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 Internet of Things. De term “het internet van dingen" is een visie waarin systemen in staat zijn om via het internet verbinding met elkaar en met de fysieke wereld te hebben.

Tijdens de Cisco Live 2013 conferentie in Orlando, waar 20.000 IT-beslissers aanwezig waren, heeft Cisco CEO John Chambers de volgende levensfase van Internet of Things aangekondigd, waarbij Things wordt vervangen door Everything (oftewel IoE). Hierbij worden volgens John Chambers mensen, data, dingen via het internet aan elkaar gekoppeld. Het Internet of Everything 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 verder gaande convergentie tussen kantoorautomatisering (IT) en procesautomatisering (OT) en fysieke beveiliging. Cisco is hierin een van de leidende spelers. De slag om te komen tot het Internet of Everything is gaande en evolueert snel. 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 die variëren van computers tot “smart devices” die “slimme” functionaliteiten bezitten, dit 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 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 Internet of Everything moet een intelligente, beheerbare en veilige infrastructuur bieden die kan opschalen 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 is duidelijk dat het Internet of Everything eisen stelt aan de apparaten die worden toegepast. Grofweg zijn er vijf belangrijke kenmerken waaraan apparaten moeten voldoen:

- Ieder aangesloten apparaat dient te beschikken over een eigen uniek IP-adres dat wordt gebruikt voor identificatie en communicatie.
- Elk aangesloten apparaat, mobiel of vast, dient een unieke (soms virtuele) locatie te hebben. Dit is noodzakelijk om de onderliggende communicatie infrastructuren efficiënt te laten werken.
- 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 overstijgen.
- Er zijn complexe voorzieningen voor security, analyse en beheer nodig, die het mogelijk maken groepen apparaten te formeren die via IP-netwerken met elkaar verbonden zijn.
- Bij het verwerken of generen van enorme hoeveelheden data zijn tijd en locatie van cruciaal belang.

Belangrijke rol security

Aan het IoE zijn ook risico’s verbonden, sterker nog het is voor hackers een zeer interessant doelwit om aan te vallen. Met de groei van IoE zullen de kansen op aanvallen alsmaar 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 architectuur op te bouwen in lagen ontstaat de mogelijkheid de beveiliging per laag te regelen. In de allerondeste 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 dikwijls zeer goedkoop zijn en vaak zijn gemaakt voor »

» het verrichten van slechts één functie. Vele end-points in het veld 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 een aantal 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. Gelukkig kunnen veel end-points autonoom functioneren.

Boven de laag met de end-points bevindt zich de multi-service edge laag. In deze laag bevindt zich netwerkapparatuur die verbinding heeft met de end-points. De multi-service edge laag faciliteert een reeks van protocollen en technieken. Er moet voorkomen worden dat end-points onbe¬schermd zijn. De security servi¬ces binnen de multi-service edge laag spelen hierbij een belangrijke rol. Zoals eerder aangegeven is peer-to-peer verkeer tussen end-points een belangrijk gegeven in het kader van netwerk efficiëntie. Boven de multi-service edge laag bevinden zich het IP/MPLS-core netwerk en de datacenters met al hun mainstream IT-beveiligingsmechanismes.

Fysieke beveiliging

Binnen de fysieke beveiliging speelt de overgang naar IP-technologie al jaren, althans als we de branche mogen geloven. In de praktijk zien we in een gebouw nog vaak een fysieke scheiding tussen de verschillende IP-netwerken. Vaak wordt het IP-netwerk voor kantoorautomatisering fysiek gescheiden van het ook op IP-technologie gebaseerde beveiligingsnetwerk. Ook de proces automatiseringsnetwerken (PCS, SCADA) zijn heel vaak gescheiden van de overige IP-netwerken. Door deze praktijken worden de fundamenten van de “Internet of Everything” visie geweld aan gedaan. Alhoewel Cisco inzet op Internet of Everything en ook fysieke beveiliging daar wil in meenemen beperkt het zich tot toegangscontrole en videosurveillance. Andere fysieke beveiliging onderwerpen zoals inbraakdetectie passen nog niet in de “Internet of Everything” visie van Cisco. Toch zou het in theorie mogelijk moeten zijn om de functionaliteit inbraakdetectie te faciliteren vanuit het “Internet of Everything”. Zoals reeds 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 en procesautomatisering en fysieke beveiliging is duidelijk voelbaar in de markt. 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 “Internet of Everything” gedachte. Ook Kristian Steenstrup, research vice-president bij de onafhankelijke markt analist 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 het ondertussen door dat met convergentie kosten bespaart kunnen worden en dat hierdoor efficiënter management kan plaatsvinden. Hoewel de uitdagingen van de integratie convergentie tussen kantoorautomatisering (IT) en procesautomatisering (OT) en fysieke beveiliging groot zijn, zijn er genoeg voordelen te noemen: gestroomlijnde budgetten, gecoördineerde planning, consistente technologische beslissingen en een gemaximaliseerde koopkracht.

Door Ronald Eygendaal (Principal security consultant bij eygendaals services, bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN)