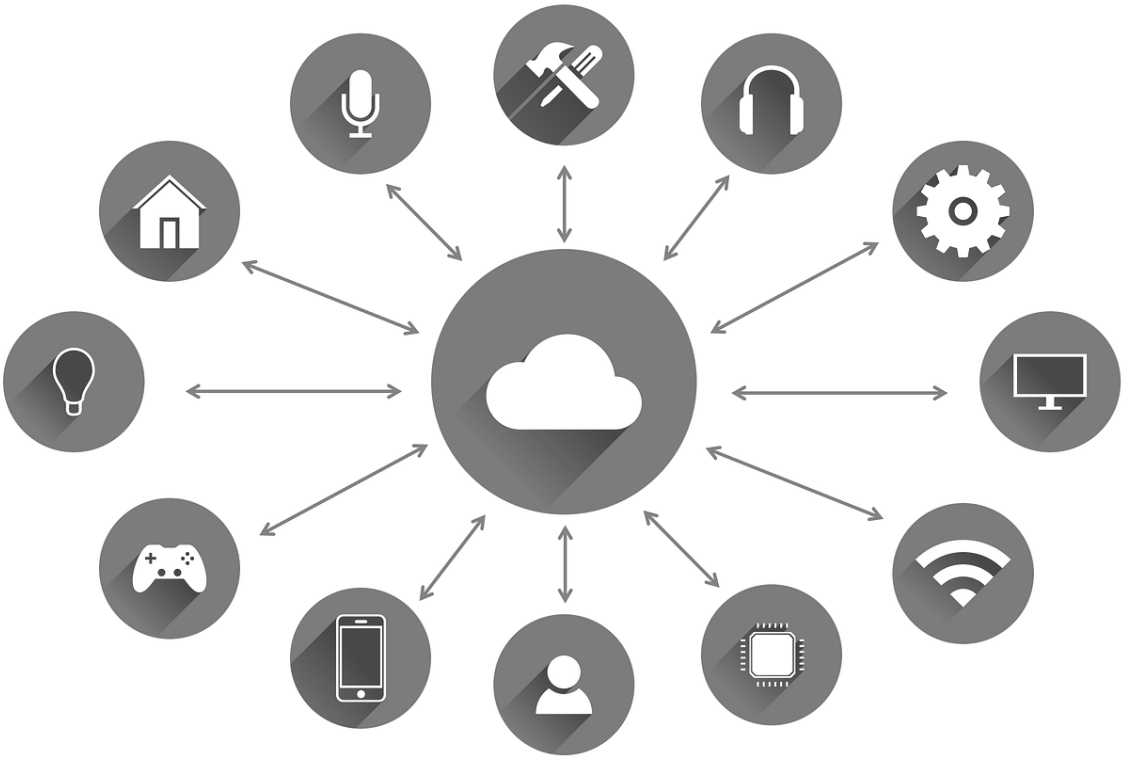
Internet of Things



De veiligheidsaspecten

Door Tim Spies

Inhoud

1. Introductie

Stel u zich het volgende scenario voor:

Het is 5 uur 's middags, je loopt na een lange dag werken terug naar jouw auto. Zodra je binnen vijf meter afstand komt ontgrendeld de auto zichzelf en de deur van de bestuurderskant gaat uit zichzelf open. Je stapt in en rijdt naar huis. Nog voordat je je straat inrijdt, slaat de verwarming thuis aan. Je parkeert de auto en loopt naar binnen, het koffiezetapparaat heeft al een warme kop voor je klaarstaan.

Dit scenario is tegenwoordig steeds realistischer aan het worden. Door ontwikkelingen op het gebied van technologische communicatie is in de nabije toekomst alles met elkaar verbonden.

Stel uzelf dan vooral de volgende vraag:

"Als mijn thermostaat weet wanneer ik wel- en niet thuis ben, wie kan dat dan nog meer te weten komen?"

Dit rapport gaat de veiligheidsaspecten van een "Smart Home" en "Internet of Things" behandelen.

Veiligheid wordt soms over het hoofd gezien wanneer nieuwe technologieën op de markt worden gebracht. Het doel van dit rapport is dan ook om u, de consument, meer bewust te maken van de veiligheidsaspecten in nieuwe technologieën.

2. Wat is Internet of Things?

In het kort is Internet of Things (IoT) een netwerk van alledaagse apparatuur, met elkaar verbonden door middel van internet. Meerdere apparaten die via het internet met elkaar verbonden zijn, kan men een IoT-systeem noemen. De functie van een IoT-systeem is om een omgeving te monitoren, een reactie op veranderingen in de systeemomgeving mogelijk te maken, te helpen of te automatiseren.

Het doel van een IoT-systeem is de kwaliteit van leven te verbeteren. Dit doet een IoT-systeem door de beste reactie op een veranderingen in de omgeving mogelijk te maken (denk aan thuis komen na een werkdag). Een IoT-systeem biedt responsieve diensten die specifiek zijn toegespitst op de behoeften van de eindgebruiker. (Ruth Ande, 2020)

IoT-systemen zijn overal te vinden.
In huis, waar met een simpel verzoek aan de Google Home speaker de gewenste muziek wordt afgespeeld. In de supermarkt van de toekomst, waar geen kassières of vakkenvullers meer te zien zijn. Maar ook in grote warenhuizen, hierin worden pakketten automatisch gesorteerd en op de juiste locatie afgegeven door robots. Dit alles wordt mogelijk gemaakt door apparatuur die via het internet met elkaar communiceert.

3. Wat zijn de risico's

Veiligheid is aan de kant geschoven bij het ontwerpen en ontwikkelen van IoT. Dit heeft vooral bij de opkomst van IoT voor veel beveiligingsproblemen gezorgd. In de huidige vorm van IoT is veel meer rekening gehouden met dreigingen van kwaadwillende personen en risico's op datalekken. (Ruth Ande, 2020)

Voor het accuraat monitoren van een omgeving met veel variabelen, is veel data nodig. Een IoT-systeem verzameld en verwerkt al deze data om te kunnen reageren op veranderingen in de omgeving. Al deze data wordt gecommuniceerd over het internet, om te voorkomen dat iedereen deze communicatie af kan luisteren en de verstuurde data in handen krijgt, is deze communicatie versleuteld.

Helaas zijn de hackers van tegenwoordig heel slim en beschikken ze over tools die hun werk heel gemakkelijk maken. Het is dus mogelijk dat de communicatie tussen de apparaten wordt afgeluisterd door kwaadwillende personen en de versleuteling wordt gekraakt. De data die de kwaadwillende persoon dan in handen heeft kan bijvoorbeeld helpen bij het plannen van een inbraak.

Het grootste risico van IoT is dat de persoonlijke en gevoelige data, die in het IoT-systeem gecommuniceerd wordt, in de verkeerde handen valt.

4. Conclusie

Als de eindgebruiker deze risico's niet accepteert en veel kennis heeft van IT, dan kan deze gebruiker opzoek gaan naar manieren om het IoT-systeem beter te beveiligen tegen dreigingen van buitenaf.

Het is uiteindelijk aan de gebruiker van een IoT-systeem om op zijn/haar manier met de risico's om t gaan. Voor degene die deze risico's niet willen accepteren adviseer ik om IoT zoveel mogelijk te mijden

Verwijzingen

Ruth Ande, B. A. (2020, Maart). *Internet of Things: Evolution and technologies from a security perspective*. Opgeroepen op September 8, 2020, van ScienceDirect: https://www.sciencedirect.com/science/article/pii/S2210670719303725?casa_token=5JdxS6pKQf8AAAAA:IU8Yw12OtsQ02SSlq44rjLcDGnBX8pElxEGBNfgYtDxuZmDKB8Uii_28cUpsnx34xWJ2r60U8LM#bib0490