht worden gegeven van de bestaande wet- en regelgeving, zowel nationaal, Europeesrechtelijk als internationaal?

4.5 Zelfredzaamheid gebruikers

De leden van de VVD-fractie zijn benieuwd hoe de initiatiefnemer de verantwoordelijkheid van de zelfredzaamheid nu precies ziet. Is de uitvoering van de vier voorstellen de volledige verantwoordelijkheid van

de overheid? Waar begint en houdt deze op en welke verantwoordelijkheid heeft de gebruiker zelf? Hoe ziet de initiatiefnemer dit?

De leden van de PvdA-fractie zijn van mening dat met name de gebruikers een cruciale rol spelen in het slagen van een veiliger Internet der Dingen. Is de initiatiefnemer het met deze leden eens? Is keuzevrijheid van consumenten nog houdbaar als het gaat om het delen van data met derden? Wanneer en waar moet de overheid wat de initiatiefnemer betreft een grens trekken als het gaat om data-uitwisseling? Voornoemde leden willen de initiatiefnemer erop wijzen dat niet elke internetgebruiker voldoende zelfredzaam te maken is op internet als het gaat om het veilig maken van hun data. Hoe gaat de initiatiefnemer deze groep minder vaardige gebruikers ondersteunen? Inloggen met Facebook moet volgens de aan het woord zijnde leden aan banden worden gelegd, gezien ook de omgang van Facebook met privacy en het niet transparante gebruik van privégegevens. Hoe gaat de initiatiefnemer hier in zijn voorstellen mee om?

Ook het Internet of Toys moet in het vizier komen als het gaat om (regels voor) het Internet der Dingen, zo menen de aan het woord zijnde leden. Zij hebben aandacht gevraagd voor het beter informeren van ouders over de veiligheid van speelgoed. Kan de initiatiefnemer hierop reageren?

De aan het woord zijnde zijn voorts van mening dat kwetsbare internetgebruikers, en daarmee gebruikers van Internet der Dingen-apparaten, bijzondere aandacht nodig hebben. Iedereen moet privacy-voorwaarden kunnen begrijpen en niet automatisch op akkoord klikken. Kan de initiatiefnemer dit beamen? Welke (extra) consequentie heeft dit vervolgens voor de aanbieder/producent van apparaten die via internet gegevens uitwisselen? Is de initiatiefnemer het ermee eens dat het niet de vraag is of de aanbieders van aan internet gekoppelde apparaten verantwoordelijk moeten worden gemaakt voor de maatschappelijke consequenties van hun product of dienst, maar hoe? En dat, bij aantoonbare schade voor de gebruiker, de producent altijd een zorgplicht heeft? Kan de initiatiefnemer in dit verband reageren op de uitzending van Zembla van 30 november 2016, getiteld «Hacken voor Dummies» waarin de aansprakelijkheid van leveranciers (van software) aan de orde komt? Onderzoek doen mag wat deze leden betreft geen vertragende factor zijn. Denkt de initiatiefnemer dat (het regelen van) softwareaansprakelijkheid hoogste prioriteit moet hebben?

4.6 Een onafhankelijk, sterk en actief NCSC

De leden van de VVD-fractie vragen of de initiatiefnemer specifieker kan aangeven waarom het NCSC onafhankelijker moet worden.

De leden van de CDA-fractie vragen de initiatiefnemer aan te geven in hoeverre het NCSC momenteel te kort schiet als het gaat om de werkzaamheden die zouden moeten verricht in het kader van cybersecurity en welk bedrag de initiatiefnemer in gedachten heeft om het NCSC concreet te versterken.

5. Financiële paragraaf

De leden van de VVD-fractie vragen of de initiatiefnemer kan aangeven wat het doorvoeren van deze zes voorstellen zou kosten. Wie deze kosten zou moeten dragen?

De leden van de SP-fractie zijn benieuwd in hoeverre de initiatiefnemer wel een schatting kan maken van de financiële gevolgen van zijn afzonderlijke voorstellen. Wat heeft de oprichting van het bedreigingsanalyseteam in de Verenigde Staten bijvoorbeeld gekost?