"ROEP OM FULLTIME SECURITY-OFFICER GROTER DAN OOIT"

DE VEILIGHEID VAN HET INTERNET OF THINGS

Het Internet of Things (IoT) is een van de belangrijkste ontwikkelingen in de afgelopen tijd, die nadrukkelijk een modernisering van ict teweegbrengt. Vrijwel elke bedrijfstak kan met een flinke dosis creativiteit profiteren van de toegevoegde waarde van het IoT. Maar het is nog zo nieuw dat velen de impact op de organisatie nog niet goed kunnen inschatten, zo stelde Eelco Stofbergen, Thoughtleader Cybersecurity bij CGI, tijdens een rondetafelsessie. "Met het IoT lopen we het risico alle fouten uit het verleden opnieuw te maken, ook in securitymanagement."

Het IoT is geen 'packaged revolution', het is in feite een bundeling van een aantal samenvallende ontwikkelingen die al wat langer bestaan. Nog niet eerder waren chips en connectiviteit zo goedkoop – en niet eerder was het mogelijk die in vrijwel elk device aan te brengen. Met de stand van de technologie van dit moment is een flink aantal beperkingen uit de klassieke IT weggevallen. Dat alles maakt een geheel nieuw concept mogelijk. Met creativiteit en inventiviteit zijn in vrijwel elke bedrijfstak fantastische toepassingen met IoT te bedenken. Er komen zeer aansprekende plannen op tafel met prachtige businesscases. Helaas is er daarbij vaak weinig aandacht voor data- en netwerksecurity. Té weinig, vindt Stofbergen. "Juist bij IoT-toepassingen is security van primair belang: de slim gemaakte apparaten zijn inherent kwetsbaar. Bovendien is elk connected device blootgesteld aan aanvallers. De twee hoofdbestanddelen van het IoT creëren dus tegelijk een beveiligingsprobleem."

Gevoelig

Is een IoT-omgeving dus gevoeliger dan andere IT-netwerken? Niet per se. Stofbergen: "Maar besef dat we zaken met internet gaan verbinden die dat eerst niet waren – een waterkoker, een sluisdeur, of een complete industriële installatie. Daarbij is dus nooit over cybersecurity nagedacht." Dan is er druk vanuit de 'consumentgedreven IoT-revolutie', zoals hij dat noemt, waarbij in hoog tempo connected producten voor consumenten van de tekentafels komen. Producten die allemaal zo goedkoop en zo snel mogelijk hun gebruikers moeten bereiken. Het gevolg: weinig aandacht voor beveiliging. Maar Stofbergen weet ook dat security in het algemeen een sluitpost is in IT-omgevingen. "Achteraf security inbouwen is vaak bijzonder lastig en kostbaar. Beter is het security van meet af aan mee te nemen in het design. En te zorgen dat security een standaard requirement is, dat mee moet evolueren in de lifecycle van het project. Security moet beschouwd worden als een functionele randvoorwaarde, een succesfactor."

Databeveiliging

Volgens sommigen is specifieke sensordata minder interessant voor hackers, maar daar is Stofbergen het hardgrondig mee oneens. *Security by obscurity*, noemt hij dat. "Data die voor een leek minder begrijpelijk lijkt, is niet intrinsiek veiliger. Dat is een gevaarlijke aanname en een onderschatting van de vijand. Het leger cybercriminelen is bijzonder

divers en elke datadief heeft zijn eigen beweegredenen. Data is in het digitale tijdperk gewoon heel erg waardevol", waarschuwt hij. Het feit dat sensordata eenvormig is, maakt het voor criminelen gemakkelijk een script toe te passen om de data te analyseren. Bovendien is de sensordata nooit volledig gescheiden van de operationele IT-omgeving en maakt het onderdeel uit van de big data in hybride dataomgevingen zoals Hadoop. "Sensordata hoort in alle gevallen thuis in de cybersecuritystrategie."

Eelco Stofbergen, Thoughtleader Cybersecurity bij CGI: "Een moderne organisatie met grootschalig gebruik van ict kan eigenlijk niet zonder een fulltime securitymanager."

Security-officer

Een moderne organisatie met grootschalig gebruik van ict kan eigenlijk niet zonder een fulltime securitymanager, daarvan is Stofbergen overtuigd. "Alleen al door de toenemende wet- en regelgeving, denk aan de meldplicht rondom datalekken en privacy. Maar ook aan de nieuwe wetgeving op het gebied van digitale infrastructuur waarbij incidenten gemeld moeten worden, ook als er geen datalekken hebben plaatsgevonden. Security is te belangrijk geworden om het er maar een beetje bij te doen." Hij tekent daarbij aan dat veel security officers in de praktijk blijken te rapporteren aan de CIO of IT-manager. "In omgevingen met een hoog risico is het veel beter om security te beschouwen als een verbijzondering van operational riskmanagement zoals in de financiële wereld gebruikelijk is. Dat geeft de security-officer een betere positie om als sparringpartner van de ict-afdeling op te treden.

GSM-partnership

Hoewel LoRa (long radio waves) in opkomst is, vormt gsm – via 3G en simkaart – in de meeste gevallen de sensorverbinding met het thuisnetwerk. Op de veiligheid van die belangrijke component in IoT heeft de gebruiker geen invloed: dat ligt helemaal bij de telecomprovider. Op dat vlak zoekt CGI altijd naar een partnership, een alliance. "De afhankelijkheid op zich is geen probleem, in de moderne wereld is iedereen over en weer afhankelijk van elkaar. Maar je moet de juiste maatregelen treffen om daarmee om te gaan. Natuurlijk kun je in een contract SLA's en KPI's vastleggen. Maar ik pleit ervoor om meer samenwerking met de providers te zoeken. En als alliantie dit soort verbindingen neer te zetten en te beveiligen."

INTERNET OF PUBLIC SPACES

IBOR (integraal beheer openbare ruimte) is een cloud-based service van CGI, bedoeld voor de besturing van objecten in de publieke ruimten. Rijkswaterstaat gebruikt deze service voor het actief besturen van snelwegverlichting in de regio Oost-Nederland. Hiermee kan de dienst op afstand de snelwegverlichting beveiligd in- en uitschakelen. Het resultaat: kostenverlaging en een verminderde milieubelasting.
Voor de gemeente Utrecht is een proef uitgevoerd met IBOR voor het operationeel beheer van lichtmasten. Daarmee kon de gemeente direct reageren op een lampstoring, lampen bijtijds vervangen en het onderhoud adequaat plannen.
Ook Deutsche Bahn heeft onlangs een testprogramma van drie maanden uitgevoerd voor de besturing van verlichting op stations.

Cloud

De opslag en verwerking van de – soms extreem – grote hoeveelheid sensordata vereist een speciaal ingerichte omgeving. Meestal is het bestaande IT-landschap van organisaties daarvoor niet geschikt. Bovendien worden investeringen in een eigen IoT-omgeving, die qua complexiteit en schaalgrootte niet in verhouding staat tot het bestaande landschap, bij voorkeur vermeden. Veel organisaties kiezen daarom voor een cloudoplossing, met alle bekende voordelen daarvan, zoals het kostenmodel. Stofbergen: "Belangrijk is dat je als organisatie heel klein kunt beginnen en bij gebleken succes gemakkelijk kunt opschalen. En dan is er het grote voordeel op het gebied van security: gespecialiseerde serviceproviders zijn de top als het gaat om informatiebeveiliging. Cloud en Internet of Things vormen alleen daarom al een perfect duo." ✖