OPTIMALE BESCHERMING VAN HARDWARE VAAK ONDERSCHAT

‘Fysieke IT-security begint met bewustwording’

Cyberincidenten en vormen van malware komen bijna dagelijks in het nieuws. Het belang hardware-devices goed te beschermen en de impact van falende fysieke IT-security wordt zelden belicht. Zes professionals gingen erover met elkaar in gesprek.

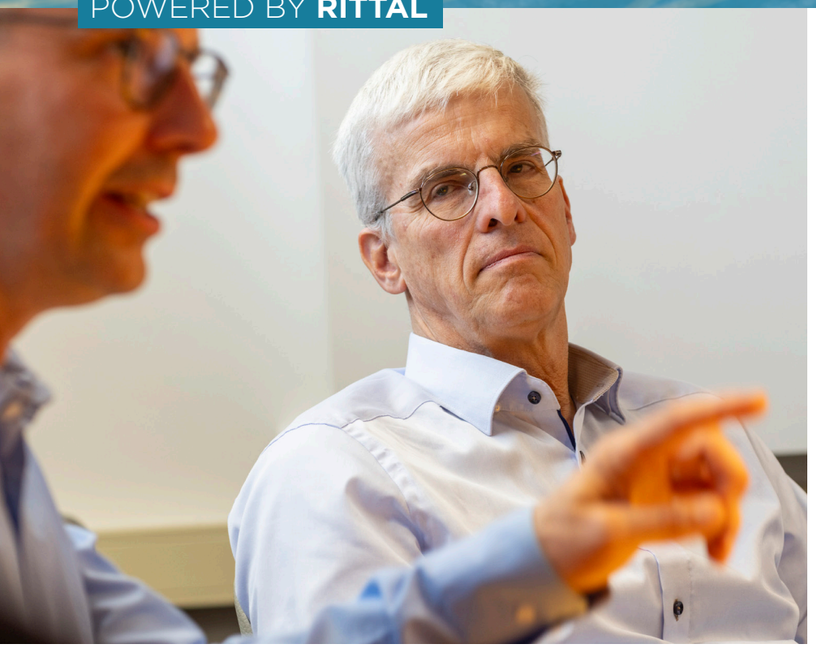
Tekst: Mels Dees

“In veel organisaties hebben IT-medewerkers meerdere taken, waardoor het fysieke deel van de IT er vaak ‘een beetje bij gedaan’ wordt”

André Hiddink, Product Manager IT bij Rittal, initieerde een Grotetafeldiscussie, die samen met de redactie van ChannelConnect werd georganiseerd. Rittal is leverancier van gestandaardiseerde, modulaire systeemtechnologie, die rack, power, cooling, security en monitoring omvat. Van compacte single-rack-installaties tot colocatie- en hyperscale-datacenters.

Aan het begin van de bijeenkomst legt Hiddink uit waarom hij het thema ‘fysieke IT-beveiliging’ wil adresseren: “Cybersecurity is hot, iedereen heeft het erover. En dat is terecht. Er is geen twijfel dat organisaties dit zo goed mogelijk op orde moeten hebben. Daar zijn inmiddels ook normen en richtlijnen voor en die worden steeds strenger, kijk naar wetgeving als AVG en NIS2. Fysieke IT-security is een onderwerp dat weinig belicht wordt.”

Dat wil Hiddink adresseren in een discussie met specialisten uit de markt. “Het gaat daarbij niet alleen om de toegang tot de serverruimte, of het slot op de serverkast, maar ook om bewustwording. Om de vraag: wat is het belang van fysieke IT-beveiliging?”



Stelling 1: Het mkb is druk met zijn eigen werkzaamheden, waardoor de fysieke security van IT een lage prioriteit heeft.

Thimo Keizer (beveiligingsspecialist RisicoRegisseurs) reageert als eerste op de stelling. “Als ik kijk naar de volwassenheid op het gebied van fysieke IT-beveiliging dan is die laag in de markt. Ja, er zijn rolluiken, sloten en camera’s voor het pand, maar er worden geen of in mindere mate maatregelen getroffen voor de beveiliging van de fysieke IT.”
Vincent Toms (CISO en beveiligingsspecialist) herkent dit. Het mkb is volgens hem bezig met de business van de onderneming. Niet met beveiliging. “Bij die ondernemingen moet eerst iets gebeuren voordat actie wordt ondernomen,” vult Marc van Rijssen (X-ICT, dat computerruimtes bouwt) aan. “Bij een goede relatie van ons heeft een brand plaats gevonden. Tot dat moment zagen zij geen aanleiding om te investeren in een detectie- en blusgassysteem. Geconfronteerd met de impact van een brand wordt nu iedere nieuwe computerruimte van een blusgassysteem voorzien.”

Toms signaleert dat fysieke beveiliging vooral wordt geassocieerd met mannen met oortjes die rond het pand lopen. Fysieke beveiliging is een mbo-functie, cyberbeveiliging is hbo of universitair. Die praten te weinig met elkaar. “En de directie investeert er niet in,” sluit Lex Borger (van msp Tesorion) af. De trigger om te investeren in automatisering is het verhogen van de efficiëntie of het verlagen van de arbeidskosten. Als het gaat om de fysieke omgeving is de opvatting: het werkt en het is goed genoeg: we blijven er vooral vanaf.

Risicoprofiel
Daarbij is het zo dat incidenten die samenhangen met fysieke IT-beveiliging zelden de krant halen. Het is wellicht ook een taboe. Het is geen sterk verhaal als een serverrack uit is gevallen doordat de plant die erop stond te veel water kreeg. “Plofkraken halen wel de krant, dat rolluik mag wat kosten,” is de analyse van Toon Cooijmans van het Catharina Ziekenhuis, die als eindgebruiker is aangeschoven. “Maar de IT-apparatuur staat bij een mkb-onderneming in de bezemkast tussen de schoonmaakspullen. Daar heeft men geen gevoel bij. Een goed serverrack mag niets kosten, die koop je voor een paar honderd euro online.” Voor Hiddink wordt daarmee de kern van het probleem geraakt. “Bedrijven zijn echt wel met beveiliging bezig, zoals het aanmelden van bezoekers en poortjes bij de ingang. Maar pas als, door gebrekkige beveiliging van de hardware, de boel platgaat investeert men.”
Keizer nuanceert dat toch iets. “Paaltjes bij de juwelier worden voorgeschreven door de verzekeraar. Maar het is ook schijnveiligheid. Wie houd je daarmee tegen? Niet de zware crimineel, want die pleegt een plofkraak als hij de spullen echt graag wil hebben.” Hij betoogt dat elke vorm van beveiliging gebaseerd moet zijn op het risicoprofiel.

Stelling 2: Externe partijen moeten een rol spelen bij het verhogen van de bewustwording.

In verzekeringspolissen gaat het niet of nauwelijks over fysieke IT-beveiliging, weet Hiddink. “Als de fysieke hardware wordt gestolen zijn die kosten gedekt, maar er wordt niet gestuurd op de kwaliteit van de behuizing van de apparatuur, bijvoorbeeld door een lagere premie als die omgeving op orde is.”
Dat voordeel levert de klant te weinig op, is de overtuiging van Keizer. De lagere premie weegt immers niet op tegen de forse investering in een IT-behuizing. X-ICT is het daar als leverancier van dergelijke ruimtes niet mee eens. Zij verzorgen jaarlijks bij de klanten een soort APK. “Dan kijken we ook naar de security, of er een camera in de ruimte is en naar de brandveiligheid. Als externe partij hebben we dan zeker autoriteit.”

> **“De behuizing staat qua verantwoordelijkheid los van de servers die erin staan. Dat leidt dan echter weer tot silo’s’”**

Deelnemers aan het Grotetafelgesprek

André Hiddink
Product Manager IT bij Rittal. Leverancier van compacte single-rack-installaties tot edge-, enterprise-, colocatie- en hyperscale-datacenters.

Lex Borger
Security Consultant bij Tesorion, een Security Service Provider. Tesorion levert vooral IT-security, “maar fysieke beveiliging komt eigenlijk altijd aan de orde.”

Toon Cooijmans
Datacenter beheerder / floormanager bij het Catharina Ziekenhuis in Eindhoven. Eerder werkte hij in en voor het mkb, onder meer als systeembeheerder, en bij msp’s.

Marc van Rijssen
Business Developerbij X-ICT. Werkte in zijn loopbaan ook voor IT-distributeurs. X-ICT bouwt computerruimtes.

Vincent Toms
CISO en beveiligingsexpert met ruim 20 jaar ervaring in informatiebeveiliging. “Bij digitale hygiëne is ook de fysieke beveiliging heel belangrijk.”

Thimo Keizer
eigenaar van RisicoRegisseurs, interim-securitymanager, consultant en auditor, “en dan specifiek op het gebied van fysiek beveiligingsbeheer.”

Stelling 3: Wie moet binnen een bedrijf verantwoordelijk zijn voor fysieke IT-beveiliging?

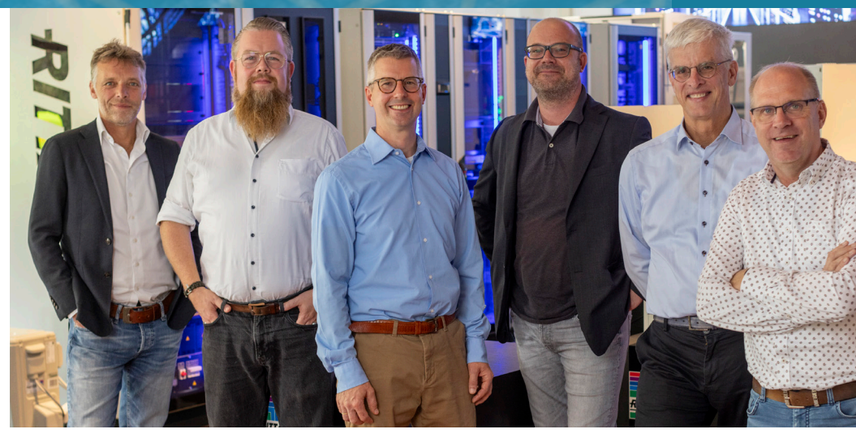
In de praktijk voelt niemand zich daar verantwoordelijk voor, is de stellige uitspraak van Hiddink. "Alles ín de computerruimte is IT, de ruimte en de toegang ertoe is facilitair, maar het sleutelbeheer kan zomaar bij HR liggen." Cooijmans speelt het onderwerp door naar Van Rijssen (X-ICT): "Wie zijn dan eigenlijk jouw gesprekspartners? De IT-verantwoordelijke, de directeur, de boekhouder, of zelfs de controller?" "In het mkb doet eigenlijk iedereen alles, dat maakt het niet overzichtelijker," luidt het antwoord.
"In een hoop organisaties, vaak kleiner dan corporates of enterprises, hebben veel IT-medewerkers meerdere taken, waardoor het fysieke deel van de IT er vaak 'een beetje bij gedaan' wordt," weet Cooijmans. "Daar zet de systeembeheerder servers in een kast op de afdeling en zegt 'succes ermee'." Bij grotere organisaties wordt dit opgepakt door een team binnen de IT-organisatie en is sprake van een duidelijke functiescheiding. Deze verschillen laten zien dat grotere organisaties dit serieus nemen en als een volwaardige taak zien.
"De behuizing staat qua verantwoordelijkheid los van de servers die erin staan." Dat leidt dan echter weer tot silo's: "Dan moet je mensen aanmoedigen met elkaar te communiceren."
Borger (Tesorion) benadrukt daarom dat een analyse van de risico's de basis van de beveiliging vormt. "Als je dat gedegen doet, kom je vanzelf tot de juiste maatregelen. Dat zijn misschien cybermaatregelen, of fysieke maatregelen. Of een training van personeel."
En dan nog is dat geen garantie voor een gedegen beveiliging. "Ik vind dat mijn huis goed beveiligd is," geeft Toms aan. "Maar is dat zo? Ik laat dat nooit checken. Dus waarom dat dan wel van een organisatie verwachten? De driver ontbreekt."

Stelling 4: Installerend Nederland vult fysieke beveiliging in naar eigen interpretatie en norm.

Datacenters steken energie in het voldoen aan normen. Er zijn uitgeschreven richtlijnen. Hiddink: "Hun verkoopargument is 99,999% continuïteit." Maar als het gaat om die paar servers die nog on-premise staan, doet men maar wat. Dat verbaast Cooijmans (Catharina Ziekenhuis) niet. "Uptime is de heilige graal voor een datacentrum. Maar het mkb met die paar servers in het pand kijkt daar toch echt anders tegenaan. Je zult bij een transportbedrijf heel wat moeten uitleggen eer ze die mooie behuizing van Rittal kopen en ook nog eens op de beste plek neerzetten." Keizer (RisicoRegisseurs) stelt dat bedrijven de gevolgen van uitval nog steeds onvoldoende overzien.
Toms (Global Cyber Risk & Security Expert) onderschrijft dit: "Het gaat om bedrijfscontinuïteit. Daar is veel te weinig aandacht voor." Het punt, volgens Hiddink, is dat installateurs hun eigen gang kunnen gaan zonder duidelijke norm. "Dit terwijl het mkb helemaal afhankelijk is van de expertise van die installateur." Zorg daarom voor een norm die duidelijke minimumeisen stelt.
Volgens Toms leidt dat al snel tot 'rule based' gedrag. "Eigenlijk moet een norm een kader geven om ná te denken." In de AVG wordt eigenlijk niets concreets over fysieke IT-beveiliging gezegd. "Als het niet concreet is, wordt er geen geld uitgegeven," weet Borger van Tesorion. Van Rijssen (X-ICT) brengt de discussie tot een conclusie: "Wet- en regelgeving hebben pas echt impact."
Toch zou Hiddink (Rittal) willen onderzoeken of je een bepaald normenkader niet toch kunt introduceren. Keizer (RisicoRegisseurs) heeft in dat verband een advies: "Een certificering of normenkader kun je met een brancheorganisatie realiseren. Zoals veel branches, van elektriciens tot Keurslagers certificeringen of normen hebben."
Borger wijst daarbij wel op een mogelijke consequentie: "Als je dan naar die norm reageert op een RFP, dan zal de prijs van jouw oplossing stijgen. Het is de vraag of je bij dit thema dan nog steeds de opdracht krijgt. Wellicht prijs je jezelf met een normenkader wel uit de markt."
Cooijmans (Catharina Ziekenhuis) herkent dit wel: wie alle risico's op een rij zet vindt vast veel aspecten die beter kunnen. "Dat gaat geld kosten, en zeker bij het mkb is voor dit onderwerp nu eenmaal weinig tot geen budget."

Bewustwording

Dat nu is volgens Hiddink precies het probleem. Daarom begint elke vorm van verbetering volgens hem met bewustwording. "De eindklant weet het niet, dus moeten wíj de kennis in de markt vergroten. Zo is het uiteindelijk bij cybersecurity ook gegaan." De bewustwording moet dan in zekere zin beginnen met de partijen die het mkb van apparatuur en services voorzien.
Borger denkt met Hiddink mee: "De meeste partijen verdienen hun geld echter niet aan die beveiliging maar aan de data, de services, de hardware in de IT-behuizing. Dat is een heel andere rol." Hiddink geeft het niet op. "Dan moet die installateur, of IT-reseller wellicht samen met iemand die verstand heeft van gebouwbeveiliging op pad."
Toms (Global Cyber Risk & Security Expert) reageert op een eerdere uitspraak: "Als je de bewustwording op een hoger niveau wilt vergroten dan zou dat theoretisch moeten starten op het hoogste niveau: de overheid. Die komt dan met normen. Dat werkt kostenverhogend voor iedereen, maar maakt de BV Nederland wel veiliger." Nu vult regelgeving als NIS2 dit deels wel in, "maar echte bewustwording moet uit de sector zelf komen."



Hoe nu verder?

Aan het eind van het gesprek keert André Hiddink namens medeorganisator Rittal terug naar de initiële vraag van de discussie: zijn er mogelijkheden om bedrijfscontinuïteit vorm te geven door aan de fysieke IT-beveiliging meer aandacht te besteden? Hij geeft een opsomming van de thema's die in dat kader tijdens de bijeenkomst aan bod kwamen. "Moet er een norm, een bewustwordingscampagne of een richtlijn komen, of vinden we NIS2 en AVG genoeg?"
In het verlengde daarvan: "stel dat iemand te maken heeft gehad met dataverlies of een ander incident als gevolg van niet toereikende of fout geplaatste racks, of behuizingen, bij wie kan die dan terecht voor advies om een herhaling te voorkomen?" Er is, constateert Hiddink, geen grip op het thema: iedereen geeft een eigen invulling aan de bouw en inrichting van de omgevingen voor de fysieke IT. "We zien of onderkennen de risico's niet, tenzij we te maken hebben met een incident."
"Je moet en zult bij risicoanalyses ook de fysieke beveiliging moeten inbedden," is de reactie van Toms (Global Cyber Risk & Security expert). Keizer vult aan: "Maar niet voordat je een gedegen dreigingsprofiel hebt opgesteld waarbij een directie zich de vraag moet stellen tegen welke concrete risico's beveiliging georganiseerd moet worden. Beide elementen zorgen in elk geval voor bewustwording bij het management."
Borger (Tesorion) is het daarmee eens en brengt het vraagstuk terug tot de kern: "Als je de risico's goed snapt zijn toereikende maatregelen eenvoudig te verzinnen." Hij gaat erop door als hij stelt dat je door na te denken over processen in een organisatie eigenlijk automatisch ook op de fysieke risico's, en het belang van fysieke beveiliging, komt. "Als je simpelweg naar een proces kijkt met de vraag: wat kan hier fout gaan? Hoe is dit proces te manipuleren?" Dan constateer je al snel dat een simpel slot niet afdoende is.
Cooijmans (Catharina Ziekenhuis), spiegelt die uitspraak aan zijn eigen organisatie: "Als je bedenkt wat er bij een zorginstelling aan data op de servers staan, dan is duidelijk dat het daarbij gaat om de meest privacygevoelige gegevens. Die wil je beschermen. De waarde en het belang van die data overstijgen de waarde van de fysieke server." Hij zegt daarmee indirect: relateer de prijs van de serverkast niet alleen aan de kostprijs van de hardware die erin staat, maar realiseer je dat het belang van een goede fysieke IT-omgeving veel verder gaat. Van Rijssen (X-ICT) onderschrijft dit. "Zoals elke vorm van beveiliging moet je het denken in silo's overstijgen. Security gaat over alle disciplines heen." ■