NIS2-richtlijn

KAAP HOORN
KAAPHOORN ICT SECURITY

Wat staat er in de wet?

De Network and Information Security-richtlijn (NIS2) is ontwikkeld door de Europese Unie en bestaat uit 13 eisen: Opleidingsplicht (1), Zorgplicht (2-12) en Meldplicht (13). Daarnaast worden organisaties die onder de richtlijn vallen, onder toezicht geplaatst. De richtlijn is gericht op de verbetering van de digitale weerbaarheid van belangrijke en essentiële diensten en organisaties.

De Europese datum voor de implementatie van de NIS2-richtlijn is vastgesteld op 17 oktober 2024. Op deze datum zullen veel landen binnen de EU de nieuwe NIS2-richtlijn gaan invoeren.

NIS2-vereisten

We delen de NIS2 eisen onder in:

1 Opleidingsplicht (1)

Bestuurders, commissarissen en toezichthouders moeten een opleiding doen waarmee ze voldoende kennis en vaardigheden opdoen om risico's op het gebied van cyberbeveiliging

2 Zorgplicht (2-12)

De organisatie moet een risicobeoordeling (laten) uitvoeren. Op basis daarvan moeten er passende maatregelen worden genomen om essentiële diensten te beschermen.

3 Meldplicht (13)

De organisatie moet incidenten die de essentiële dienstverlening ernstig kunnen verstoren binnen 24 uur melden aan de toezichthouder.

Waarom komt de wet er?

De reden waarom Europa met deze nieuwe NIS2 richtlijnen komt is om te voorkomen dat cybersecurityincidenten mogelijk leiden tot situaties waarin grote aantallen Europese burgers ernstige hinder zouden ondervinden.

Wanneer komt de wet er?

De NIS2-wet bestaat nog niet en heet officieel de Europese NIS2-richtlijn. Op 1 juli 2025 wordt de NIS2 opgenomen in de Nederlandse Wet beveiliging netwerk- en informatiesystemen (Wbni).

NULMETING

Risico beoordeling o.b.v. de CIS18-controls, een internationaal erkend raamwerk voor best practices op het gebied van informatiebeveiliging.

- **Nulmeting**: Tijdens de nulmeting zullen we de huidige IT- en beveiligingsprocessen in kaart brengen, inclusief technische, organisatorische en procesmatige aspecten. Op basis hiervan voeren we een gap-assessment uit waarin we de huidige situatie van uw organisatie vergelijken met de vereisten van de NIS2-richtlijn, aangevuld met de best practices van de CIS18.

GAP-ANALYSE

Dit traject begint met een nulmeting van de bestaande beveiligingsmaatregelen, gevolgd door een gedetailleerde gap-analyse.

- **Analyse:** Een grondige analyse van de technische en organisatorische beveiligingsmaatregelen.
- **Beoordelen:** Beoordeling van risicobeheersing, toegangsbeheer, netwerkbeveiliging, incidentmanagement, en data-integriteit.
- **Gap:** De ontbrekende of onvoldoende beveiligingsmaatregelen (gaps) die nodig zijn om NIS2-compliance te bereiken.

Voor wie geldt wat?

Onder de NIS2-richtlijn vallen entiteiten die bij uitval van diensten zorgen voor een ontwrichtende impact op de economie en de samenleving. Hierbij wordt een onderscheid gemaakt tussen 'essentiële' en 'belangrijke' entiteiten.

Essentiële sectoren	Belangrijke sectoren
Organisaties met minimaal 250 werknemers of een jaaromzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro in de volgende sectoren.	Organisaties met minimaal 50 werknemers of een jaaromzet en balans totaal van meer dan 10 miljoen euro in de volgende sectoren.
• **Energie:** Elektriciteit, gas, olie, district verwarming. • **Vervoer:** Luchtvaart, spoor, watervervoer (zowel maritiem als binnenlands), wegtransport. • **Bankwezen:** Financiële instellingen, zoals banken. • **Infrastructuur van de financiële markt:** Beursplatforms, betalingsdiensten. • **Gezondheidszorg:** Ziekenhuizen, klinieken, gezondheidscentra, inclusief digitale zorg. • **Drinkwater en afvalwaterbeheer:** Distributie en zuivering van water. • **Digitale infrastructuur:** Internetaanbieders, datacenters, DNS-dienstverleners. • **Ruimtevaart:** Infrastructuren die essentieel zijn voor ruimtevaartactiviteiten.	• **Post- en koeriersdiensten.** • **Afvalbeheer.** • **Voedsel:** Productie, verwerking en distributie van levensmiddelen. • **Fabrikanten van bepaalde producten:** Bijvoorbeeld fabrikanten van medische apparatuur, farmaceutische producten, chemische stoffen, en elektronische componenten. • **Digitale aanbieders:** Cloudcomputing, online marktplaatsen, zoekmachines.

Kijk voor meer informatie op: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Er is geen officiële lijst om te controleren of jouw organisatie onder een van deze sectoren valt. De overheid gaat ook geen officiële lijst beschikbaar stellen.

Ook als je niet onder de belangrijke of essentiële entiteiten valt, kun je als toeleverancier te maken krijgen met de NIS2.

Opleidingsplicht (1)

Directie en bestuur moeten een opleiding volgen om cybersecurity beter te begrijpen en te kunnen managen. Dit is geen IT-feestje; het moet een onderwerp voor de board worden. Net zoals we BHV-oefeningen doen, moeten we ook regelmatig cybersecurity-oefeningen houden.

OPLEIDING

Bestuurder dienen op de hoogte te zijn van de laatste ontwikkelingen, bedreigingen en maatregelen in cybersecurity.

VERANTWOORDELIJK

Bestuurders zijn verantwoordelijk voor het waarborgen van de naleving van de NIS2-richtlijnen binnen hun organisatie, inclusief risicomanagement en incidentrespons.

BIJSCHOLEN

Bestuurders moeten worden bijgeschoold om adequaat te kunnen reageren op veranderende dreigingslandschappen.

AANSPRAKELIJK

Als een organisatie niet voldoet aan de NIS2-verplichtingen en dit leidt tot een incident, kunnen bestuurders persoonlijk aansprakelijk worden gesteld.

De beste hackers ter wereld hou je niet tegen met basismaatregelen.
Maar met 20% van de maatregelen ben je al 80% veiliger.

Wat valt er onder de zorgplicht (2-12)?

De organisatie moet een risicobeoordeling (laten) uitvoeren. Op basis daarvan moeten er passende maatregelen worden genomen om essentiële diensten te waarborgen en informatie te beschermen.

1. **Procedures gebruikerstoegang**
Een logische toegangsbeveiligingsprocedure zorgt ervoor dat alleen geautoriseerde medewerkers toegang hebben tot systemen, applicaties en data die nodig zijn voor hun werkzaamheden.

2. **Periodieke risico-analyse**
Periodieke risico-analyses uitvoeren ten aanzien van cyberbeveiliging en aantonen dat op basis van de uitkomsten maatregelen genomen worden om de beveiliging te verbeteren.

3. **Proces voor opvolgen cyberincidenten**
Het proces voor de opvolging van cyberincidenten (Incident Response Plan) heeft als doel om zo snel mogelijk te reageren op een incident en de impact ervan te minimaliseren.

4. **Zicht op de cybersecurity van leveranciers**
Het proces omvat het evalueren van de cybersecurity van leveranciers, het monitoren van hun activiteiten en het nemen van passende maatregelen om eventuele zwakke plekken te verhelpen.

5. **Veilige netwerk- en informatiesystemen**
Om vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen en risico's op cyberaanvallen te minimaliseren dienen er voldoende beveiligingsmaatregelen te worden geïmplementeerd.

6. **Volledig zicht op aanvalsoppervlakte**
De ICT-omgeving van uw organisatie is wellicht groter dan waar u zicht op heeft. Het is vereist om volledig zicht te krijgen en te houden op de ICT-omgeving.

7. **Verantwoordelijke voor naleven van de zorgplicht**
Het bestuur van de NIS2-entiteit is eindverantwoordelijk voor het naleven van de zorgplicht. Zij kunnen voor het niet naleven aansprakelijk worden gesteld.

8. **Bedrijfscontinuïteitsplannen**
Beleid, procedures en maatregelen waarmee de continuïteit van uw organisatie kan worden gewaarborgd in het geval van onvoorziene omstandigheden of calamiteiten worden verplicht.

9. **Beleid ten aanzien van encryptie**
Een encryptiebeleid zorgt ervoor dat alle gevoelige en vertrouwelijke informatie van klanten en medewerkers goed beschermd wordt.

10. **Managementproces voor kwetsbaarheden**
Om veilig te blijven voor kwetsbaarheden, moeten organisaties een combinatie van technische en operationele maatregelen gebruiken om kwetsbaarheden te identificeren en te verminderen

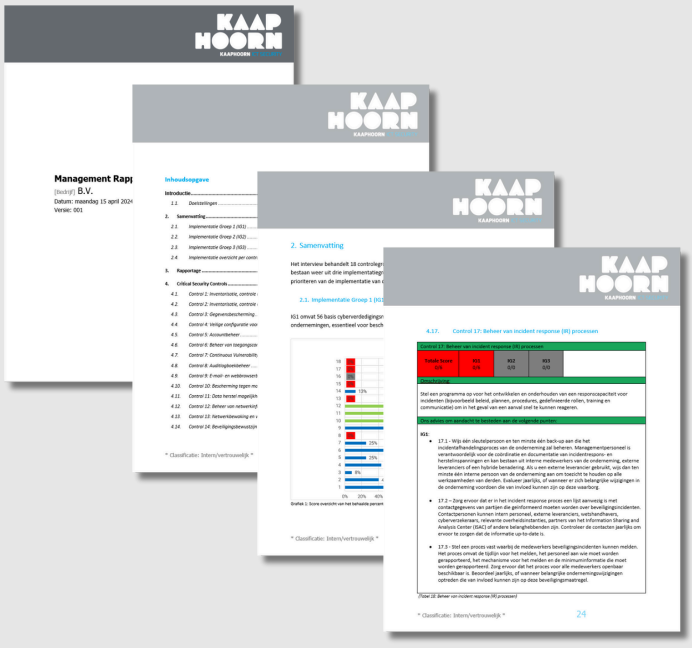
11. **Evaluatieproces cyberbeveiligingsmaatregelen**
Evalueren van de beveiligingsmaatregelen op basis van de laatste ontwikkelingen op gebied van cybersecurity, testen van maatregelen en maatregelen om zwakke plekken te verhelpen.

12. **Multifactor authenticatie process**
Het multifactor authenticatie proces is een extra beveiligingslaag die gebruikt wordt om de toegang tot gevoelige informatie te beschermen.

RAPPORTAGE

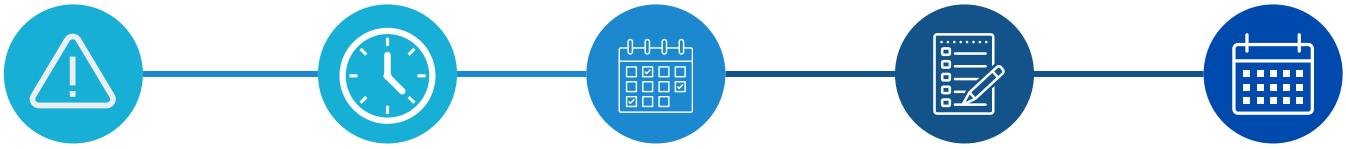
Wat kunt u verwachten van onze rapportage?

- We analyseren uw huidige beveiligingsbeleid en identificeren sterke punten en mogelijke zwakke plekken.
- Onze experts zullen specifieke acties voorstellen om uw beveiliging te verbeteren. Geen vage suggesties, maar praktische stappen die u meteen kunt implementeren.



Meldplicht (13)

Organisaties moeten incidenten die de essentiële dienstverlening ernstig kunnen verstoren binnen 24 uur melden aan de toezichthouder. Cyberincidenten moeten ook worden gemeld bij het Computer Security Incident Response Team (CSIRT), dat vervolgens hulp en bijstand kan verlenen. Criteria voor meldingswaardige incidenten zijn onder andere het aantal getroffen personen, de duur van de verstoring en mogelijke financiële verliezen.



INCIDENT

Een incident is een gebeurtenis die de beveiliging, beschikbaarheid, integriteit, of vertrouwelijkheid van netwerk- en informatiesystemen negatief beïnvloedt.

BINNEN 24 UUR

Geef een vroegtijdige waarschuwing dat er een significant cybersecurity incident heeft plaatsgevonden.

BINNEN 72 UUR

Geef een initiële beoordeling met belangrijke details over het incident.

STATUSVERSLAG

Op verzoek van de CSIRT of relevante authoriteit.

BINNEN 1 MAAND

Lever een eindrapport dat het incident, de oorzaak en de genomen maatregelen beschrijft.

"Organisaties die onder de richtlijn vallen, worden onder toezicht geplaatst. Een onafhankelijke toezichthouder zal de naleving van de verplichtingen, zoals de zorg- en meldplicht controleren. Momenteel wordt uitgewerkt welke sectoren onder welke toezichthouder komen te vallen."

National Cyber Security Centre (NCSC)

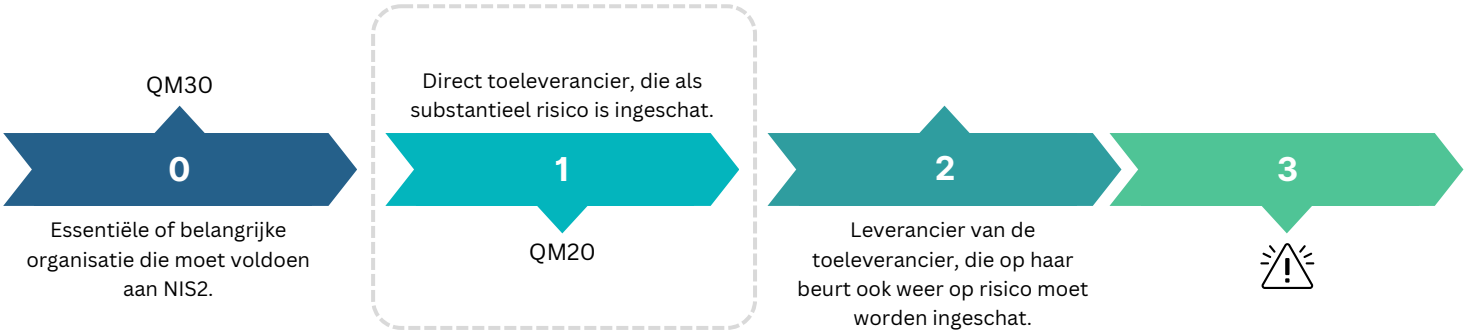
Zorg voor een procedure om beveiligingsincidenten binnen 24 uur te rapporteren aan de bevoegde autoriteiten.

Leveranciers

Risico-inventarisaties brengen in kaart welk risico samenwerken met een leverancier met zich mee kan brengen. Met name gaat het hier over de impact die een leverancier heeft op jouw bedrijf of organisatie als de leverancier wordt getroffen door een cybersecurityincident.

Leverancierskеten

In dit voorbeeld is het cascade risico in beeld gebracht van de toeleverancierskеten.



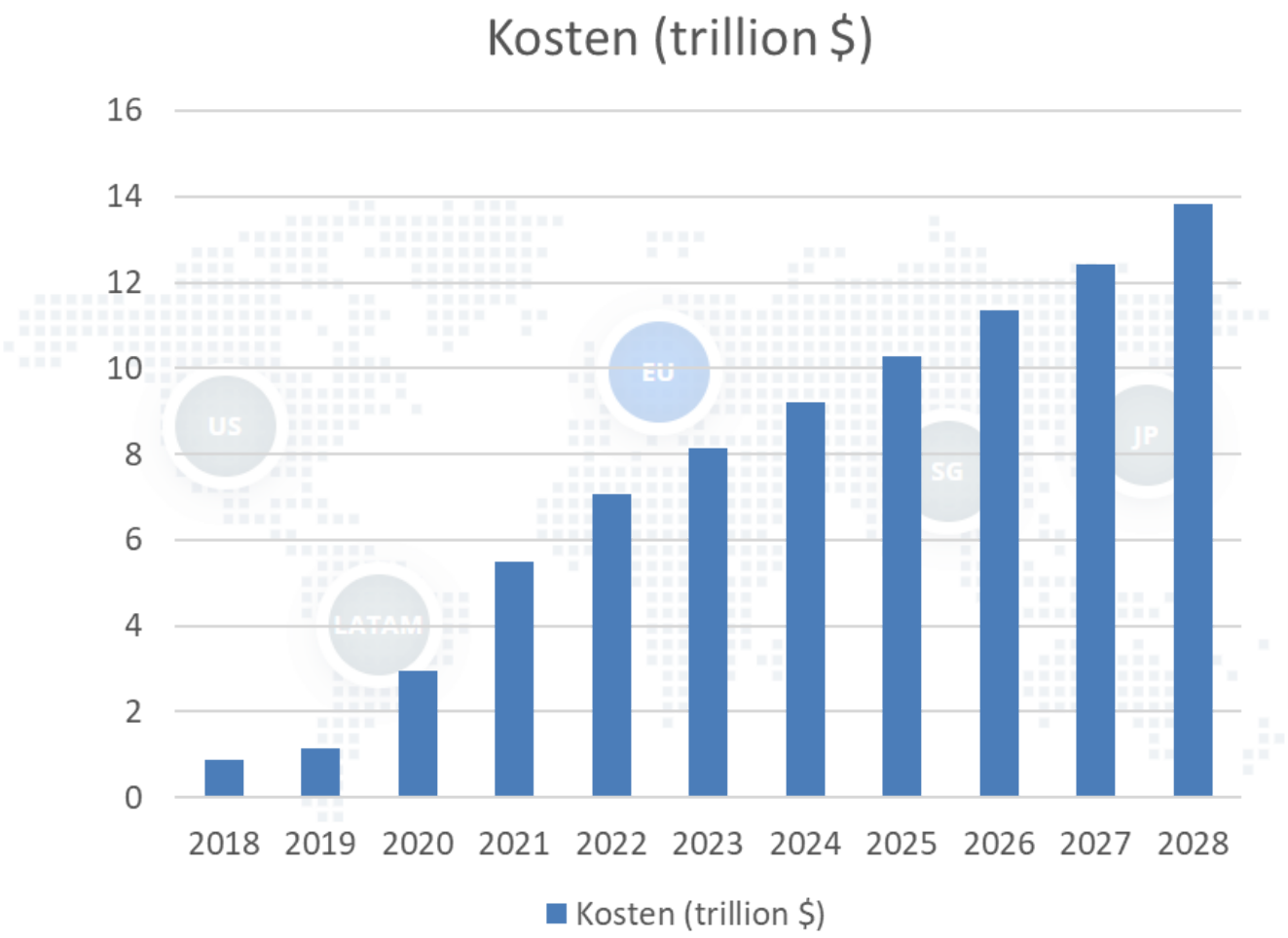
"Er zijn ongeveer 10.000 essentiële en belangrijke (vaak grote) organisaties en bedrijven in Nederland die cybersecuritymaatregelen moeten gaan opleggen aan al hun directe toeleveranciers op basis van artikel 21.2d van de NIS2-richtlijn. Het aantal maatregelen dat opgelegd moet worden is afhankelijk van de risico-inventarisatie die elk bedrijf moet gaan maken voor elk van zijn toeleveranciers."

Samen Digitaal Veilig

Essentiële en belangrijke bedrijven moeten samenwerken met hun directe leveranciers om de toeleveringsketen te beveiligen.

Wacht niet te lang

Ondanks dat het nog even duurt, benadrukt het ministerie het belang van vroegtijdige voorbereidingen op de NIS2 richtlijn, gezien de ernstige tekorten aan cybersecurityspecialisten en de voortdurende dreiging van cybercriminaliteit.



"Volgens schattingen zullen de wereldwijde kosten van cybercrime de komende vier jaar fors stijgen, van $9,22 biljoen in 2024 naar $13,82 biljoen in 2028. Cybercrime wordt vaak alleen in verband gebracht met ransomware, waardoor er als gevolg verstoring van de normale bedrijfsvoering na een aanval optreedt. Echter, de financiële gevolgen van forensisch onderzoek, herstel en verwijdering van gehackte data en systemen, en reputatieschade worden vaak ernstig onderschat."

Statista's Market Insights

Een veilige omgeving begint met een 360-graden aanpak.

Over ons

We doen allemaal dat wat we het beste kunnen en voor ons is dat cyber security. Daarmee dragen wij ons steentje bij aan een prettigere en veiligere samenleving. Samen staan we sterk.

Contactgegevens

We leren u graag kennen om samen te bepalen wat we voor u kunnen betekenen. Voor een vrijblijvende kennismaking, bel of mail ons.

Telefoon: 0229 799 800
E-mail: kasperdewaard@kaaphoorn.net