



Cybersecurity checklist voor de transportsector

Bescherm uw systemen, voertuigen en gegevens

Digitale systemen maken transport sneller en efficiënter, maar ook kwetsbaarder. Hackers vinden steeds nieuwe manieren om gegevens te stelen of systemen en voertuigen te gijzelen voor losgeld. Die cyberaanvallen zijn niet alleen een zorg voor grote transportbedrijven. Met de Europese NIS2-richtlijn, die nieuwe eisen stelt aan digitale veiligheid, gaan grote opdrachtgevers ook strengere eisen stellen aan toeleveranciers en ondervoerders. Dus ook als uw transportbedrijf niet direct onder de wet valt, u krijgt er wel mee te maken. Gebruik deze checklist om belangrijke cyberrisico's te herkennen en maatregelen te nemen. Het Nationaal Cyber Security Centrum (NCSC) helpt u daarmee op weg.

Ransomware legt alles stil

Hackers blokkeren uw systemen en eisen losgeld. Planningen lopen vast, vracht komt niet aan en het kan dagen duren tot alles weer draait. U loopt omzet mis, reputatieschade ligt op de loer en herstelkosten kunnen flink oplopen.

Dit kunt u doen

- ✓ Maak elke dag data back-ups en test ze regelmatig
- ✓ Houd de software up-to-date, vooral beveiligingsupdates
- ✓ Gebruik betrouwbare antivirussoftware

Leveranciers als zwakke schakel

Hackers komen via uw leveranciers in uw digitale netwerk. Bijvoorbeeld via besmette bestanden of software die gekoppeld is aan uw planningstool. Zulke aanvallen zijn lastig te ontdekken en kunnen logistieke processen lang verstoren.

Dit kunt u doen

- ✓ Controleer de digitale beveiliging van uw leveranciers
- ✓ Beperk toegang van leveranciers tot uw systemen
- ✓ Leg beveiligingsafspraken vast in contracten

Phishing misleidt uw medewerkers

Cybercriminelen sturen overtuigende nepmails om inloggegevens of toegang tot systemen te krijgen. Een bericht over pakketverzending kan zomaar toegang geven tot uw interne systemen. U loopt het risico op datalekken, financiële fraude of zelfs complete bedrijfsonderbreking of stilstand.

Dit kunt u doen

- ✓ Train uw medewerkers in het herkennen van phishing
- ✓ Zet multifactor-authenticatie (MFA) in voor beveiligde toegang tot systemen
- ✓ Gebruik spamfilters en anti-phishing software

Hackers misbruiken slimme apparaten in voertuigen

Apparaten zoals GPS-trackers, scanners of sensoren kunnen worden gehackt. Voertuigen en lading verdwijnen van de radar, planningen worden verstoord en er kunnen zelfs gevaarlijke situaties op de weg ontstaan.

Dit kunt u doen

- ✓ Gebruik sterke wachtwoorden
- ✓ Deel uw netwerk op in kleinere delen zodat een indringer niet overal bij kan
- ✓ Monitor verdachte activiteit en beperk externe toegang

Meer cybersecurity gevaren en tips

■ Malware legt uw transportmanagementsysteem plat

Gebruik gespecialiseerde detectie- en preventiesoftware (EDR-oplossingen), voer penetratietesten uit en segmenteer uw netwerk.

■ Cloudgegevens zonder beveiliging zijn kwetsbaar

Gebruik MFA toegang tot systemen, versleutel data en monitor activiteiten.

■ Klantgegevens kunnen op straat komen te liggen

Gebruik Data Loss Prevention (DLP)-oplossingen, beperk toegang en voer audits uit.

Digitale veiligheid op orde: check deze 10 maatregelen

De Europese NIS2-richtlijn wordt in Nederland ingevoerd met de Cyberbeveiligingswet. Maar wacht niet tot het moet, begin nu. Of u nu een groot of kleiner transportbedrijf runt: bescherm uw systemen, gegevens en voertuigen. Het Nationaal Cyber Security Centrum (NCSC) heeft 10 praktische maatregelen die u vandaag al kunt nemen. Dan bent u ook alvast goed voorbereid op wat de wet straks van u vraagt.

Bekijk de checklist op ncsc.nl



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.

