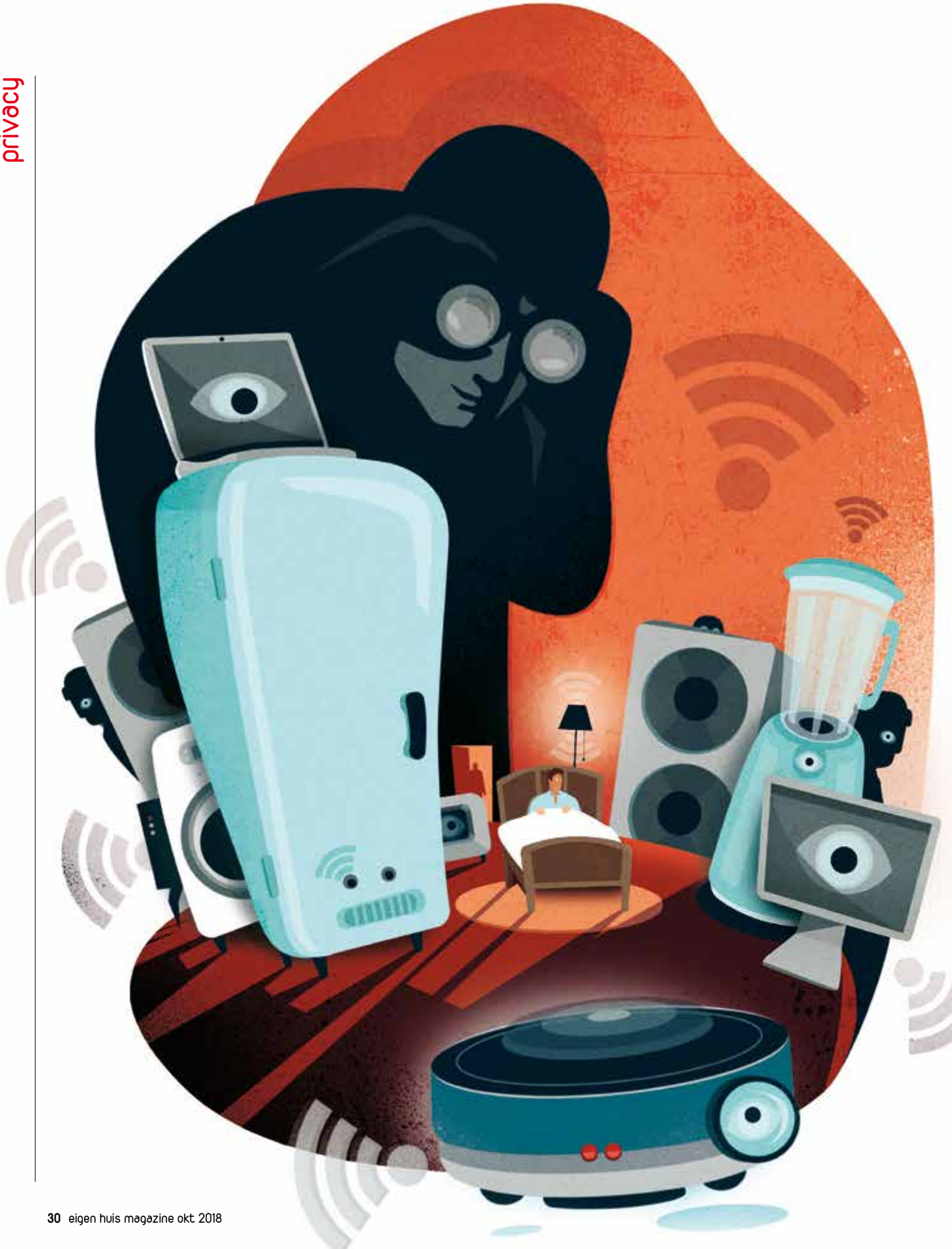


Hoe we ons huis digitaal veiliger kunnen maken

Via de koelkast komen hackers binnen

Apparaten van deursloten tot koelkasten krijgen tegenwoordig een internetaansluiting. Digitaal zijn die vaak slecht beveiligd – dan is het voor hackers een koud kunstje op je thuisnetwerk te komen.

TEKST **ILSE AKKERMANS** BEELD **STUDIO VONQ**

Een slim voordeurslot, een slimme beveiligingscamera, de koelkast, wasmachine, thermostaat of robotstofzuiger: je kunt het zo gek niet bedenken of je kunt apparaten tegenwoordig aan het internet koppelen en via een app op je telefoon bedienen. Handig en leuk.

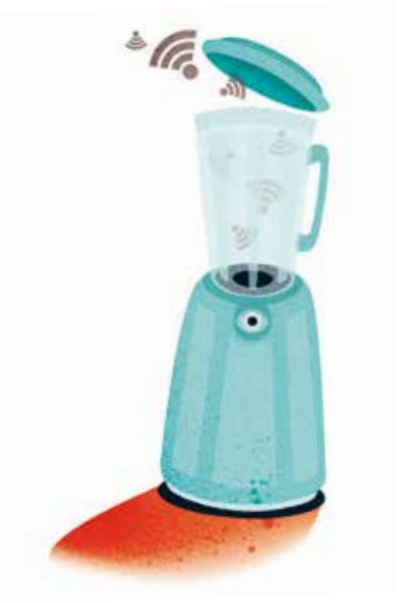
Maar toezichthouder Agentschap Telecom waarschuwde afgelopen zomer voor de risico's ervan. Slimme apparaten zijn vaak digitaal onveilig, software is verouderd en updates worden niet uitgevoerd. Daardoor zijn de apparaten een makkelijk doelwit voor cybercriminelen. Die kunnen 'lekke' apparaten overnemen en er alles mee doen wat ze willen.

'De vraag is niet of je gehackt wordt, maar wanneer en hoe vaak', zegt Sijmen Ruwhof, specialist in internetveiligheid en ethisch hacker – iemand die met toestemming van opdrachtgevers inbreekt op hun computersystemen om, uiteindelijk, de beveiliging daarvan te verbeteren.

Zo kan het gebeuren dat hackers je slimme voordeurslot openen, zonder dat je het wilt. Dat ze – om mensen de stuipen op het lijf te jagen – 's nachts het geluid van krakende deuren en thrillers uit je slimme speakers laten klinken; dat ze je robotstofzuiger met camera laten rondrijden. Dat een vreemde via de babyfoon met je kind praat, en dat de inhoud van je slimme harde schijf met al je persoonlijke gegevens op internet komt te staan, zonder dat je dat in de gaten hebt.

'Slimme apparaten vormen allemaal deurtjes naar je thuisnetwerk'

'Mensen kopen slimme apparaten voor de luxe ervan', zegt Ruwhof. 'De apparaten zijn makkelijk te bedienen, maar voor veel mensen zijn ze een *black box*: niemand weet hoe ze werken. Ondertussen vormen ze allemaal deurtjes naar je thuisnetwerk.' Hij geeft het voorbeeld van een gezin dat hem inschakelde omdat het door de internetprovider werd afgesloten van het internet. 'Het netwerk in hun huis bleek een broeinest van virussen', zegt hij. 'Ze hadden onder andere beveiligingscamera's in huis, een smart-tv en een →



slimme harde schijf. Bijna alle apparaten hadden ernstige veiligheidslekken. Beveiligingscamera's in en rond het huis waren gehackt, meerdere hackers waren de afgelopen twee jaar op de harde schijf geweest, en ook diverse laptops, tablets en telefoons bleken gehackt. Verschillende hackers gebruikten de slimme apparaten van het gezin om websites aan te vallen, onafhankelijk van elkaar. Het gezin had er geen idee van dat dat gebeurde.'

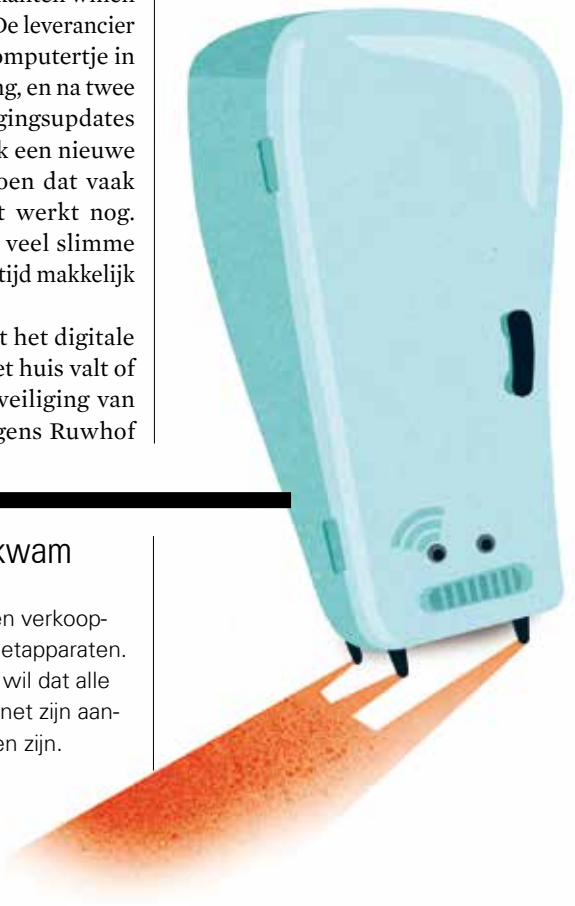
90 procent van de huishoudens

Nederland hoort volgens het Rathenau Instituut bij de meest gedigitaliseerde landen ter wereld: bijna iedereen heeft een computer, meer dan 90 procent van de huishoudens heeft internet. Ondertussen groeit het aantal aan internet te koppelen apparaten, het '*internet of things*', wereldwijd hard. Inmiddels zijn er meer slimme apparaten dan mensen op de wereld. In 2020 zullen het er volgens onderzoeksbureau Gartner al 20 miljard zijn. Ons leven is steeds meer verbonden met internet, maar de gebrekkige beveiliging ervan maakt ons kwetsbaar. Voor het manipuleren of saboteren van apparaten dus, maar ook voor gijzelingssoftware en voor diefstal van persoonlijke gegevens.

'Ik heb zelf bewust niet veel van dat soort apparaten in huis', zegt Ruwhof. 'Een thermostaat en tv hoeven voor mij niet slim te zijn. Ik hang geen camera's in mijn huis. Ik heb een robotstofzuiger, maar zonder internetverbinding. Die producten staan nog in de kinderschoenen, het duurt nog jaren voordat ze veiliger worden. Fabrikanten willen er vooral mee verdienen. De leverancier stopt er een goedkoop computertje in voor de internetverbinding, en na twee jaar krijg je geen beveiligingsupdates meer en moet je eigenlijk een nieuwe kopen. Consumenten doen dat vaak niet, want het apparaat werkt nog. Daarom is een huis met veel slimme apparaten na verloop van tijd makkelijk te hacken.'

Neem de voordeur met het digitale slot. De veiligheid van het huis valt of staat met de digitale beveiliging van het slot. En die laat volgens Ruwhof

'Ik hang geen camera's in mijn huis. Ik heb een robotstofzuiger, maar zonder internetverbinding. Het duurt nog jaren voordat ze veiliger worden'



Gooit de boel in de war

Een internationale expertmeeting van de Cyber Security Raad concludeerde in 2016 dat de opkomst van het *internet of things* een van de meest disruptieve hedendaagse ontwikkelingen is.

Verbod dat er niet kwam

D66 riep in 2016 op tot een verkoopverbod op onveilige internetapparaten. Kamerlid Kees Verhoeven wil dat alle apparaten die op het internet zijn aangesloten veilig te gebruiken zijn.

nog dikwijls te wensen over. ‘Een slim voordeurslot kun je met een mobiele app openen via een internetverbinding’, zegt Ruwhof. ‘De technologie is vaak nog experimenteel, de focus ligt meer op innovatie dan op veiligheid. Maar als een hacker dan een beveiligingslek vindt, kan hij je voordeurslot hacken en de deur openen.’

De code van het deurslot

Er kunnen ook andere dingen misgaan. ‘Zo maakte een aanbieder van digitale sloten een fout in een software-update’, zegt Ruwhof. ‘Vervolgens konden alle vijfhonderd gebruikers hun huis niet meer in.’ Ruwhof logeerde zelf enkele maanden geleden via Airbnb in een huis. ‘Ik kreeg de code van het deurslot’, zegt hij. ‘Die code bleek al een half jaar dezelfde. Dus iedereen die het voorbije halfjaar in dat huis had gelogeerd, ongeveer tachtig mensen, kon bij dat huis naar binnen.’ Ook deed een gebruiker vanaf zijn vakantieadres via de app op zijn telefoon per ongeluk de voordeur van zijn huis open.

En als een hacker je beveiligingscamera’s hackt kan hij je bespioneren, zegt Ruwhof. Huiseigenaren die echt beveiligingscamera’s in huis willen, raadt hij dan ook aan de camera’s te richten op minder gevoelige plekken in huis. ‘Richt de camera op ramen, gang en deuren, niet op je bed of andere privégedeeltes’, zegt Ruwhof. ‘En plak de camera op je smart tv af, want die staat gericht op je bank. Zo minimaliseer je de impact als het misgaat.’

Vaak geven fabrikanten apparaten een standaard wachtwoord. Die standaard wachtwoorden staan op het internet – hackers weten ze te vinden. Als de koper nalaat het wachtwoord te veranderen, heeft een hacker dan ook zo toegang. En niet alleen tot het product, maar ook tot het interne thuisnetwerk van de eigenaar. Via de beveiligingscamera of slimme harde schijf bijvoorbeeld. ‘Hij kan dan bijvoorbeeld gijzelingssoftware installeren op verbonden apparaten die al een tijd geen beveiligingsupdates hebben ontvangen’, zegt Ruwhof. ‘En aan het interne netwerk is bijvoorbeeld ook je printer gekoppeld. Bijna niemand zet een wachtwoord op zijn printer. De hacker kan dan bestanden gaan printen en rare berichten afleveren in je huis.’

Kamervragen

In januari van dit jaar stelden D66 en CDA Kamervragen over de oproep van Amerikaanse experts om gebrekkige beveiliging van op internet aangesloten apparaten te verbeteren.

Koop verstandig

Slim apparaat kopen?

- Zoek uit of de leverancier betrouwbaar is.
- Lees productreviews.
- Let op of het apparaat een CE-keurmerk heeft: dan voldoet het aan Europese regels.
- ‘Pas op met aanbiedingen van goedkope elektronica op het web die uit landen buiten de EU komen’, stelt Agentschap Telecom. ‘De kans is dan groter dat zulke apparaten onveilig zijn en geen software-updates krijgen.’
- Vraag je af of bediening via internet wel nodig is.
- Zoek uit wie beschikking krijgt over je gegevens.
- Hoe lang krijgt het apparaat updates? ‘Vraag ernaar bij de verkoper’, adviseert ethisch hacker Sijmen Ruwhof.
- Vraag ook wie aansprakelijk is mocht er iets misgaan.
- Koop je het product? Lees dan het instructieboekje, verander meteen het wachtwoord en installeer regelmatig updates.
- Zet het slimme apparaat op een apart deel van je thuisnetwerk, dus niet op hetzelfde netwerk als de computer. Op een gastnetwerk bijvoorbeeld.
- Slimme apparaten moet je onderhouden, beheren. Ruwhof: ‘Vind je dat te ingewikkeld? Vraag dan een it’er. Of koop het product niet.’

BRONNEN: ETHISCH HACKER SIJMEN RUWHOF EN AGENTSCHAP TELECOM

→

‘Het groeit de overheid ook boven de pet. Het internet is het Wilde Westen’

Agentschap Telecom geeft het voorbeeld van een slimme thermostaat. Een hacker die toegang heeft tot de thermostaat, kan op afstand iemands verwarming aan- of uitzetten. ‘Maar hij heeft ook waardevolle informatie over wanneer iemand thuis is of afwezig’, zegt Jasper Nagtegaal, projectmanager toezicht cybersecurity van het agentschap.

Een hacker heeft niet altijd lang nodig voor een hack. ‘Het ligt helemaal aan het slimme apparaat hoe lang dat duurt’, zegt Ruwhof. ‘Gerenommeerde leveranciers zijn veel beter in veiligheid dan startende bedrijven. Een ervaren hacker kan vaak al in een paar dagen een ernstig lek vinden in een slim apparaat dat net op de markt is. In nog eens een paar dagen kunnen hackers het internet scannen op alle kwetsbare apparaten van hetzelfde merk. Dat gebeurt geautomatiseerd. Je hebt zelfs openbare websites die het internet voortdurend scannen op lekke apparaten. Die zijn een soort Google voor hackers. Als een hacker alle apparaten wil van beveiligingscamera x of harde schijf y, dan krijgt hij daarvan een lijst met IP-adressen. Die apparaten kan hij dan aanvallen en overnemen. Het is schrikbarend dat dat kan. Maar ook logisch, want niemand die het opruimt. Die lijsten met lekke apparaten heeft de politie ook, maar die kan of doet vaak niets: niet het mandaat, de menskracht of de expertise ervoor.’

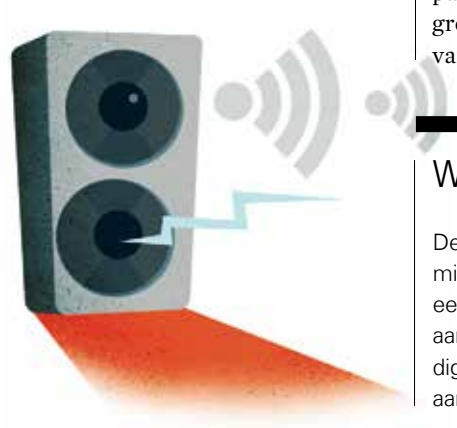
Wachtwoorden en naaktfoto’s

Meestal verzamelen hackers zo massaal gegevens van mensen, zoals wachtwoorden en creditcardgegevens, die ze op internet verkopen aan andere hackers en fraudeurs. ‘Die maken er vervolgens misbruik van’, zegt Ruwhof. ‘Hackers hebben vaak een specialisatie. Een specialist in afpersing gaat op zoek naar gegevens waarmee hij mensen kan afpersen. Naaktfoto’s bijvoorbeeld.’

Hackers kunnen ook de internetverbinding van gehackte apparaten gebruiken om websites en internetplatforms aan te vallen. Via grote DDoS-aanvallen met honderdduizenden slimme apparaten leggen ze dan bijvoorbeeld grote webwinkels, DigiD of websites van banken plat. Als eigenaar van de apparaten merk je daar meestal niks van. Je merkt alleen dat je niet kunt inloggen bij de instelling die slachtoffer is van zo’n aanval.

Volgens Ruwhof wordt het allemaal veel te ingewikkeld voor de consument. ‘Het is een wereld waarop mensen geen zicht hebben, waarover ze geen controle hebben’, zegt hij. ‘Veel slachtoffers weten niet dat ze al jaren gehackt zijn. En het groeit de overheid ook boven de pet. Bijna alles hebben we in het leven buiten het internet goed geregeld. Op het internet niet. Het is het Wilde Westen. En de impact ervan op ons leven wordt steeds groter.’

Huiseigenaren hebben lang niet altijd meer een keuze of ze apparaten in huis willen met een internetverbinding. ‘Overheid en energiemaatschappijen willen alle huishoudens uitrusten met een slimme energiemeter en de standaard televisie is tegenwoordig een smart-tv’, schrijft het Rathenau Instituut in het rapport: ‘Een nooit gelopen race, over cyberdreigingen en versterking van weerbaarheid’. ‘Maar voor de doorsnee burger is het onbegonnen werk om de beveiliging van deze apparaten voor zijn rekening te nemen.’ Mensen kunnen het nu al niet aan en



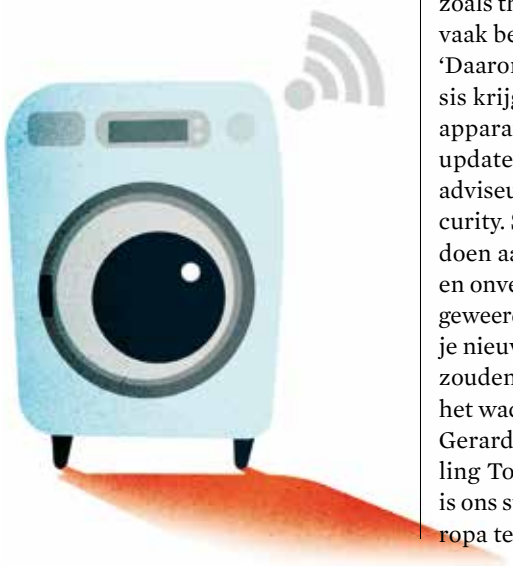
Wegenkaart

De ministeries van Justitie en Economische Zaken kondigden in het voorjaar een ‘roadmap’ veilige hard- en software aan. Daarin staan maatregelen die de digitale veiligheid van hard- en software aanzienlijk moeten verbeteren.

95 miljoen

In het regeerakkoord is structureel 95 miljoen euro gereserveerd voor cybersecurity. Een deel van dat geld wordt ingezet voor voorlichtingscampagnes.

‘Regelmatige software-updates zijn net zo belangrijk als een goed wifi-wachtwoord’



hebben al moeite om hun computer of smartphone goed te beveiligen. Daarom moeten overheid en bedrijfsleven volgens Rathenau hun verantwoordelijkheid nemen.

Agentschap Telecom, dat onder het ministerie van Economische Zaken valt en toezicht houdt op het veilig gebruik van apparaten en digitale infrastructuur zoals het internet, is het daarmee eens. Gebruikers weten vaak niet welke apparaten veilig zijn en welke niet, stelt het agentschap. En slimme apparaten zoals thermostaten en koelkasten zijn vaak bedoeld voor jarenlang gebruik. ‘Daarom moet het een wettelijke basis krijgen dat de software in slimme apparaten een bepaald aantal jaren updates krijgen’, zegt Paul Wijninga, adviseur *internet of things* en cybersecurity. Slimme apparaten moeten voldoen aan minimum beveiligingseisen en onveilige apparatuur moet worden geweerd van de Europese markt. ‘En als je nieuwe apparaten uit de doos haalt, zouden ze pas mogen werken nadat je het wachtwoord hebt aangepast’, zegt Gerard Kuipers, adviseur bij de afdeling Toezichtbeleid en Sancties. ‘Dat is ons streven. We proberen het in Europa te regelen. Daarvoor hebben we voorstellen ingediend bij de Europese Commissie.’

Sterk wachtwoord

Huiseigenaren die een slim apparaat willen kopen, kunnen in ieder geval een aantal dingen zelf doen (zie kader ‘Koop verstandig’).

Is het hele probleem niet te voorkomen met een goed wifi-wachtwoord? ‘Nee’, zegt Ruwhof. ‘Een goed wifi-wachtwoord is natuurlijk belangrijk, maar het is net zo belangrijk regelmatig software-updates op je router te installeren. Ik ken bijna niemand die dat doet. En het idee van veel slimme apparaten is dat je ze ook met je smartphone kunt bedienen als je niet thuis bent. Ze worden met hun publieke IP-adres aan het internet verbonden, niet per se aan wifi. Dus het apparaat zelf heeft ook een sterk en uniek wachtwoord nodig.’

Op laatjeniethackmaken.nl geeft Sijmen Ruwhof met vijf andere ethisch hackers tips voor hoe je als consument veilig kunt blijven op het internet. ■

dit vindt de vereniging

De vereniging vindt de groei van het aantal onveilige slimme apparaten voor in huis zorgelijk. ‘De beveiliging van deze apparaten kan niet overgelaten worden aan consumenten’, zegt Nico Stolwijk, manager Belangenbehartiging. ‘Het is belangrijk dat er aandacht is voor regelgeving, een goede beveiliging en het weren van onveilige apparatuur.’

Doe maar een slim huis

49 procent van de Nederlanders is geïnteresseerd of zeer geïnteresseerd in een slim huis, blijkt uit onderzoek van bureau GfK. Dat is minder dan vorig jaar, toen was dat nog 59 procent.

Angst voor hacks

De grootste belemmeringen om slimme oplossingen voor in huis aan te schaffen zijn de kosten (41 procent) en de toegenomen zorgen over hacken en privacy (beide 36 procent).