ABN·AMRO

Cybersecurity voor logistiek dienstverleners

Zo beschermt u de digitale continuïteit van uw bedrijf

AON
Empower Results®

TLN

>>

Inhoudsopgave

Management Summary

Deze publicatie is bedoeld om logistiek dienstverleners te informeren over de impact van nieuwe digitale dreigingen voor de continuïteit van uw bedrijf. 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

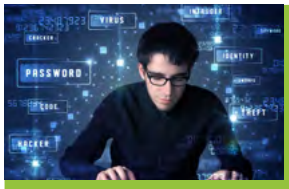
Midden in de digitale transformatie: cybersecurity vergt aandacht

- 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 TLN Quick Scan

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 standaardprocedure.
4. Intern beheer van IT-systemen vraagt om zorgplicht.
5. Beleid omtrent gebruik privéapparaten ontbreekt.
6. Gebruik van Windows XP risicovol.



Wet- en regelgeving cybersecurity: uw verantwoordelijkheid

- 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 science fiction. Collega-bedrijven hebben hiermee te maken en u zeer waarschijnlijk eveneens (ook wanneer u denkt dat dit 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 te staan. 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. Dit geldt voor uw continuïteit op zowel korte als langere termijn, ook financieel. Er zijn voorbeelden van netwerkonderbrekingen die bedrijven in grote financiële problemen hebben gebracht. In enkele gevallen zelfs met faillissement tot gevolg. Wees ook voorbereid op de financiële schade door digitale fraude.

Dit moet u doen

Uw 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 van 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 zult 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 hiervan kunt beperken;
- zorg voor een procedure voor stel een procedure op voor maak 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;
- wees in staat om 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.

Kom in actie

Net als in 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 u bewust van de mogelijke risico's en bedrijfsschade die door deze nieuwe dreigingen kunnen 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 uw organisatie voor op het goed reageren op 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.

1. Midden in de digitale transformatie

Als ondernemer in de sector Transport en Logistiek wordt u steeds afhankelijker van digitale informatie. Veel activiteiten binnen uw bedrijf hangen direct samen met de tijdige beschikbaarheid van juiste informatie. Digitalisering kan veel voordelen bieden, juist in de logistieke keten. Dat geldt zeker in een tijd waarin alle betrokken ketenpartijen én maatschappij vragen om nieuwe, duurzame logistieke oplossingen.

Informatie-uitwisseling zal bestaande processen verder stroomlijnen, met een betere inzet van capaciteit tot gevolg. Ook de administratie verloopt digitaal. Neem de elektronische vrachtbrief als concreet voorbeeld.

Toch heeft digitalisering ook een keerzijde. In feite maakt technologie ons kwetsbaarder dan ooit. Bedrijfscontinuïteit staat of valt met de beschikbaarheid van data en IT. Technische en organisatorische fouten kunnen grote gevolgen hebben. Daarnaast zien we digitale vormen van criminaliteit. Afpersing is van alle tijden, maar verschuift steeds meer naar online. Voor veel ondernemers is cybercrime ongrijpbaar, en daardoor extra bedreigend. Oppassen dus, zou je denken. Maar uit onderzoek blijkt dat cybercrimepreventie op managementniveau niet de aandacht krijgt die het verdient. 'Dat overkomt ons toch niet', hoor je vaak. Helaas, niets is minder waar. De zorgvuldigheid waarmee u en uw medewerkers met informatie omgaan, zegt veel over de digitale veiligheid van uw bedrijfsprocessen. En daarmee over de continuïteit van uw organisatie.

In deze publicatie staat uw digitale continuïteit centraal. We geven u als logistiek dienstverlener hiervoor waardevolle suggesties, ook op het gebied van digitaal risicobeheer.

1.1 Het informatietijdperk is nog maar net gestart

Alles lijkt inmiddels om informatie te draaien. Smartphones en tablets zijn niet langer alleen privé, maar ook zakelijk onmisbare apparaten. Connectiviteit neemt met grote snelheid toe. Dit blijkt ook uit de meest recente TLN Automatiseringsenquête (2015). Het zakelijk gebruik van smartphones en tablets steeg in 2015 ten opzichte van 2014 van 52 naar 70 procent. Bovendien komen er steeds meer nieuwe informatiebronnen bij, zoals sensortechnologie en publieke data. Informatie en applicaties lijken definitief het 'nieuwe goud' te zijn geworden.

In eerste instantie waren het met name ziekenhuizen en banken die aandacht hadden voor informatiebeveiliging. Gezien de gevoelige informatie die er circuleert, geldt voor de zorg- en bankensector specifieke regelgeving. Inmiddels zijn informatiestromen voor alle bedrijven van cruciaal belang in de race naar vernieuwing.

In het bijzonder binnen Transport & Logistiek is informatie dé route naar hogere efficiency, lagere kosten en minder verspilling in de keten. U verwerft nog steeds inkomsten via fysieke goederenstromen, maar de achterliggende processen zijn in toenemende mate technologisch gedreven. De snel oprukkende digitale transformatie geldt overigens voor alle bedrijven binnen deze sector, van klein tot groot. Het belang dat u er als ondernemer aan toekent, neemt toe. Van de groep 'grote bedrijven' beschouwt 96 procent ICT als 'zeer belangrijk'. De resterende 4 procent vindt het 'belangrijk'. In de categorie 'kleine bedrijven' zijn deze percentages 12 procent (zeer belangrijk) en 45 procent (belangrijk). Logische verschillen, want kleine bedrijven zijn minder afhankelijk van geavanceerde ICT-systemen.

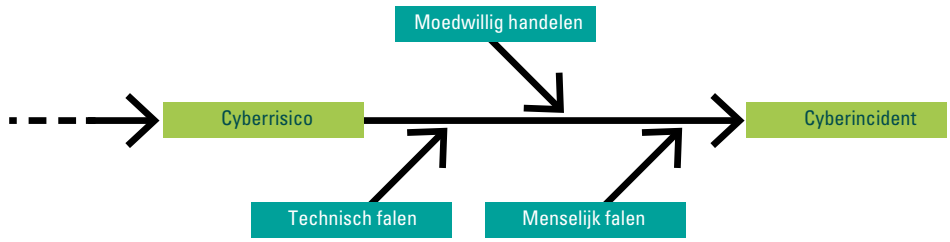
Van bricks naar bytes

Voorheen bepaalden vooral fysieke productiemiddelen de waarde van logistieke bedrijven. Denk aan gebouwen, vloot en menselijk kapitaal. Tegenwoordig zijn digitale middelen steeds belangrijker in dit proces en genereren ze waarde voor uw bedrijf. Een logische bijkomstigheid van digitalisering, maar daarom niet minder interessant. Kortom: we gaan van *bricks* naar *bytes*.

Onder digitale middelen verstaan we alle hardware, applicaties en data die cruciaal zijn voor uw onderneming om te functioneren. Denk aan de ICT-kerninfrastructuur waar zowel uw bedrijf als uw klanten van afhankelijk zijn. Het belang (en gebruik) van digitale middelen neemt in alle sectoren toe; dit geldt dus ook voor logistiek dienstverleners. Voorbeelden hiervan zijn plannings- en logistieke systemen, maar ook ICT-leveranciers. Daarnaast zijn management- en klantdata productiefactoren geworden. Deze zijn inmiddels voor elk bedrijf in de Transport & Logistiek essentieel

1.2 Digitale veiligheid en continuïteit: van criminaliteit tot alledaagse fouten

Cybercriminaliteit wordt vaak omschreven als *'het door derden onrechtmatig verkrijgen van bedrijfsgevoelige gegevens. Vaak om deze informatie in te zetten voor een onrechtmatig doel.'* Het lijkt dus vooral een bedreiging van buitenaf te zijn, maar staart u zich hier niet blind op. De risico's die met digitalisering samenhangen, gaan verder dan cybercriminaliteit. De grootste bedreigingen voor uw bedrijfscontinuïteit kunnen uiteraard een crimineel karakter hebben, maar veel vaker is de oorzaak meer alledaags. In de praktijk blijkt 25 procent van de cyberincidenten te ontstaan door factoren die niets met criminaliteit te maken hebben. Bijvoorbeeld doordat de techniek faalt, met systeemuitval als mogelijk gevolg. Ook de menselijke factor speelt vaak een rol, zoals bij programmeerfouten of dataverlies. In een ander kwart van de gevallen begint het probleem bij leveranciers.



Figuur 1.1 bron: Cyber Risk Practice, Aon Global Risk Consulting

Figuur 1.1 maakt duidelijk dat de oorzaken voor digitale incidenten breder zijn dan moedwillig handelen (criminaliteit). Technisch en menselijk falen blijven belangrijke oorzaken van cyberincidenten.

Het gevaar groeit voor de Transport en Logistiek

Naast ondernemingen in andere sectoren, zijn ook logistiek dienstverleners een interessant doelwit geworden voor internetcriminelen. Cybercriminaliteit heeft een vlucht genomen in onze sector, waardoor er de laatste jaren meer aandacht voor is. Hierdoor werd duidelijk dat ook transportcriminelen een digitaliseringsslag hebben gemaakt. Voorbeelden genoeg. Denk maar aan de manipulatie van systemen met vrachtinformatie, datagijzeling (ransomware) of de diefstal van gegevens. De belangrijkste wake-upcall voor de logistiek was misschien wel in 2013: de georganiseerde digitale ladingdiefstal via de systemen van de Antwerpse haven. Ook privacybescherming is een issue. Ieder bedrijf met een personeels- en/of klantenbestand is kwetsbaar voor datadiefstal. Zeker nadat de privacywetgeving op 1 januari 2016 is verzwaard, onder andere door de Meldplicht Datalekken[1].

Twee kanten van de Nederlandse medaille

Bijna een derde van het MKB is de afgelopen 2 jaar de dupe geworden van online criminaliteit. Volgens de de rapportage uit 2016 van de nationale autoriteit NCSC is cyber een beroepscriminaliteit geworden. Ransomware heeft een grote vlucht genomen. Nederland is top in Logistiek. Echter, deze positie betekent dat wij ook kwetsbaar zijn voor dit soort nieuwe risico's .

In de sector Transport & Logistiek wisselen ketenpartners (opdrachtgevers en vervoerders) iedere seconde een enorme hoeveelheid data uit, al dan niet via de cloud. Tracking & Tracing-systemen zijn volledig ingeburgerd en een uitkomst voor verladers, logistiek dienstverleners én consumenten. We willen namelijk precies weten wanneer onze goederen zich waar bevinden. Maar tegelijkertijd vergroot dit de kans op cyberincidenten.

Ook andere innovaties dwingen tot een nieuwe visie op risico. Denk aan de mogelijkheid dat trucks in *platoons* zullen gaan rijden. Een bijzondere ontwikkeling, met voordelen als kostenbesparing en

CO_2-reductie voor verladers en logistiek dienstverleners. Ook hier zijn informatie-stromen leidend, en dus liggen cyberkapers[2] op de loer om de beschikking te krijgen over uw goederen.

1.3 Soorten digitale risico's

Er zijn grofweg twee typen digitale risico's die de continuïteit van uw bedrijf kunnen bedreigen:

1. Directe risico's
Deze hebben rechtstreeks impact op uw inkomstenstroom en financiële positie. Daarom bepalen ze uiteindelijk uw digitale risicoprofiel.

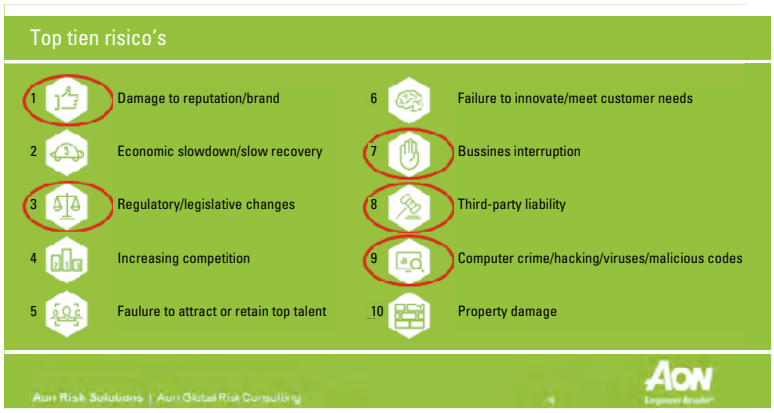
2. Indirecte risico's
Deze liggen in eerste instantie bij uw partners in de digitale supply chain, zoals (ICT-)leveranciers, klanten en andere ketenpartijen. De kwaliteit van hun risicobeheersing bepaalt mede of u dezelfde risico's loopt, en in welke mate.

Uw informatie is geld waard, en dus kwetsbaar

Bedreigingen die met digitalisering samenhangen, worden doorgaans niet doorzien. Laat staan dat ze snel worden geadresseerd. Dit komt onder andere doordat digitale risico's in hoge mate virtueel zijn, en dus onzichtbaar. Bovendien blijkt het voor niet-IT'ers vaak lastig om digitale risico's in te schatten. Dit is niet anders in de sector Transport & Logistiek, waar het logistieke proces van fysieke goederen (waarde) wordt aangestuurd op basis van informatie (bijvoorbeeld planningsystemen). Deze combinatie maakt uw sector bij uitstek gevoelig voor cyberrisico's. Bedrijven die met dataopslag en het delen van data werken, zijn het ideale en vaak makkelijke slachtoffer voor hackers. Kortom: hoog tijd om uw risicobeheer aan te passen aan de digitale transformatie van uw bedrijf.

Ken (en neem) uw verantwoordelijkheid

Door de ketenpositie die uw bedrijf inneemt, brengt cyberveiligheid en continuïteit specifieke verantwoordelijkheden én aansprakelijkheden met zich mee. Als logistiek dienstverlener staat u immers garant voor kwaliteit. Bovendien vormen digitale risico's een grote continuïteitsbedreiging voor uw organisatie. Vergeet daarbij niet de samenhang van cyberrisico's met andere risico's (zie figuur 1.2). Reputatieschade bijvoorbeeld, of een gebeurtenis waardoor de supply chain mogelijk stilvalt. Op dit punt moet er dus een tandje bij. En dat kan, want er zijn steeds meer beveiligingsmaatregelen en verzekeringen beschikbaar die bedrijven moeten beschermen tegen digitale incidenten.



Figuur 1.2 Bron: Aon Global Risk Management Survey

Staat digitale continuïteit hoog op uw agenda?
Bewustwording van digitale risico's en van de impact die deze kunnen hebben op uw bedrijfscontinuïteit en -veiligheid is een eerste stap richting de oplossing. Ons advies: blijf vooral informatie toepassen op basis van nieuwe technologie. Dat is de toekomst. Het digitale tijdperk is pas net begonnen, en nu al bepalend voor uw dagelijkse operatie. Uw mensen moeten optimaal gebruik kunnen maken van informatiesystemen, maar dan wel in een veilige digitale omgeving. Dit geldt ook voor de bedrijven waarmee u dagelijks direct in verbinding staat. U kunt er niet omheen: de digitale transformatie vereist een aanpassing van uw risico management agenda. Hoe hoog staat digitale continuïteit op de uwe?

[1] Zie hoofdstuk 2
[2] Cyberkaping: het overnemen van een vliegtuigaansturing of beïnvloeden van een routeplanning

2. Onderzoeksresultaten TLN Cybersecurity Quick Scan

Informatiebeveiliging noodzakelijk

Binnen de logistieke keten is het uitwisselen van informatie van cruciaal belang. Denk aan informatie die nodig is binnen de operatie: van WMS/TMS/ vrachtbrieven CMR en klantgegevens tot financiële gegevens en voertuig-posities. Dankzij internet is papier bijna verleden tijd: informatie-uitwisseling gebeurt steeds vaker digitaal. Makkelijker en sneller, vanzelfsprekend. Maar zolang informatie onbeveiligd blijft, kunnen derden er relatief eenvoudig bij.

2.1 Incidenten cybercriminaliteit

Cybercrime gaat over alle criminaliteit op het internet, met ICT als middel én doelwit. De beoogde buit is informatie die niet toegankelijk zou moeten zijn voor derden.

Er zijn veel soorten cybercrime-incidenten, maar de meest voorkomende hebben betrekking op:

- onderling delen van persoonlijke inloggegevens tussen medewerkers;
- malware;
- phishing;
- hacking;
- ransomware.

Quick scan TLN	
Soort cyberincident	**percentage ondervraagden dat hiermee te maken heeft gehad**
malware	**63,0%**
phising	**61,6%**
hacking	**6,8%**
ransomware	**>10%**

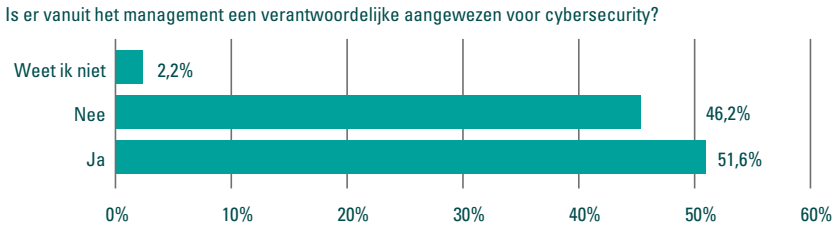
2.2 Resultaten Cybersecurity Quick Scan

In mei 2016 heeft Transport en Logistiek Nederland (TLN) een onderzoek laten uitvoeren om te achterhalen in welke mate TLN-leden bezig zijn met cybersecurity. Welke risico's lopen ze? En zijn de financiële informatiestromen wel echt de kroonjuwelen? Om hier meer inzicht in te krijgen, heeft TLN de Cybersecurity Quick Scan ontwikkeld.

Belangrijkste conclusies

1. Bewustzijn informatiebeveiliging bij directie en medewerkers is te beperkt

Bij de helft van de bedrijven is er een verantwoordelijke aangewezen voor cybersecurity. Dit betekent dus dat er in de helft van de gevallen nog géén verantwoordelijke is! Voor een branche die met zo veel vertrouwelijke gegevens werkt, is dat zorgwekkend.



Belangrijke vraag: is dit bewust of onbewust? In de Quick Scan antwoordt 51,6 procent bevestigend dat cybercrime een belangrijk aandachtspunt is van het management. Het staat daarmee volgens ons nog onvoldoende op de agenda van de directie.

Zolang beveiliging niet prominent op de agenda staat van de directie, zal het bewustzijn van cybercrime bij medewerkers ook minimaal zijn. De meest voorkomende gevallen van onveilige situaties:

- medewerkers die onderling en met derden persoonlijke inloggegevens delen;
- medewerkers die op het werk onveilige e-mailbijlagen openen;
- medewerkers die privé-e-mail via webbrowsers openen.

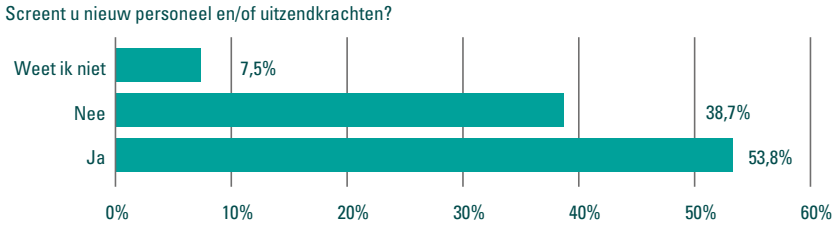
2. Informatiebeveiliging is beperkt

Uit de Quick Scan komt naar voren dat de respondenten informatiebeveiliging niet zien als onderdeel van de gehele goederentransportketen. Terwijl volgens hen de meest kwetsbare digitale informatie hier wel een cruciaal onderdeel van is. 54 procent geeft aan dat hun bedrijf voldoende beveiligd is tegen cyberrisico's. Dit is een subjectieve inschatting; om beveiligingsniveaus objectief vast te stellen, zijn er vervolgtrajecten nodig. Een substantieel aantal van de ondervraagden geeft ook aan dat ze niet goed weten of hun digitale informatie goed beveiligd is. Wij vermoeden dat veel bedrijven onvoldoende beschermd zijn tegen cyberaanvallen. Er is tenslotte niemand die over de kwaliteit van de cyberbeveiliging waakt.

Verder bleek dat 63 procent van de respondenten weleens een malware-infectie geeft opgelopen binnen hun IT-omgeving. Daarnaast is meer dan 10 procent ooit het slachtoffer geweest van ransomware.

3. Screening personeel is geen standaard procedure

In veel gevallen blijkt dat de criminele daad vanuit de interne organisatie wordt gepleegd, of dat er sprake is van hulp van binnenuit. De logistieke sector blijkt extra kwetsbaar door opslag en transport van vaak aantrekkelijke goederen. Er is een hoge mate van interne betrokkenheid bij criminaliteit. Dit betekent dat er meer aandacht moet komen voor personeelsscreening bij indiensttreding. Slechts 53,8 procent van de ondervraagde ondernemers screent het personeel.



Zorgvuldige werving en selectie van personeel is noodzakelijk. Het is belangrijk dat u hier op structurele wijze tijd aan besteedt: screening moet een standaard onderdeel zijn van werving en selectie. Daarnaast is het belangrijk om te bepalen welke informatie met derden wordt uitgewisseld en welke niet.

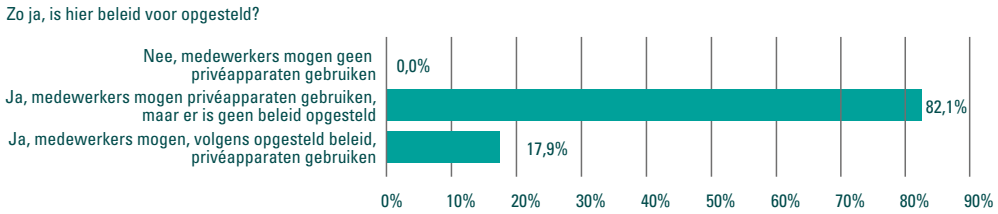
De logistieke sector beschikt over een registratiesysteem: het Waarschuwingsregister Logistieke Sector (WLS). Doel hiervan is een integere bedrijfstak met minder criminaliteit. Het WLS is bedoeld als instrument voor werving en selectie. De check via het WLS is gericht op alle werknemers in de logistieke sector. Meer informatie over het WLS vindt u online.

4. Intern beheer van IT-systemen vraagt om zorgplicht

50,5 procent van de respondenten geeft aan dat hun bedrijf de IT-systemen intern beheert. Redenen die ze noemen: zelf beheren is veiliger, goedkoper, en zorgt voor een betere beschikbaarheid. Veel 'voordelen' dus, maar intern beheer vereist wel een degelijke zorgplicht. Bij deze bedrijven is het van belang dat een medewerker verantwoordelijk wordt gesteld voor zowel functionerende als up-to-date IT-security.

5. Beleid over gebruik privéapparaten ontbreekt

30 procent van alle respondenten mag privéapparaten voor werkzaamheden gebruiken. Dit vormt niet direct een probleem. Wel blijkt dat meer dan 80 procent van de bedrijven die dit toestaan, geen beleid hierover voert. Het ontbreken van dergelijk beleid kan al gauw tot incidenten leiden, doordat privéapparaten vaak niet goed beveiligd zijn.



6. Ondernemen zonder cyberverzekering

Uit de Quick Scan blijkt dat bijna 80 procent weleens te maken heeft gehad met cybercrime. Toch heeft 83,9 procent geen cyberverzekering, bedoeld om schade als gevolg van een cyberincident te dekken. Bijvoorbeeld omzetverlies door een cyberaanval, waarbij een website of webshop offline wordt gehaald. Van de respondenten geeft 35% aan niet te weten of een cyberverzekering noodzakelijk is voor hun bedrijf.

Een cyberverzekering dekt ook de schade van ransomware, zelfs wanneer u besluit om de digitale gijzeling af te kopen. Vaak vergoedt de verzekeraar ook de bijkomende kosten van onderzoek en systeemherstel na een cyberaanval. Cyberverzekeringen hebben verschillende polisvoorwaarden. Het is daarom van belang dat u op de hoogte bent van de mogelijkheden. Zo kunt u bepalen of een cyberverzekering geschikt is voor uw specifieke bedrijfssituatie. En zo ja, welke.

7. Gebruik van Windows XP risicovol

Van alle respondenten gaf 18 procent aan Windows XP als besturingssysteem te gebruiken. Doordat Windows sinds april 2014 (!) voor XP geen beveiligingsupdates meer uitbrengt, groeit voor gebruikers hiervan het risico op cyberaanvallen met de dag.

3. Wet- en regelgeving rond cybersecurity: úw verantwoordelijkheid

Een centraal juridisch kader voor het begrip cybersecurity ontbreekt tot dusver. Dit betekent dat de reguliere wet- en regelgeving op het gebied van ‘informatiebeveiliging’ en ‘datalekken’ erop van toepassing is. U dient zich als ondernemer ervan te vergewissen of u hieraan voldoet.

3.1 Centraal juridisch kader ontbreekt

Er is discussie over de vraag hoe informatiebeveiliging zich verhoudt tot cybersecurity. Informatiebeveiliging gaat over de maatregelen en procedures om de beschikbaarheid, exclusiviteit en integriteit van informatievoorziening te garanderen. En in het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen, en de gevolgen van incidenten tot een acceptabel niveau te beperken. Cybersecurity wordt vaak zo omschreven:

'Vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT, of door misbruik van ICT. Bijvoorbeeld door beperking van de beschik- en betrouwbaarheid van ICT'.
(Cybersecurity Beeld Nederland 2016)

Toch wordt de term cybersecurity ook vaak gebruikt om *'de beveiliging van cyberspace'* aan te duiden. Maar een centraal juridisch kader voor het begrip cybersecurity ontbreekt tot dusver. Dit betekent dat de reguliere wet- en regelgeving op het gebied van 'informatiebeveiliging' en 'datalekken' erop van toepassing is.

3.2 Informatiebeveiliging

In de Wet bescherming persoonsgegevens (Wbp) richt artikel 13 zich op beveiligingsmaatregelen op het gebied van informatiebeveiliging. Dit artikel houdt in dat de verantwoordelijke 'technisch en organisatorisch passende maatregelen neemt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking'.

Ieder land hanteert nu nog zijn eigen privacywetgeving, met alle onderlinge verschillen van dien. In Nederland is de Autoriteit Persoonsgegevens (AP) toezichthouder, in het kader van de Wbp. In Europees verband is de Algemene Verordening Gegevensbescherming 2016/679 (AVG) de opvolger van de Europese richtlijn uit 1995. Op 25 mei 2016 is de AVG in werking getreden en gelden in alle lidstaten van de EU/EER dezelfde privacyregels. Uiterlijk 25 mei 2018 moeten ondernemers deze nieuwe regels hebben geïmplementeerd. Tot die datum geldt in Nederland de Wbp en is er dus min of meer sprake van een overgangssituatie. Als ondernemer doet u er verstandig aan nu al met de transitie naar de AVG te beginnen. De ervaring heeft geleerd dat die termijn absoluut nodig is.

3.3 Enkele praktische voorbeelden van de AVG-wetgeving

Als ondernemer moet u rekening houden met de privacygevoeligheid en -risico's van en voor personen in of via uw informatiesystemen, zoals Tracking & Tracing of videocamera's. Op basis van een risicoanalyse dient u passende beveiligingsmaatregelen te nemen, zodat u kunt aantonen dat de verwerking van persoonsgegevens via die systemen in overeenstemming is met de AVG. Deze maatregelen moet u bovendien evalueren en zo nodig actualiseren.[3] Dit kan onder meer met behulp van:

- vulnerability scans: kwestbaarheidsanalyse;
- pen-testen: testen van bestaande beveiligingsmaatregelen;
- netwerksecurity scans: werken de bestaande beveiligingsmaatregelen?;
- intrusion detection: testen van bestaande monitoringssoftware.

Wanneer u voor de verwerking van persoonsgegevens of het beheer van informatiesystemen gebruikmaakt van ICT-service providers (zogenaamde 'bewerkers') – en welke ondernemer doet dat niet – dan mag u uitsluitend werken met service providers (cloud computing) die afdoende beveiligingsgaranties bieden. U zult zich ervan moeten overtuigen dat dit het geval is.

Dit kan eigenhandig, door zelf inspecties of audits bij de service provider uit te voeren. Maar voor de meeste logistiek dienstverleners zal het erop neerkomen dat zij de service provider vragen om aan te tonen dat hij *cyber secure* en *privacy compliant* is. Bijvoorbeeld door middel van een certificering op basis van de in paragraaf 2.6 genoemde standaarden voor informatiebeveiliging, en met een aanvullende privacycertificering. De Autoriteit Persoonsgegevens (AP) zal ook toezicht uitoefenen op de naleving van de AVG.

3.4 Meldplicht Datalekken

Daarnaast moet u als ondernemer voldoen aan de Meldplicht Datalekken. Er is sprake van een datalek als er zich daadwerkelijk een beveiligingsincident heeft voorgedaan waarbij mogelijk persoonsgegevens verloren zijn gegaan. Of waarbij onrechtmatige verwerking van persoonsgegevens niet uit valt te sluiten.

U doet alleen aangifte bij de AP wanneer een datalek:

- *leidt* tot een aanzienlijke kans op ernstig nadelige gevolgen voor de bescherming van persoonsgegevens;
- ernstig nadelige gevolgen *heeft* voor de bescherming van persoonsgegevens.

Enkele voorbeelden van datalekken

Een onversleutelde usb-stick, laptop of telefoon die kwijtraakt of wordt gestolen, een hacker die inbreekt in uw informatiesysteem? Schoolvoorbeelden van datalekken. Maar er is ook sprake van een datalek wanneer ransomware uw bestanden met persoonsgegevens versleutelt. Immers, iemand moet toegang tot die bestanden hebben gehad om ze te kunnen versleutelen.

Datalekken kunnen een onderneming en haar personeel ernstig bedreigen, ook binnen de Transport & Logistiek. Zo proberen criminelen toegang te krijgen tot Tracking & Tracing- en videocamerasystemen, om vervolgens data over goederenstromen te manipuleren. Door bijvoorbeeld losadressen te veranderen, worden de goederen niet op het juiste adres afgeleverd. Ze kunnen zelfs de boordcomputers van transportmiddelen overnemen of buiten werking stellen, uiteraard met rampzalige gevolgen.

Juridische basis en consequenties

Als het om gevoelige persoonsgegevens gaat, bent u in het algemeen verplicht het datalek te melden. In elk geval bij de AP, en eventueel ook aan de personen op wie de gegevens betrekking hebben. Het gaat dan om gegevens uit onder meer incidentenregisters, waarschuwings-, toegangs-, Tracking & Tracing- en controlesystemen. Maar ook om (gekopieerde) gegevens die voor identiteitsfraude kunnen worden gebruikt, zoals identiteitsbewijzen, Burgerservicenummers en inloggegevens van systemen met dit soort gevoelige data. Meldt u een datalek, dan kan dit voor de AP aanleiding zijn te onderzoeken welke beveiligingsmaatregelen u heeft getroffen. De AP heeft een boetebevoegdheid van maximaal € 820.000,- of zelfs 10 procent van uw jaaromzet.

De juridische grondslag van de meldplicht is artikel 34a, lid 1 van de Wbp. Doordat dit specifieke artikel in de huidige Wbp is opgenomen, geldt deze meldplicht al sinds 1 januari 2016. Met andere woorden: de wetgever heeft niet gewacht op definitieve implementatie van de AVG. Dit betekent vanzelfsprekend dat u ervoor moet zorgen dat persoonsgegevens goed zijn beveiligd. U kunt hierop worden aangesproken.

3.5 Wat doet u bij een (vermoedelijk) datalek?

U moet een datalek 'onverwijld' melden aan de AP. Dat wil in dit geval zeggen: zonder onnodige vertraging en (zo mogelijk) niet later dan 72 uur na de ontdekking ervan. Dit houdt in dat u – nadat u een mogelijk datalek heeft ontdekt – enige tijd mag nemen voor nader onderzoek om een onnodige melding te voorkomen. Blijkt ondertussen uit uw onderzoek dat het incident niet onder de Meldplicht Datalekken valt, dan vervalt de meldplicht. Wat u in een concreet geval onder 'onverwijld' moet verstaan, hangt af van het geval en de omstandigheden. De termijn waarbinnen u een datalek moet melden, start zodra u op de hoogte raakt van een incident dat mogelijk onder de Meldplicht Datalekken valt. Doordat u dit zelf heeft ontdekt, of via een bewerker[4] die u heeft ingeschakeld.

U leest meer over de meldplicht in het document 'Beleidsregel Meldplicht Datalekken' van de AP. Hierin krijgt u door middel van stroomschema's snel inzicht in de vraag of een incident wel of niet onder de meldplicht valt. We adviseren u daarnaast om met de bewerker afspraken vast te leggen in de bewerkersovereenkomst over hoe om te gaan met datalekken. Sinds de meldplicht in werking is getreden, heeft de AP circa 4.000 meldingen ontvangen.

Wees voorbereid op datalekken: implementeer procedures

De impact van een datalek wordt over de volle breedte van het bedrijfsleven vaak onvoldoende onderkend. Dit geldt trouwens voor alle privacy-gerelateerde vraagstukken met mogelijk ernstige consequenties. U moet zelf kunnen aantonen dat uw organisatie voldoende 'in control' is als het gaat om alle privacy- en beveiligingsregels. U wordt geacht een privacy- en beveiligingsbeleid te hebben dat is vertaald in concrete maatregelen en procedures.

En u moet – *last but not least* – aan kunnen tonen dat informatiebeveiliging en privacybescherming een vanzelfsprekende plaats hebben binnen uw management control-cyclus.

Samengevat: het is essentieel dat u de persoonsgegevens die u verwerkt goed beveiligt. Hieronder leest u een aantal aanbevelingen, onderverdeeld in drie categorieën:

1. Neem Verantwoordelijkheid

- Ken de beleidsregels 'Meldplicht Datalekken' van de AP: check of u alles goed heeft begrepen en geregeld.
- Volg – indien nodig – een praktijktraining 'Privacy, security en datalekken melden'.
- Controleer de afspraken met uw bewerkers (ICT-service providers) en pas deze zo nodig aan.
- Leg deze afspraken vast in een bewerkersovereenkomst. Dit is niet alleen belangrijk, maar ook verplicht.
- Informeer uw medewerkers over de risico's van een datalek en de impact die dit kan hebben op uw bedrijf.

2. Voorkom cyberincidenten

- Werk met toegangsbeveiliging: zorg dat alleen bevoegden bij de data kunnen.
- Richt een incidenten- en calamiteitenbeheer in, inclusief een specifieke procedure voor datalekken.
- Doe een Privacy Impact Assessment (PIA) om privacyrisico's inzichtelijk te maken.
- Laat audits en/of pentest uitvoeren om uw beveiliging te meten.
- Denk na over een juiste informatiescheiding, houd gevoelige informatie apart van minder kwetsbare data.

3. Wees Voorbereid op cyberincidenten

- Beslis wie (welk team) in de organisatie datalekken beoordeelt en meldt bij de AP.
- Denk na over hoe u betrokkenen informeert bij een datalek.
- Bereid u voor op een mogelijke follow-up van de AP.
- 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.
- Denk na over hoe u om wilt gaan met signalen uit de buitenwereld over mogelijke datalekken.
- Mitigeer de impact van een datalek door middel van encryptie/hashing.

3.6 Algemeen aanvaarde standaarden voor informatiebeveiliging

De naleving van onderstaande standaarden kan door onafhankelijke partijen worden geaudit:

- ISO 27001/27002; een internationale norm voor informatiebeveiliging, gepubliceerd door de International Organization for Standardization (ISO).
- NIST SP 800-53; de standaard voor de beveiliging van cloud computing van het Amerikaanse National Institute of Standards and Technology (NIST SP 800-53).
- ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cybersecurity Centrum (NCSC) van het Ministerie van Veiligheid en Justitie.

3.7 Wetboek van Strafrecht en Wetboek van Strafvordering

De huidige editie van het Wetboek van Strafrecht bevat een aantal artikelen over strafbare handelingen die met computers of via computernetwerken worden verricht. De huidige grondslag om gegevens te vorderen door politie en justitie ligt in het Wetboek van Strafvordering. Het wetsvoorstel bestrijding cybercrime (computercriminaliteit III) ligt op dit moment bij de Tweede Kamer. Doel van het wetsvoorstel is zorgen voor meer mogelijkheden en nieuwe bevoegdheden in het kader van opsporing en vervolging.

[3] Zie voor de volledige tekst art. 24.1 AVG: Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

[4] Als eerder gezegd: bewerkers zijn service providers. De bewerker is juridisch gesproken (ingevolge artikel 1, onder e, Wbp) degene die namens de verantwoordelijke persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag te zijn onderworpen. De bewerker verwerkt derhalve gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid.

4. Cyberincidenten: welke bedrijfsschade kunt u verwachten?

In dit hoofdstuk beschrijven we de impact van vijf realistische risico's, gebaseerd op waargebeurde digitale incidenten bij logistiek dienstverleners. Hiermee laten we zien welke bedrijfsschade u kunt verwachten als gevolg van een cyberincident. Ieder actueel risico voor de logistiek hebben we voorzien van een verhaallijn. Daarin leest u met welke risico's u mogelijk wordt geconfronteerd en welke gevolgen deze hebben voor uw bedrijf en klanten. Afsluitend geven wij u aan de hand van de 'vier V's' concrete voorbeelden van maatregelen u kunt nemen om:

1. uw Verantwoordelijkheid te nemen;
2. digitale risico's te Voorkomen;
3. uw organisatie Voor te bereiden op digitale risico's;
4. de impact van digitale risico's te Verminderen.

4.1 Ransomware: losgeld voor bedrijfsgegevens

Een logistiek dienstverlener wordt slachtoffer van ransomware. Het gaat om een bedrijf met ongeveer 200 vrachtauto's en 15.000 m^2 magazijn. Aansturing van de administratieve en logistieke processen verloopt vrijwel volledig digitaal.

Via het algemene e-mailadres van de organisatie komt om 10.00 uur een factuur binnen. De receptiemedewerker maakt dit wel vaker mee, dus stuurt ze de factuur door naar de financiële afdeling. Daar opent een financieel medewerker om 11.30 uur de bijlage om de factuur te betalen. Deze blijkt besmet met ransomware, die na opening op de achtergrond wordt gedownload. De medewerker merkt hier vooralsnog niets van. Doordat hij toegang heeft tot alle bedrijfssystemen, is het aantal bestanden dat wordt versleuteld enorm. De ransomware treft onder andere het systeem voor warehouse management.

Om 12.30 uur komt de eerste melding binnen: een van de medewerkers kan niet meer bij de actuele voorraadgegevens. Hij krijgt een melding dat er € 900 moet worden betaald om weer toegang te krijgen. De medewerker licht de ICT-afdeling in, die direct het hele netwerk van de organisatie afsluit om de ransomware te verwijderen. Uit principieel oogpunt besluit de directie geen geld te betalen om de versleutelde bestanden terug te krijgen.

Om 13.30 uur is de ransomware verwijderd en de back-up van het einde van de vorige werkdag teruggeplaatst. Op dat moment beginnen de problemen pas echt: voorraadniveaus blijken niet meer te kloppen, facturen zijn kwijt, net als de laatst binnengekomen bestellingen. Het kost de logistiek dienstverlener ruim een week om alle informatie binnen de ICT-systemen weer kloppend te krijgen. Verschillende klanten klagen over niet nagekomen afspraken. Weken later wordt de financiële afdeling nog steeds gebeld over onbetaalde facturen, maar die staan nergens in het systeem. De vervolgschade voor het bedrijf is omvangrijk en loopt in de tienduizenden euro's.

Risico	**Ransomware**
Beschrijving	Ransomware is een vorm van malware die een computer, of de gegevens die erop staan, versleutelt. Voor een doorgaans klein bedrag bieden de criminelen een key aan, waarmee je de computer of bestanden weer kunt gebruiken. Zonder zo'n sleutel krijg je onmogelijk toegang tot je bestanden.
Kans	Zeer groot. Ransomware is het meest voorkomende risico en elke organisatie is een potentieel doelwit.
Impact klantvertrouwen: financiële positie: bedrijfscontinuïteit: wet- en regelgeving:	 klanten ervaren vertraging of kwaliteitsproblemen; verliezen kunnen oplopen tot € 50.000; reële kans op ontoelaatbaar lange bedrijfsonderbreking; mogelijk sprake van een meldenswaardig datalek en/of overtreding van de privacywetgeving.
Bedrijfsschade	**Groot ******

4.2 Ladingdiefstal 2.0: het nieuwe stelen gebeurt op afstand

Door middel van phishing is een criminele organisatie erin geslaagd een logistiek bedrijf met malware te besmetten. De criminelen hebben zo toegang gekregen tot gegevens van het bedrijf, en vinden binnen mum van tijd een interessante kostbare lading in het systeem. Hiervan wijzigen ze de ontvangstbestemming, waardoor de lading keurig bij de criminelen wordt afgeleverd; niet bij de oorspronkelijke klant. Heel slinks, want de chauffeur heeft niets in de gaten. Na enkele dagen ontvangt het logistieke bedrijf de eerste klachten over goederen die niet zijn geleverd.

Het bedrijf stelt een onderzoek in en al snel is het lek boven water. Derden hebben ongeoorloofd toegang verkregen tot gevoelige gegevens. Het probleem wordt opgelost, maar er zijn meerdere ladingen buitgemaakt, waaronder laptops en smartphones. De directe schade bedraagt enkele tienduizenden euro's. De totale indirecte schade is moeilijk in te schatten, maar in ieder geval moeten alle gegevens worden gecontroleerd. Want het is onduidelijk welke gegevens nog meer zijn gewijzigd.

Risico	**Digitale ladingdiefstal**
Beschrijving	Digitale ladingdiefstal is een oud fenomeen, uitgevoerd met moderne hulpmiddelen. Criminelen gebruiken een cyberaanval om informatie te verzamelen of manipuleren, om zo eenvoudig een lading buit te maken.
Kans	Groot. Het is relatief eenvoudig om toegang te krijgen gevoelige gegevens en deze te bekijken of zelfs te manipuleren. Niet alleen door inbreuk op systemen.
Impact	
klantvertrouwen:	zeer grote impact, leveringen aan individuele klanten vinden niet plaats;
financiële positie:	verlies van materieel en lading (vaak eigendom van de klant);
bedrijfscontinuïteit:	minimaal, digitale ladingdiefstal vindt doorgaans alleen op kleine schaal plaats;
wet- en regelgeving:	minimaal, digitale ladingdiefstal vindt doorgaans alleen op kleine schaal plaats; mogelijk is er sprake van een meldenswaardig datalek en/of overtreding van de privacywetgeving.
Bedrijfsschade	**Aanzienlijk *****

4.3 Directiefraude: directeur of fraudeur?

Een financieel medewerker met de verantwoordelijkheid om betalingen uit te voeren, krijgt een e-mail van de CEO. Het verzoek: voer een vertrouwelijke en urgente betaling uit, in het kader van een overname. De medewerker vertrouwt het niet helemaal, omdat het verzoek afwijkt van de gebruikelijke procedure. In de e-mail staat een telefoonnummer van het over te nemen bedrijf. Wanneer hij hiernaartoe belt, bevestigt de financiële afdeling van het 'bedrijf' dat deze betaling noodzakelijk is voor de transactie. Omdat de betaling vertrouwelijk is, durft de medewerker niet te overleggen met collega's. Hij controleert nogmaals de e-mail, maar die lijkt helemaal te kloppen. Onderaan staat: verzonden vanaf mijn iPhone. Dit klopt: iedereen op de hogere niveau's krijgt een iPhone voor zakelijk gebruik. De schrijfstijl is precies zoals die van de CEO: kort en zakelijk. De medewerker twijfelt niet langer en maakt het betalingsbedrag van € 50.000,- over.

Risico	**CEO-fraude**
Beschrijving	Fraudeurs sturen namens de bedrijfsleiding een e-mail naar een financieel medewerker, met de opdracht een geldbedrag over te maken. De criminelen verzamelen vooraf zo veel mogelijk informatie om een zo realistisch mogelijke e-mail op te stellen.
Kans	Elk bedrijf met een wat grotere afstand tussen medewerkers en directie kan ermee te maken krijgen. Deze vorm van fraude komt overigens steeds vaker voor.
Impact	
klantvertrouwen:	geen impact op de klant;
financiële positie:	in deze casus gaat het in eerste instantie om een bedrag van € 50.000,-;
bedrijfscontinuïteit:	geen stagnatie, wel serieuze impact op de financiële gezondheid van de onderneming;
wet- en regelgeving:	geen sprake van een datalek.
Bedrijfsschade	**Aanzienlijk *****

4.4 Datalek: voor u het weet, bent u in overtreding

Van een medewerker bij personeelszaken wordt een laptop gestolen. Heel vervelend voor haar, maar voor het bedrijf zijn de gevolgen niet te overzien. De laptop is niet beveiligd en bevat de personeelsgegevens van alle 110 medewerkers, waaronder hun bankgegevens, NAW-gegevens en kopieën van ID-kaarten. Daarnaast heeft de laptop toegang tot het volledige bestand van klantgegevens. Het bedrijf is niet voorbereid op dit scenario; niemand weet dus wat er moet gebeuren. Pas na een week wordt de directeur erop geattendeerd dat er sprake is van een datalek en dat een melding bij de Autoriteit Persoonsgegevens verplicht is.

Het onderzoek van de Autoriteit Persoonsgegevens naar maatregelen tegen lekken van persoonsgegevens pakt niet gunstig uit. De gegevens op de laptop waren immers niet versleuteld. Het bedrijf moet zijn medewerkers informeren dat er mogelijk privacygegevens in handen zijn gekomen van derden. Ook klanten moeten op de hoogte worden gesteld.

Risico	**Datalek**
Beschrijving	Bij een datalek komen privacygevoelige op straat te liggen. Door een daadwerkelijke inbreuk op de systemen, of door een menselijke fout. Het lek moet binnen 72 uur worden gemeld bij de Autoriteit Persoonsgegevens. Afhankelijk van de situatie, moeten belanghebbenden (personeel, klanten) worden geïnformeerd.
Kans	Groot. Vaak is er sprake van menselijke fouten.
Impact klantvertrouwen: financiële positie: wet- en regelgeving:	 vertrouwelijke klantgegevens raken openbaar; er moeten maatregelen getroffen worden om het datalek goed af te handelen; er is mogelijk sprake van een meldenswaardig datalek en/of overtreding van de privacywetgeving.
Bedrijfsschade	**Groot ******

4.5 Netwerkonderbreking: overleeft u zonder ICT?

Een logistiek dienstverlener met ruim 150 medewerkers heeft de ICT-voorziening van het bedrijf nog in eigen beheer. Door een onbekende oorzaak valt aan het begin van een werkdag de ICT uit. De ICT-afdeling schat het in als een klein probleem en vermoedt dat het systeem binnen 30 minuten wel weer in de lucht is. Maar na een uur moet de ICT-afdeling toegeven dat het probleem ingewikkelder is dan aanvankelijk gedacht. Na kort overleg met de directeur neemt de afdeling contact op met een extern bureau. Een uur later komen er twee specialisten Een uur later komen er twee specialisten langs. Maar doordat het probleem complex is, kost het ze meer dan vijf uur om de boel weer aan de gang te krijgen.

In totaal is het netwerk van de organisatie ruim acht uur niet beschikbaar. Door de onverwachte uitval zijn er gegevens verloren gegaan; op het eerste gezicht is het niet duidelijk welke. Daarnaast kunnen veel medewerkers hun belangrijkste taken niet uitvoeren. Offline zijn er nog wel een paar klussen, maar de meeste krachten zijn veel minder productief. Enkele klanten van het bedrijf krijgen hun producten te laat en personeel moet na werktijd blijven om de achterstand weg te werken. De totale schade bedraagt ongeveer € 60.000,-. Wanneer de netwerkonderbreking langer had geduurd, waren de gevolgen desastreus geweest. Eén of enkele dagen geen ICT kan tot faillissement leiden.

Risico	**Netwerkonderbreking**
Beschrijving	Netwerkonderbreking is een periode waarbinnen het netwerk van een organisatie niet beschikbaar is.
Kans	Groot. Bij elke organisatie kunnen ICT-voorzieningen uitvallen.
Impact	
klantvertrouwen:	klanten ervaren vertragingen en communicatieproblemen;
financiële positie:	in deze casus bedroeg de totale schade € 60.000,-;
bedrijfscontinuïteit:	zeer grote impact – langdurige uitval van ICT zorgt voor stagnatie van het primaire proces, met hoogoplopende kosten als gevolg;
wet- en regelgeving:	geen overtreding van Wet bescherming persoonsgegevens.
Bedrijfsschade	**Groot ******

4.6 Wat moet u doen?

Hieronder vindt u een aantal maatregelen om de genoemde scenario's te voorkomen. En om u voor te bereiden op een situatie waarin u alsnog slachtoffer wordt van cybercrime. Tot slot leggen we uit hoe u de impact van een incident kunt verminderen. Houd hierbij in uw achterhoofd dat cyberincidenten vandaag of morgen binnen uw bedrijf kunnen plaatsvinden. Ons advies is om nu al na te denken over maatregelen die het risico hierop beperken. Alleen: voorzorgsmaatregelen kunnen het risico weliswaar verminderen, maar nemen het nooit helemaal weg. Er blijft altijd een rest-risico. Dit komt doordat cyberrisico's snel veranderen als gevolg van innovaties, en door de ontwikkeling en toepassing van nieuwe technologieën.

1. Neem uw Verantwoordelijkheid

Het waarborgen van uw (digitale) continuïteit vergt specifieke aandacht én investering in uw IT en de gegevensbescherming door uw organisatie. Niet alleen voor uw eigen bedrijfscontinuïteit, maar ook die van uw klanten en uw (toekomstige) inkomsten. En om te kunnen voldoen aan (nieuwe) wet- en regelgeving op het gebied van privacybeperkingen.

2. Voorkom cyberincidenten

- Zorg dat uw systemen up-to-date en up to standard zijn. Denk aan besturingssystemen, software, firewalls en antivirussoftware.
- Maak uw medewerkers door voorlichting bekend met de verschillende vormen van cybercrime en vertel wat zij kunnen doen om de risico's hierop te beperken.
- Test de alertheid van uw medewerkers, bijvoorbeeld door een eigen phishing-actie te organiseren.
- Monitor uw netwerk om ongeoorloofde activiteiten en malware zo snel mogelijk te detecteren.
- Zorg voor een goede versleuteling van uw bestanden, zeker als ze persoonsgegevens bevatten.
- Zorg dat u de belangrijkste applicaties en de locatie van vertrouwelijke gegevens kent (voer daartoe bijvoorbeeld een (privacy) impact analyse uit). Breng daarnaast in kaart welke risico's een bedreiging vormen voor deze systemen.
- Informeer uw medewerkers over de wettelijke verplichtingen voor adequate gegevensbescherming (persoons- en klantgegevens).
- Zorg ervoor dat u uw IT-dienstverleners deelgenoot maakt van uw risico's, en maak afspraken over hoe zij uw risico's helpen beperken en schade door eventuele incidenten zullen verminderen.

3. Wees Voorbereid op cyberincidenten

- Voorzie in regelmatige back ups op afgescheiden locaties (extern en/of bij leveranciers).
- Test back-ups regelmatig door ze terug te zetten en te controleren op bruikbaarheid.
- Verken of een cyberverzekering geschikt is om de financiële restrisico's en bedrijfsschade door incidenten voldoende af te dekken.
- Stel een duidelijke procedure op voor het geval er een cyberincident plaatsvindt: wie doet wat, wie is er verantwoordelijk, welke externen moeten op afroep beschikbaar zijn, hoe informeert u uw klanten?

- Neem de autorisatie-instellingen van uw netwerk kritisch onder de loep. Door de toegang tot systemen te beperken, voorkomt u fouten en ongewenste toegang.
- Zorg voor duidelijke betalingsrichtlijnen, zonder veel uitzonderingen. Moet er een uitzonderlijke betaling worden uitgevoerd? Laat dan altijd een collega of leidinggevende een extra check doen.
- Overweeg uitbesteding van de primaire IT-processen aan een hosting provider die standaard een hoog security-niveau biedt, incidenten snel opspoort en eventuele schade vlug herstelt.
- Check uw contracten met IT-dienstverleners op hoe zij hun respons op uw incidenten organiseren: hoe is hun beschikbaarheid (ook buiten kantooruren) en is incidentrespons onderdeel van hun dienstverlening.
- Leg een incidenten- of crisisprocedure vast en stel een (IT-)continuïteitsplan op. Zo weet u hoe uw bedrijf dient te handelen bij incidenten om verdere schade te beperken.
- Zorg ervoor dat specifieke expertise snel kan worden gemobiliseerd (juristen, IT-specialisten, communicatie-adviseurs)

4. Verminder de impact van cyberincidenten

- Meld afwijkingen en incidenten zo snel mogelijk en zorg ervoor dat er snel en adequaat kan worden gehandeld.
- Activeer het crisisplan en breng het continuïteitsplan ten uitvoer.
- Zorg dat de oorzaak zo snel mogelijk wordt gevonden en weggenomen, eventueel met behulp van externe expertise.
- Meld de schade bij uw verzekeraar/verzekeringsmakelaar.
- Vind zo snel mogelijk uit welke systemen en data er zijn geraakt en of de integriteit van de data is aangetast.
- Zorg dat uw systemen zo snel mogelijk weer operationeel zijn en maak de gegevens up-to-date.
- Communiceer duidelijk naar uw medewerkers en eventueel betrokken klanten.
- Achterhaal de oorzaak van het incident en voorkom herhaling.
- Doe altijd aangifte als er sprake is van een crimineel incident.

Bijlage

Begrippenlijst

Malware
Malware is software om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.

Phishing
Phishing is een vorm van internetfraude en wordt gebruikt om mensen op te lichten door ze een valse website te laten bezoeken. In de meeste gevallen een namaakversie van een bank- of creditcardwebsite. Een variant van phishing is het zogeheten *spear phishing*, waarbij persoonlijke gegevens van het doelwit worden gebruikt om vertrouwen te scheppen. Denk aan een mailtje dat compleet op u of uw bedrijf is toegespitst. Hierdoor komt het bericht in eerste instantie heel vertrouwelijk over. De 'afzender' verwijst u naar de nepwebsite, met als doel uw computer te infecteren of gegevens te ontfutselen. De meeste vormen van phishing gebeuren via e-mail, maar tegenwoordig ook telefonisch. Wees altijd alert als u wordt benaderd voor uw gegevens. Bij twijfel adviseren we om uw bank te bellen ter verificatie.

Ransomware
Ransomware betekent letterlijk 'gijzelsoftware'. Hiermee blokkeren criminelen uw computer, of de bestanden hierop. De digitale afpersers doen zich voor als bijvoorbeeld de politie, Buma/Stemra, Microsoft of Europol. Ze vertellen u dat u zich schuldig heeft gemaakt aan strafbare feiten en daarom een boete moet betalen. Niets is minder waar: het bericht is afkomstig van criminelen en betalen heeft vaak geen zin. De politie adviseert om u tegen ransomware te wapenen door antivirusprogramma's te gebruiken, updates te installeren en back-ups van uw gegevens te maken.

Op de website van de politie vindt u meer informatie over ransomware, hoe u zich ertegen beschermt en wat u moet doen als u slachtoffer bent.

Colofon

Dit rapport is een uitgave van ABN AMRO, TLN en Aon Risk Solutions.
ABN AMRO, TLN en Aon Risk Solutions werken in dit kader samen om de bedrijfsrisico's voor logistiek dienstverleners te beperken. Deze publicatie is bedoeld om logistiek dienstverleners te informeren over de impact van nieuwe digitale dreigingen voor de continuïteit. Met deze publicatie beogen we de bewustwording van logistiek dienstverleners van digitale risico's – waaronder cybercriminaliteit – te verhogen. Tevens bieden wij logistiek dienstverleners concrete aanbevelingen om het bedrijf te versterken tegen nieuwe digitale bedreigingen.

Auteurs
ABN AMRO
Bart Banning, Sector banker Transport en Logistiek

TLN
Hélène Minderman, Secretaris Beleid en Deelmarkten
TLN
Babiche van de Loo, Secretaris Beleid TLN

Aon Risk Solutions
Dennis de Hoog, Ma MSc, Managing Consultant,
Aon Cyber Risk Practise

Redactie
Tekstwerf

Fotoverantwoording
Shutterstock, I-stock

Distributie
https://insights.abnamro.nl/

Inhoudsopgave >