Alles communiceert met alles

Op weg naar Internet of Everything

De Britse technologie pionier Kevin Ashton en medeoprichter van het Massachusetts Institute of Technology (MIT) staat bekend als de bedenker van het Internet of Things. De term “het internet van dingen” is een visie, waarin systemen in staat zijn om via het internet verbinding met elkaar én met de fysieke wereld te hebben. Inmiddels is de volgende fase aangekondigd: Internet of Everything.

tekst Ronald Eygendaal

→

Tijdens de Cisco Live 2013 conferentie in Orlando, waar 20.000 IT-beslissers aanwezig waren, heeft Cisco CEO John Chambers de volgende levensfase van het Internet of Things aangekondigd, waarbij Things wordt vervangen door Everything. Hierbij worden volgens Chambers mensen, data, dingen via het internet aan elkaar gekoppeld. Het Internet of Everything (IoE) gaat niet alleen over machine-to-machine communicatie, maar ook over machine-to-people communicatie en in de optiek van Cisco zelfs over people-to-people communicatie. Kortom, een volledige vermenging van communicatie tussen mens en mens, mens en machine, en machine en machine. Dat alles moet leiden tot meer kennis en productiviteit. Een van de fundamenten onder Internet of Everything is de steeds verdergaande convergentie tussen kantoorautomatisering (IT), procesautomatisering (OT), en fysieke beveiliging.

De slag om te komen tot het Internet of Everything is gaande en snel evoluerend. Het is heterogeen en omvat zowel verticale als horizontale producten en diensten. Het kan worden toegepast in zowel wired als wireless infrastructuren. Deze infrastructuren kunnen zich zowel binnenshuis als buitenshuis bevinden. De Internet of Everything infrastructuur wordt bevolkt door apparaten, variërend van computers tot smart devices die 'slimme' functionaliteiten bezitten vanwege de infrastructuren en diensten waarop zij aansluiten. Een smart device is een elektronisch apparaat, dat verbinding heeft met andere apparaten of netwerken zoals Internet, Bluetooth, Zigbee, Near Field Communication (NFC), WiFi, 3G en 4G. In de basis zijn het op IP technologie gebaseerde apparaten. Het IoE faciliteert consumenten en bedrijven en heeft invloed op alle aspecten van het dagelijks leven in de moderne samenleving.

Op IP technologie gebaseerde infrastructuren spelen hierbij een cruciale rol. Het IoE moet een intelligente, beheerbare en veilige infrastructuur bieden welke op kan schalen tot miljarden contextbewuste apparaten. Het intelligente netwerk luistert, leert en reageert met open interfaces voor betere beveiliging, grotere eenvoud, betrouwbaarheid, continuïteit, innovatie, en misschien wel meer comfort als ooit tevoren.

EISEN IoE APPARATEN

Het moge duidelijk zijn dat het IoE eisen stelt aan de apparaten die worden toegepast. Er zijn vijf belangrijke kenmerken vast te stellen waaraan apparaten moeten voldoen:

1 Elk aangesloten apparaat dient te beschikken over een *eigen uniek IP adres* dat wordt gebruikt voor identificatie en communicatie.

2 Elk aangesloten apparaat, mobiel of vast, dient een *unieke (soms virtuele) locatie* te hebben, noodzakelijk om de onderliggende communicatie-infrastructuren zo efficiënt mogelijk te laten werken.

3 Er is sprake van een situatie waarin een apparaat *informatie dient te verwerken of te generen.* De hoeveelheid informatie waar we het hier over hebben, zal de door mensen voortgebrachte informatie al snel gaan overstijgen.

4 Er zijn *complexe voorzieningen voor security, analyse en beheer* benodigd die het mogelijk maken groepen apparaten te formeren die via IP netwerken met elkaar verbonden zijn.

5 Bij het verwerken of generen van enorme hoeveelheden data zijn *tijd en locatie van cruciaal belang.*

Aan het IoE zitten ook risico's. Sterker nog, het is waarschijnlijk voor hackers een zeer interessant doelwit om aan te vallen. Met de groei van IoE zullen de kansen op aanvallen alleen maar toenemen. Het is dus van cruciaal belang dat security zeer veel aandacht krijgt.

De beveiliging van IoE kan voor een groot deel worden gefaciliteerd vanuit de netwerkarchitectuur. Door deze op te bouwen in lagen ontstaat de mogelijkheid de beveiliging per laag te regelen. In de onderste laag bevinden zich de zogenaamde end-points. Dit zijn embedded systemen, sensoren, actuators, camera's en dergelijke. Kortom, een zeer gevarieerd spectrum van apparaten, die vaak zeer goedkoop zijn en zijn

Fundament onder IoE is de convergentie tussen kantoorautomatisering, proces-automatisering, en fysieke beveiliging

gemaakt voor het verrichten van slechts één functie. Veel end-points zijn voorzien van de mogelijkheid om aan te sluiten op een IP netwerk. Ondanks deze mogelijkheid is het daadwerkelijk aantal aangesloten end-points nog laag. Soms komt dat doordat de benodigde infrastructuur niet aanwezig is, in andere gevallen staan de kwaliteitssystemen en de regelgeving dit soort apparaten niet toe. Zo zijn er bijvoorbeeld infrarood detectors te koop die kunnen worden aangesloten op een IP netwerk. Maar staat het kwaliteitssysteem voor inbraakdetectie installaties, de zogenaamde BORG regeling, het gebruik van IP infrarood detectors niet toe.
Boven de laag met de end-points bevindt zich de multiservice edge laag. In deze laag bevindt zich netwerkapparatuur dat verbinding heeft met de end-points. Deze laag faciliteert een reeks van protocollen en technieken. Voorkomen moet worden dat end-points onbeschermd zijn. De security services binnen de multiservice edge laag hebben hierbij een belangrijke rol.

FYSIEKE BEVEILIGING

Binnen de fysieke beveiliging speelt de overgang naar IP technologie al jaren. Toch zien we in de praktijk in één gebouw vaak nog een fysieke scheiding tussen de verschillende IP netwerken. Regelmatig wordt het IP netwerk voor het kantoorautomatisering fysiek gescheiden van het ook op IP technologie gebaseerde beveiligingsnetwerk. Ook de procesautomatiseringsnetwerken (PCS, SCADA) zijn vaak gescheiden van de overige IP netwerken. Door deze praktijken worden de fundamenten van de IoE visie geweld aan gedaan. Alhoewel Cisco inzet op Internet of Everything en ook fysieke beveiliging daarin wil meenemen, beperkt Cisco zich tot toegangscontrole en videosurveillance. Andere fysieke beveiligingsonderwerpen zoals inbraakdetectie passen nog niet in de IoE visie van Cisco. Toch zou het in theorie mogelijk moeten zijn om de functionaliteit inbraakdetectie te faciliteren vanuit het IoE. Zoals eerder beschreven zijn er bijvoorbeeld infrarood detectors te koop die kunnen worden aangesloten op een IP netwerk. Ook zou men in plaats van infrarood detectoren camera's met motion detection kunnen gebruiken. Hiermee zou het mogelijk moeten zijn om met de data die uit de end-points (lees infrarood detectoren & camera's) komt deze functie te creëren.

MARKTBEWEGING

De beweging naar convergentie tussen kantoorautomatisering, procesautomatisering en fysieke beveiliging is in de markt duidelijk voelbaar. De eerste aanbestedingen waarin men deze convergentie vraagt, staan in de markt. In deze aanbestedingen lees je de natuurlijke spanning tussen het traditionele denken en de IoE gedachte. Ook *Kristian Steenstrup*, research vice-president bij de onafhankelijk marktanalist Gartner, signaleert dat de aard van de procesautomatisering aan het veranderen is. Deze systemen en de onderliggende technologieën krijgen steeds meer de kenmerken van de mainstream IT. Dit ziet hij ook terugkomen in de platforms, software, beveiliging en communicatie. Volgens Steenstrup worden IT-leiders beïnvloed door de convergentie van mainstream IT en procesautomatisering.
Ook in de bestuurskamer dringt ondertussen door dat met convergentie kostenbesparingen kunnen worden gerealiseerd en dat hierdoor efficiënter management kan plaatsvinden. Hoewel de uitdagingen van de integratie convergentie tussen kantoorautomatisering (IT), proces-automatisering (OT) en fysieke beveiliging groot zijn, zijn er wel genoeg voordelen te noemen: gestroomlijnde budgetten, gecoördineerde planning, consistente technologische beslissingen, en een gemaximaliseerde koopkracht.

Ronald Eygendaal is werkzaam als principal security consultant bij Eygendaals Services (www.eygendaals.nl) en heeft meer dan twintig jaar ervaring in bewaking & beveiliging, technisch beveiliging, fraude-onderzoek en informatiebeveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsmanagers Nederland (VBN).