Slimme apparaten: veilig tot de voordeur?

Hoe serieus gaan fabrikanten met veiligheid van slimme apparaten om?

Consumentenbond, januari 2020

Interactief

Om door de pagina's te bladeren klik je op de iconen ‹ / › om respectievelijk naar de vorige of volgende pagina te gaan. Om terug te gaan naar de inhoudsopgave klik je op ⌂ icoon. Bij de inhoudsopgave zijn de hoofdstukken aanklikbaar.

Samenvatting

Belangrijkste uitkomsten

1 19 van de 32 (bijna 6 op de 10) onderzochte slimme apparaten heeft een beveiligingsprobleem, 1 op de 4 zelfs een ernstig probleem.

2 Voor fabrikanten is het verhelpen van veiligheidsrisico's nog lang geen vanzelfsprekendheid. We rapporteerden in totaal 27 kwetsbaarheden aan fabrikanten, waarvan 14 ernstige. Zelfs van deze 14 ernstige kwetsbaarheden werden er slechts 9 opgelost.

Vanwege (1) en (2) is het des te belangrijker om als consument vooraf te weten of en hoe lang je product veiligheidsupdates krijgt, maar:

3 43 van de 50 fabrikanten geven online geen duidelijke informatie over hoe lang hun slimme producten nog (veiligheids)updates zullen krijgen - en dus veilig zullen blijven. Voor 11 van de 16 slimme productgroepen is er geen enkele belangrijke fabrikant die duidelijk vertelt hoe lang je updates krijgt.

Conclusie: fabrikanten nemen de veiligheid van slimme apparaten nog veel te weinig serieus

Inhoud

Wat wil de Consumentenbond?

Betere veiligheid wettelijk afdwingen

1 Fabrikanten mogen alleen slimme apparaten op de markt brengen die voldoen aan **minimale veiligheidseisen**.

2 Fabrikanten worden verplicht om slimme apparaten **gedurende de gehele gebruiksduur** te voorzien van veiligheids- en functionele updates.

3 Consumenten die schade lijden doordat hun slimme apparaat slecht beveiligd is, hebben **recht op schadevergoeding**.

Betere informatievoorziening

4 Bedrijven moeten consumenten **actief informeren** over kwetsbaarheden in hun slimme producten.

5 Consumenten moeten **eenvoudig kunnen controleren** of hun slimme producten onveilig zijn.

Handhaving

6 Onveilige producten moeten **van de markt afgehaald worden** en mogen pas weer de markt op als de fabrikant heeft aangetoond dat ze voldoen aan de minimale veiligheidseisen.

7 Er moet **stevige handhaving** komen op bovenstaande punten.

Over het onderzoek

Onderzoek veiligheid IOT-producten

De Consumentenbond voerde in 2019 4 vergelijkende productonderzoeken uit naar 32 slimme apparaten in 4 productgroepen waarbij ook de digitale veiligheid werd onderzocht (beveiligingscamera's voor buiten, slimme babycamera's, slimme deurbellen en slimme lampen).

Naast deze vergelijkende tests zijn in de tweede helft van 2019 in opdracht van de Consumentenbond nog eens 10 producten onderworpen aan een hacktest, waarvan we aanwijzingen hadden dat de veiligheid niet in orde was.

Onderzoek updatebeloften IOT-fabrikanten

Tot slot is in januari 2020 bij 50 fabrikanten met 16 slimme productgroepen onderzocht of zij consumenten over hun slimme apparaten vooraf toezeggen hoe lang deze producten nog (veiligheids)updates ontvangen.

Resultaten onderzoek veiligheid slimme producten

Deel 1
Resultaten vergelijkende tests 4 productgroepen

Wat is er getest?

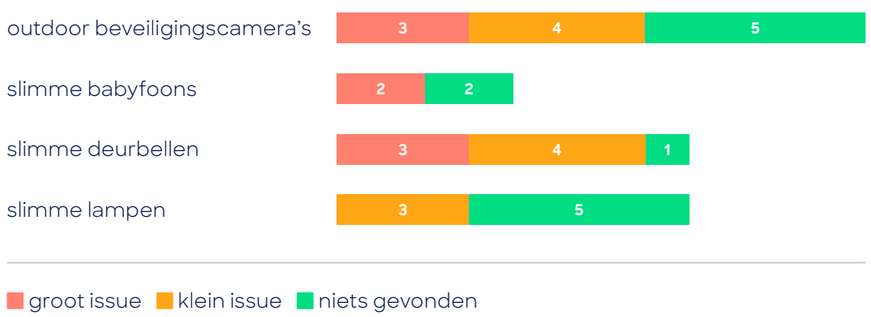
- 12 outdoor beveiligingscamera's, publicatie juli 2019
- Test 8 Slimme lampen, publicatie oktober 2019
- Test 8 slimme deurbellen, publicatie september 2019
- Test 4 slimme babycamera's (waaronder 1 app), publicatie december 2019

In totaal ging het om 32 producten van 22 verschillende merken.

Belangrijkste uitkomsten

- Bij 6 op de 10 slimme apparaten (19 van de 32 producten) is de beveiliging niet op orde, 1 op de 4 (8 van de 32) heeft zelfs een grote kwetsbaarheid. Dat wil zeggen dat een kwaadwillende hacker zonder al te veel moeite controle kan krijgen over het apparaat en/of toegang tot gevoelige gegevens.
- Zwakke beveiliging is een probleem dat breed speelt: van de 22 merken in de 4 vergelijkende tests, had meer dan de helft (13 van de 22 merken) één (of meer) producten met een kwetsbaarheid; bij 7 van de 22 merken was dit zelfs een groot issue.

Grafiek 1 Veiligheidsproblemen per test



Voorbeelden grote kwetsbaarheden:

1. UPnP (een manier om apparaten in huis direct met elkaar te laten communiceren) staat standaard open, waardoor in- en uitgaande poortjes naar de buitenwereld open staan.
2. Het gebruik van standaard gebruikersnamen en wachtwoorden, zeker eenvoudige als admin-admin
3. Er wordt helemaal niet om een wachtwoord gevraagd
4. Gevoelige / persoonlijke data zoals wachtwoord en username worden onversleuteld verstuurd

Voorbeelden van wat er dan kan gebeuren:

- Iemand kan op afstand controle overnemen over apparaat
- Iemand kan meekijken met videobeelden
- Bezoek aan verkeerde website kan leiden tot controle over apparaat

Deel 2
Reacties fabrikanten op gerapporteerde kwetsbaarheden

Hoe zijn we te werk gegaan?

Elk veiligheidsprobleem dat we tegenkwamen, groot en klein, hebben we gerapporteerd aan de fabrikant met het verzoek om de kwetsbaarheid te verhelpen. De reacties hierop hebben we beoordeeld als ofwel positief, ofwel negatief. Positief is het daadwerkelijk verhelpen van het probleem of een toezegging daartoe. We waren dus mild: we vonden een toezegging om een probleem te verhelpen ook al positief. Negatief is het uitblijven van een concrete actie of toezegging of überhaupt geen reactie.

Voor dit deel van het onderzoek hebben we in 2019 naast de 4 vergelijkende tests ook 10 producten onderworpen aan een hacktest, waarvan we wisten die veiligheidsproblemen hadden. Ook deze fabrikanten hebben we benaderd.

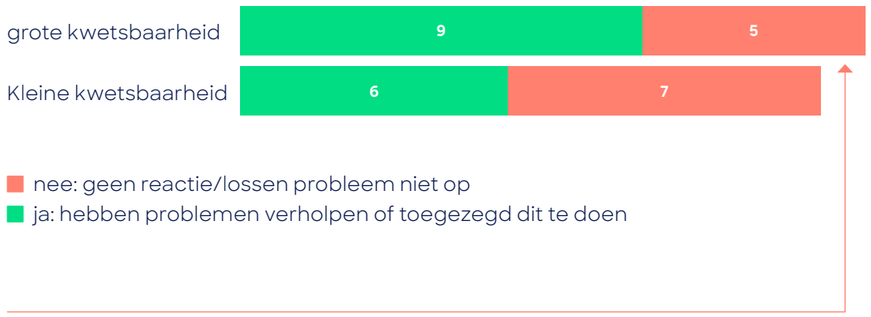
Producten in losse hacktests:

2 seksspeeltjes (Lovesense, Svakom)
2 kinder-gps-horloges (One2track, Q90)
2 wifi-printers (Brother, Epson)
2 slimme babycamera's (Alecto, Sannce)
1 router (TP-Link)
1 slimme set lampen (Action)

In totaal hebben we in 29 producten kwetsbaarheden aangetroffen: 19 uit de vergelijkende onderzoeken plus 10 uit de hacktests. Hier zaten 3 varianten van de Ring-deurbel bij met dezelfde kwetsbaarheid, die hebben we als 1 kwetsbaarheid geteld. Uiteindelijk komen we dan uit op 27 producten met kwetsbaarheden van 22 verschillende fabrikanten, waarbij we vanwege een gevonden probleem om een reactie hebben gevraagd. 14 keer was er sprake van een groot issue, 13 keer een klein probleem.

Belangrijkste uitkomst
Te vaak wordt een kwetsbaarheid niet (direct) opgelost: In 12 van de 27 gevallen kregen we een negatieve reactie. Kijken we alleen naar de 14 grote problemen, dan kregen we 5 keer een negatieve reactie. Deze fabrikanten vinden de veiligheid van consumenten kennelijk niet belangrijk.

Grafiek 2 Reactie fabrikanten op gerapporteerde kwetsbaarheden



Deze 5 fabrikanten reageerden negatief op het verzoek een groot veiligheidsprobleem op te lossen:

- **Svakom** (seksspeeltje): zei aanvankelijk toe met een fix te komen, maar doet dat niet. Gaan alleen de productie stoppen. Zie ook de aparte paragraaf hierover.
- **Sannce** (babyfoon) : heeft niet gereageerd op onze vraag om verbeteringen.
- **Epson** (printer), **D-Link** (beveiligingscamera): vinden het gevonden probleem niet belangrijk genoeg om (direct) op te lossen.
- **Eminent** (beveiligingscamera): “Deze suggestie zullen we meenemen bij de ontwikkeling van nieuwe firmware”.

Voorbeeld slim apparaat met slechte beveiliging:

De Svakom Siime Eye slimme vibrator

Wat is het? De Siime Eye is een slimme vibrator met een app en een ingebouwde camera. Hij is te koop bij bol.com voor €130. Je kunt hiermee filmpjes maken en die delen met anderen. Volgens het onderzoekslab is het beveiligingsniveau van dit apparaat zeer slecht. We zijn overigens niet de eersten die dit ontdekken: online circuleren al bijna 3jaar (!) handleidingen over hoe je dit apparaat kunt hacken.

Wat is er mis met de beveiliging? De Siime Eye heeft een ingebouwde wifizender met een herkenbare naam (‘Siime Eye’) en standaardwachtwoord (‘88888888’) die voor alle Siime Eye’s hetzelfde is. Als de vibrator aanstaat, zie je hem als wifizender tussen de andere wifizenders. Het is wifi, dus je ziet het ook op straat.

Wat is het risico? Als de vibrator aanstaat, kan iedereen binnen het wifi-bereik van de zender (maximaal 100 meter) en die technisch een beetje handig is, met de camera in het apparaat meekijken.

Hoe reageerde de fabrikant? Fabrikant Svakom liet ons aanvankelijk weten de kwetsbaarheden uiterlijk eind 2019 op te lossen. Bij navraag blijkt nu dat ze niets gaan oplossen, maar in plaats daarvan alleen de productie stopzetten en gebruikers hebben geïnstrueerd hun wachtwoord te wijzigen. Ze verhelpen het probleem dus niet. En dan te bedenken dat het product medio januari 2020 gewoon nog te koop is bij bol.com (https://www.bol.com/nl/p/svakom-siime-eye-camera-vibrator-met-app-control-licht-roze/9200000052524205/). bol.com heeft inmiddels toegezegd het product uit de verkoop te halen.

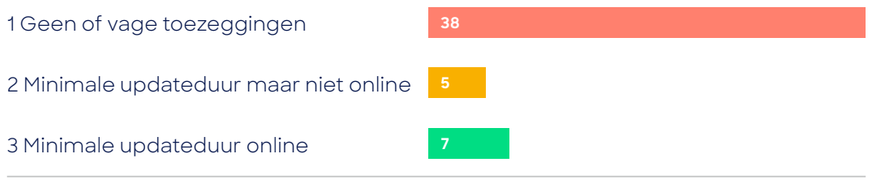
Resultaten onderzoek updatebeloften IOT-fabrikanten

Wat is er onderzocht? In januari 2020 hebben we de onderzocht bij de (in totaal 50) belangrijkste fabrikanten van 16 slimme productgroepen, of zij consumenten op hun website informeren hoe lang hun ‘slimme’ producten nog van veiligheidsupdate voorzien worden. Met andere woorden: kun je er als consument voor de koop achter komen hoe lang je die producten veilig kunt gebruiken?
Hiervoor hebben we deze bedrijven gevraagd om informatie over hun updatebeleid. Daarnaast hebben we zelf op de websites van die fabrikanten gezocht naar informatie over hoe lang je veiligheidsupdates krijgt op plaatsen waar je die informatie verwacht.

Belangrijkste uitkomst:
Slechts 7 van de 50 (1 op de 7) fabrikanten geven consumenten online vooraf informatie over hoe lang hun IOT-producten (veiligheids)updates zullen krijgen. Je krijgt dan als het ware een auto met autogordels waarvan je niet weet hoe lang die het blijven doen. En dan doen 3 van die 7 fabrikanten dat nog niet eens voor alle slimme productgroepen die ze leveren. Bij 13 van de 16 slimme productgroepen is er geen enkele belangrijke fabrikant die duidelijk vertelt hoe lang je updates krijgt.

Toelichting:
Bij verreweg de meeste onderzochte fabrikanten (44 van de 50, dus 7 van de 8) is online geen informatie te vinden hoe lang hun slimme producten nog veiligheidsupdates zullen ontvangen.

Grafiek 3 Mate waarin fabrikanten toezeggingen doen over toekomstige updates



We hebben de informatie die fabrikanten gaven onderverdeeld in 3 groepen:

1 **Fabrikanten die geen of vage informatie geven over toekomstige updates.**
Dit is de grootste groep: 38 van de 50 (76%).

We onderscheiden hierbinnen verschillende subgroepen:

- **Geen informatie of beleid:** De grootste subgroep: Er is helemaal geen informatie te vinden of beschikbaar over updateduur.
- **Vage beloften:** Er worden vage beloftes gedaan waarbij je in de praktijk niet weet aar je aan toe bent, zoals ‘we offer ongoing support without a fixed timeframe’ (Google Nest thermostaat), ‘this product is scheduled to continue to receive security updates’ (Motorola smartphones), of ‘We always strive to deliver relevant updates for as many of our products as possible (AVM routers). Vaak wordt als reden voor de vage formulering aangevoerd dat vooraf niet te zeggen is hoe lang de hardware nog ondersteund kan worden.
- **Onduidelijke informatie:** zoals: ‘Normaal gesproken stopt HP na 10 jaar met het ondersteunen van producten.’ Niet duidelijk is of updaten hier ook onder valt.
- **Garantie tot de deur:** In een enkel geval nog erger, krijg je zelfs botweg ‘garantie tot de deur’, zoals iBaby (“iBaby is not obligated to provide any updates”) en Apple (“Naar eigen goeddunken levert Apple in de toekomst mogelijk software-updates.”).

2 **Fabrikanten die een minimale updateduur garanderen, maar (nog) niet online**.
Soms blijkt er bij navraag wel een minimale updateduur te zijn (‘zeker 2 jaar na introductie’), of zelfs ‘oneindig’, maar is die (nog) nergens online te vinden (‘daar werken we aan’). Daar heb je dan als consument natuurlijk weinig aan. Het gaat hier om 5 fabrikanten, waaronder Huawei (smartphones) en iRobot en Blaupunkt (robotstofzuigers).

3 **Fabrikanten die een minimale updateduur toezeggen die ook online te vinden is.**
Het gaat voorlopig om slechts 7 van de 50 fabrikanten, in 5 van de 16 productgroepen:

- Smartphones: Google Pixel-smartphones (3 jaar na introductie) en telefoons van andere merken met het Android One-besturingssysteem: 3 jaar (veiligheids- en andere) updates na introductie en Samsung (2 jaar na introductie). Samsung meldt de updategarantiedatum (dankzij de rechtszaak van de Consumentenbond!) ook op de productpagina van elke smartphone.
- Slimme thermostaten: Eneco Toon (gedurende de hele levensduur).
- Slimme verlichting: Philips (Hue) (3 jaar nadat de verkoop is gestopt) en KlikAanKlikUit (5 jaar nadat product uit assortiment is genomen).
- Beveiligingscamera’s: KlikAanKluit (5 jaar nadat product uit assortiment is genomen) en Eminent (2 jaar na introductie)
- Routers: Eminent (2 jaar na introductie)

N.B. We hebben de websites van alle fabrikanten bezocht, en daarnaast alle fabrikanten gevraagd welke informatie ze vooraf geven over updates. Slechts 23 van de 50 fabrikanten reageerden tijdig (binnen de uiterste termijn van 15 werkdagen).

Bijlage: tabellen

Tabel B-1 Gevonden kwetsbaarheden per merk in de 4 vergelijkende tests

Rijlabels	Grote kwetsbaarheid	Kleine kwetsbaarheid	Geen kwetsbaarheid	Eindtotaal
Alecto	3			3
Arlo			2	2
D-Link	1			1
Elro	1			1
Eminent	1			1
Ezviz	1	1		2
Foscam		1		1
Ikea			1	1
Innr			1	1
klikAanKlikUit		1	1	2
Lifx		1		1
Logitech			1	1
Luvion	1			1
Nest			2	2
Netatmo			1	1
Paulmann		1		1
Philips			1	1
Ring		3*	1	4
Sleekbit			1	1
Smartwares		2		2
TP-Link			1	1
Wiz		1		1
Eindtotaal	**9**	**10**	**13**	**32**

*het gaat om drie Ring-deurbellen met dezelfde (kleine) kwetsbaarheid.

Tabel B-2 Reacties fabrikanten op de gevonden kwetsbaarheden. Welke fabrikanten reageerden positief (toezegging of actie ondernomen om probleem te verhelpen), welke negatief (geen toezegging of actie).

Merk	Reactie negatief	Reactie positief	Eindtotaal
Alecto		4	4
Brother		1	1
D-Link	1		1
Elro		1	1
Eminent	1		1
Epson	1		1
Ezviz	1	1	2
Foscam	1		1
klikAanKlikUit		1	1
Lifx	1		1
Lovesense		1	1
LSC (Action)		1	1
Luvion		1	1
One2Track		1	1
Paulmann	1		1
Q90	1		1
Ring	1		1
Sannce	1		1
Smartwares		2	2
Svakom	1		1
TP-Link		1	1
Wiz	1		1
Eindtotaal	**13**	**14**	**27**

Tabel B-3 Lijst fabrikanten in onderzoek updatebeloften

Action (LSC Smart Connect)
AEG
Alecto
Amazon
Apple
Arlo
Asus
AVM

Blaupunkt
Brother
Bosch/Siemens (BSH-groep)

Canon

Delonghi
D-Link

Ecovacs
Elro
Eminent
Eneco (Toon)
Epson
Eufy
Ezviz

Foscam

Google/Google Nest

Honeywell (Residio)
HP
Huawei

iBaby
Ikea
iRobot

Jura

KlikAanKlikUit

LG
Linksys
Luvion

Melitta
Miele
Motorola

Neato
Netatmo
Netgear

Oral B

Panasonic
Paulmann
Philips
Plugwise

Ring

Samsung
Sony

TP-Link

Xiaomi

Tabel B-4 Lijst slimme productgroepen in onderzoek updatebeloften:

Babycamera's
Beveiligingscamera's

Deurbellen

Espressomachines

Koelkasten

Lampen

Printers

Robotstofzuigers
Routers

Smartphones
Smart speakers

Tandenborstels
Televisies
Thermostaten

Vaatwassers

Wasmachines

Contact

Consumentenbond
Enthovenplein 1
Postbus 1000
2500 BA Den Haag
Telefoon 070 445 45 45
consumentenbond.nl