Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 613 Initiatiefnota van het lid Verhoeven: «Het Internet der Dingen: maak apparaten veilig!»

Nr. 2

INITIATIEFNOTA

1. Inleiding

De afgelopen decennia zijn steeds meer apparaten aangesloten op het internet. Internet der Dingen-apparaten gebruiken het internet om kleine hoeveelheden data te versturen of ontvangen waardoor een dienst op maat kan worden geboden. Steeds meer apparaten die we dagelijks gebruiken zijn op die manier verbonden met het internet. Denk aan slimme thermostaten die vanaf je smartphone bediend kunnen worden en als je thuis bent automatisch de verwarming aanzetten. Maar we sluiten ook koelkasten, auto's, sluizen, energiecentrales, stoplichten, lantaarnpalen en zorgapparaten aan op het internet.

Deze apparaten bieden ons gebruiksvoordelen en -gemak. Tegelijkertijd schuilen er ook kwetsbaarheden in, zoals datalekken, gestolen gegevens en hacks waarbij het apparaat van buiten af wordt stilgelegd of overgenomen met alle gevolgen van dien.

Met de toename van het Internet der Dingen is het tijd om een aantal waarborgen te creëren voor veilig gebruik. Die waarborgen zijn niet alleen een zorgplicht van aanbieders en gebruikers. Ook de overheid kan er aan bijdragen dat veilig gebruik van op het internet aangesloten apparaten wordt gewaarborgd.

In de Verenigde Staten heeft de Minister van Justitie besloten onderzoek te doen naar de beveiliging van Internet of Things-apparaten zoals zelfrijdende auto's, medische apparatuur en slimme thuisapparaten. Een bedreigingsanalyseteam is opgezet om apparaten beter te beveiligen tegen cyberaanvallen van terroristen, hackers en kwaadwillenden. Daarmee kan gebruikers meer bescherming worden geboden tegen diefstal van persoonlijke, maar ook van gevoelige economische en politieke informatie.

kst-34613-2
ISSN 0921 - 7371
's-Gravenhage 2016

2. Het plan in het kort

Initiatiefnemer vindt dat Nederland – als digitale koploper in Europa – stappen moet zetten om het veilig gebruik van Internet der Dingen-apparaten voor consumenten te waarborgen.
Deze apparaten bieden veel mogelijkheden die we als samenleving graag willen benutten. Dat kan alleen als ook het veilige gebruik ervan is gewaarborgd. We willen zoveel mogelijk voorkomen dat er wordt ingebroken op apparaten waardoor de werking van het apparaat in het geding komt. Apparaten die zijn aangesloten op internet verzamelen, analyseren en gebruiken persoonlijke en vaak intieme data van de gebruikers. Die informatie moet versleuteld zijn en daarmee afgeschermd voor derden. Welke keuzes hebben mensen wanneer zij een apparaat op het internet aansluiten? Hoe waarborgen we de veilige werking van aangesloten apparaten? Hoe wordt persoonlijke data van gebruikers beschermd tegen misbruik?

Initiatiefnemer vindt het tijd dat op die vragen antwoorden komen. Daarin ligt een taak voor bedrijven die apparaten en software aanbieden. Maar ook de overheid heeft een rol bij het waarborgen van cybersecurity en cyberhygiëne door consumenten advies te geven over het veilig gebruiken van op internet aangesloten apparaten.

Deze initiatiefnota is een stimulans voor het kabinet om niet aan de zijlijn toe te kijken. Nederland moet als innovatieleider in Europa samen met technologiebedrijven de nodige stappen te zetten naar een Internet der Dingen waarbij de kansen gegrepen worden en de risico's voor consumenten zo klein mogelijk worden gemaakt. Deze initiatiefnota gaat met name in op de risico's.

Initiatiefnemer stelt voor:
1. *Richt een Nederlands bedreigingsanalyseteam op*
2. *Creëer standaarden voor cyberveiligheid van apparaten.*
3. *Onderzoek mogelijkheden voor software aansprakelijkheid.*
4. *Investeer in de zelfredzaamheid van consumenten voor veilig gebruik van Internet der Dingen-apparaten.*
5. Een onafhankelijk, sterk en actief Nationaal CyberSecurity Centrum (NCSC)

3. Het Internet der Dingen

Wat is het Internet der Dingen?

Het Internet der Dingen zijn apparaten, voertuigen, gebouwen en infrastructuur die aangesloten worden op het internet, onderling kunnen communiceren en uitgerust worden met sensoren die data genereren op basis waarvan beslissingen genomen kunnen worden.

Denk aan slimme thermostaten die vanaf je smartphone gecontroleerd kunnen worden en op basis van sensoren inschatten of je thuis bent en vervolgens de CV lager zetten. Maar we sluiten ook koelkasten, auto's, sluizen, energiecentrales, stoplichten, lantaarnpalen en zorgapparaten aan op het internet.

Internet der Dingen-apparaten verzamelen (persoons-)gegevens en wisselen deze uit. De informatie die apparaten verzamelen kan vervolgens geanalyseerd en gebruikt worden voor beslissingen. Dat is de meerwaarde van het Internet der Dingen.

Deze toepassing kan grote voordelen hebben. Bruggen en sluizen kunnen van afstand bestuurd worden om de verkeersdoorstroming te verbeteren of om een brug gesloten te houden wanneer een hulpvoertuig nadert. Met slimme thermostaten kunnen mensen makkelijk energie en geld besparen. Met sporthorloges kunnen we onze sportactiviteiten beter bijhouden en gezonder leven. Ook andere toepassingen, zoals robotstofzuigers die hun werk doen zodra we het huis uit gaan, maken ons leven simpelweg makkelijker.

De ontwikkeling dat steeds meer apparaten zijn aangesloten op het internet vindt al een tijd plaats. De toepassingen nemen toe zowel wat betreft (vitale) infrastructuur als in het aanbod voor de consument die over steeds meer «smart» apparaten beschikt. In 2006 waren 2 miljard[1] apparaten aangesloten op het internet, in 2016 zullen het er meer dan 6 miljard zijn en in 2020 liefst 25 miljard.[2] Dit begon met computers, tablets en smartphones, maar inmiddels sluiten we ook sluizen, bruggen, fabrieken, teddy beren, tandenborstels, thermostaten, koelkasten, CAT-scanners, horloges en hartslagmeters aan op het internet. De meeste aangesloten apparaten vinden we bij productiebedrijven en in de zorg; denk aan de robots die auto's in elkaar zetten of medische apparaten. Veel van die apparaten zijn geen consumentengoed, maar bedoeld voor bedrijfsmatige toepassing. Op dit moment zijn nog geen 10% van de aangesloten apparaten consumentengoederen. Tegelijkertijd zien we dat consumenten wel steeds vaker gebruik maken van apparaten die zijn (of kunnen worden) aangesloten op het internet.

4. Risico's

Het succes van het Internet der Dingen en de voordelen die daarmee gepaard gaan, hangen af van de mate waarin we erin slagen de kwetsbaarheden voor veilig gebruik het hoofd te bieden. Kwetsbaarheden die verder gaan dan datalekken of gestolen gegevens. Apparaten die zijn aangesloten op het internet worden ook gebruikt als hulpstuk voor bepaalde toepassingen in ziekenhuizen, auto's en ook persoonlijke hartslagmeters. Doordat deze apparaten gebruik maken van het internet zijn ze vatbaar voor digitale inbraak met alle gevolgen voor de integriteit en beschikbaarheid van het apparaat van dien. Er zijn drie categorieën van risico's die onze aandacht vragen:

4.1 Werking van apparaten

Het eerste risico is dat de werking van apparaten in het geding komt doordat criminelen, buitenlandse mogendheden of andere kwaadwillenden zichzelf toegang verschaffen tot toepassingen die zijn aangesloten op het internet of de werking ervan blokkeren.

In de Verenigde Staten zijn verschillende voorbeelden bekend van ziekenhuizen waar ICT-systemen besmet raakten met ransomware. Daardoor konden patiënten niet behandeld worden.[3] Ook in Nederland is in ten minste twee ziekenhuizen sprake geweest van een malware besmetting.[4]

Vaak zijn ransomware besmettingen ongerichte aanvallen. Mensen klikken op een verkeerde link of browsen naar een verkeerde website, waardoor automatisch een virus gedownload wordt. Ook zijn er tal van voorbeelden

---

[1] http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[2] http://www.gartner.com/newsroom/id/3165317
[3] http://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack/
[4] https://zoek.officielebekendmakingen.nl/ah-tk-20152016–3098.html

van gerichte aanvallen bekend. Bijvoorbeeld het Stuxnet virus, dat een nota bene niet op het internet aangesloten kernreactor toch wist te saboteren.[5] Recenter, eind 2015, haalden hackers een energiecentrale in Oekraïne offline, waardoor honderdduizenden inwoners zonder elektriciteit zaten.[6] Ook zijn er voorbeelden van cybersecurity-onderzoekers die erin slaagden om auto's te hacken en van een afstand konden controleren. Hetzelfde geldt voor vrijwel alle andere consumentengoederen die we op het internet aansluiten.[7] Kortom, het is geen denkbeeldige digitale dreiging maar een reëel en fysiek gevaar dat direct ingrijpt in ons dagelijks leven.

4.2 Persoonlijke keuzes

Het tweede risico is dat persoonlijke en vaak intieme informatie, gegenereerd door op internet aangesloten apparaten, zonder expliciete toestemming of zonder keuze voor de consument naar de maker van het apparaat of aan derden doorgegeven of zelfs verkocht wordt.

Slimme apparaten bevatten veel informatie over hun gebruikers. Door apparaten op het internet aan te sluiten, kunnen deze apparaten worden ingezet om persoonlijke informatie over mensen te verzamelen en door te geven aan de aanbieder van een toepassing, de maker van de software. We zien ook dat veel winkels en gemeenten, bijvoorbeeld via Wifi-tracking, proberen bij te houden hoeveel mensen de winkel binnengaan, om loopstromen in kaart te brengen en bij te houden hoe lang bezoekers op een bepaalde plaats verblijven.

Op dit moment is het vaak onduidelijk op wat voor manier toestemming gegeven wordt voor het delen van informatie die gegenereerd wordt door gekochte apparaten, zoals auto's, slimme thermostaten of slimme horloges. Soms staat het diep in de gebruikersvoorwaarden verstopt. Soms wordt simpelweg het kopen van een apparaat al gezien als het geven van toestemming om informatie te delen. Mensen hebben daardoor nauwelijks grip op de toegang die anderen hebben tot hun persoonlijke informatie, wat er met hun data gebeurt en hoe de toepassing is beveiligd tegen misbruik door derden. Door deze risico's is de maatschappelijke verantwoorde toepassing van het Internet der Dingen nu niet optimaal geregeld.

4.3 Economische en politieke informatie

Het derde risico is dat economische en politieke informatie wordt buitgemaakt door terroristen, criminelen of andere kwaadwillenden. In 2015 is in Nederland een recordaantal digitale spionageaanvallen gemeten. Het Ministerie van Veiligheid en Justitie schrijft daarover in de begroting voor 2017: «Deze cyberdreiging kan de integriteit van politiek-bestuurlijke en democratische besluitvorming, het functioneren van de vitale infrastructuur en het verdienvermogen van de Nederlandse samenleving ernstig aantasten.» Naast het in de praktijk brengen van goede cyberhygiëne door mensen in kritieke functies,[8] is het belangrijk dat ook veiligheidswaarborgen worden gecreëerd voor informatie die via het op internet aangesloten apparaten buitgemaakt kan worden. Zo werd in 2011 de Amerikaanse Kamer van Koophandel, die zich ook bezig houdt

[5] Het Stuxnet virus is een virus dat speciaal gemaakt was (waarschijnlijk door de Verenigde Staten of Israel) om een bepaalde nucleare reactor in Iran te saboteren.
[6] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[7] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[8] https://tweakers.net/nieuws/111285/minister-kamp-gaat-door-met-gebruik-gmail-voor-communicatie-met-ambtenaren.html

met internationale handelsverdragen, gehackt door Chinese hackers via een «slimme thermostaat» in het kantoor op «Capitol Hill».[9]

5. Onderzoek en adviezen

De risico's van het Internet der Dingen worden al langer erkend.

5.1 Wetenschappelijke Raad voor Regeringsbeleid

Zo wijst de Wetenschappelijke Raad voor Regeringsbeleid (WRR) in het recente advies «Big Data in een vrije en veilige samenleving» erop dat we toegaan naar steeds verdergaande koppelingen van databronnen, dat het steeds aantrekkelijker wordt om het analyseproces te automatiseren en de grens tussen data uit publieke en private bronnen zal vervagen. Als één van de grootste zorgen noemt de WRR de inmenging in de persoonlijke levenssfeer:

«De grootschalige verzameling, opslag en analyse van data door overheden, waaronder inlichtingen- en veiligheidsdiensten, kunnen ertoe leiden dat mensen het gevoel krijgen dat hun privacy en vrije meningsuiting in gevaar zijn, waardoor zij hun gedrag daarop aanpassen. Bovendien worden burgers steeds transparanter voor de overheid, terwijl de profielen, algoritmen en methoden die overheidsorganisaties gebruiken nauwelijks transparant of navolgbaar voor die burgers zijn. Nu met Big Datatoepassingen steeds grotere groepen burgers in beeld komen – naast verdachte ook niet-verdachte burgers – gaat dat gebrek aan transparantie steeds meer wringen.

Daarnaast kunnen Big Data-toepassingen leiden tot een toename van sociale stratificatie, met een ongelijke verhouding tussen maatschappelijke groepen als gevolg.
Dit gebeurt doordat Big Data onregelmatigheden en afwijkingen in datasets kan reproduceren, resulterend in uitkomsten die een onevenredige sociale impact hebben. Zonder correctie vertaalt zich dit op termijn in een cumulatief nadeel (discriminatie en oneerlijke behandeling) voor bepaalde groepen in de maatschappij.
Ook zijn Big Data-toepassingen zeer gevoelig voor «function creep», oftewel gebruik van gegevens anders dan voor het doel waarvoor de data zijn verzameld.
De reden hiervan is dat het secundair gebruik van gegevens bij Big Datatoepassingen een grote meerwaarde oplevert.».[10]

5.2 Het Rathenau Instituut

Het Rathenau Instituut betoogt in haar recente onderzoek «Beyond control» dat aandacht nodig is voor hoe technologie ons dagelijks leven beïnvloedt. Dat gaat onder andere in op hoe we omgaan met «profiling» en met verborgen overtuigingstactieken die de keuzevrijheid van consumenten beïnvloeden. Bij een toename van het Internet der Dingen moeten we op zoek gaan naar praktische manieren om fundamentele menselijke waarden als zelfbeschikking en menselijke waardigheid, te waarborgen.[11]

---

[9] M. Goodman, Future Crimes, p.328
[10] WRR, «Big Data in een vrije en veilige samenleving»; WRR
[11] Rathenau Instituut, «Beyond control» explanatory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things. Rathenau

5.3 De Autoriteit Persoonsgegevens

Ook de Autoriteit Persoonsgegevens wijst op risico's van het Internet der Dingen en big data. Deze autoriteit pleit voor een maatschappelijk verantwoorde toepassing en transparantie over wat er met persoonsgegevens gebeurt.[12]

5.4 Europees Actieplan

Op Europees niveau is al in 2009 over het Internet der Dingen een actieplan voor Europa opgesteld. Daarin wordt op de kansen gewezen voor een reeks van maatschappelijke uitdagingen zoals gezondheidsbewaking, ecologie en milieubescherming en vervoer. Daarnaast werd toen al gewezen op de gecompliceerde processen van gegevensverwerking die gepaard gaan met het Internet der Dingen en de risico's voor privacy en cyberterrorisme. Inmiddels zijn we zeven jaar verder en zien we steeds meer Internet der Dingen-toepassingen. Tegelijkertijd is er bij gebruikers nog onvoldoende bewustzijn over het veilig gebruik van op internet aangesloten apparaten. Ook zijn er onvoldoende waarborgen om de risico's zo klein mogelijk te houden voor consumenten.[13]

5.5 Europese Toezichthouder voor Gegevensbescherming

De Europese Toezichthouder voor Gegevensbescherming bracht in september 2015 een advies uit «Naar een nieuwe digitale ethiek: data, waardigheid en technologie.[14] Daarbij wijst de Europese toezichthouder op de technologische vooruitgang, zoals big data en machinaal leren, die «het inzamelen en het gebruik van persoonsgegevens mogelijk maakt op steeds ondoorzichtigere en complexere manieren die belangrijke bedreigingen voor de privacy en de menselijke waardigheid vormen». De toezichthouder roept op tot een «open en gefundeerde discussie over digitale ethiek waarmee we de voordelen van technologie voor de samenleving en de economie kunnen realiseren en tegelijkertijd de rechten en vrijheden van personen versterken, in het bijzonder het individuele recht op privacy en gegevensbescherming».

6. Oplossingen

Het genereren, opslaan en analyseren van persoonlijke, economische en politieke informatie is de afgelopen jaren fors toegenomen. De toepassingen die met behulp van het internet hier gebruik van maken, zijn volop in ontwikkeling. Initiatiefnemer vindt dat de overheid een aantal stappen in Nederland moet zetten om interactieve informatieuitwisseling tussen apparaten die verbonden zijn met het internet op een veilige manier te waarborgen.
Initiatiefnemer doet daartoe de volgende voorstellen:

---

[12] Autoriteit Persoonsgegevens, nieuwsbericht 17 oktober 2014 «meer aandacht voor privacy bij Internet of Things» en Agenda 2016, «Internet of Things en profiling». Autoriteit Persoonsgegevens Agenda_2016

[13] Europese Commissie, 18 juni 2009, «het Internet van de dingen – een actieplan voor Europa» (COM/2009/0278).

[14] Europese toezichthouder voor gegevensbescherming, 11 september 2015, «Naar een nieuwe digitale ethiek: data, waardigheid en technologie» Europese toezichthouder

6.1 Nederlands bedreigingsanalyseteam

Richt in Nederland, net als in de Verenigde Staten[15], een bedreigingsanalyseteam op. Dit team moet potentiële gevaren en uitdagingen signaleren voor de kritieke infrastructuur van Nederland die voortkomen uit op internet aangesloten apparaten. Vervolgens moeten zij gerichte en concrete voorstellen doen voor de beveiliging ervan. Dit team van experts kan bestaan uit beveiligingsexperts en aanbieders van apparaten en toepassingen.

6.2 Keurmerk en standaarden voor cyberveiligheid van apparaten.

Net zoals er standaarden zijn voor de brandveiligheid van apparaten, zo moeten er ook normen en standaarden komen voor de cyberveiligheid van apparaten. Deze moeten een minimumstandaard voor cyberveiligheid van Internet der Dingen-apparaten garanderen. Hierbij kan men denken aan standaarden voor versleuteling van data, eisen aan standaard wachtwoorden, het doorvoeren van software-updates en beveiligingsmeldingen, en instructies aan gebruikers. Voldoet een apparaat niet aan deze standaarden, dan mag het niet verkocht worden. Deze standaarden zullen op Europees niveau gesteld moeten worden. Tegelijkertijd kunnen we in Nederland al een keurmerk oprichten, gebaseerd op dezelfde standaarden, om consumenten in te lichten over de cyberveiligheid van apparaten.

In de Verenigde Staten zijn Internet-of-Things apparaten doorgaans veiliger, omdat bedrijven verplicht zijn specificaties van apparaten te melden in een openbaar register van de toezichterhouder, de FCC.[16] Initiatiefnemer wil het effect van dit register onderzoeken en, indien gewenst, een dergelijke Europees register oprichten. Dit register kan ook input leveren voor (aanscherping van) het keurmerk.

6.3 Innovatievraag veilige IoT-apparaten.

De overheid kan een innovatievraag formuleren om startups die actief zijn in digitale toepassingen en Internet der Dingen, na te laten denken over manieren om het Internet der Dingen duurzaam te beveiligen tegen inbraak en integriteitsschendingen.[17]

6.4 Software aansprakelijkheid.

Gegevensverwerking op, en via op internet aangesloten apparaten, wordt steeds complexer. Nu we meer op digitale diensten vertrouwen, vertrouwen we ook op de juiste werking van de software hierachter. Steeds meer bedrijven zijn tegenwoordig softwareontwikkelaar en moeten zich bewust zijn van de verantwoordelijkheid die hoort bij het leveren van software. Met het Internet der Dingen groeit ook het belang van duidelijke aansprakelijkheid voor softwaresystemen[18] of het van toepassing laten zijn van consumentenbeschermingsregels, zoals een garantie. Zo weten organisaties dat zij met het aanbieden van een nieuwe dienst of product ook de verantwoordelijkheid aangaan deze veilig en deugdelijk te houden. Natuurlijk is software nooit 100% veilig. Maar niet genoeg aandacht besteden aan de kwaliteit van software of het niet tijdig updaten van

---

[15] http://www.darkreading.com/iot/doj-announces-team-to-oversee-security-of-internet-of-things/d/d-id/1326881

[16] https://fccid.io/

[17] Dit kan via een Small Business Innovation Research programma.

[18] Ook het CPB pleit hiervoor: http://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-6juli2016-Risicorapportage-cyberveiligheid-economie.pdf

software is een vorm van nalatigheid. Net zoals het nalatig is om niet over de brandveiligheid van producten na te denken. Kortom, de regering moet onderzoek doen naar de beste manier om softwareaansprakelijkheid te regelen.

6.5 Zelfredzaamheid gebruikers

Geef consumenten meer grip op hun persoonlijke informatie door ze zelfredzaam te maken in het veilig houden van hun data. Biedt consumenten ook de keuze met betrekking tot wat wel en niet wordt gedeeld met derden. Dat kan door:

a) ***Onderwijs in veilig internetgebruik op school.*** Een veiliger Internet der Dingen begint bij goed ingelichte gebruikers die weten wat ze wel en niet moeten doen om hun data veilig te houden. Het standaard wachtwoord wijzigen, software updaten, sterke wachtwoorden gebruiken, niet op verdachte links klikken, beseffen dat een apparaat niet geïsoleerd is maar is aangesloten op het internet, etc.[19]
b) ***Campagne voeren voor goede cyberveiligheid en cyberhygiëne***. We kennen allemaal de «maak het ze niet te makkelijk»-campagne tegen inbrekers, maar de «alert online»-campagne kent vrijwel niemand. Dat moet anders aangezien cybercrime een steeds groter probleem wordt.
c) ***Heldere en begrijpelijke privacy-voorwaarden verplicht stellen.*** Gebruikers van apparaten moeten weten wat er met hun gegevens gebeurt. Privacy-voorwaarden zijn nu nog te vaak te onduidelijk. De gebruiker moet actief geïnformeerd worden voordat hij nadrukkelijk toestemming kan geven. Daarom moet de nieuwe Europese privacyrichtlijn streng gehandhaafd worden en moet er expliciet duidelijk gemaakt worden hoe deze richtlijn zich tot het Internet der Dingen verhoudt.
d) ***Geen geautomatiseerde besluitvorming.*** Steeds meer «Big Data» wordt gegenereerd door op internet aangesloten apparaten. Steeds vaker zullen op basis van deze data door algoritmes beslissingen genomen worden die de levens van mensen significant beïnvloeden. De nieuwe Europese privacyrichtlijn stelt dat een gebruiker het recht heeft op uitleg van een beslissing. Dat heeft mogelijk gevolgen voor geautomatiseerde besluitvorming, zowel door de overheid als door bedrijven. Hier moet zo snel mogelijk duidelijkheid over komen. Initiatiefnemer is van mening dat Nederland voorop kan lopen door dit «recht op uitleg» en de relatie tot geautomatiseerde besluitvorming duidelijk in de implementatiewet op te nemen.

Aan- en uitknop voor gegevensdoorgifte aan derden. Simpelweg het feit dat iemand een apparaat koopt betekent niet dat hij of zij toestemming geeft om data te delen met de fabrikant ervan of met derden. Hiervoor dient expliciet toestemming verleend te worden die altijd, en op een makkelijke manier, weer in te trekken is.

6.6 Een onafhankelijk, sterk en actief NCSC

Het Nationaal CyberSecurity Centrum moet onafhankelijk worden om de cyberveiligheid in Nederland nog beter te dienen. Vergelijkbaar met het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) moet het NCSC onafhankelijk van politieke druk advies kunnen geven en toezicht kunnen houden op de cyberveiligheid in Nederland. Ook moet het NCSC een actievere rol kunnen spelen om lokale overheden en semi-overheidsinstellingen, zoals ziekenhuizen, te helpen met het op orde

[19] https://www.ncsc.nl/actueel/factsheets/factsheet-10-vuistregels-voor-veilig-internetten.html

brengen van de cyberveiligheid. Om deze rol te vervullen moet het NCSC additionele middelen ontvangen.

7. Financiële paragraaf

De financiële gevolgen van de voorstellen zijn afhankelijk van de wijze waarop de voorstellen worden overgenomen en ingevuld. De kosten zijn zodoende nog niet bekend.
Wel kan worden opgemerkt dat een veilig gebruik van apparaten het aantal inbreuken dat tot mogelijke schade leidt, verkleint.

Verhoeven