VIJF BERUCHTE IOT-DREIGINGEN EN HOE U ZE OPLOST

Het Internet of Things (IoT) krijgt binnen steeds meer organisaties voet aan de grond. Een mooie ontwikkeling, want de technologie biedt indrukwekkende mogelijkheden op het gebied van automatisering, productiviteit en efficiëntie. Toch blijft IoT-security vaak nog wat onder de radar. Een overzicht van courante IoT-dreigingen én praktische tips om deze risico's tegen te gaan.

1 Ondermaats wachtwoordgebruik

De grootste dreiging voor de veiligheid van het IoT zijn systemen die zijn uitgerust met zwakke wachtwoorden. Denk hierbij aan voor de hand liggende wachtwoorden die makkelijk te kraken zijn. Ook standaardwachtwoorden van de fabrikant vormen een groot risico. Dat kan worden opgelost door systemen te beveiligen met complexe cijfer- en lettercombinaties, en deze periodiek te wijzigen.

2 Onveilige netwerkverbindingen

Het IoT is in feite een groot netwerk van devices die via het internet verbonden zijn. Als de tussenliggende verbindingen kwetsbaar zijn levert dat risico's op, zoals hacks. Zorg er daarom voor dat deze verbindingen goed zijn beveiligd. Een andere oplossing is om een volledig gescheiden netwerk aan te leggen voor het IoT.

> Het IoT is in feite een groot netwerk van devices die via het internet verbonden zijn

3 Gebrek aan device management

Om de mogelijkheden van het IoT volledig te kunnen benutten is een goed doordacht beleid belangrijk. Denk hierbij aan zaken als asset management, systeembeheer en veilige verwerking van oude devices. Door op deze gebieden de vinger aan de pols te houden kunnen een hoop veiligheidsrisico's worden voorkomen.

4 Gebrek aan periodieke updates

Net als mobiele devices draaien IoT-netwerken op firmware. Het is belangrijk dat deze regelmatig wordt geüpdatet om kwetsbaarheden te dichten. Updates zouden dan ook moeten worden toegepast op het moment dat deze beschikbaar zijn. Is dat niet altijd mogelijk, dan is het verstandig om te kijken of er een gescheiden netwerk kan worden aangelegd dat niet toegankelijk is voor externe dreigingen.

5 Onveilige doorvoer en opslag van data

IoT-devices wisselen continu data met elkaar uit. Het verzenden, verwerken en opslaan van die data moet veilig gebeuren. Dat kan worden bereikt door de data te versleutelen. In het geval van een datalek zijn de gegevens in ieder geval onbruikbaar voor kwaadwillenden.

> Security is een toetssteen tijdens iedere fase van onze dienstverlening

IoT maakt steeds vaker het verschil

Steeds meer bedrijven omarmen de voordelen van het IoT, en benutten de technologie in hun nationale en internationale vestigingen. Een populair praktijkvoorbeeld is de verregaande mogelijkheden tot automatisering. Deze innovatieve techniek heeft de potentie om een belangrijke gamechanger te worden. De organisatie die het IoT strategisch inzet weet zich al snel verzekerd zien van een sterke concurrentiepositie.

Wij zijn er voor al uw IoT-vraagstukken

Het beveiligen van IoT-netwerken kan een ingewikkelde klus zijn. Computacenter beschikt over de juiste know-how om u hier nationaal en internationaal in te ondersteunen. Dat doen we op basis van internationale expertise, best practices en regievoering, waarbij we u van a tot z ondersteunen. Security is een toetssteen tijdens iedere fase van onze dienstverlening. Zo voegen we samen nog meer innovatie toe aan uw bedrijfsbrede IT, en behoudt u uw zakelijke voorsprong.

Computacenter

Postbus 300, 1180 AH Amstelveen
nl.sales@computacenter.com
+31 (0)88 4358222

www.computacenter.com/nl