

'CYBERSECURITY MOET 'CHEFSACHE' ZIJN:
EEN VERANTWOORDELIJKHEID VAN DE
GEHELE BOARDROOM DIE CONTINU OP
DE AGENDA STAAT'

CYBERMAFFIA PROBEERT ELKE DEUR



NIEUWE EN PERMANENTE DREIGING

Recepturen of klantgegevens open en bloot op straat. Of je bedrijf dagenlang plat omdat de computersystemen zijn gegijzeld met ransomware. Een nachtmerrie voor elke ondernemer. Hoe wapen je jezelf tegen oprukkende cybercriminelen?

TEKST: REDACTIE VERF & INKT
ILLUSTRATIES: ISTOCK

Volgens Hans de Jong, covoorzitter van de Nederlandse Cyber Security Raad namens VNO-NCW, is de totale schade van cybercrime in Nederland moeilijk zichtbaar te maken. "Er is zowel directe als indirecte schade. Daarnaast doen maar heel weinig bedrijven aangifte wanneer zij slachtoffer zijn geworden van cybercriminelen. Dat is belangrijk zodat we een scherper beeld krijgen van cybercrime en hier effectiever op kunnen inspelen."

De Nederlandse Cyber Security Raad -een nationaal en onafhankelijk adviesorgaan van het kabinet met wetenschappers en hooggeplaatste vertegenwoordigers uit de private sector en publieke sector- spreekt van een 'permanente en toenemende dreiging'.

Hans de Jong: "Cyberveiligheid is van levensbelang, voor de Nederlandse samenleving en economie. Toonaangevende rapporten laten zien dat de risico's alleen maar toenemen en dat de investeringen niet navenant meegroeien. Om Nederland welvarend en veilig te houden, moet er flink geïnvesteerd worden in onze cyberweerbaarheid."

Sterke keten

Ook niet-vitale bedrijven, zoals de verf- en drukinktindustrie, moeten voldoende cyberweerbaar zijn, vindt De Jong. "Zij kunnen onderdeel uitmaken van een vitaal proces, en de keten is zo sterk als de zwakste schakel. Hackers kunnen onvoldoende beveiligde bedrijven gebruiken om toegang te krijgen tot andere meer cruciale bedrijven. In 2018 is dan ook het Digital Trust Center opgericht, speciaal om ook hen te ondersteunen."

Het Digital Trust Center (DTC) geeft ondernemers advies op het gebied van cyberweerbaarheid, deelt informatie en stimuleert samenwerkingsverbanden tussen bedrijven op het gebied van cyberweerbaarheid. Doel is Nederland een 'safer place to do business' maken. De Jong: "Ondanks dat Nederland op sommige ranglijsten in de top staat, is dit zeker geen reden om achterover te leunen. Het komende kabinet moet in actie komen. In het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' pleit de raad daarom voor een investering van 833 miljoen in onze cyberweerbaarheid om ons beter te kunnen wapenen tegen de toenemende cyberaanvallen."



\$18 MILJARD LOSGELD

Tien jaar geleden was het mijnen van bitcoins een interessante bezigheid waarbij zoveel mogelijk computers (ongezien) op afstand aan het werk werden gezet. Die goudmijn is opgedroogd door betere firewalls en dus hebben hackers de aandacht verlegd, vooral naar ransomware: gijzelsoftware. Via een aanval of een klik op een 'phishing mail' nemen hackers de controle over computersystemen over. Die krijgt een bedrijf pas terug na betaling van losgeld. In 2020 is wereldwijd zeker 18 miljard dollar betaald aan cybercriminelen aldus beveiligingsbedrijf Emsisoft. De digitale inhaalslag die bedrijven aan het begin van de coronapandemie maakten om zoveel mogelijk mensen thuis te kunnen laten werken, zorgde bovendien voor meer kansen voor hackers. Snelheid ging vaak even boven veiligheid.

Geen enkele ondernemer, groot of klein, kan zich veilig wanen. Het maakt cybercriminelen niet uit aan wie ze hun bitcoins verdienen. Bij de aanval van de hackgroep REvil begin juli werden meer dan 800 grote, maar ook kleinere bedrijven getroffen. De criminelen kwamen binnen via software van Kaseya dat systemen van klanten op afstand beheert, en hanteerden een speciale prijslijst. Ondernemers die besloten hun systemen vrij te kopen, betaalden losgeld naar rato van de grootte van hun bedrijf.

cilindrische verfblikken ImCare®

optimale bescherming

bodem, ring en deksel

RL en TT sluitingen

3-delig

premium uitstraling

offset bedrukking

zelfklevend etiket

met draaghengsel

100% recyclebaar

van 125 ml t/m 4 liter

Mus Verpakkingen



Blik bepalend



Mus Verpakkingen BV | Herfordstraat 9 | 7418 EX | NL - Deventer
T +31 (0)570 629 229 | info@musverpakkingen.nl | www.musverpakkingen.nl

ARJAN MULDER,
BUSINESS PROCESS MANAGER,
KONINKLIJKE VAN WIJHE VERF, ZWOLLE

CA. 220 MEDEWERKERS, EIGEN ICT-AFDELING

Worst case scenario?

Een hack waarbij bedrijfsgeheimen zoals recepturen worden gestolen of een aanval met ransomware waardoor de hele bedrijfsvoering stilligt.

Lig je er wakker van?

Cybersecurity staat hoog op de agenda hier en wij zijn ons ervan bewust dat dit ook altijd een belangrijk onderdeel moet blijven.

Aanpak?

Goed beveiligde software en zorgen dat alles altijd up-to-date is. Wij trainen ook het personeel over de risico's en laten de beveiliging regelmatig doorlichten door externe deskundigen.

Incidenten gehad?

Incidenten zijn er altijd, maar tot op heden hebben wij hier altijd heel adequaat op kunnen reageren en hadden deze weinig tot geen impact.

Jullie zijn veilig?

Je mag je nooit veilig rekenen op dit gebied. Cybercriminelen zitten immers niet stil en wij doen er alles aan om onze beveiliging op orde te houden. Vitale bedrijven en publieke organisaties lopen misschien meer risico, maar bij ons leeft zeker niet de gedachte dat een bedrijf als het onze niet geraakt zal worden.

Nog tips voor collega-bedrijven?

Een frisse blik van buiten door externe specialisten kan ik zeker aanraden. Dit veld is continu in beweging, dat moet je goed beseffen.



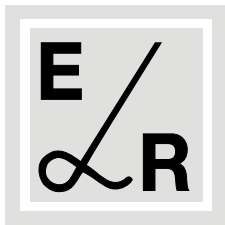
Spionage en sabotage

De Jong: "Cybercrime is evident een grensoverschrijdend vraagstuk. Geen enkel land kan dit alleen oplossen en het is belangrijker dan ooit dat we goed samenwerken. Maar dat neemt niet weg dat er ook op nationaal niveau actie kan en moet worden ondernomen. De verf- en drukinktindustrie kan bijvoorbeeld een Information Sharing and Analysis Centre (ISAC) starten om zo gezamenlijk de cyberweerbaarheid van de branche te versterken. Er zijn goede voorbeelden in ons land waar grote bedrijven kleinere bedrijven helpen." De Cyber Security Raad is er voor adviezen aan het kabinet, toch heeft De Jong ook een belangrijke boodschap aan alle ondernemers. Cybersecurity moet 'chefsache' zijn: een verantwoordelijkheid van de gehele boardroom die continu op de agenda staat. De IT-afdeling speelt uiteraard ook een belangrijke rol, maar elke boardroom moet op strategisch niveau de kaders bepalen voor het formuleren, implementeren, bewaken en handhaven van het cybersecuritybeleid in de organisatie.

DE BASISPRINCIPES VOOR GOEDE CYBERWEERBAARHEID - ALDUS HET DIGITAL TRUST CENTER

- 1. Maak een risicoanalyse:** Hoe kwetsbaar is de onderneming? Inventariseer hard- en software risico's. Het Digital Trust Center (DTC) biedt een stappenplan hiertoe.
- 2. Kies veilige instellingen:** Leveranciers gebruiken standaardinstellingen die installatie en toegankelijkheid eenvoudig maken. Bekijk de instellingen kritisch en kies defensieve opties.
- 3. Snelle updates:** Installeer beveiligingsupdates direct. Schakel automatische updates in zodat apparaten en software altijd draaien met de laatste versie.
- 4. Beperk toegang:** Bepaal per medewerker tot welke systemen en data toegang nodig is, en zorg dat deze toegangsrechten up-to-date blijven.
- 5. Voorkom virussen/malware:** train medewerkers in veilig gedrag, gebruik antivirusprogramma's, download apps veilig en beperk installatiemogelijkheden van software

Bron: www.digitaltrustcenter.nl



E & R B.V.

Proven Excellence.

NETZSCH *Alpha*® NEOS de nieuwe standaard!



Al meer dan 40 jaar uw vertrouwde partner in procesmachines voor de verf- en inkt industrie.



Samen met onze partners NETZSCH Feinmahltechnik GmbH en J. De Vree & Co N.V. bieden wij innovatie dispergeersystemen, parelmolens, mengmachines, afvulmachines & turnkey projecten voor de verf- & inkt industrie.

Optimaal dispergeren, malen, mengen en afvullen. Hogere productiviteit. Kortere omsteltijden. Besparen op energie, koelwaterverbruik en onderhoud.

Wij vertellen u er graag meer over!



DEVREE DEVREE

er-bv.com

NETZSCH
Proven Excellence.

RECENTE GROTE HACKS:

Colonial Pipeline (april 2021) - het grootste oliepijpleidingbedrijf van de Verenigde Staten moet leidingen sluiten na een hack. Er dreigt een brandstoftekort en burgers hamsteren benzine.

JBS Foods (juni 2021) - de computersystemen van het grootste vleesverwerkende bedrijf ter wereld worden door ransomware stilgelegd. JBS betaalt elf miljoen dollar in bitcoins om haar slachterijen in de VS, Australië en Canada weer te kunnen gebruiken.

Kaseya hack (juli 2021) - hackers gijzelen zeker duizend grote en kleine bedrijven via software voor beheer van klantsystemen op afstand. In Zweden moet supermarktketen COOP alle achthonderd winkels sluiten, in Nieuw-Zeeland staan computerschermen op scholen op zwart. In Nederland worden onder meer Hoppenbrouwers Techniek en ICT-bedrijf VelzArt en haar klanten getroffen.



'DE TOTALE SCHADE VAN CYBERCRIME IN NEDERLAND IS ONDUIDELIJK. NIET ALLE BEDRIJVEN DOEN AANGIFTE EN ER IS MEESTAL ZOWEL DIRECTE ALS INDIRECTE SCHADE'

PATRICK VAN DEN BOOM,
DIRECTEUR/EIGENAAR, DROST COATINGS, VENLO

CA. 35 MEDEWERKERS,
ICT-DIENSTEN INGEHUURD VIA PERCOM

Worst case scenario?

Formules en klantgegevens die op straat liggen, dat is dodelijk voor je bedrijf

Lig je er wakker van?

Eerlijk gezegd maak ik me drukker over de grondstofaanvoer. Maar na zo'n hack als laatst gaat er wel een belletje naar PerCom: zijn we veilig? Dat werd al snel bevestigd.

Aanpak?

PerCom zorgt voor antivirusprogramma's, een firewall en maakt elke nacht een versleutelde back-up. Ze wijzen er ons ook op als er nieuwe investeringen nodig zijn omdat hard- of software dreigt te verouderen.

Incidenten gehad?

Een workstation hier is eens vastgelopen door een aanval, maar dat was gelukkig binnen een dag opgelost zonder schade. En regelmatig stuur ik verdacht uitziende mails door naar PerCom.

Jullie zijn veilig?

Zo goed als dat kan, denk ik. Ik heb gelukkig ook nog nooit van collega's in de verf gehoord dat er iets ernstigs is gebeurd. Maar we moeten alert blijven. Het is zo gebeurd: even snel snel in de drukte je mails wegwerken en op een verkeerde link klikken ...

Nog tips voor collega-bedrijven?

Haal de expertise in huis wanneer je die zelf niet hebt.



Your trusted distribution
partner for innovative
ingredients and specialty
chemicals



Blanket coverage of
Asia Pacific and
Western Europe



Focus on **Life Science**
and **Industrial**
Specialties



Over
30,000 customers served



48 formulation labs



1,260 employees



90 regulatory experts



DKSH Performance Materials is a **leading pure specialties player**
Discover more at www.dksh.com/pm



Delivering growth – in Asia and beyond.