‘Naar een veilig verbonden digitale samenleving’

Advies inzake de cybersecurity van het Internet of Things (IoT)

CSR
Cyber Security Council
Cyber Security Raad

‘Naar een veilig verbonden digitale samenleving’

Advies inzake de cybersecurity van het Internet of Things (IoT)

Gericht aan:

De minister van Justitie en Veiligheid
De staatssecretaris van Economische Zaken en Klimaat
De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Tevens is ondersteuning van het advies gevraagd aan de voorzitter VNO-NCW

CSR
Cyber Security Council
Cyber Security Raad

CSR-advies 2017, nr. 3

Excellenties,

Nederland heeft een uitstekende uitgangspositie om de economische kansen van de digitale toekomst voluit te benutten. De mate van digitalisering, het vestigingsklimaat, de beschikbare infrastructuur: allemaal factoren die maken dat Nederland in Europa een koppositie inneemt. Het is daarom des te belangrijker dat de randvoorwaarden voor economisch succes goed worden geborgd: veiligheid, vertrouwen en betrouwbaarheid van de digitale infrastructuur. Nieuwe technologieën ontwikkelen zich razendsnel en zijn een belangrijke drijfveer voor innovatie en economische groei. Eén van die technologische ontwikkelingen is het Internet of Things (IoT).

Het IoT is een netwerk van 'slimme' apparaten, sensoren en andere objecten die (vaak verbonden met het internet), gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen en/of acties nemen die van invloed zijn op hun omgeving.

Het IoT zal een steeds prominentere rol gaan spelen in het dagelijks leven. De fysieke en digitale wereld zullen verder met elkaar vervlochten raken. Het zal effect hebben op onder andere werkgelegenheid, gezondheidszorg, mobiliteit en welvaart. De toepassingen van het IoT zijn breed en variëren van eHealth, smart homes, smart industries, smart cities tot digitale infrastructuur. Denk bijvoorbeeld aan pacemakers, slimme stofzuigers, zelfrijdende voertuigen, zonnepanelen en sluizen.

Kansen en bedreigingen

Het IoT is geen apart domein. Het is onderdeel van de bredere opgave om dringend de cyberveiligheid te verbeteren van onze online diensten en systemen, zoals die al aan de orde is gesteld in het rapport Verhagen[1]. Wel brengt het IoT bepaalde problemen nog urgenter voor het voetlicht, omdat securityproblemen zich nu manifesteren buiten de conventionele ICT-domeinen.

De technologische en economische kansen van het IoT gaan hand in hand met digitale dreigingen voor economische groei, veiligheid en vrijheid. Om deze reden heeft de Cyber Security Raad (CSR) het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) verzocht een verkennend onderzoek[2] te doen. Uit dit onderzoek blijkt dat als er geen maatregelen worden getroffen het IoT ingrijpende gevolgen kan hebben. IoT-toepassingen zijn op dit moment vaak slecht beveiligd en vormen daarmee een bedreiging voor onze veiligheid en privacy. Het Mirai-botnet, bestaande uit gehackte IoT-apparaten, laat zien dat de impact nu al groot kan zijn en dit zal in de toekomst alleen nog maar toenemen. Het is van belang dat de veiligheids- en privacyrisico's worden aangepakt om schade zoveel mogelijk te beperken en voorkomen. Om onze welvaart en ons welzijn voor nu en de toekomst veilig te stellen is gerichte actie nodig.

Belangrijkste uitdagingen

De belangrijkste uitdagingen die het IoT met zich meebrengt zijn:

De kwetsbaarheid neemt toe door de schaal waarop apparaten met onvoldoende beveiliging met elkaar en met het internet worden verbonden.

Het probleem is dat er een wildgroei van onveilige apparaten en toepassingen ontstaat die met elkaar verbonden zijn. Het gaat niet alleen om nieuwe apparaten, ook oudere - per definitie onveilige - apparaten worden aan het internet verbonden. Het betreft aan elkaar verbonden technologie waarin samenhang ontbreekt, met als gevolg dat netwerkbeveiliging heel moeilijk valt te realiseren. De

[1] 'De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten', Herna Verhagen, september 2016

[2] '(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen', WODC, juni 2017

kwaliteit van de huidige software laat vaak te wensen over en de update-mogelijkheden van nieuwe apparaten ontbreken of zijn zeer beperkt.

De hoeveelheid data die kan worden verzameld is enorm. De beveiliging van data is lastig te regelen.

De basis voor veel (economische) kansen is gelegen in het feit dat door het IoT grote hoeveelheden data beschikbaar komen. Echter, de beschikbare data en/of toepassingen kunnen ongewild ook voor criminele doeleinden worden aangewend. Consumenten en bedrijven zijn onvoldoende op de hoogte van de risico's en nemen onvoldoende maatregelen.

Het handhaven van zorgplichten en aansprakelijkheid van de producten en diensten die geleverd worden is buitengewoon complex.

Het IoT-speelveld is groot, grenzeloos en kent een complexe internationale samenstelling. Bij de productie of het gebruik van IoT-producten zijn vaak verschillende partijen betrokken. Fabrikanten combineren of 're-branden' verschillende hard- en software van andere fabrikanten. Door de grote hoeveelheid aan veelal buitenlandse spelers op de IoT-markt ontbreekt het aan overzicht. Hierdoor is het onduidelijk wie waarvoor verantwoordelijk is en daarop kan worden aangesproken. Dit probleem wordt verergerd doordat landen verschillende standaarden en regels hanteren. Vooralsnog zijn er weinig incentives om veilige hard- en software te produceren en te onderhouden. Voor de meeste producenten is de *time-to-market* en een lage kostprijs belangrijker dan de kwaliteit van een product. Bedrijven spannen zich onvoldoende in om de verplichtingen na te komen en cybercriminelen maken hier dankbaar gebruik van. Ook is de wetgeving op het gebied van zorgplichten binnen de EU (en wereldwijd) niet of nauwelijks op elkaar afgestemd.

Advies

De CSR ziet zes strategische oplossingsrichtingen om de uitdagingen die het IoT met zich meebrengt het hoofd te bieden, mede op basis van het WODC-rapport. We adviseren daarbinnen de volgende concrete acties:

1. Certificering, keurmerken en toegangseisen
    - De staatssecretaris van Economische Zaken en Klimaat verkent hoe het voorgestelde EU Cybersecurity Certification Framework[3] en eventueel de CE-marketing gebruikt kunnen worden om onveilige IoT-apparaten van de Europese markt te weren. Via certificering dienen minimumeisen te worden geformuleerd voor wat betreft de duur dat het product door de leverancier dient te worden onderhouden, de wijze waarop security-updates ter beschikking dienen te worden gesteld, de periode waarbij de bewijslast voor conformiteit op de leverancier rust, en de eis dat het apparaat van het internet kan worden afgeschakeld met behoud van de 'reguliere' functionaliteit. Als het Europese kader onvoldoende mogelijkheden biedt, dan ontwikkelt de minister een (wets)voorstel om deze eisen te borgen, bijvoorbeeld via het regime van koopregels.
    - De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties richt in gezamenlijkheid met de (de)centrale overheid het inkoopbeleid zodanig in dat er standaard digitale veiligheidseisen aan leveranciers worden gesteld, ook in het kader van smart cities.
    - De minister van Justitie en Veiligheid coördineert een voorstel voor het toevoegen van cybersecurity-normen aan bestaande bindende sectorale veiligheidseisen in belangrijke sectoren als gezondheidszorg, vervoer en energie.

2. Transparantie
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid financieren een onafhankelijke monitor van gehackte en kwetsbare IoT-apparaten, zodat publieke informatie beschikbaar komt over welke fabrikanten en leveranciers hun apparaten onvoldoende beveiligen.

3. Bewustwording
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid vragen een duidelijke toezegging van de producenten en leveranciers van IoT-apparaten om via een ‘labelling-systeem’ (bijv. stickers op de verpakkingen) consumenten te informeren over (i) het level van beveiliging van het betreffende apparaat; (ii) of het apparaat automatisch security-updates kan ontvangen; (iii) de duur dat het product door de leverancier wordt onderhouden; en (iv) of het apparaat van het internet kan worden afgeschakeld met behoud van de 'reguliere' functionaliteit.
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid financieren een voorlichtingscampagne en laten een eenvoudige handleiding opstellen die consumenten informeert over het nieuwe 'labelling-systeem’ en helpt om te gaan met de risico’s van IoT.

[3] Joint Communication to the European Parliament and the Council, ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’, European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Brussels, 13.9.2017 JOIN(2017) 450 final.

4. Productaansprakelijkheid
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid komen met een (wets)voorstel om veiligheid van ICT-producten en diensten beter in te passen in het regime van productaansprakelijkheid, waardoor fabrikanten wettelijk aansprakelijk gehouden kunnen worden voor ook economische schade. Dit voorstel sluit bij voorkeur aan op maatregelen die de Europese Commissie in juni 2018 zal presenteren.[4]
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid identificeren welke Nederlandse toezichthouders, analoog aan de Amerikaanse Federal Trade Commission[5] op grond van bestaande zorgplichten fabrikanten kunnen aanspreken op basale veiligheidsproblemen, zoals het niet tijdig verstrekken van security patches. Hierbij kunnen onder andere de Handreiking Zorgplichten[6] en de FTC Richtlijn[7] de basis vormen.

5. Intermediaire verantwoordelijkheden
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid maken samen met de industrie richtlijnen voor het onderbrengen van de veiligheid van IoT in de bestaande zorgplichten van intermediair aanbieders.
    - De staatssecretaris van Economische Zaken en Klimaat en de minister van Justitie en Veiligheid vragen een duidelijke toezegging van de internetaanbieders dat zij besmette IoT-apparaten in hun netwerken helpen opruimen, analoog aan de succesvolle aanpak van botnets (bijvoorbeeld in AbuseHub).

6. Versterking handhaving
    - De minister van Justitie en Veiligheid coördineert een voorstel van alle betrokken ministeries om voldoende mandaat en capaciteit bij toezichthouders op te bouwen zodat handhaving van cybersecurity-normen en regels structureel is geborgd in alle sectoren.

’s-Gravenhage, december 2017

Namens de Cyber Security Raad,

Jos Nijhuis
Covoorzitter CSR

Dick Schoof
Covoorzitter CSR

[4] Joint Communication to the European Parliament and the Council, ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’, European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Brussels, 13.9.2017 JOIN(2017) 450 final (p. 6).

[5] Zie: https://www.ftc.gov/about-ftc

[6] ‘Ieder bedrijf heeft digitale zorgplichten: een handreiking voor bedrijven op het gebied van cybersecurity’, CSR, februari 2017

[7] Zie: https://www.ftc.gov/news-events/press-releases/2017/06/ftc-offers-comment-process-aimed-improving-security-internet