Marcel de Boer, CFO Hoppenbrouwers Techniek:

‘Cybersecurity is geen IT-feestje’

In juli 2021 legden Russische hackers wereldwijd duizenden bedrijven plat. Hoppenbrouwers Techniek bleek één van de slachtoffers. Een weekend lang was het alle hens aan dek om de gaten te dichten. De schade viel uiteindelijk mee, maar bij Hoppenbrouwers is een gevoel van kwetsbaarheid blijven hangen. “Het internet is als het Wilde Westen en elke dag rammelen boeven aan je deuren”, zegt financieel directeur Marcel de Boer.

De hack vond plaats op vrijdagavond 2 juli, ergens rond zeven uur ’s avonds. En hoe zoiets opgemerkt wordt? Waarschijnlijk vaak op dezelfde manier, namelijk door een werknemer die bij de ICT-afdeling melding maakt dat hij het systeem niet in kan. Meestal is dat niet iets om je erg veel zorgen over te maken, maar dat veranderde dit keer snel. ICT kon de problemen niet oplossen, ontdekte verdachte bestandjes op de server en ziet vervolgens op Twitter dat er wereldwijd bedrijven met het probleem te maken hebben. Hoppenbrouwers blijkt te zijn gehackt door REvil, een Russische hackersclub, die laat weten de systemen weer vrij te geven als Hoppenbrouwers 50.000 dollar overmaakt, binnen zes dagen. En deed Hoppenbrouwers dat niet, dan verdubbelde het bedrag.

Dat valt voor een bedrijf met destijds 1500 werknemers en een omzet van 250 miljoen euro wel mee eigenlijk.

“Het was een generieke aanval, REvil had geen zicht op welke bedrijven het aanviel. Meestal wordt bij dit soort hacks een bedrag aan losgeld geëist dat ongeveer 2 procent van de jaaromzet bedraagt. Voor ons viel dat dus wel mee, maar wij hebben dat niet betaald.”

Waarom niet?

“Die vraag hebben wij ons niet eens gesteld. Wij hebben namelijk al heel snel onze cybersecurityverzekeraar Chubb ingeschakeld en zij hebben toen IT-securitybedrijf Northwave naar ons toegestuurd, dat wél op het linkje klikte dat REvil in zijn bestandje had meegestuurd. Northwave heeft een protocol over hoe ze dit soort zaken oppakken. Zij zijn toen in contact getreden met REvil.”

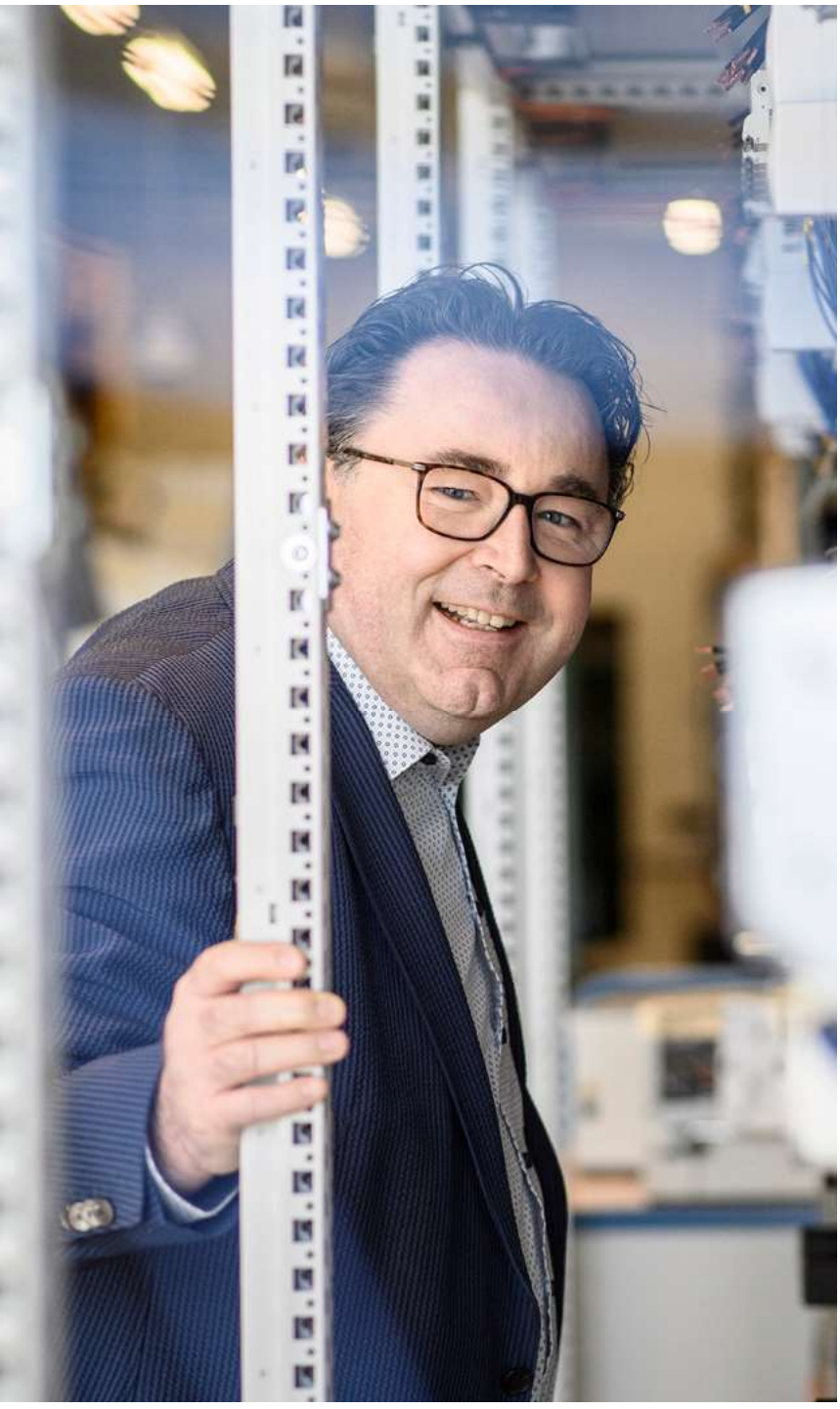
Auteur
Tijdo van der Zee

Marcel de Boer

Foto's: Christiaan Krop

Jullie hebben na afloop van de digitale kidnapping een boek geschreven met de eenvoudig maar doeltreffende titel 'Hack'. Daarin wordt van uur tot uur beschreven hoe het er in dat weekend aan toeging. Ik kan me niet aan de indruk onttrekken dat het op de een of andere manier erg gezellig was.

"Iedereen werd opgetrommeld. Natuurlijk de mensen van IT, maar ook alle andere werknemers die verstand hebben van de techniek. Mensen die bijvoorbeeld werken bij industriële automatisering. Wat dat betreft zitten we als installatiebedrijf natuurlijk goed. Veel mensen moesten noodgedwongen hun kinderen meenemen, dus daar werd dan weer opgepast door andere collega's en zo ontstond er inderdaad een hartverwarmend saamhorigheidsgevoel. En daar word je dan ook wel trots van."



"Wat ik van dat weekend geleerd heb, is dat cybersecurity geen IT-feestje is. Dat wist ik al wel, want bij Hoppenbrouwers heeft IT al een plek aan de bestuurstafel, maar door zo'n aanval word je daar extra bewust van. Onze mensen van ICT klapten hun laptop open en gingen als een razende aan de slag, maar daarmee was het probleem niet opgelost. Er moest nog zoveel meer geregeld worden.

'Hoe goed je beveiliging ook is, je blijft kwetsbaar'

Zo heeft onze directeur Henny de Haas in dat weekend de leiding genomen en zoveel mogelijk mensen gemobiliseerd. Daarnaast heeft hij vragen van de pers open en eerlijk beantwoord en er is door onze communicatie-afdeling gecommuniceerd naar alle klanten. Een aantal klanten hebben daarop contact opgenomen en om extra informatie gevraagd.

Daarnaast moest er een organisatie worden opgetuigd om heel snel al onze laptops uit het hele land naar het hoofdkantoor in Udenhout te brengen. We hadden daarbij het geluk dat onze e-mails op een andere server draaide, die niet was aangevallen. Maar verder moest het allemaal gebeuren terwijl we de stekker uit al onze systemen hadden getrokken."

Jullie waren na het weekend weer up and running. Hoeveel schade hebben jullie geleden?

"Al met al was dat zo'n 4 ton, die we vergoed hebben gekregen van de verzekeraar."

Waar zat het probleem?

"REvil had ingebroken op Kaseya, dat is servermanagementsoftware die wij gebruikten. En via Kaseya konden ze inbreken op systemen van duizenden gebruikers wereldwijd. Een paar weken eerder hadden ethische hackers van de Nederlandse non-profit DIVD al gewaarschuwd voor kwetsbare plekken in Kaseya. Maar het lukte Kaseya niet snel genoeg om die te repareren. Een paar dagen na de hack kregen we een berichtje van Kaseya of ze nog iets konden doen. Ik dacht: 'Had die vraag vorige week aan ons gesteld!'. We waren al van plan om afscheid te nemen van Kaseya, maar die hack heeft dat proces natuurlijk enorm versneld. We hebben nu beveiliging van Microsoft.

Dit heeft me wel doen beseffen dat cybersecurity iets is wat je in de hele keten moet aanpakken, omdat veel systemen zo vervlochten zijn. Kaseya zat met zijn software werkelijk op alle devices binnen ons bedrijf. Dan maakt dat je erg afhankelijk."

Maar andersom geldt dat ook: Hoppenbrouwers is ongetwijfeld verbonden met gebouwbeheersystemen van klanten. Dat maakt dus dat jullie voor die klanten ook een potentieel risico zijn.

"Ja, dat is waar en daarom hebben wij in dat weekend voor de zekerheid ook al die stekkers eruit getrokken en die klanten geïnformeerd. Het is bij Hoppenbrouwers niet zo dat dan ineens de lichten uitgaan in de gebouwen die wij beheren. Er draaien bij ons geen systemen die rechtstreeks klantsystemen aansturen; hun gebouwbeheersystemen draaien op zichzelf."

Marcel de Boer

Marcel de Boer is 52 jaar. Hij studeerde bedrijfseconomie in Eindhoven en heeft daarna nog verschillende opleidingen gevolgd waaronder HOFAM tot Qualified controller en aan de Erasmus Universiteit. Marcel werkt sinds 1997 bij Hoppenbrouwers Techniek. In deze jaren groeide het bedrijf van 70 naar 1700 medewerkers. Sinds 2008 is hij financieel directeur bij Hoppenbrouwers waar hij naast financiën ook verantwoordelijk is geweest voor onder andere IT.

Zijn er data-gegevens gestolen?

"Gelukkig niet. Daar waren we natuurlijk heel erg bang voor, maar daar is REevil niet op uit geweest. Maar bij een volgende hack kan dat zomaar wel het geval zijn."

Jullie vertellen in alle openheid jullie verhaal en dat is prijzenswaardig. Deels zal dat ermee te maken hebben dat jullie de cybersecurity al goed geregeld hadden. Dan valt er jullie dus niet zoveel kwalijk te nemen. Wat is nou een tip die andere bedrijven direct ter harte zouden moeten nemen?

"Je kan vanaf morgen al aan de slag met een aantal technische maatregelen. Een heel belangrijke is Two Factor Authentication, 2FA, waarbij je alleen via een tweestapsmethode kan inloggen op het bedrijfsnetwerk. Veel grote bedrijven hebben dat waarschijnlijk al lang geregeld, maar Northwave vertelde me dat 90 procent van de bedrijven dit nog helemaal niet ingevoerd heeft. Die werken met een simpele gebruikersnaam en een wachtwoord, dat vaak ook nog eens makkelijk te kraken is. Dat vind ik eigenlijk onverantwoord. Je maakt het hackers dan wel heel makkelijk en je neemt ook je verantwoordelijkheid niet in de al eerder genoemde keten.

Je moet bedenken dat een wachtwoord van acht karakters in enkele milliseconden te kraken is. Northwave monitort nu het aantal aanvallen dat op ons bedrijf gepleegd wordt en dat zijn er honderden per dag. Ik heb een wat grimmiger beeld gekregen van het internet. Het was niet dat ik het vroeger zag een fleurig paradijs, maar nu beschouw ik het wel een beetje als het Wilde Westen, waar boeven aan de lopende band aan je deuren rammelen om te kijken of ze ergens een ingangetje kunnen vinden."

Jullie hebben nu een stevige digitale beveiligingsmuur om je bedrijf heen gebouwd, maar 100 procent veiligheid zal toch een illusie zijn.

"Ja, dat besef ik goed. Je hebt altijd het risico dat een werknemer op een ongeconcentreerd ogenblik op een linkje in een phishingmail klikt en je hebt een probleem. Sterker nog, ik sluit niet uit dat het mij ooit overkomt. Die aanvallen zijn steeds geraffineerder. Maar ik geloof wel dat we ons nu zo georganiseerd hebben, dat we aanvallen, ook als de aanvallers eenmaal binnen zijn, sneller de baas zijn. Maar goed, elke aanval is anders en ik geloof dan ook niet dat je in een calamiteitenhandboek alle details zou moeten uitwerken. Noteer de namen en contactgegevens van de mensen die ingeschakeld moeten worden, verdeel intern de rollen en dan is het op het moment dat het gebeurt toch improviseren en doen wat er gedaan moet worden."

'Veiligheid moet je ook in de keten organiseren'