Cyberveiligheid in de Transport & Logistiek

De keten is zo sterk als de zwakste schakel

Of ze nu spullen inkopen, leveren of produceren: vrijwel alle bedrijfstakken in Nederland maken gebruik van transport. Vaak zijn hele ketens afhankelijk van onderlinge levering of bezorging, ondersteund vanuit digitale transport- en warehousemanagementsystemen. Er ligt dus veel druk op de sector Transport & Logistiek, waarbij 'tijd' de achilleshiel lijkt. Als één schakel niet verder kan, liggen vaak ook de volgende stil. In dat geval is losgeld betalen bij gijzelsoftware verleidelijk voor vervoerders. En dat weten cybercriminelen maar al te goed.

Recente cyberaanvallen in de sector

- In 2024 zijn Schneider Logistics en AB Texel aangevallen door de hackersgroep Cactus. De groep gebruikte daarvoor ransomware – software die data buitmaakt en vasthoudt tot het slachtoffer losgeld betaalt. Na de aanval is een 'hersteloperatie' in gang gezet, aldus een woordvoerder van AB Texel. Ook zijn de politie en Autoriteit Persoonsgegevens op de hoogte gesteld.
- Het Amerikaanse bedrijf Expeditors is in 2023 geraakt door een ransomware-aanval. Het bedrijf heeft z'n logistieke activiteiten wereldwijd stilgelegd en alle besturings- en boekhoudsystemen uitgeschakeld, om zo hun gegevens en infrastructuur te beschermen.
- De websites van de havens van Rotterdam en Delfzijl (Eemshaven) zijn in juni 2023 enkele uren uit de lucht geweest door een DDoS-aanval, uitgevoerd door pro-Russische hacktivisten. De hackers hebben geen schade aangericht: ze zijn niet tot de systemen doorgedrongen, hebben niets gestolen of vergrendeld en eisten dus ook geen losgeld.
- In 2023 werd Royal Dirkzwager – sinds 1872 verantwoordelijk voor de registratie van alle in- en uitgaande zeeschepen in de Rotterdamse haven – slachtoffer van Play-ransomware. Naast diefstal van (scans van) identiteitsbewijzen, paspoorten, contractgegevens en bedrijfsinformatie, werd de maritiem dienstverlener in het zenuwcentrum getroffen: namelijk in het systeem dat klanten realtime informeert over de aankomst van schepen en de ROAM-service om scheepsverkeer te monitoren. Zes dagen later draaide alles weer, maar het opruimwerk duurde veel langer – ondanks onderhandelingen met de criminelen.

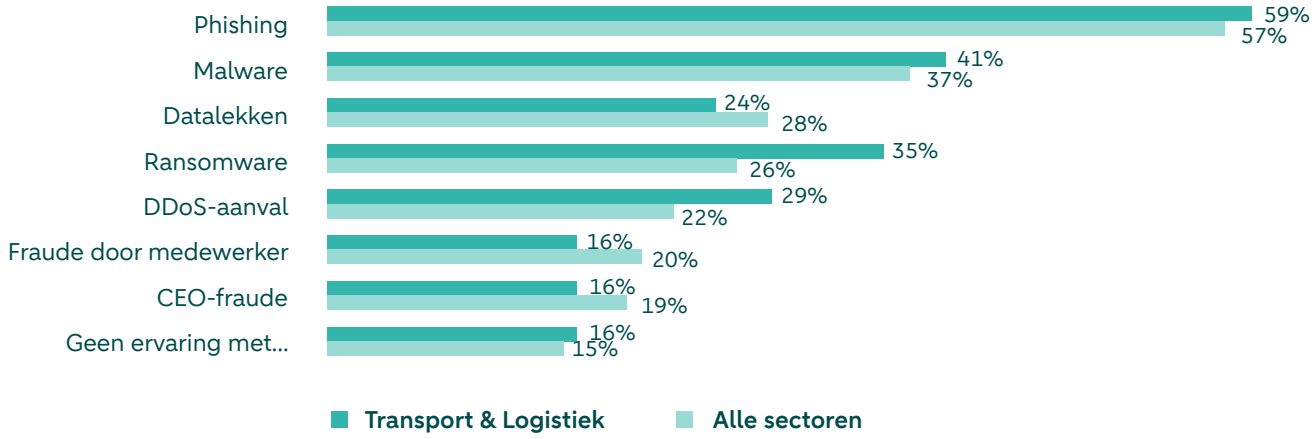
Cyberveiligheid in de sector

Uit recent onderzoek van ABN AMRO onder transport-ondernemers blijkt dat 80% cybercriminaliteit als risico voor de organisatie ziet. Bedrijven maken zich vooral zorgen over phishing e-mails, ransomeware en DDoS-aanvallen. De belangrijkste maatregelen die worden genomen zijn preventief en gericht op zowel technologische (71%) als menselijke (63%) kwetsbaarheden. Uit hetzelfde onderzoek blijkt dat bedrijven steeds meer investeren in de beveiliging van hun digitale omgeving. Van alle deelnemers geeft 67% aan in 2023 – vanwege de toenemende dreiging – meer geld aan cyberbeveiliging te hebben uitgegeven dan in 2022. In 2024 verwacht 45% meer te investeren in cyberbeveiliging dan vorig jaar; de helft van de deelnemers denkt hetzelfde uit te geven als in 2023.

ABN·AMRO

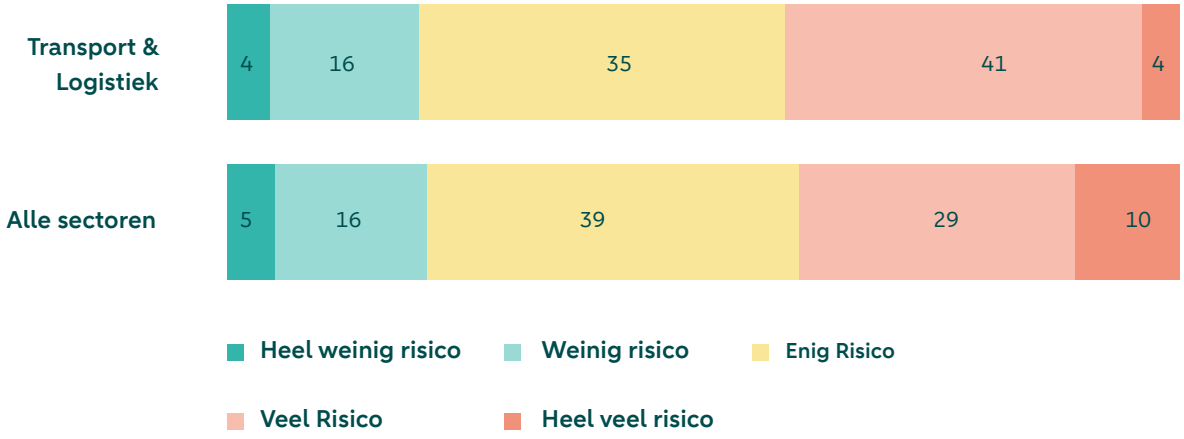
Cyberdreiging voor de Transport & Logistiek: bovengemiddeld, met accent op ransomware en DDoS

*Met welke van de volgende vormen van cybercriminaliteit heeft u binnen uw organisatie weleens te maken gehad?**



Sector heeft voorzichtig-realistisch zelfbeeld over cyberrisico's: 'iets hoger dan gemiddeld'

*In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie?**



* Bron: enquête van ABN AMRO en MWM2 onder 895 Nederlandse organisaties, maart 2024

NIS2: nieuwe Europese wetgeving moet cyberweerbaarheid verbeteren

Om de cyberveiligheid in Europa te verbeteren, gaat in oktober 2024 een nieuwe wet in: NIS2, de opvolger van de Network and Information Security Directive (NIS). Organisaties die belangrijk of essentieel zijn voor de maatschappij, moeten zich aan deze richtlijn houden om de impact van cyberaanvallen en -verstoringen te beperken.

Het is de bedoeling dat Europese lidstaten de richtlijn naar landelijke wetgeving vertalen, maar Nederland loopt hierbij vertraging op. Toch is het verstandig om uw organisatie al op de invoering voor te bereiden. Omdat de wet er hoe dan ook komt, maar ook omdat klanten of leveranciers in andere Europese landen de richtlijn wél vanaf oktober 2024 volgen.

De Europese Unie beschouwt de infrastructuur rondom transport als essentieel. Dat geldt vooral voor vracht die over zee of via de lucht wordt vervoerd – wegvervoerders horen in verreweg de meeste gevallen niet tot 'essentiële' bedrijven uit de NIS2. Hoe dit precies gedefinieerd wordt, is nog niet duidelijk. Wel is duidelijk dat een aantal weg-vervoerders, actief in specifieke segmenten, onder NIS2 gaat vallen – denk aan het transport van olie, post- en koeriersdiensten, afvalstoffenbeheer, en de distributie van levensmiddelen en chemicaliën.

Benieuwd of uw organisatie onder de NIS2-richtlijn valt?
Lees ons rapport: **Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker,**
of vul de **Zelfevaluatie NIS2** van het Nationaal Cyber Security Centrum in.

Verhoog de cyberveiligheid van uw organisatie

Steeds meer organisaties worden slachtoffer van cybercriminaliteit – criminelen hebben maar een kleine ingang nodig. Mogelijk loopt u nu al risico. Daarom is het belangrijk om passende maatregelen op het gebied van cyberveiligheid te nemen. Om u en uw mensen daarbij te helpen, zetten we verschillende oplossingen en downloads op een rij.

Cyberveiliger in drie stappen

1 **Maak een risico-analyse**
Breng de 'kroonjuwelen' van uw organisatie in kaart. Welke zaken zijn cruciaal voor uw bedrijf of dienstverlening? Denk aan klantgegevens, productiemethoden of intellectueel eigendom. Identificeer vervolgens welke dreigingen deze kroonjuwelen in gevaar kunnen brengen: bijvoorbeeld kwetsbaarheid in software of een medewerker die op een malafide link klikt. Nu kunt u de risico's analyseren. Wat is het gevolg van deze risico's, hoe waarschijnlijk zijn ze en wat doet u al om ze te beperken?

2 **Neem adequate maatregelen**
Uw risico-analyse bepaalt welke maatregelen de juiste zijn. De basismaatregelen van het Nationaal Cyber Security Centrum en de basisprincipes van het Digital Trust Center vormen in ieder geval een goed startpunt. Daarnaast kunt u:
- veilig gedrag van uw medewerkers stimuleren;
- bepalen en vastleggen wie de eigenaar van bepaalde gegevens is;
- risico's met uw partners en leveranciers bespreken.

Een cybersecurity-specialist kan u helpen om de juiste maatregelen te nemen.

3 **Stel een Cyber Response Plan op**
Ten slotte is het essentieel om procedures te ontwikkelen waarmee u cyberincidenten detecteert en afhandelt. Deze legt u vast in een Cyber Response Plan.

Whitepaper over Employee Awareness (Download onze whitepaper)
Cybercriminelen komen vaak via medewerkers uw digitale systemen binnen. Houd uw medewerkers scherp en maak ze bewust van de risico's van cybercrime. U leest er alles over in ons whitepaper.

Checklist: Third-Party Risk Management (Bekijk de checklist)
Als u met partners en leveranciers samenwerkt, kunnen er veiligheidsrisico's optreden. Met Third-Party Risk Management brengt u deze in kaart.
- Identificeer mogelijke cyberrisico's
- Deel de checklist met uw klanten en leveranciers voor meer veiligheid

Cyber Response Plan (Maak uw Cyber Response Plan)
Een Cyber Response Plan helpt u om cybercrime-incidenten op te sporen, af te handelen en eventuele schade te herstellen.
- Stel uw eigen Cyber Response Plan op
- Bereid uw bedrijf en medewerkers voor op een cyberaanval

Cyberveiligheidsrapport (Lees het complete rapport)
Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval. Lees alle feiten en ontwikkelingen in het jaarlijkse rapport 'Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker'.

NIS2-praktijkgids (Check onze NIS2-praktijkgids)
Elke sector kent verschillende cyberrisico's. In de industriële sector is vaak de productie het doelwit van cybercriminelen, terwijl ze in de gezondheidszorg uit zijn op patiëntgegevens. Benieuwd naar de risico's en dreigingen in uw sector?

Zo helpt ABN AMRO

Cyber Veilig & Zeker van MMOX
Voor een midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid.
- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen

Bekijk Cyber Veilig & Zeker

Cyberverzekering
Voor zakelijke klanten die zich willen indekken tegen cyberschade.
- Bescherming via onze cyberverzekering
- Uitgebreide dekking
- 24/7 hulp van onze specialisten

Ontdek onze cyberverzekering

Vrijblijvend cybergesprek
Voor ondernemers die willen weten hoe ze ervoor staan op het gebied van cyberveiligheid.
- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

Plan vrijblijvend een gesprek in

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze nieuwsbrief