ABN·AMRO

Cybersecurity voor logistiek dienstverleners

Zo beschermt u de digitale continuïteit van uw bedrijf

AON
Empower Results®

TLN

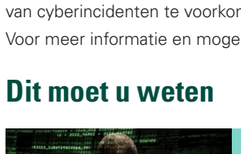
Management Summary

Deze publicatie is bedoeld om logistiek dienstverleners te informeren over de impact van nieuwe digitale dreigingen voor de continuïteit. ABN AMRO, TLN en Aon Risk Solutions vertellen u wat u moet weten en wat u moet doen om bedrijfsschade als gevolg van cyberincidenten te voorkomen en beperken. Hieronder vindt u een samenvatting van onze belangrijkste inzichten en aanbevelingen. Voor meer informatie en mogelijkheden om uw digitale veiligheid te versterken verwijzen wij u naar de afzonderlijke hoofdstukken.

Dit moet u weten

Midden in de digitale transformatie: cybersecurity vergt aandacht

- In de sector Transport & Logistiek is informatie dé route naar hogere efficiency, lagere kosten en minder verspilling in de keten.
- De waarde van uw bedrijf wordt niet langer alleen bepaald door fysieke productiemiddelen als uw vloot, warehouses en menselijk kapitaal. Digitale productiemiddelen zoals data, applicaties en ICT-hardware zijn steeds bepalender voor de waarde van uw onderneming.
- Logistiek dienstverleners zijn nog niet altijd voldoende bewust van de risico's die samenhangen met toenemende afhankelijkheid van data, applicaties en ICT-hardware. Risico's als cybercriminaliteit, maar ook technisch falen en menselijke fouten vormen een steeds grotere bedreiging voor de continuïteit van logistieke bedrijven.
- Er is een duidelijke samenhang van cyberrisico's met andere risico's zoals reputatierisico of het stilvallen van de supply chain.
- Door de ketenpositie die u als logistiek dienstverlener inneemt, brengt cybersecurity specifieke verantwoordelijkheden én aansprakelijkheden met zich mee. Adequate beheersing van IT-, informatie- en privacyrisico's wordt dan ook steeds belangrijker
- Het kennen van uw belangrijkste digitale risico's stelt u in staat de continuïteit van uw bedrijf te versterken



Resultaten van de quickscan uitgevoerd door TLN

De belangrijkste conclusies zijn:

1. Informatiebeveiliging is beperkt.
2. Bewustzijn informatiebeveiliging bij directie en medewerkers is te beperkt.
3. Screening van het personeel is geen standaard procedure.
4. Intern beheer van IT-systemen vraagt om zorgplicht.
5. Beleid omtrent gebruik privé apparaten ontbreekt.
6. Gebruik van Windows XP risicovol.

Uw verantwoordelijkheid: cybersecurity wet- en regelgeving

- Zorg dat u op tijd begint met de implementatie van de Algemene Verordening Gegevensbescherming 2016/679 (AVG).
- Wees voorbereid op een datalek en implementeer procedures.

Cyberincidenten welke bedrijfsschade kunt u verwachten

- Digitale risico's zijn geen toekomstmuziek. Collega-bedrijven hebben hier mee te maken en u zeer waarschijnlijk eveneens (ook wanneer u denkt dat niet het geval is).
- Risico's als ransomware, digitale ladingdiefstal, digitale fraude, netwerkonderbreking en datalekken komen ook in de logistiek steeds vaker voor. Ogenschijnlijk onschuldige risico's kunnen grote impact op uw bedrijf hebben, vanwege de grote en groeiende afhankelijkheid van data en IT.
- De impact van deze digitale incidenten is groot. De dienstverlening aan en het vertrouwen van uw klanten komt onder druk. De financiële gevolgen zijn potentieel fors en lopen in de tienduizenden Euro's. Ook bestaat door de steeds stringentere regelgeving de plicht om privacygevoelige informatie over medewerkers en klanten te beschermen. Wetsovertreding ligt op de loer.
- De totale bedrijfsschade door digitale incidenten voor uw continuïteit kan niet worden onderschat. Dat geldt zowel voor uw korte termijn continuïteit, uw continuïteit op de langere termijn als voor uw financiële continuïteit. Er zijn voorbeelden van netwerkonderbreking als gevolg waarvan de betreffende bedrijven in grote financiële problemen zijn geraakt met in enkele gevallen faillissement tot gevolg. Wees ook voorbereid op de financiële schade door digitale fraude.

Dit moet u doen

Verantwoordelijkheid nemen

Accepteer uw verantwoordelijkheid voor het beperken van bedrijfsschade als gevolg van digitalisering.

- **Het waarborgen van uw (digitale) continuïteit vergt specifieke aandacht én investering in uw IT en de gegevensbescherming door uw organisatie; doe dit niet alleen voor uw eigen bedrijfscontinuïteit, maar ook die van uw klanten en uw (toekomstige) inkomsten.**
- **Voldoe aan (nieuwe) wet- en regelgeving op het gebied van privacybeperkingen.**
- **Ken de beleidsregels 'Meldplicht Datalekken': check of u alles heeft begrepen en geregeld.**
- **Controleer de afspraken met uw bewerkers (ICT-service providers) en pas deze zo nodig aan.**
- **Leg deze afspraken vast in een bewerkersovereenkomst; niet alleen belangrijk, maar ook verplicht.**

Voorkomen

Beperk uw digitale bedrijfsrisico's door:

- uw belangrijkste IT-, informatie- en privacyrisico's te kennen én de meest bedreigende risico's actief te beheersen;
- cybersecurity en informatiebeveiliging te beschouwen als noodzakelijk onderdeel van uw bedrijfsvoering;
- relevante privacywetgeving te kennen en te voldoen aan de huidige en toekomstige eisen (van kracht per medio 2018);
- uw medewerkers bewust te maken van de risico's wanneer er niet zorgvuldig wordt omgesprongen met ICT en data;
- met uw IT-dienstverleners te spreken over hoe zij uw risico's zullen beperken en leg dit formeel vast;
- doe een Privacy Impact Assessment (PA) om privacyrisico's inzichtelijk te maken;
- laat audits en/of pentests uitvoeren om uw beveiliging te meten.

Voorbereiden

Accepteer dat u nooit in staat zal zijn om digitale incidenten uit te sluiten. Wees dan ook voorbereid op incidenten, zodat u de schade voor uw bedrijf kunt beperken door de volgende acties:

- zorg ervoor dat u investeert in mogelijkheden om cybercriminaliteit tijdig te ontdekken;
- organiseer uw digitale bedrijfshulpverlening ('BHV'): weet hoe u moet handelen bij ICT incidenten en de impact kunt beperken;
- heb een procedure voor datalekken;
- voorzie in een pasklaar plan om uw bedrijfscontinuïteit en dat van uw klanten bij incidenten te kunnen realiseren;
- investeer in een cyberverzekering om financiële schade door cyberincidenten te beperken;
- maak een communicatieplan voor verdere informatie over het datalek, binnen en buiten uw onderneming;
- sta stil bij uw risico's op het gebied van bedrijfs- en imagoschade, en hoe u deze gaat beheersen;
- beperk de gevolgen van een datalek door privacygevoelige informatie te versleutelen.

Verminderen

U kunt incidenten nooit voorkomen, maar door adequaat te reageren kunt u de schade aanzienlijk verminderen:

- neem signalen en meldingen altijd serieus; escaleer liever te snel naar de bedrijfsleiding dan te laat;
- ben in staat om ook buiten kantooruren en tijdens vakanties snel de noodzakelijke collega's bij elkaar te krijgen;
- zorg ervoor dat noodzakelijke expertisepartners snel ter plaatse kunnen zijn om te ondersteunen (IT-specialisten, juristen, communicatiespecialisten, verzekeringsadviseurs);
- tref direct continuïteitsmaatregelen: stel uw onderneming en uw klanten in staat om de gewenste continuïteit te kunnen waarborgen;
- doe in het geval van cybercriminaliteit altijd aangifte.

Call to action

Net als andere sectoren neemt digitalisering ook binnen de logistieke sector met grote snelheid toe. Het bewustzijn van de mogelijke digitale risico's die hier een gevolg van kunnen zijn verdient meer aandacht van zowel management als ook de medewerkers van logistiek dienstverleners in de sector Transport en Logistiek. Door de ketenpositie die uw bedrijf inneemt, brengt cyberveiligheid en continuïteit specifieke verantwoordelijkheden én aansprakelijkheden met zich mee. Op diverse thema's zoals 'screening van personeel' en 'de aandacht voor interne digitale informatiebeveiliging' moeten concrete stappen worden gezet.

1. **Cybercrime vormt (ook) een actuele dreiging voor logistiek dienstverleners. Wees bewust van de mogelijke risico's en bedrijfsschade die door deze nieuwe dreigingen kan ontstaan;**
2. **Investeer in adequate IT- en informatiebeveiliging / gegevensbescherming, zodat uw digitale productiemiddelen goed beschermd zijn en u de risico's van cybercriminaliteit beperkt;**
3. **Bereid de organisatie voor op het goed reageren en afhandelen van incidenten. Dat stelt uw bedrijf in staat om schade als gevolg van cybercriminaliteit te beperken en uw continuïteit te waarborgen.**

Digitale veiligheid (Cybersecurity) is een belangrijk onderwerp dat hoger op ieders agenda moet staan; niet morgen, maar vandaag.