Security in een veranderende omgeving

De digitale samenleving, de wereld van Internet of Things, het Internet der gebouwen; deze thema's komen dagelijks voorbij. Waarom? Omdat technologie innovatie mogelijk maakt en met steeds minder 'resources' meer bereikt dient te worden. Energiegebruik, operationele efficiëntie, verbeterde veiligheid en klanttevredenheid; in elke sector zijn dit actuele onderwerpen. Nieuwe technologie vraagt ons anders na te denken over onze manier van wonen, werken en leven.

R. (Rik) Chorus, P. (Peter) Dijkstra;
Cisco Systems

Er zijn organisaties die deze nieuwe ontwikkelingen in verschillende segmenten succesvol weten op te pakken, denk aan Über binnen de taxiwereld, Airbnb binnen de verhuurmarkt van woningen en Tesla binnen de auto-industrie. Al deze organisaties hebben één ding gemeen, namelijk het ontwrichten van bestaande markten met nieuwe technologieën en veelal een ander businessmodel dan traditioneel binnen deze sectoren wordt toegepast.
Gebeurt dit ook binnen de gebouwautomatisering? De eerste tekenen zijn zichtbaar. Denk aan verschillende platformtechnologieën waarin gewerkt wordt met apps gebaseerd op een open programmeertaal in plaats van op dure software-applicaties, het netwerk dat steeds verder richting IP gaat en alle technische installaties ontsluit met standaard open protocollen, of wellicht de ontwikkeling van Power over Ethernet devices zoals verlichting. Neelie Kroes sprak recent nog uit dat data de olie van de toekomst zijn. Welke organisaties weten deze data om te zetten in bruikbare informatie? Hier zal het onderscheidend vermogen komen te liggen voor organisaties, ook binnen de gebouwautomatisering. Daarnaast zal men zien dat het samenbrengen van verschillende silo's, zoals beveiliging, klimaat, verlichting en IT, nieuwe innovatie met zich meebrengt, inclusief het gebruik van internet als het uitwisselingsplatform van real time-data tussen systemen, applicaties en platformen. Denk hierbij aan gebouwen die communiceren met smart grids en hun energiebehoefte kunnen afstemmen op vraag en aanbod, maar ook aan beveiligingscamera's die ook gebruikt worden om mensen te tellen die in- en uitlopen bij een sanitaire voorziening, waarbij deze data beschikbaar wordt gesteld aan de schoonmaak.
Is er dan geen keerzijde? Jazeker, denk aan onderwerpen als dataprivacy: wie is de eigenaar van de data, wat is de sociale impact. Dit zijn onderwerpen die zeker niet genegeerd mogen worden. En wat te denken van cybercrime? Data is de nieuwe olie, dat weet de cybercrime-industrie ook, en we spreken bewust van een industrie, want we hebben niet meer te maken met een scholier of een uit de hand gelopen hobby. Het zijn goed georganiseerde organisaties die zeer professioneel te werk gaan. Dit betekent dat cybersecurity vandaag de dag harde noodzaak is, ook binnen de wereld van gebouwautomatisering.
De tijd dat we simpelweg met een VPN en een traditionele firewall af kunnen is voorbij. Het hacken van gebouwautomatiseringssystemen staat op plek 6 van de 'The 10 Most Terrifying IoT Security Breaches you aren't aware of (so far)'. Waarom? Vanwege het feit dat gebouwautomatiseringssystemen een steeds grotere 'span of control' krijgen, die in de toekomst van 'The internet of Buildings' alleen maar verder zal toenemen. Daarnaast is de kennis rondom cybersecurity veelal beperkt binnen de sector; kortom relatief eenvoudig om te hacken.

SECURITY UITDAGINGEN

Hackers zijn uitermate innovatief en vinden altijd weer nieuwe manieren om personen en organisaties aan te vallen. Voor veel organisaties is security een uitdaging. Complexiteit en fragmentatie van de security-oplossingen, remote access, cloud-omgevingen en natuurlijk het constant veranderende dreigingslandschap. Het managen van meerdere platformen is voor veel organisaties geen eenvoudige taak. Vaak worden de beste producten per productgroep gekozen en is er een beleid van meerdere merken. Hierdoor ontstaat een enorme wildgroei aan oplossingen en managementplatformen. Tel daarbij nog op dat er veelal een tekort aan security specialisten is. Het implementeren van security-oplossingen is overigens maar 20% van de beveiliging. Uiteindelijk moeten alle data worden geanalyseerd en waar nodig moet ingegrepen kunnen worden.
Gebruikers die gebruik willen maken van bijvoorbeeld remote access en op allerlei plaatsen inloggen kunnen eenvoudig ten prooi vallen aan slimme trucjes van hackers waardoor de systemen worden gecompromitteerd. Remote access wordt veel toegepast voor beheer op afstand van gebouwen. De gebruikers komen in het bedrijfsnetwerk binnen en besmetten, zonder het in de gaten te hebben,

dit netwerk met 'malware'. Gemiddeld kost het organisaties 250 dagen om een succesvolle aanval van een hacker te ontdekken. Dit betekent dat een hacker 250 dagen de tijd heeft om data te verzamelen, te manipuleren of erger nog, de controle over te nemen van de systemen. Veelal komt dit door het gebrek aan 'zichtbaarheid' binnen het netwerk.

SECURITY VISIE

Voor iedere organisatie groot of klein geldt dat de basis van security niet in oplossingen wordt gelegd. Een goed informatiebeveiligingsbeleid is een must en het gebruik van een framework (bijvoorbeeld Cobit information security) vormen het fundament om uiteindelijk een concrete security architectuur te kunnen realiseren. Tot op heden zagen we dat het technische netwerk veelal buiten het beheer van de IT-afdeling valt. Toch is deze afdeling veelal wel verantwoordelijk voor het informatiebeveiligingsbeleid. De vraag is hoe dit zich in de toekomst gaat ontwikkelen.
Er komen verschillende aspecten en disciplines kijken bij security waarbij medewerkers, processen en stafafdelingen van belang zijn voor het uitdragen en handhaven van het beleid. Eenvoudige modellen als het CIA-model (Confidentiality, Integrity and Availability) geven enige vorm van houvast om risico's vast te stellen. Het bepalen van de risico's en een correcte kosten-batenanalyse hierover vormen een goed uitgangspunt om door te werken naar een gedegen security architectuur.
De visie op het gebied van security ligt met name op oplossingen waarbij de architectuur een prominente plek inneemt. Immers security problematiek is vaak niet op te lossen met de zogenaamde 'silver bullet' (één oplossing voor alles). Voor de meeste uitdagingen zijn meerdere oplossingen en slimme integraties noodzakelijk. Deze aanpak vraagt specifieke kennis en kunde. Inmiddels zien we veel nieuwe organisaties ontstaan die zich specifiek richten op deze materie en een complete dienstverlening ontwikkelen op het gebied van cybersecurity.
De gedachten dat alle aanvallen gestopt kunnen worden of dat een groot hekwerk om het netwerk heen voldoende is, is niet meer van deze tijd. Deze houding zorgt er veelal voor dat er een separate verbindingen worden gerealiseerd middels bijvoorbeeld een 3G/4G-modem, dat veelal zwak beveiligd is. Externe verbindingen zijn niet meer weg te denken om aan de vraag te voldoen van dienstverleners, om data van het gebouwbeheersysteem ter beschikking te stellen voor beheer op afstand, analyse etc. Zeker in de nabije toekomst, wanneer gebouwen communiceren met andere gebouwen binnen smart grids, kunnen

aanvallen ongemerkt langs de bestaande oplossingen 'sluipen', waardoor het niet meer te vermijden zal zijn om een gelaagd security model toe te passen. In zo'n model is het van belang inzicht te krijgen in de fase voorafgaand aan de aanval, tijdens de aanval en na de aanval; kortom het 'before, during en after'-principe. Alleen met dit inzicht zijn we in staat adequaat te reageren op aanvallen.

OPLOSSINGEN

Voor alle organisaties geldt dat er een aantal primaire oplossingen 'in place' dient te zijn rondom cybersecurity, naast het eerdergenoemde informatiebeveiligingsbeleid. Daarnaast is ook de beveiliging van bijvoorbeeld een controller of applicatie belangrijk. Uiteraard zijn deze veelal voorzien van wachtwoordbeveiliging, encryptie en authenticatie, maar het levert geen 'end to end' integraal beveiligingsbeleid op. Hier kan beveiliging binnen het netwerk een belangrijke rol spelen met oplossingen als 'next generation firewalling', 'identity management' en 'intrusion prevention' systemen. Met 'end to end' bedoelen we van het datacenter (Cloud) tot aan het device, bijvoorbeeld een sensor of controller. Next-generation firewalling is een must voor organisaties om de wildgroei en mogelijkheden van onder andere webapplicaties in toom te houden. Daarbij moet er nog steeds een gatekeeper aan de rand van het netwerk actief zijn. Een stap verder is identity management, waarbij kan worden vastgesteld in het netwerk wie met welk device vanaf welke locatie/netwerk en wanneer toegang krijgt tot de applicaties en bestanden van de organisatie. Dit onderscheid wordt met de komst van alle devices en de mogelijkheden voor remote access cruciaal om de veiligheid te waarborgen. Middels identity management is men immers in staat bepaalde richtlijnen te automatiseren. Wanneer er gekeken wordt naar datacenteromgevingen is het belang van een intrusion prevention systeem (IPS) steeds groter. Het monitoren van de verkeersstromen en daarbij kunnen toepassen van diepere inspecties is raadzaam om de slimme aanvallen te kunnen weerstaan. Ook dienen organisaties ervan uit te gaan dat niet alle aanvallen kunnen worden gedetecteerd en dat toepassingen, zoals Advanced Malware Protection (AMP), hierbij een uitkomst kunnen bieden. Een vereenvoudigde weergave hiervan zijn bestanden die door gebruikers worden gedownload. Als een bestand bij de organisatie aankomt (perimeter) kan dit worden getoetst door een globale intelligence database. Hierbij wordt gekeken of het bestand bekende malware is of juist niet. omdat hackers zich bewust zijn van het feit dat sandboxing technieken worden toegepast. Mocht dit alles falen en er toch nog malware op het endpoint terechtkomen, dan kan, als het bestand toch malware blijkt, retrospective security worden toegepast. Oftewel historisch terugkijken waar het bestand als eerste is binnengekomen en kijken of dit zich verder in het netwerk heeft verspreid. Voor genoemde oplossingen geldt dat deze aangepast dienen te zijn aan de omgeving waarbinnen ze worden toegepast. De huidige beschikbare IT-oplossingen functioneren in mindere mate, vanwege het feit dat deze de protocollen die worden toegepast in gebouwautomatisering, zoals BACnet, Modbus, KNX etc. niet herkennen en de mogelijke dreiging binnen deze protocollen negeren. Inmiddels zijn er leveranciers binnen het cybersecurity domein die specifieke producten ontwikkelen voor gebouwautomatisering.

SECURITY SENSOR

Voor organisaties die meer inzicht willen krijgen in wat er precies gebeurt in het netwerk is het vooral van belang dat de security oplossingen op een slimme manier informatie met elkaar kunnen uitwisselen. Dit om sneller en beter vast te kunnen stellen of er een dreiging bestaat en, zo ja, waar deze dreiging zich bevindt. Door het gebruik van netflow analytics kan veel inzicht worden verkregen over verkeersstromen en afwijkend gedrag in het netwerk. Door deze oplossing te integreren met een Identity Services Engine kan daarnaast snel informatie worden verkregen over waar deze dreiging zich precies bevindt en of andere systemen zijn geïnfecteerd.
De conclusie is dat de nieuwe technologie de leveranciers binnen gebouwautomatisering legio kansen biedt. Cybercrime is inmiddels een professioneel georganiseerde industrie waarin veel geld omgaat. Deze industrie richt zich ook op het vakgebied van gebouwautomatisering en met de toenemende span of control van het gebouwbeheersysteem is het van belang dat cybersecurity serieus wordt genomen. Hierbij is het beveiligen van een controller, enkele verbinding of applicatie te beperkt en moet een 'end to end' architectuur gehanteerd worden om de veiligheid te borgen. Mocht een aanval plaatsvinden, dan dienen er instrumenten aanwezig te zijn om deze te detecteren, te analyseren en te voorkomen. Data is de nieuwe olie, onderschat de waarde niet! Wat voor de één waardeloos lijkt is voor de ander zeer waardevol.