De 10 zorgplichtmaatregelen uit de Cyberbeveiligingswet

De op handen zijnde Cyberbeveiligingswet (Cbw) schrijft tien maatregelen voor waar organisaties ten minste aan moeten voldoen. Voor onderwijs en onderzoek geldt dat het hbo en wo aan deze wet moeten gaan voldoen. Het Nationaal Cyber Security Centrum (NCSC) heeft een overzicht gemaakt van hun kennisproducten voor die tien maatregelen. Specifiek voor onze sector biedt SURF, via het Security Expertise Centrum, verschillende voorbeelden en hulpmiddelen aan die je kunnen helpen om deze maatregelen ook te nemen. Cyberbeveiligingswet of niet; onze sector is sowieso goed op weg!

Maatregel 1: Maak een risicoanalyse

Artikel 21 lid 2 sub a:
Beleid inzake risicoanalyse en beveiliging van informatiesystemen

Het uitvoeren van een risicoanalyse is een belangrijk startpunt voor het verbeteren van de cyberweerbaarheid van je organisatie. Het biedt inzicht in waar de grootste risico's liggen en maakt duidelijk op welke plekken beveiligingsmaatregelen het meest urgent zijn.

- De toolkit risicobeoordeling biedt praktische handvatten voor het uitvoeren van risicoanalyses binnen je instelling.
- Er zijn diverse templates beschikbaar, waaronder risicomanagementbeleid, een risicoregister, risicomatrix en procedures voor risicobeheer.
- SURF biedt regelmatig de training IT-risicobeoordeling aan. Hierin staan de basisprincipes van risicomanagement centraal en leer je hoe je een risicobeoordeling uitvoert. De actuele trainingsdata staan in de agenda op de SURF-website.

Maatregel 2: Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer

Artikel 21 lid 2 sub i:
Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa

Informatiebeveiliging begint bij de basis: mensen, toegang en systemen. Besteed daarom aandacht aan beveiligingsaspecten van personeel, toegangsbeheer en het inventariseren en beheren van je hardware en software. Denk daarbij aan vragen als: wie heeft toegang tot welke informatie, en met welke rechten? Door deze aspecten zorgvuldig te regelen en passende maatregelen te treffen, versterk je de cyberbeveiliging en vergroot je de veerkracht van je netwerk- en informatiesystemen.

- SURF biedt een beleidspiramide die houvast geeft bij het structureren van informatiebeveiligingsbeleid. Deze begint bij een template strategisch informatiebeveiligingsbeleid en wordt ondersteund door onderliggende standaarden, richtlijnen en procedures.
- Gebruik het beschikbare template voor HR-beleid, waarin aandacht is voor beveiligingsaspecten gedurende de hele medewerkerlevenscyclus.
- Bekijk ook de templates voor identiteits- en toegangsbeheer, die helpen bij het inrichten van rollen, rechten en autorisaties binnen je organisatie.

Maatregel 3: Maak een bedrijfscontinuïteitsplan

Artikel 21 lid 2 sub c:
Bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer

Langdurige verstoringen van primaire processen kunnen grote gevolgen hebben. Een bedrijfscontinuïteits-plan (BCP) helpt om voorbereid te zijn op incidenten zoals stroomuitval, cyberaanvallen of andere onverwachte gebeurtenissen. Met een goed doordacht BCP beperk je de impact van verstoringen en zorg je ervoor dat essentiële processen snel en gecontroleerd kunnen worden hervat.

- Het stappenplan helpt om stapsgewijs bedrijfscontinuïteitsmanagement binnen je organisatie op te zetten.
- Er zijn diverse templates beschikbaar, waaronder voor een business impact analyse (BIA), een bedrijfscontinuïteitsplan en het bijbehorende beleid.
- Gebruik de scenariokaarten en de handleiding voor tabletop-oefeningen om je organisatie voor te bereiden op verschillende soorten verstoringen en crisissituaties.

Maatregel 4: Richt Incident Response in

Artikel 21 lid 2 sub b:
Incidentbehandeling

Verstoringen, datalekken of cyberaanvallen kunnen grote impact hebben op je organisatie. Een snelle en doeltreffende reactie is essentieel om schade te beperken. Met een Incident Response Plan (IRP) leg je vast hoe je organisatie handelt bij een incident, zodat je gestructureerd en effectief kunt optreden op het moment dat het nodig is.

- SURFcert is het sectorale Computer Emergency Response Team (CERT) voor onderwijs en onderzoek. Lees de vijf meest gestelde vragen om snel inzicht te krijgen in de rol en huidige werkwijze van SURFcert. Met de aanwijzing van het hbo en wo krijgt SURFcert een andere en meer uitgebreide rol. SURF onderzoekt de verschillende scenario's met oog voor behoud van de collectiviteit.

- Technische securityspecialisten die werken bij een aangesloten instelling kunnen lid worden van SURF Community of Incident Response Teams (SCIRT). Hiermee blijven zij op de hoogte van actuele dreigingen en incidenten binnen de sector.
- Sta je aan de start van een CERT of ben je er net begonnen? Volg dan een van de TRANSITS-trainingen van SURF. Deze bieden een stevige basis in CERT-vaardigheden. De actuele data vind je in de agenda op de SURF-website.
- Wil je meer weten over incident response? Neem dan contact op met SURFcert of het Security Expertise Centrum.

Maatregel 5: Zorg dat cyberhygiëne op orde is

Artikel 21 lid 2 sub g:
Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging

Het vergroten van de cyberweerbaarheid begint bij inzicht in assets en risico's, maar daarmee stopt het niet. Het doorvoeren van basismaatregelen voor cyberhygiëne is een logische vervolgstap. Denk aan veilige wachtwoorden, up-to-date software en het herkennen van phishing. Door medewerkers te trainen in het naleven van deze basispraktijken, versterk je de weerbaarheid van je organisatie op de lange termijn.

- Met de Cybersave Yourself toolkit en de awarenessmetingen help je medewerkers bewust te worden van hun rol in cyberveiligheid en maak je hen tot een sterke schakel in de beveiligingsketen.
- De publicatie Voorbij de e-learning, mede ontwikkeld door SURF, biedt praktische handvatten om veilig digitaal gedrag te bevorderen — met aandacht voor effectievere interventies dan alleen e-learning.
- SURF organiseert regelmatig awarenesstrainingen voor security- en privacy-officers. Deze trainingen helpen om kennis over cyberrisico's te vergroten en veilig gedrag te stimuleren. Kijk voor actuele data in de Agenda op de SURF-website.

Maatregel 6: Schrijf beleid op de beveiliging van netwerk- en informatiesystemen

Artikel 21 lid 2 sub e:
Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden

Instellingen zijn sterk afhankelijk van hun netwerk- en informatiesystemen voor het uitvoeren van onderwijs en onderzoek (de primaire processen). Wanneer deze systemen niet beschikbaar zijn of wanneer gevoelige informatie uitlekt, kan dat grote impact hebben. Het is daarom belangrijk om maatregelen te treffen die dergelijke risico's beperken en de continuïteit van de bedrijfsvoering beschermen.

- De sector streeft gezamenlijk naar volwassenheidsniveau 3 op het SURFaudit toetsingskader informatiebeveiliging. Er zijn hiervoor diverse beleidstemplates beschikbaar die instellingen kunnen aanpassen aan hun eigen context. Zo is er onder andere een template voor een strategisch informatiebeveiligingsbeleid, waaronder specifieke beleidsdocumenten vallen, zoals beleid voor toegangsbeheer (zie maatregel 2) en bijbehorende handreikingen voor beveiligingsbeheer.
- Er zijn handreikingen beschikbaar gericht op het versterken van technische weerbaarheid waaronder weerstand bieden tegen ransomware, weerstand bieden tegen *Man-in-the-Middle* aanvallen, veilige cybersecurity configuraties in netwerken en het beveiligen van e-mail.

Maatregel 7: Maak je toeleveringsketen veilig

> *Artikel 21 lid 2 sub d:*
> *Beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners*

Veel instellingen zijn afhankelijk van producten en diensten van externe leveranciers. Digitale koppelingen maken deze afhankelijkheid nog groter: een beveiligingsprobleem bij één partij kan gevolgen hebben voor de hele keten. Het is van belang om passende maatregelen te nemen om de digitale toeleveringsketen te beveiligen.

- SURF biedt diverse templates en handreikingen voor het omgaan met leveranciers van ict-middelen. Deze ondersteunen je bij het beoordelen van risico's en het vastleggen van beveiligingseisen.
- De dienst SURF Vendor Compliance voert namens instellingen privacy- en securityrisicoanalyses uit op leveranciers. Hiermee geven we gezamenlijk invulling aan wettelijke verplichtingen. Door het bundelen van expertise realiseren we kostenbesparing, kennisdeling en hebben we namens de onderwijs- en onderzoekssector een sterkere onderhandelingspositie richting leveranciers.

Maatregel 8: Maak beleid op cryptografie en encryptie

> *Artikel 21 lid 2 sub h:*
> *Beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie*

Cryptografie speelt een cruciale rol in het beschermen van vertrouwelijke informatie. Door gegevens te versleutelen, zorg je ervoor dat alleen bevoegde personen gegevens kunnen lezen. Het is de basis om de vertrouwelijkheid en integriteit van bedrijfsgegevens en digitale assets te waarborgen. Encryptie, als toepassing van cryptografie, maakt gebruik van algoritmes om data veilig en onleesbaar te maken voor onbevoegden.

- Het template standaard voor cryptografie beschrijft de standaard voor cryptografie, inclusief de vereisten met betrekking tot het beheer van cryptografische sleutels en digitale certificaten gedurende hun levenscyclus. Daarnaast stelt het de principes vast die de basis vormen voor de Richtlijn Cryptografie en de Procedure Sleutelbeheer.

Maatregel 9: Gebruik MFA of andere beveiligde authenticatieoplossingen

> *Artikel 21 lid 2 sub j:*
> *Wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit*

Voor veilige toegang tot netwerken en informatiesystemen is het belangrijk dat gebruikers, apparaten en andere middelen betrouwbaar worden herkend. Het toepassen van meervoudige authenticatie (MFA) of continue authenticatie versterkt de controle op wie — of wat — toegang krijgt. Dit verkleint het risico op misbruik en vormt een belangrijke basis voor veilige bedrijfsvoering.

- De standaard voor Identiteits- en toegangsbeheer biedt een kader voor het inrichten van betrouwbaar toegangsbeheer binnen onderwijs en onderzoek.
- Onder deze standaard vallen verschillende richtlijnen, waaronder de richtlijn meervoudige authenticatie.

Maatregel 10: Hanteer processen om de effectiviteit van maatregelen te beoordelen

> *Artikel 21 lid 2 sub f:*
> *Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen*

Het regelmatig beoordelen van de effectiviteit van beveiligingsmaatregelen is van belang om risico's beheersbaar te houden en te voldoen aan wet- en regelgeving, zoals de NIS2-richtlijn. Door te evalueren wat goed werkt en waar verbeterpunten liggen, kun je gericht bijsturen. Dit vergroot het vertrouwen van interne en externe belanghebbenden en helpt je instelling om mee te bewegen met een voortdurend veranderend dreigingslandschap.

- Met het SURFaudit toetsingskader informatiebeveiliging breng je in kaart hoe ver je bent met de implementatie van beveiligingsmaatregelen en waar nog actie nodig is.
- Onze hulpmiddelen voor testen en oefenen geven een inzicht in of er gaten in de verdediging zitten en of iedereen weet wat ze moeten doen in het geval van een incident of crisis.

Interessante links

[1] NCSC, samenvatting NIS2-richtlijn
https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/samenvatting-nis2-richtlijn

[2] NCSC, informatiebrochure cyberbeveiligingswet
https://www.ncsc.nl/over-ncsc/documenten/brochures/2024/8/13/informatiebrochure-cyberbeveiligingswet

[3] NCSC, infosheet NIS2-verplichtingen: Meldplicht
https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/oktober/08/infosheet-meldplicht

[4] NCSC, infosheet NIS2-verplichtingen: Registratieplicht
https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/april/30/infosheet-registratieplicht

[5] NCSC, infosheet NIS2-verplichtingen: Zorgplicht
https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/februari/27/infosheet-nis2-verplichtingen-zorgplicht

[6] NCSC, overzicht van tien zorgplichtmaatregelen
https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn

[7] SURF, wat betekent de NIS2-richtlijn voor de leden van SURF
https://sec.surf.nl/richtlijn-netwerk-en-informatiebeveiliging-nis2-wat-betekent-het-voor-de-leden-van-surf/

[8] SURF, de NIS2-richtlijn bekeken vanuit publieke waarden
https://sec.surf.nl/nis-2-richtlijn-bekeken-vanuit-publieke-waarden/