TEKST: MARCEL TE LINDERT | **FOTO'S:** TWITTER, DALTI, TESORION, BAKKER, PEXELS, FREESTOCK, KEES TORN

Elk transportbedrijf kan slachtoffer worden van gijzelsoftware

Voorkom de hack!

Het aantal incidenten met gijzelsoftware stijgt, ook in de transportsector. De technologische en organisatorische oplossingen zijn veelal beschikbaar, maar een gebrek aan aandacht staat implementatie daarvan in de weg. Pas na een hack lijken transportbedrijven in actie te komen. Goede cybersecurity kost echter wel geld.

In juni 2017 was Maersk Line een van de zevenduizend bedrijven die werden getroffen door een wereldwijde aanval met gijzelsoftware. De containerrederij kon enkele weken niet werken en moest twee containerterminals in de Rotterdamse haven tijdelijk sluiten. Uiteindelijk moest het bedrijf 4.000 servers, 45.000 pc's en 2.500 applicaties herinstalleren. De totale schade wordt geschat op 300 miljoen euro.

Maersk is niet de enige. In de nacht van 4 op 5 april jongstleden werd Bakker Logistiek het slachtoffer van gijzelsoftware, waardoor de operatie in de warehouses in Zeewolde, Tilburg en Heerenveen stil kwam te liggen. De logistiek dienstverlener kon geen orders ontvangen, geen goederen verzamelen en geen ritten plannen. Dat leidde tot grote gevolgschade bij Albert Heijn, dat dagenlang kampte met lege kaasschappen.

OOK MKB-BEDRIJVEN

Het zijn allang niet meer alleen de grote bedrijven die het doelwit zijn van hackers. Op een vrijdag in november vorig jaar was het raak bij Janssen Logistics, een transportbedrijf met 25 medewerkers uit Ittervoort. De hackers kwamen binnen via een openstaande poort in het Remote Desktop Protocol (RDP), waarmee van afstand kan worden ingelogd op een Windows-server. Vanwege een lek in de gijzelsoftware bleef de schade beperkt en konden de chauffeurs de maandag erop gewoon weer de weg op.

René Knapen is niet verbaasd dat ook mkb-bedrijven slachtoffer worden. "Probeer je eens te verplaatsen in een hacker. Die probeert eerst de grote vissen in de vijver te vangen. Maar als die zich daartegen weten te wapenen, komen uiteindelijk ook de kleinere vissen aan de beurt", stelt de voorzitter van Dalti, de belangenvereniging van ICT-leveranciers in transport en logistiek.

Cybersecurityspecialist Tesorion ziet het aantal meldingen over hacks van zowel grote als kleine bedrijven snel stijgen. "Met name in het begin van het jaar was het zo druk dat we regelmatig 'nee' moesten verkopen en moesten doorverwijzen naar andere partijen", vertelt Lodi Hensen, verantwoordelijk voor het Computer Emergency Response Team (CERT) van Tesorion. "Wij vormen de digitale brandweer. Als bedrijven een incident melden, komen wij hen helpen. Veel meldingen gaan over gijzelsoftware, maar ook over gehackte mailboxen. En bij oplossingen zoals Microsoft 365 bieden de accounts die aan deze mailboxen zijn gekoppeld ook weer toegang tot andere applicaties zoals Sharepoint."

AANDACHTSPROBLEEM

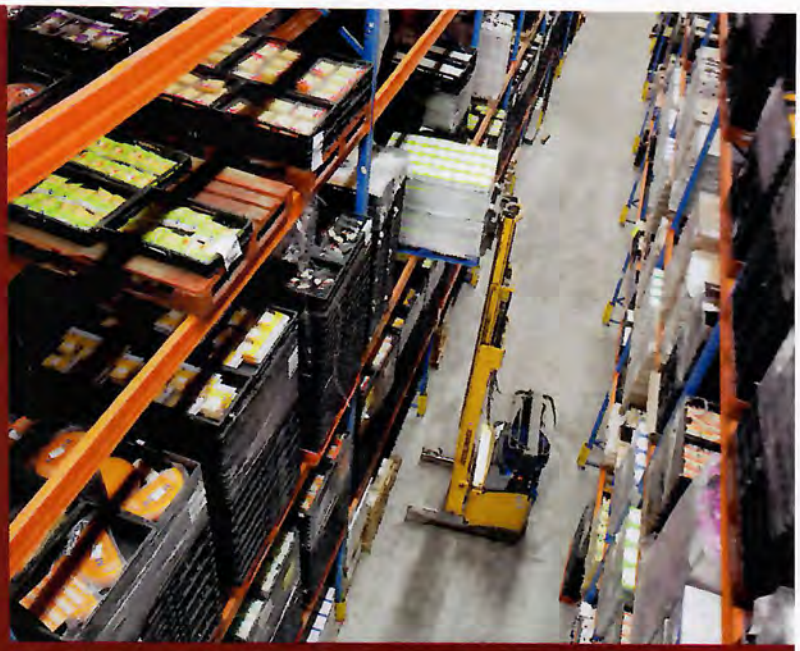
Hackers die een slachtoffer uitzoeken, kijken niet zozeer naar de waarde van het bedrijf maar naar de wijze waarop het bedrijf omgaat met cybersecurity. "Het is veel meer een aandachtsprobleem dan een technisch probleem. Als cybersecurity niet op de agenda staat van het management, is het bedrijf vroeg of laat een keer aan de beurt", stelt Knapen, die eraan toevoegt dat in veel transportbedrijven niet alleen het bewustzijn maar ook de kennis ontbreekt. "Een transportondernemer weet precies wat hij moet doen als in zijn vrachtauto het lampje van het oliepeil aanspringt. Maar als je hem vraagt wat hij moet doen als hij gijzelsoftware aantreft, blijft een antwoord vaak uit."

Veel transportbedrijven weten bovendien niet hoe kwetsbaar hun netwerk is. Tesorion constateert regelmatig dat ze geen volledig zicht hebben op de apparatuur die aan het netwerk hangt. "Onlangs waren we bij een bedrijf waarbij het probleem zat in het camerasysteem dat aan het internet was gekoppeld. Dat had ongetwijfeld een goede reden, bijvoorbeeld om vanaf huis het bedrijfspand in de gaten te kunnen houden. Maar dat bood ook toegang tot het bedrijfsnetwerk", verklaart Hensen.

GESTOLEN DATA

Cybersecurity vraagt niet alleen om aandacht van managers, maar van alle medewerkers binnen het bedrijf. Knapen geeft het voorbeeld van een klant van zijn eigen softwarebedrijf TANS, leverancier van trans-

portmanagementsystemen. "Die klant belde op omdat alle commerciële data waren gestolen. De dader was een voormalige medewerker. Twee maanden voor zijn uitdiensttreding had hij van een collega het wachtwoord geleend met de smoes dat hij zijn eigen inloggegevens kwijt was. Na zijn uitdiensttreding heeft hij dat geleende wachtwoord gebruikt om in te breken."
Het bewustzijn vergroten hoeft volgens Knapen niet moeilijk te zijn. "Vraag bijvoorbeeld in functioneringsgesprekken wanneer medewerkers voor het laatst hun wachtwoord hebben gewijzigd. Als je in gesprekken daaraan structureel aandacht blijft besteden, wordt cybersecurity vanzelf een thema dat gaat leven."
Belangrijk is tweestapsverificatie, een extra beveiliging om te checken of de gebruiker inderdaad de persoon is aan wie de inloggegevens van een applicatie zijn toegekend. Denk aan een cijfercode die naar de telefoon wordt gestuurd en die op het scherm ingevoerd moet worden. "Het verbaast me dat niet meer software- en cloudleveranciers hun verantwoordelijkheid nemen en beveiligingsoplossingen zoals tweestapsverificatie als standaard inlogprocedure opnemen. Als je een nieuwe vrachtwagen koopt, verwacht je ook dat die standaard werkende remmen heeft. En niet dat je die als extra optie moet aanvinken", stelt Hensen.



Het warehouse met versproducten bij Bakker Logistiek kon niet meer goed functioneren na de aanval met gijzelsoftware.

GROEN SLOTJE

Naast tweestapsverificatie zijn nog meer technische maatregelen nodig. Denk aan een goede firewall en antivirussoftware die correct zijn geïmplementeerd en voortdurend worden geactualiseerd. Of aan segmentatie van het bedrijfsnetwerk, zodat een aanval op één applicatie niet kan overslaan op andere. Vervang daarnaast oude hardware die niet meer goed beveiligd kan worden. Migreer naar de laatste versie van de software en zorg dat de laatste beveiligingsupdates geïnstalleerd zijn. Beveilig de website met een SSL-certificaat, herkenbaar aan het groene slotje. Zeker als die wordt gebruikt voor het invoeren van orders of uploaden van bestanden.
Het delen van data met opdrachtgevers of andere ketenpartners vereist extra aandacht. Wie databestanden uitwisselt, moet daarvoor een beveiligde SFTP-server gebruiken. Die bestanden kunnen met encryptietechnologie worden versleuteld, waarbij de sleutel separaat naar de andere partij wordt verstuurd. Voor het inloggen of integreren van externe systemen heeft de logistieke sector onder de naam iSHARE een afsprakenstelsel opgezet, dat waarborgt dat de externe partij betrouwbaar is. Bij een dataverbinding tussen twee vestigingen verdient het aanbeveling om een Virtual Private Network te creëren. Met een dergelijke VPN-verbinding beschikken bedrijven over hun eigen beveiligde tunnel, zodat niemand het dataverkeer kan onderscheppen.

GOEDE BACK-UP

Als het goed is, zou het terugzetten van een back-up voldoende moeten zijn om een aanval met gijzelsoftware te stoppen. Maar het maken van een back-up wordt vaak onderschat. Belangrijk is de vraag hoeveel dataverlies het bedrijf zich kan permitteren en hoe snel het IT-systeem moet worden hersteld. Dat bepaalt hoe vaak een back-up moet worden gemaakt. De volgende vraag is waar die wordt opgeslagen. Daarvoor zijn speciale kluizen of beveiligde clouds beschikbaar. "Als de back-up op dezelfde server staat waarop ook de hacker zit, schiet dat niet op. De hacker kan de back-up dan onklaar maken", zegt Hensen. Knapen: "En vergeet niet af en toe de back-up te controleren door die terug te zetten. Net zoals we bij een brandslang ook af en toe de kraan moeten opendraaien om te checken of er nog steeds water uitkomt."
De ontwikkeling richting cloud is een stap vooruit als het gaat om veiligheid. Over het algemeen is werken in de cloud zoals die van Microsoft een stuk veiliger dan werken met een server onder je bureau. "Maar dat ontslaat je niet van de verplichting om de beveiliging op orde te brengen", waarschuwt Hensen. "Zonder aanvullende beveiligingsmaatregelen zoals tweestapsverificatie heeft een hacker nog steeds aan een gebruikersnaam en een wachtwoord voldoende om toegang te krijgen tot de data in die cloud."

GEVOLGSCHADE

Het incident bij Bakker Logistiek laat zien dat niet alleen logistiek dienstverleners kunnen worden getroffen, maar ook opdrachtgevers en afnemers. Met name bij versproducten kan de gevolgschade groot zijn. Als de hack lang duurt, moeten versproducten worden weggegooid. Als de levering weer op gang komt en een inhaalslag moet plaatsvinden, is het de vraag of toeleveranciers snel genoeg nieuwe versproducten kunnen aanleveren. "De hele keten raakt verstoord. Het kan twee maanden duren voordat het effect daarvan is verdwenen", aldus Knapen.
De voorzitter van Dalti roept transportbedrijven op om een risico-inventarisatie te maken. Wat kan er fout gaan en wat zijn de consequenties daarvan? Wat is de mogelijke schade die ontstaat? Dekt de verzekering alleen de directe schade of ook de vervolgschade? "Probeer daarin transparant te zijn. Bespreek de risico's met opdrachtgevers en andere ketenpartners. Logistiek dienstverleners kunnen zich op dit punt onderscheiden. Bedrijven die hun transport hebben beveiligd en TAPA-gecertificeerd zijn, vragen ook een ander tarief."
Hensen raadt aan om naast een risico-inventarisatie ook een draaiboek te maken. "Het is handig dat je van tevoren weet wat je moet doen bij een cyberaanval. Al is het maar een telefoonnummer van degene die kan helpen bij het oplossen van het probleem. En realiseer je dat niet elk incident goed afloopt. In principe is het advies om bij een aanval met gijzelsoftware geen losgeld te betalen, want dat houdt een crimineel businessmodel in stand. Maar soms is dat de enige oplossing, omdat het bedrijf anders helemaal opnieuw moet beginnen met een grote kans om failliet te gaan. En na betaling is het de vraag of het lukt om de oude situatie te herstellen en of het ontsleutelprogramma daadwerkelijk doet wat het belooft. Helaas zijn niet alle hackers zijn even goed in het maken van gijzelsoftware."

EISEN IN TENDERS

Cybersecurity kost geld, geeft Knapen toe. "Veel transportbedrijven reserveren geen geld voor investeringen in ICT, laat staan in ICT-beveiliging. Maar dat geld is wel nodig. Transportondernemers doen 's avonds wel hun achterdeur op slot als ze naar bed gaan. Dat slot kost ook geld."