TVM onderzoek
Cybersecurity

Steeds meer transport-bedrijven versterken hun digitale veiligheid

Cyberaanvallen in de top drie grootste bedreigingen voor transportbedrijven

Cyberaanvallen behoren tot de top drie grootste bedreigingen voor transportbedrijven. Dit blijkt uit een onderzoek dat onderzoeksbureau Markteffect in opdracht van TVM heeft gedaan. Toch blijkt dat veel ondernemingen hun digitale risico's onderschatten.

Driekwart van de ondernemers (74%) ziet cybercriminaliteit als een reële dreiging, maar minder dan de helft zegt goed voorbereid te zijn op een mogelijke aanval. De sector erkent het risico en steeds meer bedrijven zetten stappen richting digitale weerbaarheid. Tegelijkertijd is er nog ruimte voor groei op het gebied van voorbereiding.

Cyberdreigingen zijn complex en veel bedrijven missen de kennis of capaciteit om zich goed te wapenen. Toch kunt u als ondernemer zélf al veel doen om risico's te verkleinen.

Meer weten over het cyberonderzoek?

Het begint met inzicht en bewustwording

74% van de transport-ondernemers ziet cybercriminaliteit als een reële dreiging

27% toch heeft slechts 27% cybersecurity opgenomen in het calamiteitenplan

48% en 48% voelt zich voorbereid op een aanval

Het bewustzijn is er. En dat is de eerste stap naar verbetering. De volgende stap? Samen werken aan een plan, concrete maatregelen nemen en cyberweer-baarheid structureel onderdeel maken van uw bedrijfsvoering.

Cybersecurity in de transportsector: wat kunt u zelf doen?

1. Maak cybersecurity bespreekbaar

   Medewerkers voelen zich niet voldoende voorbereid, maar geven wel aan dat er al cybermaatregelen genomen worden. Toch maakt een ruime meerderheid zich zorgen over de cybersecurity van de organisatie. Maak cyber-security bespreekbaar, geef trainingen en werk met duidelijke protocollen voor verdachte situaties.

2. Breng uw digitale risico's in kaart

   Weet u waar uw kwetsbaarheden zitten? Denk aan oude software, zwakke wachtwoorden of onvoldoende back-ups. Maak hiervan een inventarisatie en bespreek dit met uw IT-adviseur.

3. Maak cybersecurity onderdeel van uw calamiteitenplan

   Wat doet u als uw scherm op zwart gaat? Weten uw medewerkers wat de eerste stappen zijn? Bij slechts 27% van de bedrijven is cyber meegenomen in het bestaande noodplan. Dat kan beter.

4. Werk samen met een betrouwbare ICT-partner

   Niet elk transportbedrijf heeft een eigen IT-afdeling. Maar u kunt wél een externe specialist inschakelen die uw sector begrijpt en met u meedenkt over maat-regelen, updates en snelle herstelmogelijkheden.

5. Neem de NIS2-richtlijnen serieus

   Vanaf 2025 gelden strengere eisen voor digitale weer-baarheid in Europa. Ook kleinere bedrijven kunnen hiermee te maken krijgen. Toch kent 35% van de onder-nemers de richtlijnen niet. Informeer u tijdig en bekijk welke maatregelen u alvast kunt treffen.

Lees meer tips in de cyberchecklist

"Hackers worden steeds slimmer"

"Een aantal jaren geleden kon je bijvoorbeeld door de hoeveelheid taalfouten in de mail direct zien dat het een hack was. Tegenwoordig ziet het er steeds echter uit. Ook door de komst van AI waardoor het ook al mogelijk is om stemmen te klonen. Je zult alert moeten blijven."

Klanten vertellen over hun ervaringen met cyber

“We waren alles kwijt”

“Als je het zelf hebt meegemaakt, weet je pas hoe erg het is. We waren alles kwijt, echt alles. We konden nergens meer bij, chauffeurs wisten niet welke lading ze nodig hadden, waar de lading stond of waar het heen moest, we hadden geen klantgegevens meer en de hele financiële administratie was weg.”

Lees meer klantervaringen met cyberveiligheid

Cybercriminaliteit is een belangrijk onderwerp in de transportsector

63% ziet cybercrime als 1 van de 3 grootste bedreigingen in de transportsector

82% denkt dat de risico’s even groot of groter zijn in de transportsector ten opzichte van andere sectoren

31% heeft te maken gehad met cybercriminaliteit

Heeft uw organisatie weleens te maken gehad met cybercriminaliteit?

“Je kunt de impact van een cyberaanval verkleinen”

“De bewustwording wordt wel groter nu het bijna dagelijks in het nieuws is. Je kunt je niet voor 100% beschermen, maar wel de impact verkleinen áls er iets gebeurt.”

Cyberexperts vertellen over cyberveiligheid

Wat doet u als uw scherm op zwart gaat?

Veelgehoorde antwoorden

“Alle stekkers eruit trekken in het hele kantoor en uit onze server”

“Contact opnemen met de ict-afdeling en hen vragen hoe verder en vervolgens het MT inlichten dat er een probleem is!”

“Mijn IT-man bellen”

“Gillen”

“Geen idee. In ieder geval de grootste opdracht-gevers bellen dat we een probleem hebben.”

“Stekker uit computer trekken en direct iedereen informeren om hetzelfde te doen. Externe partner bellen om te zorgen dat die de rest regelt qua beveiliging.”

“Geen idee”

“Politie bellen”

“Alle medewerkers hebben een taak als beveiliger van systemen en gegevens”

“Je kunt een voertuig uitrusten met allerlei rijhulpsystemen, maar het blijft de chauffeur die bepaalt hoe hij ermee omgaat. En zo is het ook bij cybersecurity. Alle medewerkers van het bedrijf hebben eigenlijk een belangrijke taak als beveiliger van de systemen en gegevens waar ze mee werken.”

Lees het verhaal van Johan Hemmen, manager Preventie en risicobeheer TVM

Steeds meer bedrijven zetten stappen richting NIS2

De nieuwe Europese NIS2-richtlijnen moeten bedrijven beter beschermen tegen cyberdreigingen. 35% van de ondervraagden kent deze richtlijnen nog niet. Van de groep die de NIS2-richtlijnen wel kent, heeft maar liefst 70% al actie ondernomen om eraan te voldoen.

Heeft u nog geen kennisgemaakt met NIS2? Dan is dit hét moment om u te verdiepen in wat deze richtlijnen voor uw onderneming betekenen. De richtlijn biedt een waardevol kader voor verdere professionalisering. Door nu stappen te zetten, voorkomt u verrassingen en vergroot u de weerbaarheid van uw bedrijf tegen cyberdreigingen. Begin klein en breng samen met uw ICT-partner in kaart waar u nu staat. Daarna kunt u de vervolgstappen bepalen.

Lees meer over NIS2 en wat dit voor u betekent

Zijn er binnen uw bedrijf al stappen gezet om te voldoen aan de NIS2-richtlijnen?

Hulp nodig? Bespreek de maatregelen met uw IT-afdeling, of laat u adviseren door cybersecurity experts.
Bel TVM preventie en risicobeheer op (0528) 29 29 30 bij vragen, of mail ons via preventie@tvm.nl.
We denken mee en brengen u graag in contact met specialisten.

TVM verzekeringen | Van Limburg Stirumstraat 250 | Postbus 130 | 7900 AC HOOGEVEEN
+31 (0)528 29 29 99 info@tvm.nl www.tvm.nl