

Cyberveiligheid in de zakelijke dienstverlening

De zakelijke dienstverlening is een aantrekkelijk doelwit voor cybercriminelen

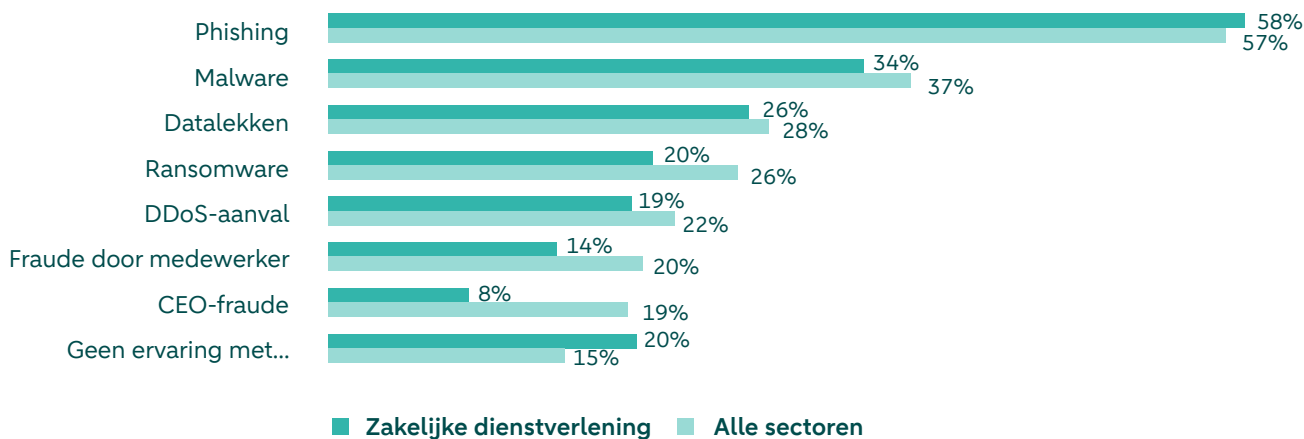
Bedrijven binnen de zakelijke dienstverlening beheren tal van persoonlijke en financiële data. Ze bezitten vooral veel vertrouwelijke gegevens – denk aan intellectueel eigendom en beroepsgeheimen. In de sector, waar veel digitaal gewerkt wordt, is cybercriminaliteit sinds het begin van de COVID-19-epidemie met zeshonderd procent toegenomen. Dat is vooral te verklaren door de overgang naar werken op afstand. Bedrijven in de zakelijke dienstverlening willen geen reputatieschade oplopen, en betalen daarom vaak losgeld in gevallen van ransomware.

Recente cyberaanvallen in de sector

- In november 2023 werd het Londense advocatenkantoor Allen & Overy [gehackt door Lockbit](#). Daarbij is een aantal opslagservers getroffen, maar bleef het e-mail- en documentbeheersysteem onaangetast. Als reactie op de hack heeft Allen & Overy getroffen klanten op de hoogte gesteld, en onderzocht welke gegevens zijn gestolen. Lockbit gaf het advocatenkantoor een 'onderhandeldeadline' – het is niet bekend of het kantoor daarop is ingegaan, en of er losgeld is betaald.
- In maart 2023 werd er [ingebroken in de systemen](#) van softwarebedrijf Nebu. Daarin stonden de klantgegevens van enkele miljoenen Nederlanders. Ook verschillende ministeries en andere overheidsinstellingen werden getroffen. Een van de klanten van Nebu is onderzoeksbureau Blauw. In eerste instantie wilde het softwarebedrijf weinig kwijt over het datalek, waarop Blauw het bedrijf voor de rechter sleepte.
- JobMotion – het uitzendbureau van de Universiteit Leiden – werd in 2022 [slachtoffer van een ransomware-aanval](#). Hackers wisten het salarisverwerkingsysteem plat te leggen, waarin onder andere adressen, bankgegevens en burgerservicenummers staan. JobMotion meldde het incident bij de Autoriteit Persoonsgegevens. Volgens een woordvoerder heeft de universiteit na de aanval 'stappen gezet om beter tegen cyberaanvallen beschermd te zijn'.
- Accountantskantoor Crowe Foederer was in 2022 slachtoffer van een [aanval met ransomware](#). Gijzelsoftware blokkeerde de bestanden en computerprogramma's van het kantoor. Ook het mailsysteem werkte niet meer. Na de aanval heeft Crowe Foederer hun systemen ontkoppeld en geïsoleerd, en cliënten op de hoogte gesteld. Het is niet bekend of er losgeld is geëist.

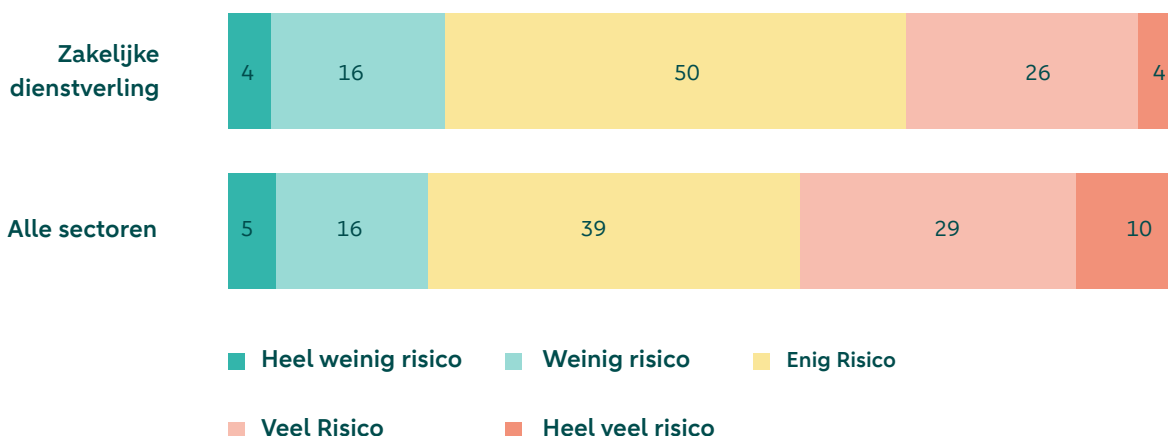
Bovengemiddeld veel phishing in de zakelijke dienstverlening

Met welke van de volgende vormen van cybercriminaliteit heeft u binnen uw organisatie weleens te maken gehad?*



Bedrijven in de zakelijke dienstverlening lopen gemiddeld risico op cybercriminaliteit

In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie?*



* Bron: enquête van ABN AMRO en MWM2 onder 895 Nederlandse organisaties, maart 2024

NIS2: nieuwe Europese wetgeving moet cyberweerbaarheid verbeteren

Om de cyberveiligheid in Europa te verbeteren, gaat in oktober 2024 een nieuwe wet in: NIS2, de opvolger van de Network and Information Security Directive (NIS). De NIS2-wetgeving geldt voor bedrijven met minimaal vijftig werknemers, of een jaaromzet en balanstotaal van meer dan € 10 miljoen. Organisaties die belangrijk of essentieel zijn voor de maatschappij, moeten zich aan deze richtlijn houden om de impact van cyberaanvallen en -verstoringen te beperken. Dit geldt ook voor bedrijven in de keten van deze vitale organisaties, zoals klanten, partners en toeleveranciers.

Het is de bedoeling dat Europese lidstaten de richtlijn naar landelijke wetgeving vertalen, maar Nederland loopt hierbij vertraging op. Toch is het verstandig om uw organisatie al op de invoering voor te bereiden. Omdat de wet er hoe dan ook komt, maar ook omdat klanten of leveranciers in andere Europese landen de richtlijn wél vanaf oktober 2024 volgen.

Benieuwd of uw organisatie onder de NIS2-richtlijn valt?

Lees ons rapport: [Steeds verfyndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker](#), of vul de [Zelfevaluatie NIS2](#) van het Nationaal Cyber Security Centrum in.

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 drie stappen

1 Maak een risico-analyse
Bring 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 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 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.



Whitepaper over Employee Awareness ([Download onze whitepaper](#))

Cybercriminelen komen vaak via medewerkers uw digitale systemen binnen. Houd uw medewerkers scherp en maak ze bewust van de risico's van cybercrime. U leest er alles over in ons whitepaper.

Checklist: Third-Party Risk Management ([Bekijk de 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

Cyber Response Plan ([Maak uw 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

Cyberveiligheidsrapport ([Lees het complete rapport](#))

Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval. Lees alle feiten en ontwikkelingen in het jaarlijkse rapport 'Steeds verfyndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker'.

NIS2-praktijkids ([Check onze NIS2-praktijkids](#))

Elke sector kent verschillende cyberrisico's. In de industriële sector is vaak de productie het doelwit van cybercriminelen, terwijl ze in de gezondheidszorg uit zijn op patiëntgegevens. Benieuwd naar de risico's en dreigingen in uw sector?

Zo helpt ABN AMRO

Cyber Veilig & Zeker van MMOX

Voor een midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid.

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

Cyberverzekering

Voor zakelijke klanten die zich willen indekken tegen cyberschade.

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

Vrijblijvend cybergesprek

Voor ondernemers die willen weten hoe ze ervoor staan op het gebied van cyberveiligheid.

- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

[Bekijk Cyber Veilig & Zeker](#)

[Ontdek onze cyberverzekering](#)

[Plan vrijblijvend een gesprek in](#)

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze [nieuwsbrief](#)