Domotica en privacy

Arnold van Overeem

In diverse films, zoals The Matrix, Swordfish en Black Hat wordt een beeld geschetst van een Orwelliaanse wereld waarin anderen via alom tegenwoordige digitale communicatiemiddelen controle hebben over ons leven.

Ik ga u nu vertellen hoe u eraan bijdraagt om dit (schrik-)beeld te verwerkelijken.

Om anderen controle over uw leven te laten krijgen, moet u aan drie voorwaarden voldoen:

1. U moet afhankelijk zijn van smart (slimme) elektrische apparaten die op afstand bestuurbaar zijn. Nog beter is het wanneer u verslaafd bent aan een apparaat (zoals een smartphone voor sommige mensen). Een pacemaker, gehoorapparaat of insulineautomaat met remote besturing kan ook.
2. Er moet een communicatiemedium zijn waarmee derden toegang kunnen krijgen tot uw smart elektrische apparaten. In de meeste gevallen is dat een draadloze verbinding: wifi, 4G, 5G, Bluetooth of NFC.

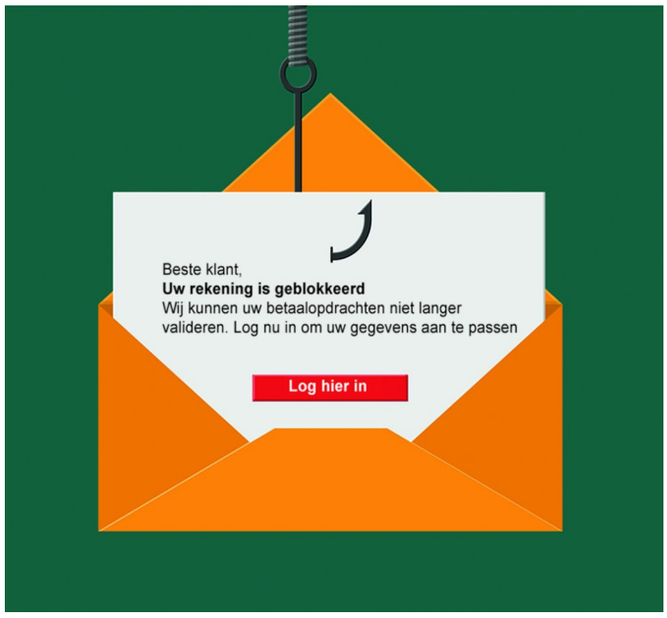
3. Derden moeten zich meester kunnen maken van de besturing van de smart elektrische apparaten. Daarvoor moet het apparaat een niet te moeilijk wachtwoord hebben, of u hebt een account op het apparaat waarmee u derden vrijwillig toegang tot dat apparaat hebt verschaft.

In dit artikel ga ik u uitleggen hoe u dit mogelijk maakt, en ook hoe u juist kunt voorkomen dat u dit mogelijk maakt, mocht u toch liever zelf de regie over uw leven behouden.

Smart apparaten overal

In dit artikel gaat het over domotica, en dus over het gebruik van smart elektrische apparaten die uw leven gemakkelijker en aangenamer kunnen maken. Het geeft dan geen pas te roepen dat u die apparaten maar niet moet gebruiken, om te voorkomen dat voorwaarde 1 wordt vervuld.
U kunt wel ervoor kiezen om niet afhankelijk te worden van smart apparaten, en wel door ook te blijven beschikken over een aantal ‘domme’ apparaten. Wanneer een apparaat niet op afstand bestuurd kan worden, kan een derde deze besturing ook niet overnemen. Nu is dit wellicht gemakkelijk gezegd, want te verwachten is dat de industrie steeds meer en steeds goedkopere smart apparaten in de handel brengt, en dat, als we die met z’n allen massaal blijven kopen, de domme apparaten langzamerhand zullen verdwijnen.
De industrie helpt nog een handje mee doordat smart apparaten een ander verdienmodel kunnen hebben dan domme apparaten. Wanneer smart apparaten allerlei informatie over hun gebruik en liever nog over hun omgeving kunnen verzamelen en verzenden naar een besturingsapparaat, krijgt de eigenaar van dit besturingsapparaat verhandelbare privacygevoelige informatie. Het apparaat zelf kan dan goedkoper of zelfs gratis worden aangeboden. Ieder smart apparaat dat minder kost dan een vergelijkbaar dom apparaat is dus verdacht. Dat kan niet waar zijn of u betaalt met uw privacy, en wellicht in de toekomst ooit met de machtsovername over uw leven via dat apparaat.

Nu zult u wellicht zeggen dat één smart Hue-lamp het verschil niet zal maken. Dat ben ik met u eens, maar over 10 - 20 jaar is uw auto smart, is uw aansluiting op het energiebedrijf smart, zijn al uw huishoudelijke apparaten smart, is al uw verlichting smart, staat uw huis vol met spionageapparatuur, die door een vertrouwde Nederlandse leverancier uit China is geïmporteerd en kunt u op ieder moment uitgekozen worden om te worden gebruikt als slaaf van degene die de controle heeft over al uw smart apparatuur. En wellicht doet u het uzelf aan door te reageren op een al te verleidelijk nepmailtje of WhatsApp berichtje.



U bent nu gewaarschuwd.
Misschien is er wel wetgeving nodig om de industrie en de handel te verplichten om naast de smart apparaten ook domme apparaten te blijven leveren met dezelfde functionaliteit, maar dan zonder de besturing op afstand, en voor maximaal dezelfde prijs. Zo moeilijk hoeft dat niet te zijn. Indien in het ontwerp daarmee rekening wordt gehouden, kan een universeel apparaat, door het verwijderen van een ingeplugde chip, in één handeling dom worden gemaakt. Daarvoor is dan wel een betrouwbare Europese certificatie nodig, om zeker te weten dat het verwijderen van die smartplug inderdaad het gewenste effect heeft.

Universeel netwerk alom

Voor de communicatie met smart apparaten staat een veelheid van mogelijkheden ter beschikking. U kunt natuurlijk veelal gebruik maken van een netwerkkabel, die u zo nodig direct altijd kunt los trekken, maar voor de meeste toepassingen wordt handig gebruik gemaakt van radiocommunicatie in allerlei vormen: veel huidige systemen maken gebruik van productspecifieke frequenties en protocollen, zodat besturing alleen mogelijk is met bijpassende apparatuur van hetzelfde merk. Dat is wel zo veilig, maar het nadeel is dat als een apparaat kapot gaat, dit als onderdeel niet meer is te vervangen, omdat de fabrikant allang is overgestapt op een nieuwere productlijn met allerlei technische voordelen, maar voor u het nadeel dat uw investering in het systeem opeens veel minder waard is. Het komt ook voor dat gebruik gemaakt wordt van een zendfrequentie waarvan de licentie verloopt en dan door het verliezen van een veiling opeens niet meer beschikbaar is.

Dat is onlangs Stedin en Liander overkomen, die daardoor alle reeds uitgezette smart energiemeters vóór 2024 moeten gaan vervangen door meters met een andere communicatie technologie. Uiteraard gaat u dat betalen via uw aansluittarief.

Er zijn ook systemen die gebruik maken van standaarden die wel langdurig beschikbaar zijn én licentievrij. Deze worden gewoonlijk gekenmerkt door een beperkte bandbreedte en een beperkt zendbereik, zodat u in ieder geval niet al te beducht hoeft te zijn voor radiosignalen die van buitenaf naar uw apparaten gestraald worden. De DECT-standaard voor draadloze telefoons leent zich uitstekend voor deze toepassing. De bandbreedte is maximaal 32 kbit/s per apparaat en in iedere radiocel is maximaal ruimte voor gelijkertijd 120 apparaten. DECT-verbindingen zijn altijd encrypted, en tamelijk storingsvrij. Een zendbereik van 50 m binnenshuis en 300 m buitenshuis concurreert prima met andere technologieën.

Ten behoeve van domoticatoepassingen is DECT sinds 2013 uitgebreid met de ULE-standaard. En deze weer met de HAN-FUN-standaard. Alle DECT ULE-apparaten kunnen in beginsel met elkaar communiceren.

Fritz!Box en Smarthome

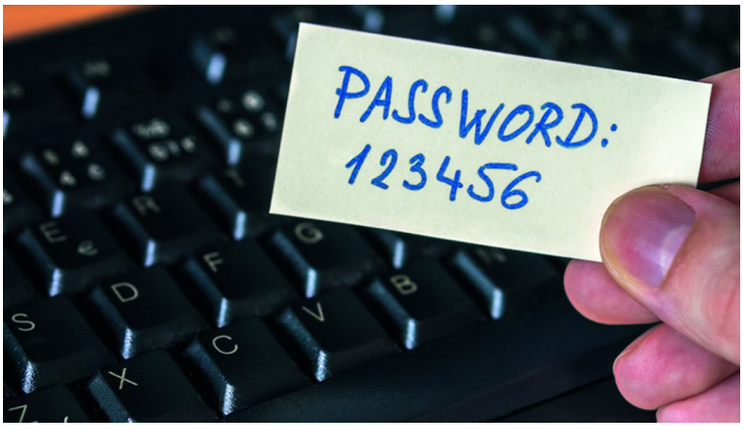
De meeste door een aantal internetproviders (o.a. XS4ALL, Freedom Internet, Solcon, TriNED, KPN (tegen meerprijs), Tweak (naar keuze), en wellicht nog andere providers in bruikleen verschafte FRITZ!Boxen en een deel van de zelf aangeschafte FRITZ!Boxen beschikt over een ingebouwd DECT-basisstation dat behalve voor telefonie ook voor smart schakelaars, thermostaatkranen en Hue-lampen gebruikt kan worden. Uiteraard kunt u deze apparaten dan ook met een DECT-telefoon bedienen. Door de aard van het DECT-protocol en de wijze van implementatie is dit systeem van buitenaf niet te hacken. In Nederland is een gedeelte van de Smart Home-componenten die door de leverancier van de FRITZ!Box geleverd worden nog niet op de markt gebracht. DECT-telefoons zijn via de GAP-standaard onderling compatibel. DECT-domotica via ULE- en HAN-FUN-standaard. U kunt bij voorbeeld moeiteloos een Gigaset DECT-telefoon verbinden met een FRITZ!Box-basisstation. Uitbreiding tot meercellige DECT-systemen behoort ook tot de mogelijkheden.

Onder meer in Duitsland en Zwitserland, waar de privacywetgeving aanmerkelijk strenger is dan in Nederland, is al redelijk veel DECT ULEcompatibele apparatuur te koop, onder andere: rook melder, temperatuurregeling, vochtmelder, bewegingssensor, aan/uitschakelen, IR-sensor, besturing rolluiken of markiezen, automatisch bellen naar een alarmcentrale of naar jezelf, invalidenalarm, etc. Op surveillancecamera's na kunt u met deze technologie prima uit de voeten. Degenen die via hun internetprovider over een FRITZ!Box beschikken hebben deze technologie overigens al in huis. Zie kaderFRITZ!BoxFRITZ!Box. Bij de huidige modellen FRITZ!Box is het maximale aantal DECT apparaten beperkt tot een lager aantal dan volgens de DECT standaard maximaal mogelijk is. Het is te verwachten dat deze grenzen bij volgende generaties apparatuur of software versies wel opgerekt zullen worden.

De meeste nieuwere systemen zijn echter gebaseerd op de wifi-standaarden. Dat heeft een aantal voordelen voor u en voor de leverancier of fabrikant. Uw voordelen zitten in de universele uitwisselbaarheid en de maximaal beschikbare bandbreedte, die bij de nieuwste standaarden tot meer dan 1 Gbits/s kan oplopen. Nu heb je die bandbreedte voor de meeste domoticatoepassingen helemaal niet nodig, maar voor videosurveillance en voor spionage is het wel handig. Ervan uitgaande dat de meeste kopers van domoticaapparatuur toch niet controleren of er heimelijk een microfoon in zit en/of dat de video-opnames naar een server in China of elders gestuurd worden, en bij installatie akkoord aanvinken onder de algemene voorwaarden te hebben gelezen, die overigens in de meeste gevallen in onbegrijpelijke taal zijn gesteld, is voor de fabrikant of leverancier een interessant business-model mogelijk.

Het grootst voordeel voor hen zit hem in de beveiliging van wifi. In tegenstelling tot bijvoorbeeld DECT, is wifi op zichzelf niet veilig. U kunt het wel beveiligen door de SSID te verbergen, een sterk wachtwoord te kiezen en WPA3 te gebruiken, maar hoeveel van de gebruikers doen dat? En als het apparaat zelf door de gebruiker bij zijn wifi netwerk is

aangemeld, wie controleert dan met welke servers er allemaal gecommuniceerd wordt?



Als u er toch niet gerust op bent, kunt u toch wel wat maatregelen nemen. Allereerst een bekabelde netwerkverbinding en liever geen wifi, die door de omgeving afgeluisterd kan worden. Ten tweede een apart VLAN, of, als bekabeling echt geen optie is, een aparte (verborgen) SSID, die via een extra router met het gewone LAN en uiteindelijk de server verbonden wordt, zodat het verkeer met de server via extra strenge firewall-regels gecontroleerd kan worden. En uiteraard voor ieder smart apparaat een verschillend voldoende lang wachtwoord dat niet te raden is en dus afhankelijk is van het gebruik van een goede password-manager.

Van wie is de server?

De verschillende producten die op de markt zijn, proberen klanten vooral te verleiden met aantrekkelijk uitziende apps die op uw smartphone of tablet, en soms in een webbrowser, toegang geven tot het beheer van uw smart apparatuur. Zo'n app maakt via een persoonlijk account verbinding met een server. En dan begint de onduidelijkheid.

In de meeste gevallen wordt in de documentatie niet over een server gesproken, maar het is wel degelijk zo dat er een (virtuele) server bestaat en dat in deze server de configuratiegegevens van al uw smart apparaten liggen opgeslagen, en dat de toegang tot die gegevens voor u heel gevoelig kan worden, zeker als opslag van gegevens zo goedkoop is dat de leverancier of de fabrikant ervoor kan kiezen uitgebreid historische gegevens op te slaan. Voor enkele euro's per jaar kun je nu al een TB (terabyte) aan data opslaan, en de prijzen per TB van harde schijven dalen nog steeds. Met

Bigdata-analyse kunnen dan patronen ontdekt worden in uw leven waarvan u zelf niet wist dat ze bestaan.
En dit alles gebeurt automatisch, zonder dat iemand ernaar kijkt.

Totdat uw profiel blijkt te voldoen aan iets dat uitermate geschikt is voor een doelstelling waaraan u beslist niet had willen meewerken. Ik hoef maar te verwijzen naar Cambridge Analytica om bevestiging te krijgen dat dit inderdaad bestaat. Niet alleen in China of Rusland of Nigeria. Weet u inmiddels al waar de gegevens van uw Smart Home zijn opgeslagen? Bij de leverancier van het product? Of bij de fabrikant? Of bij de hostingprovider van de server? Of bij de cloudserviceprovider van de hostingprovider van de server van de Smart Homeserviceprovider van de importeur van uw Smart Homeproducten? En weet u onder welke wetgeving uw gegevens nu zijn opgeslagen?

En dan heb ik het nog niet gehad over cybercriminelen die het gemunt hebben op de servers van Smart Homeproducten, waarvan je al weet dat ze kwade bedoelingen hebben, en die zich van wetgeving sowieso niets aantrekken. Als er slachtoffers gaan vallen, zult u vast niet de enige zijn, maar dat is een schrale troost. Misschien moet u nog maar eens een paar films bekijken van de categorie die ik in begin van mijn artikel genoemd heb, om u er een voorstelling van te kunnen maken.

Als u toch liever niet wilt meewerken aan dat scenario, moet u dus zorgen dat u zelf de controle heeft en behoudt over de hardware en de software van de server die voor uw Smart Home wordt gebruikt. Dit kan uw router zijn (zoals een FRITZ!Box) of een Raspberry Pi met geschikte open-source-software, een app of een Docker-image op een NAS in uw huis, of een andere eigen oplossing. U kunt ook aan risicospreiding doen door te voorkomen dat alle smart apparaten via één server bestuurd kunnen worden.

docker

Er gaat hier vast nog een hele markt voor ontstaan van enthousiaste hobbyisten die wel het beste met u voor hebben. Of u kunt natuurlijk het heft in eigen hand nemen. Wie pakt de handschoen op?