Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker

ABN·AMRO

Inhoudsopgave

Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker

Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval, zo blijkt uit een enquête onder 895 organisaties door ABN AMRO in samenwerking met onderzoeksbureau MWM2. Hoewel de nadelige gevolgen van cyberaanvallen veelvuldig in het nieuws komen, moet een ondernemer vaak eerst schade hebben geleden voordat deze de risico's erkent. De schade van een aanval beperkt zich echter vaak niet tot het bedrijf dat is gehackt. Een al te optimistische risico-inschatting kan daarmee de hele keten in gevaar brengen. Nu er nieuwe Europese wetgeving in de maak is, moeten ondernemers samen met hun klanten en leveranciers de zaken snel op orde krijgen.

Onder het grootbedrijf, met een jaaromzet van minimaal 25 miljoen, werd maar liefst 86 procent van de ondernemingen aangevallen. In het midden- en kleinbedrijf (mkb) zag 71 procent zich verleden jaar geconfronteerd met een aanval, onder zelfstandigen was dit 55 procent. Helaas schatten die laatste twee groepen de risico's van cybercriminaliteit relatief laag in.

Ondernemers blijken de risico's pas vooral te onderkennen op het moment dat een aanval tot schade heeft geleid. Te denken valt aan financiële kosten voor het herstel van systemen, gederfde inkomsten door stilstand van het bedrijf, of reputatieschade door gelekte klantgegevens. Uit onderzoek van verzekeraar **Hiscox** blijkt dat Nederland wereldwijd op nummer twee staat wat betreft hoogste financiële schade door cybercriminaliteit.

Ondertussen veranderen de aanvalsmethoden van cybercriminelen in rap tempo. Zo is phishing nog steeds een populaire – en door ondernemers gevreesde – methode om binnen te komen bij bedrijven, maar bedienen criminelen of bijvoorbeeld kwaadwillende overheden zich ook massaal van kant-en-klare inloggegevens om ongemerkt toegang te krijgen tot bedrijfssystemen. Eenmaal binnen leidt dat bijvoorbeeld tot de installatie van schadelijke software. Van de bedrijven zag 37 procent zijn systemen al eens geïnfecteerd met malware; bij 19 procent van de bedrijven gebeurde dit (onder andere) vorig jaar. Met gijzelsoftware heeft 26 procent van de bedrijven ervaring, waarvan 19 procentpunt vorig jaar. Ook datalekken zijn een reëel risico. Meer dan een kwart van de bedrijven verloor al eens vertrouwelijke gegevens; bij 15 procent gebeurde dit in de afgelopen twaalf maanden.

Meer dan de helft van de bedrijven ziet vernieuwingen op het gebied van kunstmatige intelligentie, oftewel 'artificial intelligence' (AI), als bedreiging voor de cyberveiligheid van de organisatie. Vorig jaar was dit nog geen kwart. De risicoperceptie is het sterkst bij de grootste bedrijven, iets wat mogelijk wordt gevoed door spectaculaire berichten die recent in de media verschenen. Zo maakte een financieel medewerker van een multinational in Hong Kong meer dan **25 miljoen dollar** over naar fraudeurs, nadat hij in een videovergadering terechtkwam met een deepfakeversie van de CFO en andere collega's. Bij de Nederlandse onlinebank Bunq werd een soortgelijke poging gewaagd met een AI-kloon van topman Ali Niknam.

Om de cyberweerbaarheid in Europa te verbeteren wordt in oktober 2024 een nieuwe richtlijn van kracht: NIS2, de opvolger van de eerdere Network and Information Systems-richtlijn (NIS). Het dwingt organisaties uit zeventien sectoren om onder andere de cyberweerbaarheid van toeleveranciers en klanten kritisch onder de loep te nemen. Hoewel Nederland vertraging oploopt met de implementatie van de richtlijn, worden binnenlandse bedrijven al opgeschrikt door kritische vragen vanuit Duitse en Belgische klanten waar het vormgeven van nationale wetten wel volgens planning verloopt.

Bijna driekwart (72 procent) van de respondenten uit het grootbedrijf bevraagt zijn eigen klanten, leveranciers en partners al "zeer regelmatig" of "regelmatig" over cybersecurity; 66 procent zegt dat zijzelf van hun ketenpartners ook dergelijke vragen krijgen. Bij de mkb-respondenten liggen deze percentages lager, met respectievelijk 52 en 37 procent. Ook de mate waarin concrete afspraken worden gemaakt met ketenpartners, ligt in het grootbedrijf stukken hoger dan in het mkb.

Maarten Roerink, CEO van cybersecuritydienstverlener MMOX erkent het belang van een benadering ver buiten de bedrijfsmuren. "Als onze klanten gehackt worden, gaat dat heel vaak via-via. Soms zijn ze zelf het doelwit, soms worden kwetsbaarheden in hun netwerken gebruikt om door te dringen tot de netwerken en data van partners. De aloude vraag 'wat valt er nou bij mijn bedrijf te halen?' is dan ook niet meer relevant."

Ondernemers erkennen cyberrisico vooral na schade

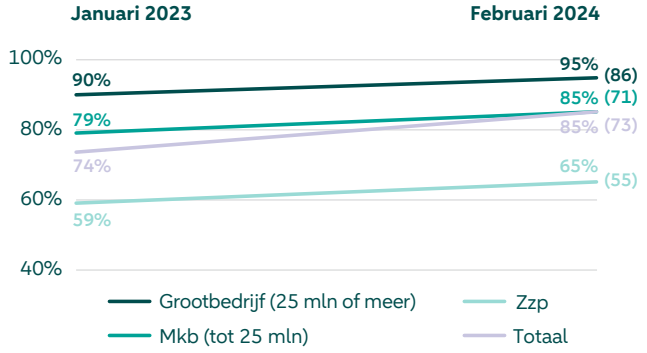
Een overgrote meerderheid van de bedrijven heeft al eens te maken gehad met een cyberaanval. Toch zijn ondernemers geneigd de bijbehorende risico's te onderschatten. Vooral op het moment dat een organisatie schade heeft geleden, bijvoorbeeld in de vorm van gederfde inkomsten of financiële kosten voor systeemherstel, worden de risico's erkend.

Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval, zo blijkt uit een enquête door ABN AMRO onder 895 organisaties.

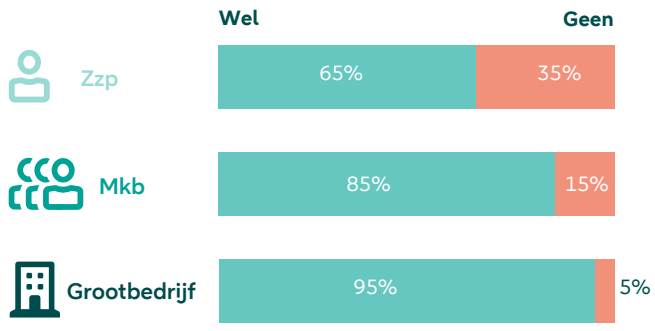
Onder het grootbedrijf, met een jaaromzet van minimaal 25 miljoen, ligt dit percentage met 86 procent het hoogst. In het midden- en kleinbedrijf (mkb) zag 71 procent zich verleden jaar geconfronteerd met een aanval. Meer dan de helft van de zelfstandigen (55 procent) was het doelwit. Aan het onderzoek werkten 232 grote bedrijven mee, 524 bedrijven uit het mkb en 139 zelfstandigen.

Figuur 1: Een meerderheid van de bedrijven is al eens geconfronteerd met cybercriminaliteit

Percentage bedrijven dat aangeeft weleens te maken te hebben gehad met cybercriminaliteit. Het percentage tussen haakjes geeft het aandeel bedrijven weer waarbij dit (in ieder geval) in de afgelopen twaalf maanden is gebeurd.



Ervaring met cybercriminaliteit

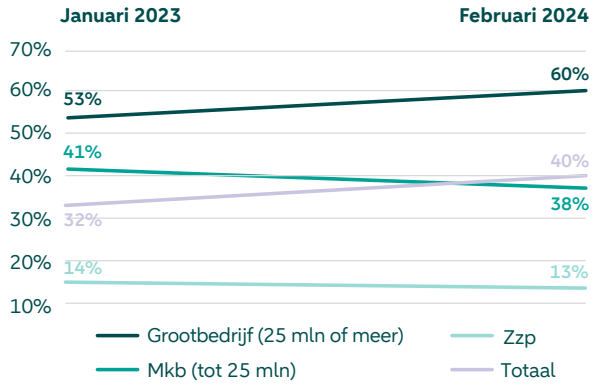


Bron: ABN AMRO en MWM2

De kans is inmiddels bijzonder groot dat een bedrijf ooit het doelwit wordt van een cyberaanval; bij 95 procent van het grootbedrijf is dit al eens het geval geweest, tegenover 85 procent van de mkb'ers en 65 procent van de zzp'ers. Hoewel dit percentage jaarlijks – logischerwijs – oploopt voor alle bedrijfsgroottes, geldt dit voor de risicoperceptie niet over de hele linie. In zowel het mkb- als zzp-segment is het percentage ondernemingen dat cybercriminaliteit als "veel" of "heel erg veel risico" ziet voor de organisatie zelfs iets afgenomen. Respectievelijk 38 en 13 procent schat de risico's dit jaar hoog in, zo blijkt. Dit geldt voor een veel hoger percentage van de ondernemingen in het groot bedrijf: 60 procent, tegenover 53 vorig jaar.

Figuur 2: Risicoperceptie is enkel gestegen bij ondernemers in het grootbedrijf

Percentage bedrijven dat aangeeft cybercriminaliteit als "(heel) veel risico" te zien voor de organisatie.



Vraag: In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie?
Bron: ABN AMRO en MWM2

Inmiddels hebben cyberaanvallen bij 59 procent van het grootbedrijf en 43 procent van het mkb tot schade geleid, zoals financiële kosten voor het herstel van systemen, gederfde inkomsten door stilstand van het bedrijf of reputatieschade door gelekte klantgegevens. Dit komt beduidend minder voor in de zzp-populatie, waar slechts 6 procent aangeeft ooit schade te hebben ondervonden door een cyberaanval.

Hogere risico-inschatting na schade

Uit nadere analyse blijkt dat de risico's gemiddeld hoger worden ingeschat door bedrijven die daadwerkelijk al eens schade hebben geleden door een aanval. Van hen ziet 63 procent cybercriminaliteit als (heel) veel risico voor de organisatie. Van de bedrijven die nog geen schade hebben geleden door een aanval, schaart slechts 26 procent zich achter deze risico-inschatting. Dit is vergelijkbaar met de risico-inschatting van de bedrijven die überhaupt nog nooit zijn aangevallen.

Toch ziet CEO Roerink van MMOX dat ook ervaringen van soortgelijke bedrijven kunnen dienen als 'wake-up call'. "Ondernemers die van hun buurman op het bedrijventerrein horen over een vervelende cyberaanval, zijn eerder geneigd om zich te gaan oriënteren op oplossingen. Ze lopen niet direct weg met een contract, maar zijn zich in ieder geval al meer bewust van de risico's."

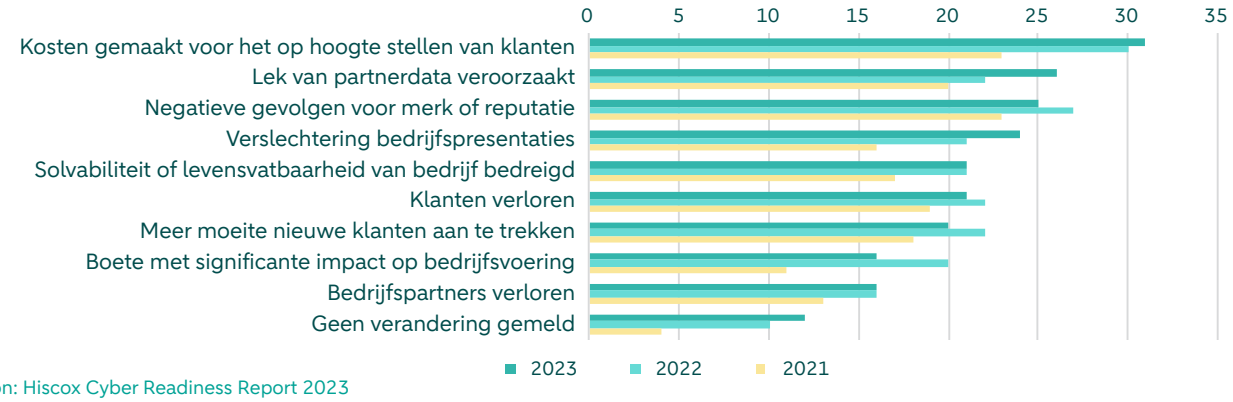
Aanval kan grote gevolgen hebben

Dat de gevolgen van een aanval groot kunnen zijn, blijkt uit verschillende recente voorbeelden. DP World, een grote Australische havenexploitant, moest eind 2023 na een cyberaanval vier havens **sluiten**. De systemen werden van het internet afgesloten, waardoor vrachtwagens geen vracht meer konden lossen of ophalen in de havens. Dertigduizend containers strandden ter plaatse. Pas na een week was de operatie weer op het oude niveau. Eerder dit jaar werd ook de Duitse batterijfabrikant Varta **getroffen** door een cyberaanval. Het bedrijf zag zich genoodzaakt om vijf fabrieken stil te leggen. Omdat ook de financiële administratie was geraakt, werd de publicatie van het jaarverslag uitgesteld. Varta's aandelenprijs ging met bijna vijf procent omlaag. Wereldwijd heeft een **kwart** van de industriële bedrijven zijn operatie wel eens moeten stopzetten vanwege een cyberaanval.

Overigens is er geen garantie dat de alertheid na een geslaagde aanval van blijvende aard is, zegt Arwi van der Sluijs, algemeen directeur van cybersecuritydienstverlener NFIR. "Een half jaar na een aanval worden we dan gebeld met de vraag of de maatregelen 'echt zo strikt' moeten." NFIR richt zich op de bovenkant van het mkb, zorginstellingen, gemeentes en provinciale instellingen.

In Nederland bedroegen de mediane kosten door cyberaanvallen in 2023 zo'n 21.000 dollar per bedrijf, zo rapporteert verzekeraar **Hiscox**. Hiermee staat ons land wereldwijd op nummer twee wat betreft hoogste financiële schade door cybercriminaliteit, achter het Verenigd Koninkrijk en vlak voor de Verenigde Staten.

Figuur 3: Klantcommunicatie en lekken van partnerdata meest genoemd als gevolg cyberaanval
Percentage bedrijven dat een bepaald gevolg heeft genoemd



Bron: Hiscox Cyber Readiness Report 2023

Kader A | Schade door cyberaanvallen komt in vele vormen

Verzekeraar Hiscox werpt in zijn jaarlijks uitkomende **Cyber Readiness Report** licht op de verschillende negatieve gevolgen die bedrijven hebben ervaren door een cyberaanval. Het meest gemeld in 2023 waren kosten voor het op de hoogte stellen van klanten (31 procent van de getroffen bedrijven), gevolgd door gelekte data van partners (26 procent).

Opvallend is dat dit laatste percentage ten opzichte van het vorige jaar met maar liefst vier procentpunt is toegenomen – een bevestiging van het feit dat cyberrisico's zich niet enkel beperken tot de eigen bedrijfsvoering. Bij 16 procent van de bedrijven heeft dit soort incidenten zelfs tot het verlies van partners geleid.

Een kwart van de organisaties meldde negatieve gevolgen voor het merk of de bedrijfsreputatie; bij ongeveer een vijfde liepen klanten weg, of werden moeilijkheden ervaren met het aantrekken van nieuwe klanten. Ook zagen veel bedrijven hun prestaties verslechteren (24 procent); bij 21 procent was er zelfs sprake van een bedreiging van de levensvatbaarheid van de organisatie.

Dreigingslandschap evolueert razendsnel

De aanvalsmethoden van cybercriminelen veranderen in rap tempo. Zo is phishing nog steeds een populaire methode om binnen te komen bij bedrijven, maar bedienen aanvallers zich ook massaal van kant-en-klare inloggegevens om ongemerkt toegang te krijgen tot bedrijfssystemen. Olie op het vuur vormt kunstmatige intelligentie, dat de gereedschapskist voor cyberaanvallen op vernuftige wijze uitbreidt.

Phishing werd door alle bedrijfsgroottes het meest gerapporteerd; ongeveer de helft zag zich in 2023 geconfronteerd met phishingmails of -smsjes. Hierbij worden berichten verstuurd die de ontvanger aanzetten tot een – zo blijkt later – schadelijke actie. Dit varieert van klikken op een link die een automatische download van schadelijke software in gang zet tot het openen van een nagemaakte inlogpagina waar gegevens met kwaadwillende derden worden gedeeld.

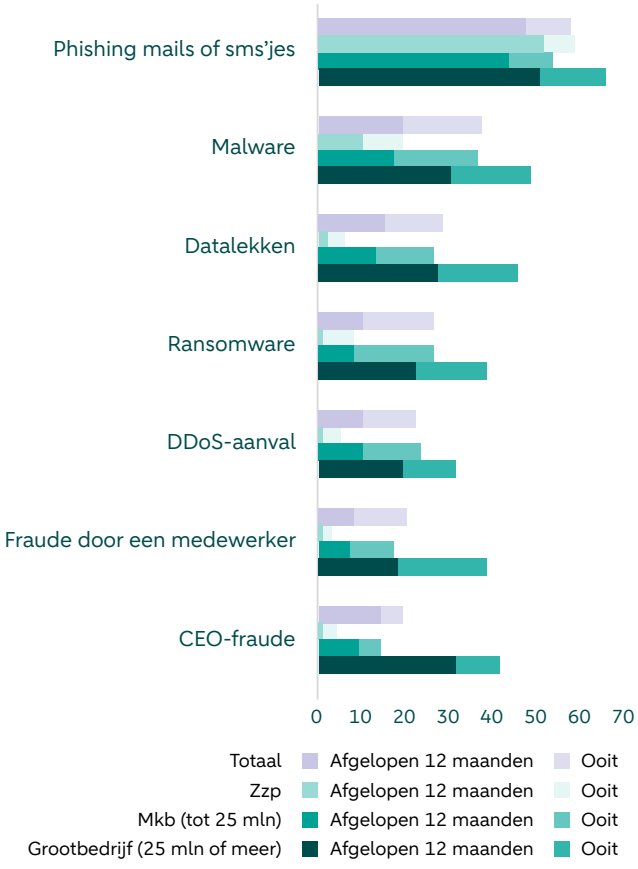
Zorgvuldig onderzoek voor gerichte aanval

CEO-fraude is een specifieke vorm van phishing, ook wel bekend als 'whaling'. Oplichters doen zich hierbij voor als CEO of lid van hoger management en benaderen vanuit diens naam medewerkers. De gebruikte communicatiekanalen lopen uiteen van e-mail tot Whatsapp en zelfs telefoongesprekken. Het gaat meestal om dringende verzoeken om geld over te maken, facturen te betalen of gevoelige informatie te verstrekken. De aanvallers hebben dan vaak al zorgvuldig onderzoek gedaan. Allereerst om de relevante contactgegevens te achterhalen, maar ook om bijvoorbeeld de communicatiestijl van de manager goed te kunnen nabootsen. Maar liefst 33 procent van de respondenten uit het grootbedrijf kreeg vorig jaar een dergelijke aanval voor de kiezen.

Phishing is een populaire manier voor kwaadwillenden om een cyberaanval te starten, maar kan pas tot schade leiden als de ontvanger daadwerkelijk heeft 'gehapt'. Daarom starten aanvallers hun reis door het IT-landschap van hun doelwit steeds vaker door simpelweg in een van de systemen in te loggen met gebruikersnaam en wachtwoord. In 2023 begon bijna een derde (30 procent) van de cyberaanvallen op deze manier, terwijl dit aandeel in 2022 nog slechts 16 procent betrof – aldus IBM X-Force (zie kader B). Deze inloggegevens kunnen kant-en-klaar worden ingekocht, of met grof rekengeweld worden geraden. Het is een onopvallende manier om binnen te komen, die de indringer een hoop tijd geeft om te zoeken naar verdere kwetsbaarheden en informatie.

Figuur 4: Bedrijven krijgen te maken met een mix aan aanvallen

Percentage bedrijven dat aangeeft met onderstaande vormen van cybercriminaliteit te maken hebben gehad, zowel in bredere zin als specifiek in de afgelopen twaalf maanden



Vraag:
1. Met welke van de volgende vormen van cybercriminaliteit heeft u binnen uw organisatie wel eens te maken gehad?
2. Wat heeft in de afgelopen 12 maanden plaatsgevonden?

Bron: ABN AMRO en MWM2

Kader B | Aanvallers komen steeds vaker binnen via gestolen of geraden accountinformatie

Cybercriminelen beginnen hun aanval steeds vaker door op bedrijfssystemen in te loggen met gebruikersnaam en wachtwoord. Hiermee wordt deze strategie inmiddels even vaak toegepast als phishing, dat juist aan populariteit inboette als initiële aanvalsmethode; in 2022 was phishing nog in maar liefst 41 procent van de gevallen het startpunt van een cyberaanval.

Uit deze verschuiving blijkt dat het voor cybercriminelen wel heel gemakkelijk is geworden om toegang te krijgen tot combinaties van gebruikersnamen en wachtwoorden. Daar hoeft in veel gevallen dus zelfs geen losse phishingcampagne meer voor te worden opgetuigd, waarbij slechts een klein percentage van de ontvangers de 'gewenste' actie zal uitvoeren. Voor kant-en-klare datasets betalen kwaadwillenden dan ook graag grof geld. Dit is een van de redenen dat criminele groeperingen die zich eerder toelegden op ransomware, hun focus verleggen naar de creatie van malware die speciaal gemaakt is om informatie te stelen.

Onopgemerkt binnenkomen

Aanvallers kunnen op verschillende manieren aan die inloggegevens komen. Soms weten zij de hand te leggen op kant-en-klare lijsten met gelekte gebruikersaccounts, die veelal via het 'dark web' worden aangeboden. Zij proberen met deze gegevens vervolgens ook op bedrijfssystemen in te loggen, en maken daarmee dankbaar gebruik van het feit dat mensen voor verschillende accounts vaak dezelfde combinaties van gebruikersnamen en wachtwoorden aanhouden. In andere gevallen ontbreken de wachtwoorden op de gelekte lijsten en worden de wachtwoorden met behulp van enorme rekenkracht geraden. Deze laatste werkwijze vormde ook het startpunt van een Chinese cyberspionage-operatie bij de Nederlandse chipfabrikant NXP, die startte in 2017 maar tot 2020 onopgemerkt bleef. De hackers hadden hierdoor lange tijd toegang tot intellectueel eigendom van de fabrikant, zoals chipontwerpen.

Top-3 van startpunten cyberaanval in 2023

Uitbuiten van kwetsbaarheden

Ook kwetsbaarheden in met het internet verbonden programma's waren in 2023 een populair startpunt van cyberaanvallen. Dergelijke achterdeurtjes kunnen worden misbruikt om systemen binnen te dringen, nog voordat er een oplossing of 'patch' voor beschikbaar is. Misbruik vond onder andere plaats via nieuw gevonden **kwetsbaarheden** in de besturingssystemen Windows, iOS en Android, en webbrowsers Chrome en Safari. Vaak zijn cybercriminelen er als de kippen bij; in 2023 werden bij een **kwart** van deze 'zero-days' al binnen een dag pogingen ondernomen om deze uit te buiten.

Combinatie van maatregelen belangrijk

Deze top drie van 'initial access vectors' onderstreept het belang voor bedrijven om een combinatie van maatregelen toe te passen. Zo kan het aantal succesvolle phishing-pogingen naar beneden worden gebracht door medewerkers te trainen in het herkennen ervan, en is het toepassen van 'multifactor-authenticatie' belangrijk om te voorkomen dat gelekte of buitgemaakte inloggegevens worden misbruikt. Bij deze authenticatiemethode worden een of meerdere extra checks gedaan, bijvoorbeeld via een bevestiging in een mobiele app of een code die per SMS wordt toegezonden. Misbruik van kwetsbaarheden in programma's en apparaten benadrukt het belang van regelmatige software-updates en een goede check op het cyberveiligheidsbeleid van IT-leveranciers.

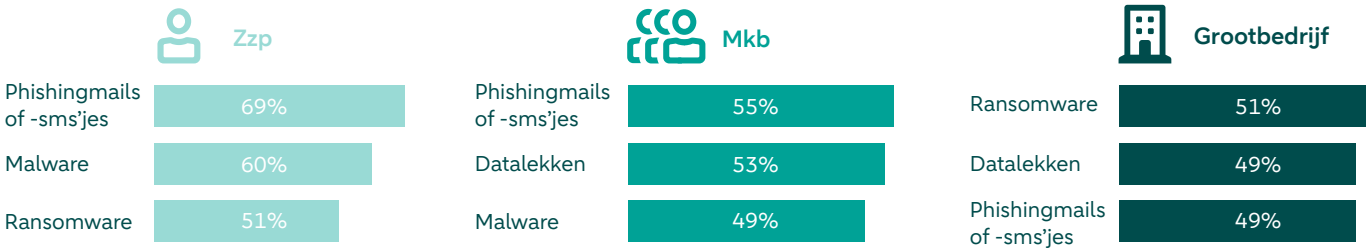
Recordbedrag buitgemaakt met gijzelsoftware

Waar phishing en ogenschijnlijk legitieme logins veelal het startpunt vormen van een aanval, zijn het andere instrumenten die worden ingezet op het moment dat het slachtoffer dieper in de fuik is beland. Zo is de installatie van malware een prominente strategie van cybercriminelen om hun uiteindelijk doel te bereiken. Deze kwaadaardige software kan bijvoorbeeld dienen om data te stelen, diensten te verstoren, of te spioneren. Bijna een kwart (23 procent) van de ondervraagden kreeg hier in 2023 mee te maken.

Het grootbedrijf werd het vaakst slachtoffer (32 procent), gevolgd door mkb (19 procent) en de zzp'ers (16 procent).

De meest ingezette vorm van malware is 'ransomware', dat systemen blokkeert en data versleutelt totdat de getroffen partij overgaat tot het betalen van losgeld. Het staat bij zowel het grootbedrijf als de zzp-gemeenschap in de top drie van meest gevreesde cyberaanvallen. In het mkb haalt ransomware de top drie niet, maar wordt malware in bredere zin wel genoemd.

Figuur 5: Phishing meest gevreesd door kleinere ondernemers, ransomware eerste zorg van grootbedrijf
De top-3 van soorten cybercriminaliteit waarover bedrijven zich de meeste zorgen maken



Vraag: Over welke maakt u zich het meest zorgen voor uw organisatie voor de toekomst? Kies uw top 3.
Bron: ABN AMRO en MWM2

Deze gijzelsoftware blijkt grootschaliger te worden ingezet dan ooit; in 2023 werden wereldwijd 4399 ransomware-aanvallen geregistreerd. Samen legden slachtoffers een recordbedrag van 1,1 miljard dollar neer – bijna een verdubbeling ten opzichte van 2022, toen deze vorm van cybercriminaliteit even op zijn retour leek. Het relatief bescheiden bedrag van 567 miljoen dollar in 2022 blijkt nu een uitzondering te zijn geweest in een verder eenduidige trend.

Hoewel de stijging in aanvallen en opgehaald losgeld groot is, blijkt juist een kleiner percentage van de slachtoffers daadwerkelijk te betalen. Waar dat in 2019 en 2020 zo tussen de 70 en 80 procent lag, was dit percentage in het vierde kwartaal van 2023 gedaald naar 29 procent. Het in 2023 betaalde bedrag kan dan ook grotendeels worden verklaard door een focus van cybercriminelen op bedrijven die zich absoluut geen verstoringen in hun systemen kunnen veroorloven en daarnaast in staat zijn het losgeld op te hoesten. Driekwart van het totaalbedrag vloeit voort uit betalingen van meer dan een miljoen dollar. Van der Sluijs van NFIR: "Kleinere bedrijven zijn minder bereid om te betalen, ze hebben het er simpelweg niet voor over. Dat ze daardoor bepaalde data verliezen, accepteren ze."

Eind vorig jaar werd ook Tunstall Healthcare het slachtoffer van ransomware. Het bedrijf is gespecialiseerd in oplossingen die zorg op afstand mogelijk maken en produceert onder andere draagbare noodknoppen voor ouderen. Deze gebruiken het systeem om snel hulp te kunnen krijgen bij bijvoorbeeld een valpartij, maar hun meldingen kwamen door de hack niet meer door bij de meldkamer. Met de hulp van een extern cybersecuritybedrijf kon het systeem binnen enkele dagen weer worden hersteld; in de tussentijd werd cliënten geadviseerd om te allen tijde een mobiele telefoon bij zich te dragen.

Reputatierisico door gelekte klantgegevens

Datalekken worden gevreesd door zowel grootbedrijf als mkb. Binnen deze segmenten kregen respectievelijk 45 procent en 26 procent van de ondervraagde bedrijven met een dergelijk incident te maken. Er kleven stevige reputatierisico's aan, bijvoorbeeld wanneer vertrouwelijke klantgegevens op straat komen te liggen. Op basis van data over 2022 stelt de Autoriteit Persoonsgegevens dat het aantal datalekken is gestabiliseerd, maar de ernst ervan is toegenomen. In dat jaar hebben de drie grootste cyberaanvallen in de zorg er bijvoorbeeld voor gezorgd dat medische gegevens van zo'n 900.000 patiënten in verkeerde handen zijn gevallen.

"Ga ervan uit dat je persoonlijke gegevens al eens gelekt zijn, of dat dit nog gaat gebeuren", waarschuwt de privacywaakhond in zijn rapport. Recente voorbeelden zijn er dan ook legio. Zo kreeg parkeerapp EasyPark te maken met een datalek nadat de systemen van het

bedrijf waren gehackt door cybercriminelen. Daarbij zijn niet alleen namen, telefoonnummers en adressen van klanten gelekt, maar ook gecodeerde wachtwoorden. Juweliersketen Brandfield zette de persoonsgegevens van 60.000 klanten in de etalage door een slecht beveiligde cloudomgeving. Eind 2023 werd ook de inmiddels failliete winkelketen Sprinter Sports het slachtoffer van een cyberaanval waarbij klantgegevens zijn buitgemaakt. De getroffen klanten kunnen te maken krijgen met onder andere identiteitsfraude of gepersonaliseerde phishing-pogingen.

Manipulatie wordt verfijnder door AI

Meer dan de helft van de bedrijven ziet vernieuwingen op het gebied van kunstmatige intelligentie, oftewel 'artificial intelligence' (AI), als bedreiging voor de cyberveiligheid van de organisatie. Vorig jaar was dit nog geen kwart. De risicoperceptie is het sterkst bij de grootste bedrijven.

AI lijkt vooral op het gebied van 'social engineering' de aanvalskracht te verhogen. Hierbij worden mensen gemanipuleerd om bijvoorbeeld vertrouwelijke informatie te delen of een anderszins schadelijke actie uit te voeren. Met AI kan deze manipulatie nog slinkser en overtuigender plaatsvinden. Zo maakt generatieve AI het nu wel heel gemakkelijk om phishing-mails te creëren. Deze vorm van AI is in staat om op basis van enkele instructies zelf teksten te schrijven – grammaticaal correct, zonder spelfouten en in een taal naar keuze. Volgens IBM X-Force daalt de ontwikkeltijd van een phishing-mail hierdoor van zestien uur naar vijf minuten.

Ook interactieve gesprekken kunnen nu aan AI-modellen worden uitbesteed. In een automatische chat kunnen bijvoorbeeld inloggegevens worden ontfutseld of betalingen in gang worden gezet. Door toepassing van 'deepfake'-technologie, waarbij beeld- of geluidsmateriaal wordt gecreëerd dat niet van echt te onderscheiden is, kunnen kwaadwillenden hun slachtoffer doen geloven dat ze met iemand anders van doen hebben. In Hong Kong maakte een financieel medewerker van een multinational meer dan 25 miljoen dollar over naar fraudeurs, nadat hij in een videovergadering terechtkwam met een deepfake-versie van de CFO en andere collega's. In oktober vorig jaar werd bij de Nederlandse onlinebank Bunq een soortgelijke poging ondernomen, toen een medewerker werd uitgenodigd voor een videogesprek met – zo bleek later – een AI-kloon van topman Ali Niknam. In een LinkedIn-bericht noemt Niknam de kloon "overtuigend".

Volgens het Britse National Cyber Security Centre (NCSC) zullen alle soorten aanvallers profiteren van deze nieuwe mogelijkheden op het gebied van social engineering, van geavanceerde staatshackers tot de minder capabele cybercriminelen. Ook het automatisch scannen van bedrijfsdata op waarde wordt voor alle kwaadwillenden gemakkelijker, waardoor de schade door datalekken de komende jaren waarschijnlijk zal groeien.

AI maakt capabele aanvallers nog sterker

Generatieve AI wordt ook toegepast om malware te schrijven. De Britten schatten in dat vooral de reeds zeer capabele aanvallers hiervan zullen profiteren. Staatshackers die bijvoorbeeld al grote datasets met malware tot hun beschikking hebben, kunnen hiermee AI-modellen trainen om nieuwe schadelijke software te maken die de huidige beveiligingssystemen niet kunnen detecteren.

Het NCSC stipt aan dat de ontwikkeling van malware vooralsnog ook menselijke expertise vergt – iets wat volgens hen eveneens geldt voor 'lateral movement', waarbij indringers overspringen van het ene naar het andere systeem. Dit betekent dat minder professionele hackers niet ineens op alle fronten exponentieel slagvaardiger worden door AI. "Het kan wel een steuntje in de rug vormen", stelt Roerink van MMOX. "Beginnende hackers kunnen zo eerder tot kwaadaardige codes komen."

Kader C | AI als wapen tegen cybercriminaliteit

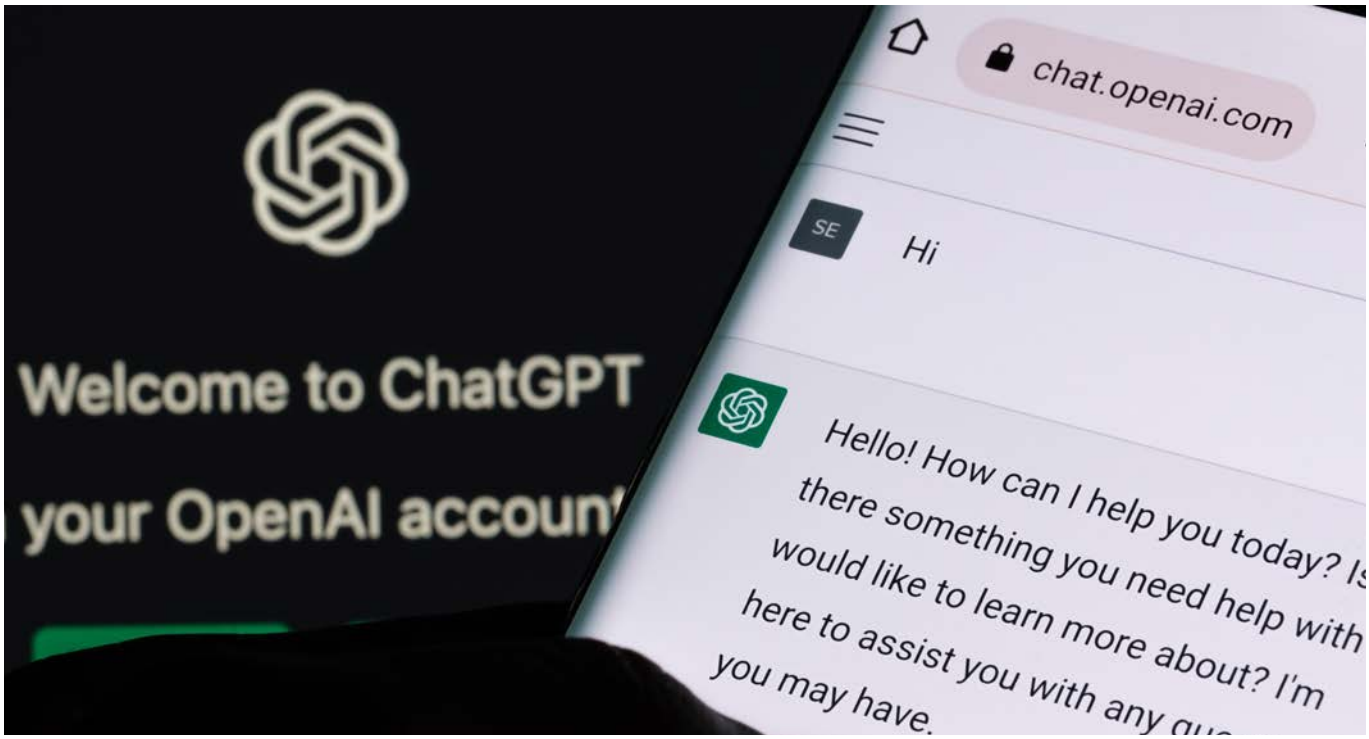
AI kan ook ten behoeve van cyberveiligheid worden gebruikt. “Het zijn altijd de boefjes die als eerste een bepaalde technologie omarmen, maar het duurt nooit lang voordat ook de verdediging ermee aan de slag gaat”, zegt Van der Sluijs van NFIR. Zo kan AI helpen om nieuwe patronen te identificeren die duiden op verdachte activiteit in een netwerk. Waar het identificeren van zulke patronen voorheen gebeurde door handmatig grote hoeveelheden data te bestuderen en bureauonderzoek te doen, kan dit nu grotendeels automatisch. “Sterker nog: dank zij AI kunnen we incidenten gaan voorspellen.

De huidige dynamiek krijgt overigens steeds meer weg van een wapenwedloop. In een wereld waarin door AI gegenereerde malware en phishing-mails een feit zijn, moeten beveiligingssystemen op hun beurt deze nieuwe dreigingen leren herkennen. Dat kan ook middels AI. Wel moet het onderliggende model dan genoeg voorbeelden hebben gezien van deze nieuwe generatie boosdoeners. Goedwillende bedrijven zetten daarom eerst generatieve AI in om malware en phishing-mails te schrijven, en gebruiken deze vervolgens om een effectief herkenningsmodel mee te trainen

Datalekken door chatbots

Bedrijven die zelf gebruikmaken van slimme chatbots op basis van generatieve AI, lopen het risico dat medewerkers in deze gesprekken vertrouwelijke informatie delen. Samsung riep het gebruik van generatieve AI-tools door medewerkers een halt toe nadat was gebleken dat een van hen een stuk broncode had ingevoerd in ChatGPT in de hoop dat de chatbot met een oplossing kon komen voor een fout in de code. Ook kwamen er transcripten van interne meetings in de gesprekken terecht.

Op deze manier kan gevoelige data niet alleen weglekken naar de AI-leverancier, maar kan ongewild ook informatie met andere gebruikers worden gedeeld. In maart 2023 rapporteerden meerdere ChatGPT-gebruikers dat zij de onderwerpen uit de chathistorie van andere gebruikers konden zien in hun eigen account. Daarnaast kunnen gevoerde gesprekken weer als trainingsdata worden gebruikt om het AI-model te verfijnen, en juist die trainingsdata blijken niet altijd goed vergrendeld te zijn. Eind vorig jaar brachten Google-onderzoekers naar buiten hoe zij ChatGPT van concurrent OpenAI hadden verleid tot het prijsgeven van trainingsdata. Het risico op datalekken via chatbots is daarmee reëel.



© Ascannio / Shutterstock.com

Beperkt bewustzijn nieuwe wetgeving maakt kwetsbaar

Om de cyberweerbaarheid in Europa te verbeteren, wordt in oktober 2024 een nieuwe wet van kracht: NIS2, de opvolger van de eerdere Network and Information Systems-richtlijn (NIS). Het dwingt organisaties om onder andere de cyberweerbaarheid van toeleveranciers en klanten kritisch onder de loep te nemen. Vooral kleinere bedrijven zijn nog niet voorbereid op kritische vragen uit de keten – iets wat ze klanten kan kosten.

De wet omvat een set aan regels die primair gericht is op bedrijven waarvan een verstoring brede maatschappelijke impact kan hebben. Zowel de Europese energie-infrastructuur als het spoornetwerk zijn bijvoorbeeld het doelwit van Russische staatshackers. Waar de focus van NIS zes sectoren omvatte, waaronder de energievoorziening, digitale infrastructuur en gezondheidszorg, reikt opvolger NIS2 veel verder. Ook levensmiddelenbedrijven, overheid en chemische industrie vallen nu bijvoorbeeld onder de nieuwe wet. In totaal gaat het om 10.432 Nederlandse bedrijven die aan de nieuwe regels moeten voldoen, verspreid over zeventien sectoren (zie kader D).

Bedrijven in de relevante sectoren zijn straks onder andere verplicht om basisveiligheidsmaatregelen toe te passen, waaronder het gebruik van sterke wachtwoorden en het uitvoeren van software-updates. Ook moeten zij de continuïteit van de organisatie na een ernstige aanval kunnen garanderen, bijvoorbeeld via back-ups en crisismanagement. Daarnaast moeten zij zich registreren en zijn zij verplicht om bij de toezichthouder melding te maken van cyberincidenten in hun bedrijf. Het gaat om bestaande nationale toezichthouders die per sector kunnen verschillen.

Kader D | Scope van- en verplichtingen onder NIS2

Welke sectoren vallen direct onder NIS2?

Reeds gereguleerd onder NIS1 | Toegevoegd onder NIS2

Sectoren bijlage 1	Sectoren bijlage 2
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 hulp-middelen, machines en transportmiddelen
Drinkwatervoorziening	Digitale aanbieders (onlinemarktplaatsen, zoekmachines en sociale media)
Afval- en afvalwaterverwerking	Onderzoek
Overheid	
Ruimtevaart	
Beheer van IT-diensten (B2B)	

Welke bedrijven moeten zich aan de nieuwe wetten houden?

Essentiële bedrijven	Belangrijke bedrijven
Hieronder vallen **grote** organisaties actief in een van de sectoren onder 'bijlage 1'. Op deze bedrijven wordt proactief toezicht gehouden, dus middels audits en scans.	Hieronder vallen **grote** organisaties actief in een van de sectoren onder 'bijlage 2' en **middelgrote** organisaties actief in een van de sectoren onder 'bijlage 1' of 'bijlage 2'. 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 en balanstotaal van meer dan 10 miljoen euro.

***Kleinere bedrijven** vallen in principe niet onder de NIS2-richtlijn, maar kunnen wel individueel kunnen aangewezen op basis van een risicobeoordeling door het ministerie dat verantwoordelijk is voor de desbetreffende sector.*

Welke bedrijven worden 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.

Aan welke verplichtingen moeten bedrijven onder NIS2 voldoen?

De vertaalslag van deze vernieuwde richtlijn naar concrete wetten wordt per EU-lidstaat gemaakt. Twee zaken staan daarin centraal: **zorgplicht**, **meldplicht** en **registratieplicht**.

Zorgplicht verwijst naar de verantwoordelijkheid van organisaties om passende en proportionele maatregelen te nemen om de beveiliging van hun netwerk- en informatiesystemen te waarborgen. Volgens het **Digital Trust Center** gaat ten minste om:

- Een risicoanalyse en beveiliging van informatiesystemen
- Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets
- Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen
- Incidentenbehandeling
- Basiscyberhygiëne en trainingen op het gebied van cyberbeveiliging
- Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op - en bekendmaking van kwetsbaarheden
- Beveiliging van de toeleverancierskеten
- Beleid en procedures over het gebruik van cryptografie en encryptie
- Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen
- Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen

De **meldplicht** betekent dat naast datalekken ook andere cyberincidenten zoals ransomwareaanvallenmoeten worden gerapporteerd.

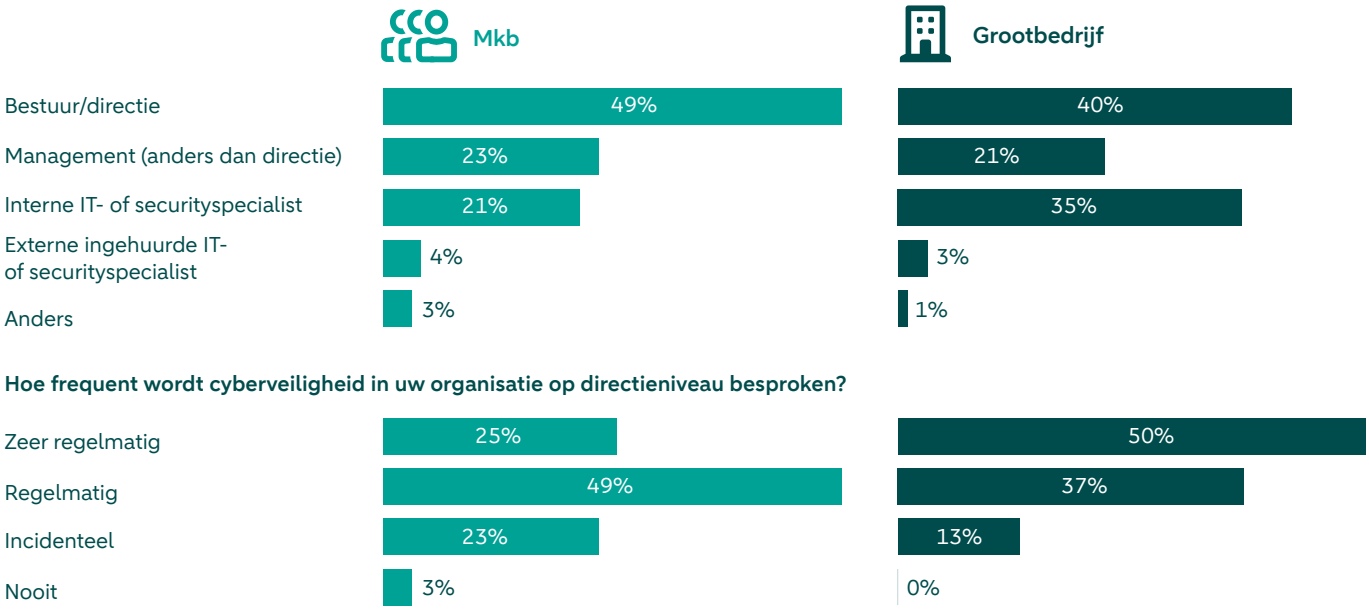
Volgens de **registratieplicht** moeten bedrijven die vallen onder de NIS2-richtlijn zich registreren bij het Nationaal Cyber Security Centrum (NCSC).

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.

Directie nog niet optimaal betrokken bij cyberveiligheid

De eindverantwoordelijkheid voor cyberveiligheid legt NIS2 op directieniveau neer; als deze haar verplichtingen onder de nieuwe wet niet nakomt, kunnen individuele directieleden zelfs persoonlijk aansprakelijk worden gesteld. Het grootbedrijf heeft daar echter nog een slag te maken; bij slechts 40 procent van deze ondervraagden is de directie al de eindverantwoordelijke op het gebied van cybersecurity; bij bijna evenveel bedrijven (35 procent) ligt die rol bij een interne IT- of securityspecialist. Wel bespreekt de helft van de grote bedrijven cyberveiligheid "zeer regelmatig" op directieniveau en door meer dan een derde (37 procent) "regelmatig".

Figuur 6: Directie moet steviger aan het stuur om te kunnen voldoen aan NIS2



Bron: ABN AMRO en MWM2

Volgens Van der Sluijs van NFIR valt er nog een kloof te dichten tussen de directie enerzijds en de IT- en securityexperts anderzijds. Zo lukt het de specialisten lang niet altijd om de urgentie van bepaalde maatregelen over te brengen. “Ze moeten het niet alleen over de technische oplossing hebben, maar kunnen beter spreken in termen van concrete risico’s voor het bedrijf. Anders bestaat de kans dat een goed security-initiatief wordt afgeschoten puur op basis van de kosten.” Andersom verkeren veel directies in de onjuiste veronderstelling dat de IT- en securityafdelingen met een beperkt budget volledig ‘in control’ kunnen zijn. “Als de IT-medewerkers na een cyberaanval dan het verwijt krijgen dat ze een steek hebben laten vallen, is dat heel pijnlijk.”

In vergelijking met het grootbedrijf blijken de mkb-directies al iets steviger aan het stuur te zitten – mogelijk vanwege de beperktere schaal van deze bedrijven. De helft van de mkb-bedrijven (49 procent) ziet de directie als eindverantwoordelijk voor cyberveiligheid. Overigens wordt het onderwerp minder vaak op directieniveau besproken dan in het grootbedrijf; een kwart doet dit “zeer regelmatig” en ongeveer de helft “regelmatig”.

Hoewel eigenaarschap op directieniveau essentieel is voor beter beveiligde bedrijven, brengt de NIS2-verplichting ook een nieuw soort risico met zich mee. “Ik voorzie een situatie waarin bedrijven in extreme mate gaan sturen op compliance, om maar te voorkomen dat individuele directie- en bestuursleden aansprakelijk worden gesteld voor cyberincidenten”, zegt Daan Hoogendijk, programmadirecteur van Samen Digitaal Veilig. Het platform, een samenwerkingsverband van grote brancheorganisaties, helpt bedrijven met informatie en oplossingen op het gebied van digitale veiligheid. “Er wordt dan eerder een papieren werkelijkheid gecreëerd dan dat men in de echte wereld bezig is om de cyberweerbaarheid naar een hoger plan te tillen. Het is belangrijk dat bedrijven dat risico erkennen.”

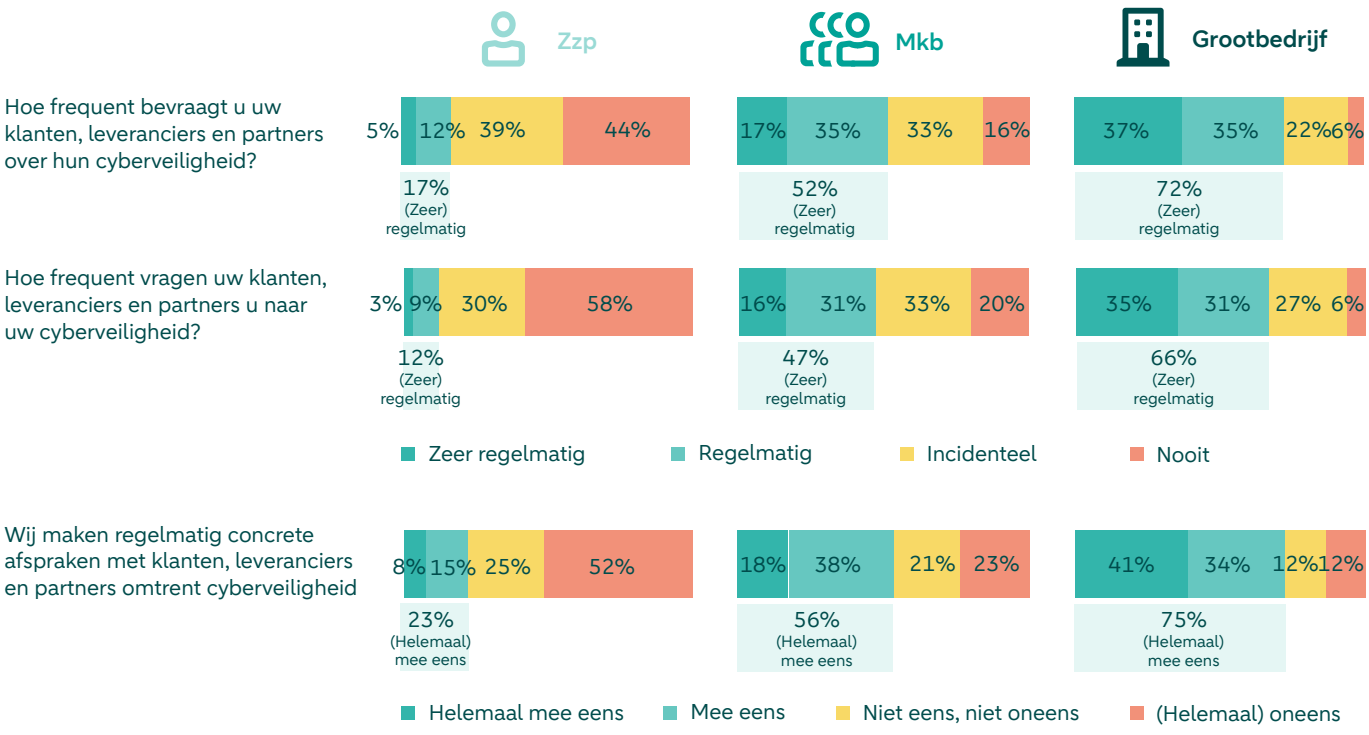
Ook mkb moet zich voorbereiden op vragen vanuit de keten

De nieuwe wet schrijft voor dat bedrijven ook de cyberrisico’s in beeld moeten hebben vanuit hun eigen toeleveringsketen, en dat afspraken rond cyberveiligheid contractueel moeten worden vastgelegd met deze ketenpartners. Dit is volgens Roerink van MMOX geen overbodige luxe. “Als onze klanten gehackt worden, gaat dat heel vaak via-via. Soms zijn ze zelf het doelwit, en soms worden kwetsbaarheden in hun netwerken gebruikt om door te dringen tot de netwerken en data van partners. De aloude vraag ‘wat valt er nou bij mijn bedrijf te halen?’ is dan ook niet meer relevant.”

Bijna driekwart (72 procent) van de respondenten uit het grootbedrijf bevraagt zijn eigen klanten, leveranciers en partners hierover al “zeer regelmatig” of “regelmatig”; 66 procent zegt dat zijzelf van hun ketenpartners ook dergelijke vragen krijgen. Bij de mkb-respondenten liggen deze percentages lager, met respectievelijk 52 en 47 procent. Ook de mate waarin concrete afspraken worden gemaakt met ketenpartners, verschilt per bedrijfsgrootte. Van de respondenten uit het grootbedrijf doet 75 procent dit, tegenover 56 procent van het mkb.

Toch is het een realiteit waar ook de kleinere bedrijven rekening mee moeten zullen houden. Zo legde een grote supermarktketen bij al zijn Nederlandse toeleveranciers alvast het dringende verzoek neer om hun beleid op het vlak van cyberveiligheid toe te lichten, vertelt Hoogendijk van Samen Digitaal Veilig. “De boodschap luidde: ofwel jullie laten een certificaat zien, ofwel we zetten de samenwerking stop. Het gros van deze foodbedrijven heeft helaas nog te weinig focus op cybersecurity.” Het is volgens Hoogendijk exemplarisch voor de houding van het gros van de mkb-bedrijven. Ze zijn veelal afwachtend, en andere prioriteiten zitten serieuze stappen in de weg.

Figuur 7: Hoe groter de organisatie, hoe prominenter cyberveiligheid terugkomt als gespreksonderwerp met klanten, leveranciers en partners



Bron: ABN AMRO en MWM2

Risico op verlies van Europese klanten

Hoewel NIS2 een Europese wet is, werken verschillende landen met verschillende snelheden. Zo zijn Duitsland en België al bijna klaar voor de nationale implementatie, maar heeft de Nederlandse overheid aangegeven de deadline van 17 oktober hoogstwaarschijnlijk niet te gaan halen. De consultatie, waarbij marktpartijen hun feedback op de wetvoorstellen kunnen geven, is al een paar keer doorgeschoven en de benodigde nationale toezichthouders zijn nog niet volledig opgelijnd. Hiermee loopt Nederland achter op zijn grootste handelspartners; Duitsland legt de laatste hand aan de wetteksten, en België presenteert binnenkort haar wetteksten ter goedkeuring.

Dit betekent voor Nederlandse bedrijven echter geen uitstel; niet alleen omdat de voorbereidingen tijdrovend kunnen zijn, maar ook omdat klanten elders in Europa van hun Nederlandse leveranciers NIS2-compliance zullen eisen. Kan deze niet worden gegarandeerd, dan riskeren deze leveranciers hun Europese klanten te verliezen. Grote bedragen staan hiermee op het spel. Volgens het Centraal Bureau voor de Statistiek (CBS) exporteerde Nederland in 2023 voor zo’n 500 miljard euro aan goederen binnen de Europese Unie, waarvan 241 miljard naar Duitsland en België (zie kader E)

Kader E | Export naar Duitsland en België mogelijk onder druk

Nederland heeft sterke economische banden met zijn buurlanden. Voor Duitse en Belgische bedrijven zijn onder andere de Nederlandse industrie en agrovoedingsproducenten belangrijke toeleveranciers. Deze toeleveranciers moeten ondanks de lokale vertraging in de NIS2-implementatie rekening houden met kritische vragen omtrent cyberveiligheid vanuit hun Duitse en Belgische klanten.

Duitsland is voor Nederland de belangrijkste exportbestemming, met een totale waarde van **165,3 miljard euro** in 2023. Naar België bedroeg de goederenexport 75,9 miljard euro. Het gaat in het bijzonder om chemische producten en industriële (half)fabricaten, machines, apparaten en vervoersmiddelen, en agrarische- en voedingsproducten.

Categorie	Exportwaarde van Nederland naar Duitsland en België (2023), in euro's
Chemische producten en industriële (half) fabricaten	54 miljard
Machines, apparaten en vervoersmiddelen	43 miljard
Agrarische- en voedingsproducten	40 miljard

Cyberweerbaarheid kunnen aantonen

Vanuit de Duitse cultuur van formaliteit en strikte naleving van regels, is de kans groot dat toeleveringsketens inderdaad kritisch onder de loep worden genomen – ongeacht of de NIS2-wetten in Nederland al van kracht zijn. Om succesvol te zijn en te blijven in Duitsland, is het essentieel dat Nederlandse ondernemingen niet alleen vaart zetten achter hun NIS2-voorbereidingen, maar ook een open en effectieve communicatielijn onderhouden over hun compliance-inspanningen. "Zorg dat je op zijn minst kunt aantonen, bijvoorbeeld met een certificaat, dat je investeert in de weerbaarheid van je organisatie", zegt Hoogendijk daarover.

Roerink onderschrijft dit vanuit zijn eigen ervaring. "We zien dat bedrijven op zoek zijn naar een stempel om naar hun partners te kunnen aantonen dat ze compliant zijn. Een ISO27001- of Cyber Essentials-certificering helpt dan. Sommige ondernemers laten zich ook certificeren om concurrentievoordeel te behalen."

Omdat een dergelijk certificeringstraject veel voeten in de aarde heeft, hebben brancheorganisaties samen met specialisten en bedrijven een nieuw keurmerk ontwikkeld speciaal voor het mkb. Het zogenoemde NIS2 Quality Mark is beschikbaar via het platform van Samen Digitaal Veilig en bestaat er in verschillende niveaus. Zo kunnen ook kleinere organisaties hun cyberweerbaarheid aantoonbaar opkrikken zonder zich standaard aan een zware ISO-certificering te hoeven committeren.

Rennen voorafgaand aan implementatie

Hoewel er dus beweging in de markt is, gebeurt er bij de meeste mkb-bedrijven volgens Hoogendijk "heel weinig" en gaat wat er gebeurt "tergend traag". Hoogendijk: "Ik vrees dat het de maanden voorafgaand aan de implementatie van NIS2 rennen wordt voor iedereen. Dat hebben we ook gezien bij de invoering van de AVG." Slechts 38 procent van de ondervraagde mkb-bedrijven heeft zich al "heel veel" of "veel" in de NIS2-wetgeving verdiept, tegenover 58 procent uit het grootbedrijf.

Toch kijkt de programmadirecteur met optimisme naar de nieuwe wet. "Uiteindelijk wordt de ketenbenadering hierdoor de standaard", blikt Hoogendijk vooruit. "En ik verwacht dat binnen een jaar of drie ook het mkb zijn cyberhygiëne op orde heeft." Hij verwijst naar een set aan basisveiligheidsmaatregelen die elk bedrijf standaard zou moeten toepassen, waaronder het gebruik van sterke wachtwoorden en het uitvoeren van software-updates. "Vergelijk het met je deur op slot doen, dat is ook een routine die je elke dag automatisch toepast." Van de ondervraagde organisaties uit het grootbedrijf zegt 40 procent deze maatregelen al volledig toe te passen; in het mkb en onder zzp'ers bedraagt dit percentage ongeveer een kwart.

Maatregelen steeds meer gericht op mensen

Van de set aan maatregelen die bedrijven kunnen nemen om hun cyberweerbaarheid te vergroten, krijgen de maatregelen gericht op menselijke kwetsbaarheden steeds meer aandacht. Daarnaast zijn met name ondernemers in het grootbedrijf geneigd om steeds meer budget uit te trekken voor cybersecurity, voornamelijk gedreven door de toegenomen dreiging.

Het gros van de ondervraagden treft maatregelen tegen cybercriminaliteit. Onder zzp'ers is dit percentage echter een stuk lager (82 procent) dan onder de respondenten uit het mkb en grootbedrijf (respectievelijk 95 en 97 procent). Preventieve maatregelen op technologische kwetsbaarheden zijn, in lijn met de resultaten uit eerdere jaren, onder alle bedrijfsgroottes het meest populair. Voorbeelden hiervan zijn de installatie van virusscanners, het versleutelen van gegevens en het toepassen van firewalls.

Vinger aan de pols blijft noodzakelijk

Ook als dergelijke maatregelen worden toegepast, blijft een vinger aan de pols noodzakelijk. Hackers wisten praktisch gelijktijdig binnen te komen bij 22 Deense energiebedrijven via een kritieke kwetsbaarheid in de firewalls van Zyxel, apparaten die juist zijn bedoeld om kwaadaardig verkeer uit het bedrijfsnetwerk te weren. Als de indringers niet eerder waren ontdekt, hadden zij via deze gecoördineerde cyberaanval controle kunnen krijgen over een deel van de vitale infrastructuur van Denemarken.

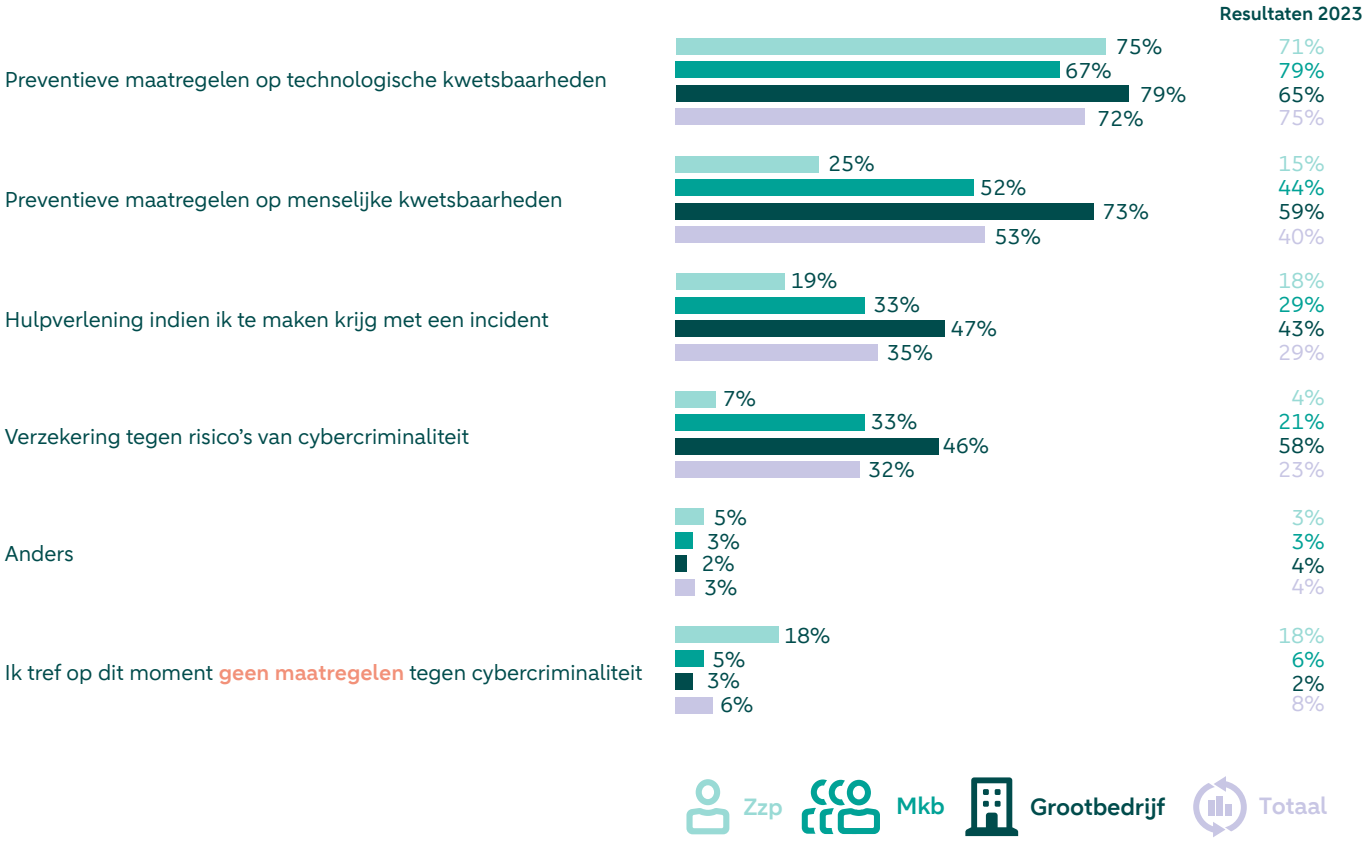
Hoewel relatief vroeg in het aanvalsproces kon worden ingegrepen, hadden diverse energiebedrijven duidelijke steken laten vallen in hun beveiliging. Volgens een rapport van het Deense cybersecuritycentrum voor vitale infrastructuur hadden diverse bedrijven nagelaten beveiligingsupdates van de firewalls te installeren. Zij waren bijvoorbeeld in de onterechte veronderstelling dat hun IT-leverancier de updates zou installeren, of hadden updates afgehouden omdat de leverancier installatiekosten in rekening zou brengen. Andere bedrijven wisten simpelweg niet dat zij het Zyxel-apparaat in hun netwerk hadden.

Toenemende focus op menselijke kwetsbaarheden

Menselijke kwetsbaarheden krijgen meer aandacht; het percentage bedrijven dat op dit vlak maatregelen neemt, steeg van 40 procent in 2022 naar 53 procent vorig jaar. Voorbeelden zijn trainingen om medewerkers de basishygiëne op het gebied van cybersecurity bij te brengen, of het simuleren van phishing-aanvallen om de alertheid op dergelijke mails te vergroten. "Zulke oefeningen moet je dan wel maandelijks laten terugkeren", adviseert Van der Sluijs van NFIR. "Koppel er ook een toets aan om de kennis omtrent cyberveiligheid te monitoren, en laat HR de resultaten bijhouden."

Figuur 8: Preventieve technologische maatregelen het meest populair, maar maatregelen op menselijke kwetsbaarheden nemen toe

Op welk gebied treft uw organisatie op dit moment maatregelen tegen cybercriminaliteit?



Bron: ABN AMRO en MWM2

Het vooraf inregelen van hulp op het moment dat zich een cyberincident voordoet is met 35 procent een minder wijdverbreide maatregel. Hetzelfde geldt voor het afsluiten van verzekeringen tegen de schade (32 procent).

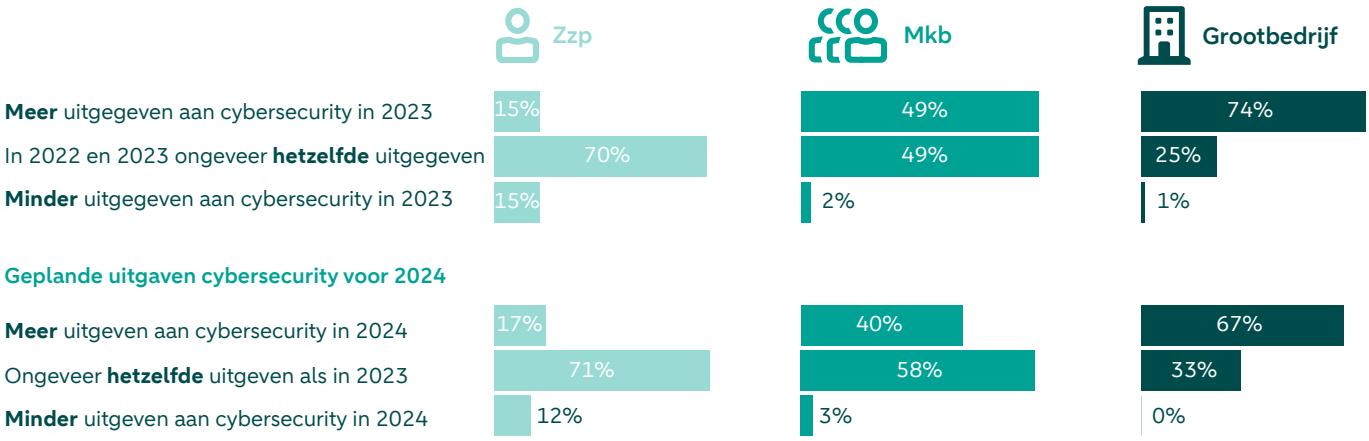
Roerink van MMOX onderstreept het belang van een mix aan maatregelen. "De cybersecuritymarkt is van oudsher gedreven vanuit IT en technologische maatregelen", vertelt de CEO. "Maar als je een risicogestuurde aanpak hanteert, merk je al gauw dat er ook ingrepen nodig zijn op procesniveau en menselijk vlak. Welke bedrijfsdata zijn bijvoorbeeld gevoelig of waardevol, en welke medewerkers hebben toegang tot die data? De betreffende medewerkers moeten dan extra opleidings- en beveiligingsmaatregelen ontvangen, of hun toegang tot een bepaald systeem moet worden ingetrokken."

Cybersecurityuitgaven stijgen het sterkst in het grootbedrijf

Het gros van de ondernemers gaf in 2023 minimaal evenveel uit aan cyberveiligheid als in het voorgaande jaar. Voor driekwart van de organisaties uit het grootbedrijf vielen de uitgaven zelfs hoger uit. Dit gold voor ongeveer de helft van de ondervraagde mkb'ers en slechts 15 procent van de zzp'ers. Vooruitblikkend op de uitgaven voor 2024 valt eenzelfde trend waar te nemen, hoewel het percentage dat een stijging verwacht een stukje lager uitvalt.

Figuur 9: Grootbedrijf trekt steeds meer geld uit voor cybersecurity

Uitgaven cybersecurity 2023 ten opzichte van 2022



Geplande uitgaven cybersecurity voor 2024

Vraag 1: Heeft uw organisatie in 2023 meer geld uitgegeven aan cybersecurity dan in 2022?
Vraag 2: Gaat uw organisatie in 2024 meer geld uitgeven aan cybersecurity dan in 2023?
Bron: ABN AMRO en MWM2

De belangrijkste drijfveren achter deze stijging zijn een toename van de cyberdreiging, genoemd door 55 procent van de respondenten, het voldoen aan de AVG-wetgeving (41 procent) en de digitale transformatie van de organisatie (39 procent). NIS2 wordt door 32 procent van de organisaties genoemd als reden voor hogere uitgaven aan cybersecurity. De digitale transformatie van de organisatie wordt door de respondenten uit het grootbedrijf overigens significant vaker genoemd dan door de ondervraagde mkb'ers. Ook de eisen van toeleveranciers en partners worden in dit segment vaker genoemd, wat duidt op een nadrukkelijkere ketenbenadering in het managen van cyberrisico's.

Verhoog de cyberveiligheid van uw organisatie

Steeds meer organisaties worden slachtoffer van cybercriminaliteit – criminelen hebben maar een kleine ingang nodig. Mogelijk loopt u nu al risico. Daarom is het belangrijk om passende maatregelen op het gebied van cyberveiligheid te nemen. Om u en uw mensen daarbij te helpen, zetten we verschillende oplossingen en downloads op een rij.

Cyberveiliger in 3 stappen

1 **Maak een risico-analyse**

Breng de 'kroonjuwelen' van uw organisatie in kaart. Welke zaken zijn cruciaal voor uw bedrijf of dienstverlening? Denk aan klantgegevens, productiemethoden of intellectueel eigendom. Identificeer vervolgens welke dreigingen deze kroonjuwelen in gevaar kunnen brengen: bijvoorbeeld een kwetsbaarheid in software of een medewerker die op een malafide link klikt. Nu kunt u de risico's analyseren. Wat is het gevolg van deze risico's, hoe waarschijnlijk zijn ze en wat doet u al om ze te beperken?

2 **Neem adequate maatregelen**

Uw risico-analyse bepaalt welke maatregelen de juiste zijn. De basismaatregelen van het Nationaal Cyber Security Centrum en de basisprincipes van het Digital Trust Center vormen in ieder geval een goed startpunt. Daarnaast kunt u:

- veilig gedrag van uw medewerkers stimuleren;
- bepalen en vastleggen wie de eigenaar van bepaalde gegevens is;
- risico's met uw partners en leveranciers bespreken.

Een cybersecurity-specialist kan u helpen om de juiste maatregelen te bepalen en te nemen.

3 **Stel een Cyber Response Plan op**

Ten slotte is het essentieel om procedures te ontwikkelen waarmee u cyberincidenten detecteert en afhandelt. Deze legt u vast in een Cyber Response Plan.

Ga meteen aan de slag

Whitepaper over Employee Awareness

Cybercriminelen komen vaak via medewerkers binnen in uw digitale systemen. Houd uw medewerkers scherp en maak hen bewust van de risico's van cybercrime – gebruik hiervoor onze whitepaper.

Download onze whitepaper

Third-Party Risk Management Checklist

Als u met partners en leveranciers samenwerkt, kunnen er veiligheidsrisico's optreden. Met Third-Party Risk Management brengt u deze in kaart.

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

Bekijk de checklist

Cyber Response Plan

Een Cyber Response Plan helpt u om cybercrime-incidenten op te sporen, af te handelen en eventuele schade te herstellen.

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

Maak uw Cyber Response Plan

Zo helpt ABN AMRO u

Cyber Veilig & Zeker van MMOX

Voor midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid

- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen

Bekijk Cyber Veilig & Zeker

Cyberverzekering

Voor zakelijke klanten die zich willen indekken tegen cyberschade

- Bescherming via onze cyberverzekering
- Uitgebreide dekking
- 24/7 hulp van onze specialisten

Ontdek onze cyberverzekering

Vrijblijvend cybergesprek

IVoor ondernemers die willen weten hoe zij ervoor staan op het gebied van cyberveiligheid

- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

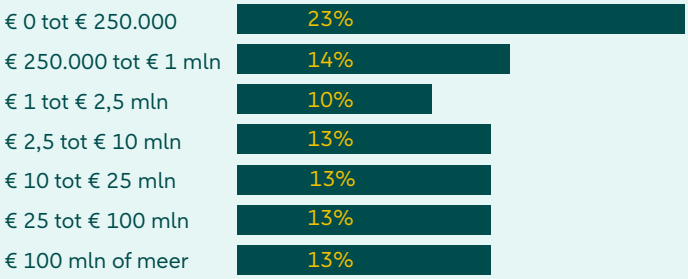
Plan vrijblijvend een gesprek in

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze nieuwsbrief

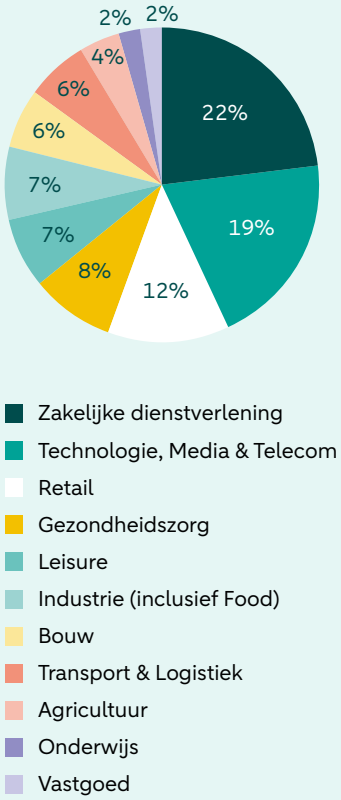
Steekproef

Het door MWM2 uitgevoerde onderzoek vond plaats in februari 2024. In totaal werden 895 ondernemers ondervraagd, waarvan 139 zzp'ers, 524 mkb-bedrijven (jaaromzet tot 25 miljoen euro) en 232 grote bedrijven (jaaromzet vanaf 25 miljoen euro).

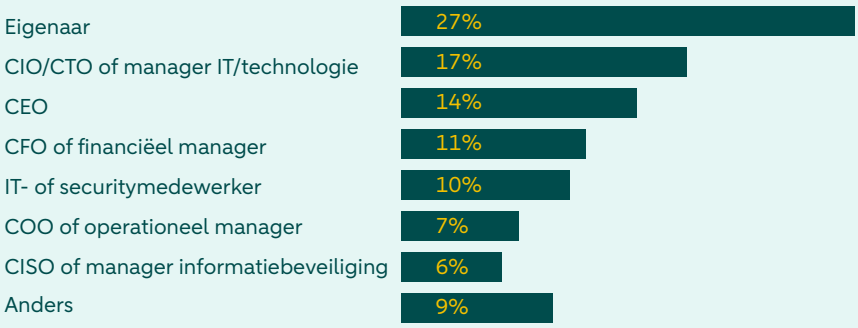
Omzet



Sectoren



Rol binnen de organisatie



Colofon

Dit is een uitgave van ABN AMRO.

Auteur
Julia Krauwer, sector banker Technologie, Media & Telecom (TMT)
julia.krauwer@nl.abnamro.com

Met dank aan
Daan Hoogendijk en Maarten Roelfs, Samen Digital Veilig
Maarten Roerink en Matthijs Blokker, MMOX
Arwi van der Sluijs, NFIR
Michel Verhagen, Digital Trust Center
Richard Verbrugge en Stephanie Kraai, ABN AMRO

Onderzoekspartner
MWM2

Eindredactie
Bendert Zevenbergen

Illustraties en opmaak
Kollerie Reklame-Advies & Promoties

Fotoverantwoording
Shutterstock.com

Distributie
abnamro.nl/tmt