OP WEG NAAR INTERNET OF EVERYTHING

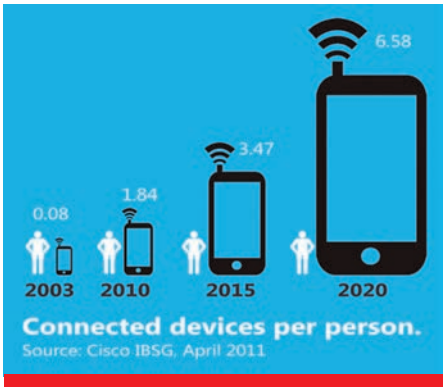
ALLES COMMUNICEERT MET ALLES

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

De Britse technologie pionier en medeoprichter van het Massachusetts Institute of Technology (MIT) Kevin Ashton 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 dus 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 snel evoluerende. 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. Het Internet of Everything infrastructuur wordt bevolkt door apparaten welke variëren van computers tot "smart devices" welke 'slimme' functionaliteiten bezitten, dit vanwege de infrastructuren en diensten waarop zij aansluiten. Een smart device is een elektronisch apparaat, wat verbinding heeft met andere apparaten of netwerken zoals Internet, Bluetooth, Near Field Communication (NFC), WiFi, 3G en 4G. In basis zijn het op IP-technologie gebaseerde apparaten. Het Internet of Everything *faciliteert* consumenten en bedrijven en heeft invloed op alle aspecten van het dagelijks leven in de moderne samenleving.



Aantal verbonden apparaten per persoon (Bron: Cisco)

Op IP-technologie gebaseerde infrastructuren spelen hierbij een cruciale rol. Het Internet of Everything 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 Internet of Everything eisen stelt aan de apparaten die worden toegepast. Grofweg zijn er vijf belangrijke kenmerken vast te stellen waaraan apparaten moeten voldoen. Deze kenmerken zijn:

1. Ieder aangesloten apparaat dient te beschikken over *eigen uniek IP adres* wat wordt gebruikt voor identificatie en communicatie.
2. Elke aangesloten apparaat, mobiel of vast, dient een *unieke (soms virtuele) locatie* te hebben, dit is noodzakelijk om de onderliggende communicatieinfrastructuren zo efficiënt te laten werken.
3. Er is sprake van een situatie waarin een apparaat *informatie dient te verwerken of te generen.*

Alles met alles verbonden (Bron: Flickr)

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 Internet of Everything zitten ook kwetsbaarheden, sterker nog, het is waarschijnlijk voor kwaadwillenden een zeer interessant doelwit om aan te vallen. Met de groei van het Internet of Everything zullen de kansen op aanvallen alleen maar toenemen. Het is dus van cruciaal belang dat security zeer veel aandacht krijgt, maar dan wel zo dat daarmee het Internet of Everything ook weer niet onbruikbaar wordt.

De beveiliging van Internet of Everything 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 aller-onderste laag bevinden zich de zogenaamde end-points. Dit zijn embedded systemen, sensoren, actuators, cameras en dergelijke. Kortom een zeer gevarieerd spectrum van apparaten, met allerlei cpu-types, OS'en, geheugenstructuren en -omvangen en dergelijke. Veel van die apparaten zijn zeer goedkoop en verrichten slechts één functie. Er zijn reeds vele end-points in het veld voorzien van de mogelijkheid om aan te sluiten op een IP-netwerk. Echter ondanks de mogelijkheid om aan te sluiten 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 welke 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 welke verbinding heeft met de end-points. De multi-service edge laag faciliteert een reeks van protocollen en technieken. Dit zijn zowel vaste als draadloze technieken zoals Zigbee, (*open standaard* voor draadloze verbindingen tussen apparaten op korte afstand), IEEE 802.11, 3G en 4G. Vanwege de grote diversiteit aan protocollen en technieken speelt security hier een belangrijke rol. Voorkomen moet worden dat end-points onbeschermd zijn, de security services binnen multi-service edge laag hebben hierbij een belangrijke rol. Zoals eerder aangegeven is peer-to-peer verkeer tussen end-points een belangrijk gegeven in het kader van netwerkefficiëntie. 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 één gebouw vaak nog een fysieke scheiding tussen de verschillende IP-netwerken. Vaak wordt het IP-netwerk voor het 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 in wil meenemen beperkt Cisco 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 detectoren te koop welke 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 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 Internet of Everything 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 ze met convergentie kostenbesparend 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 wel genoeg voordelen te noemen: gestroomlijnde budgetten, gecoördineerde planning, consistente technologische beslissingen en een gemaximaliseerde koopkracht. ●

Links

http://www.hays.co.uk/features/HAYS_411714
http://iotevent.eu/
http://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf
http://www.slideshare.net/CiscoIBSG/internet-of-everything