LAGARDE GROEP SCHETST BEVEILIGING ALS INTEGRAAL GEHEEL

ZWAKKE SCHAKELS UITBANNEN

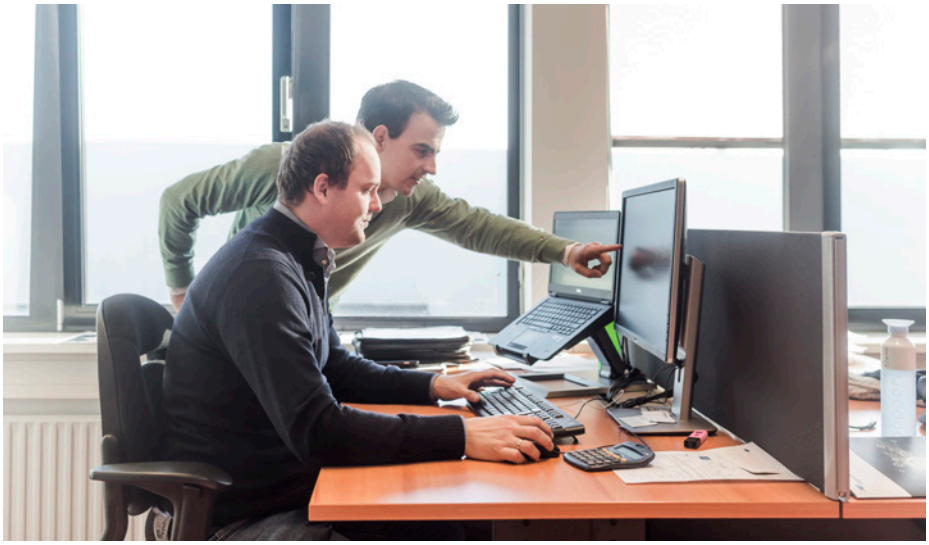
De snel veranderende wereld, aangewakkerd door 'the internet of things', werpt telkens nieuwe risico's voor bedrijven op en die zitten veelal in een onverwachte hoek. Lagarde Groep benadrukt dat je je daartegen alleen kunt wapenen door op alle fronten je beveiliging op orde te hebben en de verschillende onderdelen samen te smeden tot een integraal geheel.

TEKST: AART VAN DER HAAGEN
FOTOGRAFIE: MARCEL KRIJGSMAN

The internet of things brengt het bedrijfsleven veel, ook in de zin van beveiliging, maar maakt ondernemingen kwetsbaarder dan zij zelf inschatten. "Kijk maar naar de recente DDOS-aanvallen, die gebruik maken van de rekencapaciteit van cameraobservatiesystemen, door daarop in te breken," zegt Wim de Graaf, salesmanager bij Entris, het bedrijf binnen Lagarde Groep dat zich met ICT-security bezighoudt. "In het verleden kon je een netwerk als een kasteel met wachttorens beschouwen, waarbij de grenzen goed bewaakt werden. Nu zie je dat kennis en data overal binnenkomen en naar buiten gaan, alleen al door medewerkers die met hun laptop in- en uitlopen. Je dient dus in kaart te brengen en te beheren wie zich waar bevindt en wanneer toegang krijgt tot welke gegevens. Bedrijven die veel verschillende softwarepakketten gebruiken verliezen al gauw het overzicht over welke mensen waarmee werken. Wanneer iemand ontslag neemt of krijgt, worden dan alle wachtwoorden geblokkeerd? Je kunt per persoon een profiel met een toegangspas aanmaken en dat precies inregelen. Trouwens, wie zorgt ervoor dat al die software tijdig updates ondergaat, om actueel te blijven op het gebied van beveiliging? Dat moet je centraal beheren."

PATRONEN EN AFWIJKINGEN

"Goed ingerichte toegangscontrole is van essentieel belang en veelomvattend," stelt collega Arnold Versteeg, salesmanager bij Lagarde en gespecialiseerd in fysieke en elektronische beveiliging. "Dat doe je via een intelligente koppeling tussen je ICT-omgeving en cameraobservatie, met een gedegen analyse van data die op één plek ontsloten wordt, waarbij de verantwoordelijke over een 'dashboard' beschikt. Daarmee registreer je niet alleen wie het pand verlaat of betreedt, maar kun je ook patronen vastleggen en afwijkingen daarin signaleren, met herkenning van unieke personen. Als voorbeeld van specifiek gedrag noem ik maar even het ongeoorloofd gebruiken van camera's in een sauna. Dat komt sneller aan de oppervlakte als je weet wie wanneer inlogt. Denk ook aan incidenten in de zorg. Sta je 's nachts als medewerker alleen en



gaat de bel op het moment dat je net met een patiënt bezig bent, wat doe je dan, als je met één druk op de knop de deur op afstand kunt openen? Zo'n dilemma, met alle gevaren van dien, wend je af door je toegangscontrole goed te regelen. Personen die binnen mogen beschikken over een tag, eventueel gekoppeld aan bepaalde tijdzones en aan bepaalde ruimten. Ook hier geldt dat je overzicht moet hebben. Dan weet je altijd wie er in het pand rondloopt, wat ook relevant is in het kader van onder meer brandveiligheid. In de beveiliging gaan we steeds meer toe naar het voorspellen van mogelijke incidenten, bijvoorbeeld door bewakingscamera's met deep learning te combineren. Dan kun je op basis van ervaring vooraf actie ondernemen."

APPS BLOKKEREN

De salesmanagers van Lagarde en Entris geven nog wat andere voorbeelden die risico's blootleggen. Fysieke beveiliging, ingebed in een ICT-omgeving vormt een cruciale factor in de voedingsmiddelenindustrie. "Wanneer een vrachtwagen uitrijdt en niet alle veiligheidsprocedures opgevolgd zijn, kan het zomaar zijn dat de klant de lading afkeurt en het transport terugstuurt, wat in veel gevallen zal betekenen dat je de inhoud moet weggooien," zegt De Graaf. "Je dient dus alles te borgen en traceerbaar te maken. Bij scholen, die de verantwoordelijkheid dragen over alle leerlingen die zich binnen de muren begeven, wil je weten wat de jongeren uitvoeren. Bezoeken ze 'foute' websites, maken ze stiekem foto's op het toilet of van de antwoorden bij tentamens? Naast het afschermen van wifi kun je zelfs apps op de telefoons blokkeren. De toepassing hiervan in combinatie met camerasystemen hangt natuurlijk samen met de policy van de school, waarbij ouders moeten tekenen om toestemming te geven."

INZAGE IN BEDRIJFSGEHEIMEN

"Het verbaast mij soms hoe makkelijk bedrijven onbewust gelegenheid scheppen voor mensen om binnen te lopen," zegt Versteeg. "Dan denk je misschien in eerste instantie aan iemand die laptops en andere waardevolle spullen weghaalt op het moment dat iedereen zit te lunchen, maar het gaat soms nog veel verder: dat iemand zich uitgeeft voor een adviseur van de directeur, dagenlang binnen zit te werken en zichzelf inzage verschaft in allerlei bedrijfsgeheimen. Zo liggen in een kennisomgeving als Wageningen University & Research allerlei diefstalgevoelige patenten. Sommige kwaadwillenden stellen brutaalweg allerlei vragen aan medewerkers om hen informatie te ontfutselen. Naast het regelen van een gepersonaliseerde toegangscontrole, gekoppeld aan bepaalde ruimten, helpt het ook om mensen gewoon aan te spreken; dat heeft een afschrikkende werking. Een opkomende bedreiging voor bedrijven betreft het gebruik van drones om te inspecteren welke waardevolle data en spullen je waar precies hebt liggen en hoe je beveiliging geregeld is. Ze kunnen zelfs op je wifi inbreken."

END-TO-END-SECURITY

De beveiligingsmaterie wordt door the internet of things steeds complexer en zal ondernemers gauw boven het hoofd groeien. Lagarde Groep concentreert zich op alle disciplines, die in een volstrekt veilige omgeving niet zonder elkaar kunnen: telefonie, ICT, camera's, toegangscontrole en alarmsystemen. "Dan praat je over end-to-end-security, dat wil zeggen alles aan elkaar koppelen en zo inregelen dat er geen zwakke schakels meer bestaan," licht De Graaf toe. "Wil je het goed doen, dan moet je naar een totale integratie van alle elementen toe. Wanneer wij voor een opdrachtgever aan de slag gaan om zo'n allesomvattende beveiliging op te zetten, beginnen we met een checklist op techniek en daarna lichten we op eenzelfde manier de organisatie door. Op basis van onze bevindingen ten aanzien van de situatie en de risico's stellen we een compleet security-plan op." Versteeg: "Beveiliging betekent enerzijds proactief en anderzijds reactief bezig zijn. Onder die laatste noemer valt bijvoorbeeld het vermogen om de aanleiding tot ongewenste gebeurtenissen terug te halen, om dingen te reconstrueren. Daarna tref je maatregelen om ze in de toekomst te voorkomen. Als Lagarde Groep hebben wij met onze vijf bedrijven alle kennis in huis van de verschillende disciplines, maar vooral ook van de essentiële integratie daarvan."

www.lagardegroep.nl