# Waarom slim ziekenhuis voor een goed netwerk moet zorgen

17 januari 2020

Stelt u zich eens voor hoe het momenteel werkt in een ziekenhuis: er draait een veelvoud aan machines op het netwerk, die continu honderden mensen monitoren, meten en analyseren. En in een ziekenhuis is het een komen en gaan van mensen, dus moet het systeem altijd alert zijn. Dit is de ideale omgeving voor slimme, connected devices met een grote autonome, voorspellende en analytische capaciteit.

Door een in silo's opgedeelde, device-gedreven omgeving te transformeren naar een verbonden omgeving, kunnen bestaande activiteiten aanzienlijk worden verbeterd: snelheid, efficiëntie en betrouwbaarheid en uiteindelijk de patiëntenzorg en -ervaringen. Niet gek dus, dat ziekenhuizen in Amerika al naar schatting tien tot vijftien IoT-apparaten per bed hebben, volgens onderzoek door Zingbox.

## Security-overwegingen

Heel belangrijk zijn de nodige security-overwegingen, die gevolgen kunnen hebben voor zowel patiëntdata als de zorg. Het is sinds de komst van de AVG-wetgeving vorig jaar nog belangrijker geworden voor medische instellingen om uiterst zorgvuldig met hun data om te gaan. Uit rapporten blijkt dat tot wel 89 procent van de zorginstellingen met een IoT-strategie te maken heeft gehad met een IoT-gerelateerd datalek. Patiëntgegevens zijn dan ook een van de meest gezochte gegevens door hackers (volgens Trustwave levert dit op de zwarte markt zo'n 250 dollar per patiënt op).

Wat kunnen ziekenhuizen doen om de risico's van toenemende connectiviteit in de toekomst af te vangen? En hoe kunnen ze hun netwerk zo instellen dat ze hier een antwoord op hebben?

## Anticiperen op, overwinnen van IoT-risico's

Om een antwoord te kunnen geven op deze vragen, is de eerste stap voor netwerkbeheerders het herkennen van de zwakke plekken die inherent zijn aan grote netwerken met connected devices. Aangezien elke component een mogelijke ingang voor hackers kan zijn, betekent hoe meer apparaten een ziekenhuis gebruikt, hoe groter het risico op een aanzienlijk datalek.

Maar het lekken van patiëntgegevens is niet eens het ergst denkbare scenario. Nog erger zijn de mogelijke gevolgen voor patiëntenzorg. Zo kan een apparaat dat zelfstandig medicijndoseringen afmeet en aanbiedt, te maken krijgen met een softwarestoring of worden overgenomen door een malafide aanvaller. En in het geval van onverwachte downtime kan het voorkomen dat apparaten die minder kritiek zijn, zoals een MRI-scanner, voorrang krijgen boven echt kritiek apparatuur zoals een hartmonitor.

Dit lijken extreme scenario's, maar ziekenhuizen en zorgverleners moeten hier wel degelijk rekening mee houden. Om zich hiertegen te kunnen wapenen, zal een belangrijke bron van IoT-kwetsbaarheden moeten worden aangepakt: inzicht in het netwerk.

## Veilig, zichtbaar en onder controle

Het beveiligen van een grootschalig netwerk met IoT-apparaten is op zijn zachtst gezegd een uitdaging. Het is alleen mogelijk wanneer alles – tot aan de laatste sensor – afzonderlijk gelogd, beveiligd en gemonitord wordt. Zonder een systeem waarmee alles op deze manier exact is vastgelegd en vervolgens beheerd kan worden, kunnen zwakke plekken ontstaan waar misbruik van gemaakt kan worden.

Nu ziekenhuizen steeds meer IoT-apparaten in huis hebben en deze bovendien steeds geavanceerder worden, wordt beveiliging ervan voor netwerkbeheerders steeds moeilijker. Veel IoT-apparaten kunnen niet op de traditionele manier in profielen ingedeeld worden, waardoor ze generiek en niet te onderscheiden zijn.

Toch is het absoluut noodzakelijk om een onderscheid te kunnen maken tussen apparaten. Een probleem met een geautomatiseerd insulinetoedieningssysteem vereist immers heel andere acties dan een met slimme sensoren op het parkeerterrein van het ziekenhuis. Kritische zorgapparaten die continu moeten werken, kunnen niet op dezelfde manier behandeld worden als apparaten die indien nodig ontkoppeld kunnen worden.

## AI biedt meer inzicht

Er is een oplossing voor dit gebrek aan inzicht – namelijk in de vorm van een toenemend aantal AI- en machine-learningoplossingen, zoals ClearPass Device. Deze oplossingen zijn ervoor gemaakt om elk apparaat dat op een netwerk is aangesloten, te monitoren op het juiste niveau. ClearPass draait op een speciaal daarvoor ontworpen platform, en gebruikt een reeks machine-learningmodellen om onderscheid te maken tussen apparaten met soortgelijke IT-attributen, en om zeer gedetailleerde profielen te bouwen op basis van gedrag, voor iedereen die verbonden is met het netwerk.

Het in 2018 geopende Ommelander ziekenhuis Groningen in Scheemda is met hun platform ook volledig gericht op de toekomst. Artsen die met andere specialisten overleggen via video calls en patiëntdata real time kunnen inzien op tablets, zijn niet meer weg te denken uit het beeld van een modern ziekenhuis, maar ook achter de schermen gebeurt er veel.

## Beveiliging netwerk in spotlights

Wanneer het gaat om de toekomst van de gezondheidszorg, ligt de focus – begrijpelijk – vaak op medische staf, patiënten en apparaten. Maar nu slimme ziekenhuizen werkelijkheid worden, zal de aandacht gaan verschuiven richting de minder zichtbare rol van de netwerksecurity-beheerder. Daar komt veel verantwoordelijkheid bij kijken, maar ook de kans om een bepalende rol te spelen in de huidige revolutie van het moderne zorgsysteem.

In het IoT-tijdperk is vooruitgang net zo afhankelijk van effectieve beveiliging als van hardware-innovaties en digitale zorgverlening. Dokters kunnen beter voor hun patiënten zorgen, als netwerkbeheerders de juiste tools gebruiken om voor het slimme ziekenhuis te zorgen. Het is tijd om een juiste diagnose te stellen van de netwerk-security.