



Apparaat uit de test:
Google Home Mini
(slimme speaker)

Een huis vol slimme spionnen?

Experiment: 4 weken 'smart' apparaten in huis

Een 'smart home' vol slimme apparaten maakt je leven makkelijker, is de belofte. Maar is dat ook echt zo? Redacteur-onderzoeker Celine Burgering nam een maand lang de proef op de som, terwijl ethisch hackers onderzochten wat die apparaten via internet doorsturen. Ze schrok van de resultaten.

Tekst: **Celine Burgering** /cburgering@consumentenbond.nl

Apparaat uit de test:
HP Envy 5030
(wifiprinter)



Negen apparaten gaan de komende maand taken van mij overnemen, van slim espressoapparaat en babycam tot wifiprinter en slimme lampen. Ik kijk uit naar al het gemak dat mijn slimme apparaten me gaan bieden, want mijn leven is met man, twee kinderen en een drukke baan best hectisch. Het lijkt me wel wat als ik niet meer hoeft te stofzuigen, er koffie voor me wordt gezet en ik al die apparaten met een smartphone-app vanuit mijn luie stoel kan bedienen.

Maar al die apparaten zijn ook continu met internet verbonden en sturen gegevens naar de fabrikant. Wat komen zij allemaal van mij te weten? En zijn die apparaten wel bestand tegen hackers? Om daar achter te komen schakelen we ethisch hackers in van beveiligingsspecia-

Feiten & cijfers

DE DATA ZIJN GEBASEERD OP
6 VAN DE 9
APPARATEN



De apparaten:
→ twee Google Homes
→ twee camera's
→ robotstofzuiger
→ printer





Celine Burgering met haar gezin

Apparaat uit de test:
Blaupunkt Bluebot
Xsmart (stofzuiger)

Over het onderzoek

Redacteur-onderzoeker Celine Burgering gebruikte thuis van 6 juni tot 4 juli negen slimme apparaten. Ze koos apparaten waarvan ze de meeste toegevoegde waarde verwachtte. Ze spitte de privacyverklaringen door en beschreef haar ervaringen. Ethisch hackers van beveiligingsbedrijf Nixu taptten de gegevens en checkten of er privacygevoelige gegevens tussen zaten, zoals wachtwoorden, cookies en andere data die zijn te herleiden naar personen, of informatie die iets prijsgeeft over de samenstelling of de leefpatronen van het gezin. Nixu heeft ook geprobeerd of het mogelijk is om versleutelde datastromen alsnog te ontcijferen via een 'Man in the Middle (MiTM)' aanval: dan wurmt de hacker zich tussen de apparaten en de server op internet.

list Nixu onder leiding van Mattijs van Ommeren. Zij houden in de gaten wat er op de achtergrond gebeurt.

Trage start

Ik heb er een dag voor nodig gehad om mijn huis slim te maken. Eerst moet ik voor elk apparaat een app downloaden, accounts aanmaken en wachtwoorden verzinnen. Dan moet ik de apparaten installeren. De beveiligingscamera had ik

zo aan de praat, maar het koppelen van mijn verlichting aan de Google Home vergde meer handelingen. Dan heeft elke fabrikant ook nog zijn eigen privacyverklaring. Normaal scan ik die eventjes, maar voor dit experiment lees ik ze alle negen goed door – bij elkaar zo'n 100 pagina's. Ik lees dat er geen gegevens met 'derden' worden gedeeld, maar vaak wel met 'partners'.

En met servers in allerlei landen, weet →

Aantal servers
die data
ontvingen

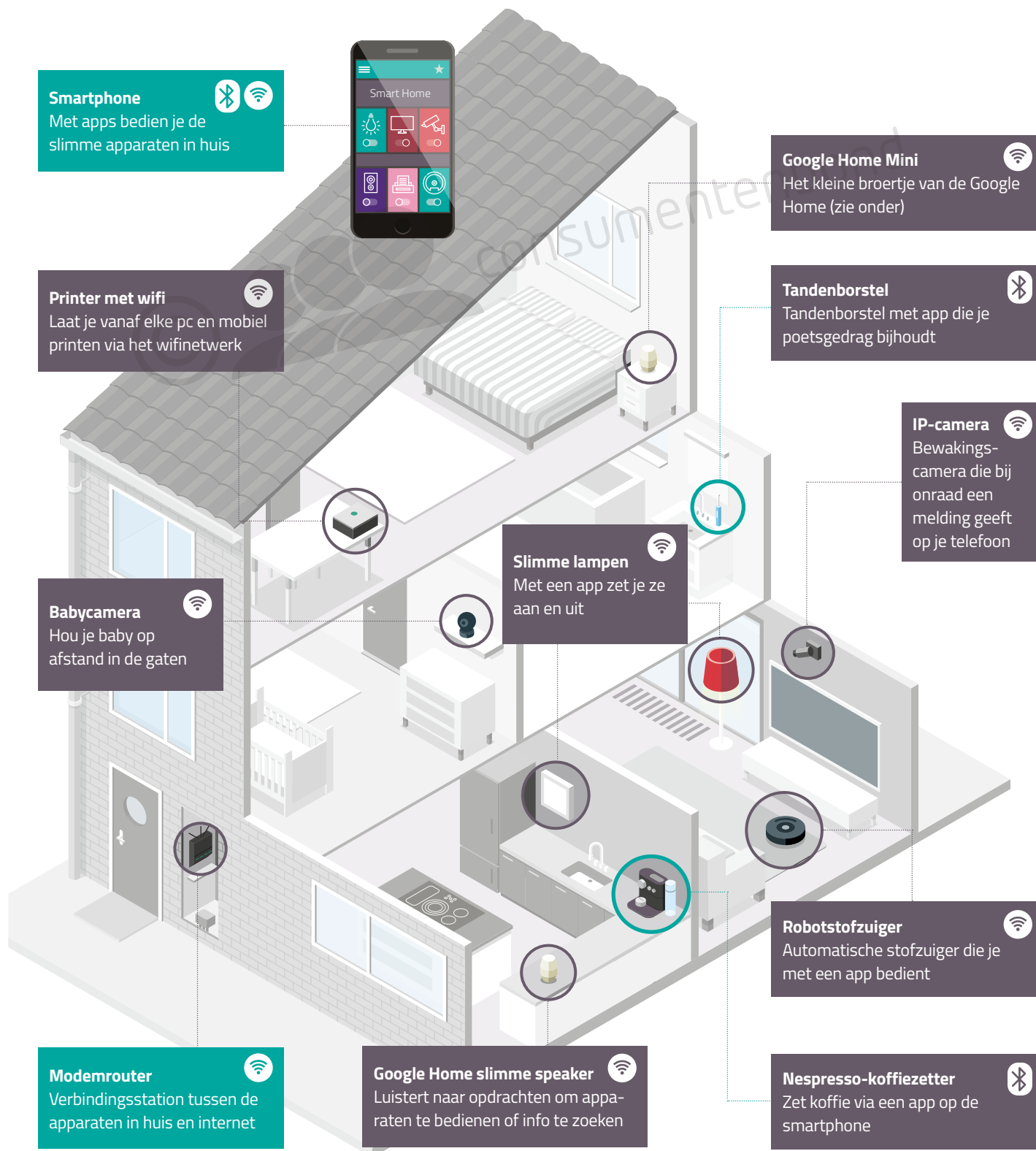
339



DE SERVERS
WAREN
VERSPREID
OVER
9 LANDEN



Celines 'smart home' in beeld



Mattijs: 'Jouw beveiligingscamera stuurt data naar vijf landen. Naar China, Ierland, Nederland, Singapore en de VS. Dat komt doordat veel fabrikanten de digitale diensten die nodig zijn om het apparaat *smart* te maken over de hele wereld bij elkaar scharrelen. Vervolgens worden de data ook naar al die bedrijven gestuurd.' Ik ben nog niet begonnen of er zit al een deuk in mijn gevoel van privacy.

Hub en skill

Nu ik al mijn slimme apparaten aan de praat heb gekregen, wil ik nog een stap verdergaan. Ik haal de Google Home in huis om mijn slimme apparaten met spraakopdrachten te gaan bedienen. Om hem aan de praat te krijgen, is alleen makkelijker gezegd dan gedaan.

Om mijn slimme Ikea-lampen aan en uit te kunnen zetten, heeft Google Home een extra apparaat nodig: een hub. Ook die installeren gaat niet vanzelf, want daarvoor is een zogenoemde skill (een soort extensie) nodig die ik in de Google Home-app moet inschakelen. Een app, een hub en een skill verder kan ik uiteindelijk mijn lampen bedienen. Behalve die met dimmers, want daar kunnen de slimme Ikea-lampen niet mee omgaan.

Mattijs weet nog te melden dat de veiligheid rammelt van de verbinding van de Ikea-lampenapp: 'Als de app wordt gebruikt in een onvertrouwd netwerk, bijvoorbeeld een publieke wifihotspot, kan een hacker jouw lampen bedienen.' Dat gevaar is gelukkig niet zo groot, maar ik word er niet bepaald vrolijk van.

Meer mis

De Ikea-lampenapp is niet de enige met een veiligheidsprobleem. Dit geldt ook voor de apps van mijn tandenborstel,

Slim huis verzamelt continu data



espressomachine, stofzuiger en baby-camera.

Mattijs: 'Geen van deze apps gebruikt "certificaatvalidatie". Het verkeer is wel versleuteld, maar er wordt niet gecontroleerd of de encryptiesleutel wel bij de verzender hoort. Een hacker kan zich met een vals certificaat tussen het verkeer nestelen en de besturing overnemen.' De reden: haast. 'Fabrikanten willen snel nieuwe apparaten op de markt brengen, en beveiliging is een sluitpost. In het gunstigste geval is het onwetendheid, maar het woord nalatigheid zou beter op zijn plaats zijn.'

Spontaan aan

Tussen de installatiesores en de privacy-zorgen is er ook tijd voor humor. Ook al spreken we nog Engels met Google – een Nederlandstalige versie komt eraan – het is indrukwekkend hoe gevat Google soms reageert op onze opdrachten.

De kinderen vragen de Google Home om dierengeluiden te maken, tot 100 te tellen en grappige kattenfilmpjes af te spelen op de tv. Ze vinden de robotstof-

Van de 6 apparaten waarvan we meetgegevens hebben, stuurden er 5 lange periodes elk uur, dag en nacht, gegevens door. Alleen de robotstofzuiger hield zich vaak geïd.



29
dagen
duurde
de test



Totaal aan
data naar buiten
verstuurd
378 MB

De iBaby stuurde
de data naar liefst
215 verschillende
servers in 5 landen



Apparaat uit de test:
Klikaanklikuit IPCAM-2000
(beveiligingscamera)



Maak je slimme huis veiliger

→ Kies sterke wachtwoorden voor je (modem)router en je apparaten en hun accounts.

Minstens 12 tekens met zowel cijfers als hoofd- en kleine letters en het liefst ook leestekens. Als het even kan, zijn ze verschillend voor alle apparaten en accounts. In een slim huis wordt dat snel onoverzichtelijk, installeer daarom een wachtwoordmanager op je computer en telefoon.

→ Verander de naam van je wifinetwerk.

De standaardnaam van je draadloze netwerk bevat vaak het typenummer van de router of de naam van je provider. De naam moet niet te herleiden zijn naar je huis.

→ Doorloop het hele installatieproces.

Sla geen stappen over, ook al gebruik je de slimme functies van een apparaat niet. Zo zorg je dat in ieder geval de aanbevolen veiligheidsinstellingen zijn geactiveerd.

→ Houd je apparaten up to date.

Ga zelf regelmatig op zoek naar updates. Fabrikanten wijzen je er vaak niet op.

→ Schakel WPS, Remote Access en UPnP uit je modemrouter.

Zo maak je het hackers moeilijker om toegang te krijgen tot je thuisnetwerk en je apparaten.

→ Gebruik het gasten-netwerk.

Veel draadloze routers hebben de mogelijkheid voor het instellen van een gastennetwerk. Daarop kunnen apparaten wel toegang hebben tot internet, maar niet tot je privénetwerk. Dit is een prima manier om je slimme apparaten aan te sluiten.

→ Pas extra op met (te) goedkope of merkloze apparaten.

De kans is groter dat fabrikanten weinig aandacht hebben besteed aan de veiligheid van de producten. Maar ook bij duurdere apparaten is de veiligheid niet altijd in orde.

zuiger schattig, maar van de Google Home zijn ze nog meer onder de indruk. De Google Home Mini gebruiken we als intercom. Vertel je Google dat het eten klaar is, dan horen de kinderen boven 'Dinner's ready, come and get it!'. De nieuwe generatie is slim en stuurt terug: 'No, thank you'.

Er gebeuren ook vreemde dingen. Op willekeurige momenten springt de Home spontaan aan, zonder dat ik activeer met 'Oké, Google'. Word ik afgeluisterd? Google-woordvoerder Rachid Finge laat weten dat de Google Home soms ten onrechte even aanslaat omdat hij denkt 'Oké Google' te horen. Dat moet beter worden als Google Home straks Nederlands verstaat.

Stress

Aan het begin van dit experiment keek ik nog uit naar alle tijd die mijn slimme huis me zou besparen. Dat pakt anders uit. De stofzuiger is geregeld de weg kwijt en ik krijg de ene melding na de andere. Ik moet om 12 uur 's middags m'n tanden poetsen, de espressomachine moet nú schoongemaakt worden en de babycam vindt dat de kinderkamer te warm is. De printer vraagt nóg een keer of ik geen abonnement wil op inktcartridges. Het witte-tandenprogramma schrijft voor dat ik minstens drie keer per dag moet poetsen. Eenmaal boven aangekomen, kan ik weer naar beneden: telefoon vergeten. Die heb ik namelijk ó-ver-al bij nodig. Ik begin me inmiddels af te vragen hoe mijn slimme huis me eigenlijk helpt.

Druk verkeer

Dat het doorlopend een drukte van belang is in mijn huis, is ook te

Apparaat uit de test:
iBaby M6S
(babycamera)



Van de 6 apparaten stuurden er 5 vrijwel elk uur - dagen nacht - gegevens door.



Alleen de robotstofzuiger hield zich vaak gedeisd

Apparaat uit de test:
Ikea Tradfri
(verlichting)

zien aan de datastromen. Er wordt continu data verstuurd door vrijwel alle apparaten, dag én nacht (zie de grafiek op pagina 13). De babycamera doet dat zelfs elke seconde. Is dat normaal? Mattijs: 'Nee, dat is helemaal niet nodig voor de stand-bystand. Apparaten moeten alleen in de gaten houden of er beweging is en of je tegen ze praat. Maar dat betekent niet dat alle gegevens naar allerlei servers gestuurd moeten worden.'

Van de babycamera heeft Mattijs het sterke vermoeden dat het om videobeelden gaat, maar daar komen we niet achter want de data zijn versleuteld en de fabrikant reageert niet op onze vragen. Hij ziet wel dat de versleuteling zwak is: 'een aanvaller die de moeite zou nemen, kan de beelden bekijken.'

Wachtwoord opgezogen

Waar ik wel blij van word, is dat ik de woonkamer niet meer hoeft te stofzuigen. Dat doet mijn Bluebot robotstofzuiger voor me. En ook al rijdt hij soms naar buiten als de achterdeur open staat, de hagelslag die mijn kinderen op de grond achterlaten, ruikt hij netjes op.

Maar de lach op mijn gezicht is snel verdwenen als Mattijs nieuws heeft over de stofzuigerapp. 'Uit de data blijkt dat de app jouw gegevens doorstuurt naar de fabrikant. Dat gebeurt wel versleuteld, maar die sleutel was eenvoudig te kraken. Ik heb je e-mailadres en wachtwoord kunnen onderscheppen.'

Al loop ik ook hiermee niet direct gevaar, mijn vertrouwen in mijn slimme

huis neemt nog verder af. De fabrikant laat weten snel met een oplossing te zullen komen.

Overbodige luxe

Als echte koffiedrinker had ik veel verwacht van mijn slimme Nespresso-apparaat. Dit blijkt de grootste teleurstelling. Ik kan geen temperatuur instellen en geen smaak of intensiteit kiezen.

Ja, ik kan met de app een kopje koffie zetten. Wauw. Op het apparaat zelf hoeft je alleen maar op een knop te drukken. Als we er een app bij doen, dan verkoopt het wel, lijken ze bij Nespresso gedacht te hebben.

Conclusie

Wat we weten na een maand, is dat de slimme apparaten continu gegevens verzenden. De ethisch hackers hebben weinig data echt kunnen inzien. Mattijs: 'We zagen wel dat die data vaak op een onveilige manier worden verstuurd, of met obscure protocollen waarvan we niet weten of die veilig zijn. Dit roept de vraag op hoe veilig er verder met de gegevens wordt omgegaan.'

Ik ben dus niet veel wijzer geworden, maar de fabrikanten waarschijnlijk wel. Wanneer je stofzuigt, je je tanden poetst of je lampen aan en uit doet, zegt veel over je levensstijl. Ik ben blij dat alle slimmigheid mijn huis inmiddels heeft verlaten. Tegen de tijd dat apparaten echt slim zijn, maar ook veilig en niet onnodig gegevens doorsturen, doe ik een nieuwe poging. Tot die tijd rust ik uit van een maand apparatenchaos.



Mattijs van Ommeren, ethisch hacker bij Nixu analyseerde de datastromen: 'De data worden vaak op een onveilige manier verstuurd.'

Apparaat uit de test:
Oral-B Genius 9000
(tandenborstel)



Ons standpunt

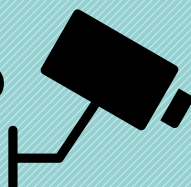
De Consumentenbond vindt dat slimme producten en diensten veilig, eerlijk en gemakkelijk in het gebruik moeten zijn én blijven. Fabrikanten moeten meer aandacht hebben voor veiligheid en privacy. Denk hierbij aan:

- het dataverkeer goed versleutelen
- het apparaat veilig houden.
- gegevens delen met 'derden' moet optioneel zijn

De Consumentenbond gaat de komende jaren ruim aandacht besteden aan dit onderwerp.

100%
In van alle meeturen stuurde minstens één apparaat data door

98%
In van alle uren werd minder dan 0,5 MB verstuurd



Uitschieter: de bewakingscamera verstuurd op 12 juni tussen 8 en 9 uur aan data

32 MB