HOE VEILIG ZIJN UW DATA?

WAT JE KAN MAKEN, KAN JE KRAKEN

ICT biedt vele voordelen, zoals vergevorderde procesautomatisering, de opkomst van Industrie 4.0, big data en 3D. Maar er duiken ook risico's op zoals cybercrime, een vorm van criminaliteit die niet meer weg te denken is. Hoe goed zijn bedrijven in de maakindustrie hiertegen opgewassen? PT Industrieel Management ging op onderzoek en bemerkte dat echt iedereen slachtoffer kan worden.

Tekst **Evi Husson**

Wat is cybercrime en waar komt het vandaan?

De term cybercrime komt uit het Amerikaanse recht als algemene aanduiding van misdrijven waarbij computers of netwerken worden gebruikt. De eerste vorm van cybercrime zou zijn gepleegd in 1903 in Groot-Brittannië. Daar werd een draadloze telegraaf gesaboteerd waardoor de "kwajongen" schunnige teksten de ether in kon zenden. Deze daad had weliswaar geen grote gevolgen, maar de toon was gezet.
In de jaren zeventig kon een Amerikaan een telefoonsysteem kraken zodat hij gratis kon bellen. In de jaren tachtig werd de eerste malware ontwikkeld. *Malicious software* zoals computerwormen oftewel zichzelf verspreidende computerprogramma's en computervirussen die zich vasthechten aan bestanden en daarna schade kunnen aanrichten aan bestanden of gegevens.
In 1999 verschenen de eerste virussen die zich in computers "verstopten" om de geïnfecteerde computers later tot slaaf te maken. Een extern persoon kan dan via een externe computer de "slavencomputers" bepaalde functies laten uitvoeren. Cybercriminelen verhuren zelfs zogenaamde botnets aan bedrijven om zo de systemen van concurrenten te vertragen of uit de lucht te halen.

Industrie

Er zijn diverse voorbeelden te noemen in het bedrijfsleven, maar de industriële sector blijft niet buiten schot. In 2010 werd het schadelijke computervirus Stuxnet in Iran ontdekt, dat de werking van Siemens' S7 PLC's op schadelijke wijze beïnvloedt. Het zou ontwikkeld zijn om Iraanse ultracentrifuges te saboteren die worden gebruikt voor het maken van nucleaire brandstof. De worm wijzigt de PLC waarmee de motoren van de centrifuges worden aangestuurd.
Dichter bij huis probeerden criminelen in 2012 bij DSM de inloggegevens van het chemieconcern te stelen door op een parkeerplaats van DSM usb-sticks met spionagesoftware te leggen. De usb-sticks bevatten software die in staat was om inloggegevens naar externe websites te versturen.
Het zijn slechte een paar voorbeelden van cybercriminaliteit, maar het aantal "geslaagde" aanvallen is ontelbaar. En dat kost bedrijven en organisaties geld. Veel geld.

Kosten

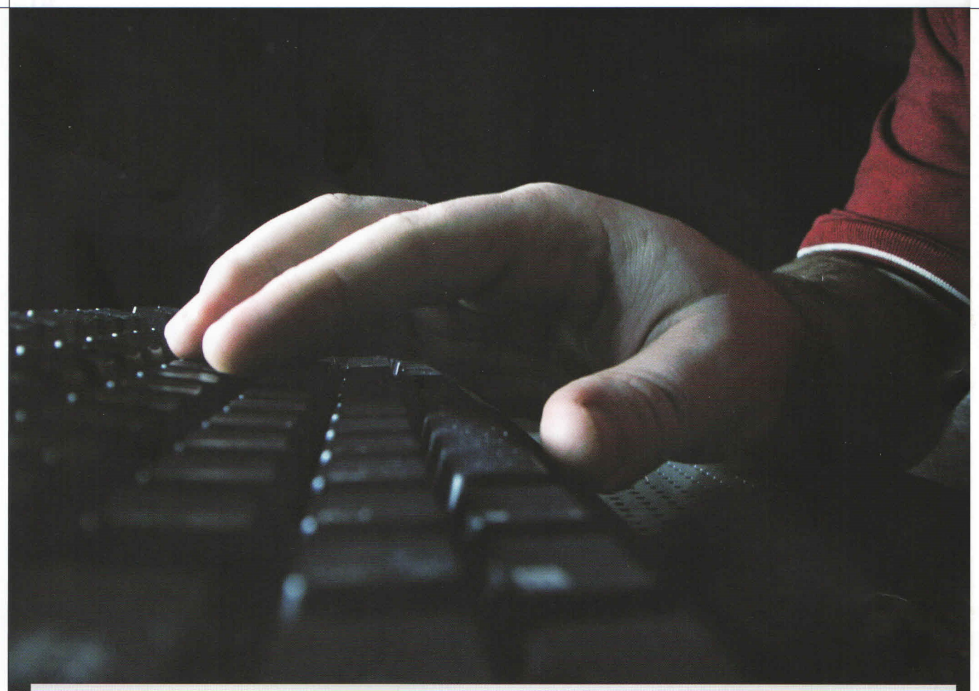
Volgens een in juni verschenen rapport van beveiligingsbedrijf McAfee en de Amerikaanse denktank *Center for Strategic and International Studies* zouden de wereldwijde kosten van cybercrime oplopen tot 325 miljard euro per jaar. Voor Nederland zou de schade 8,8 miljard bedragen, voor België 3,5 miljard euro. Vooral digitale financiële fraude komt steeds vaker voor, omdat het relatief eenvoudig is geworden om malware aan te kopen die bankgegevens steelt, en er in veel gevallen weinig technische kennis nodig is.
Financiële fraude is helaas niet de enige soort fraude. Schade wordt ook veroorzaakt door diefstal van intellectueel eigendom van bedrijven. De kosten hiervan zijn veel moeilijker te berekenen, om maar niet te spreken van reputatieschade en de invloed daarvan op klanttevredenheid en leveranciers. Bedrijven melden dit vaak niet of hebben soms helemaal niet door dat ze zijn getroffen door cybercriminelen.

Trends rond cybercrime

Toch is er geen reden tot enorme ongerustheid, stelt Marcel Jutte. Hij is voorzitter van ISA Nederland (International Society for Automation) en managing director van Hudson Cybertec, gespecialiseerd in cyber security waar techniek een cruciale rol speelt. 'Ja, je moet bezorgd zijn als bedrijf, maar dat is niet het allerbelangrijkste. Je moet als bedrijf vooral zorgen voor voldoende *awareness* binnen het bedrijf. De maakindustrie wordt zich gelukkig steeds bewuster van potentiële risico's. Vroeger werd alles wat met cyber te maken had al snel als science fiction bestempeld, maar tegenwoordig zien bedrijven steeds meer de ernst ervan in. Er is uiteraard nog heel veel werk aan de winkel, maar het wordt steeds meer bespreekbaar.'
Mark Buningh, werkzaam bij Aon als senior consultant risicomanagement, richt zich al enige jaren specifiek op het beheersen van cyberrisico's in de bedrijfswereld. Volgens hem zijn er binnen cybercrime diverse trends gaande. Hij licht er twee uit; ten eerste het bekende phishing, het oplichten van mensen door ze te lokken naar een valse (bank)website, om geheime informatie te ontfutselen en ten tweede datalekken. 'Organisaties zijn nooit honderd procent veilig of te beveiligen. De vraag is: hoeveel is voldoende? Afhankelijk van het motief zullen andere methodes worden gekozen, maar binnen de maakindustrie zal het risicoprofiel op dit vlak zich veelal concentreren rondom de diefstal van waardevolle zaken als inloggegevens, vertrouwelijke bedrijfsinformatie en intellectueel eigendom.'
Wat er feitelijk gebeurt, is dat informatie wordt gewijzigd, ontvreemd of versleuteld. 'Veel bedrijven hebben een hek om het bedrijf staan, maar als je eenmaal binnen bent, dan ontbreekt er vaak toezicht en monitoring. Wat je ziet, is dat bij datalekken de aanvaller vaak al maanden binnen is in een bedrijfsnetwerk voor men dit in de gaten heeft. Bedrijfsgeheimen, handelsovereenkomsten, intellectueel eigendom en copyright worden dan ontvreemd. Zonder namen te noemen kan ik stellen dat bepaalde maak- of productiebedrijven in Nederland hebben moeten vaststellen dat hun producten in China eerder op de markt zijn gekomen dan in Nederland. Een map op een computer binnen de R&D-afdeling bleek al

Kan ik waarnemen of ik ben gehackt?

Een monitoringssysteem is erg belangrijk om te kunnen nagaan wat er gebeurt, vertelt Jutte. Hij geeft een voorbeeld. 'Een fabriek maakt gebruik van toeleveranciers. Is er iets stuk, dan komt een storingsmonteur van de leverancier van de machine op bezoek die zijn laptop aansluit op het systeem om het defect te verhelpen. Maar hoe weet je honderd procent zeker dat die pc niet vol staat met malware, virussen of dat hij gegevens uit je systeem trekt? Staat er vertrouwelijke data in het systeem waar de laptop van de monteur aan wordt gekoppeld? Je moet weten wat er allemaal op je netwerk gebeurt en wie er op je netwerk zit. Als de storingsmonteur van een machinefabrikant op je netwerk is geweest, en later blijkt dat er andere problemen opduiken of ontstaan, dan moet je heel eenvoudig kunnen terugvinden of nagaan in de logfiles dat er een vreemde pc is ingelogd op het netwerk. En je moet er vervolgens ook iets mee doen. Beheers je netwerk en leg een en ander vast in de policy en procedures van het bedrijf. Dat wordt vaak vergeten.'



Misvattingen rond cyber security

Misvatting 1: Verhoog het IT budget en je bent veilig
Een gedachte die bedrijven soms hebben, is dat als je het computertechnisch voldoende beveiligt, je het wel redt. Dat klopt absoluut niet, stelt Buningh. Hij staaft dit met een voorbeeld uit de Bloomberg Government Study - *The Price of Cybersecurity: Big Investments, Small Improvements*: 'Bij een S&P500 genoteerd bedrijf stelde het management de IT'ers voor om hun budget te verdubbelen zodat ze een volledige garantie zouden krijgen dat het bedrijf veilig was tegen cybercrime. Dat konden ze niet. Ook met een vertienvoudiging van het budget zouden ze het nooit voor honderd procent dicht kunnen timmeren. En dit zal nu en ook in de toekomst nooit kunnen gebeuren.'
De IT-afdeling is wél de plek waar een voorsprong bestaat ten aanzien van de inhoudelijke kennis ter zake, en waar de bedrijfsautomatisering veelal wordt uitgevoerd en beheerd, maar is niet de afdeling die verantwoordelijk kan worden gehouden voor ICT-beleid en besturing, en de waarborging daarvan, voor de organisatie als geheel.'

Misvatting 2: Met IT-beveiliging beveilig je ook OT
Veel bedrijven laten zich adviseren door hun bestaande IT-leverancier. Jutte: 'Cyber security betekent niet zomaar dat je voldoende veilig bent door je IT te beveiligen. Je moet ook je OT (operational technology) omgeving beveiligen en daar komt vaak meer bij kijken dan alleen de techniek die we kennen in een kantooromgeving. Je hebt hier te maken met geheel andere systemen in een soms gevaarlijke omgeving, met een andere (werk)cultuur. Als dit oncontroleerbaar wordt, kan dit grote gevolgen hebben. Denk hierbij aan het stilvallen van de installatie, milieu schade, ongevallen en zelfs doden. Heel veel bedrijven gaan hieraan voorbij, maar dat is een grove misvatting, stelt Jutte.

Missvatting 3: We weten wat er op ons netwerk gebeurt
Uit de praktijk blijkt dat mensen zelden weten wat er precies in hun netwerk gebeurt, stelt Jutte. Er wordt bijgebouwd, zaken worden aangepast, systemen krijgen een update, storingen worden verholpen. Als bedrijf moet je je afvragen hoe dit alles is georganiseerd en wie dit allemaal bijhoudt. Als er modules of onderdelen worden aangepast of bijgeplaatst, wordt dit dan doorgevoerd in de documentatie? Heel vaak wordt dit vergeten.

Misvatting 4: Een installatie die niet gekoppeld is aan internet, loopt geen gevaar
Een vierde misvatting is dat apparaten of computers die niet aan het internet zijn gekoppeld, geen gevaar lopen. Dit klopt niet, stelt Jutte. 'Een apparaat zonder enige connectie met andere systemen is in principe ook kwetsbaar, althans als er behoefte is aan de informatie van die systemen. Zodra je een usb-stick of een ander device gebruikt om gegevens uit te wisselen, heb je eigenlijk ook al een connectie.'

Wie zit erachter?

Wie er achter cybercrime zit, is vaak onbekend. Meestal gaat het om hackers van buitenaf, maar niet altijd. Buningh, richt zich al enige jaren specifiek op het beheersen van cyberrisico's in de bedrijfswereld. Uit onderzoek van Aon, zo stelt Buningh, blijkt dat het eigen personeel evenzeer kan toeslaan. Hij geeft een voorbeeld. 'Van een bedrijf in de Nederlandse maakindustrie was sprake van een opvallend hoog verloop op één van de IT-afdelingen in het Verre Oosten. Heel doelbewust waren ze van plan om kort in dienst te zijn en tijdens die periode zoveel mogelijk informatie van het netwerk naar hun privé-account/mail te sturen. Deze praktijken komen ook in Nederland voor.'

maanden gecompromitteerd. Informatie en kennis wordt vaak niet voldoende beschermd. Ons advies? Behandel uw data als geld!'

Voorzorgsmaatregelen?

Bedrijven moeten daarom zowel extern als intern kijken naar cyberrisico's en daarbij passende beheersmaatregelen nemen, gaat Buningh verder. 'Wanneer een bedrijf werkt met patenten en hoogwaardige technologie, is het bijvoorbeeld noodzakelijk dat een HR-afdeling screent op antecedenten en referenties. En zeker bij R&D-werknemers maatregelen treft zoals aanvullende autorisatie, authenticatie en verificatie.'
Risico's moeten op alle niveaus worden onderzocht, maar ook is onderlinge samenwerking noodzakelijk. 'Een salesafdeling wil mogelijk zoveel mogelijk informatie over klanten verzamelen en wil zich profileren als 'big data company'. Het gebruikt de gegevens om het bedrijf sterker te maken en te laten groeien. De juridische afdeling geeft wellicht de voorkeur aan het zijn van een 'minimal data company' om te voorkomen dat informatie zoek raakt of in verkeerde handen terechtkomt. Dat zijn conflicterende belangen waarbij overkoepelend op bestuurlijk niveau een beleid moet komen. Cyberrisico is daarmee een organisatie-breed aandachtsgebied.

Drie pilaren

Het belang van bestuurlijk beleid en de organisatorische samenhang in de uitvoering daarvan, wordt ook onderschreven door Jutte. Het is volgens hem één van de drie pilaren die binnen het bedrijf in balans moeten zijn, naast mens en techniek. Als één van deze drie niet in balans is, dan werkt het niet, stelt hij. En zoals altijd is de mens daarbij de zwakste schakel.
'Zorg als bedrijf dat iedereen in het bedrijf zich voldoende bewust is van de risico's. Je kunt een wachtwoord heel lang en ingewikkeld kiezen, maar als je het ergens opschrijft om het te onthouden, dan helpt een lang en moeilijk wachtwoord niet. Of stel dat de hoofd techniek heel goed omgaat met zijn gegevens, maar zijn laptop mee naar huis neemt om daar verder te werken. Zoonlief heeft misschien ook tijdelijk toegang tot de computer of het netwerk. Zonder het te willen, of zonder je ervan bewust te zijn, kan er heel wat misgelopen.'
De tweede pijler is techniek, gaat Jutte verder. 'Zorg voor firewalls en anti-virus/anti-malware programma's, dat het netwerk juist is ge(re)designed, dat de switches en firewall's juist zijn geconfigureerd en zorg voor een geschikt monitoringsysteem.'
Dan kom je uit op de derde pijler, organisatie. 'Uit de praktijk blijkt dat mensen zelden weten wat er precies in hun netwerk gebeurt. Hoe zit het met aangeleverde units? Als modules bijvoorbeeld worden aangepast, wordt dit dan doorgevoerd in de documentatie? Heel vaak wordt dit vergeten. Dat is ook één van de grote verschillen tussen OT (operational technology) en IT (information technology).'
Jutte geeft een voorbeeld. 'Een storing moet zo snel mogelijk worden verholpen om verdere productie-achterstand te voorkomen. De storingsmonteur bedenkt een (tijdelijke) oplossing om de productie weer te kunnen laten draaien. Maar door de bedrijfscultuur, of wanneer de druk weer van de ketel is, vergeet men de aanpassing te documenteren. De tijdelijke oplossing om alles weer draaiende te krijgen, wordt vergeten en zit wellicht over tien jaar nog steeds in het systeem. Wat er op tekening staat, gebeurt niet altijd in het netwerk en daar sluipt het gevaar.' ◁