ABN·AMRO

Mkb isoleert zich door beperkt bewustzijn cyberdreiging

Cyberveiligheid moet ‘boardroom-topic’ worden

Mei 2023

Inhoudsopgave

Mkb isoleert zich door beperkt bewustzijn cyberdreiging

Cybercriminelen verleggen hun aandacht naar kleinere bedrijven, zo blijkt uit onderzoek van ABN AMRO onder 233 zakelijke klanten. Waar vorig jaar het grootbedrijf nog significant meer werd aangevallen dan het mkb, zijn die verschillen nu nog marginaal. Kleinere bedrijven lijken op deze ontwikkeling weinig acht te slaan; hun risicoperceptie is gelijk gebleven. Bij grotere organisaties steeg de risicoperceptie wel sterk. Kleine bedrijven moeten dan ook het been bijtrekken, mede om te voorkomen dat ze als gevolg van nieuwe wetgeving geen opdrachten meer krijgen.

Hoewel veel bedrijven zich veilig wanen, is de kans groot dat zij vroeg of laat slachtoffer worden van cybercriminaliteit. Bedrijven zijn namelijk digitaal op allerlei manieren met elkaar vervlochten. Onlangs meldden meerdere marktonderzoeksbureaus datalekken nadat een hack op softwareleverancier Nebu de deur naar de privégegevens van zeker twee miljoen Nederlanders wijd open had gezet. Deze bureaus, veelal in de mkb-categorie, peilen de klanttevredenheid namens grotere organisaties zoals NS, VodafoneZiggo en CZ.

Terwijl bedrijven in rap tempo hun IT-landschap uitbreiden, voegen daarnaast ook kwaadwillenden steeds meer innovatieve technologieën toe aan hun gereedschapskist. Zo helpt kunstmatige intelligentie met het razendsnel kraken van wachtwoorden, het vormgeven van overtuigende 'phishing'-campagnes, en de creatie van kwaadaardige programma's die zichzelf automatisch verbeteren. "Bedrijven lopen steeds verder achter op de hackersgemeenschap", zegt Matthijs Blokker van cyberveiligheidsbedrijf MMOX.

Een integrale aanpak van cyberweerbaarheid is vereist om de toenemende bedreiging van phishing, malware en ransomware in te dammen. Toch wordt die urgentie niet over de gehele linie gevoeld. Terwijl het percentage ervaringsdeskundigen in het midden- en kleinbedrijf (mkb) en onder zelfstandigen (zzp'ers) in rap tempo toeneemt, is hun risicoperceptie ten opzichte van vorig jaar praktisch gelijk gebleven.

Onder de grootste organisaties daarentegen laat de risicoperceptie een duidelijke stijging zien. Omdat grote bedrijven in de regel met meer partners samenwerken, meer toeleveranciers hebben en meer klanten bedienen, zijn zij meer kwetsbaar voor cyberaanvallen. Die kwetsbaarheden via derden worden door kwaadwillenden momenteel volop benut, met name middels aanvallen op IT-bedrijven die een breed scala aan klanten bedienen.

Met het toenemende risicobewustzijn van grote bedrijven groeien ook de cybersecuritystandaarden waaraan zij hun partners houden. Kleinere bedrijven riskeren dat zij de cyberveiligheidstoets van hun grotere klanten niet doorstaan en zichzelf buiten spel zetten, los van schade aan hun eigen bedrijf. En het zijn juist de kleine bedrijven die voor het eerst meer door cybercriminaliteit worden geraakt dan grote.

De kritische blik op ketenpartners zal nog extra worden versterkt door nieuwe Europese regelgeving op het gebied van cybersecurity. NIS2, de opvolger van de eerdere Network and Information Systems-richtlijn (NIS), spoort namelijk bedrijven aan om afspraken rond cyberveiligheid contractueel vast te leggen met hun directe leveranciers en partners. Ondanks dat NIS2 niet van toepassing is op de kleinste bedrijven, zullen grotere klanten naar aanleiding van de nieuwe wet wel degelijk met kritische vragen kunnen komen.

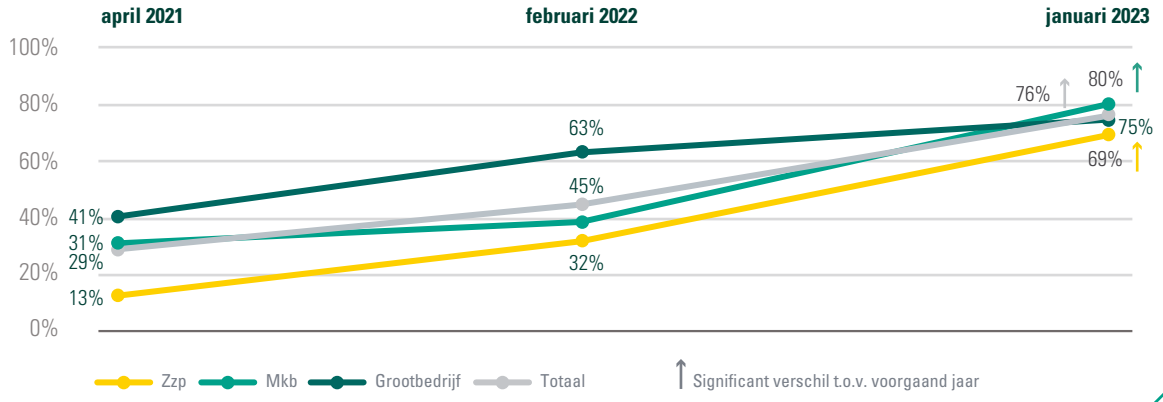
Het is dan ook belangrijk dat cyberveiligheid binnen bedrijven een integraal onderdeel is van de bedrijfsvoering. Wat dat betreft ziet Erik Michielen, managing consultant bij SEQRIT, een positieve trend. "Eindelijk zitten er ook directeuren aan de tafel om mee te denken over cyberveiligheid."

Risicoperceptie versus realiteit

Mkb voor het eerst vaker doelwit dan grootbedrijf

Meer dan driekwart van de bedrijven heeft wel eens te maken gehad met cybercriminaliteit, zo blijkt uit onderzoek onder klanten van ABN AMRO. Bij de meting van vorig jaar gold dit nog voor 'slechts' 45 procent van de ondervraagden. De toename onder mkb'ers – met een jaaromzet van minder dan 10 miljoen – gaat opvallend snel; inmiddels is 80 procent van hen eens het doelwit geweest van kwaadwillenden. Hiermee zijn aanvallen in het mkb-segment voor het eerst dieper doorgedrongen dan in het grootbedrijf, waarvan 75 procent van de ondervraagden te maken heeft gehad met cybercriminaliteit. Voor zzp'ers is dit percentage 69 procent.

Figuur 1. Cyberdreiging neemt toe onder alle bedrijfsgroottes
Percentage bedrijven dat te maken heeft gehad met een cyberaanval (n=233)



Helft van de ondernemers geconfronteerd met phishing

De aanvallen doen zich allerlei gedaanten voor. 'Phishing' is het meest wijdverbreid; meer dan de helft (66 procent) van alle ABN AMRO-panelleden heeft hier wel eens mee te maken gehad. Via e-mails, sms- of WhatsApp-berichten en telefoontjes worden mensen verleid om een actie uit te voeren die later schadelijk blijkt. Het is een relatief simpele aanvalsmethode die niet leunt op grof technologisch geschut maar op psychologische manipulatie. Dat neemt overigens niet weg dat kwaadwillenden de mogelijkheden van de nieuwste innovaties graag benutten (zie kader A). Zo roepen cybercriminelen de hulp in van artificial intelligence (AI) om overtuigende phishing-mails te schrijven en kan de gekloonde stem van een CEO aan de telefoon het laatste zetje vormen om een grote bankoverschrijving te doen naar een frauduleuze bankrekening.

Een phishing-aanval kan gericht zijn op direct financieel gewin, zoals in bovenstaand CEO-voorbeeld, maar kan ook het startpunt zijn van een grotere aanval. Volgens de jaarlijkse 'X-Force Threat Intelligence Index' van IBM verkregen kwaadwillenden in 2022 in 41 procent van de cyberincidenten de toegang tot informatie of systemen via phishing. De buitgemaakte gebruikersnamen en wachtwoorden van IT-systemen en mailaccounts kunnen worden gebruikt om verder in de systemen van de organisatie binnen te dringen. Berichten kunnen daarnaast aansturen op het openen van een downloadlink of bijlage die 'malware' bevat – een kwaadaardig programma dat bijvoorbeeld systemen kan monitoren voor spionagedoeleinden of deze zelfs volledig kan platleggen.

KADER A | Kunstmatige intelligentie als instrument voor kwaadwillenden

Op het gebied van cybersecurity brengt elke nieuwe technologie een golf van kansen en bedreigingen met zich mee. 'Generatieve Artificial Intelligence' is een snel opkomend fenomeen in de wereld van kunstmatige intelligentie en het buzzwoord van cybersecurity-specialisten. Generatieve AI kan niet alleen unieke teksten, maar ook afbeeldingen en muziek genereren op basis van patronen die gedetecteerd zijn uit een dataset.

Eind 2022 veroverde chatbot ChatGPT in korte tijd het internet met teksten die bijna niet te onderscheiden zijn van teksten geschreven door mensen. De nieuwste AI-technologieën bieden echter niet alleen ondernemers, maar ook kwaadwillende hackers een kans om nieuwe verdienmodellen te ontwikkelen. Minder bekwame hackers hebben via de onderliggende taalmodellen – 'large language models' (LLM) – namelijk toegang tot een schatkamer aan programmeercodes.

Uit onderzoek is gebleken dat generatieve AI reeds gebruikt is bij verschillende vormen van cyberaanvallen. Echt gealarmeerd over deze ontwikkeling zijn de bevraagde bedrijven overigens niet; nog geen derde (29 procent) ziet vernieuwingen op het gebied van AI als substantiële bedreiging voor de cyberveiligheid van de organisatie.

Wachtwoorden kraken

'Password', '123456' en '123456789' vormen de top drie van de meest gebruikte wachtwoorden. Met de huidige technologie zijn dergelijke wachtwoorden – en eigenlijk alle wachtwoorden met een lengte van minder dan acht karakters – binnen een paar seconden gekraakt. Voor het kraken van langere exemplaren heeft de huidige software input nodig in de vorm van een lijst met (veel) voorkomende wachtwoorden. Een belangrijk verschil tussen huidige toepassingen en toepassingen gebaseerd op generatieve AI is dat laatstgenoemde nieuwe wachtwoorden kan kraken zonder enige a priori kennis. Een model kan patronen in huidige wachtwoordstructuren herkennen en op basis hiervan nieuwe wachtwoorden genereren die niet in de dataset voorkomen. In 2017 hebben onderzoekers aangetoond dat zo'n model 10.478.322 (24,2 procent) van de 43.354.871 toentertijd gelekte LinkedIn-wachtwoorden kon voorspellen zonder toegang tot de gelekte dataset.

Phishing

Door de opkomst van LLM's wordt het voor kwaadwillenden steeds eenvoudiger om phishing-berichten op te stellen zonder spellings- en grammaticafouten. Uit recent onderzoek van Darktrace blijkt dat de taalkundige complexiteit van phishing-mails sinds de lancering van de chatoplossing met 17 procent is toegenomen. Tegelijkertijd richten cybercriminelen zich steeds meer op zogenoemde spearphishing-berichten; zulke berichten zijn doorgaans goed geschreven en specifiek gericht op een individu. Cybercriminelen kunnen via social media waardevolle informatie verzamelen over een mogelijk slachtoffer. Met ChatGPT of soortgelijke tools kan de crimineel binnen enkele seconden een overtuigend en goed geschreven nepbericht versturen dat nauwelijks van echt te onderscheiden is. En nu ook stemmen kunnen worden gekloond op basis van een audiofragment van enkele seconden, krijgen kwaadwillenden nog een extra stuk gereedschap in handen om zich voor te doen als een bekende.

Malware

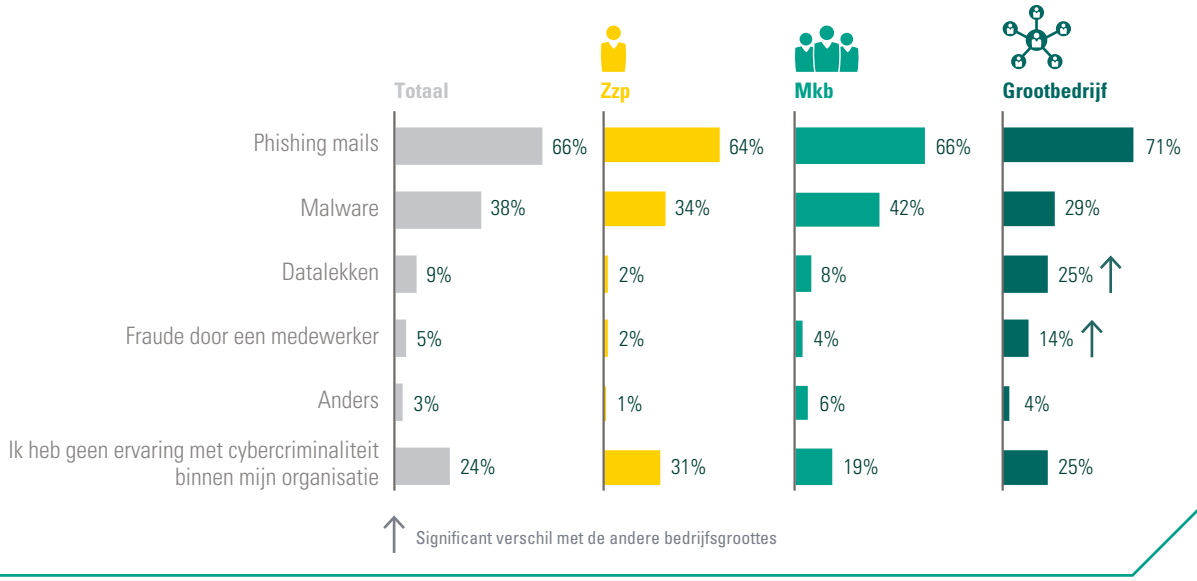
Cybercriminelen proberen handig gebruik te maken van generatieve AI bij het ontwikkelen van malware. Een veelgebruikte methode is het creëren van zogenoemde polyforme malware waarvan de onderliggende computercode constant muteert. Voor traditionele antivirussoftware is het detecteren en neutraliseren van zulke malware vrijwel onmogelijk. Een ander gevaar is dat het cybercriminelen in staat stelt om op een schaalbare manier malware te creëren, waardoor de frequentie van aanvallen waarschijnlijk zal toenemen.

Biometrische veiligheidssystemen ondermijnen

Het genereren van videobeelden en stemgeluid is een van de meest opwindende toepassingen van generatieve AI, maar tegelijkertijd een ontwikkeling die velen zorgen baart. Zo kunnen cybercriminelen met 'deepfakes' de biometrische veiligheidssystemen van apparaten en diensten ondermijnen. Een journalist wist recentelijk toegang te krijgen tot de saldo- en transactie-informatie van zijn bankaccount via een AI-versie van zijn stem, en onderzoekers van PennState University trokken de conclusie dat juist de biometrische oplossingen die 'echte' gezichten moeten herkennen veelal niet opgewassen zijn tegen de huidige deepfake-technologie.

Figuur 2. Ondernemers meest geconfronteerd met phishing

Percentage bedrijven dat te maken heeft gehad met onderstaande soorten cybercriminaliteit (n=233)



Ook met malware heeft een flink deel van de ondervraagden ervaring: 38 procent. De verspreiding van deze kwaadaardige programma's gaat gemakkelijk in een tijdperk waarin de toegang tot allerlei software en software-componenten met een paar muisklikken geregeld is. Zo worden 'open source'-componenten door kwaadwillenden gekloond en met malware geïnjecteerd, in de hoop dat ze worden gedownload en terechtkomen in software van derden (zie kader B). De schaamteloosheid van cybercriminelen is daarbij overigens opvallend. Zij gebruiken regelmatig Google-advertenties om internetgebruikers naar websites te leiden waar ogenschijnlijk legitieme programma's kunnen worden gedownload, maar die in werkelijkheid met malware zijn besmet.

KADER B | Race tegen de klok door Log4J

Robert Párhonyi, consultant bij IT-dienstverlener Incentro, belandde in een race tegen de klok toen eind 2021 een kritieke kwetsbaarheid in Log4J werd ontdekt. Het is een publiekelijk beschikbaar softwareonderdeel dat in allerlei IT-oplossingen wordt gebruikt en daardoor deel uitmaakt van het systeemlandschap van vrijwel alle bedrijven. Párhonyi: "Ik moest zo snel mogelijk alle relevante afdelingen en onze IT-partners bellen om inzicht te krijgen in de risico's voor onszelf en de klanten waarvoor we oplossingen hebben ontwikkeld. Gebruikten wij en onze partners zelf Log4J? Vervolgens was het zaak onze klanten te bellen en te bepalen wie van ons op welk moment de maatregelen zou implementeren."

Binnen enkele dagen was de inventarisatie afgerond en waren alle maatregelen genomen, maar de les is volgens Párhonyi simpel: overzicht is essentieel. Zo noemt de consultant het belang van een klantlijst inclusief de cybersecurity-contactpersonen aan klantzijde. Ook de geleverde oplossingen, de locatie waar deze worden gehost, en de afspraken die zijn gemaakt omtrent service en beheer maken idealiter deel uit van zo'n overzicht."Daar gaat veel tijd in zitten. Zulke overzichten maken we dus voortaan op een rustig moment in plaats van gehaast en onder stress."

ENISA, het Europees Agentschap voor Cyber Security, ziet een verhoogd risico op malware-aanvallen op zogenoemde 'Operational Technology'-netwerken (OT). Dit zijn de systemen die bijvoorbeeld machines in fabrieken aansturen en niet altijd de regelmatige beveiligingsupdates krijgen die zo gebruikelijk zijn in de hoek van IT. Michielen van SEQRIT, het cybersecuritymerk van netwerkspecialist Routz, maakt zich zorgen. "Tegenwoordig zijn al die machines op het internet aangesloten. OT-managers hebben niet het besef dat hackers via hun machines kunnen binnendringen en de productie kunnen platleggen.

Ransomware nog steeds prominent in Europa

Een bekende en gevreesde vorm van malware is 'ransomware', dat bestanden versleutelt en pas weer vrijgeeft op het moment dat het getroffen bedrijf losgeld heeft betaald. Hoewel het aantal ransomware-aanvallen vorig jaar wereldwijd afnam, steeg in Europa het aantal aanvallen met 83 procent. "Het is een plaag", zegt directeur Blokker van cybersecurityspecialist MMOX. Dergelijke aanvallen leiden tot flinke risico's voor de bedrijfscontinuïteit. Zo ging tandartsketen Colosseum Dental Benelux in 2022 over tot betaling nadat het in Nederland 120 filialen noodgedwongen had moeten sluiten na een ransomware-aanval. Veelal wordt gedreigd met het vrijgeven van gevoelige data, zoals persoonlijke gegevens van klanten. Maar hoewel de druk om te betalen groot is, is het vaak geen definitieve remedie. Blokker: "De kans dat ze bij je terugkomen is groot."

Datalekken kunnen het gevolg zijn van een ransomware-aanval, maar ook bijvoorbeeld doordat buitenstaanders de beschikking hebben gekregen over inloggegevens van systemen waar data worden beheerd. De grotere bedrijven in het onderzoekspanel meldden significant vaker datalekken dan de kleinere bedrijven, hoogstwaarschijnlijk omdat zij in de regel meer klantgegevens verwerken. De Autoriteit Persoonsgegevens meldt dat het aandeel datalekken veroorzaakt door cyberaanvallen is toegenomen. In 2021 betrof dat 9 procent van alle 25.000 datalekmeldingen, tegenover 5 procent het jaar daarvoor.

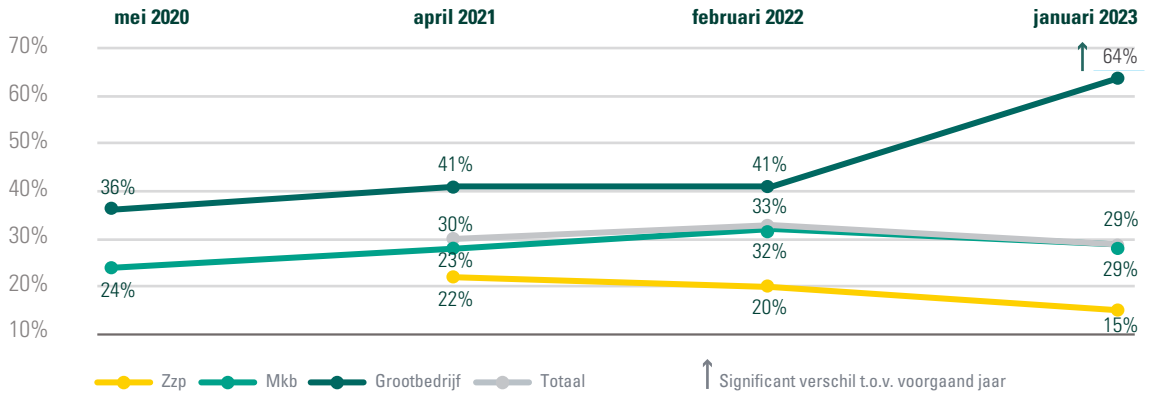
Ook fraude door medewerkers wordt significant vaker genoemd door grotere bedrijven. Dit kan onder andere gebeuren op het moment dat werknemers het bedrijf verlaten en gevoelige informatie meenemen. Er zijn ook voorbeelden van hackers die medewerkers tegen betaling proberen te bewegen om malware te verspreiden binnen het bedrijf.

Risicoperceptie kleinere bedrijven blijft achter

Terwijl het percentage ervaringsdeskundigen onder mkb'ers en zzp'ers in rap tempo toeneemt, is hun risicoperceptie juist gedaald. Deze daling is statistisch niet significant, maar de risico-inschatting van deze bedrijven loopt sterk uit de pas met de daadwerkelijke dreiging. Onder de grootste organisaties – met een jaaromzet van 10 miljoen euro of meer – laat de risicoperceptie juist een duidelijke stijging zien: achtte in 2022 nog 41 procent van de ondervraagden cybercriminaliteit een "groot" of "heel erg groot risico" voor de organisatie, het jaar erop is dit meer dan de helft (64 procent).

Figuur 3. Risicoperceptie neemt toe bij grootbedrijf, maar blijft achter bij mkb

Percentage bedrijven dat cybercriminaliteit ziet als "veel" of "heel erg veel risico" voor de organisatie (n=233)



Volgens René van Etten van cyberveiligheidsspecialist ThreadStone zijn cyberrisico's voor kleinere ondernemers ongrijpbaar. "Een brand of een inbraak kun je zien, maar een hack niet", zegt de oprichter. "En terwijl de media volop berichten over de grootste zaken, wordt het mkb-perspectief veel minder sterk belicht."

Het beperkte gevoel van urgentie bij kleinere bedrijven wordt ook herkend door Frank Breedijk. Vanuit zijn rol als CISO bij IT-dienstverlener Schuberg Philis schakelt hij met grotere bedrijven. Als 'ethisch hacker' voor de stichting Dutch Institute for Vulnerability Disclosure (DIVD) ziet hij daarnaast ook hoe het er soms in het mkb aan toegaat. "Als ik een security-issue meld bij een klein bedrijf, krijg ik regelmatig iets terug in de trant van: dankjewel, ik zal het aan de systeembeheerder melden. Alleen blijkt deze lang niet alle dagen te werken, terwijl juist haast geboden is."

Met een dergelijke houding maken bedrijven zich tot een gemakkelijk doelwit. Breedijk: "Een cyberaanval kan iedereen overkomen, maar degenen die hun beveiliging het slechtst op orde hebben zijn als eerste aan de beurt." Ook Van Etten van ThreadStone ziet het opportunisme van cybercriminelen. "Hackers struinen het internet af om gemakkelijke slachtoffers in de val te lokken. Zorg er daarom voor dat je spreekwoordelijke fiets net iets beter op slot staat dan die van de buurman."

Cybercriminelen maken dus eenvoudig een zakelijke kosten-batenanalyse. Binnendringen bij grotere, beter beveiligde bedrijven vergt steeds meer inspanning. Deze bedrijven zijn zich sterker bewust van de risico's en nemen daardoor meer verschillende maatregelen (zie kader C). Risicobewuste bedrijven kiezen bijvoorbeeld voor preventie via technologische en mensgerichte oplossingen, in combinatie met hulpverlening na een incident en een verzekering. Ook hebben grote bedrijven meer budget beschikbaar voor cyberveiligheid. De tweedeling is afgelopen jaar zelfs groter geworden, daar grote bedrijven hun cybersecuritybudgetten hebben verhoogd en kleine bedrijven deze juist sterk hebben teruggebracht. Dit blijkt uit een recent rapport van cyberverzekeraar Hiscox. "Er is sprake van een waterbed-effect", zegt Breedijk van Schuberg Philis. "Cybercriminelen verleggen hun aandacht van het grootbedrijf naar het mkb."

Kwaadwillenden volgen de weg van de minste weerstand, weet ook Wouter van Rooij, Global IT Security Director bij Leaseweb. "Cybercriminelen hoeven ook niet per se één grote klapper te maken, zoals de mannen achter de Heineken-ontvoering dat ooit probeerden." In plaats daarvan zoeken ze meerdere kleine slachtoffers waarvan de individuele opbrengsten optellen tot grote bedragen.

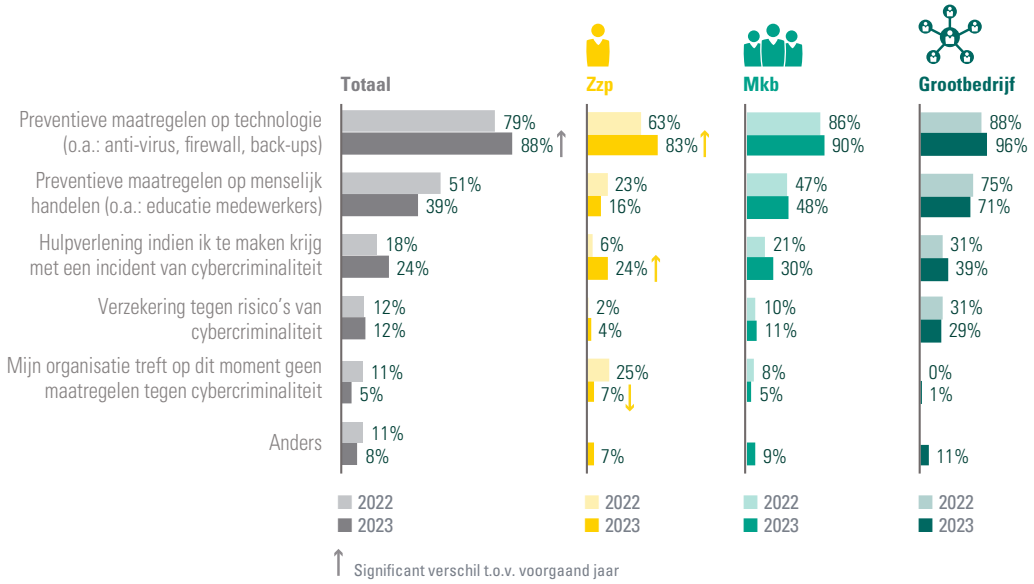
KADER C | Voorkeur voor technologische maatregelen ter preventie van cyberaanvallen

Met 95 procent neemt een groot deel van de ondervraagden maatregelen tegen cybercriminaliteit. Onder zzp'ers was een opvallende verbetering zichtbaar: liet vorig jaar nog een kwart van hen maatregelen achterwege, dit jaar was dat nog slechts 7 procent.

Het zijn vooral preventieve maatregelen waar bedrijven op inzetten, met een zwaartepunt op technologische oplossingen; bij alle drie de bedrijfsgroottes worden die het meeste genoemd. Voorbeelden zijn antivirussoftware, firewalls en het maken van back-ups.

Preventieve maatregelen over menselijke handelen staan op nummer twee, zoals het trainen van medewerkers om phishing-pogingen te herkennen en het toepassen van het vierogenprincipe bij grote betalingen. Opvallend is dat mkb-bedrijven en zzp'ers het zwaartepunt leggen bij technologische maatregelen, terwijl de grotere bedrijven een meer gebalanceerd beeld laten zien. Zij kiezen bijvoorbeeld voor preventie via technologische en mensgerichte oplossingen, in combinatie met hulpverlening na een incident en een verzekering.

Figuur 4. Grote bedrijven nemen een meer gebalanceerde set aan maatregelen
Percentage bedrijven dat onderstaande maatregelen neemt (n=233)



Een set aan verschillende maatregelen heeft volgens Van Etten van ThreadStone de voorkeur. "Je kunt niet een kastje kopen waarmee het allemaal is opgelost", vertelt de oprichter. "Het gaat om de combinatie van beleid, techniek en menselijk bewustzijn." Een groot deel van de cyberaanvallen vindt namelijk plaats door manipulatie van medewerkers. Zo gebeurt in 41 procent van de gevallen de initiële aanval via 'phishing', waarbij medewerkers bijvoorbeeld worden verleid om te klikken op een link in een e-mail of sms. Daarachter kan malware verstopt zitten, of een proces waarmee inloggegevens afhandig worden gemaakt.

Hoewel veel bedrijven zich veilig wanen, is de kans groot dat zij vroeg of laat slachtoffer worden van cybercriminaliteit. Ook het vooraf inregelen van hulp na een eventueel incident is daarom aan te raden, iets wat bijna een kwart van de respondenten doet. Van de ondervraagde organisaties heeft 12 procent een cyberverzekering. Bedrijven in risicovolle sectoren, zoals IT-bedrijven, ziekenhuizen en transportbedrijven, moeten aan strengere voorwaarden voldoen. Zij krijgen verder te maken met hogere premies en lagere maximumvergoedingen.

Toeleveringsketen onder druk

IT-bedrijven populair startpunt voor aanval

Een enkele zwakke schakel kan leiden tot substantiële schade verderop in de keten. Zo zorgde een aanval met gijzelsoftware op logistiek bedrijf Bakker in 2021 voor lege kaasschappen bij Albert Heijn. Bakker kon geen orders meer aannemen, bestellingen vinden in de magazijnen of transporten plannen. Het incident, ook wel bekend als de 'kaas-hack', begon bij een lek in Microsoft Exchange Server, een veelgebruikte mailserver voor organisaties.

Kwaadwillenden richten zich in toenemende mate op IT-leveranciers, zoals cloudbedrijven, IT-dienstverleners en softwareontwikkelaars. Naast het feit dat verstoringen in het IT-landschap van een bedrijf zowel de eigen operatie als die van ketenpartners kunnen raken, vormen kwetsbaarheden in IT-systemen ook een potentiële ingang naar een bredere set aan slachtoffers. Zulke mogelijkheden worden sinds de hack op softwareontwikkelaar SolarWinds in 2020 steeds vaker ingezet door 'statelijke actoren' (zie kader D).

"Heb je als cybercrimineel een kritieke kwetsbaarheid gevonden bij een belangrijke leverancier, dan kun je vervolgens het net sluiten rond een heleboel bedrijven tegelijk", bevestigt Van Rooij van Leaseweb. Van Rooij haalt de hack bij softwareontwikkelaar Nebu aan, waardoor zeker twee miljoen klantgegevens van Nederlanders op straat kwamen te liggen. Het softwarebedrijf bedient verschillende marktonderzoeksbureaus, die elk op hun beurt klantonderzoek doen voor tientallen andere organisaties. Hierdoor moesten onder andere de NS, telecombedrijf VodafoneZiggo en zorgverzekeraar CZ hun klanten informeren over het lekken van hun gegevens. "Dat zijn heel veel vliegen in een klap", aldus Van Rooij.

KADER D | Statelijke actoren drukken stempel op dreigingsbeeld

In de aanloop naar de oorlog in Oekraïne klonken veel gelijksoortige geluiden: dit zou een cyberoorlog worden zoals de wereld nog nooit gezien heeft. Een deel van de oorlog wordt inderdaad aan het digitale front uitgevochten, maar de 'traditionele' grondoorlog blijft dominant. Zo heeft Rusland meermaals via hacks flinke schade aan het Oekraïense elektriciteitsnet weten aan te richten, maar zijn raket- en drone-aanvallen telkens gemakkelijker en effectiever gebleken. Dat geopolitieke factoren de cyberveiligheid van een land kunnen raken, staat echter buiten kijf.

Het Russische cyberleger is sinds de invasie van Oekraïne steeds actiever betrokken bij cyberaanvallen gericht op de kritische infrastructuur in West-Europa, waaronder elektriciteit, internettoegang, drinkwatervoorziening en betalingsverkeer. De pro-Russische groep genaamd Killnet voerde begin 2023 DDos-aanvallen uit op Nederlandse ziekenhuizen en Z-CERT, een expertisecentrum gericht op cybersecurity in de zorg. De website van het Universitair Medisch Centrum Groningen lag daardoor enkele dagen plat. Ook bedrijven die op de een of andere manier Oekraïense organisaties ondersteunen, kunnen het doelwit worden van hackgroepen uit Rusland.

Statelijke actoren zoeken steeds meer hun heil in aanvallen op toeleveringsketens. De hack op softwareontwikkelaar SolarWinds in 2020 is een inmiddels berucht incident dat het startsein vormde van een rits aan soortgelijke, geopolitiek gemotiveerde cyberaanvallen. Russische staatshackers integreerden malafide code in Orion, software die wereldwijd wordt gebruikt door bedrijven om hun servers te monitoren. Hierdoor hadden kwaadwillenden lange tijd toegang tot geheime informatie van onder andere 'Fortune 500'-bedrijven en Amerikaanse overheidsinstanties.

Volgens Europees cyberagentschap ENISA zijn statelijke actoren daarnaast actief op zoek naar onontdekte zwakke plekken – zogenoemde 'zero-day vulnerabilities' – in de veelgebruikte digitale producten van onder andere Google, Microsoft, Apple en Adobe. Omdat het meestal even duurt voordat daarvoor een oplossing, of een 'patch', is gevonden en alle gebruikers de bijbehorende updates hebben uitgevoerd, is de kans groot dat kwaadwillenden in de tussentijd al verdere schade hebben kunnen aanrichten.

Vaak blijft schade voor lange tijd uit of volgt deze überhaupt niet. "Je kunt het zien als een soort offensieve verdedigingslinie", legt Van Rooij van Leaseweb uit. "Statelijke actoren dringen alvast de systemen van andere landen binnen. Mocht een geopolitiek conflict hoog oplopen, dan staan zij al opgesteld om de zaken lokaal te ontwrichten."

Toeleveringsketen onder druk

Cybercriminelen spelen ook op andere manieren in op de afhankelijkheden binnen toeleveringsketens. Het Nationaal Cyber Security Centrum (NCSC) ziet dat gijzelsoftware-aanvallen steeds vaker gepaard gaan met 'tweevoudige' of 'drievoudige afpersing'. Waar bij een 'gewone' ransomware-aanval de toegang tot gegevens of systemen wordt afgesloten en deze na betaling van losgeld weer worden vrijgegeven, voegt tweevoudige afpersing extra urgentie toe door te dreigen met publicatie van data als niet wordt betaald. Dit kan schadelijk zijn voor leveranciers, partners en klanten. Bij drievoudige afpersing worden deze derden direct in het verhaal betrokken, en krijgen ook zij een losgeldseis opgelegd.

Grote bedrijven, die automatisch samenwerken met meer partners, zijn door dergelijke praktijken kwetsbaarder. Volgens een recent rapport van het World Economic Forum (WEF) kreeg maar liefst 39 procent van de bedrijven met meer dan duizend werknemers in 2022 te maken met een cyberincident dat begon bij een leverancier, dienstverlener of partner. Onder bedrijven met minder dan duizend werknemers bedroeg dit percentage slechts een kwart.

Grote organisaties houden de cyberweerbaarheid van hun partners en leveranciers daarom kritisch tegen het licht. "Ze gaan steeds hogere eisen stellen aan hun toeleveranciers", zegt Breedijk van Schuberg Philis. "En hebben deze hun cybersecurity niet goed voor elkaar, dan doen ze geen zaken." Partijen als BitSight, Security Scorecard, RiskLedger en Hellios spelen in op deze beweging en bieden met hun oplossingen inzicht in de cyberweerbaarheid van derden.

Regelgeving zet meer bedrijven op scherp

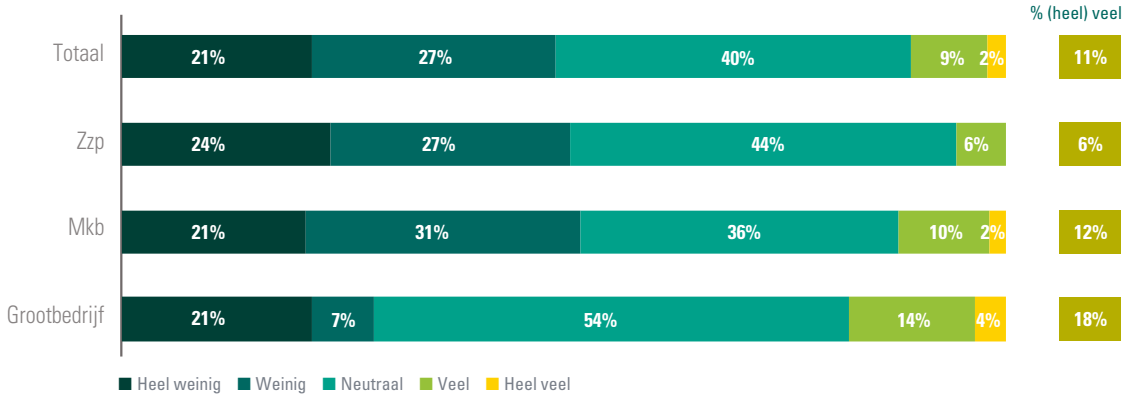
De kritische blik op ketenpartners zal nog extra worden versterkt door nieuwe Europese regelgeving op het gebied van cybersecurity. NIS2, de opvolger van de eerdere Network and Information Systems-richtlijn (NIS), spoort namelijk bedrijven aan om afspraken rond cyberveiligheid contractueel vast te leggen met hun directe leveranciers en partners. Een dergelijke benadering is volgens Blokker van MMOX geen overbodige luxe. "Degene waar is ingebroken is vaak niet degene die de meeste schade lijdt", verklaart hij.

De nieuwe richtlijn geldt voor veel meer bedrijven dan zijn voorganger (zie kader E), wat leidt tot een exponentiële toename van het aantal leveranciers dat aan de tand kan worden gevoeld. Ook organisaties op wie NIS2 niet direct van toepassing is moeten dus anticiperen op kritische vragen over hun eigen cybersecuritybeleid.

Dat lijkt geen hypothetische situatie. Een meerderheid van de beslissers beschouwt hun partners namelijk als minder weerbaar dan zijzelf, zo bericht het eerdergenoemde WEF-rapport. Dit geldt voor 54 procent van de business-leiders en maar liefst 61 procent van de cyber-leiders. Bedrijven die hun cyberveiligheid niet goed op orde hebben – en dit zijn met name kleine bedrijven – dreigen zichzelf buiten spel te zetten. Vanaf oktober 2024, wanneer de EU-lidstaten NIS2 hebben vertaald naar lokale wetten en ook boetes kunnen worden uitgedeeld aan bedrijven die hun cyberrisico's niet goed beheersen, zal dit scenario van uitsluiting nog reëler worden.

Figuur 5. Grootbedrijf heeft zich meer verdiept in NIS2

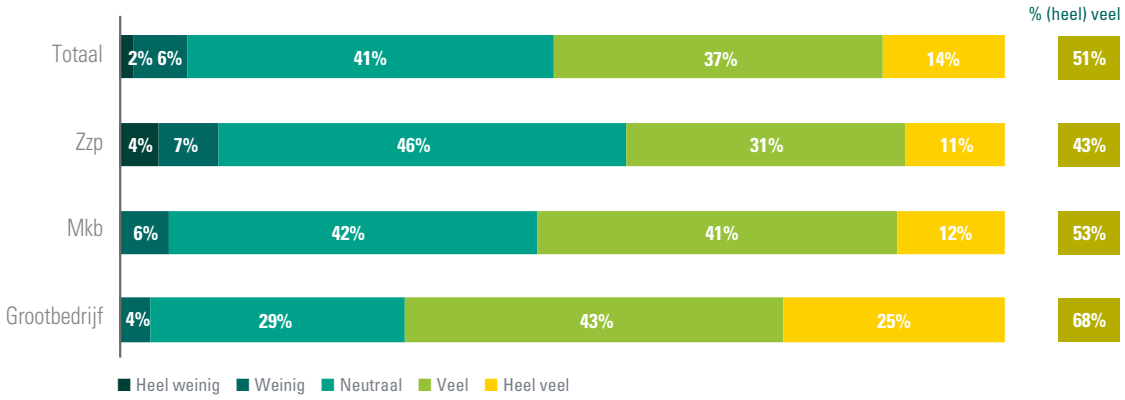
Vraagstelling: "Kunt u aangeven in hoeverre u zich heeft verdiept in de nieuwe NIS2-wetgeving en de impact hiervan op uw bedrijf?" (n=233)



Over de gehele linie blijken bedrijven zich nog niet in hoge mate te hebben verdiept in deze nieuwe regulering; slechts 11 procent van alle ondervraagden. Michielen van SEQRIT: "De urgentie is er vaak nog niet. NIS2 voelt voor veel ondernemers nog ver van hun bed omdat de wetten "pas" over anderhalf jaar van kracht zijn. Maar over een tijdje zie je allerlei publicaties langskomen en raakt iedereen in paniek. Pas dan gaat men beseffen hoeveel werk en kennis er nodig is om tijdig aan de wetgeving te kunnen voldoen." Het grootbedrijf staat er relatief gezien nog het beste voor; minder dan een derde van hen heeft zich "weinig" of zelfs "heel weinig" in de regulering verdiept, tegenover ongeveer de helft van de mkb'ers en zzp'ers.

Onderaan de streep vertrouwt een meerderheid van de bedrijven er overigens op dat zij voldoen aan wet- en regelgeving op het gebied van cyberveiligheid; binnen de mkb-doelgroep is dit 53 procent, en bij grote bedrijven bijna 70 procent.

Figuur 6. Helft van de bedrijven heeft vertrouwen dat zij aan cyberregelgeving voldoen
Vraagstelling: "Kunt u aangeven in hoeverre u er vertrouwen in heeft dat uw bedrijf voldoet aan cyberregelgeving?" (n=233)



Hoewel veel ondernemers nog onvoldoende urgentie voelen, ziet Michielen ook hoe hogere eisen vanuit de keten een positief sneeuwbaleffect kunnen veroorzaken. "Een bedrijf waarvoor wij werken besloot serieus aan de slag te gaan met cybersecurity nadat zijn eigen klant dit eiste", vertelt de consultant. "Zij hebben nu een eigen cybersecurity-afdeling en zijn ook begonnen hún leveranciers op dit vlak te bevragen."

KADER E | NIS2

NIS2 is de opvolger van de Network and Information Systems-richtlijn (NIS), die sinds 2016 zogenoemde 'essentiële bedrijven' verplicht om hun cyberweerbaarheid te vergroten. De nieuwe richtlijn voegt enkele nieuwe sectoren toe onder de definitie 'essentieel' en introduceert ook de categorie 'belangrijke bedrijven'. "Betreft het nu nog zo'n 300 bedrijven voor wie de wettelijke cybersecurityeisen gelden, bij NIS2 gaat het zeker om 5000 à 6000 bedrijven", schat Michielen van SEQRIT.

Welke bedrijven gaan iets merken van NIS2?

NIS1 - Toegevoegd onder NIS2

Essentiële sectoren	Belangrijke sectoren
Energievoorziening	Post- en koeriersdiensten
Vervoer	Afvalstoffenbeheer
Bankwezen en infrastructuur voor financiële markten	Levensmiddelenbedrijven
Gezondheidszorg	Productie-, verwerking en distributie van chemische stoffen
Digitale infrastructuur (waaronder communicatie-netwerken, datacenters en cloudaanbieders)	Productie van onder andere medische hulpmiddelen, machines en transportmiddelen
Drinkwatervoorziening	Digitale aanbieders (onlinemarktplaatsen, zoekmachines en sociale media)
Afval- en afvalwaterverwerking	Onderzoek
Overheid	
Ruimtevaart	
Beheer van IT-diensten (B2B)	

Verplicht zich aan de nieuwe wetten te houden:

Essentiële bedrijven	Belangrijke bedrijven
Hieronder vallen grote organisaties actief in een essentiële sector. Op deze bedrijven wordt proactief toezicht gehouden, dus middels audits en scans.	Hieronder vallen middelgrote organisaties actief in een essentiële- of belangrijke sector. Op deze bedrijven wordt reactief toezicht gehouden, wat betekent dat er enkel wordt ingegrepen als er aanwijzingen zijn dat iets niet goed gaat.
'Groot' houdt in: meer dan 250 werknemers of; een netto omzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro.	'Middelgroot' houdt in: minimaal 50 werknemers of; een jaaromzet of balanstotaal van meer dan 10 miljoen euro.

Indirect geraakt:

Leveranciers van essentiële- en belangrijke bedrijven

De bedrijven 'in scope' worden geacht kritisch naar de cyberveiligheid van hun leveranciers te kijken. Leveranciers krijgen dus via hun klanten te maken met de nieuwe wetten, ook als zij zelf niet in de categorie 'essentieel' of 'belangrijk' vallen. Dit betekent dat het speelveld ook voor kleinere bedrijven kan veranderen.

Wat zijn de verplichtingen?

De vertaalslag van deze vernieuwde richtlijn naar concrete wetten zal per EU-lidstaat worden gemaakt.
Wel is al duidelijk dat twee zaken centraal zullen staan: zorgplicht en meldplicht.

De **zorgplicht** houdt onder andere in dat de bedrijfsnetwerken adequaat moeten worden gemonitord, medewerkers moeten worden opgeleid en minimale beveiligingseisen zullen gelden – bijvoorbeeld 'tweefactorauthenticatie', waarbij iemand bij het inloggen op een apparaat nog een extra code dient in te voeren die is ontvangen op een ander apparaat.

De **meldplicht** betekent dat naast datalekken ook andere cyberincidenten zoals ransomware-aanvallen moeten worden gerapporteerd.

Bedrijven die wel onder de richtlijn vallen, maar niet aan de bijbehorende wetten voldoen, riskeren een boete. Deze kan oplopen tot 10 miljoen euro of 2 procent van de wereldwijde jaaromzet. Verantwoordelijken binnen een organisatie kunnen daarnaast persoonlijk aansprakelijk worden gesteld voor het niet naleven van de richtlijn.

Cybersecurity als 'boardroom-topic'

Een dergelijke integrale benadering is tegenwoordig essentieel. Met de afhankelijkheid van verschillende cloud-diensten, open source-softwarecomponenten waar ontwikkelaars gretig gebruik van maken en nieuwe technologie die in rap tempo wordt ingebed in de bedrijfsvoering, groeit het aanvalsoppervlak. Ook worden IT-landschappen steeds complexer. "We maken met zijn allen een enorme IT-ontwikkeling mee", vertelt Breedijk van Schuberg Philis. "Functionaliteit wordt op functionaliteit gestapeld, maar zonder de aandacht die nodig is om ook op securityniveau bij te blijven." Ook Blokker van MMOX ziet deze ontwikkeling. "Bedrijven digitaliseren sneller dan dat zij hun risico-management op orde brengen. Dit zet ze op achterstand ten opzichte van de hackersgemeenschap."

Het is daarom belangrijk dat cybersecurity overal in de bedrijfsvoering wordt ingebed. Veiligheid en commercie kunnen namelijk op gespannen voet met elkaar staan.
Kiest een bedrijf er bijvoorbeeld voor om zo snel mogelijk naar de markt te gaan met een nieuwe functionaliteit of nieuwe app, dan kan dit maar zo ten koste gaan van de cyberveiligheid van de IT-oplossing. Onder hoge tijdsdruk is de kans immers groter dat onvoldoende wordt getest op veiligheid, of dat opgemerkte kwetsbaarheden bewust worden 'geparkeerd' ten faveure van een snelle markt-
introductie. Ook kost het tijd en geld om applicaties veilig te houden; iets waarop bedrijven, zolang er nog niets is gebeurd, eerder geneigd zijn te bezuinigen.

Gelukkig wordt de interne samenwerking steeds intensiever, zo blijkt uit het onderzoek van het World Economic Forum. Meer dan de helft van de cybersecurity-beslissers voert minimaal eens per maand overleg met de directie. Wel zien de onderzoekers ruimte voor verbetering, bijvoorbeeld in een betere vertaalslag van geïdentificeerde veiligheidsissues naar concrete risico's voor de bedrijfsvoering.

Andersom moet ook de bedrijfstop meer verantwoordelijkheid accepteren voor cyberveiligheid, zo is de consensus onder de bevraagde experts. Van Etten van Threadstone: "Cyberaanvallen vormen een operationeel risico dat je niet enkel bij de IT'er kan neerleggen. De directie moet ervoor zorgen dat het onderwerp in de gehele organisatie wordt vertaald naar maatregelen." Wat dat betreft ziet Michielen van SEQRIT een positieve trend. "Waar ik in het verleden vooral met de IT-managers en CISO's sprak, zit nu ook de directeur of vergelijkbare stakeholder aan tafel. Deze kan dan een afweging maken: wat kost cyberveiligheid mij, en wat levert het mij op?"

De baten van een solide cybersecuritybeleid – of de kosten van de afwezigheid daarvan – worden in ieder geval steeds evidenter. Bedrijven beschermen daarmee namelijk niet alleen hun eigen operatie en financiën, maar leggen ook de basis voor een goede relatie met hun partners op de lange termijn.

Verhoog de cybersecurity van uw onderneming

Veilig ondernemen met ABN AMRO

Het aantal incidenten stijgt en 1 op de 3 ondernemers wordt zelfs slachtoffer van cybercriminaliteit. Omdat cybercriminelen maar een kleine ingang nodig hebben, is het belangrijk om passende maatregelen op het gebied van cybersecurity te treffen. Om ondernemers en hun medewerkers te helpen, bieden wij diverse cybersecurity-oplossingen en downloads aan waarmee u zich kan wapenen tegen cybercrime.

Veelgekozen oplossingen

Online Cyberscan van ThreadStone

- Eenmalige, supersnelle en veilige Cyberscan
- Inclusief risicorapport en persoonlijk gesprek
- Voor mkb'ers die inzicht willen in online kwetsbaarheden

Bekijk de online Cyberscan

Cyber Veilig & Zeker van MMOX

- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen
- Voor midden- en grootbedrijf dat ontzorgd wil worden op cyberrisico

Bekijk Cyber Veilig & Zeker

Cyberverzekering

- Bescherm uw bedrijf met onze cyberverzekering
- Krijg uitgebreide dekking
- 24/7 hulp van onze specialisten
- Voor ABN AMRO zakelijke klanten die zich willen indekken tegen cyberschade

Alles over onze verzekering

Vrijblijvend cybergesprek

- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen
- Voor ondernemers die willen weten hoe zij ervoor staan

Vrijblijvend cybergesprek plannen

Tips & tools

Cyberwebinars

Om ondernemers en medewerkers in diverse sectoren te helpen cybercrime te herkennen en de kans erop te verlagen, organiseerden onze cyberspecialisten meerdere webinars:

- De wereld van cybercriminaliteit
- Leer risico's herkennen

Kijk het webinar

Cyber Response Plan

Een Cyber Response Plan helpt u in het geval van cybercrime incidenten op te sporen, te reageren en schade te herstellen.

- Stel zelf uw eigen Cyber Response Plan op
- Bereid uw bedrijf en medewerkers voor op een cyberaanval

Bekijk de download

Third-Party Risk Management Checklist

Third-Party Risk Management helpt u om veiligheidsrisico's die ontstaan als u samenwerkt met partners en leveranciers in kaart te brengen.

- Check mogelijke cyberrisico's
- Deel de checklist met uw klanten en leveranciers voor meer veiligheid

Bekijk de download

Whitepaper over Employee Awareness

Cybercriminelen komen (vaak) via medewerkers binnen in uw digitale systemen. Houd uw medewerkers scherp met onze whitepaper.

- Ontdek hoe u uw employee awareness kunt verhogen
- Lees over manieren om uw medewerkers bewuster van cybercrime te maken

Bekijk de download

Alle artikelen over cybersecurity

Abonneren op de nieuwsbrief

Waarom helpt ABN AMRO bij meer dan bankieren?

ABN AMRO wil ondernemers graag helpen met de groei van hun onderneming. Daar heeft u als zakelijke klant natuurlijk meer voor nodig dan alleen bankproducten. Daarom bieden wij toekomstbestendige oplossingen aan die u helpen veiliger, duurzamer en slimmer te ondernemen. Hiermee doet ABN AMRO meer dan alleen bankieren.

Colofon

Dit is een uitgave van ABN AMRO.

Contact
Julia Krauwer, sector banker Technologie, Media & Telecom (TMT)
(06) 22 61 34 32 of julia.krauwer@nl.abnamro.com

Amad Khan, sectoranalist Technologie, Media & Telecom (TMT)
(06) 15 96 45 54 of julia.krauwer@nl.abnamro.com

Auteurs
Julia Krauwer en Amad Khan, ABN AMRO Sector Expertise

Interviews
Matthijs Blokker, MMOX
Frank Breedijk, Schuberg Philis
René van Etten, ThreadStone
Erik Michielen, SEQRIT
Robert Párhonyi, Incentro
Wouter van Rooij, Leaseweb

Eindredactie
Bendert Zevenbergen

Illustraties en opmaak
Kollerie Reklame-advies & Promotions

Fotoverantwoording
shutterstock.com

Distributie
abnamro.nl/tmt

abnamro.nl