De NIS 2 komt eraan; een Quick Scan

De nieuwe Europese 'cyber security'-richtlijn is niet mals: bedrijfsleven, bereid je voor!

Ieder Europees bedrijf, groot of klein, dat 'essentiële activiteiten' uitvoert of zakendoet met een 'essentieel' bedrijf valt per 2023 onder nieuwe 'cyber security'-richtlijnen.
Een hoop Nederlandse bedrijven zullen volgend jaar ineens niet meer aan Europese wetgeving voldoen.
Waar moet je straks allemaal aan voldoen? Hier lees je hoe het zit.

Europa is druk bezig met wetgeving op het gebied van cyber security zoals de 'NIS 2'.
Deze Quick Scan heeft betrekking op de wijziging van de zg. NIS-richtlijn (te weten: NIS 2) en de mogelijke gevolgen voor de Wet beveiliging netwerk- en informatiesystemen.

De NIS 2 richtlijn is een richtlijn die overal in de EU een steeds grotere hoeveelheid organisaties (m.n. bedrijven met een groot belang voor economie en maatschappij) dwingt de kwaliteit van hun cybersecurity naar een hoger niveau te brengen en een bepaalde minimum cybersecurity moet garanderen.

NIS staat voor de richtlijn 'Network and Information Security'. Deze richtlijn komt uit 2016, en binnenkort komt daar dus **de NIS 2** (zwaardere) versie van. De NIS is in Nederland geïmplementeerd in de **Wet beveiliging netwerk- en informatiesystemen (Wbni)** en heeft in de basis drie pijlers van beveiliging:

1. Security risico's in kaart brengen
2. Risico's beperken door bescherming en detectie
3. De gevolgen van cyberincidenten beperken

Deze drie pijlers zijn de basis van de beveiligingseisen voor vitale sectoren zoals ze vaak worden aangeduid (ook wel digitale dienstverleners en aanbieders van essentiële diensten genoemd).

Zoals het er nu uitziet gaat het **in de NIS 2 om de volgende sectoren**:

- energie,
- vervoer,
- bankwezen,
- financiële marktinfrastructuren,
- gezondheidzorg,
- drinkwater,
- afvalwater,
- digitale infrastructuur,
- ruimtevaart,
- post- en koeriersdiensten,
- afvalbeheer,
- chemie,
- voedingsproductie,
- industrie,
- openbaar bestuur,
- overheidsorganisaties en
- digitale aanbieders.

NIS 2 is ook bedoeld om de veiligheid van toeleveringsketens te verbeteren door de eis voor individuele bedrijven om cyberveiligheidsrisico's in toeleveringsketens en leveranciersrelaties te beheersen. De voorgestelde wijzigingen hebben ook tot doel de cyberbeveiliging van de toeleveringsketen voor belangrijke informatie- en communicatietechnologieën op Europees niveau te versterken.
Deze Quick Scan bevat een (juridische) duiding van de inhoud van de beoogde nieuwe regelgeving en tevens een duiding van de mogelijke strategische en organisatorische gevolgen ervan.

1. Inleiding NIS richtlijn - Wbni

De Europese Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de 'NIS-richtlijn') was het eerste stuk EU-wetgeving op het gebied van cyberbeveiliging. Deze richtlijn beoogde de digitale weerbaarheid van de Europese Unie te vergroten en de gevolgen van cyberincidenten te verkleinen.
Deze richtlijn is in Nederland geïmplementeerd in de Wbni die in 2018 in werking is getreden.

De Wbni bevat een zorgplicht en meldplicht voor aanbieders van essentiële diensten (AED's) en andere vitale aanbieder, zoals energie of drinkwater, Luchtverkeersleiding Nederland of KvK én digitale dienstverleners (digital service provider, DSP's), zoals onlinemarktplaatsen en -zoekmachines en cloud- computerdiensten. Aanbieders van Essentiele Diensten (AED's) worden aangewezen in het

Besluit beveiliging netwerk- en informatiesystemen. Dit is een Algemene Maatregel van Bestuur (AMvB).
De Wbni verplicht vitale aanbieders en DSP's om passende technische en organisatorische maatregelen te nemen ter beveiliging van hun netwerk- en informatiesystemen (zorgplicht). Ook verplicht de Wbni deze groepen om ernstige ICT-incidenten te melden bij de voor hen aangewezen instantie voor de verlening van bijstand bij digitale dreigingen en incidenten (Computer security incident response teams, CSIRT) en bij de bevoegde autoriteit die belast is met toezicht en handhaving (meldplicht).
Daarnaast regelt de Wbni het toezicht op en de handhaving van de naleving van deze verplichtingen. Het toezicht is belegd bij sectorale toezichthouders, zoals Agentschap Telecom.

De minister van JenV is verantwoordelijk op het terrein van cybersecurity. De daarbij behorende taken en bevoegdheden worden in de praktijk uitgevoerd door het Nationaal Cyber Security Centrum (NCSC). Het NCSC heeft als primaire taak om vitale aanbieders en aanbieders die deel uitmaken van de rijksoverheid te informeren en te adviseren over digitale dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen en hen in dat kader bijstand te leveren bij het treffen van maatregelen. Ook heeft het NCSC de taak om ten behoeve daarvan analyses en technisch onderzoek te verrichten. Het NCSC kan bij de uitoefening van zijn primaire taken de beschikking krijgen over dreigings- en incidentinformatie over de netwerk- en informatiesystemen van aanbieders die niet behoren tot de doelgroep (vitaal en rijksoverheid). Deze aanbieders worden ook wel "andere aanbieders" genoemd. De Wbni regelt dat het NCSC die data kan delen met in de Wbni genoemde schakelorganisaties. Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten.

In december 2020 heeft de Europese Commissie een voorstel ingediend, dat een jaar later door de Raad is overgenomen, om de NIS-richtlijn te vervangen. In de nieuwe NIS 2-richtlijn moeten de beveiligingseisen aangescherpt, de beveiliging van toeleveringsketens aangepakt de rapportageverplichtingen gestroomlijnd en strengere toezichtmaatregelen en handhavingsvereisten ingevoerd worden, waaronder geharmoniseerde sancties in de hele EU. Het voorstel kent ook een uitgebreid toepassingsgebied, waarbij meer entiteiten en sectoren worden verplicht maatregelen te nemen. Dit alles zou het niveau van cyberbeveiliging in Europa op de langere termijn moeten verhogen.

Omdat het om een richtlijn gaat, moet deze door de EU-lidstaten in hun nationale wetgeving worden omgezet. De termijn hiervoor is twee jaar na de datum van inwerkingtreding van de richtlijn. Het is te verwachten dat voor Nederland de richtlijn NIS 2 zal worden opgenomen in de nieuwe Wbni.

Hierna wordt in deze notitie de inhoud van NIS 2 verder uitgewerkt en wordt een inschatting gegeven van wat de wijziging van NIS 2 voor een gevolgen heeft voor nationale wetgeving.

2. Inhoud - hoofdlijnen NIS 2

- NIS2 breidt het toepassingsgebied van de huidige richtlijn uit door nieuwe sectoren toe te voegen. De richtlijn gaat voor de volgende sectoren gelden: energie, vervoer, bankwezen, financiële marktinstellingen, gezondheid, drinkwater, afval-water, digitale infrastructuur, overheidsdiensten, ruimtevaart, post- en koeriersdiensten, afvalbeheer, chemie,

voeding, industrie, en digitale aanbieders. Tevens zal het onderscheid tussen exploitanten van essentiële diensten en aanbieders van digitale diensten wordt opgeheven.

- Naast een uitbreiding van de sectoren die onder NIS 2 gaan vallen, verscherpt het de beveiligingseisen door het opleggen van een aanpak voor risicobeheersing met een lijst van minimale basisbeveiligingselementen die toegepast moeten worden. Ook zullen meer precieze bepalingen over de procedure voor incidentenmelding, de inhoud van de meldingen en de termijnen voorgeschreven gaan worden.
- Entiteiten (zoals in Nederland de NCSC) moeten elkaar en het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) op de hoogte brengen van belangrijke cyberincidenten en -dreigingen. Een nieuw op te richten Europees Netwerk van verbindings-organisaties voor cybercrises (EU-CyCLONe, https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management) dient de samenwerking tussen de autoriteiten van lidstaten te verbeteren en het delen van informatie te faciliteren.
- Daarnaast stelt de Europese Commissie voor om de veiligheid van toeleveringsketens en relaties met leveranciers aan te pakken. Door individuele bedrijven te verplichten cyberbeveiligingsrisico's in toeleveringsketens en relaties met leveranciers en/of partners aan te pakken.
- Tot slot zullen strengere toezichtmaatregelen voor nationale autoriteiten, harmonisatie van sanctieregelingen en rapportageverplichtingen in de lidstaten en strengere handhavingsvereisten gaan gelden.

3. Uitwerking algemeen van NIS 2 - Wbni

- Werkingssfeer uitgebreid
  De huidige NIS-richtlijn (Wbni) heeft tot doel de cyberbeveiliging te versterken in sectoren die sterk afhankelijk zijn van informatietechnologie, met een focus op de bescherming van kritische infrastructuur (energie, vervoer, infrastructuur voor banken en de financiële markt, gezondheid, drinkwater, digitale infrastructuur) en bepaalde digitale dienstverleners in de EU-lidstaten.
  De voorgestelde NIS2-richtlijn voorziet in een ruimere dekking van sectoren en diensten die van vitaal belang worden geacht voor de Europese interne markt. Naast de genoemde sectoren die al onder de huidige richtlijn vallen, worden nieuwe sectoren in het toepassingsgebied opgenomen, waaronder telecommunicatie, chemicaliën, levensmiddelen, post- en koeriersdiensten, bepaalde industrieën, overheidsdiensten, platforms voor sociale netwerken, ruimtevaart, afvalbeheer en afvalwaterbeheer. Verder zullen entiteiten van het openbaar bestuur van centrale overheden onder NIS2-richtlijn vallen, en kunnen lidstaten besluiten om het toepassingsgebied uit te breiden tot soortgelijke entiteiten op regionaal en lokaal niveau.

- Sectorspecifieke regelgeving
  Wordt de voorgestelde NIS2-richtlijn goedgekeurd, dan zal deze van toepassing zijn naast sectorspecifieke wetgeving. De belangrijkste daarvan om hier te vermelden is de onlangs voorgestelde ‘DORA’-verordening inzake digitale operationele veerkracht voor de financiële sector.

- Extraterritoriale werking uitgebreid
  Ten slotte wordt de extraterritoriale werking van de richtlijn uitgebreid. Daardoor vallen aanbieders van digitale infrastructuur of digitale diensten die weliswaar geen Europese vestiging hebben, maar wel diensten die onder de NIS 2-richlijn vallen aanbieden in de EU, ook

onder het toepassingsgebied van de voorgestelde NIS 2-richtlijn. Dit zal onder meer gevolgen hebben voor aanbieders van cloud computing-diensten, aanbieders van datacenterdiensten en andere online dienstverleners zoals marktplaatsen, zoekmachines en sociale netwerken.

- Essentiële en belangrijke entiteiten
  In de voorgestelde NIS 2-richtlijn wordt niet langer een onderscheid gemaakt tussen aanbieders van essentiële diensten en aanbieders van digitale diensten, maar worden entiteiten ingedeeld in 'Essentieel' en 'Belangrijk'. Voor zowel Essentiële als Belangrijke entiteiten zullen dezelfde eisen inzake een actief cyberbeveiligingsbeheer en rapportage gelden, maar de toezichts- en sanctieregelingen zullen verschillen. Terwijl voor Essentiële entiteiten een volwaardig ex ante toezicht-regime zal gelden, geldt voor Belangrijke entiteiten een lichter ex post toezicht in het geval van bewijzen of aanwijzingen van niet-naleving.

- 'Size-cap'
  In het voorstel voor de NIS 2 richtlijnen wordt, in plaats van de huidige identificatie van individuele aanbieders op nationaal niveau, een 'size-cap' ingevoerd die binnen de genoemde sectoren alle middelgrote en grote ondernemingen bestrijkt. Kleinere entiteiten zijn vrijgesteld, tenzij zij een hoog veiligheidsrisicoprofiel hebben. Bij de bespreking van het voorstel zijn aanvullende criteria toegevoegd om te bepalen welke entiteiten onder NIS2-richtlijn moeten vallen.

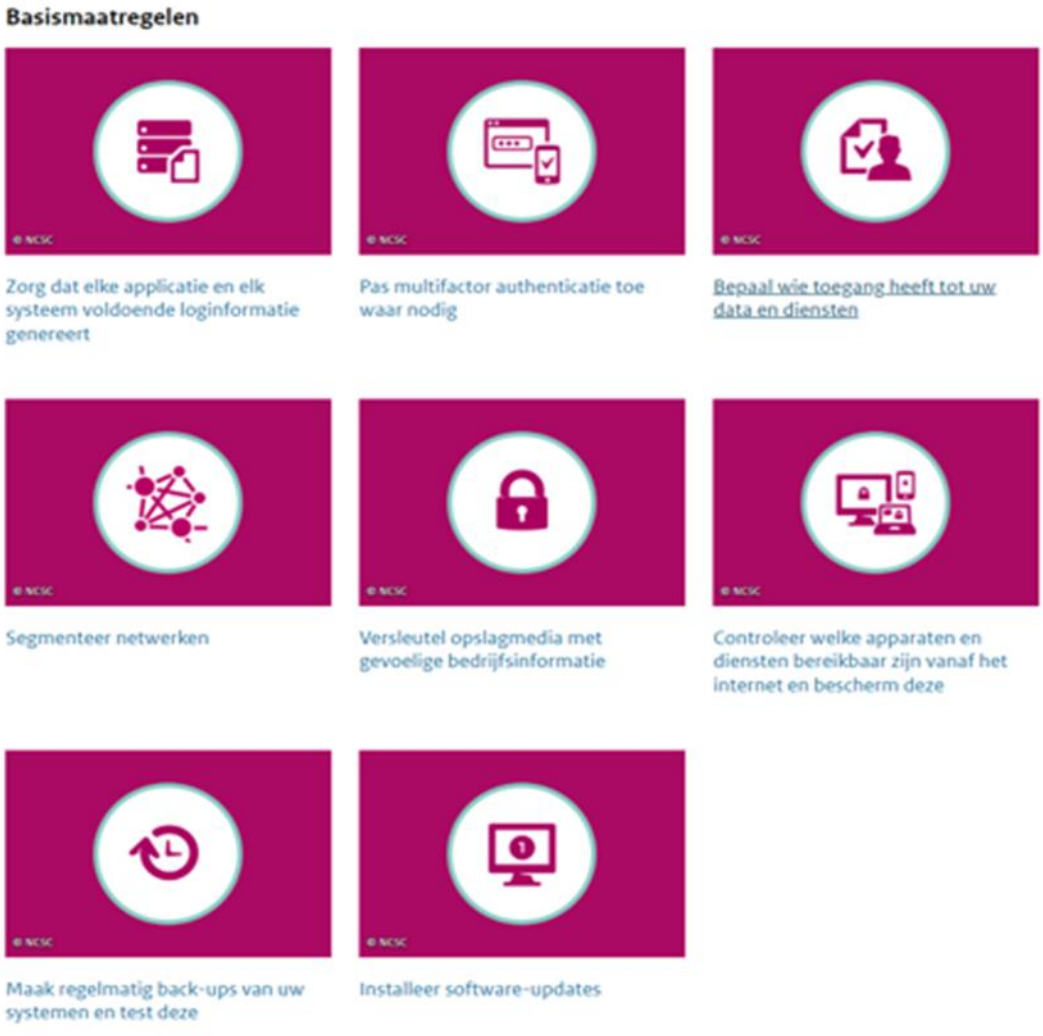
- Governance
  De nieuwe regels voeren voor het eerst expliciete governance-vereisten in, op grond waarvan het bestuur van entiteiten die vallen binnen het toepassingsbereik van de NIS 2-richtlijn maatregelen voor het managen van cyberbeveiligingsrisico's moet goedkeuren en daarop toezicht moet houden. Ook moet het bestuur cyberbeveiligingstrainingen volgen.

- Aansprakelijkheid
  In de nieuwe richtlijnen is ook sprake van een expliciete aansprakelijkheid voor elke natuurlijke persoon die verantwoordelijk is voor of optreedt als vertegenwoordiger van een essentiële entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om toezicht uit te oefenen op deze entiteit. Een dergelijke persoon/personen dienen nl. de bevoegdheid te hebben om ervoor te zorgen dat deze entiteit de in deze richtlijn vastgestelde verplichtingen nakomt. De lidstaten zorgen ervoor dat deze natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om de in deze richtlijn vastgestelde verplichtingen na te komen (art. 29, lid 6 van de richtlijn).

- Rapportage
  Ook worden rapportageverplichtingen uitgebreid. Zo zullen alle Essentiële en Belangrijke entiteiten moeten rapporteren over incidenten die een aanzienlijke impact hebben op de levering van hun diensten.
  Het betekent dat niet alleen datalekken (bij de Autoriteit Privacy), maar ook cybersecurity incidenten (bij de NCSC) zullen moeten worden gemeld en gerapporteerd.

- Hogere boetes
  Het meest in het oog springende element van het pakket aan nieuwe maatregelen is misschien dat de EU-lidstaten aanzienlijk hogere administratieve boetes kunnen opleggen die kunnen oplopen tot ten minste 10 miljoen Euro of 2% van de totale wereldwijde omzet (op ondernemingsniveau), naargelang welk bedrag het hoogst is, met de intentie dat hierop ook strenger zal worden gehandhaafd. In overeenstemming met de strengere handhavingsregeling die op hen van toepassing is, kunnen voor Essentiële entiteiten die in gebreke blijven, ook vergunningen worden geschorst of kan het hoger management worden geschorst in de uitoefening van zijn leidinggevende functies (telkens totdat de nodige corrigerende maatregelen zijn genomen). Het is nog de vraag of dit onder Nederlands recht zal leiden tot mogelijke bestuurdersaansprakelijkheid.

- Minimale beveiligingselementen



  Wat het cyberbeveiligingsrisicobeheer zelf betreft, wordt in de voorgestelde herziening de open norm gehandhaafd dat, gelet op de stand van de techniek en het aanwezige risico, ‘passende’ en ‘evenredige’ maatregelen moeten worden genomen. Nieuw is dat een aantal minimale basisbeveiligingselementen wordt toegevoegd waarin in elk geval moet worden voorzien.
  https://www.ncsc.nl/onderwerpen/basismaatregelen
  Belangrijk is dat de voorgestelde NIS 2-richtlijn in afwijking van de huidige NIS-richtlijn expliciete eisen invoert voor het beheer van risico's van derden in toeleveringsketens en relaties met

leveranciers en partners. Daarmee wordt een van de belangrijkste uitdagingen op het gebied van cyberbeveiliging van dit moment aangepakt. Het voorstel bepaalt dat de Europese Commissie de technische en methodologische specificaties van de minimumeisen zal vaststellen, en voorziet dat entiteiten kunnen (en bepaalde Essentiële entiteiten: moeten) aantonen dat zij aan de eisen voldoen door een cyberbeveiligingscertificering te verkrijgen.

- Openbaarmaking van kwetsbaarheden
  Belangrijk is ten slotte dat de voorgestelde NIS 2-richtlijn gecoördineerde praktijken voor de openbaarmaking van kwetsbaarheden introduceert, waarbij een entiteit buitenstaanders (vaak 'ethische hackers') uitnodigt om kwetsbaarheden te melden op een manier die het mogelijk maakt een diagnose te stellen en de kwetsbaarheid te verhelpen voordat deze aan derden wordt bekendgemaakt (en mogelijk door derden wordt misbruikt). Daartoe zou het EU-cyberbeveiligingsagentschap ENISA een Europees kwetsbaarheidsregister moeten ontwikkelen en bijhouden om Belangrijke en Essentiële entiteiten en hun leveranciers van netwerk- en informatiesystemen in staat te stellen kwetsbaarheden in ICT-producten of ICT-diensten bekend te maken en te registreren.

4. Kernboodschap

De afgelopen decennia is de maatschappij, inclusief kritische sectoren als vervoer, energie, gezondheidszorg en financiën, steeds afhankelijker geworden van digitale technologieën om kernactiviteiten uit te voeren. Het stelt de samenlevingen echter ook bloot aan cyberdreigingen. Het aantal, de complexiteit en de omvang van cyberincidenten nemen toe, evenals hun economische en sociale impact. De wereldwijde schadepost door ransomware alleen al bedroeg in 2021 naar schatting US$ 20 miljard. Ook de situatie in verband met de oorlog in Oekraïne laat een toename zien van cyberincidenten. Het licht daarom voor de hand dat de wetgeving rondom informatiebeveiliging wordt uitgebreid en verscherpt.

Ook de Nationaal Coördinator Terrorismebestrijding en Veiligheid acht het beschermen van een veilig digitaal Nederland van cruciaal belang (https://www.nctv.nl/themas/cybersecurity).
Het is van belang om de richtlijnen van de nieuwe Wbni op te volgen en op te nemen in een actief beleid en programma conform het nieuwe informatiebeveiligingsbeleid.

5. Inwerkingtreding - planning

Europees Parlement en Raad hebben op 13 mei 2022 een politiek akkoord over cybersecurity richtlijn bereikt. Nu het politiek akkoord tussen het Europees Parlement en de Raad is bereikt zal het eerst door de twee medewetgevers formeel dienen te worden goedgekeurd. Twintig dagen na de bekendmaking daarvan in het Publicatieblad van de EU zal de NIS 2-richtlijn dan in werking treden, waarna de lidstaten de nieuwe elementen ervan in nationaal recht moeten omzetten, voor Nederland in de nieuwe Wbni. De lidstaten hebben hiervoor 21 maanden de tijd. De verwachting is dat de nieuwe Wbni eind 2024 van kracht zal worden.
https://ecer.minbuza.nl/-/europees-parlement-en-raad-bereiken-politiek-akkoord-over-cybersecurity-richtlijn

6. Klanten en toeleveranciers

NIS 2 in relatie tot uw klanten
Hoewel deze maatregelen vooral op het bordje van de IT-afdeling van een onderneming lijken te liggen, is het belangrijk dat ook de bedrijfsjurist zich hierin verdiept. Zo zou hij of zij over de risico's van cyberincidenten zich onder andere de volgende vragen kunnen stellen over contracten met klanten:

- Zijn klanten aangemerkt als Essentiële Aanbieder dan wel Belangrijke Aanbieder (op het moment dat de NIS 2-richtlijn van kracht is) ?
- En zo ja, welke aanvullende verplichtingen ten aanzien van het voorkomen van cyberincidenten zijn van toepassing?
- Welke verplichtingen voor het voorkomen van cyberincidenten worden door klanten opgelegd (ook als het geen Essentiële Aanbieders of Belangrijke Aanbieders zijn)?
- Welke beveiligingsverplichtingen voor geleverde 'as a service' diensten worden er opgelegd met betrekking tot het voorkomen van cyberincidenten?

NIS 2 in relatie tot uw toeleveranciers
Niet alleen contracten met klanten zijn van belang om tegen het licht te houden. Ook toeleveranciers spelen ingevolge de NIS2-richtlijn in toenemende mate een rol in het voorkomen van cyberincidenten.
Daarnaast zullen klanten steeds vaker eisen dat afgesproken cybermaatregelen worden doorgelegd aan toeleveranciers.
Dit alles maakt het relevant om onder meer de contracten met toeleveranciers te bekijken. Een rol die lijkt te zijn weggelegd voor de bedrijfsjurist waarbij hij of zij zich de volgende vragen zou kunnen stellen:

- Worden toeleveranciers verplicht om organisatorische en technische maatregelen te nemen die de beschikbaarheid van producten en/of diensten waarborgen?
- Welke beveiligingsstandaarden worden aan toeleveranciers opgelegd?
- Worden toeleveranciers verplicht om eventuele kwetsbaarheden en beveiligingsincidenten in producten en/of diensten te herstellen?
- Worden toeleveranciers verplicht om voor langere periode te voorzien in (kosteloze) beveiligingsupdates en upgrades van geleverde software?
- Is er in overeenkomsten met toeleveranciers een audit right opgenomen ten aanzien van afspraken die over het voorkomen van cyberincidenten zijn gemaakt en zo ja, worden deze toeleveranciers bij aanvang van de overeenkomst als ook gedurende de looptijd van de overeenkomst hierop ge-audit?
- Is er in overeenkomsten met toeleveranciers een meld- en informatieplicht ten aanzien van cyberincidenten opgenomen?

7. Cyberincidenten
Hoezeer een organisatie zich ook van het voorgaande rekenschap geeft, zal iedere organisatie op enig moment in directe of indirecte zin te maken krijgen met cyberincidenten. Dat kan zijn bij de organisatie zelf, maar dit kan ook toeleveranciers en klanten overkomen. Het is dan ook belangrijk om goed voorbereid te zijn op dergelijke incidenten en waar mogelijk deze te voorkomen.

Bereid je in je organisatie voor en oefen regelmatig. Zorg dat er een Incident Response Team paraat staat en is voorbereid op dit soort incidenten. Betrek de IT-afdeling, Corporate Security, Communicatie en Insurance. Bij een groot incident is het verstandig om de lijnen met het bestuur open te houden. Als het een incident betreft bij een toeleverancier, betrek dan de betreffende inkoper en als het bij een klant is het sales contact om contact te blijven houden met de klanten. Oefen regelmatig met incidenten en let op of men op tijd de juiste informatie boven tafel kan krijgen.

Als leidraad kan het verstandig zijn om het antwoord op deze tien vragen paraat te hebben liggen:

- Wat zijn de meest waarschijnlijke incidenten en welke rollen moeten daarbij vervuld worden?
- Zijn die rollen voor de organisatie helder?
- Wie is straks de functionaris gegevensbescherming en wil/kan/mag die persoon dat eigenlijk wel?
- Wat zijn de digitale kroonjuwelen binnen mijn organisatie?
- Zijn er externe specialisten on call die daadwerkelijk voor ons klaarstaan?
- Zijn de eventuele meldplichten alvast helder op een rijtje?

Bronvermelding

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf
https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2
https://www.ngb.nl/nieuws/nis2-richtlijn-cybersecurity-voer-voor-de-bedrijfsjurist
https://www.agconnect.nl/artikel/brussel-breidt-cybersecurityregels-uit-en-dreigt-met-boetes
https://www.emerce.nl/achtergrond/de-nieuwe-europese-cyber-security-richtlijn-is-niet-mals-mkb-bereid-je-voor
https://www.ncsc.nl/onderwerpen/basismaatregelen/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen