Cybercriminaliteit binnen de **transport en logistiek**

De grootste risico's en het belang van cyberbescherming

AON
Empower Results®

Het toenemend cybergevaar voor de logistiek:

de grootste risico's en het belang van cyberbescherming

Logistieke bedrijven, spoorwegen, rederijen en havens zijn steeds vaker een doelwit voor cybercrime. Criminelen willen financieel gewin behalen door de diefstal van vertrouwelijke informatie of geld. Organisaties krijgen steeds meer te maken met dit risico vanwege hun afhankelijkheid van informatietechnologie, connectiviteit en de digitale transformatie. Omdat systemen die bijvoorbeeld telefoonverkeer, betalingen, beveiliging en transport regelen volledig geautomatiseerd zijn, onderling verbonden en opereren in een web met allerlei leveranciers en tussenbedrijven is overzicht lastig. Met alle risico's van dien.

Toen de systemen van containerbedrijf Maersk in de Rotterdamse haven plat lagen in juni 2017 kon de veiligheidsregio eerst niks doen omdat ze geen toegang hadden tot de nodige informatie. De NotPetya-aanval waarbij onder andere Maersk en TNT zwaar getroffen zijn, verspreidde zich via een Oekraïens boekhoudprogramma. Over de hele wereld werden computersystemen platgelegd. Deze hack leverde 10 miljard dollar schade op en laat duidelijk zien dat binnen de sector transport en logistiek de financiële en operationele impact enorm kan zijn. Meerdere factoren dragen bij aan het cyberrisicoprofiel van een organisatie, waaronder: bewust en onbewust gedrag door medewerkers, systeem- en programmafouten, beveiligingsmaatregelen, de aard en hoeveelheid van de verzamelde gegevens, het strategisch belang van de informatie en de afhankelijkheid van technologie.


$10
MILJARD
SCHADE DOOR
NOTPETYA-AANVAL

De **kwetsbaarheden** en grootste cyberrisico's voor logistieke bedrijven

Het is een hardnekkig misverstand dat u een gewild doelwit moet zijn om met cybercrime te maken te krijgen. De meeste cyberaanvallen zijn niet gericht op individuele bedrijven, maar worden uitgevoerd op duizenden slachtoffers tegelijkertijd. Cybercriminelen richten zich bijvoorbeeld op bedrijven die gebruikmaken van een specifiek type software, besturingssystem of router. Als een cybercrimineel eenmaal binnen is in uw systeem, kan hij u chanteren met ransomware zodat u geen toegang meer heeft tot uw systemen. Of hij treft interessante informatie aan waarvoor hij achteraf pas een koper zoekt.
U hoeft vooraf niet al interessant te lijken al interessant te lijken voor een hacker om slachtoffer te worden. De impact op uw bedrijf is vrijwel altijd groter dan verwacht.

Wat maakt uw organisatie gevoelig voor cybercrime?

- verzamelen, onderhouden, verspreiden of opslaan van privé-informatie;
- hoge afhankelijkheid van elektronische processen of computernetwerken;
- vertrouwen op kritieke infrastructuur;
- wet- en regelgeving;
- afhankelijkheid van leveranciers en onafhankelijke aannemers;
- netwerkconnectiviteit met andere organisaties;
- kwetsbare beveiliging in apparaten en -producten (bijv. autonome voertuigen, wifi-thermostaten) .
- systeem- en programmafouten;
- beveiligingsmaatregelen;
- de aard van en hoeveelheid data

Welke cyberrisico's spelen er in de sector transport en logistiek?

- hackers gericht op aansturingssoftware;
- bedrijfsonderbreking door een cybergebeurtenis geleden door een cyberincident bij een externe verkoper of leverancier;
- bedrijfsstilstand of gederfde inkomsten door een cyberincident;
- (opzettelijk) handelen van medewerkers;
- ransomware-aanvallen;
- politieke of strategische waarde;
- mogelijk lichamelijk letsel en materiële schade als gevolg van cyberincidenten;
- afhankelijkheid van technologie.

"Veel organisaties pakken het cyberrisico niet aan, omdat zij denken dat de afdeling ICT ervoor zorgt dat hen niets overkomt. ICT zorgt ervoor dat systemen werken en is niet verantwoordelijk voor afspraken met leveranciers en klanten aangaande het verwerken van gegevens. ICT heeft ook geen invloed op hoe medewerkers met gegevens omgaan. Die verantwoordelijkheid ligt uiteindelijk bij de directie."

Maarten de Jonge,
Managing consultant Privacy & Cyber

Maak het cybercriminelen lastiger, voorkom een aanval

Een cyberincident valt weliswaar nooit helemaal te voorkomen. Maar waarom zou u het cybercriminelen makkelijk maken? Zodra u weet via welke deuren een ‘inbreker’ binnen kan komen, heeft u de eerste stap naar een goede beveiliging gezet. De volgende stap is zorgen dat deze deuren zo goed mogelijk gesloten zijn.

Veel organisaties pakken het cyberrisico niet aan, omdat zij veronderstellen dat de afdeling ICT of de (externe) ICT-beheerder hiervoor zorgt. De verantwoordelijkheid voor de uitwisseling en verwerking van gegevens ligt uiteindelijk bij de directie. Het is namelijk essentieel dat iedereen binnen uw hele organisatie bewust is van cyberrisico’s. Mensen blijven de zwakste schakel wanneer het om cyberincidenten gaat. Uit de praktijk blijkt dat onwetende, nalatige of kwaadwillende werknemers bijna driekwart van de cyberaanvallen veroorzaken. Dus zonder bewuste medewerkers geen veilige organisatie.

Voorbereidingen die u direct kunt treffen:

- Zorg voor een actief systeem dat voorziet in herstel
- Gebruik goede antivirussoftware om uw systeem te beschermen
- Open nooit bijlagen in e-mails van iemand die u niet kent
- Zorg dat alle software op de computer up-to-date is
- Door een phishing-campagne meet u hoe bewust uw medewerkers omgaan met externe data
- Controleer welke toegangsrechten medewerkers hebben en of deze actueel gehouden worden.
- Door de rechten van medewerkers te beperken, verkleint u het ‘insider-risico’ en de kans op een cyberincident
- Besteed regelmatig op directieniveau aandacht aan bewustwording binnen de organisatie. De directie moet het belang en de urgentie uitdragen. Het is namelijk niet de vraag óf uw organisatie slachtoffer wordt van een cyberincident, maar wanneer.

Beperk de impact van een cyberincident voor uw organisatie

Een cyberincident kan grote gevolgen hebben. Wat kost een dag stilstand? Naast directe financiële schade voor uw eigen organisatie en mogelijk voor anderen, heeft u ook te maken met reputatieschade. U ligt na een cyberincident direct onder een vergrootglas bij klanten, leveranciers en mogelijk de media.

Zorg dat u goed kunt uitleggen welke maatregelen u al had genomen om gegevens te beveiligen. Kunt u dit niet, dan leidt dit onherroepelijk tot flinke reputatieschade.

Systeemuitval: **wat nu?**

Het uitvallen van uw digitale systeem kan altijd gebeuren, maar wanneer het gebeurt is onzeker. Hoe lang duurt het, wat is de oorzaak en wie kan het oplossen? Systeemuitval kent twee kanten. Een kant betreft de IT, waarbij het van ultiem belang is het systeem zo snel mogelijk weer operationeel te krijgen. In veel gevallen besteden organisaties hier al aandacht aan en is een IT-recovery plan aanwezig. De andere kant betreft de operationele continuïteit van de bedrijfsvoering. Een crisisplan biedt de mogelijkheid om direct gecoördineerd te reageren bij het uitvallen van het systeem. Het biedt duidelijke, concrete handvaten om de bovengenoemde prioriteiten in goede banen te leiden.

Wijs binnen uw organisatie iemand aan die crisismanager is op het moment dat uw organisatie wordt gehackt, zodat u direct tot actie over kunt gaan wanneer er een incident plaatsvindt.

> Wie binnen uw organisatie (h) erkent en bepaalt dat jullie gehackt zijn? En wat is die actie op dat moment? Leg deze beslissingen en de te ondernemen acties vast in een protocol, vergelijkbaar met het protocol dat in werking treedt wanneer er brand uitbreekt in uw organisatie.
>
> Ralf Willems, cyberspecialist

De impact van een cyberaanval op uw logistieke organisatie

Transport

De meeste chauffeurs zijn door middel van IT-systemen/VMS in de cabine van hun vrachtwagen constant verbonden met de planningsafdeling op kantoor. In veel gevallen maakt dit een dynamische ritplanning mogelijk en is de chauffeur in grote mate afhankelijk van deze systemen om zijn werkzaamheden tijdig en accuraat uit te voeren. In toenemende mate worden vrachtbrieven en dergelijke ook door de chauffeur elektronisch bij aflevering aangeboden.

Warehouse

In warehouses wordt in de meeste gevallen gewerkt met een digitaal WMS systeem. Bij een hack zal ook dit systeem niet meer functioneren. Wat zal leiden tot bedrijfsstilstand. Goederen kunnen niet gepickt worden en zullen niet op tijd kunnen worden uitgeleverd. Zeker in het geval van bederfelijke- en just in time goederen (JIT) vormt dit een risico.

Terreinen & vastgoed: toegangscontrole

In toenemende mate wordt toegang tot terreinen en panden elektronisch beheerd met toegangspassen, vinger- en irisscanning of kentekenherkenning. In het geval van systeemuitval is toegang moeilijk of zelfs onmogelijk.

Communicatie

In geval van een systeemstoring zult u dit zowel intern als extern moeten communiceren. Hoe zijn de klantcontactgegevens snel te vinden als de gebruikelijke IT-systemen niet meer functioneren? Welke procedure volgt u bij systeemuitval om binnen de onderneming (crisismaatregelen) te communiceren met de medewerkers?

Ketenimpact

Hoe snel kunnen ketenpartners hun werkzaamheden via andere kanalen inrichten? Elke onderneming is (direct of indirect) onderdeel van een keten van leveranciers en afnemers. In welke mate bent u aansprakelijk voor (financiële) schade die ketenpartners lijden als gevolg van uw systeemuitval? Wordt uw reputatie geschaad? Stappen klanten en partners over naar de concurrent?

Impact op de omgeving

Systeemuitval heeft niet alleen direct invloed op de bedrijfscontinuïteit van het getroffen bedrijf, het kan ook directe impact hebben op de omgeving van de bedrijfslocatie. Bijvoorbeeld wanneer toegang tot terreinen onmogelijk is geworden en filevorming ontstaat. Denk hierbij aan de situatie op de A15 toen de Maersk Europoort terminal gesloten werd als gevolg van een systeemuitval. Eenzelfde situatie kan ontstaan door uitval van het WMS-systeem waardoor goederen op alternatieve locaties gelost/opgeslagen moeten worden. Vaak zijn deze locaties minder geschikt en kan de opslag hiervan leiden tot overlast voor de omgeving.

Administratie

Administratie is vaak het kloppende hart van de onderneming. Facturatie, contractmanagement, treasury functies, cash management, leveren van actuele managementinformatie, allemaal zaken die van groot belang zijn voor de bedrijfscontinuïteit. Wat doet u als er geen toegang meer is tot de systemen?

Wij helpen u graag succesvol te ondernemen

De sector transport en logistiek wordt gekenmerkt door sterke concurrentie en kleine marges. Het financiële plaatje is daarom meestal doorslaggevend bij het nemen van beslissingen. Het is verleidelijk om liever nu op kosten te besparen, dan te investeren in zaken die niet direct geld opleveren. Helaas heeft een cyberincident een grote impact op de dagelijkse gang van zaken binnen uw bedrijf. Wanneer uw werkproces wordt onderbroken kost u dat veel tijd, geld en misschien wel klanten.

Cyberrisicomanagement is meer dan het reduceren van de kans op cyberrisico's door beveiligingsmaatregelen en het verzekeren van risico's om de kosten van een schade te herstellen. Het draait vooral om focus op interne bedrijfsprocessen en afspraken op het gebied van cyberveiligheid. Wij helpen u bij het beheersbaar maken van cyberrisico's en cybercriminaliteit voor uw organisatie. Met de ondersteuning van experts reageert u snel en adequaat op een incident, waardoor u zorgt dat uw bedrijf altijd kan blijven draaien. Goed risicomanagement leidt ertoe dat organisaties de cyberrisico's volledig inzichtelijk en onder controle hebben. Hierdoor leert u hoe u moet moeten handelen als er zich een incident voordoet.

Mocht zicht toch een hack voordoen, dan ondersteunen wij u tijdens het incident. Een goede voorbereiding op een mogelijke cybercrises begint bij bewustwording. Tijdens een cybercrisis komen er in korte tijd veel zaken op u af. Cruciale en vaak moeilijke beslissingen bepalen het vervolg van de zaken. Weet u wat u zou doen?
Door inzichtelijk te maken waar de kritieke punten in uw systemen zitten kunt u adequaat reageren op een crisis en de gevolgen beperken. Hoe zit het met uw voorbereiding en respons? Onze consultants helpen u bij de belangrijkste acties zijn ten tijde van een crisis.

Bent u benieuwd naar de (financiële) impact van een cyberincident op uw organisatie en wat u kunt doen om deze te beperken? Of bent u al zo ver om uw cybercrisismanagement in te richten? Onze specialisten kijken graag met u mee en geven een passend advies ten behoeve van de continuïteit van uw bedrijf.

Claudia de Koning
Industrie Expert
+31 (0)6 462 941 86
claudia.de.koning@aon.nl

Cristina Stamate
Cyber Risk Consultant
+31 (0) 650411705
cristina.stamate@aon.nl

Aon.nl/logistiek

Over Aon

Aon plc (NYSE:AON) is een toonaangevende wereldwijde adviseur op het gebied van risico-, pensioen- en gezondheidsoplossingen. Aon analyseert de personele risico's en bedrijfsrisico's, geeft passend risicoadvies, zorgt voor de (financiële) oplossing en staat klanten bij als een incident de bedrijfscontinuïteit bedreigt. Zo helpen wij klanten succesvol te ondernemen.

Aon heeft in Nederland 15 locaties met 2.600 medewerkers en wereldwijd meer dan 50.000 medewerkers in ruim 120 landen.

Ga voor meer informatie naar **www.aon.nl**.

19.0088-04-V3

Empower Results®