ROOD-WIT VERBINDT:

DIGITAAL SLOT OP KAS ÉN KASTEEL

Elk bedrijf wil een veilige werkplek zijn. Daar hoort ook digitale veiligheid bij, zodat cybercriminelen geen vrij spel krijgen. BICT Groep biedt oplossingen en expertise om digitale aanvallen en datalekken te voorkomen. Dat het bedrijf hiermee niet alleen in de glastuinbouw succesvol is, bewijst het op Het Kasteel.

Vrijwel iedereen krijgt er vroeg of laat mee te maken: cybercriminaliteit. Recent nog verschenen berichten in het nieuws over een ransomware-aanval op MediaMarkt, waarbij 43 miljoen euro aan losgeld werd geëist in ruil voor toegang tot de gegijzelde systemen. Criminelen azen meer en meer op data van bedrijven en dus is het zaak om die gegevens goed te beschermen. Of je nu een tuinbouwbedrijf bent of een betaald voetbalclub.

NIET AAN- OF UITZETTEN

BICT Groep biedt betrouwbare IT-security voor bedrijven, ongeacht de grootte of achtergrond. Binnen de glastuinbouw geniet het bedrijf inmiddels veel bekendheid door de samenwerking met toonaangevende partijen, maar ook buiten de sector heeft BICT Groep relaties die tot de verbeelding spreken. Zoals voetbalclub Sparta uit Rotterdam. “Samen met ESET, dat beveiligingssoftware ontwikkelt, ontzorgen wij Sparta volledig op gebied van IT en cybersecurity”, vertelt directeur Bas Voermans. “Als BICT Groep hebben wij goede IT-systemen en datacenteroplossingen, maar cybersecurity is echt een apart specialisme. Daar moet je dedicated mee bezig zijn. Daarom zijn wij een partnership met ESET aangegaan en kunnen wij nu een IT-oplossing aanbieden waarin het cybersecurity-portfolio van ESET in het DNA zit verwerkt. Je kunt dat als klant niet aan- of uitzetten, het zit er gewoon in. Daarmee zorgen wij ervoor dat de basis goed is.”

Concreet omhelst dat volgens Voermans drie stappen, de zogenoemde ‘driehoek’, waarmee een groot deel van het digitale domein onder controle wordt gehouden. “Endpoint security is in feite de antivirussoftware, die we preventief inzetten om virussen te weren. Endpoint encryptie wordt toegepast op het moment dat het kwaad toch is geschied, zodat dit niet systeem-breed impact heeft en de risico’s beperkt blijven. Tweefactorauthenticatie tot slot zet wachtwoorden van gebruikers om in een stukje geautomatiseerde beveiliging, waardoor je niet meer hoeft te werken met wachtwoorden die te kraken zijn.”

TOP 3 BEDRIJFSRISICO’S

ESET ontwikkelt deze oplossingen voor bedrijven en consumenten over de hele wereld en is inmiddels uitgegroeid tot het grootste IT-securitybedrijf van de Europese Unie. Het bedrijf beschermt en monitort 24/7 op de achtergrond en werkt beveiliging in real-time bij om gebruikers veilig te houden en bedrijven zonder onderbreking te laten werken, zo geeft CEO Dave Maasland aan. “Daarbij geloven wij heel sterk in de samenwerking met IT-dienstverleners zoals BICT Groep. In principe hebben wij geen directe klantrelatie zonder dat daar een IT-dienstverlener bij zit, omdat je beveiliging niet enkel kunt bekijken met een ‘securitybril’. Het gaat om een bedrijfsrisico, dus daar moet een IT-partner bij betrokken zijn die het bedrijf kent en die weet hoe het bedrijf waarde creëert. Cybersecurity is een van de vele risico’s waarmee een bedrijf te maken krijgt. Ik ben van mening dat het in de top 3 hoort, maar uiteindelijk is het aan de ondernemer zelf om te bepalen hoe belangrijk hij dit onderwerp vindt.”

Bas Voermans, directeur BICT Groep

Sparta-directeur Manfred Laros onderkent het belang van cybersecurity. Volgens hem zit de waarde ervan in de continuïteit van de onderneming. “Continuïteit betekent dat iedereen binnen de organisatie kan doen waarvoor hij of zij is aangenomen. Vaak is dat ICT-gerelateerd. Valt dat weg, dan komt de continuïteit in gevaar en kost dat uiteindelijk klanten en omzet. Om wedstrijden te kunnen spelen zijn wij volledig afhankelijk van ICT. Er komen op wedstrijddagen bijna 11.000 supporters in een piek naar het stadion, waardoor visuele controle niet meer mogelijk is. Je zult die supporters dus geautomatiseerd gefaseerd binnen moeten laten, maar je wilt ook weten wie er binnenkomen. Werkt de ICT niet, dan hebben wij dus direct een probleem met het zorgdragen dat supporters op een ordelijke manier het stadion binnenkomen. We willen wedstrijden organiseren waarbij supporters op een fijne en veilige manier aanwezig kunnen zijn. Dat is een van de grondbeginselen van het bestaan van een betaald voetbalorganisatie.”

NIET ÓF, MAAR WANNEER

Voermans: “Maar denk ook aan de betaalde voorzieningen voor eten en drinken voor supporters, de wifi in het stadion en het

verzenden van informatie vanuit de club. Voor een betaald voetbalorganisatie is omzet essentieel om op het veld te kunnen presteren. Dat mag dus niet stil komen te liggen." Toch is het volgens Voermans niet de vraag óf, maar wanneer je als bedrijf wordt getroffen door een cyberincident. "Als je op dat moment niets hebt geregeld, ga je enorm nat." Manfred Laros verduidelijkt dat een 'cyberincident' niet per definitie betekent dat je wordt gehackt of dat er een ransomware-aanval plaatsvindt. "Een verkeerd mailtje dat per ongeluk door een medewerker wordt aangeklikt, kan ook het hele netwerk plat leggen. Het kan soms dus iets heel simpels zijn waardoor het misgaat." Juist daarom is awareness bij gebruikers ook zo belangrijk, geeft Voermans aan. "Wij richten campagnes in om medewerkers te laten zien wat de risico's zijn. Daarbij gaat het niet alleen om dat mailtje van DHL, Interim Justitia of KPN, maar ook om mails die van jouw eigen leveranciers lijken te komen. Daarin wordt verwezen naar een specifieke order en alle gegevens in de mail kloppen, alleen het rekeningnummer is net even anders. Dat moet dan toch de trigger zijn om die mail niet te vertrouwen." Om bij het voetbal te blijven, iets soortgelijks overkwam Feyenoord enkele jaren geleden bij het overmaken van een transfersom naar een verkeerd rekeningnummer. "Feyenoord heeft die miljoenen niet teruggekregen", geeft Dave Maasland aan. "Zij hebben dat overleeft, maar zoiets kan bij elke voetbalclub zomaar de continuïteit in gevaar brengen."

Laros knikt instemmend. "Tijdens de transferperiodes draait het om aanzienlijke bedragen. Die worden vrij eenvoudig afgesproken met elkaar. Je kent de mensen vaak niet waarmee je zaken doet, alles gaat per mail. Dan komt die factuur en betaal je gewoon. Gezien de geldsommen waarom het gaat, is het essentieel dat het geld ook daadwerkelijk binnenkomt bij de club en dat dit niet ergens wordt onderschept. Daar zit onze kwetsbaarheid als voetbalclubs. De data van Sparta is waarschijnlijk minder interessant voor cybercriminelen."

DIGITALE HARTSTILSTAND

Toch moeten ook de gevolgen van een datalek volgens Voermans niet worden onderschat.

Directeur Dave Maasland van ESET

"Realiseer je goed dat gezichtsverlies ook een probleem kan worden. Bij dataverlies hebben bedrijven een meldingsplicht. Los van de waarde en inhoud van die data kunnen de consequenties enorm zijn. Het lekken van persoonsgegevens kan je als organisatie behoorlijk duur komen te staan en kan wel degelijk voor schade zorgen." Maasland: "Het gaat er ook niet om wat de data waard is voor criminelen, het gaat erom wat die data waard is voor het bedrijf zelf. Want die data wordt op slot gezet en wat is het jou dan waard om weer bij jouw eigen gegevens te kunnen? Bij het ene bedrijf zal de impact groter zijn dan bij het andere bedrijf. Maar in veel gevallen zal een ransomware-aanval leiden tot een digitale hartstilstand."

Maasland noemt het woord 'hartstilstand' bewust. "Want IT is de levensader van de organisatie. Tot nu toe realiseerden veel ondernemers zich dat onvoldoende, maar gelukkig begint dat langzaamaan te veranderen." Volgens Voermans komt dat gebrek aan urgentie bij bedrijven ook door het lage kennisniveau van veel IT-bedrijven die hen daarover moeten adviseren. "Ik zal zeker niet beweren dat wij de beste zijn, maar wij spelen wel topsport op dit gebied en kunnen onze klanten, mede door de samenwerking met ESET, daardoor goed adviseren en uitleggen wat nodig is en wat goed is. Als je wilt kun je eindeloos investeren in cybersecurity, maar het gaat er wat ons betreft om dat je een fundament hebt dat volstaat. En dan zeggen wij: goed is goed genoeg."

IN GESPREK BLIJVEN

Duidelijkheid en transparantie is waar bedrijven behoefte aan hebben, geeft Laros aan. "Of het nu gaat om een teler of de directeur van een voetbalclub, van al die moeilijke IT-termen begrijpen we allebei niet zoveel. Daarom is het belangrijk dat we in gesprek blijven met onze IT-partner, dat we uitleg krijgen wat er gebeurt en dat we kunnen vertrouwen op het advies dat we krijgen." Maasland meent dat bedrijven ook veel profijt kunnen hebben door kennis en ervaringen uit te wisselen. "Dat gebeurt bij banken, maar bijvoorbeeld ook in de Brainport Eindhoven en de Port of Amsterdam. Door jezelf als sector te verenigen en IT-mensen bij elkaar aan tafel te zetten, kun je heel veel leren."

De komende jaren blijft BICT Groep hard werken om de klant op termijn 'onsterfelijk' te maken als het gaat om cybersecurity. "We hebben geïnvesteerd in een eigen Security Operations Center, gebaseerd op de oplossingen van ESET. Maar wat als die medewerker dan toch een kwetsbaar mailtje heeft geopend of als er toch ransomware actief is? Op dat moment kunnen wij het systeem door middel van 'Disaster Recovery' (DR) binnen een half uur terugbrengen in de oorspronkelijke situatie", zegt Voermans. "Heb je alleen een databackup, dan kost het dagen tot weken voordat je alles hebt hersteld. Wij maken met onze DR snapshots van de complete omgeving, dat wil zeggen de systeemstatus en de datum, waarmee we alles heel snel kunnen restoren als dat moet. Dat wordt naar de toekomst toe nog veel belangrijker."