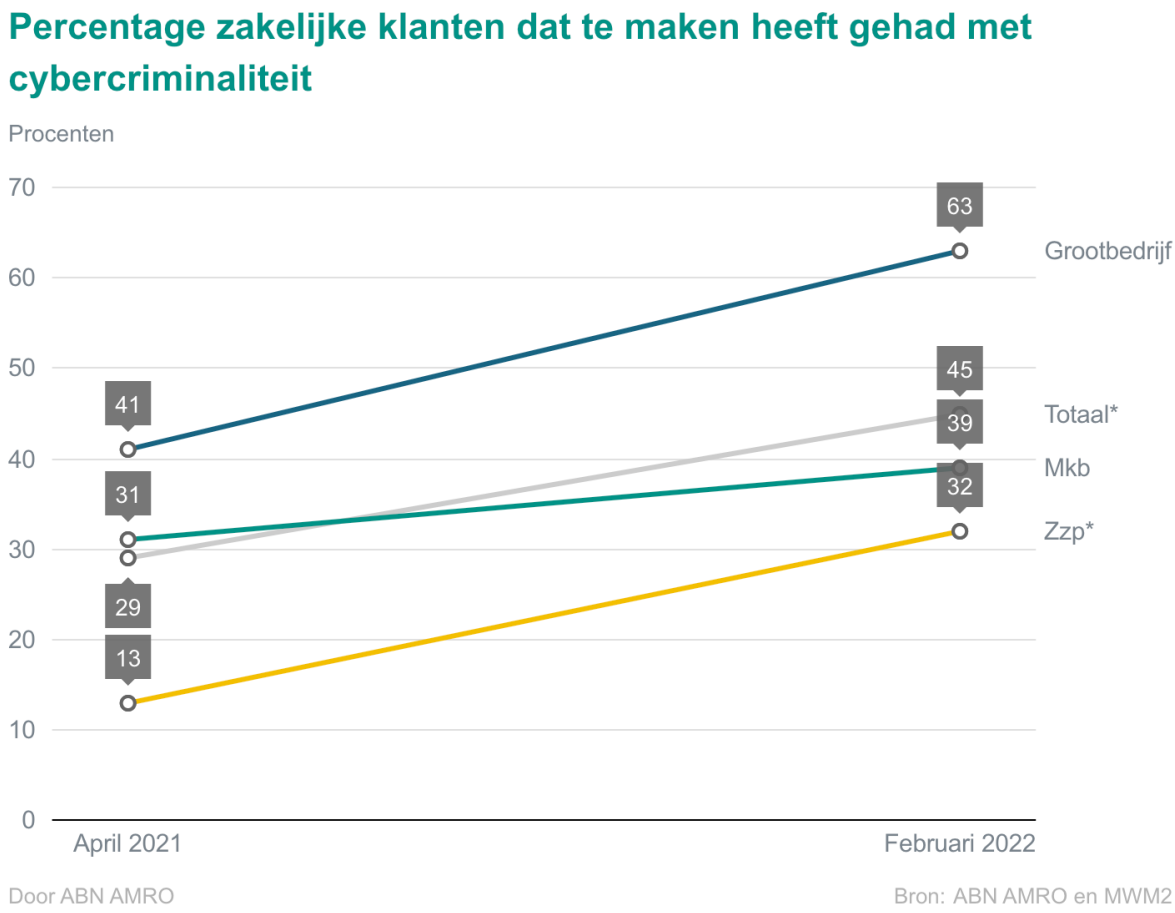
Cyberdreiging zet ondernemers aan tot maatregelen

Het aantal bedrijven dat te maken heeft gehad met een cyberaanval is het afgelopen jaar sterk gestegen. Hoewel de risicoperceptie van ondernemers vrijwel gelijk is gebleven, blijkt uit onderzoek van ABN AMRO onder 233 bedrijven dat de bereidheid tot het nemen van maatregelen toeneemt. Dat is gunstig, want cyberdreiging is een reëel operationeel risico geworden.

08/04/2022
Julia Krauwer

Dit heeft allereerst te maken met een groter aanvalsoppervlak door verregaande digitalisering, gecombineerd met professionalisering van cybercriminelen. Het feit dat geopolitieke spanningen steeds meer tot uiting komen in digitale aanvallen geeft extra aanleiding tot zorg. Zo leidt de oorlog tussen Rusland en Oekraïne ook voor Nederlandse ondernemingen tot een verhoogd cyberrisico. “Bovenop de structurele toename in cyberaanvallen zagen we in de aanloop naar de escalatie van het conflict een duidelijke piek. Dit was nog voordat het grote publiek via het nieuws hoorde welke kant het in Oekraïne op zou gaan”, zegt Bastiaan van Nunen, Managing Director bij cyberbeveiligingsbedrijf MMOX.

Het percentage bedrijven dat, los van de oorlog, te maken heeft gehad met cybercriminaliteit is gestegen. Was dit vorig jaar nog 29 procent van alle ondervraagden, dit jaar is het 45 procent. Dat blijkt uit onderzoek van ABN AMRO in samenwerking met onderzoeksbureau MWM2 onder 233 zakelijke klanten die eind- of medeverantwoordelijk zijn voor de cyberveiligheid van hun bedrijf.



* Significante stijging (p<0.05)
Vraagstelling: Heeft uw organisatie of de organisatie waarvoor u werkt wel eens te maken gehad met cybercriminaliteit?
Steekproef 2022: zzp (n=64) | mkb (n=139) | grootbedrijf (n=27; resultaten voor deze groep indicatief van aard)

Andere bronnen bevestigen dit beeld. Zo registreerde de Nederlandse politie vorig jaar 14.000 gevallen van cybercriminaliteit, een toename van bijna een derde in vergelijking met 2020 en een verdriedubbeling ten opzichte van 2019. Ook op Europees niveau is volgens het agentschap voor de cyberveiligheid ENISA sprake van een toename in cyberaanvallen gedurende de afgelopen twee jaar.

Uit het onderzoek van ABN AMRO blijkt dat specifiek het grootbedrijf opvallend vaak in aanraking komt met cyberaanvallen; 63 procent van de respondenten uit deze categorie – gedefinieerd als bedrijven met een jaarlijkse omzet hoger dan tien miljoen euro – kreeg al eens te maken met cybercriminaliteit, waarvan 22 procent in het afgelopen jaar.

Schade niet beperkt tot grote bedrijven

Toch is ook onder kleinere bedrijven alertheid geboden. Zij krijgen namelijk eveneens in toenemende mate te maken met cybercriminaliteit. Ligt volgens de meting in februari 2022 het percentage zelfstandigen zonder personeel (zzp'ers) dat ervaring heeft met cyberaanvallen op 32 procent, in april 2021 was dit nog slechts 13 procent. Ook in het midden- en kleinbedrijf (mkb) wordt een stijging waargenomen, hoewel die statistisch gezien niet significant is.

De trend is volgens Van Nunen in ieder geval duidelijk: niet enkel grote bedrijven worden slachtoffer. Daar ligt volgens hem een heldere strategie aan ten grondslag. “Een groep cybercriminelen zal liever een paar honderd kleine bedrijven aanvallen met een kleinere opbrengst en een kleinere pakkans dan een handvol grote bedrijven die al in een verhoogde staat van alertheid zijn”, zegt Van Nunen. Achterover leunen is er volgens hem in ieder geval niet bij: “Het zou naïef zijn om te denken dat cyberaanvallen zzp’ers niet zouden raken. Dat dacht men een jaar geleden ook over het midden- en kleinbedrijf.” Trish McGill, expert op het gebied van cyberveiligheid bij Nederlandse IT-dienstverlener Ilionx, sluit zich hierbij aan: “Uiteindelijk wordt iedereen een keer gehackt, het is slechts een kwestie van tijd.”

Lees ook: Threat Intelligence: Essentiële tips voor het MKB

Verwevenheid van digitaal landschap zorgt voor risico’s

Wanneer een bedrijf te maken krijgt met een cyberaanval, is dit vaak geen geïsoleerd evenement. Zo kunnen aanvallen op grotere bedrijven verstrekkende gevolgen hebben voor kleinere partijen. Dit is zeker het geval op het moment dat grote technologieaanbieders het doelwit worden. Dat werd in 2021 eens te meer duidelijk toen hackers zich via een beveiligingslek in mailprogramma Microsoft Exchange toegang wisten te verschaffen tot zeker 1200 Nederlandse mailservers. Zo kon van allerlei bedrijven vertrouwelijke informatie worden buitgemaakt.

Het risico is voor alle bedrijven onmiskenbaar gegroeid. “Door kwaadwillenden wordt meer dan ooit gebruikgemaakt van de mogelijkheden die digitalisering met zich meebrengt”, stelt Van Nunen. Dit is een structurele ontwikkeling die direct te koppelen valt aan het steeds groter wordende aanvalsoppervlak. Steeds meer bedrijven digitaliseren hun bedrijfsvoering, een ontwikkeling die door de coronacrisis in een stroomversnelling is gekomen. De vele clouddiensten – vaak van allerlei verschillende aanbieders – en apparaten die daarmee gemoeid zijn, vormen alle een potentieel toegangspunt voor cybercriminelen.

Hackers worden professioneler

Tegelijkertijd worden cybercriminelen steeds professioneler. Dit is onder andere te merken aan de manier waarop zij hun afwegingen maken. Beide experts geven aan dat er vaak een ‘business case’ aan ten grondslag ligt. “Steeds vaker start een cyberaanval met een grondig onderzoek om te bepalen wat er bijvoorbeeld aan data bij een bedrijf te halen valt. Een eigen accountant brengt vervolgens de potentiële waarde van de aanval in kaart”, zegt McGill. Van Nunen herkent dit principe: “Op het moment dat cybercriminelen een bedrijf in het vizier hebben voor een ransomware-aanval, maken ze gerust een rekensom om vast te stellen wat het beste bedrag is om aan een partij te vragen. Wat kost het per dag als de operatie stil komt te liggen van een bedrijf met een omzet van acht miljoen? Wat is de ondernemer dus bereid te betalen?”

De hackers van nu zijn niet te vergelijken met die van vroeger, stelt McGill. “Voorheen waren hackers gewoon ‘script kiddies’ die bij hun moeder in de kelder zaten te

coderen. Hetzelfde soort mensen kan nu zijn ei kwijt in het maken van TikTok-filmpjes. Het soort aanvaller dat tegenwoordig actief is, is van een hele andere orde, dat zijn professionals.” Volgens McGill ontwikkelen de vaardigheden van cybercriminelen zich in lijn met de technologische ontwikkelingen. “Telefoons en laptops evolueren constant in termen van veiligheid. Waar voorheen een virus een bedrijf gemakkelijk op zijn grondvesten kon laten trillen, is daar tegenwoordig veel grover geschut voor nodig. Aanvallers kunnen niet achterblijven, die moeten blijven innoveren om schade aan te kunnen richten.”

Daarnaast organiseren hackers zich niet alleen in toenemende mate, ook zijn zij steeds vaker werkzaam in organisaties die zich specifiek toeleggen op cybercriminaliteit. Zulke organisaties bieden allerlei soorten aanvallen aan kwaadwillenden aan als een kant-en-klaar pakket. Ook gijzelsoftware – ook wel ‘ransomware’ genoemd – is via deze weg beschikbaar. De bijbehorende ‘Ransomware-as-a-Service’-bedrijven hebben alles wat een legaal opererend technologiebedrijf ook heeft, van een onderzoeks- en ontwikkelingsafdeling tot een klantenservice die de aankopende partij helpt de software te implementeren. Het verschil ten opzichte van reguliere technologiebedrijven is de zogenaamde ‘slachtofferservice’, die gegijzelde ondernemingen begeleidt in het betalen van de borgsom.

Verschillende motieven voor een cyberaanval

De motieven van hackers lopen uiteen. Waar de één uit is op direct financieel gewin en gijzelsoftware inzet om grote sommen geld te eisen van het bedrijf waarvan het systeem is lamgelegd, handelt de ander primair vanuit politieke beweegredenen. In het laatste geval gaat het om bijvoorbeeld het inbreken in overheidssystemen om gevoelige militaire informatie buit te maken, of het platleggen van belangrijke lokale bedrijven om een politieke tegenstander op de knieën te dwingen. Weer anderen vallen in de categorie ‘ethisch hacker’. Deze zetten hun vaardigheden in om kwetsbaarheden in systemen te ontdekken en met deze informatie het beveiligingsniveau naar een hoger niveau te helpen tillen. Hackers werken soms in opdracht van de overheid, dan weer volledig uit eigen initiatief.

De oorlog tussen Rusland en Oekraïne heeft tot gevolg dat de dreiging van politiek gemotiveerde cyberaanvallen toeneemt. Volgens Van Nunen van MMOX is de digitale aanval een van de wapens in het arsenaal: “Cyberoorlog maakt deel uit van de hedendaagse oorlogsvoering. Het wordt bijvoorbeeld ingezet om een land of regio te destabiliseren. Zo hebben statelijke actoren eerder via een cyberaanval geprobeerd de nucleaire reactors in Iran plat te leggen. Het is simpelweg een van de manieren om een ander land je wil op te leggen.”

Oorlog zorgt voor dreiging, maar nog geen substantiële schade

Voor zover bekend hebben vooralsnog geen directe Russische aanvallen op Nederlandse bedrijven plaatsgevonden, bijvoorbeeld als vergelding tegen Europese sancties tegen Rusland of Europese wapenleveranties naar Oekraïne. Het Nationaal Cyber Security Centrum (NCSC) schat de kans hierop laag in,

maar adviseert organisaties ‘vanwege de onvoorspelbaarheid van de situatie alert te blijven’.

Nederlandse ondernemingen zijn wel al op een meer indirecte manier betrokken geraakt bij het conflict. Zo werd in maart bekend dat enkele honderden routers van Nederlandse bedrijven waren gehackt om in een ‘botnet’ in te lijven. Dit is een netwerk van geïnfecteerde apparaten die worden ingezet om grote hoeveelheden verzoeken te sturen naar servers van derden. In maart werd de malware ‘CyclopsBlink’ gebruikt om een botnet te creëren waarmee Oekraïense bedrijven en overheden werden aangevallen. Deze malware werd volgens ingewijden vrijwel zeker ontwikkeld door een groep hackers die verbonden is aan een Russische inlichtingendienst.

Hoewel het voor ondernemers een onprettig idee zal zijn dat hun IT-apparatuur wordt ingezet in een cyberoorlog, zullen bedrijven niet snel merken dat zij zijn ingelijfd in een botnet. Hun apparatuur verstuurt wellicht enkele verzoeken per uur. Dit heeft geen invloed op hun dagelijkse operatie.

Directe aanvallen elders kunnen ook hier effect hebben

Een groter risico vormen zogenaamde ‘overloopeffecten’. Dit is de schade die aanvankelijk enkel wordt toegebracht aan de IT-systemen van bedrijven of overheden in het conflictgebied, maar overslaat op betrokkenen elders. Een bekend voorbeeld is de ‘NotPetya’-malware, die in 2017 via een update van een lokaal veelgebruikt boekhoudprogramma werd verspreid. Op deze manier raakten de systemen van allerlei bedrijven in Oekraïne geïnfecteerd. Via deze bedrijven verspreidde de malware zich vervolgens wereldwijd. Zo werden door NotPetya meerdere containterterminals van rederij Maersk in de Rotterdamse haven stilgelegd en kwam een groot deel van de operatie van farmaceut Merck tot stilstand. De besmetting kostte beide bedrijven vele miljoenen aan herstelkosten en misgelopen inkomsten.

Soortgelijke malware is ook in de aanloop naar de Russische inval in Oekraïne ingezet. Het ging hier om zogenaamde ‘wipers’, zeer destructieve software die alle bestanden op een geïnfecteerde computer kan vernietigen en deze veelal zelfs verhindert op te starten. Daarom is alertheid geboden bij elk bedrijf dat een vestiging heeft in het conflictgebied, gebruikmaakt van IT-diensten die daar worden gehost, of daar klanten of leveranciers heeft.

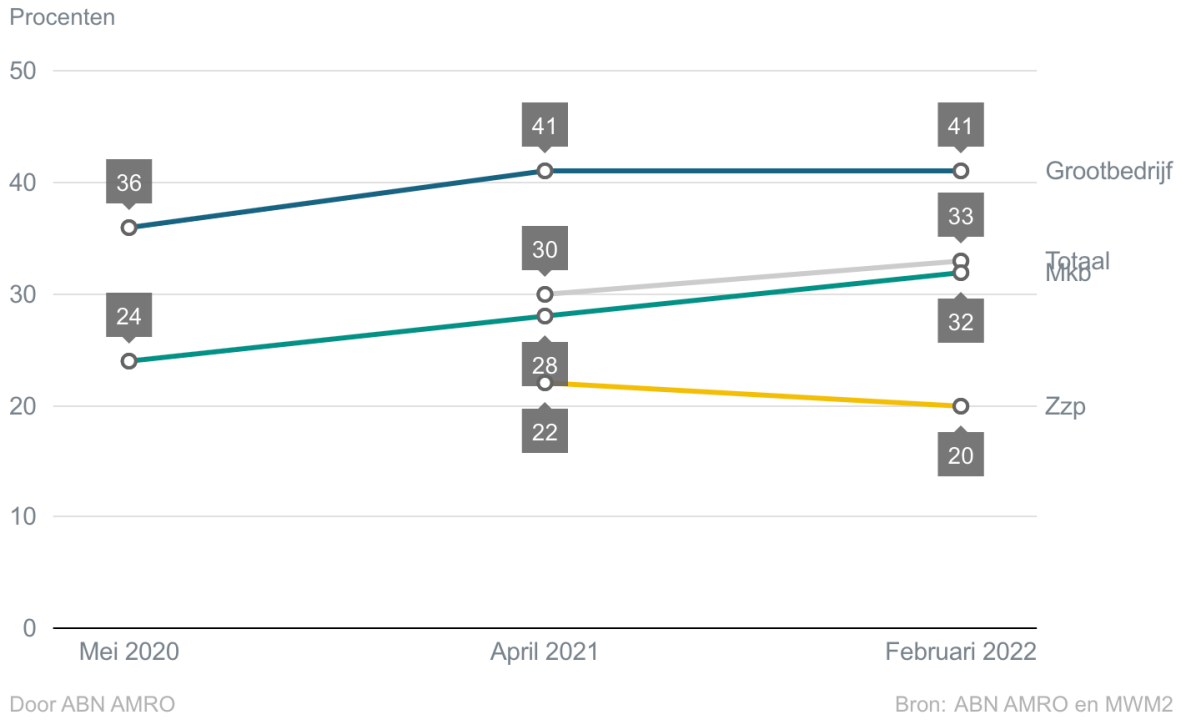
Een andere manier waarop de oorlog leidt tot toegenomen dreiging, is het feit dat cybercriminelen de bereidheid tot het geven van hulp misbruiken. Dergelijke groepen zijn geen partij in de oorlog zelf, maar grijpen de omstandigheden bijvoorbeeld aan in ‘phishing-campagnes’. Zo zijn er oplichters actief die uit naam van Giro555, een samenwerkingsverband tussen Nederlandse hulporganisaties, e-mail-, WhatsApp- of sms-berichten versturen waarin wordt gevraagd om een donatie.

Risicoperceptie blijft achter bij feitelijke dreiging

De cyberdreiging is dus om meerdere redenen stevig toegenomen. De risicoperceptie van ondernemers blijft daarbij echter achter. Waar vorig jaar 30 procent van de ondervraagden cybercriminaliteit als “veel” of “heel erg veel” risico zag voor de eigen organisatie, blijkt dit met 33 procent in 2022 niet significant toegenomen.

Risicoinschatting van zakelijke klanten ten aanzien van cybercriminaliteit

Percentage zakelijke klanten dat cybercriminaliteit als "veel" of "heel erg veel" risico ziet voor de eigen organisatie



Door ABN AMRO

Bron: ABN AMRO en MWM2

Vraagstelling: In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie? (1 = helemaal geen risico; 5 = heel erg veel risico)
Steekproef 2022: zzp (n=64) | mkb (n=139) | grootbedrijf (n=27; resultaten voor deze groep indicatief van aard)

Ook Van Nunen ziet dat de risicoperceptie van ondernemers vaak nog niet in lijn is met de realiteit. Volgens hem zijn cyberaanvallen echter een risico waar bedrijven rekening mee moeten houden. “Bedrijven verzekeren zich tegen brand en diefstal, maar minder snel tegen cybercriminaliteit. Het risico op brand is echter 1 op 8000, terwijl het risico om in aanraking te komen met een cyberaanval, of pogingen daartoe, minimaal 1 op 8 is.”

De discrepantie tussen risicoperceptie en de feitelijke dreiging valt volgens McGill deels te verklaren door culturele factoren. “Nederland is op het wereldtoneel slechts een kleine speler. Dat vormt de risicoperceptie van de bedrijven hier. Dat zij ook wel eens slachtoffer kunnen worden van hackers buiten de eigen landsgrenzen, wordt minder sterk gevoeld.” Het concept van ‘lokale bedrijven’ wijst ze dan ook resoluut af: “Op het moment dat een bedrijf verbonden is aan het internet, is het een internationaal bedrijf. Met alle risico’s en uitdagingen van dien.”

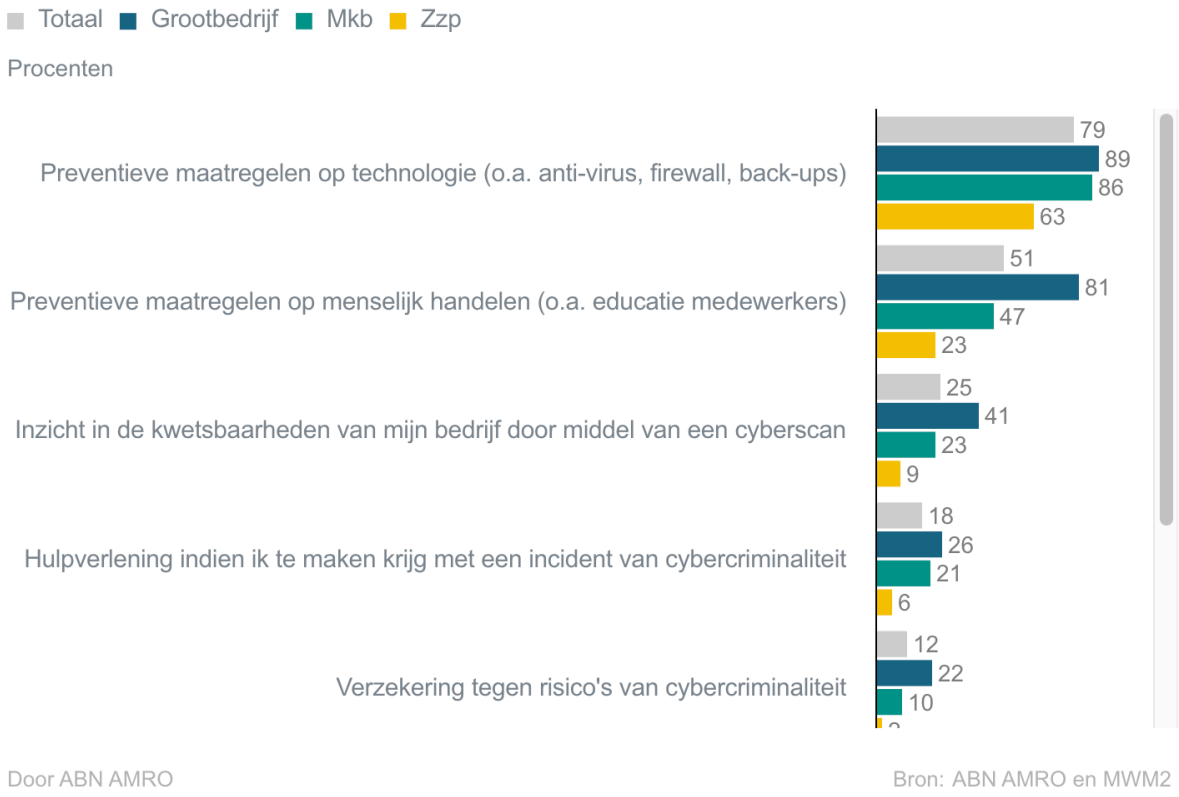
Het helpt volgens haar overigens niet dat Nederland weinig wet- en regelgeving op het gebied van cyberveiligheid kent. “Hier bestaan bijvoorbeeld geen wetten die voorschrijven dat je het moet melden als je bent geraakt door een cyberaanval.” McGill maakt een vergelijking met het Verenigd Koninkrijk: “Daar is, anders dan in Nederland, een duidelijke handhavingscultuur. Het resultaat is dat er ook standaarden en overheidsorganen zijn die bedrijven heel concreet helpen hun beveiliging op orde te krijgen. In Nederland hebben ze dat niet, enkel richtlijnen en zachte aanbevelingen.”

Lees ook: Ondernemers onderschatten het risico op cybercriminaliteit

Risicoperceptie bepaalt of er maatregelen worden genomen

De minimale verandering in risicoperceptie betekent helaas ook een beperkte verbetering in de digitale weerbaarheid van ondernemers. Uit statistische analyses blijkt namelijk dat respondenten met een hogere risicoperceptie (“veel” of “heel erg veel risico”) meer maatregelen nemen dan respondenten die de cyberrisico’s voor hun organisatie lager inschatten (“weinig” of “helemaal geen risico”).

Overzicht van de meest genomen maatregelen tegen cybercriminaliteit



Vraagstelling: Op welk gebied treft uw organisatie op dit moment maatregelen met betrekking tot cybercriminaliteit?
Steekproef: zzp (n=64) | mkb (n=139) | grootbedrijf (n=27; resultaten voor deze groep indicatief van aard)

De top drie van meest genomen maatregelen zijn geheel preventief van aard. Het meest populair zijn technologische maatregelen zoals antivirussoftware, firewalls en

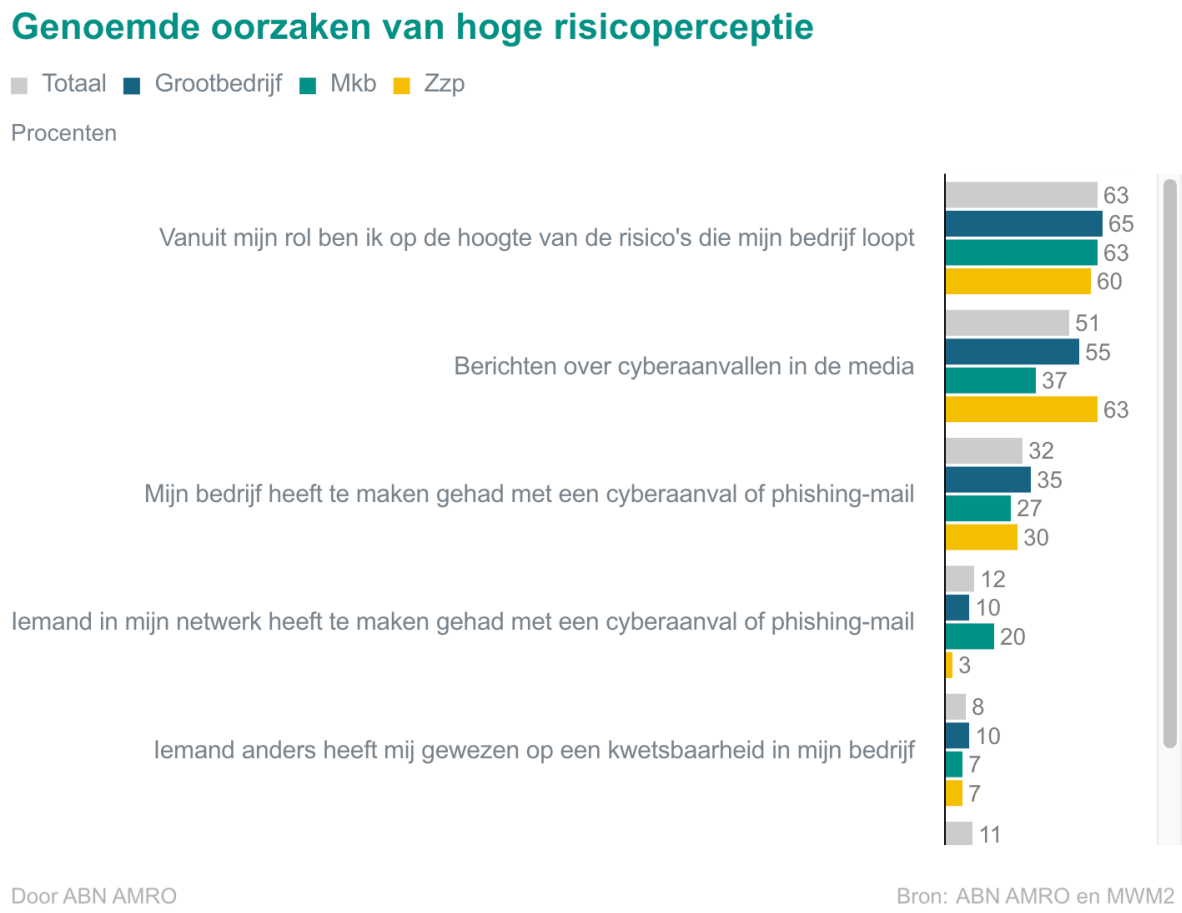
het maken van back-ups; deze worden door 79 procent van de ondervraagden genomen. Preventieve maatregelen gericht op menselijk handelen worden door 51 procent ingezet. Overigens hecht juist het grootbedrijf een groot belang aan de menselijke rol; maar liefst 81 procent van de respondenten uit deze categorie zegt preventieve maatregelen op menselijk handelen te nemen.

Op plaats drie staat het (laten) uitvoeren van een cyberscan die inzicht geeft in de kwetsbaarheden van het bedrijf. Van de ondervraagden maakt 25 procent hier gebruik van. Minder populair is het inrichten van hulpverlening indien het bedrijf te maken krijgt met een incident van cybercriminaliteit (18 procent) of het afsluiten van een verzekering (12 procent). Van de ondervraagden geeft 11 procent aan helemaal geen maatregelen te treffen. Dit betreft uitsluitend zzp'ers en mkb-bedrijven.

Verschillende oorzaken voor hoge risicoperceptie

Een hogere risicoperceptie leidt dus uiteindelijk tot meer barrières voor cybercriminelen, maar betekent in sommige gevallen dat het kwaad al is geschied. Ongeveer een derde van de ondernemers geeft namelijk aan dat hun risicoinschatting voortkomt uit een eerdere ervaring met een cyberaanval of phishing-mails. McGill ziet dit ook terug in de praktijk: "Voor een deel van de mensen geldt dat ze het risico pas écht onderkennen op het moment dat ze significante schade hebben ondervonden door een aanval."

De respondenten zelf noemen overigens andere redenen als meer doorslaggevend om te handelen. Zo'n twee derde van hen verklaart de hoge risicoperceptie door hun rol binnen het bedrijf – veelal eigenaar of directeur – en het bijbehorende inzicht in de risico's. Eveneens zeer bepalend blijken berichten in de media over cyberaanvallen. Onder zzp'ers wordt dit door maar liefst 63 procent genoemd als trigger. Dezelfde reden wordt door 55 procent van de respondenten uit het grootbedrijf genoemd, en door 37 procent van de ondervraagden uit het midden- en kleinbedrijf.



Vraagstelling: U heeft aangegeven dat uw organisatie redelijk tot heel erg veel risico loopt getroffen te worden door een cyberaanval. Wat heeft die risicoperceptie veroorzaakt?
Steekproef; indien risicoschatting “redelijk” (3) tot “heel erg veel risico” (5) | ZZP (n=30), SME (n=94), CB (n=20; resultaten voor deze groep indicatief van aard)

Mediaberichten over cyberaanvallen verhogen risicobewustzijn

Cyberdreiging is het afgelopen jaar in de media breed uitgemeten. Zo kwam vorig jaar naar buiten dat een ransomware-aanval diverse systemen van elektronicawinkel Mediamarkt had stilgelegd, en De Mandemakers Groep – bekend van keukens, sanitair en meubels – eveneens het slachtoffer was geworden van gijzelsoftware. Dergelijke berichtgeving is volgens Van Nunen voor veel bedrijven een ‘wake-up call’ geweest. “Het feit dat ook grote bedrijven slachtoffer kunnen worden, doet mensen achter de oren krabben. Cyberaanvallen raken kennelijk ook partijen die hun IT in principe goed voor elkaar hebben.”

Een ongeluk kan namelijk letterlijk klein hoekje zitten, zo bleek uit de recente crisis rond ‘Log4J’ die de nodige media-aandacht kreeg. Log4J is een publiek beschikbaar software-onderdeel dat in allerlei IT-oplossingen wordt gebruikt en daardoor deel uitmaakt van het systeemlandschap van vrijwel alle bedrijven. Het feit dat een kwetsbaarheid in Log4J bijzonder gemakkelijk kon worden uitgebuit door kwaadwillenden, deed de alarmbellen van bedrijven in binnen- en buitenland rinkelen.

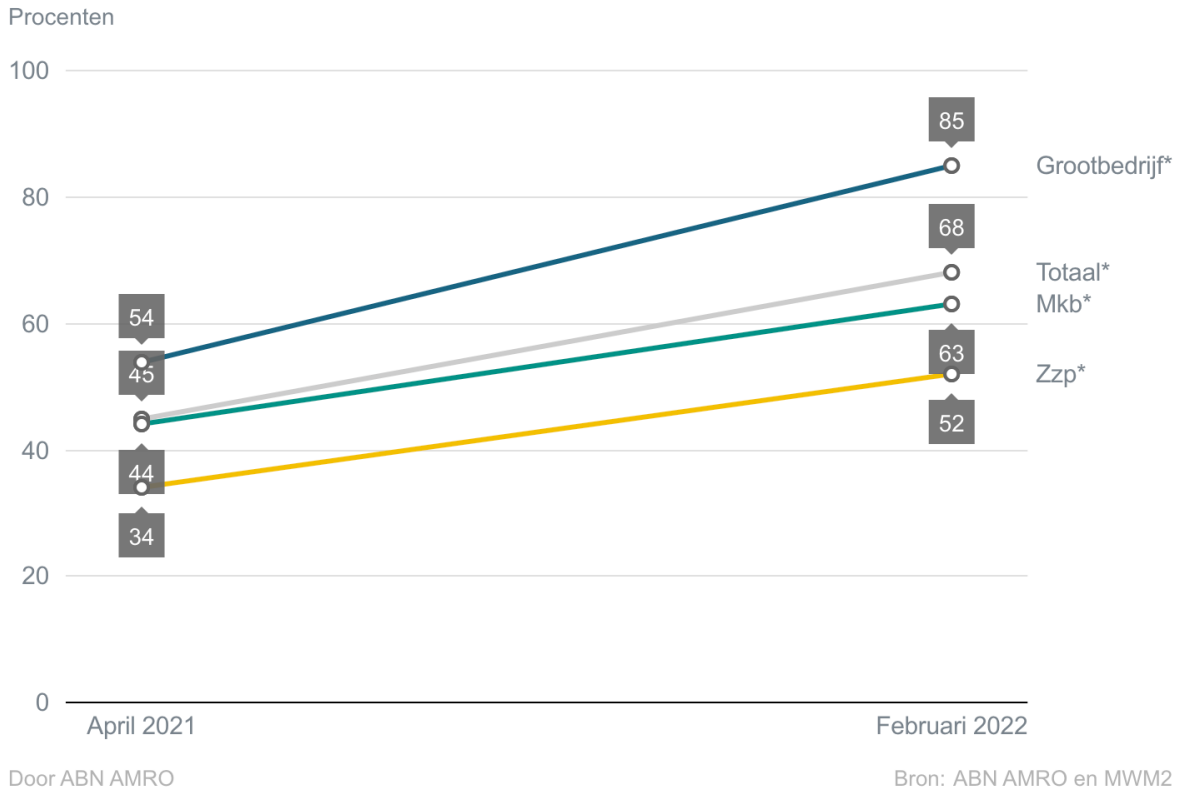
Media-aandacht voor de digitale oorlog die parallel aan de huidige fysieke oorlog in Oekraïne plaatsvindt, zal de alertheid van ondernemers mogelijk verder vergroten. Omdat de enquête is uitgezet voorafgaand aan het gros van de berichtgeving over cyberaanvallen in de context van de oorlog, is dit effect vermoedelijk slechts beperkt zichtbaar in de resultaten.

Bereidheid tot nemen van maatregelen stijgt

Ondanks de bescheiden stijging in risicoperceptie geven ondernemers aan zich de komende tijd verder te willen wapenen tegen cybercriminaliteit. Hoewel dit niet per se iets zegt over de daadwerkelijke uitvoering van de voorgenomen maatregelen, wijzen de resultaten mogelijk op een toegenomen gevoel van urgentie. Voor alle drie de onderzochte klantgroepen steeg het percentage dat van plan is extra maatregelen te treffen namelijk significant ten opzichte van vorig jaar.

Met name bedrijven die zelf te maken hebben gehad met cybercriminaliteit geven aan meer actie te willen ondernemen. Diezelfde bedrijven geven overigens ook significant vaker aan van plan zijn preventieve maatregelen op menselijk handelen te gaan treffen. Dit is gunstig, want initiële toegang tot systemen wordt vaak via de menselijke weg verkregen. Middels onder andere slim opgestelde e-mails weten cybercriminelen bijvoorbeeld inloggegevens van medewerkers te ontfutselen.

Percentage zakelijke klanten dat van plan is extra maatregelen te treffen tegen cyberaanvallen



Door ABN AMRO

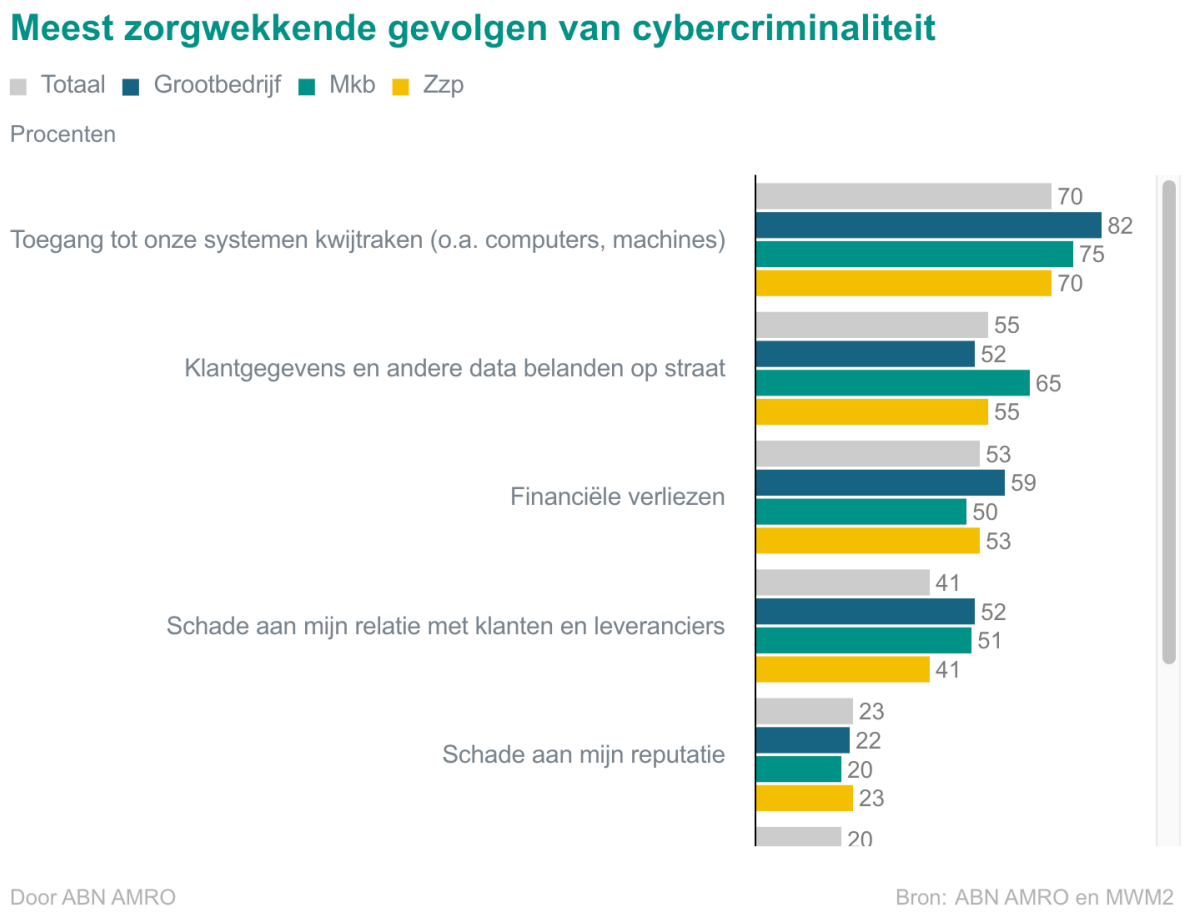
Bron: ABN AMRO en MWM2

* Significante stijging (p<0.05) Vraagstelling: Op welk gebied treft uw organisatie op dit moment maatregelen met betrekking tot cybercriminaliteit?

Steekproef: zzp (n=64) | mkb (n=139) | grootbedrijf (n=27; resultaten voor deze groep indicatief van grootbedrijf (n=27; resultaten voor deze groep indicatief van aard)

Verlies van toegang tot systemen meest zorgwekkende gevolg

Duidelijk is dat er veel op het spel staat voor ondernemers. Gevraagd naar de drie meest zorgwekkende gevolgen van cybercriminaliteit, wordt verlies van toegang tot systemen het vaakst genoemd. Op een tweede plek staat het op straat belanden van klantgegevens en andere data, gevolgd door het leiden van financiële verliezen. Net buiten de top drie, maar ook vaak genoemd: schade aan de relatie met klanten en leveranciers. Veel minder frequent genoemd worden reputatieschade en inbreuk op intellectueel eigendom.



Vraagstelling: Over welke 3 gevolgen van cybercriminaliteit maakt u zich het meeste zorgen?
Steekproef: zzp (n=64) | mkb (n=139) | grootbedrijf (n=27; resultaten voor deze groep indicatief van aard)

Het feit dat ondernemers het meest angstig zijn om toegang tot hun systemen kwijt te raken, bevestigt eens te meer hoezeer het gemiddelde bedrijf afhankelijk is geworden van digitale diensten. Dit besef alleen al zorgt ervoor dat bedrijven cyberaanvallen steeds meer als operationeel risico beschouwen en daarmee wellicht maatregelen treffen vóór ze met de harde werkelijkheid worden geconfronteerd.