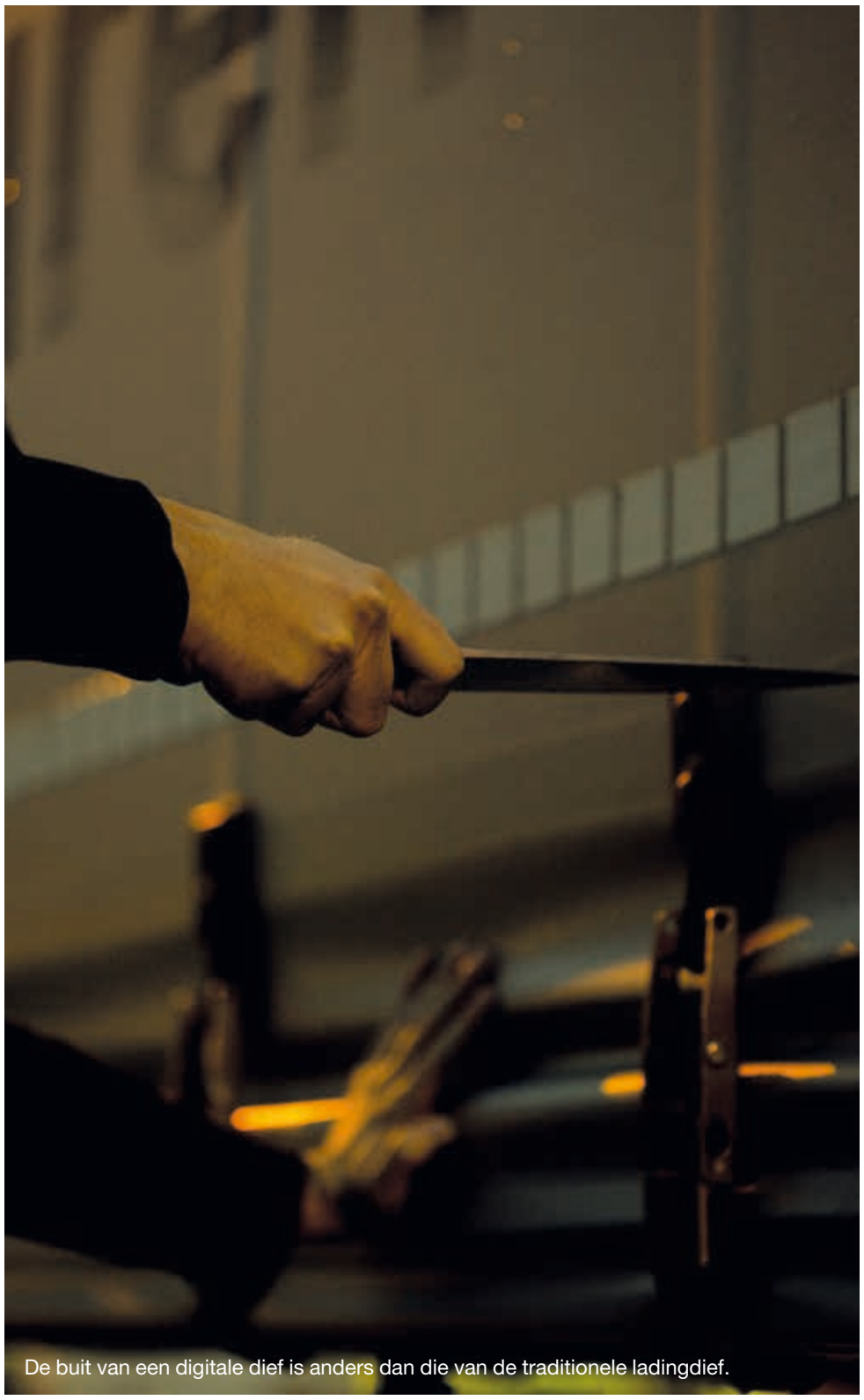
CYBERSECURITY IN DE LOGISTIEK

NIEUWE TECHNIEKEN, NIEUWE BEDREIGINGEN

De toenemende afhankelijkheid van data, applicaties en ict-infrastructuur maakt bedrijven kwetsbaar voor cyberrisico's. Die bedreigingen kunnen aanzienlijk zijn volgens het onlangs verschenen rapport 'Cybersecurity voor logistiek dienstverleners'.

Tekst **Steven van Aartrijk**



De buit van een digitale dief is anders dan die van de traditionele ladingdief.

Dennis de Hoog: “Zelfs als het vanuit ict allemaal goed is geregeld, wordt vaak de menselijke factor vergeten.”

In het recent gepubliceerde rapport ‘Cybersecurity voor logistiek dienstverleners’, opgesteld door makelaar en risicoadviseur Aon, ABN Amro en Transport en Logistiek Nederland (TLN), worden vijf waargebeurde digitale incidenten beschreven, die aantonen wat er kan gebeuren en hoeveel schade zo’n situatie kan veroorzaken. In een van de voorbeelden wordt geschetst hoe een bedrijf onvoorbereid is op een situatie waarbij de volledige ict wordt lamgelegd. Door het hardnekkige probleem krijgen klanten hun producten te laat, moeten specialisten worden ingehuurd om de situatie te verhelpen en moet personeel overwerken om achterstanden weg te werken. De werkonderbreking duurt een dag en veroorzaakt een schadepost van zestigduizend euro. Als het probleem nog langer had geduurd, had het voorbestaan van de onderneming op het spel gestaan.
Dennis de Hoog, managing consultant risico-adviseur bij Aon, helpt opdrachtgevers om zich teweer te stellen tegen risico’s verbonden met innovatie, de toepassing van nieuwe technologieën en digitalisering. Een vraaggesprek.

Het informatietijdperk is nog maar net gestart. We gaan van *bricks* naar *bytes*. Zijn bedrijven eerder geneigd om meer te investeren in de ‘leuke, geldgenererende’ mogelijkheden van ict dan in de security-kant?
“Dat zie je zeker gebeuren en dat is ook begrijpelijk. Om te overleven en te blijven groeien, zijn ondernemers continu op zoek naar toepassingen die hen in staat stellen om sneller, slimmer en beter te werken. Die drang zal voorlopig ook nog wel de overhand hebben ten opzichte van het inschatten van de risico’s die nieuwe innovaties met zich mee kunnen brengen. Nieuwe technieken omarmen is goed, maar tegelijkertijd moet je je er wel bewust van zijn dat ze ook nieuwe bedreigingen met zich meebrengen die juist negatieve invloed kunnen hebben op de continuïteit van de groei.”

Worden de cyberrisico’s groter?
“Ja. Nederland is een land met een heel uitgebreide infrastructuur en een hoge graad van digitalisering. Dat maakt ons gemiddeld genomen kwetsbaarder voor digitale criminelen. Ook eist een incident meer ‘slachtoffers’ doordat bedrijven extreem afhankelijk zijn van hun ict en tevens van partners in supply chains. Tegelijkertijd gelden voor *cybercrime* in feite dezelfde wetten als in de normale wereld; gelegenheid maakt de dief. Met andere woorden: als jouw slot beter is dan dat van de buurman, gaat de inbreker bij hem naar binnen. Die simpele parallel vertaalt zich goed naar het digitale domein. Er is een gelegenheidsstructuur gekomen voor nieuwe criminelen. Waar kunnen we ons geld verdienen, hoe goed zijn die inkomsten? Doelwit waren eerst de meer voor de hand liggende sectoren, zoals financiële instellingen, maar inmiddels is het vizier vaker gericht op logistieke bedrijven van gemiddelde omvang. Zij zijn een logischer doelwit, omdat ze over het algemeen minder investeren in zowel technische als organisatorische beveiliging.”

Schiet het bewustzijn van managers tekort als het gaat om de risico’s van cybercrime?
“Te vaak wordt het gezien als een puur technisch probleem. Tegen ict’ers wordt gezegd: ‘Alsje blieft, dit zijn jouw risico’s’, terwijl het beheersen van de risico’s van data-gedreven werken en het bewustzijn hierover aanwezig moet zijn in alle geledingen van een organisatie. Veel bedrijven bezien de problematiek nog als een technisch vraagstuk, iets wat ze niet kunnen overzien. Het blijft een abstract fenomeen, waardoor bewustwording en actie te vaak achterwege blijven. Daarnaast is de bestrijding van de risico’s natuurlijk ook een investeringsvraag. Het laten monitoren van je netwerk kan zo enkele tienduizenden euro’s kosten en als een bedrijf iemand op de payroll wil hebben met expertise op het gebied van data en privacy, is dat ook dat een kostenpost die kan drukken op de jaarrekening. Er moet worden gezocht naar een gezonde balans tussen veiligheid en werkbaarheid en die is voor elk bedrijf weer anders.”

Waarom zijn bedrijven die goederen opslaan en vervoeren extra kwetsbaar voor cybercrime?
“Veel van hun activiteiten zijn gedigitaliseerd. Denk aan klantcontacten, administratieve afwikkeling van douanezaken en het papierwerk rondom de specificaties van ladingen. Dat laatste gaat tegenwoordig ook steeds meer digitaal. Bij dit soort bedrijven staat de poort voor kwaadwillenden wellicht net iets verder open, omdat ze de beveiliging vaak in de basis niet goed op orde hebben, anders dan bijvoorbeeld een techbedrijf, dat standaard al heel veel kenners in huis heeft die hiervoor zorg

> “Een data-lek ontstaat niet altijd door de inbraak van een hacker”

kunnen dragen. Risico's voor logistieke bedrijven hangen ook samen met verantwoordelijkheid en aansprakelijkheid. Als het gaat om een lading van een klant, of data over een klant, is die klant afhankelijk van hoe goed jij je zaken op orde hebt."

Hoe is risicobewustzijn goed over te brengen op de werkvloer, van de conciërge tot de CEO?
"Dat brede bewustzijn kweken, is het moeilijkst. Zelfs als het vanuit ict allemaal goed is geregeld, wordt vaak de menselijke factor vergeten. Een data-lek ontstaat niet altijd door de inbraak van een hacker, maar wordt ook veroorzaakt doordat een medewerker onzorgvuldig omgaat met informatie. Uiteindelijk is het wel of niet hebben van voldoende bewuste medewerkers dan ook een bepalende factor. Medewerkers vinden het irritant dat ze telkens opnieuw een lang en veilig wachtwoord moeten bedenken. Toch is het zaak dat alle medewerkers zich bewust zijn van de risico's. De ondernemer moet zich afvragen; wat is ons handelingsprotocol, wat mag wel en wat niet? Wat melden we wel en wat niet? Hij moet een scherp beeld hebben van wat hij verlangt van zijn medewerkers, daar begint het."

Wat voor soort crimineel is die digitale afperser?
"Natuurlijk heeft deze crimineel een ander profiel dan de dief die met een mes het zeil van een vrachtauto opensnijdt om vervolgens de lading te stelen. In de regel hebben zij een hoger opleidingsniveau en wijkt ook hun sociaaleconomische achtergrond af van de 'standaard ladingdief'. Zijn profiel is meer *high-end* ten opzichte van de klassieke dief. Daarnaast zijn er hackersgilden, waar de prestaties van de cybercriminelen om iets voor elkaar te krijgen, gelden als een soort statusuiting. Wat kun je hacken, wat kun je platleggen? Maar het zijn ook vaak professionele, criminele organisaties die data stelen en pas weer vrijgeven als er een betaling is gedaan. Het is belangrijk om te beseffen dat de buit ook anders is. Goederen zijn maar één keer te verkopen. Data kun je onbeperkt verwerken, gijzelen, maar ook kopiëren en dus ook verkopen."

Heeft cybersecurity altijd te maken met misdaad?
"Nee zeker niet. Integendeel, zou ik bijna willen zeggen. Dat cybercrime en het fenomeen hackers veel aandacht trekken, is begrijpelijk. Tegelijk zie je echter vaak dat schade wordt veroorzaakt door eigen technisch falen, menselijk handelen of fouten van derden. Bijvoorbeeld een medewerker die een computerapplicatie verkeerd schrijft waardoor systeemfouten ontstaan, of een bouwbedrijf dat per ongeluk bij werkzaamheden aan de stoep de voeding van een serverpark doorsnijdt. Of werknemers die hun laptop laten rondslingeren. Vaak is er geen hacker nodig voor een lek. Dus wil je cyberrisico's effectief aanpakken, heb dan ook oog voor de ogenschijnlijk kleine risico's, op huis-tuin-en-keukenniveau."

Kunnen bedrijven zich verzekeren tegen cybercrime?
"In de eerste plaats moet een bedrijf zich zo goed mogelijk voorbereiden op een eventueel incident. Als onverhoopt toch blijkt dat de *firewall* niet hoog genoeg is opgetrokken, kan er iets misgaan. De vraag is dan of je dat snel genoeg ziet en snel genoeg reageert om de schade te beperken. Als een onderneming oplossende expertise niet in huis heeft, is het mogelijk om een cyberverzekering af te sluiten, waarmee het bedrijf onder meer technische en juridische hulptroepen kan laten invliegen wanneer dat nodig is. Daarnaast dekt deze verzekering gederfde inkomsten en mogelijke aansprakelijkheidsstellingen van derden. Hoe veel zo'n verzekering kost, hangt af van de eigen risicobereidheid, bijvoorbeeld ten aanzien van claims van klanten. Omdat deze cybercrime-polissen relatief nieuw zijn, zijn de instapniveaus - en daarmee ook de kosten - niet al te hoog. Het kan dus zeker interessant zijn om zo'n verzekering te overwegen."

"Het wel of niet hebben van bewuste medewerkers is een bepalende factor"

Rapport

In het rapport Cybersecurity voor logistiek dienstverleners wordt uitgebreid omschreven hoe cybercrime is te voorkomen en hoe een bedrijf zich kan voorbereiden op de situatie die ontstaat als het toch slachtoffer wordt. Het rapport is te downloaden op http://insight.aon.com/cyber-logistiek-downloaden.

Incidenten

Vijf recente digitale incidenten bij logistiek dienstverleners in Nederland.

- Een bedrijf ontvangt een e-mail met een (nep)factuur en na opening blijkt deze besmet te zijn met zogenoemde *malware*. Deze zorgt er onder meer voor dat een medewerker niet meer bij de voorraadgegevens kan. De afpersers eisen negenhonderd euro, maar het bedrijf besluit niet te betalen. Uiteindelijk is het bedrijf een week bezig alle gegevens weer kloppend te krijgen. Maximale schade van zo'n incident: vijftigduizend euro.
- Via *phishing* weten criminelen toegang te krijgen tot de gegevens van het bedrijf. Ze vinden in de administratie een kostbare lading met laptops en smartphones en vervalsen de gegevens, zodat de lading wordt bezorgd bij de criminelen. Schade: tientallen duizenden euro's.
- Een medewerker van de financiële administratie van een bedrijf ontvangt een e-mail van de CEO, die de werknemer verzoekt een vertrouwelijke en urgente betaling uit te voeren in het kader van een overname. Doordat de omstandigheden rondom dit valse verzoek zo waarheidsgetrouw mogelijk zijn gemaakt, trapt de medewerker erin en maakt hij de verzochte vijftigduizend euro over.
- De laptop van een medewerker van personeelszaken wordt gestolen. Deze is niet beveiligd en bevat privé-personeelsgegevens en klantgegevens. Een melding aan de Autoriteit Persoonsgegevens is noodzakelijk. Deze stelt vast dat de data niet beveiligd waren. Het bedrijf moet personeel en klanten ervan op de hoogte stellen dat vertrouwelijke informatie over hen is gestolen. Behalve geleden financiële schade voor het dichten van het lek, heeft het bedrijf mogelijk ook nog eens de privacywetgeving geschonden.
- Door onbekende oorzaak valt de ict bij een bedrijf uit. Het probleem is ingewikkelder dan gedacht. Het bedrijf is een hele dag niet bereikbaar, gegevens zijn verloren gegaan. Klanten krijgen hun producten te laat, personeel moet overwerken om de achterstanden weg te werken. Totale schade: zestigduizend euro. Als de storing langer had geduurd, had de situatie tot een faillissement kunnen leiden.

COLUMN

Machiel van der Kuijl, algemeen directeur evofenedex

BLIK NAAR BUITEN

Deze eerste editie van evofenedex logisticx staat bol van de logistieke en internationale ontwikkelingen die van invloed zijn op uw bedrijf; van de gevolgen van het klimaatakkoord in Parijs tot de laatste ontwikkelingen in de scheepvaart. De artikelen onderstrepen dat de wereld niet stilstaat. Ook met de Tweede Kamerverkiezingen in zicht rijst de vraag: spelen we hier op in of sluiten we onze ogen? Met andere woorden: richten we de blik naar buiten of naar binnen?

'Naar buiten', is volgens mij het enige juiste en verstandige antwoord. Als ondernemer werk je immers in een wereld die snel verandert. Een wereld ook waarin het werk steeds vaker afhankelijk is van het internationale speelveld - of je nu internationaal onderneemt of niet. In dit speelveld zijn logistiek en export met elkaar verweven geraakt. Door globalisering, door opgeknipte productieketens en door digitalisering.

Het is u vast niet ontgaan dat EVO en Fenedex zijn samengegaan in evofenedex. Of het nu gaat om een efficient en veilig magazijn, snel en slim goederenvervoer, een veilige opslag en vervoer van gevaarlijke stoffen of meer export, samen met de leden heeft evofenedex een brede blik op uw wereld en de wereld daarbuiten. Uiteraard strijdt evofenedex als één krachtig collectief van vijftienduizend handels- en productiebedrijven voor de belangen van haar leden. Regionaal, nationaal en internationaal. Dus ook in Den Haag.

Daarom voerde evofenedex in de aanloop naar de Tweede Kamerverkiezingen campagne. Niet voor zetels, maar voor een tienpuntenplan voor meer export en een slimmere logistiek. Tientallen 'evofenedexers' spraken op verschillende zaterdagochtenden met de congresgangers van politieke partijen. Zo maakte evofenedex zich bij het D66-congres hard voor minder betuttelende regels voor ondernemers die hun bestelauto als werkpaard gebruiken, pleitte de vereniging bij het congres van GroenLinks voor een werkbaar duurzaamheidsbeleid en bij de PvdA voor een gelijk speelveld in Europa.

Deze campagne zorgde er in elk geval voor dat de belangen van de leden op evofenedex op het netvlies van politici staan. Of het ook in gunstig beleid resulteert, zal na de verkiezingen blijken. Dan maakt een nieuwe regering zich hopelijk hard voor meer export en een slimmere logistiek. Pas dan is onze campagne écht geslaagd.