ABN·AMRO

Ondernemers onderschatten het risico op cybercriminaliteit

Bedrijfssectoren kampen elk met eigen risico's

Juni 2021

Inhoudsopgave

Inleiding:
Cybercriminaliteit raakt bedrijven in het hart 3

1. Meer ketenaanvallen, datalekken en gijzelsoftware 6

2. Risico's tussen sectoren lopen uiteen 8

Sectorale inzichten 10

3. TMT: professioneel, maar toch gevoelig 11

4. Logistiek: communicatie tussen bedrijven achilleshiel 14

5. Industrie: steeds vaker doelwit 17

6. Zorg: patiëntgegevens kwetsbaar 20

7. Retail: data consumenten gewild 23

8. Leisure: digitaal contact met gasten risicovol 25

9. Advocaten en accountants: datalek meest gevreesd 27

Ondersteuning door ABN AMRO 29

Colofon 30

Inleiding:
Cybercriminaliteit raakt bedrijven in het hart

De kosten van cyberaanvallen zijn vorig jaar geëxplodeerd. Vooral sectoren die sterk inzetten op digitale dataverwerking en communicatie, zoals de industrie, de retail en de zorg, blijken kwetsbaar. Diefstal van data, het gijzelen van systemen en misleiding op basis van het aannemen van een valse identiteit nemen hals over kop toe. Ondanks deze toegenomen dreiging blijft de risicoperceptie van cybercriminaliteit onder ondernemers laag.

Wie medio april een kaasje wilde kopen bij de Albert Heijn moest goed zoeken. Gijzelsoftware bij de logistieke leverancier zorgde voor lege schappen in de kaasafdeling. Door de hack waren leveringen uit de magazijnen niet mogelijk. Orders werden niet ontvangen, producten waren onvindbaar in de enorme magazijnen en transportplanning werd zodoende onmogelijk. Deze aanval staat niet op zichzelf. Het aantal cybercrimezaken is volgens het Openbaar Ministerie in 2020 meer dan verdubbeld. In het eerste kwartaal van 2021 zag de politie een verdubbeling van het aantal geregistreerde digitale misdrijven ten opzichte van het jaar ervoor. Vooral oplichting via WhatsApp, spoofing[1] en fraude in de onlinehandel springen er volgens Politie Nederland uit. Ook is de financiële schade het afgelopen jaar substantieel toegenomen. In Nederland lagen de mediane kosten in 2020 voor een cyberaanval op 74.000 euro. In 2019 was dit nog 12.000[2] euro.

De coronacrisis heeft deze toename versterkt. Steeds meer winkeliers hebben door toedoen van de lockdowns gekozen voor onlineafzetkanalen. Ook vergroot het intensiever gebruik van digitale communicatie in het werk, zorg en onderwijs het aanvalsoppervlak voor cybercriminelen.

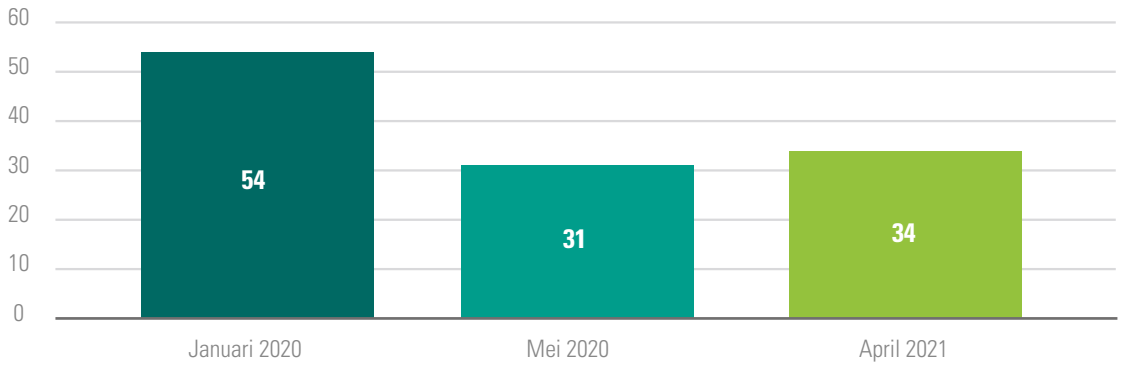
Intensievere digitale communicatie beklijft, ook als de pandemie is geluwd. Ook zal een deel van de consumenten niet terugkeren naar de fysieke winkelstraat. Uit onderzoek van ABN AMRO uit december van vorig jaar blijkt dat pers saldo 28 procent van de consumenten van plan is om minder vaak naar een fysieke winkel te gaan. Blijkbaar vinden consumenten winkels steeds minder essentieel en biedt internet een goed alternatief. Voor thuiswerkers geldt dat bijna een kwart van hen ook na de coronacrisis grotendeels thuis wil blijven werken. Dit blijkt uit onderzoek van TNO, gehouden in februari van dit jaar. Deze gedragsveranderingen hebben tot gevolg dat het aanvalsoppervlak voor cybercriminelen structureel groter wordt.

1 Spoofing is het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Dit kan bijvoorbeeld gaan om een e-mail, website, IP-adres, telefoonnummer en biometrische kenmerken.
2 Hiscox, cyber readyness report 2020

Risicoperceptie nog steeds lager dan voor corona

Ondanks de toegenomen dreiging schatten ondernemers het risico op cybercriminaliteit lager in dan voor de uitbraak van de coronacrisis. ABN AMRO heeft in samenwerking met onderzoeksbureau MWM2 168 ondernemers op drie momenten in de tijd gevraagd in welke mate zij cybercriminaliteit als een risico voor het eigen bedrijf zien: vlak voor de uitbraak van de coronacrisis, in mei vorig jaar en in april van dit jaar. In mei vorig jaar was de terugval in de risicoperceptie het grootst. Mogelijke verklaring hiervoor is dat ondernemers destijds, vlak na de uitbraak van corona, meer urgente problemen aan hun hoofd hadden dan cybercriminaliteit. De bedrijfscontinuïteit en zorgen om het personeel kregen bij veel ondernemingen de hoogste prioriteit.

In welke mate zien bedrijven cybercriminaliteit als veel of heel erg veel risico voor de eigen organisatie? (%)



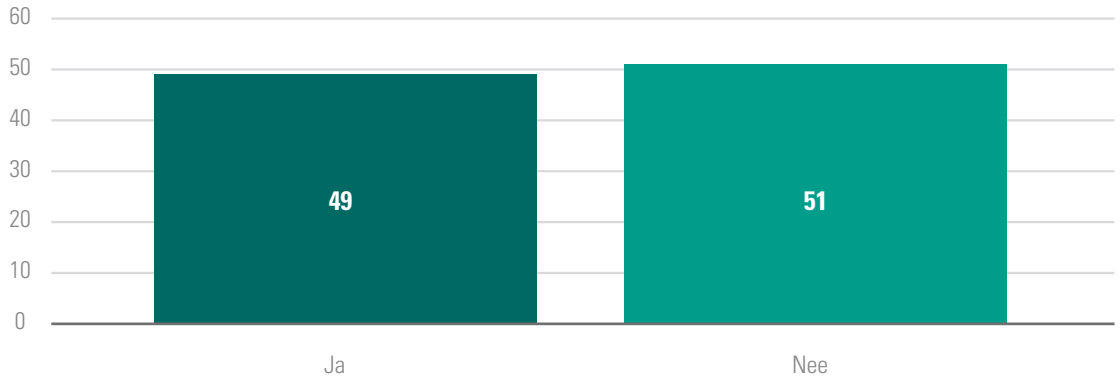
Bron: ABN AMRO

Een jaar later is het bewustzijn van ondernemers nauwelijks toegenomen. In april van dit jaar zag slechts 34 procent cybercriminaliteit als een groot risico voor de eigen organisatie. Een zeer beperkte en niet significante stijging ten opzichte van de meting van bijna een jaar eerder, toen dit percentage op 31 procent lag. De risico-perceptie is daarmee nog lang niet teruggeveerd naar het niveau van voor de uitbraak van de coronacrisis, toen nog meer dan de helft van de ondervraagden het risico op cybercriminaliteit voor de eigen organisatie als hoog inschatte. Dat is zorgelijk omdat het risico op cybercriminaliteit, zoals eerder aangegeven, juist structureel toeneemt.

Bedrijven beloven beterschap

Hoewel de risicoperceptie nog niet is teruggeveerd naar het niveau van voor de coronacrisis, is het goede nieuws dat bijna de helft van de door ABN AMRO ondervraagde ondernemingen van plan is om extra maatregelen te nemen op het gebied van cybercriminaliteit. Gevraagd naar het type maatregelen dat ondernemers van plan zijn te nemen, zegt het merendeel te willen inzetten op preventieve maatregelen. Het afsluiten van een verzekering tegen cybercriminaliteit is daarentegen een stuk minder populair.

Bent u van plan de komende tijd extra maatregelen te treffen tegen cybercriminaliteit? (%)



Bron: ABN AMRO

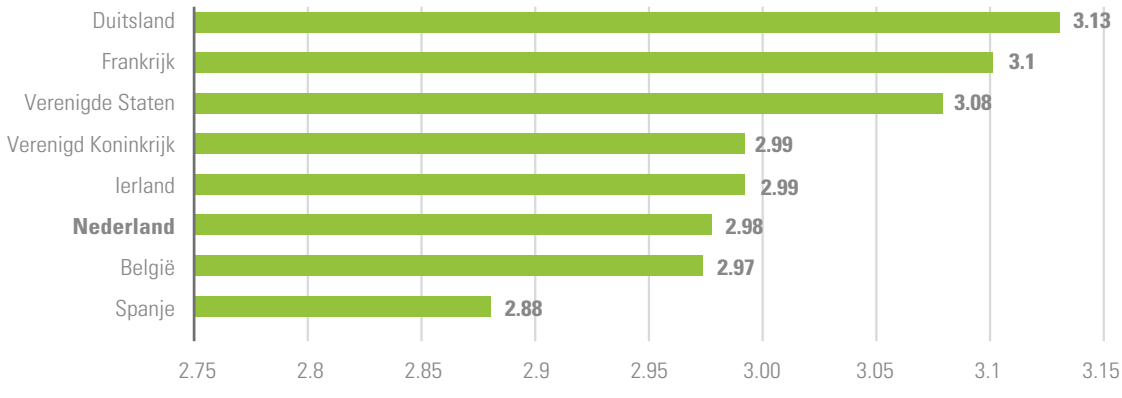
Nederlands bedrijfsleven in middenmoot

Wat betreft 'cyberweerbaarheid' behoort het Nederlandse bedrijfsleven in vergelijking met andere westerse landen slechts tot de middenmoot. Digitale criminaliteitsverzekeraar Hiscox berekende de gemiddelde scores per land op basis van verschillende variabelen, waaronder de manier waarop bedrijven toegang tot digitale diensten regelen en cyberdreigingen in beeld brengen.

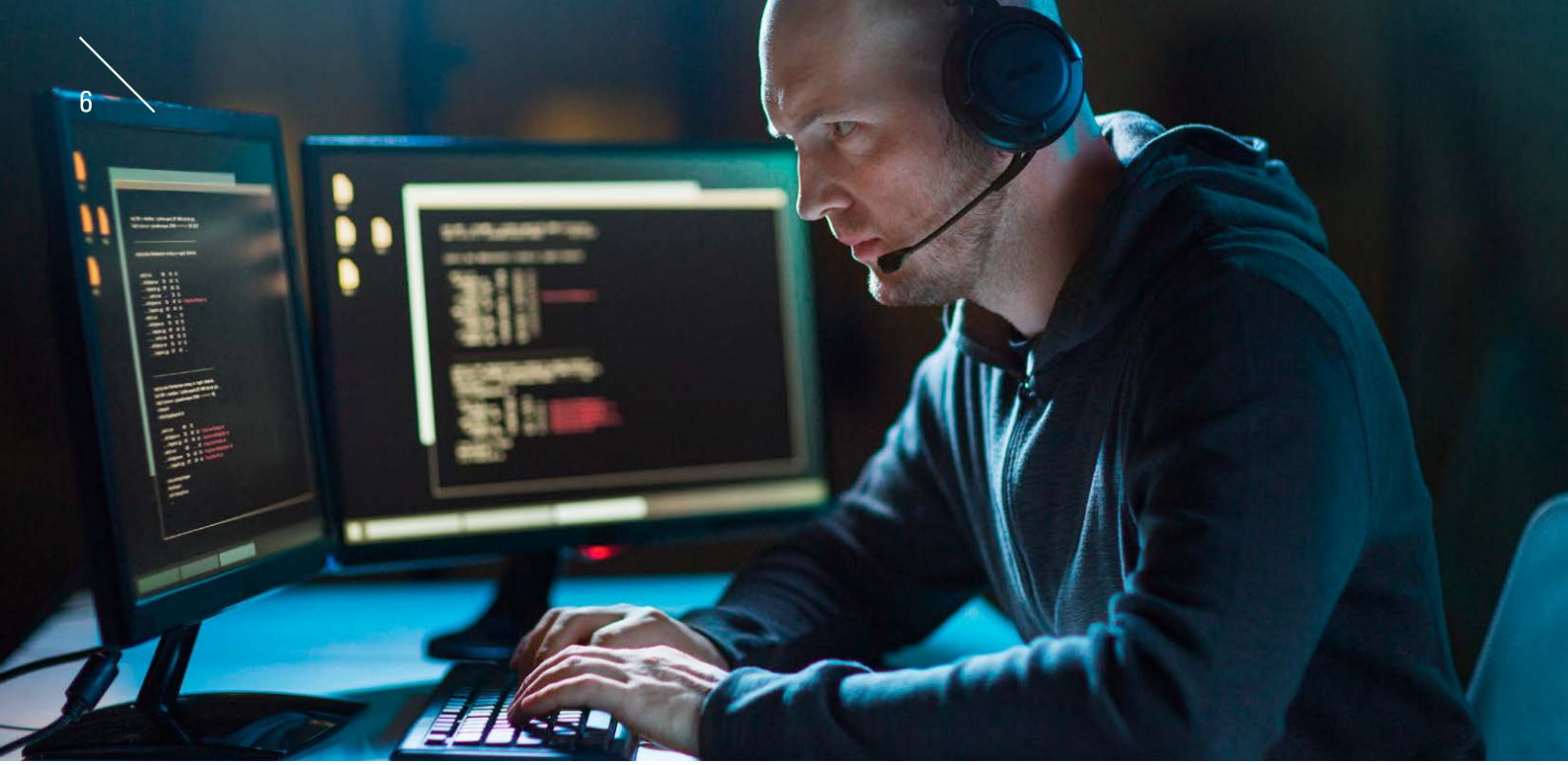
Opvallend is het relatief lage percentage Nederlandse bedrijven dat op het gebied van cyberveiligheid als 'expert' kan worden aangemerkt: slechts 12 procent. Bedrijven in de 'expert'-categorie nemen uitgebreide maatregelen in meerdere domeinen, en hebben hiervoor niet alleen de technische oplossingen in huis, maar ook de benodigde processen en betrokkenheid vanuit werknemers. Hiermee blijft ons land ver achter op koplopers Verenigde Staten en Ierland; in beide landen wordt 24 procent van de bedrijven als cyber-expert gekwalificeerd.

Voor alle landen geldt dat de cyberparaatheid bij grote bedrijven groter is dan bij kleinere, zo blijkt uit ditzelfde rapport. Grote bedrijven vormen een aantrekkelijk doelwit, waardoor zij extra genoodzaakt zijn passende maatregelen te treffen. Daarnaast kunnen ze meer (financiële) middelen inzetten in de strijd tegen cybercriminaliteit.

Gemiddelde score cyberweerbaarheid per land (%)



Bron: Hiscox 2021



1. Meer ketenaanvallen, datalekken en gijzelsoftware

Niet alleen zijn er het afgelopen jaar meer aanvallen geweest ten opzichte van eerdere jaren, de aanvallen zijn ook anders van aard. Gijzelsoftware, valse identiteiten en binnendringen via een ander bedrijf, criminelen zijn van alle markten thuis.

Zo is er een enorme toename aan supply chain-aanvallen. Een supply chain-aanval betekent dat een bedrijf wordt aangevallen via een ander bedrijf in de keten. Als aanvallers een goed beveiligd bedrijf willen aanvallen, kunnen ze voor de makkelijke weg kiezen en een minder goed beveiligd bedrijf aanvallen dat een relatie heeft met het doelwit. Dit hoeft niet altijd een gerichte aanval te zijn. Door een veelgebruikt softwareprogramma te infecteren met kwaadaardige software kan elk bedrijf dat het programma gebruikt, worden besmet. Een supply chain-aanval kan uiteraard ook gericht zijn, waarbij een leverancier of klant wordt gehackt om via een netwerkverbinding of een e-mail binnen te komen bij het doelwit.

Type cybercrime	Doel
DDos-aanval	Schade aanrichten
Malware - virus	Schade aanrichten
Malware - ransomware	Afpersing (geld)
Hacken	Stelen informatie

Hackers richtten zich het afgelopen jaar steeds vaker op het stelen van persoonsgegevens, blijkt uit de explosieve toename van het aantal geregistreerde hacks door de Autoriteit Persoonsgegevens. Met deze persoonsgegevens kunnen criminelen steeds gerichter phishen[3] of de gestolen data te koop aanbieden. In maart van dit jaar zijn bijvoorbeeld de privéadressen en telefoonnummers van miljoenen Nederlanders gestolen bij een bedrijf dat ICT-diensten aan autogarages aanbiedt. De gegevens zijn vervolgens op een hackersforum te koop aangeboden.

"We zien bovendien steeds meer ransomware-aanvallen, ook wel gijzelsoftware genoemd", aldus Lalit Bhakuni, hoofd Global Cyber Intelligence Center bij ABN AMRO. "Het risico speelt in alle sectoren, maar is het afgelopen jaar met name in de zorg toegenomen. De toenemende digitalisering en het grote maatschappelijke belang van de zorg maakt de sector kwetsbaar." Bij zo'n gijzeling worden computers of hele systemen van buiten op slot gezet en pas weer vrijgegeven na het betalen van losgeld.

Mondiaal gezien is gijzelsoftware dan ook de meest populaire vorm van cybercriminaliteit. Volgens onderzoek van ICT-reus IBM verliep 23 procent van de cyberaanvallen in 2020 via gijzelsoftware.[4] Wereldwijd kwam dit neer op een zevenvoudige toename ten opzichte van het jaar ervoor.[5] Schattingen van het aantal Nederlandse bedrijven dat in 2020 slachtoffer werd van gijzelsoftware lopen overigens uiteen. Waar Hiscox[6] een percentage van 16 noemt, stelt cyberbeveiliger Mimecast[7] dit percentage vast op 53.

Opvallend is dat de meest succesvolle gijzelsoftwaregroepen die IBM het afgelopen jaar observeerde, werkten via zogenoemde 'Ransomware-as-a-Service'-bendes. Deze bendes hebben zelf niet de kwaliteiten in huis om softwarecodes te schrijven en een eigen aanval op te zetten en kopen daarom hackersdiensten in via forums op het 'dark web'. De ontwikkelaar die de gijzelsoftware in eerste instantie bouwde, ontvangt een deel van de winst die aanvallers ophalen. Ook kan er zelfs een professionele helpdesk 'ingekocht' worden om slachtoffers te helpen met de betaling.

3 Bij een phishing-aanval worden mensen met valse berichten naar een dergelijke nepwebsite gelokt om hen geld te laten over maken, hun inloggegevens te stelen of om malware te installeren.
4 IBM Screenforce-X 2020
5 ZDNet. "Ransomware: Huge Rise in Attacks This Year as Cyber Criminals Hunt Bigger Pay Days," https://www.zdnet.com/article/ransomware-huge-rise-in-attacks-this-year-as-cyber-criminals-hunt-bigger-pay-days/. September 9, 2020.
6 Hiscox cyber readyness report 2021
7 State of Email Security 2021

2. Risico's tussen sectoren lopen uiteen

Het karakter van cyberaanvallen verschilt per sector. De industrie communiceert intensief over technische gegevens, in de leisure kunnen hotelgasten interessante data voor criminelen opleveren.

Elk jaar identificeert IBM X-Force de mondiale top 10 van meest aangevallen industrieën en rangschikt deze vervolgens tot een zeker percentage aanvallen. Volgens IBM is de financiële- en verzekeringssector al jarenlang de meest aangevallen bedrijfstak. Cybercriminaliteit is immers vaak financieel gemotiveerd. Bovendien werkt deze sector met veel bedrijfsgevoelige informatie, wat het lekken van informatie over derden tot een risico maakt.

Sector	Mondiale top tien sectoren 2020 (% aanvalsvolume van top tien sectoren)	Top drie type cyberaanvallen per sector
Financiële dienstverlening	1 (23%)	1. Ongeautoriseerde servertoegang 2. Datadiefstal 3. Gijzelsoftware
Industrie	2 (17,7%)	1. Gijzelsoftware 2. Datadiefstal 3. Aanvallen op bedrijfscorrespondentie (BEC)
Energie	3 (11,1%)	1. Datadiefstal 2. Overige type aanvallen 3. Aanvallen op bedrijfscorrespondentie (BEC)
Retail	4 (10,2%)	1. Inloggegevens diefstal 2. Gijzelsoftware 3. Ongeautoriseerde servertoegang
Professionele dienstverlening	5 (8,7%)	1. Gijzelsoftware 2. Datadiefstal 3. Ongeautoriseerde servertoegang
Overheid	6 (7,9%)	1. Gijzelsoftware 2. Datadiefstal 3. Overige type aanvallen
Zorg	7 (6,6%)	1. Gijzelsoftware 2. Ongeautoriseerde servertoegang 3. Inloggegevens diefstal
TMT	8 (5,7%)	1. Verkeerde (standaard) configuraties[8] (50%) 2. Overig (50%)
Transport en logistiek	9 (5,1%)	1. Gijzelsoftware 2. Ongeautoriseerde servertoegang
Onderwijs	10 (4,0%)	1. Overige type aanvallen 2. Inloggegevens diefstal 3. Gijzelsoftware

Bron IBM X-Force 2020

8 Wanneer beveiligingsinstellingen niet zijn gedefinieerd en enkel de standaardwaarden worden gehanteerd kan dit leiden tot misconfiguratie. De configuratie-instellingen voldoen dan niet aan de beveiligingsnormen.

Opvallend is dat de positie van de verschillende andere bedrijfstakken aanzienlijk is veranderd vorig jaar. Zo steeg de sector industrie in 2020 van de achtste naar de tweede plaats. In de industrie neemt de digitale communicatie tussen machines, producten, toeleveranciers en gebruikers snel toe, wat de sector een interessant doelwit maakt. Bovendien kent de Nederlandse industrie een aantal innovatie koplopers wiens bedrijfsgeheimen veel waard zijn.

De gezondheidszorg kampte in 2020 eveneens met meer cybercriminaliteit en steeg van plaats tien naar zeven. De coronapandemie heeft de digitalisering van de zorg in een stroomversnelling gebracht, maar heeft de sector daardoor ook kwetsbaarder gemaakt voor cybercriminelen. Op de transportsector zijn vorig jaar minder aanvallen gericht in vergelijking met 2019; een daling van plek drie naar negen. Mogelijk is dit een gevolg van een tijdelijk verminderde vraag naar transport tijdens de pandemie.

Het aanvalsvolume zegt niet alles. Zo is het aantal aanvallen op de energiesector met 11 procent nog vrij beperkt, maar is de impact van een aanval enorm. Zo heeft de regering in de Verenigde Staten recent de noodtoestand uitgeroepen omdat de energievoorziening aan de oostkust op het spel stond als gevolg van een cyberaanval op oliepijpleidingen.

Meer sectorale inzichten zijn in onderstaande verdiepingspagina's te lezen. Hierin wordt onder meer ingegaan op de grootste risico's binnen verschillende sectoren en hoe ondernemers hiermee om gaan. Achtereen volgens worden behandeld de volgende sectoren: Technologie, Media en Telecom (TMT), transport en logistiek, industrie, zorg, retail, leisure en professionele dienstverlening.

Tips

Een succesvolle aanpak vraagt om meer dan alleen technologische investeringen. Het is immers alom bekend dat gedrag van medewerkers een cruciale rol speelt in het voorkomen van cyberincidenten. Training van medewerkers in het herkennen van risicovolle situaties is daarom cruciaal. Dit kan gaan om het herkennen en melden van phishing e-mails, het gebruik van onlinediensten of verzoeken om het installeren of opwaarderen van software.

Iedere organisatie is een mogelijk slachtoffer van cybercriminelen, ongeacht de sector en hoe groot of klein de organisatie ook is. Wel kunnen de risico's verkleind worden, evenals de impact van een aanval. Deze tips helpen ondernemers op weg.

- Houd software up-to-date, installeer nieuwe versies tijdig en verwijder software die niet meer wordt gebruikt.
- Geef medewerkers alleen de rechten die nodig zijn voor de uitvoering van het werk en wees terughoudend met privileges.
- Bereid de onderneming voor op een aanval door middel van een cyber response-plan. Dit plan geeft een opsomming van acties die het bedrijf helpen om voorbereid te zijn op incidenten als gevolg van cybercriminaliteit.
- Laat regelmatig een veiligheidstest op het informatiesysteem uitvoeren. Een dergelijke test geeft waardevolle informatie over de beveiliging van informatiesystemen. Met de uitkomsten kunnen gerichte maatregelen genomen worden om kwetsbaarheden te verhelpen.

Cyber Veilig & Zeker

Cyber Veilig & Zeker is een complete cybersecurity-oplossing van ABN AMRO die het risico op een cyberincident verlaagt.

VOORKOMEN

Met innovatieve technologie, complementair aan uw huidige IT, worden incidenten voorkomen. De meest actuele dreigingen ziet u real time in uw dashboard.

VERSTERKEN

We stellen eerst het dreigingsprofiel van uw bedrijf op. Op basis daarvan krijgt u advies op maat.

VERHELPEN

Krijgt u toch te maken met een cyberincident? Dan staan onze cyberexperts 24/7 voor u klaar om de schade te beperken.

VERGOEDEN

Met onze complete cyberverzekering zijn de kosten voor aansprakelijkheid, herstelwerkzaamheden en vervangen apparaten gedekt. Ook margeverlies is meeverzekerd.

Kijk voor meer informatie over Cyber Veilig & Zeker op abnamro.nl/cyber

Sectorale inzichten

3. TMT: professioneel, maar toch gevoelig

Bedrijven uit de sector TMT zouden bij uitstek moeten weten hoe ze zich moeten beveiligen. Juist hun centrale rol binnen de digitalisering maakt deze bedrijven echter kwetsbaar. Telecommunicatie en software vormen de zwakke schakels.

In 2020 kreeg ruim de helft van de bedrijven in de technologie-, media- en telecom (TMT) wereldwijd te maken met een cyberaanval, concludeert cyberverzekeraar Hiscox. Een jaar eerder was dit nog 44 procent. Enkel in de financiële dienstverlening en de energiesector werden gelijksoortige cijfers gerapporteerd. De sector is echter niet machteloos; volgens Hiscox heeft de TMT-sector het grootste aandeel bedrijven dat zeer sterk scoort op professionaliteit in cybersecurity. Dat betekent dat ondernemers uitgebreide maatregelen treffen en hiervoor niet alleen de technische oplossingen in huis hebben, maar ook de benodigde processen en betrokkenheid van werknemers.

IT- en telecombedrijven vormen een essentiële schakel in de operatie van vrijwel elk bedrijf. Cybercriminelen kunnen door een ingreep op infrastructureel- of softwareniveau dan ook grote schade toebrengen aan organisaties. “De risico’s zijn niet beperkt tot datalekken alleen”, zegt Brian Vermeer van Snyk, een bedrijf dat oplossingen ontwikkelt voor softwareontwikkelaars om hun product veiliger te maken. “Als de servers van een bedrijf worden platgelegd, zijn hun diensten vaak ook niet meer beschikbaar. Daarmee verliezen ze klanten.”

Digitale infrastructuur

De telecommunicatiesector vormt een deel van de vitale infrastructuur van Nederland. Dat maakt de sector kwetsbaar voor staatsspionage. Zo probeerden Chinese hackers via een phishing-campagne gericht op 23 telecomoperators verspreid over de hele wereld in 2020 toegang te krijgen tot gevoelige of geheime informatie met betrekking tot 5G-technologie.[9] De uitrol van het 5G-netwerk biedt kwaadwillende figuren daarnaast nieuwe

9 ZDNet, ‘Hackers are targeting telecom companies to steal 5G secrets’, maart 2021

mogelijkheden tot netwerkinfiltratie. Veiligheidsexperts hebben zorgen geuit over de 5G-technologie van de Chinese gigant Huawei vanwege mogelijke staatsspionage die via dit netwerk kan worden uitgevoerd. Zweden en het Verenigd Koninkrijk hebben om deze reden besloten de 5G-technologie van Huawei te weren.[10] In Nederland verdwijnt Huawei eveneens uit de kern van het telecomnetwerk, blijkt uit recent verschenen stukken uit het FD.[11]

Een indirect veiligheidsrisico van 5G is het feit dat het snelle netwerk zeer geschikt is om slimme apparaten onderling te verbinden. Helaas is de beveiliging van veel van deze 'Internet of Things'-apparaten (IoT) ondermaats, wat cybercriminelen een keur aan startpunten biedt om bredere netwerken te infiltreren.

Naast telecommunicatienetwerken vormen ook datacenters een essentieel onderdeel van de ICT-infrastructuur. Zij bieden de ruimte, koeling en stroomvoorziening die nodig is om computerservers te laten draaien. Wordt schade toegebracht aan deze 'levensader', dan kunnen de systemen van bedrijven volledig plat komen te liggen.

Clouddienstverleners

De clouddienstverleners die actief zijn in deze datacenters vormen een aantrekkelijk doelwit omdat deze grote hoeveelheden data van zowel organisaties als individuen herbergen. Doordat veel bedrijven gedurende de pandemie hun IT-activiteiten of delen daarvan versneld overhevelden naar de cloud, is het totale doelwit daarnaast groter geworden. Een analyse van computer- en netwerkbeveiliger McAfee laat zien dat het aantal aanvallen op clouddiensten gedurende de eerste vier maanden van 2020 toenam met maar liefst 630 procent.[12]

Vaak wordt de initiële toegang tot deze cloudsystemen verkregen via de menselijke weg. In 2016 wisten hackers onder de campagnenaam 'Operation Cloud Hopper' gevoelige informatie van grote bedrijven uit een tal van sectoren te verkrijgen. Dit gebeurde middels 'spear phishing'. Medewerkers van clouddienstverleners kregen een e-mail waarin ze werden verleid om schadelijke software te downloaden of hun wachtwoorden te delen. Via de systemen van het cloudbedrijf konden de daders vervolgens ook toegang krijgen tot de systemen van verschillende klanten.

Waar de clouddienstverlener met alertheid op phishing in ieder geval één sleutel in handen heeft voor een betere bescherming tegen dergelijke aanvallen, is ook onder de afnemers van clouddiensten alertheid geboden. Onderzoekers ontdekten dat maar liefst 91 procent van de bedrijfsomgevingen in de cloud een 'beveiligingsgat' had, veroorzaakt door gebrekkige instellingen door de klant zelf.[13] Cloudbedrijven doen er dus goed aan om proactief het gesprek over cyberveiligheid met hun klanten aan te gaan.

10 Reuters, 'Swedish court to hear Huawei's case against 5G ban', april 2021
11 https://fd.nl/ondernemen/1384291/huawei-verdwijnt-uit-de-kern-van-nederlandse-telecomnetwerken-jue1caqGVEmk, mei 2021
12 McAfee, 'Cloud Adoption and Risk Report: Work from Home Edition', mei 2020
13 SC Magazine, 'Misconfigured servers contributed to more than 200cloud breaches', augustus 2020

Softwarebedrijven

Ook kwetsbaarheden in software worden regelmatig benut door cybercriminelen. Zo kreeg softwareontwikkelaar SolarWinds in 2020 te maken met een grootschalige hack van Orion, software die onder andere de beschikbaarheid van servers monitort. Via deze hack hadden spionnen – Russische, volgens experts – lange tijd toegang tot geheime informatie van 'Fortune 500'-bedrijven en Amerikaanse overheidsinstanties. Ook tal van Nederlandse bedrijven gebruiken de software van SolarWinds.

De prominente rol van software in de waardeketen van bedrijven brengt een grote verantwoordelijkheid met zich mee. Een recente casestudie onder drie grote softwareontwikkelaars liet echter een alarmerend beeld zien wat betreft prioriteiten. Besluitvormers binnen deze bedrijven achtten functionaliteit en 'time-to-market' van de software stelselmatig het belangrijkst, terwijl veiligheid van het product als secundair werd gezien.[14] De veronderstelling hierachter was dat klanten niet bereid waren om extra te betalen voor een veilige oplossing.

Dit beeld herkent ook Vermeer van Snyk. "Cybersecurity is onzichtbaar en de waarde ervan lastig meetbaar. Dat maakt het lastig voor softwarebedrijven om te bepalen hoeveel ze in veiligheid investeren en zouden moeten investeren." Toch wordt de businesscase voor cyberveiligheid steeds meer evident. Zo zien de onderzoekers achter bovengenoemde casestudie dat klanten in de hoek van kritieke infrastructuur, defensie en financiële dienstverlening veiligheid als centraal selectiecriterium aanhouden. Daarnaast wordt de verantwoordelijkheid voor cyberincidenten steeds vaker contractueel bij de IT-leverancier gelegd.

Aan softwarebedrijven dus de taak om zicht te houden op het 'cyberbewustzijn' van hun beslissers en ontwikkelaars. Qua personeelsbeleid is dit een uitdaging, want Nederland heeft een groot gebrek aan cybersecurityspecialisten, mede doordat deze ook in het buitenland makkelijk een baan kunnen vinden. In 2018 luidde de Cyber Security Raad, een adviesorgaan van het kabinet, hier al de noodklok over.[15] De huidige IT-opleidingen bieden vooralsnog geen soelaas, ziet Vermeer van Snyk. "In een opleiding tot softwareontwikkelaar leer je gewoon om te bouwen. Beveiligingsproblemen en -oplossingen krijgen weinig aandacht in het curriculum."

Wapenen

Het intrinsiek digitale karakter van veel TMT-producten en diensten maakt cybersecurity een uitdagend probleem. Een goede wapening tegen de gevaren is dan ook van cruciaal belang. Mats Ros, compliance officer van IT-dienstverlener ilionx, raadt zijn branchegenoten aan om een Security Health Check te doen. "Door je niveau van informatiebeveiliging inzichtelijk te maken, weet je waar de risico's liggen. Met die kennis op zak kan elk bedrijf kiezen voor een passend beschermingsniveau, hoe klein of groot je ook bent", aldus Ros. Het gaat hiermee niet simpelweg om investeringen in cybersecurity, maar ook om het in huis halen van de juiste kennis en expertise om cybercrime te herkennen, data goed te beveiligen en te herstellen bij schade.

14 Harvard Business Review, 'Is Third-Party Software Leaving You Vulnerable to Cyberattacks?', mei 2021
15 FD, 'Noodklok over Nederlandse braindrain bij cybersecurity', april 2018

4. Logistiek: communicatie tussen bedrijven achilleshiel

Het toenemend gebruik van digitale middelen binnen en vooral tussen logistieke bedrijven maakt de sector kwetsbaar. Criminelen is het vooral om informatie over waardevolle goederenstromen te doen, zoals ruim 40 procent van de logistieke ondernemingen inmiddels heeft ervaren.

Digitale dataverwerking en communicatie zijn onmisbaar voor logistieke bedrijven en hun opdrachtgevers om logistieke processen te organiseren en te sturen. De transportmiddelen zelf zijn door digitalisering en technologische innovatie onherkenbaar veranderd. Moderne schepen zijn welhaast varende computers die in nauw contact staan met tal van externe netwerken. Hetzelfde geldt voor trucks die hun routes rijden op basis van externe planningsystemen. De te verwachten exponentiële groei van robotisering in magazijnen biedt eveneens impuls aan de groei van de digitale infrastructuur.

Keerzijde is dat criminaliteit in de sector transport en logistiek zich verplaatst van de fysieke naar de digitale wereld. Logistieke bedrijven zijn bij uitstek interessant omdat ze zich bezighouden met waardevolle goederenstromen die bovendien binnen een hele keten van bedrijven worden verplaatst. Ruim 40 procent van alle Nederlandse bedrijven in de logistieke sector heeft al eens te maken gehad met een vorm van cybercriminaliteit of hacking. Volgens Consultancy.nl behoort de logistieke sector tot de top van cybergevoelige sectoren. Riskmethod stelt dat het percentage cyberaanvallen zal stijgen door verdergaande digitalisering tussen bedrijven binnen de keten en meer gebruik van de thuiswerkplek, die relatief onveilig is.

De sector is zich hiervan bewust en zet stappen in de goede richting, zo blijkt uit recent onderzoek van Transport en Logistiek Nederland. Hieruit blijkt een toenemend bewustzijn onder medewerkers die met crisisplannen worden voorbereid in het geval van een aanval. Die ontwikkeling is noodzakelijk, aangezien uit hetzelfde onderzoek blijkt dat bij 20 procent van de bedrijven de processen tijdelijk werden verstoord vanwege een cyberincident.

Bewustwording

Bij Van den Bosch, gespecialiseerd in bulktransport, is cybersecurity altijd een belangrijk thema geweest bij de ICT-afdeling. Dick Schouten is teamleider infrastructuur en verantwoordelijk voor dit thema. “We willen het bewustzijn van alle medewerkers binnen ons bedrijf vergroten. Omdat cybersecurity steeds meer aan belang wint, zijn we eind vorig jaar begonnen meer bewustzijn te creëren. Zo krijgen nu alle medewerkers regelmatig een training of extra informatie over IT-veiligheid. Daarin leggen we uit dat je niet overal op moet klikken en niet alle bijlages moet openen zonder hier kritisch naar te kijken. Vertrouw je het niet of denk je het is niet voor mij, stuur het dan altijd naar de IT-servicedesk.”

Een andere manier om criminelen buiten de deur te houden is door goed af te bakenen wie bij welke data kan. “Als logistiek dienstverlener hebben we te maken met veel verschillende partijen en afdelingen. Niet iedereen hoeft toegang te hebben tot alle data”, zegt Schouten. Ook wordt toegang tot bedrijfssystemen vanuit sommige regio’s beperkt. “Ik heb bijvoorbeeld wel eens klachten gekregen over het niet mogen inloggen op een laptop vanuit Rusland. Maar dat doen we natuurlijk niet voor niks.”

Verder krijgt Van den Bosch van klanten steeds meer vragen over hoe het zit met databeveiliging. “Wij zijn blij dat de klant hier actief mee bezig is. Naast dat wij er voor zorgen dat cybersecurity binnen Van den Bosch op orde is, willen wij dit thema ook bespreken en adviezen delen met onze klanten. Dat geeft hen het vertrouwen dat wij ook op dit gebied een betrouwbare partner zijn.”

Twee tips die Schouten wil meegeven: “neem je medewerkers mee op het gebied van cybersecurity en leg uit hoe bepaalde zaken in elkaar steken. En houd bestaande procedures regelmatig tegen het licht.”

Boardroom

Bij Jan de Rijk Logistics is cybersecurity een actueel thema, vertelt ICT-directeur Heino Kempers. “Het is een onderwerp geworden in de boardroom, waar dat in het verleden niet zo was. Waar je vroeger moest zenden als het ging over IT-onderwerpen, is het nu een interactie geworden en wordt de discussie zelfs geïnitieerd vanuit de boardroom. Ik vind dat een heel gezonde ontwikkeling. Wanneer er in de media berichten zijn over lekken in bepaalde software krijg bijvoorbeeld ik berichten van de Raad van Commissarissen of medewerkers, wat aangeeft dat het speelt binnen alle lagen van de organisatie.”

Om ervoor te zorgen dat Jan de Rijk kort op de bal zit als het gaat om cybersecurity hanteert het logistieke bedrijf een aantal methodes. Zo wordt al het personeel bewust gemaakt van de gevaren door middel van trainingen en wordt hun kennis getest. Tevens houden medewerkers van de IT-afdeling nieuws en ontwikkelingen in de gaten. “We laten verder ons netwerkt geregeld testen. Dan wordt door experts gekeken of er bepaalde lekken zijn die we gemist hebben en die we moeten dichten.”

Bij Jan de Rijk werkt de IT-afdeling volgens ISO 27001. Het concern heeft dit keurmerk nog niet, maar voldoet er al wel aan. “De reden waarom we dit keurmerk willen, is ook om extern duidelijk te kunnen maken dat we de zaken voor elkaar hebben. Het is nu al goed geregeld, maar we willen daar steeds beter in worden.” Volgens Kempers neemt het bewustzijn over cybersecurity in de transportsector toe. “Je ziet dat er gemeenschappen door grotere organisaties in het leven worden geroepen om kleine partijen te helpen. Als je in de keten zit, heb je elkaar nodig. Uiteindelijk moet dit niet een onderwerp zijn waarop je elkaar beconcurreert.”

Kennis

Hélène Minderman, expert security in de logistieke sector, ziet vooruitgang als het gaat om bewustwording van cybersecurity bij transportbedrijven. Toch is dat nog niet genoeg. “Kennis en concrete aanpak zijn nodig om in control te zijn, ook op dit thema. Vaak is het onderwerp aan het takenpakket van de IT-manager toegevoegd of wordt het uitbesteed aan een leverancier. Intern heeft men dan niet de noodzakelijke kennis en aandacht. Als je je fysieke hang- en sluitwerk op orde hebt, maar het digitale niet, dan loop je in dit digitale tijdperk flinke risico’s.”

Actie wordt vaak pas ondernomen na een incident en zelfs dan houden ondernemingen soms de boot nog af om zich er echt in te verdiepen, vertelt Minderman. “Ondernemingen denken ook dat wanneer gegevens worden gegijzeld en er simpelweg betaald wordt, de onderneming weer verder kan gaan. Maar zo gaat het natuurlijk niet. We hebben een incident gehad bij een middelgroot bedrijf dat had betaald en twee dagen later weer werd geraakt.” Na een aanval ontstaat een acute behoefte aan een plan van aanpak, legt ze uit. “De oplossing is dan: ‘het is tijd om specialisten in te schakelen’.”

Minderman vraagt om attentie bij middelgrote en kleine bedrijven. “De grote bedrijven hebben meer capaciteit, daar is het thema breder geborgd in de organisatie. Middelgrote spelers hebben moeite dit zelf op een serieuze wijze te organiseren of hebben hun lot in handen gelegd van hun IT-leverancier. Zij vertrouwen erop dat die leverancier ‘de cyberrisico’s heeft afgedekt terwijl dat niet is terug te lezen in de service level agreements.” De beleidsadviseur legt verder uit dat kleine bedrijven soms onterecht denken dat hackers alleen geïnteresseerd zijn in waardevolle lading. Maar zij zijn juist ook geïnteresseerd in informatie, zoals bijvoorbeeld bankrekeningnummers en persoonsgegevens. Dat kleinere transporteurs onderdeel zijn van de keten maakt ze interessant en dus kwetsbaar. “Neem datalekken. Ook kleinere bedrijven hebben de contactgegevens van de planner of directeur bij een ander bedrijf.”

Minderman verwacht dat partijen in de keten steeds meer eisen gaan stellen aan de IT-veiligheid bij de leverancier. Ook vanuit Europa komen meer richtlijnen om de eisen aan IT-veiligheid te reguleren. Dit zal de urgentie om cybersecurity goed op orde te hebben bij ondernemingen verhogen, zeker wanneer de opdrachtgever er eisen aan stelt. Voor ondernemingen kan de aanpak van cybersecurity daarmee toegevoegde waarde bieden. “Laat maar zien aan je opdrachtgever hoe je als bedrijf ook serieus omgaat met cyberweerbaarheid. Dat geeft vertrouwen.”

5. Industrie: steeds vaker doelwit

Productiemachines, robots en magazijnsystemen communiceren continu met elkaar om het productieproces zo efficiënt mogelijk te laten verlopen. Met besturing op afstand kan daarnaast apparatuur vanaf één centrale plek worden bediend. De industrie is geliefd bij cybercriminelen.

Industriële bedrijven zijn steeds vaker het doelwit van cybercriminelen. In de ranglijst van IBM X-force steeg de industrie zelfs met stip van plaats acht naar de tweede plaats in 2020. De industrie wordt vooral aangevallen met het doel om kostbare informatie zoals intellectueel eigendom buit te maken of om te chanteren. Met gijzelsoftware wordt dan de boekhouding vergrendeld of zelfs het productieproces stilgelegd. De enorme toename van Business E-mail Compromise (BEC)-aanvallen hebben tot doel om via een e-mailuitwisseling werknemers om de tuin te leiden en hen uiteindelijk geld over te laten maken of data te versturen naar de criminelen.

Desondanks blijkt uit onderzoek dat de gemiddelde Nederlandse industriële ondernemer zichzelf niet als interessant doelwit ziet voor cybercriminelen. De cyberparaatheid is daarom laag, vooral bij het midden- en kleinbedrijf (mkb). De FME, de brancheverenigingvoor de industrie, roept op tot versnelling en intensivering van de cybersecurity-aanpak[16]. De FME benadrukt in zijn standpunt dat cyberveiligheid een essentiële randvoorwaarde is voor het Nederlands groeivermogen en welvaartbehoud.

Datalek

Naast een papierloze kantooromgeving worden ook op de fabrieksvloer volop digitale middelen ingezet. Productiemachines, robots en magazijnsystemen communiceren continu met elkaar om het productieproces zo efficiënt mogelijk te laten verlopen. Ook buiten de fabrieksmuren is er veel data-uitwisseling. Machinedata worden bijvoorbeeld naar de backoffice van gebruiker of fabrikant gestuurd voor de planning van predictief onderhoud, controle en optimalisatie. Ook machine-onderhoud en upgrades van de ingebouwde software worden via onlineverbindingen uitgevoerd. Vooral de toeleverketens voor elektronica, auto's en hightech-machines zijn complex en internationaal. De vele schakels zijn digitaal met elkaar verbonden om zo tegen de laagste kosten te produceren, maar dit verhoogt het risico op cybercriminaliteit.

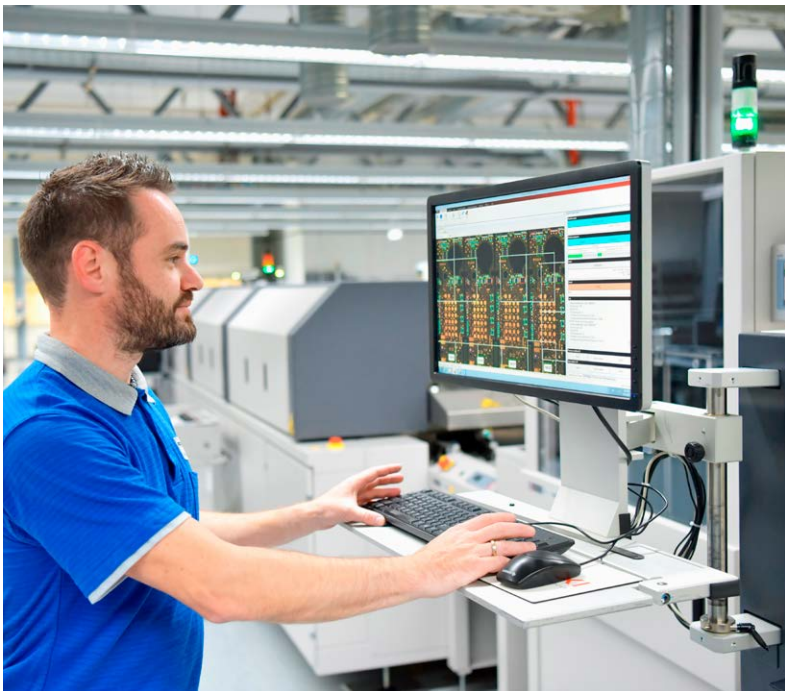
16 FME, 'Cybersecurity essentieel voor industrie', website 2021

Ook de trend van servitization, de transitie van het industriële verdienmodel van pure productie en verkoop naar het aanbieden van diensten en 'as-a-service'-proposities, verhoogt het risico op een cyberaanval en vergroot de impact van een hack. Om de afnemer te ontzorgen van bijvoorbeeld onderhoud, storingen en machine-optimalisatie heeft de fabrikant vaak online toegang nodig tot het product. De kans op een datalek wordt hierdoor vergroot, omdat het ICT-beheer bij verschillende partijen ligt. Ook gezamenlijk gebruik of hergebruik van elektronica of machines kan leiden tot verlies van vertrouwelijke informatie.

Zwakste schakel

"Kopiëren is nog altijd goedkoper dan eigen onderzoek en ontwikkeling", aldus Robert Jan Marringa van het Cyber Weerbaarheidscentrum Brainport (CWB), wijzend op de kostbare kennis die hoogtechnologische bedrijven in huis hebben. De Nederlandse industrie kent een aantal toonaangevende en innovatieve multinationals als ASML, Philips, Vanderlande en Thales waar een heel ecosysteem van toeleveranciers omheen hangt van ondernemingen als VDL, NTS en Aalberts Industries. Deze innovatieve koplopers verduren veel cyberaanvallen vanwege hun kostbare bedrijfsgeheimen. Als hackers niet binnen weten te komen bij de grote multinationals, dan rammelen ze aan de digitale poort van de kleinere en vaak minder goed beveiligde eerstelijns of tweedelijns toeleveranciers.

Dat cybercriminelen vernuftig te werk gaan, heeft ook Jeroen Roest, directeur van Ketting Import Mij. uit Nootdorp ervaren. "Begin 2020 opende een medewerker per ongeluk een geïnfecteerde pdf via de e-mail, waarna hackers met een soort spam-bot duizenden e-mails hebben verzonden vanaf onze server", vertelt Roest. "Gelukkig werd dit snel opgelost door onze ICT-partner." Toch bleek dit niet het einde te zijn. Enkele weken later bleek dat de cybercriminelen ook een e-mailadres van een bestaande leverancier in ons systeem hebben aangepast met een klein lettertje. Via dit 'bekende' e-mailadres werd een nieuw rekening-nummer doorgegeven onder het mom van een wisseling van bank. "Pas na een herinnering van onze leverancier kwamen wij erachter dat er een flink bedrag was over-gemaakt naar de valse bankrekening. Via de fraude-desk van ABN AMRO en de medewerking van de Chinese bank hebben wij het geldbedrag gelukkig kunnen terughalen", aldus Roest.



Uitbesteden

Roland Sniekers is eigenaar van Euro-Techniek in Veldhoven en is een tweedelijns toeleveranciers van veel bedrijven in de hightech, automotive en aerospace. Hij is zich zeer bewust van de gevaren en ziet ook dat zijn mkb-bedrijf steeds meer data deelt met partners buiten de fabrieksmuren. Zijn afnemers stellen steeds meer vragen over zijn veiligheidsmaatregelen. Sniekers ziet het dan ook als belangrijkste doel om zijn cybersecurity beter op orde te hebben dan andere bedrijven. Hij heeft daarvoor ook een prominente rol neergelegd bij zijn ICT-toeleverancier. "Als mkb-bedrijf is het onmogelijk om iemand intern verantwoordelijk te maken voor cybersecurity. Het is te complex om het erbij te doen, wij hebben daarom gekozen voor uitbesteding. Maar onze data bewaren we op onze eigen servers."

Liesbeth Holterman van het Cybersecurity Centrum Maakindustrie (CCM) – onderdeel van Novel-T – schat in dat binnen de industrie circa 75 procent van de bedrijven de ICT heeft uitbesteed. Voor het mkb ligt dit percentage waarschijnlijk hoger. "Veel bedrijven gaan ervan uit dat bij ICT-uitbesteding ook direct de cyberveiligheid goed geregeld is. Maar dat is echter vaak niet het geval. Cybersecurity is tegenwoordig echt een specialisme en behelst meer dan applicatiebeheer en tijdige updates", aldus Holterman.

Certificering

Het is daarom opvallend dat de toonaangevende maakbedrijven op dit moment nog geen harde certificeringseisen stellen aan haar toeleveranciers op het gebied van cybersecurity. Wel vraagt een aantal fabrikanten, zoals ASML, haar toeleveranciers om een 'self-assessment' aan de hand van een cybersecurity-vragenlijst. Ook helpen de cybersecurity-specialisten van ASML om de cyberweerbaarheid van hun toelever-netwerk te vergroten door trainingen en informatie[17].

Certificering van beveiligingsniveau blijkt voor het mkb in de praktijk lastig te zijn. Er zijn weliswaar internationale cybersecurity-normen voor zowel de informatietechnologie (IT) als de operationele technologie (OT). Voor de industrie zijn dit de twee belangrijkste domeinen: in de kantooromgeving van de fabriek gaat het om de IT: de bescherming van persoons- en bedrijfsgegevens. Hiervoor is ISO 27001/27002 de wereldwijde standaard. Op de fabrieksvloer draait het juist om de OT. Hier gaat het om de betrouwbaarheid en de continue beschikbaarheid van industriële automatiserings- en controlesystemen. Dit valt onder het IEC 62443-normenkader.
Toch zijn deze twee certificaten voor het mkb vaak te uitgebreid en te kostbaar om eraan te voldoen. De trend is wel dat door de vergaande digitalisering binnen de fabriek de IT en OT steeds meer naar elkaar toegroeien en eigenlijk ook niet meer los van elkaar gezien kunnen worden[18]. Door de vele onderlinge connecties kunnen hackers vaak beide systemen penetreren.

Er wordt hard gewerkt aan een goed keurmerk dat ook haalbaar is voor het mkb. Het door het Ministerie van Justitie & Veiligheid gefinancierde Centrum voor Criminaliteitspreventie en Veiligheid (CCV) wil per 1 juli 2021 het certificatieschema uitrollen dat is gericht op het certificeren van penetratietesten[19]. Bij zo'n 'pentest' speuren onderzoekers naar kwetsbaarheden in websites, applicaties en IT-infrastructuur, zodat daarna met gerichte maatregelen eventuele hiaten gedicht kunnen worden.

Marringa van het CWB geeft aan dat de CWB CISO-alliantie veel informatie uitwisselt en ook met een eenduidig standaardcertificaat voor de hightech industrie komt. Tot deze tijd zal het mkb, eventueel samen met afnemers en externe adviseurs, het cyberveiligheidsniveau moeten verhogen om zijn positie in de keten te behouden.

Specifiek voor het mkb bieden zowel CCM als CWB via hun websites diverse en op de industrie toegesneden diensten aan zoals kennissessies, veiligheidsscans, dreigingsinformatie en praktische adviezen om de cyberweerbaarheid van maak-bedrijven te verhogen.

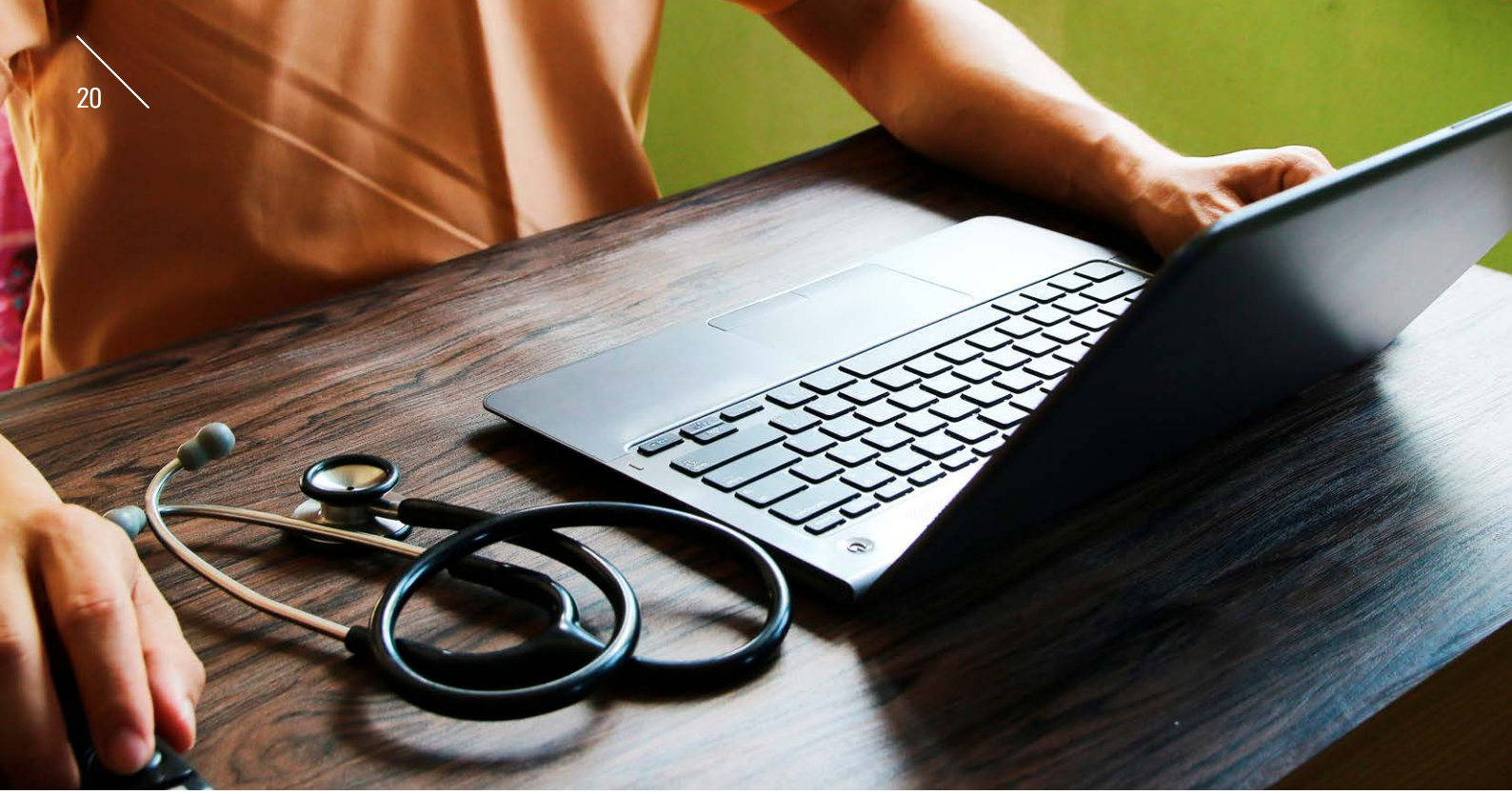
CYBERSECURITY CENTRUM MAAKINDUSTRIE

CYBER WEERBAARHEIDSCENTRUM BRAINPORT
voor de hightech industrie in Nederland

Personeel

Hackers krijgen vaak toegang tot kritieke bedrijfssystemen via 'social engineering'. Via de telefoon als nep-helpdesk medewerker, via de chat of via Facebook en LinkedIn. Gelukkig zijn steeds meer industriële ondernemers zich hiervan bewust. Het CCM krijgt daarom veel vragen over training van bewustwording en gedrag van eigen personeel. Holterman van het CCM onderschrijft het belang van training en levenslang leren. "De huidige trainingen over cybersecurity zijn vaak te generiek van opzet en daardoor minder effectief voor de industrie." Zij wijst er onder meer op dat medewerkers op de werkvloer weliswaar weinig gebruik maken van e-mail en internet, maar wel usb-sticks gebruiken voor bijvoorbeeld de overdracht van aansturingsbestanden voor de machines.

17 FD, 'ASML geeft zijn leveranciers bijles over weren hackers', mei 2021
18 Applied Risk, 'The state of industrial cyber security 2020', november 2020
19 Centrum voor Criminaliteitspreventie en Veiligheid, 'Cybersecurity Pentesten CCV Certificatieschema', april 2021



6. Zorg: patiëntgegevens kwetsbaar

Het verwerken van enorme hoeveelheden data en de beweging waarbij steeds meer zorg op afstand wordt verleend, vergroot de kans dat gevoelige patiëntgegevens in handen van criminelen vallen. De sector zorg staat bovenaan als het om datalekken gaat.

De voordelen van digitalisering voor de zorg zijn legio. Zorgverleners besparen tijd, verminderen administratieve lasten en de patiënt krijgt makkelijker inzicht in het eigen ziektebeeld. Inmiddels werkt 97 procent van de zorgverleners in Nederland met een elektronisch patiëntendossier en schrijft eenzelfde percentage digitaal medicijnen voor, zo blijkt uit onderzoek van Deloitte. Verder zijn zorgorganisaties zelf digitaal verbonden aan leveranciers in de keten en vooral ziekenhuizen zijn afhankelijk van tientallen en in sommige gevallen van zelfs honderd verschillende leveranciers. Het aantal leveranciers neemt tevens toe doordat er steeds meer technologie wordt gebruikt.

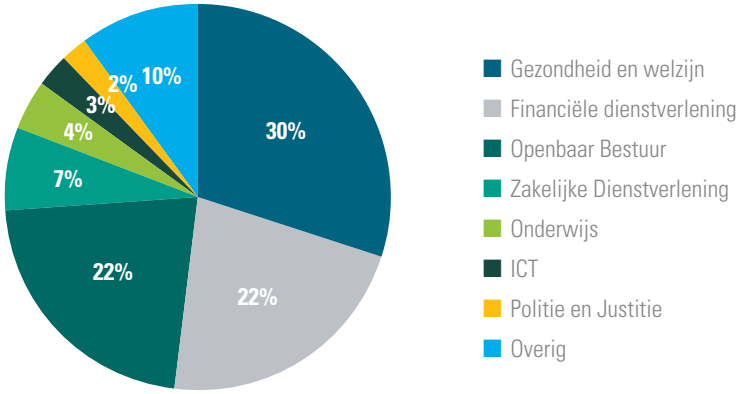
De coronapandemie heeft die digitalisering van de zorg in een stroomversnelling gebracht. Zo worden veel meer consulten op afstand gedaan nadat de Nederlandse Zorgautoriteit (NZa) het mogelijk heeft gemaakt om ook het eerste consult digitaal te doen. Verder weten zorgorganisaties de druk op de zorg te verlagen door meer thuis-monitoring in te zetten. Herstellende coronapatiënten recupereren dan thuis in plaats van in het ziekenhuis. De patiënt test zelf op zuurstofgehalte, bloeddruk en temperatuur en vult dat in, in een app of geeft het telefonisch door aan de huisarts.

Maar deze digitalisering brengt ook een extra kwetsbaarheid met zich mee, namelijk dat belangrijke gegevens of systemen kunnen worden misbruikt door criminelen. Juist in de zorg is het belangrijk dat gegevens alleen worden gebruikt door diegene die ze nodig hebben en dat systemen te allen tijde functioneren. Hoe kwetsbaar bijvoorbeeld een ziekenhuis kan zijn, bleek vorig jaar toen de gegevens van een universitair ziekenhuis in het Duitse Düsseldorf werden gegijzeld. Het ziekenhuis moest noodgedwongen de zorg afschalen en de Eerste Hulp sluiten waardoor een ambulance met een patiënt in kritische toestand naar een ander ziekenhuis moest worden gebracht.

Datalekken

Ook als het gaat om het bewaren van gegevens is de zorg kwetsbaar. De sector gezondheid en welzijn staat als branche al jaren bovenaan het lijstje datalekken dat de Autoriteit Persoonsgegevens (AP) verzamelt. In veel gevallen gaat het om het verstrekken van persoonsgegevens aan de verkeerde ontvanger. Opvallend is vooral dat kleinere zorginstellingen vaker melding maken van een datalek door hacking, malware of phishing dan grotere zorginstellingen.

Datalekmeldingen per sector (2020)[20]



De sector zelf wapent zich wel steeds meer tegen het risico op datalekken en cyberaanvallen. Zo is er stichting Z-CERT, dat in 2017 werd opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), de Nederlandse Federatie van Universitair Medische Centra (NFU) en de Nederlandse ggz in samenwerking met het ministerie van Volksgezondheid. Z-CERT houdt de IT-beveiliging van bij de stichting aangesloten instellingen in de gaten en houdt contact met bijvoorbeeld het Nationaal Cyber Security Center (NCSC) over nieuwe dreigingen. Sinds begin dit jaar zijn 168 zorginstellingen aangesloten bij de stichting.

Hoewel Z-CERT zich specifiek richt op de cybersecurity voor de aangesloten instellingen, informeert de stichting ook andere zorgorganisaties, vertelt Jan Hanstede, cybersecurityspecialist bij Z-CERT. “Als wij een lijst krijgen met gecompromitteerde IP-adressen, delen we dat natuurlijk ook met organisaties buiten onze deelnemersgroep. Dat wordt wel goed ontvangen.” Z-CERT ziet dat de zorgsector zich steeds bewuster wordt van het belang van informatiebeveiliging en IT-security. Ook proberen instellingen die te maken hebben gehad met een hack of een groot datalek andere instellingen hier inzicht in te geven zodat er lering uit kan worden getrokken.

Die cybersecurityrisico’s liggen niet alleen bij zorginstellingen zelf, maar ook bijvoorbeeld bij de leveranciers aan die zorgorganisaties, legt Hanstede uit. Huisartsen gebruiken bijvoorbeeld vaak een gespecialiseerde leverancier voor het elektronisch patiëntendossier. Hierdoor worden de dossiers van enkele honderden zorginstellingen centraal beheerd door één organisatie. “Daar maak ik mij wel eens zorgen over”, vertelt Hanstede. “Wanneer die leveranciers worden aangevallen, kunnen meteen enkele honderden zorginstellingen niet meer bij hun gegevens.”

Ziekenhuizen

Met name bij ziekenhuizen is het risico van de ketenpositie groot. Sommige ziekenhuizen zijn afhankelijk van soms wel honderd verschillende leveranciers die ook digitaal verbinding maken met de systemen van het ziekenhuis. Hanstede benadrukt dat zorgorganisaties goede afspraken moeten maken met die leveranciers om de certificering, zoals de NEN7510, op orde te houden zodat alle betrokken partijen ook weten wat ze kunnen verwachten van elkaar. Ook afspraken over periodiek testen en scannen op kwetsbaarheden zouden in een overeenkomst moeten staan.

20 Bron: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

Tijdens de coronapandemie werd de zorg geconfronteerd met een toename in het aantal aanvallen. “Tijdens de piek van het aantal besmettingen in maart vorig jaar kwam er bijvoorbeeld heel veel corona-gerelateerde spam en malware binnen”, aldus de cybersecurityspecialist. Ook probeerden hackers gebruik te maken van het thuiswerken door zorgmedewerkers. “Wanneer er een crisis is en de druk hoog, spelen de criminelen daar op in.”

Bij het Antoni van Leeuwenhoekziekenhuis beschouwt men de NEN7510 als een solide basis voor de eisen aan cybersecurity, maar niet als een eindstation, stelt Joost Boele, Chief Information Security Officer (CISO) bij het ziekenhuis. Naast preventie wordt ook aan detectie en respons meer aandacht besteed. Zo wordt er regelmatig geoefend op de paraatheid van de organisatie. “Zo cruciaal als oefenen is in de zorg, zou het ook moeten zijn in informatiebeveiliging”, vertelt Boele.

Net voor het uitbreken van de coronapandemie had de organisatie de basis gelegd voor grootschalig thuiswerken. “Dit kon dus met voorrang beschikbaar worden gemaakt, zodat zoveel mogelijk werk door kon gaan naast het directe patiëntencontact.” Hiernaast werd extra ingezet op de bewustwording van deze nieuwe manier van werken. “Zo zag je in het begin bijvoorbeeld veel zorgen om de veiligheid van Zoom.” Bij het Antoni van Leeuwenhoek proberen ze bewustwording van cybersecurity bij het personeel zoveel mogelijk aan te laten sluiten bij de dagelijkse situatie in de organisatie, zoals te zien is in dit filmpje over een nieuwe trainingsmodule.

Boele adviseert andere zorgorganisaties om cybersecurity vanaf de ontwerpfase van alle nieuwe plannen direct op de agenda te zetten. “Hoe later je nadenkt over security, hoe duurder het wordt. Dit is ongeacht of het om het ontwerp van je gebouw gaat of het ontwerp van je zorgprocessen. Denk bijvoorbeeld na over de vraag of het wel nodig is dat een bestralingstoestel of beeldvormingsapparaat met alle apparaten op het netwerk kan praten. En moet iedereen zomaar kunnen inloggen op een computer op de intensive care?”

Huisartsen

Jonathan Bouman, huisarts en cybersecurity-expert, ziet dat in de eerstelijnszorg vaak aan de menselijke kant kwetsbaarheden ontstaan. “Uiteindelijk gaat cybersecurity ook om gedrag van mensen.” In de afgelopen tien jaar heeft de eerstelijnszorg een enorme ontwikkeling meegemaakt als het gaat om het gebruik van bijvoorbeeld elektronische patiëntendossiers. Waar veel huisartsen tien jaar geleden nog met archiefkasten werkten, staan gegevens nu vaak al in de cloud bij een leverancier.

Volgens Bouman zijn steeds meer huisartsen zich bewust van het gevaar van datalekken en over hoe zij daarmee om moeten gaan. “In alle praktijken wordt daarvoor gewaakt. Ook binnen de vakvereniging zijn er richtlijnen en adviesdocumenten over en voor vrijwel alle kritieke infrastructuur is er two factor authentication. Gelukkig is er steeds meer aandacht voor veilig digitaal werken.”

Bouman maakt zich wel zorgen om verzekeringen voor cybercriminaliteit die worden aangeboden aan huisartsen. Die verzekeringen betalen uit wanneer bijvoorbeeld gegevens gegijzeld worden. Hiermee kunnen huisartsen het financiële risico van een ransomwareaanval afdekken, maar zo worden ze onbedoeld ook een aantrekkelijker doelwit voor cybercriminelen. “Hiermee leg je een premie op jezelf. Op deze manier ontstaat namelijk een beloning om huisartsen te hacken. Dat is een onderwerp waar we goed over na moeten denken.”

7. Retail: data consumenten gewild

Het intensieve contact dat retailers met hun klanten onderhouden, maakt de sector kwetsbaar voor datadiefstal. Een datalek kan leiden tot forse reputatieschade en klantverlies die het voortbestaan van een onderneming ernstig kunnen belemmeren.

Recent lagen miljoenen wachtwoorden en privégegevens van AlleKabels.nl door een hack op straat. Een database met privégegevens van 3,6 miljoen consumenten werd voor 15.000 euro te koop aangeboden op een hackersforum. Het bedrijf heeft direct melding gemaakt bij de Autoriteit Persoonsgegevens en de beveiliging maximaal opgeschroefd. Weliswaar waren de wachtwoorden van klanten versleuteld, toch werden deze gekraakt. Het zou gaan om het grootste datalek met wachtwoorden in Nederland.

Retailers worden steeds vaker getroffen door cybercriminaliteit en gebruiken steeds meer data om klanten te binden en om hun behoeften beter te kunnen voorspellen. Retailers beschikken daarom over veel klantinformatie en daar moet uiterst voorzichtig mee opgesprongen worden. De privacywetgeving Algemene Verordening Persoonsgegevens (AVG), die geldt sinds 25 mei 2018 voor de hele Europese Unie (EU), verplicht ondernemers om de klantgegevens zorgvuldig te verwerken en te beschermen. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de AVG.

De meest voorkomende risico's voor retailers als het gaat om cybercriminaliteit is het verstoren van de bedrijfsvoering met omzetverlies, het verlies aan bedrijf- en klantgegevens, financiële schade door herstelkosten en door claims van gedupeerden, en een boete op basis van de AVG die kan oplopen tot vier procent van de jaaromzet. Alertheid blijft geboden en helaas is vaak een incident nodig voor er stringente maatregelen worden genomen. Als klantgegevens in handen komen van criminelen dan kunnen klanten daar ernstige gevolgen van ondervinden zoals in het geval van identiteitsfraude of phishing. De recente datalekken bij social media als Facebook, LinkedIn en Instagram zijn voorbeelden waarbij consumenten door criminelen benaderd worden met nauwelijks van echt te onderscheiden nepberichten. Een datalek kan leiden tot forse reputatieschade en klantverlies die het voortbestaan van een onderneming ernstig kunnen belemmeren.

Schaduwwebsite

Cybercriminelen maken in de retail veelvuldig gebruik van gijzelsoftware, het stelen van inlog- en klantgegevens, het ongeautoriseerd toegang krijgen tot servers maar ook van een cyber-aanval. In Luxemburg heeft een aantal supermarkten van formule Cactus in 2020 een paar dagen hun deuren vanwege gijzelsoftware moeten sluiten. Ook autobedrijven worden vaak getroffen door gijzelsoftware. De bedrijven kunnen dan niet meer bij klant-gegevens, facturen, de planning en de voorraadgegevens komen. Dan is het heel lastig om een garagebedrijf te runnen als onbekend is welke klant die dag komt, waarvoor deze komt en welke voorraden er zijn. Ook al krijgen bedrijven na het betalen van losgeld uiteindelijk weer toegang tot hun gegevens, toch veroorzaakt een aanval een scherpe daling van het service- en kwaliteitsniveau met mogelijk verlies van klanten.

Cybercriminelen zijn in staat om in een weekend een complete website van een retailer volledig na te bouwen. Niets vermoedende consumenten bestellen en betalen online de producten en komen dan van een koude kermis thuis. Deze schaduwwebsites zijn moeilijk van echt te onderscheiden en net lang genoeg actief voordat ze ontdekt worden. Een cyberaanval op een webshop kan de onlineverkopen voor langere tijd stil leggen. Daarbij kunnen hackers de gegevens van klanten stelen met alle gevolgen van dien zoals identiteitsfraude en phishing.

Keten

Cybercrime raakt de hele keten. Leveranciers moeten daarom ook beoordeeld worden op cybersecurity omdat retailers gehackt kunnen worden via onveilige systemen van hun partners. Een ander voorbeeld van afhankelijkheid is de recente ‘kaas-hack’ waarbij begin april 2021 een hack werd geconstateerd bij logistiek bedrijf Bakker. Het betrof gijzelsoftware, waarschijnlijk via een lek in de software van Microsoft Exchange. Door deze hack hadden onder meer de supermarkten van Albert Heijn te kampen met lege schappen kaasproducten. Bedrijven die afhankelijk zijn van regelmatige leveringen van producten met een hoge omloopsnelheid zullen garanties van hun leveranciers eisen omdat dit hun eigen omzet schaadt. Een bedrijf wil absoluut niet direct of indirect geïnfecteerd worden door zijn leveranciers.

Ook bij internationale handelsketens is extra waakzaamheid geboden. CTOUCH uit Eindhoven, leverancier van groot formaat touchscreens die gebruikt worden in het klaslokaal en in vergaderruimtes, heeft dit aan den lijve ondervonden. CFO Bernard Gosselink: “Onze touchscreens worden geproduceerd in Azië en onze mensen moeten daar dus regelmatig zijn. Op elke zakenreis naar China bleken onze laptops geïnfecteerd te worden met malware of virussen. Daar moet je van bewust zijn en bescherming is daarom noodzakelijk. Wij zijn niet zo naïef om te denken dat ons niets zal overkomen, dus naast de standaard virusscanners en firewalls, leek ons een cybersecurityverzekering geen overbodige luxe.”

Training

Uit onderzoek blijkt dat 90 procent van de cybercriminaliteit begint bij ‘social engineering’. Hierbij wordt geprobeerd om via medewerkers het systeem binnen te dringen. Vorig jaar overkwam dit Bol.com die dacht 750.000 euro over te hebben gemaakt naar prullenbakkenproducent Brabantia. Cybercriminelen hadden de mail van een medewerker van Brabantia gehackt en via diens e-mailadres een bericht gestuurd naar Bol.com over een gewijzigd rekening-nummer van Brabantia. De administratieafdeling van Bol.com trapte erin. Het is dus voor retailers van cruciaal belang dat zij hun medewerkers bewust maken voor het cybergevaar en hen continu trainen. Zo wordt mogelijk voorkomen dat medewerkers klikken op foute linkjes of foute bijlagen openen, wachtwoorden intikken op valse websites of overgehaald worden om geld over te maken. In het laatste geval wordt vaak de correspondentie van leidinggevenden gehackt en urgentie gesuggereerd. Dit wordt ook wel CEO-fraude genoemd.

8. Leisure: digitaal contact met gasten risicovol

Ondernemingen uit de vrijetijdssector zetten actief digitale middelen in voor het doen van boekingen en betalingen en het informeren van hun gasten. Helaas weten cybercriminelen dat ook; databases met gegevens van rijke hotelbezoekers blijken goud waard.

Edwin Slutter was voorheen CFO van Pathé. Hackers braken in op de computers van de bioscoopketen en wisten via CEO-fraude 19,2 miljoen euro buit te maken. Nu waarschuwt hij vanuit zijn eigen adviesbureau Added Value Finance andere CFO's en topmanagers. In het FD zegt hij: "Jouw bedrijfscultuur vormt het grootste gevaar."

Hoe gaat CEO-fraude in zijn werk? Slutter: "Ze braken in op de server en volgden de communicatie. Wie communiceert met wie? Wat is de cultuur in de organisatie? Ze downloaden stukken. Die jongens zijn geschoolde professionals. Op IT-gebied, maar ook in finance." De fraudeurs creëerden een geloofwaardige omgeving met bijvoorbeeld een website van een bedrijf in Dubai en met handtekeningen om een deal goed te keuren en vervolgens geld te innen. "Toen het spel uit was, knipten ze alle banden door en waren ze in geen velden of wegen meer te bekennen. De grote vraag is dan of je het geld ooit nog terugziet."

Helaas is Pathé geen uitzondering. In het Internet Cyber Crime Report van de FBI wordt de schade van CEO-fraude geschat op ruim 26 miljard dollar. Het is een lucratieve en daardoor ook een snel groeiende vorm van internetcriminaliteit. Grotere ondernemingen in de gastvrijheidsindustrie moeten dus zich realiseren dat fraudeurs alle tijd nemen om het bedrijf en de bedrijfscultuur te leren kennen. Ze proberen in hun communicatie hierbij aan te sluiten en leggen contact met de lokale directie of de medewerkers van de financiële administratie met een dringende vraag. Te denken valt aan gevoelige overnametrajecten of aan een noodkrediet voor een ander onderdeel van hetzelfde bedrijf.

Rijke gasten

Klantdata zijn cruciaal in de sector leisure, want zij maken het mogelijk om het gedrag van specifieke doelgroepen of zelfs individuele klanten te voorspellen. Nu eindigen zakelijke reizigers bij veel hotels bijvoorbeeld nog in hetzelfde segment. Op basis van patroonherkenning kan de intelligente software vaststellen dat een zelfstandig ondernemer structureel vroeger boekt dan een zakenvrouw in loondienst, en dat kamerprijs voor die ondernemer van doorslaggevend belang is bij zijn keuze. Naast het optimale aanbod van een hotelkamer of een reis kunnen daar direct talrijke andere zaken bij betrokken worden: bewaakte parkeerplaatsen, voorgereserveerde laadpalen en allerlei andere extra's waar de nieuw gedefinieerde doelgroep blijkens de data gevoelig voor is.

Vanwege de problemen die de leisure-sector als gevolg van de coronapandemie heeft ondervonden, ebt de aandacht voor cybersecurity mogelijk weg. Een recente enquête van Hotel Leaders Network bevestigt dat aandacht van hoteliers vooral uitgaat naar de herstelfase en het werven van nieuwe medewerkers. Dat weten criminelen ook en wellicht richten zij zich juist nu op de vele herstellende bedrijven.

Desondanks realiseren veel ondernemers zich niet goed op welke goudmijn zij soms zitten. Onder meer de data van hotelketens zijn waardevol. Deze bevatten persoonlijke gegevens van vermogende zakenreizigers die als buit kunnen worden verhandeld op the dark web. Voor 'exclusieve databases' worden bedragen betaald tot 850 euro per individuele deelnemer of gast.

Ook hierom grijpen privacy-waakhonden wereldwijd hard in. Zo kreeg Marriott recent een fikse boete omdat de hotelketen in 2014 onvoldoende in staat bleek om de eigen klantdata te beschermen. Zoiets leidt tot meer dan alleen imagoschade. Gemiddeld dalen de aandelen van beursgenoteerde hotelbedrijven met 5 procent na een datalek. Volgens marktonderzoeker Igniyte went tot 7 procent van de gasten zich af van de beboete onderneming.

Restaurants

Ook voor relatief kleine ondernemingen wordt data-analyse steeds relevanter. Ondernemers die openstaan voor deze inzichten, kunnen actief profijtelijke strategieën ontwikkelen. Op het gebied van personeelskosten wordt het bijvoorbeeld veel makkelijker de inzet van personeel optimaal af te stemmen op het aantal gasten. Zo kunnen bedrijven op basis van historische data precies zien wat ze voor oproep-, tijdelijke en vaste krachten betalen op feestdagen en andere specifieke tijdstippen en periodes.

Een andere steeds vaker gebruikte mogelijkheid is het optimaliseren van een menu op basis van actuele en historische data. Dat beantwoordt aan restauranthouders vragen als welke gerechten op welke momenten het vaakst worden besteld, welke combinaties met andere gerechten of wijnen favoriet zijn of wat het effect is van kortings-acties. Deze werkwijze vereist de inzet van digitale middelen, waarmee tegelijk de deur open wordt gezet naar het ongewild delen van informatie over gasten.

9. Advocaten en accountants: datalek meest gevreesd

Professionele dienstverleners werken continu met vertrouwelijke informatie van klanten, wat ze een interessant doelwit maakt voor cybercriminelen.

Een gat in de beveiliging van Microsoft Exchange-servers leidde tot de nodige schrik onder advocaten, accountants en organisatieadviesbureaus, ook wel professionele dienstverleners genoemd. Als gevolg hiervan zijn inmiddels tientallen datalekmeldingen gemeld aan de Autoriteit Persoonsgegevens (AP). “Met zo’n Microsoft-hack, die ons gelukkig niet geraakt heeft, komt het gevaar wel heel dichtbij”, laat Bas Boris Visser, Global Head of Innovation en Business Change binnen Advocatenkantoor Clifford Chance, weten aan ABN AMRO. “Wij werken voor grote internationale bedrijven op vertrouwelijke transacties. De schade van een datalek is niet te overzien; zowel voor cliënten als voor onszelf.”

Het thema cybercriminaliteit staat dan ook hoog op de prioriteitenlijst van professionele dienstverleners. Datalekken worden hierbij om bovengenoemde redenen het meest gevreesd. Methodes die hiervoor gebruikt worden lopen uiteen van phishing tot diefstal van inloggegevens die toegang geven tot bedrijfsgevoelige informatie. Maar ook kan er toegang tot data en systemen verkregen worden via een supply chain hack – bijvoorbeeld via de softwareleverancier – of via servers die onvoldoende beschermd zijn.

De impact van een datalek is groot, stelt Francien van Erp, financieel manager bij Biersens Incasso Advocaten. Maar bij het ontfutselen van data houdt het volgens haar niet op. In de praktijk worden advocatenkantoren met allerlei type aanvallen geconfronteerd. “Geregeld komt er een poging tot CEO-fraude bij ons voorbij.”

Thuiswerken

Veel accountants, advocaten en consultants werken vanuit huis als gevolg van de coronamaatregelen. Diverse onderzoeken tonen aan dat een groot deel van hen dit ook in de toekomst blijft doen. Met name het risico dat is verbonden aan het gebruik van zogeheten ‘elevated accounts’ is door het massale thuiswerken toegenomen. Dit betreft bijvoorbeeld de systeembeheerder die hiermee op afstand een computer kan ‘overnemen’. Een cybercrimineel kan dat dus ook. De toegangscontrole en het beheer van dit type account is juist nu extra belangrijk.

Visser herkent de risico's die verbonden zijn aan het thuiswerken. Cybercriminaliteit was al prioriteit, maar sinds het thuiswerken topprioriteit volgens hem. Een voorbeeld hiervan is het ondertekenen van transacties vanuit huis. "We doen dit nu elektronisch, maar moesten dit wel op een veilige manier mogelijk maken." Ook is de frequentie van bewustwordingscampagnes opgevoerd bij veel bedrijven. "Doordat je elkaar niet ziet is het lastiger bewust te blijven van de risico's", aldus Visser.

Gedrag

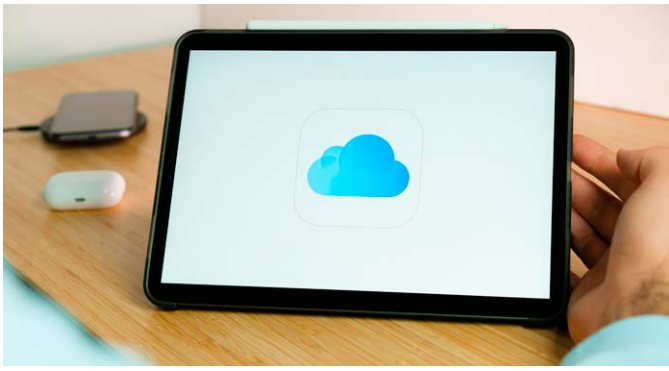
Met alleen firewalls ben je er niet, daar zijn alle geïnterviewden het over eens. Kees Plas, Partner bij accountantskantoor BDO: "Naast de technische maatregelen is het noodzakelijk om een gevoel van urgentie te creëren en medewerkers te trainen." Ook binnen Clifford Chance worden medewerkers constant uitgedaagd om geen verkeerde mails te openen. Van Erp van Bierens Incasso Advocaten traint haar medewerkers eveneens met een online tool. "Op een onverwachts moment krijgen medewerkers een mail die verleidelijk is om die te openen."

Constante aandacht voor de gedragscomponent bij cybercriminaliteit is noodzakelijk. Geïnterviewden hebben diverse phishing-pogingen meegemaakt, bijvoorbeeld bij een medewerker die op een link klikt waardoor het e-mailadres overgenomen kon worden. Vervolgens werden bij het desbetreffende kantoor vanuit Amerika e-mails verstuurd met malafide bijlagen. Het automatisch checken van het IP-adres, zodat nagegaan kan worden waar ter wereld wordt ingelogd, is een van de maatregelen die vervolgens is genomen.

Cloud

Zoals bovenstaand voorbeeld laat zien, gaat het treffen van technische maatregelen en gedragstraining hand in hand; de een kan niet zonder de ander. Visser van Clifford Chance, vertelt dat het kantoor recentelijk de overstap heeft gemaakt naar een cloudoplossing voor hun documentmanagementsysteem. "Wij vinden de cloud beter qua bescherming. Deze stap is ingegeven vanuit cyberrisico's." Het advocatenkantoor is benieuwd hoe de markt erop gaat reageren. "De norm is toch om zoveel mogelijk in eigen huis te houden", meent Visser.

© Vladimka production / Shutterstock.com



Naast het op orde hebben van hygiënefactoren zoals goede firewalls en antivirussoftware, wordt een goede onboarding van softwareoplossingen een belangrijk aandachtspunt bij professionele dienstverleners. "Bij ons is het bijvoorbeeld onmogelijk om losse programma's te installeren op laptops, dit hebben we dichtgezet", aldus Van Erp van Bierens Incasso Advocaten. Ook zijn er diverse slimme IT-oplossingen voorhanden. Zo heeft Clifford Chance recentelijk geïnvesteerd in Reynencourt; een Nederlandse startup die individuele softwareapplicaties voor juridische dienstverleners in een 'container' plaatst. Visser: "Je hoeft hierdoor niet langer individuele apps te monitoren, enkel de container. Dit is zowel gemakkelijker als veiliger."

Belemmeringen

Dergelijke cyberinvesteringen kosten geld. Voor kleinere kantoren zijn deze investeringen op zelfstandige basis vaak lastig. Marien Glerum, Managing Officer Benelux van advocatenkantoor Dentons: "Als groot internationaal kantoor hebben we schaalvoordeel en dus meer middelen om te investeren in IT-beveiliging. Dit is ook wat onze cliënten van ons verwachten. Dit geeft een competitief voordeel ten opzichte van kleinere lokale spelers." Glerum pleit ervoor om investeringen in cybersecurity los te knippen van de winst- en verliesrekening. "Zie het als een noodzakelijke investering voor de lange termijn en een randvoorwaarde om te kunnen opereren. Zo voorkom je dat deze investering wordt uitgesteld." Ook de partnerstructuur waar veel professionele dienstverleners mee werken, werkt volgens een aantal geïnterviewden belemmerend in het treffen van maatregelen. De partnerstructuur vermindert de prikkel om te investeren in zaken die niet direct een commercieel voordeel opleveren. Het gaat immers ten koste van de winstdeling

Ondersteuning door ABN AMRO

Heeft u vragen over cyberveiligheid, neem contact op met één van onze cyber adviseurs

Evelien Cornielje
Industrie & Retail
evelien.cornielje@nl.abnamro.com

Yvonne Hiemstra
TMT & Leisure
yvonne.hiemstra@nl.abnamro.com

Bonne van Weert
Zakelijke dienstverlening
bonne.van.weert@nl.abnamro.com

Anita Gebbeken
Retail & TMT
anita.gebbeken@nl.abnamro.com

Pieter van Dam
Zorg & Vastgoed
pieter.van.dam@nl.abnamro.com

Melanie van Duist
Zakelijke dienstverlening
melanie.van.duist@nl.abnamro.com

Paul Fouchier
Transport en Logistiek & Industrie
paul.fouchier@nl.abnamro.com

Barbara Heijmen
Leisure
barbara.heijmen.demmer@nl.abnamro.com

Jan Egbertsen
Bouw
jan.egbertsen@nl.abnamro.com

Colofon

Dit is een uitgave van ABN AMRO in samenwerking met onderzoeksbureau MWM2.

Contact

- **Ingrid Laane**, Sectoreconoom TMT en Zakelijke Dienstverlening, (06) 16 38 05 75 of ingrid.laane@nl.abnamro.com
- **David Kemps**, Sector banker Industrie, (0)6 30 33 20 43 of david.kemps.nl@abnamro.com
- **Henk Hofstede**, Sector banker Retail, (0)6 53 25 83 24 of henk.hofstede.nl@abnamro.com
- **Bart Banning**, Sector banker Transport en Logistiek, (0)6 51 30 13 96 of bart.banning@nl.abnamro.com
- **Stef Driessen**, Sector banker Leisure, (0)6 53 98 53 29 of stef.driessen@nl.abnamro.com
- **Anja van Balen**, Sector banker Healthcare, (0)6 51 19 06 15, anja.van.balen@nl.abnamro.com

Auteurs

Ingrid Laane, David Kemps, Henk Hofstede, Bart Banning, Stef Driessen, Anja van Balen, ABN AMRO Sector Advisory

Geïnterviewden

Mats Ros, ilionx
Brian Vermeer, Snyk
Liesbeth Holterman, Cybersecurity Centrum Maakindustrie (CCM)
Robert Jan Marringa, Cyber Weerbaarheidscentrum Brainport (CWB)
Jeroen Roest, Ketting Import Mij. BV
Roland Sniekers, Euro-Techniek BV
Bas Boris Visser, Clifford Chance
Francien van Erp, Bierens Incasso Advocaten
Marien Glerum, Dentons
Kees Plas, BDO
Jan Hanstede, Z-CERT
Joost Boele, Antoni van Leeuwenhoekziekenhuis
Jonathan Bouman, huisarts en cybersecurity-expert
Heino Kempers, Jan de Rijk Logistics
Dick Schouten, Van den Bosch
Hélène Minderman, security expert

Eindredactie

Bendert Zevenbergen

Illustraties en opmaak

Kollerie Reklame-advies & Promotions

Fotoverantwoording

Shutterstock.com

Disclaimer

De in deze publicatie neergelegde opvattingen zijn gebaseerd op door ABN AMRO betrouwbaar geachte gegevens en informatie, die op zorgvuldige wijze in onze analyses zijn verwerkt. Noch ABN AMRO, noch functionarissen van de bank kunnen aansprakelijk worden gesteld voor in deze publicatie eventueel aanwezige onjuistheden. De weergegeven opvattingen houden niet meer in dan onze eigen visie en kunnen zonder nadere aankondiging worden gewijzigd. Naast een copyright is er sprake van een right to copy. Het gebruik van tekstdelen en/of cijfers is toegestaan mits de bron duidelijk wordt vermeld. Teksten zijn afgesloten op 1 juni 2021.

©ABN AMRO, juni 2021

abnamro.nl