Cyberveiligheid in de gastvrijheidseconomie

De gastvrijheidssector krijgt opvallend vaak met phishingaanvallen te maken

Van reserveren tot betalen: gasten kunnen steeds meer digitaal. Dat maakt de sector kwetsbaar. Enerzijds zullen cybercriminelen geïnteresseerd zijn in waardevolle persoonsgegevens, anderzijds trekt het grote aantal financiële transacties de aandacht. Alles in de sector gebeurt bovendien mobiel: gasten regelen hun hotelkamer, vliegticket en taxi allemaal met hun smartphone. We zien in de vrijetijdssector bovengemiddeld veel phishing, *dark hotel attacks* en malware-aanvallen – bedrijven moeten dus maatregelen nemen om dit soort aanvallen tegen te gaan, om zo reputatieschade te voorkomen.

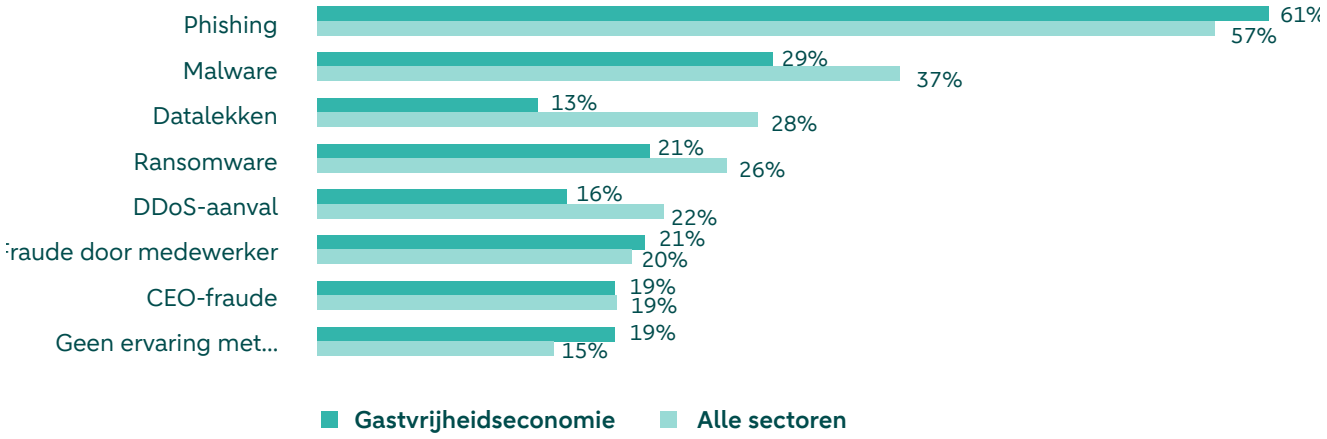
Recente cyberaanvallen in de sector

- In maart 2023 lekten de gegevens van duizenden bezoekers die meededen aan een onderzoek voor Vrienden van Amstel Live. Onderzoeksbureau Blauw voerde de enquête uit, in opdracht van Heineken. Door een datalek bij het softwarebedrijf waar Blauw mee werkt, lagen de gegevens van 22.000 enquête-afnemers op straat.
- Een onbekend aantal hotels op Booking.com was in 2023 doelwit van een phishingaanval. Gasten kregen mails uit naam van hotels, waarin ze werden aangespoord om een bestand met malware te downloaden. Booking.com geeft aan te blijven investeren in cybersecurity – bijvoorbeeld door zelflerende systemen in te zetten om verdachte activiteiten op te sporen.
- Met behulp van gijzelsoftware wist hackersgroep LockBit in maart 2023 persoonsgegevens te stelen van de KNVB. Om te voorkomen dat de hackers de gegevens zouden verspreiden, betaalde de voetbalbond uiteindelijk een flink bedrag aan losgeld – volgens RTL Nieuws gaat het om ruim € 1 miljoen.
- In de zomer van 2021 vond er bij New York Pizza een groot datalek plaats. Het systeem werd gehackt, waarbij bijna vier miljoen klantgegevens werden gestolen. Veel klanten kregen daarna een phishingmail van het bedrijf. De pizzaketen heeft een onderzoek ingesteld naar de hack, aangifte gedaan bij de politie en melding gemaakt bij de Autoriteit Persoonsgegevens.

ABN·AMRO

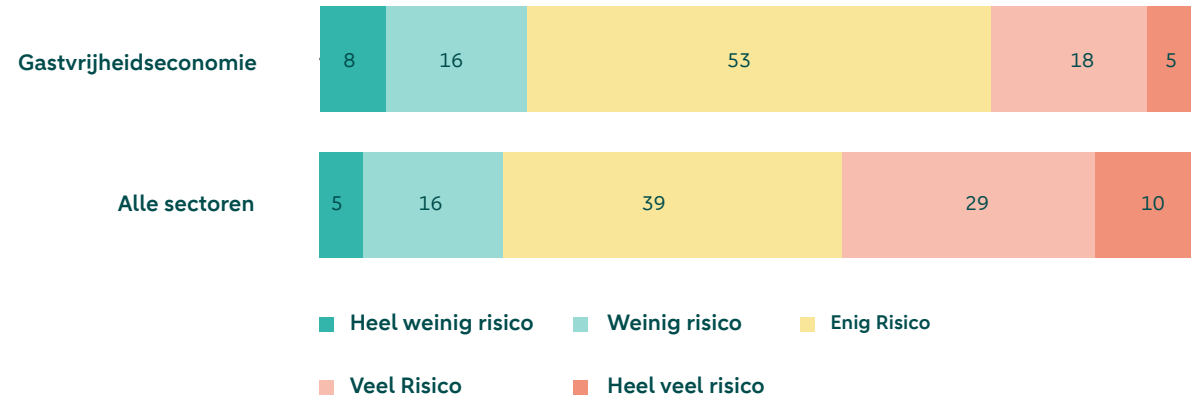
Bovengemiddeld veel phishing in de gastvrijheidssector

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



Leisure-bedrijven lopen naar eigen inschatting 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). 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.

In de gastvrijheidseconomie werken maar liefst 752.270 mensen. De NIS2-wetgeving geldt voor bedrijven met minimaal vijftig werknemers, of een jaaromzet en balanstotaal van meer dan € 10 miljoen. Dat betekent dat de wet straks van toepassing is op vrijwel alle ketens van hotels, restaurants en vakantieparken, evenals de meeste grote dagattracties en touroperators.

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