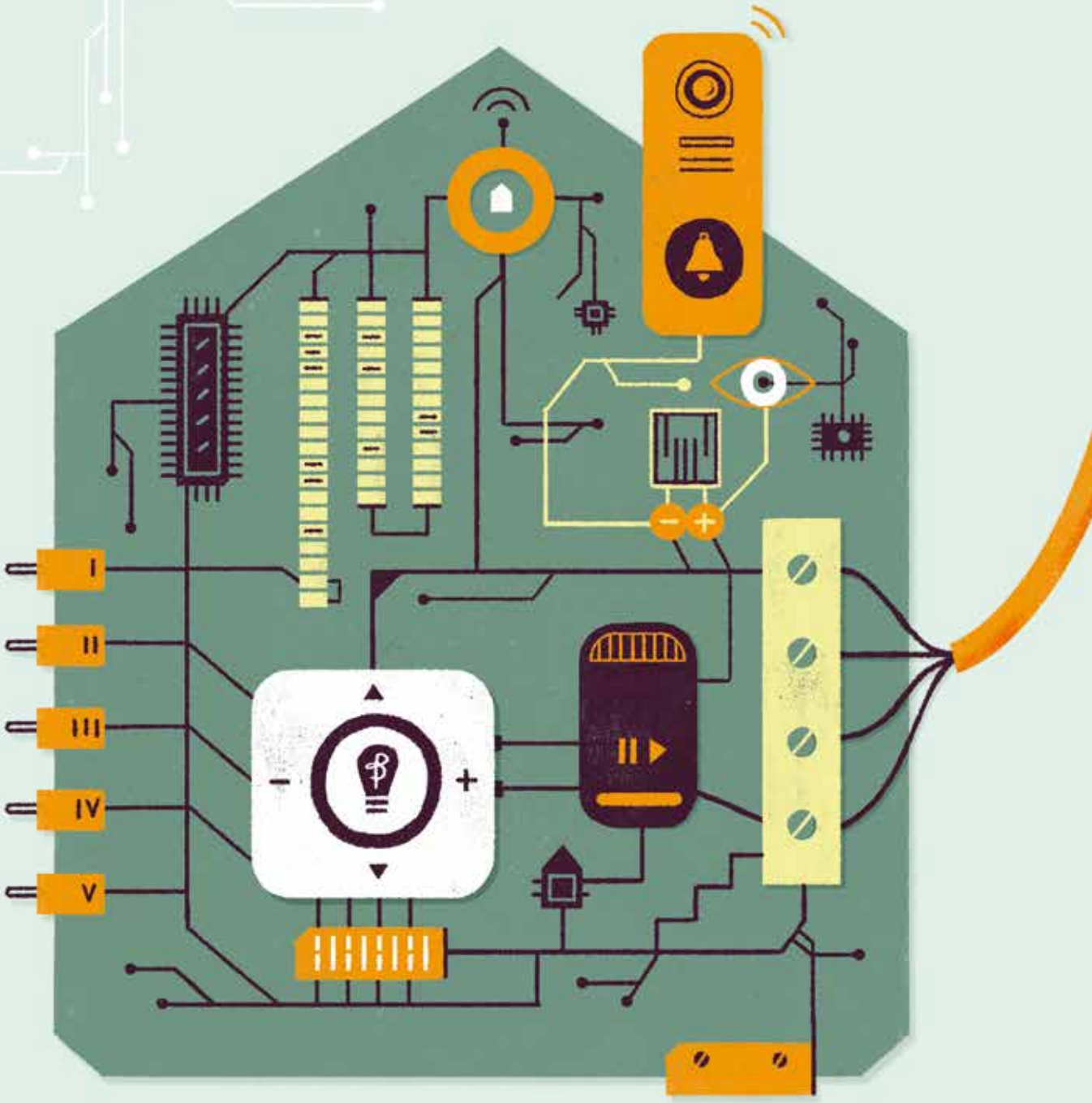


De gemakken en risico's van domotica

Hé Google

Domotica maakt het leven comfortabeler, makkelijker, energiezuiniger en veiliger. Hoewel u bij dat laatste vraagtekens kunt zetten. Want wie slimme apparaten in huis haalt die zijn gekoppeld met het internet, moet zich bewust zijn van de beveiligingsrisico's.

TEKST **SANDRA VAN DER HORST** BEELD **ANNEMARIE GORISSEN**

Gemak en comfort zijn belangrijke drijfveren om van de woning een smarthome te maken. Met één druk op de knop de gordijnen dicht en de lichten aan. Of zelfs zónder knop, gewoon wanneer het donker wordt. Wanneer u zelf niet thuis bent, werkt deze aanwezigheidssimulatie tevens preventief tegen inbraak. Handig! Bij de slimme thermostaat en de slimme deurbel zijn kostenbesparing en extra veiligheid de meest genoemde redenen bij de aanschaf, wijst onderzoek van Centraal Bureau voor de Statistiek (CBS) uit. Een slimme woonomgeving geeft comfort, bespaart energie, kan de veiligheid vergroten en ondersteuning bieden bij alledaagse zaken. Door de snelgroeiende hoeveelheid technische mogelijkheden kan een slimme woning ook zélf van alles waarnemen en kan de aanwezige technologie zelfstandig hulp bieden. Melk op? De koelkast geeft een seintje aan het online boodschappenlijstje en zo wordt het pak melk automatisch bezorgd.

Meer dan 8 op de 10 Nederlanders van 12 jaar of ouder hebben thuis een of meer slimme apparaten of systemen die met het internet zijn verbonden. Dat blijkt uit cijfers van CBS. Meestgebruikt zijn de smart-tv (60 procent) en slimme water-, gas- of elektriciteitsmeters (55 procent), gevolgd door een virtuele assistent via een app, audiosysteem of smartspeaker (39 procent). De categorieën verlichting, beveiliging en huishoudelijke apparatuur zijn tussen 2020 en 2022 ongeveer verdubbeld, zo wijst het CBS-onderzoek 'ICT-gebruik van huishoudens en personen 2022' uit. →

Goed om te weten

Vereniging Eigen Huis neemt cyberdekking binnenkort standaard op in de inboedelverzekering. Deze dekt cyberincidenten zoals diefstal van geld van uw rekening en identiteitsdiefstal. Dataherstel en vervanging van hardware wordt vergoed en u kunt gebruikmaken van de Cyberwacht. Deze geeft advies bij bijvoorbeeld cyberafpersing, maar kunt u ook bellen als u verzekerde apparatuur wilt beveiligen of wel wat hulp kunt gebruiken bij het installeren van beveiligingssoftware.

Meer informatie:
eigenhuis.nl/ehm-cyb

Wat zijn domotica en IoT?

Het woord domotica is een samentreksel van het Latijnse domus (huis) en tica, hetgeen toegepaste leer of wetenschap betekent.
Domotica is de integratie van technologie en diensten die de kwaliteit van leven en wonen moet verhogen. De eerste domoticatoepassingen zijn afkomstig uit de geautomatiseerde industrie of kantooromgeving en werden ingezet voor mensen met een functiebeperking. Op deze manier werd hun autonomie verhoogd en zelfstandig leven beter mogelijk gemaakt. Denk aan personen in een rolstoel die door domotica de belangrijkste huiselijke taken zelf konden uitvoeren.
Naast domotica wordt het begrip smarthome veel gebruikt. Het internet der dingen (ook wel Internet of Things of IoT) is het geheel aan slimme apparaten dat via internetverbindingen met andere apparaten of systemen in contact staat en daarmee gegevens uitwisselt. Zónder menselijke inmenging. Hierbij wordt het internet niet door mensen gebruikt maar door de apparaten zelf. Mogelijk zullen in de toekomst door mensen bediende computers, zoals laptops en smartphones, in de minderheid zijn op het internet. De meerderheid van de internetgebruikers zal dan uit slimme apparaten bestaan.

Het gebruik van slimme apparaten in huis neemt dus fors toe. Toch is er volgens het CBS ook een kleinere groep die thuis geen slimme apparaten gebruikt. Een ruime meerderheid daarvan zegt daar gewoonweg geen behoefte aan te hebben, maar 25 procent van de respondenten geeft aan dat ze zich zorgen maakt over de privacy en beveiliging. Volgens Guido Visman, verbonden aan de Universiteit van Groningen als docent IT-recht en facultair privacy & security coördinator, is dat deels terecht. “Bij domotica roep ik gelijk Internet of Things. (Ook wel IoT, zie kader, red.) Alle slimme apparaten die je in huis haalt, zijn uiteindelijk verbonden met het internet. IoT is een beetje een ondergeschoven kindje in privacyland. Het zijn in feite gewoon sensoren in allerlei soorten en maten die gegevens verzamelen en verwerken om hun taak uit te voeren. Daarvan wordt een deel lokaal, in je huis, verwerkt, maar er is ook altijd een verbinding met de leverancier. Dat is gemakkelijk en goedkoop, want zo kan de leverancier op afstand bijvoorbeeld updates doen.” Met deze externe internetverbinding ontstaat het veiligheidsrisico. Visman: “Als zo’n slim apparaat is geïnstalleerd dan komen de meeste gebruikers er niet meer aan. Er wordt onvoldoende gekeken naar de juiste instellingen en het fabriekswachtwoord blijft vaak onveranderd.” Omdat het gros van de gebruikers geen actief beheer op deze apparaten voert, kunnen kwaadwillenden zich dan makkelijk een ingang verschaffen tot de data van deze systemen. “Hoe vaak gebeurt het niet dat op bijvoorbeeld de router, waarmee het internet je woning in komt, nog de standaardinstellingen van KPN staan? Te vaak!”, beantwoordt Visman, die eerder lang in de IT-business werkzaam was en zich daarna omschoolde tot jurist, zijn eigen vraag. En als iemand eenmaal via die router binnen is, zijn ook alle verbonden systemen gemakkelijk te bereiken, zoals de domotica.

Aftappen

Maar hoe groot is dat risico dan? En wie is er eigenlijk geïnteresseerd in die gegevens? Uit het onderzoek van het CBS blijkt dat een kleine groep mensen (vijf procent) te maken had met beveiligings- of privacyproblemen door een hack van een apparaat of systeem, of doordat gegevens zonder toestemming zijn gedeeld. Een hacker heeft volgens Visman normaal gesproken alleen belang om via domotica bij iemand in huis binnen te komen als hij het persoonlijk heeft gemunt op die persoon. Dat risico is erg klein. “Maar als op grote schaal gegevens automatisch worden afgetapt, kunnen er profielen worden gemaakt van wijken en mensen. Met deze data kunnen leveranciers hun producten verbeteren, maar je zou er ook gedrag van mensen mee in kaart kunnen brengen, zelfs tot individueel niveau. Leveranciers en overheden zijn geïnteresseerd om patronen te herkennen waar ze iets mee zouden kunnen. En dan wordt

het spannend. Er kán dan sprake zijn van serieuze inbreuk op de privacy", vertelt Visman.
Jos Boerties, hoofd systeemtoezicht bij toezichthouder Autoriteit Persoonsgegevens ziet meerdere risico's: "We beseffen vaak niet dat deze slimme apparaten een goudmijn kunnen zijn voor cybercriminelen die bijvoorbeeld een ransomware-aanval (gijzelsoftware, red.) willen uitvoeren. Met de gegevens van klanten die zij aftappen, kunnen ze druk zetten op de producent van het product of de klanten en dreigen deze gegevens openbaar te maken." Ook wijst Boerties op een gebeurtenis die het nieuws haalde omdat een producent zijn slimme camera's niet goed had beveiligd: "Toen konden mensen niet alleen hun eigen camerabeelden zien, maar ook die van anderen. Het bleek dat de videogegevens naar de cloud werden geüpload, zelfs wanneer de gebruiker hiervoor toestemming weigerde. Ook werd op deze beelden gezichtsherkenning toegepast."

Zorgvuldig gebruik

Hoewel Visman het risico klein acht en wil benadrukken dat slimme apparaten absoluut niet eng zijn en juist heel veel voordelen bieden, pleit hij voor verstandig en zorgvuldig gebruik. Het veranderen van het wachtwoord en, als dat kan, de gebruikersnaam is een van de stappen in het beveiligen van nieuwe apparatuur. Blijf nooit een door een fabrikant ingesteld wachtwoord gebruiken. Bestudeer de instellingen, voer (beveiligings)updates altijd zo snel mogelijk uit en voer goed en actief beheer op uw wachtwoorden. Wie dat niet doet, maakt zichzelf extra kwetsbaar voor de risico's.
Boerties vult aan: "Ga daarbij ook het gesprek aan met de andere mensen in huis. Het is belangrijk dat je samen een bewuste keuze maakt over wat je in huis haalt en waarvoor. Als je alles in huis slim maakt, kunnen best veel dingen meeluisteren met wat je doet. Een slimme luidspreker die je opdrachten kan →

> "Ga het gesprek aan met huisgenoten. Het is belangrijk dat je samen een bewuste keuze maakt over wat je in huis haalt en waarvoor"

“Filmt u binnenshuis of buiten dan moet u bezoekers, denk daarbij ook aan de schoonmaakster of hovenier, daar duidelijk op wijzen”

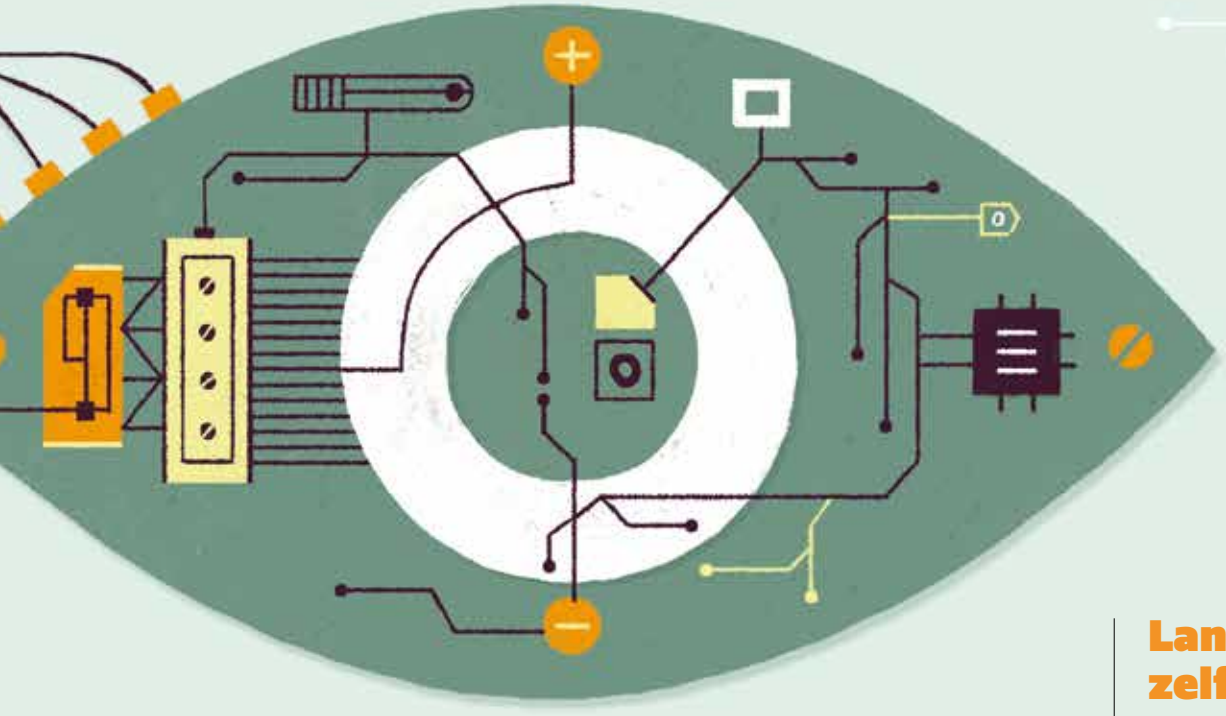
geven door je verzoek bijvoorbeeld te beginnen met ‘Hé Google’. Is die wel nodig? Je kunt ook kiezen voor een luidspreker op bluetooth zónder spraakherkenning. Zo kun je samen met je huisgenoten de risico’s afzetten tegen het gebruiksgemak.”

Senioren

Voor een oudere doelgroep is domotica extra interessant. Senioren kunnen slimme apparaten gebruiken om langer zelfstandig te blijven wonen (zie kader). Tegelijkertijd is het voor deze doelgroep een uitdaging om al deze systemen te begrijpen en regelmatig van een nieuw wachtwoord te voorzien. Visman: “Wat mij betreft ligt hier een verantwoordelijkheid bij de leveranciers. Zij zijn volgens het transparantiebeginsel in de privacywetgeving verplicht om goed uit te leggen hoe ze met persoonsgegevens omgaan en hoe hun producten precies werken. De medewerkers die de domotica komen aanleggen, zouden ter plekke de standaardinstellingen kunnen verwijderen en de gebruiker uitleggen hoe ze persoonlijke wachtwoorden invoeren en vertellen dat ze deze regelmatig moeten vervangen. Dit kost tijd en geld en zie ik leveranciers niet op eigen houtje oppakken.” Boerties beaamt dat: “Soms worden bedrijven pas wakker als het misgaat. Het is erg jammer dat ze daarna pas tot de juiste maatregelen komen. Ons team bij de Autoriteit Persoonsgegevens geeft voorlichting en benadrukt bij de verschillende sectoren, waaronder de domotica-producenten, dat ze aan de voorkant een goede privacy-check moeten doen voordat ze iets op de markt brengen.” Visman denkt hardop mee: “Brancheverenigingen kunnen hun leden ook stimuleren hun zorgplicht te vervullen. En de overheid kan helpen door meer regeldruk uit te oefenen. Aan de andere kant: hoe ga je dat handhaven? Veel meer regels hebben vaak geen zin als niemand daar op toeziet.”

Zelf privacy schenden

Bij het inzetten van domotica kunt u de dupe worden van inbreuk op uw privacy, maar u kunt ook zélf de privacy van andere schenden. Bewoners met een slimme deurbel of een camera mogen enkel filmen tot de erfgrens. Visman legt uit: “Zodra je een camera ophangt, ben je in juridische zin verwerkersverantwoordelijke voor de beelden.” Filmt u binnenshuis of in de tuin dan moet u bezoekers, denk daarbij ook aan de oppas, schoonmaakster of hovenier, daar duidelijk op wijzen.



In de praktijk blijkt dat veel woningeigenaren wél filmen buiten hun erfgrens. En dat de politie hier bij opsporing en onderzoek maar wat graag gebruik van maakt. Is dat dan geen onrechtmatig verkregen bewijs? “De politie opereert onder een ander wettelijk regime: de Wet politiegegevens. Omdat de politie opsporingstaken heeft, mogen ze op een andere manier omgaan met verkregen persoonsgegevens. De strafrechter kan besluiten deze gegevens vervolgens te gebruiken in het belang van de zaak”, verduidelijkt Visman.

Bent u het niet eens met hoe een bedrijf met uw persoonsgegevens omgaat? Heeft u de indruk dat u onrechtmatig wordt gefilmd door een buurtbewoner? Of maakt u zich zorgen over de naleving van de privacywetgeving door organisaties in het algemeen? Dan kunt u bij de Autoriteit Persoonsgegevens, nadat u eerst hebt geprobeerd er zelf uit te komen met de betreffende partij, een klacht indienen. Tippen, al dan niet anoniem, kan overigens ook. Helaas komen er zóveel klachten binnen dat de medewerkers van de Autoriteit Persoonsgegevens meldingen noodgedwongen moeten prioriteren. De meeste aandacht gaat daarom uit naar grote zaken. Voelt u zich aangetast in uw privacy door de camera van de buren? Ga dan allereerst zélf het gesprek aan. Boerties: “Soms blijkt dan al dat de buren hun camera *blurren* buiten de erfgrens of zijn ze bereid hun camera bij te stellen. Wie er gezamenlijk niet uitkomt, kan ook nog een beroep doen op buurtbemiddeling. Daarna kunnen consumenten eventueel juridische stappen nemen door bijvoorbeeld een klacht in te dienen bij de Autoriteit Persoonsgegevens.” Bedrijven of personen die niet gerechtvaardigd beeldmateriaal verzamelen kunnen van de Autoriteit Persoonsgegevens een waarschuwing en uiteindelijk een boete krijgen.

Langer zelfstandig wonen met domotica

Domotica kan in het bijzonder een uitkomst bieden aan senioren. Met slimme apparaten is het namelijk mogelijk om langer zelfstandig te blijven wonen. Waar kunt u dan aan denken? Lees er meer over op **eigenhuis.nl/ehm-slim**. Op deze pagina vindt u ook een verwijzing naar de Autoriteit Persoonsgegevens met een linkje naar veelgestelde vragen rondom de beveiliging van IoT.

eigen huis magazine

LID WORDEN?
MEER INFO OP

EIGENHUIS.NL/ LID-WORDEN

MEER ARTIKELEN LEZEN?

Word lid van Vereniging Eigen Huis en krijg net als alle 800.000 leden Eigen Huis Magazine in de brievenbus. Hierin leest u alles over het kopen, verkopen, verbouwen en verduurzamen van uw huis

PROFITEER VAN DE VOORDELEN VAN HET LIDMAATSCHAP

- Gratis advies en informatie van onze experts. Zoals checklists, voorbeeldbrieven en e-books.
- Exclusieve dienstverlening voor een aantrekkelijk tarief.
- Lagere woonlasten door collectieve inkoop.
- 10 x per jaar Eigen Huis Magazine.
- Wij zijn uw stem in Den Haag om woningbezit duurzaam en betaalbaar te houden.

Vereniging Eigen Huis is dé consumentenorganisatie die opkomt voor de belangen van (toekomstige) huiseigenaren.
Meld je aan op **eigenhuis.nl/lid-worden** of bel 033 450 77 50.

vereniging eigen huis | sta sterker