Bijlage I
De 13 NIS2 eisen, gedestilleerd uit richtlijn door BDO

Opleidingsplicht
1. Opleiding bestuur
Bestuursorganen moeten een opleiding doen waarmee ze voldoende kennis en vaardigheden opdoen om risico's op het gebied van cyberbeveiliging te herkennen en de gevolgen ervan te beoordelen op de diensten die de organisatie levert. Het is hierbij handig om tijdens de opleiding de opgedane kennis direct toe te passen op de organisatie. Met behulp van bijvoorbeeld een NIS2-checklist stelt het bestuur en de CISO samen vast in hoeverre de organisatie al klaar is voor NIS2. En maakt u afspraken om volledig voorbereid te zijn. Zo heeft u na de training direct een concreet actieplan om samen verder te werken.

Zorgplicht
2. Periodieke risico-analyse
U moet periodieke risico-analyse uitvoeren ten aanzien van cyberbeveiliging en aantonen dat op basis van de uitkomsten maatregelen genomen worden om de beveiliging te verbeteren.
Met periodieke risicoanalyses worden risico's voor de organisatie in kaart gebracht, en gewogen inclusief het inventariseren en beoordelen van beheersmaatregelen. Omdat risico's en de organisatie continue veranderen is de risicoanalyse een proces waarin dit regelmatig wordt geëvalueerd. Het is een belangrijk onderdeel van het overkoepelende risicomanagementproces waarin vervolgstappen worden bepaald om risico's naar een acceptabel niveau te brengen die passen bij de organisatie en risicobereidheid. De analyse is van toepassing op alle afdelingen en activiteiten van uw organisatie waarin risico's worden gemonitord en beheerst met adequate maatregelen.

3. Proces voor opvolgen cyberincidenten
Uw organisatie moet beschikken over een procedure om cyberincidenten passend op te volgen.
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. Het proces omvat het detecteren, analyseren en rapporteren van incidenten, evenals het nemen van maatregelen om de oorzaak van het incident te identificeren en te verhelpen.

4. Bedrijfscontinuïteitsplannen
Beleid, procedures en maatregelen waarmee de continuïteit van uw organisatie kan worden gewaarborgd in het geval van onvoorziene omstandigheden of calamiteiten worden verplicht.
Denk hierbij aan: back-up beheer, noodvoorzieningen, bedrijfscontinuïteitsplannen en incident respons plannen. Bedrijfscontinuïteitsplannen zorgen ervoor dat de activiteiten van uw organisatie kunnen blijven functioneren in geval van een calamiteit of noodsituatie. Het proces omvat het identificeren van de kritieke bedrijfsprocessen, het opstellen van plannen voor het behoud en herstel van deze processen, het testen van de plannen en het trainen van medewerkers om adequaat te reageren in geval van een noodsituatie.

5. Zicht op de cybersecurity van leveranciers
Zicht op en bijhouden van de staat en het niveau van cyberbeveiliging van uw leveranciers, is een belangrijk onderdeel van de NIS2-regelgeving. Het proces omvat het evalueren van de cybersecurity van leveranciers, het monitoren van hun activiteiten en het nemen van maatregelen om eventuele zwakke plekken te verhelpen.

6. Veilige netwerk- en informatiesystemen
Cyberbeveiliging structureel borgen bij verwerving, ontwikkeling en onderhoud van netwerk- en informatiesystemen. Om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen en de risico's op cyberaanvallen te minimaliseren dient u een voldoende beveiligingsmaatregelen te implementeren zoals firewalls, intrusion detection en prevention systemen, geavanceerde authenticatiemethoden en het monitoren van het netwerk en de systemen op mogelijke bedreigingen.

7. Volledig zicht op aanvalsoppervlakte (sub)domeinnamen.
De ICT omgeving van uw organisatie is wellicht groter dan waar u zicht op heeft. Vaak is er op het internet niet alleen allerlei informatie over de organisatie en werknemers te vinden maar kunnen er ook nog vergeten IT assets toegankelijk zijn. Over de tijd heen kunnen er bijvoorbeeld applicaties of systemen tijdelijk toegankelijk zijn gemaakt voor werknemers, klanten of leveranciers. Oude systemen zijn echter niet buiten gebruik gesteld, de externe omgeving is niet veilig geconfigureerd, er staan poorten open, of kwetsbare software is niet gepatched of niet actueel. Het is daarom vereist om volledig zicht te krijgen en te houden op de ICT omgeving.

8. Managementproces voor kwetsbaarheden
Vulnerabilities ofwel kwetsbaarheden zijn een zwakte of fout in software, netwerk, applicatie of ICT infrastructuur die door een aanvaller kan worden misbruikt om ongeoorloofde toegang te verkrijgen of schade aan het systeem te veroorzaken. Kwetsbaarheden kunnen in verschillende vormen voorkomen, waaronder softwarefouten, ontwerpfouten, configuratiefouten en zwakke authenticatiemechanismen. Deze kwetsbaarheden zijn een van de grootste oorzaken van cyberaanvallen door hackers en kunnen worden misbruikt voor ransomware, data diefstal of het verstoren van systemen. Om veilig te blijven voor kwetsbaarheden, moeten organisaties een combinatie van technische en operationele maatregelen gebruiken die zijn ontworpen om kwetsbaarheden te identificeren en te verminderen. Dit kan onder meer het gebruik van kwetsbaarheidsscanners, beveiligingsaudits, patchbeheer en penetratietesten omvatten.

9. Evaluatieproces van cyberbeveiligingsmaatregelen
Een Informatie Security Management Systeem (ISMS) is een gestructureerd en gedocumenteerd systeem dat organisaties helpt bij het beheren van hun informatie met als doel de effectiviteit van de beveiligingsmaatregelen te beoordelen en te verbeteren. Het ISMS omvat het evalueren van de beveiligingsmaatregelen op basis van de laatste ontwikkelingen op het gebied van cybersecurity, het testen van de maatregelen en het nemen van maatregelen om eventuele zwakke plekken te verhelpen.

10. Beleid ten aanzien van encryptie
Een encryptiebeleid zorgt ervoor dat alle gevoelige en vertrouwelijke informatie van klanten en medewerkers goed beschermd wordt. Dit gebeurt door middel van het versleutelen van data tijdens transport en opslag, het gebruik van sterke wachtwoorden en het beperken van toegang tot gevoelige informatie tot alleen geautoriseerde personen. Het beleid is van toepassing op alle systemen en apparaten die door een organisatie gebruikt worden, inclusief laptops en mobiele apparaten. Het doel van het encryptiebeleid is om de privacy en veiligheid van gevoelige informatie te waarborgen en te voldoen aan de wettelijke vereisten op het gebied van databeveiliging.

11. Procedures gebruikerstoegang
Een logische toegangsbeveiligingsprocedure zorgt ervoor dat alleen geautoriseerde medewerkers toegang hebben tot systemen, applicaties en data die nodig zijn voor hun werkzaamheden. Dit gebeurt door middel van het toekennen van unieke gebruikersnamen en sterke wachtwoorden, het beperken van toegang tot alleen die informatie die nodig is voor de uitvoering van de werkzaamheden en het gebruik van multi-factor authenticatie waar nodig. De procedure is van toepassing op alle systemen en applicaties die door een organisatie gebruikt worden, inclusief het netwerk en mobiele apparaten. Het doel van de logische toegangsbeveiligingsprocedure is om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen en te voldoen aan de wettelijke vereisten op het gebied van databeveiliging.

12. Multifactor authenticatie proces
Het multifactor authenticatie proces is een extra beveiligingslaag die gebruikt wordt om de toegang tot gevoelige informatie te beschermen. Het proces vereist dat gebruikers zich identificeren met twee of meer verschillende vormen van authenticatie, zoals een wachtwoord in combinatie met een token, biometrische gegevens of een smartcard. Het doel van het multifactor authenticatieproces is om de vertrouwelijkheid en integriteit van gevoelige informatie te waarborgen en te voorkomen dat onbevoegde personen toegang krijgen. Het proces is van toepassing op alle systemen en applicaties die door uw organistie gebruikt worden en wordt toegepast op gebruikers die toegang hebben tot gevoelige informatie. BDO kan in samenwerking met u in 1 dag een multifactorauthenticate procedure opstellen. Hiervoor maken wij gebruik van onze branchespecifieke templates.

13. Meldproces incidenten aan toezichthouders

Het meldproces aan toezichthouders heeft als doel om ervoor te zorgen dat eventuele incidenten of inbreuken op de beveiliging zo snel mogelijk worden gemeld aan de bevoegde toezichthouders. Het proces omvat het identificeren van de incidenten die gemeld moeten worden, het verzamelen van de relevante informatie en het indienen van de meldingen bij de betreffende toezichthouders. Het proces wordt uitgevoerd door het team dat verantwoordelijk is voor het beheer van de cybersecurity binnen uw organisatie. Het doel van het proces is niet alleen om te voldoen aan de wettelijke vereisten voor de melding van cybersecurity-incidenten maar ook om de reputatie van uw organisatie te beschermen.