Logistiek slecht beschermd tegen hackers

Logistiek dienstverleners onvoldoende beschermd tegen cybercrime

Vooral kleinere en middelgrote logistieke bedrijven zijn onvoldoende beschermd tegen cybercrime, maar ook grote bedrijven onderschatten de gevolgen. Dat constateert beleidsadviseur Hélène Minderman van Transport en Logistiek Nederland. De schades kunnen oplopen van 50.000 euro tot 1 ton per geslaagde cyberaanval. Aanleiding voldoende om beheersmaatregelen te nemen.

In totaal lijdt het Nederlands bedrijfsleven acht miljard euro (!!) schade als gevolg van cybercrime. Er is geen betrouwbaar statistisch overzicht van het aantal cyberaanvallen en de gevolgschade in de logistieke branche. Desondanks schat risicoadviseur en verzekeringsmakelaar Aon in dat bedrijven in deze sector tientallen keren per dag te maken krijgen met bijvoorbeeld pogingen tot ransomware, een chantagemethode op basis van kwaadaardige software via het internet. Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te ‘bevrijden’. En natuurlijk zijn daar de DDos-aanvallen waarbij heel veel computers – vaak vanaf verschillende locaties ter wereld – één server of website bestoken om deze traag of in het ergste geval onbereikbaar te

maken. Dit kan de supply chain en het logistieke proces van bedrijven ernstig ontregelen met alle economische schade van dien. Datalekken of onvoorzichtig omgaan met informatie kan leiden tot misbruik van vrachtboekingssystemen waardoor vrachten niet op de juiste plek van bestemming aankomen of inbreuk op privacygevoelige data van klanten en leveranciers.

Aantal cyberaanvallen in de logistieke sector neemt toe

Het aantal schademeldingen als gevolg van cybercrime neemt volgens Minderman hand over hand toe. “Helaas heb ik geen volledig beeld, want niet elk bedrijf meldt schade bij TLN. Maar uit recent onderzoek onder onze leden blijkt welke strategieën cybercriminelen gebruiken en hoe ze opereren in de logistieke sector. De modus operandi zijn heel slinks, zoals het versturen van nepmails naar personeelsleden met een link naar een zogenaamd cadeautje. Na een druk op de link wordt er malware op de server geïnstalleerd en vervolgens geld gevraagd om de malware te verwijderen. Of na een hack in de betaalgegevens manipuleert de hacker het rekeningnummer zodat het bedrag over wordt gemaakt op de rekening van de cybercriminelen”, schetst de beleidsadviseur van de brancheorganisatie de illegale praktijken.

Risicomanagement staat nog in de kinderschoenen

Volgens Minderman staan risicomanagement en beheersing van cyberdreiging in de logistieke sector nog in de kinderschoenen. De grote bedrijven hebben daar security managers voor, maar het kleine mkb kan die specialisten niet betalen of opleiden. TLN probeert wel via o.a. online voorlichting de bewustwording over de gevaren en impact van cybercrime op je organisatie op gang te brengen. Die informatie vertalen we zo veel mogelijk naar de logistieke sector, anders blijft het probleem te abstract”. Aon - cybercrimebestrijding en preventie is één van zijn specialismen - heeft de laatste jaren flink geïnvesteerd in expertise en kennisoverdracht over cybercrimebestrijding , preventie en verzekering. Specialisten zijn opgeleid om bedrijven te adviseren over informatiebeveiliging, privacybescherming en de financiële impact van cyberattacks. “We onderscheiden drie risicofactoren op dit terrein: criminaliteit, technisch systeemfalen en incidenten door onbekwaam menselijk handelen. Zo zijn er medewerkers die grote databestanden met privacygevoelige informatie

versturen via bijvoorbeeld WeTransfer. Die dienst biedt echter geen waarborgen voor databescherming, dus per definitie ongewenst voor dat soort bestanden. Maar de applicatie is lekker makkelijk in gebruik, dus de gebruiker bedenkt niet welke gevaren er kunnen ontstaan", zegt managing consultant Dennis de Hoog van Aon.

Vanuit zijn praktijkervaring heeft De Hoog de indruk dat veel logistieke bedrijven onvoldoende beschermd zijn tegen cybercrime. "Het is niet hun core-business en de IT-investeringen in een optimale bescherming zijn best wel fors voor de bedrijven, waardoor zij meestal niet voldoende investeren. Ook zijn zij vaak afhankelijk van externe partijen die hen bij moeten staan in het geval van een incident."

Logistieke data zijn interessant voor cybercriminelen

Desalniettemin is een investering wel gerechtvaardigd als je in de logistiek werkt. De sector verwerkt veel interessante data voor cybercriminelen, zoals vrachtbrieven, betaalgegevens van klanten, diefstalgevoelige goederen die vervoerd worden, et cetera. Als daar een digitale kink in de kabel komt, zijn de economische gevolgen gelijk fors: "Een stagnatie in de distributie van enkele uren kost al gauw tienduizenden euro's", becijfert De Hoog. "Of stel dat je een dag niet kunt beschikken over je WMS doordat het systeem op slot is gezet, dan gaat het al gauw om een aantal tonnen per dag vanwege kosten en omzetderving. Zeker mkb-bedrijven zijn zeer kwetsbaar voor een geslaagde cybercrime-aanval".

Aon ondersteunt bedrijven bij voorkeur in preventieve zin. "We gaan bij dit traject een bedrijf zo goed mogelijk voorbereiden op een cyberaanval. Welke digitale tools zetten we hiervoor in? Welke expertise schakelen we daarvoor in om een crisis te voorkomen? Technische maatregelen bijvoorbeeld zijn het installeren van firewalls, detectie-software van cyberaanvallen en het toekennen van autorisaties die de bedrijfsserver mogen gebruiken. Daarnaast zetten we een risico-management op poten. We gaan met het bedrijf inventariseren welke data-applicaties gevoelig zijn voor hacks, lekken en cyberaanvallen en checken in hoeverre zij beschikken over een adequate back-up mocht er data verloren gaan. En we gaan na welke databases met persoonlijke en klantinformatie gevoelig zijn voor inbreuk. Wij bieden inzicht in de belangrijkste digitale risico's en maken duidelijk hoe het management en personeel vervolgens moeten opereren om het risico te verkleinen".

Ook het verzekeren tegen cybercrime komt ter sprake. Bedrijven kunnen tegenwoordig een verzekering afsluiten die past bij hun behoeften en risicoprofiel. Deze verzekering voorziet onder andere in een aantal ´eerste hulpdiensten´ bij cyberincidenten, die de impact van een incident helpen beperken. Helaas blijkt niet alle vervolgschade te kunnen worden afgedekt, dus het nemen van preventieve maatregelen blijft noodzakelijk.

Strengere privacy-wetgeving met hogere boetes

In mei 2018 treedt nieuwe Europese wetgeving omtrent cyberrisico's in werking. De EU privacy verordening stelt strengere eisen aan informatiebeveiliging en dataprivacy. Er volgen hoge boetes voor bedrijven die hun gegevensbescherming niet voor elkaar hebben. Met deze nieuwe wetgeving worden bedrijven verantwoordelijk voor de bescherming van de privacygevoelige data van medewerkers, klanten en consumenten. Vanaf 25 mei 2018 moet elk bedrijf kunnen laten zien aantoonbaar in control te zijn. Om op tijd te kunnen voldoen aan de nieuwe eisen, moeten bedrijven op technisch en organisatorisch vlak extra inspanningen leveren.

Rijnbach Textvisual
Connect to inspire

T: 0623877200 | Sterkerstraat 31 | 7481 JV Haaksbergen|
E: info@rijnbachtextvisual.nl | I: www.rijnbachtextvisual.nl