Wie voor VSA kiest,
kiest voor gemak,
veiligheid en zekerheid.

NIS2
VSA - Specialisten in IT

Digitale veiligheid in de hotelsector: NIS2

De Europese **NIS2-richtlijn** stelt strengere eisen aan de digitale weerbaarheid van organisaties binnen vitale sectoren én hun toeleveringsketens.

Hoewel hotels op dit moment niet direct onder de NIS2-verplichting vallen, bevinden zij zich in een risicocategorie vanwege hun intensieve verwerking van persoonsgegevens, afhankelijkheid van digitale systemen en samenwerking met NIS2-plichtige organisaties.

Deze whitepaper helpt u als hotelier om inzicht te krijgen in wat NIS2 inhoudt, wat de implicaties zijn voor uw hotel en welke stappen u nu al kunt nemen om digitaal weerbaar te blijven.

www.vsa.nl

VSA 30 jaar
Specialisten in IT

Essentiële schakel in de keten

Hotels verwerken dagelijks privacygevoelige informatie van gasten, medewerkers en leveranciers, zoals paspoortgegevens en creditcardinformatie. Dit maakt hen een aantrekkelijk doelwit voor cybercriminelen.

Omdat veel hotels deel uitmaken van grotere ketens of intensief samenwerken met leveranciers van IT-diensten, reserveringssystemen en facilitaire diensten, verwacht NIS2 dat de gehele keten aantoonbaar veilig is.

Als hotelier draagt u niet alleen zorg voor uw eigen systemen, maar vervult u ook een essentiële rol binnen het bredere netwerk van digitale veiligheid. Zijn uw processen al ingericht op de eisen die partners u binnenkort kunnen stellen?

VSA 30 jaar
Specialisten in IT

Wat is NIS2?

De NIS2-richtlijn *(Network and Information Security 2)* is geen wet maar een Europese richtlijn die door lidstaten geïmplementeerd wordt in nationale wetgeving, zoals in Nederland met de Cyberbeveiligingswet.

De richtlijn benadrukt maatregelen op het gebied van netwerk- en informatiebeveiliging, incidentmelding en risico's in toeleveringsketens.

Hotels dienen rekening te houden met de mogelijkheid dat de Nederlandse overheid in de toekomst kan besluiten om ook hotels als NIS2-plichtig aan te merken.

VSA 30 jaar
Specialisten in IT

Wanneer wordt NIS2 actief?

28 november 2022: De EU neemt de NIS2-richtlijn* aan.

2023–2024: Nederland bereidt invoering voor via de Cyberbeveiligingswet.

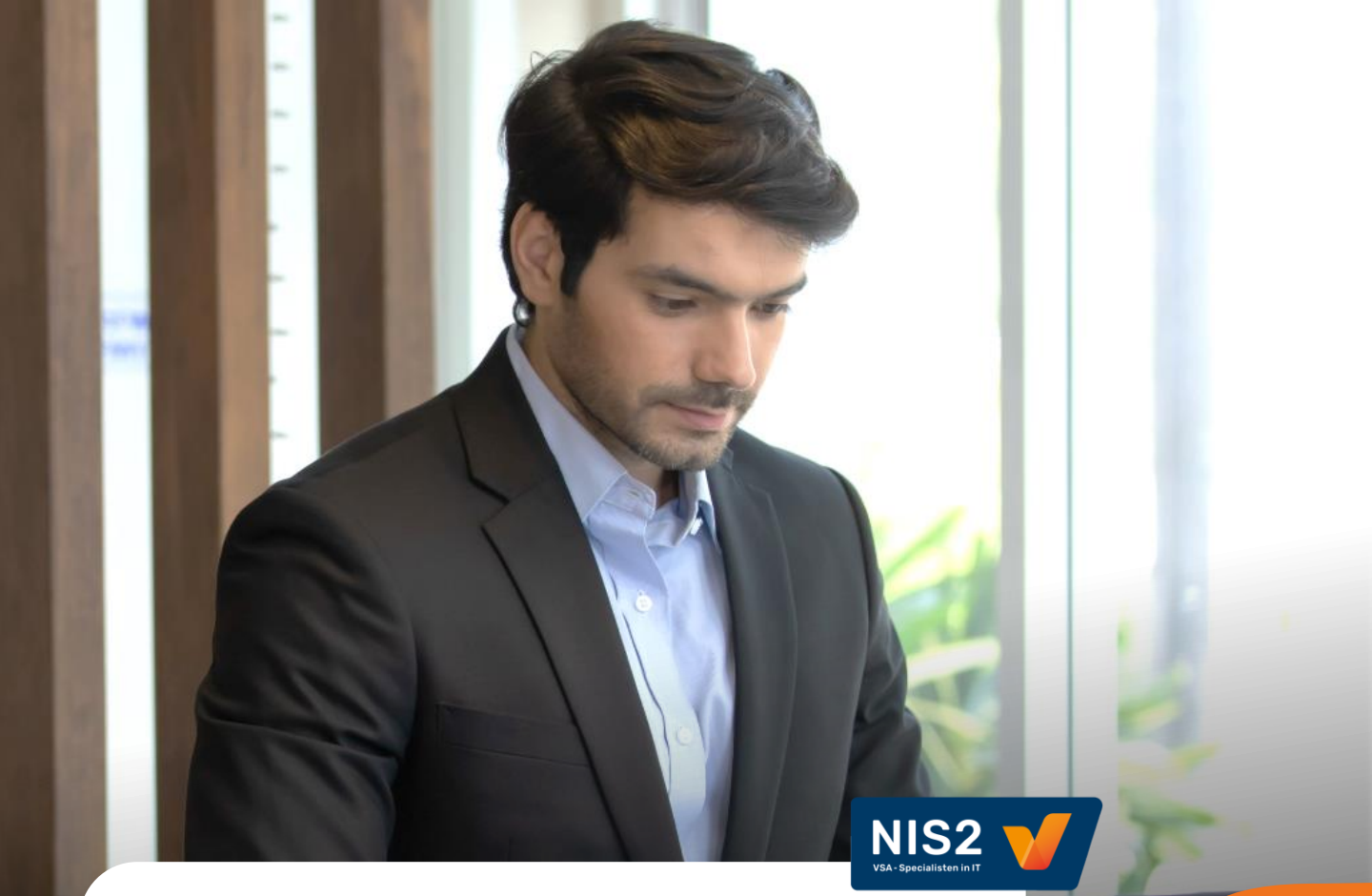
Zomer 2025: De Nederlandse wet op basis van de NIS2-richtlijn treedt in werking. Vanaf dat moment moeten aangewezen organisaties voldoen aan de verplichtingen zoals opgenomen in deze nationale wetgeving.

**NIS2 is een Europese richtlijn, geen wet. Lidstaten – zoals Nederland – zijn verplicht deze richtlijn om te zetten in nationale wetgeving.*

De richtlijn geldt voor:

1. Essentiële organisaties
2. Belangrijke organisaties
3. Ketenpartners (zoals hotels)
4. Kleine strategische doelwitten
5. Overige aangewezen organisaties

VSA 30 jaar
Specialisten in IT



Wat is het doel van NIS2?

De NIS2-richtlijn is opgesteld om de digitale weerbaarheid van vitale sectoren en hun toeleveringsketens in Europa te versterken.

Belangrijkste doelen:

- Verhogen van de **cybersecurity** binnen essentiële en belangrijke sectoren.
- Zorgen voor een **uniform niveau van digitale bescherming** binnen de EU.
- **Voorkomen van verstoringen** in kritieke diensten door cyberaanvallen.
- Verantwoordelijkheid leggen bij zowel organisaties als hun **ketenpartners.**
- Bevorderen van **samenwerking en transparantie** tussen bedrijven en overheden bij incidenten.

VSA 30 jaar
Specialisten in IT

NIS2
VSA - Specialisten in IT

Waar moet uw hotel wettelijk aan voldoen?

Hotels zijn verplicht om te voldoen aan de AVG en worden geacht passende maatregelen te nemen als ketenpartner. Dit betekent:

- **Zorgplicht:** Voer risicoanalyses uit en neem passende beveiligingsmaatregelen *(zie volgende slide).*
- **Meldplicht:** Meld datalekken (AVG) binnen 72 uur en digitale incidenten tijdig aan ketenpartners.
- **Registratie:** Nog niet verplicht, maar aansluiting op sectorinitiatieven en monitoring is aan te raden.
- **Toezicht**: NIS2-organisaties vallen onder *Rijksinspectie Digitale Infrastructuur*-toezicht. Hotels worden als ketenpartner geacht mee te bewegen.

VSA 30 jaar
Specialisten in IT

NIS2
VSA - Specialisten in IT

Welke maatregelen moeten er genomen worden?

Welke maatregelen moeten er genomen worden? Om te zorgen dat hotels voldoende voorbereid zijn op mogelijke toekomstige verplichtingen vanuit NIS2 en om hun positie als betrouwbare ketenpartner te versterken, dienen zij minimaal de volgende maatregelen te implementeren:

1. **Risicoanalyse van systemen**
2. **Beveiligingsbeleid**
3. **Back-ups en noodprocedures**
4. **Incidentmanagement**
5. **Training personeel**
6. **Beveiliging software**
7. **Screening leveranciers**
8. **Beleid voor encryptie**
9. **Veilige communicatie**
10. **Evaluatie beveiliging**

Door deze stappen nu al te zetten, blijven hotels een veilige schakel in hun keten en verminderen ze het risico op schade door toekomstige regelgeving of cyberincidenten.

VSA 30 jaar
Specialisten in IT

Gevolgen van nalatigheid

Boetes voor niet-naleving NIS2

Belangrijke organisaties:
Minimaal €7 miljoen of 1,4% van de wereldwijde jaaromzet.
Essentiële organisaties:
Minimaal €10 miljoen of 2% van de wereldwijde jaaromzet.

Wat als hotels geen maatregelen nemen?

Hoewel er momenteel geen directe wettelijke verplichting is, kan nalatigheid leiden tot verlies van partnerschappen en commerciële schade wanneer partners wel verplicht zijn te voldoen aan NIS2-normen.

Bestuurders van hotels dienen zich bewust zijn van deze risico's en proactief handelen.

VSA 30 jaar
Specialisten in IT

Wie voor VSA kiest,
kiest voor gemak,
veiligheid en zekerheid.

In drie stappen klaar voor NIS2

Hoe bereidt u zich voor?

QuickScan: Inzicht in uw situatie en de relevante maatregelen.

Plan van aanpak: Technisch, organisatorisch en juridisch advies.

Implementatie en borging: Uitvoering, training en evaluatie.

VSA begeleidt hotels stap voor stap bij het versterken van hun digitale weerbaarheid om voorbereid te zijn op eventuele toekomstige verplichtingen.

www.vsa.nl

www.vsa.nl | info@vsa.nl | +31 88 0120 530

VSA 30 jaar
Specialisten in IT