Cyberveiligheid in de Technologie, Media & Telecom

IT-leveranciers zijn een populair doelwit voor cybercriminelen

IT-, media- en telecombedrijven zijn onmisbaar voor vrijwel elke organisatie. Hun software en infrastructuur vormen de toegangspoort naar een breed publiek. Die centrale rol in ons digitale landschap maakt ze kwetsbaar: cybercriminelen kunnen deze bedrijven, hun klanten én de maatschappij grote schade toebrengen. Mogelijk vinden er daarom meer hackpogingen en pogingen tot desinformeren plaats bij bedrijven in de TMT dan in andere sectoren. Organisaties doen er goed aan om zich in ieder geval te wapenen tegen phishing, malware en datalekken: ondervraagden in de sector komen die vormen van cybercriminaliteit het meest tegen.

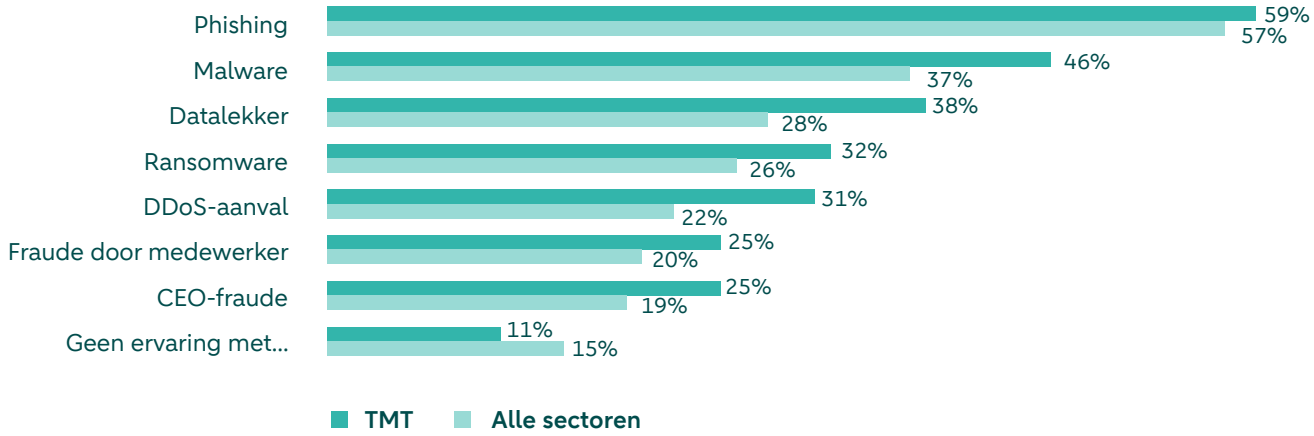
Recente cyberaanvallen in de sector

- Halverwege 2023 claimde de beruchte ransomware-groep LockBit dat ze chipgigant Taiwan Semiconductor Manufacturing Company (TSMC) hadden gehackt. Volgens het bedrijf zelf klopte dat niet: niet zij, maar hardware- leverancier Kinmax zou zijn getroffen. TSMC heeft direct na het incident de datauitwisseling met zijn leverancier stopgezet.
- In april 2023 meldde hard- en softwareontwikkelaar MSI dat het bedrijf slachtoffer was geworden van een ransomware-aanval. Hierbij zijn *private keys* gestolen, waaronder Intel Boot Guard-keys: die worden gebruikt om firmware van moederborden digitaal te ondertekenen en verifiëren. In theorie kunnen criminelen met deze buit malafide firmware uitvoeren en zo diepgaande toegang krijgen tot systemen – al acht het Nationaal Cyber Security Centrum de kans op misbruik klein.
- Eind 2022 hebben hackers de persoonsgegevens van tienduizenden klanten van Delta Fiber gestolen. Door snel ingrijpen bleef de schade relatief beperkt: het bedrijf geeft aan dat het alleen om namen, adressen, e-mailadressen, geboortedata, telefoonnummers en bankrekeningnummers ging – geen schadelijke informatie als wachtwoorden en creditcardgegevens dus. Toch moeten klanten extra alert zijn op mogelijke e-mail- en telefoonfraude, zoals phishing.
- Je kunt zelf je cyberbeveiliging goed op orde hebben, maar alsnog in verlegenheid worden gebracht doordat hackers je toeleverancier aanvallen – daar kunnen tv-providers als Ziggo en KPN sinds maart 2024 over meepraten. Toen lukte het hackers namelijk om Russische propagandafilmpjes op BabyTV uit te zenden. Ze gebruikten een stoorzender om in te breken in het satellietsignaal van Eutelsat. Omdat het de eerste keer was dat zo'n aanval plaatsvond, was niemand erop voorbereid en duurde het even voordat de hack überhaupt werd opgemerkt.

ABN·AMRO

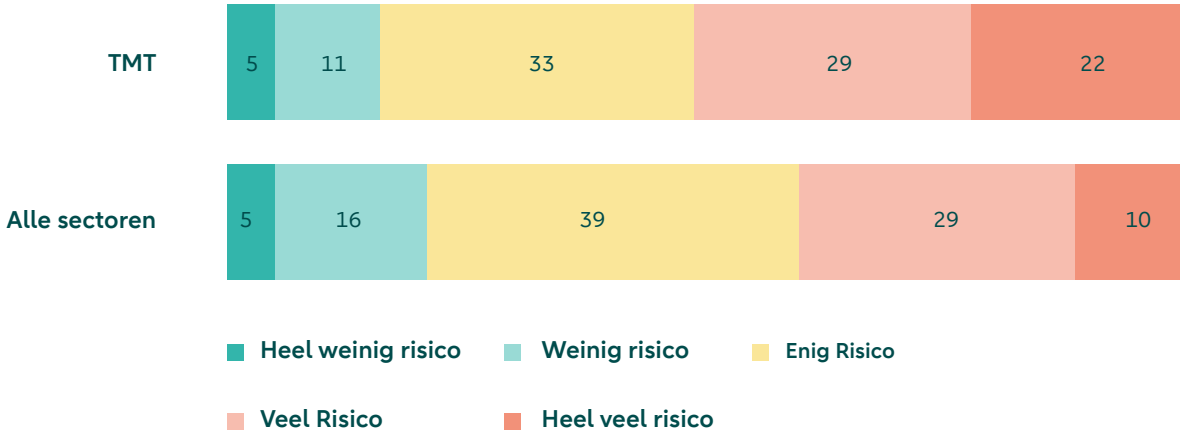
TMT-bedrijven krijgen bovengemiddeld veel cyberaanvallen te verduren

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



Risicoinschatting TMT-bedrijven is relatief hoog

*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). 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.

Binnen TMT vallen verschillende bedrijven onder de NIS2, waaronder:

- Beheer van ICT-diensten
- Digitale infrastructuur
- Digitale aanbieders

Benieuwd of uw organisatie onder de NIS2-richtlijn valt?
Lees ons rapport: **Steeds verfijndere 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

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 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 verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker'.

NIS2-praktijkgids (Check onze NIS2-praktijkgids)
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

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

Voor ondernemers die willen weten hoe ze 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