Cyberveiligheid in de detail- en groothandel

Digitale winkel populair onder cybercriminelen

In de retail zijn online verkoopkanalen inmiddels gemeengoed. Uitbreiding of verhuizing naar het digitale domein stelt detail- en groothandels in staat om hun afzetmarkt te vergroten. Toch kleeft er ook een risico aan al die besteltools en webshops: ze zitten vol met persoons- en betaalgegevens van klanten. Interessante buit voor hackers, en bovendien heeft een websitestoring direct grote operationele en financiële gevolgen. Detail- en groothandels doen er goed aan vooral op te passen voor datalekken, skimmen en de daaruit volgende reputatieschade. In de sector komt bijvoorbeeld gijzelsoftware, CEO-fraude en fraude door eigen medewerkers voor.

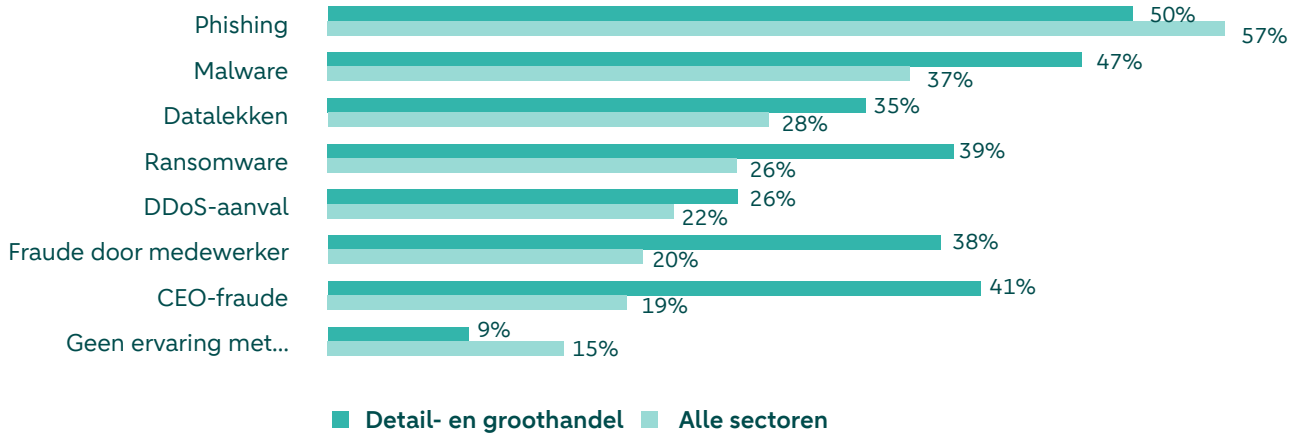
Recente cyberaanvallen in de sector

- Sofie de Decker, de eigenaar van kledingwinkel Via Sophia, kwam er in de zomer van 2023 achter dat haar persoonlijke Facebook-pagina was gehackt. Hierdoor had ze ook geen toegang meer tot haar zakelijke account en belangrijkste marketingkanaal: de vijftienduizend volgers waar ze jarenlang zorgvuldig in had geïnvesteerd, was ze plotseling kwijt.
- In oktober 2022 werden groothandel Makro en moederbedrijf Metro gehackt. Tijdens het herstel van de IT-infrastructuur stuitten ze op eerder onopgemerkte malware en verdachte activiteiten. Als gevolg hiervan zijn persoonsgegevens van medewerkers op het darknet terechtgekomen. Daarnaast lukte het tot december niet altijd om reclamefolders te verspreiden en kortingen toe te passen, en lagen zowel online kassasystemen als de bezorgdienst plat.
- Eind 2021 kreeg elektronicaketen MediaMarkt te maken met een cyberaanval van de criminele groep Hive. Die versleutelde gegevens, waardoor klanten geen producten konden afhalen en retourneren. De losgeldeis: vijftig miljoen dollar in bitcoin. Toen MediaMarkt aangaf dat niet te kunnen betalen, volgden twee weken van onderhandelingen. In die periode lukte het de retailer niet alleen om de eis te verlagen naar zo'n zes miljoen euro, maar ook om meer details over de hack los te weken én de eigen systemen te herstellen. Hierdoor heeft het bedrijf uiteindelijk geen losgeld hoeven betalen.
- De gevolgen van sommige cyberaanvallen zijn merkbaar in het dagelijks leven van veel mensen. Dit geldt bijvoorbeeld voor de hack van Tomra, de Noorse ontwikkelaar van statiegeldmachines. Honderden apparaten in Nederlandse supermarkten werkten niet of nauwelijks meer, doordat Tomra vanwege de aanval een aantal systemen moest uitschakelen. Hierdoor kon de ontwikkelaar geen updates meer uitvoeren of storingen op afstand oplossen. Volgens beveiligingsbedrijf Eset Nederland laat dit zien hoe belangrijk adequate beveiliging van digitale apparaten is.

ABN·AMRO

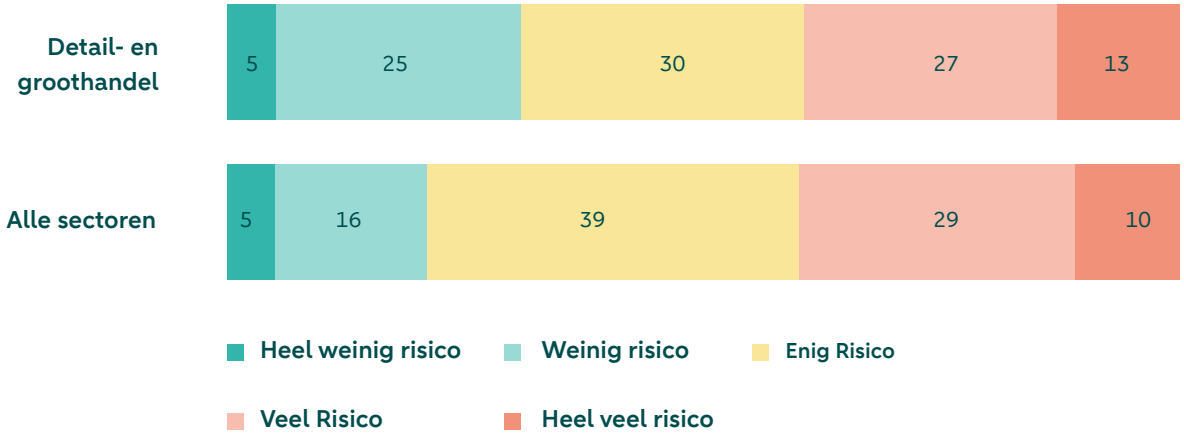
Retail krijgt bovengemiddeld veel te maken met dreiging van 'binnenuit'

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



Detail- en groothandels achten risico op cyberdreiging klein

*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.

Binnen de gezondheidszorg vallen de belangrijke of essentiële entiteiten van bedrijven onder de NIS2, waaronder:

- Supermarkten
- Digitale aanbieders
- Tank- en laadstations

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