Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Strategisch sturen op digitale weerbaarheid

Ben je de bestuurder van een organisatie die valt onder de nieuwe Network and Information Systems Directive 2 (NIS2) wetgeving en/of maakt jouw organisatie gebruik van Operational Technology (OT)? Maakt jouw organisatie bijvoorbeeld fysieke producten of beheer je fysieke processen zoals energieproductie, sluizen of transportsystemen? Dan is het belangrijker dan ooit dat je stuurt op de digitale weerbaarheid van jouw organisatie. Dit vraagt om maatregelen om jouw OT-omgeving te beschermen. Deze integratie vergt ook dat jouw organisatie de beveiliging van de OT-omgeving even serieus neemt als die van reguliere (IT)-omgevingen.

IACS *Coalitie*

De NIS2 en Operational Technology

De **NIS2-richtlijn**, in Nederland vertaald naar de **Cyberbeveiligingswet (Cbw)***, is wetgeving van de Europese Unie (EU) die beoogt de beveiliging van netwerken en informatiesystemen verder aan te scherpen. Het is de opvolger van de NIS-directive uit 2016, in Nederland beter bekend als de 'Wet beveiliging netwerk- en informatiesystemen' (Wbni). De nieuwe EU-richtlijn is een directe reactie op het **toenemende dreigingslandschap**, waarin cyberaanvallen frequenter en complexer worden. De achtergrond hiervan staat onder andere beschreven in het Cybersecurity Beeld Nederland (CSBN). De NIS2 is specifiek ontworpen om organisaties weerbaarder te maken tegen deze dreigingen door **strengere beveiligingseisen** te stellen aan organisaties.

Valt jouw organisatie onder de Cbw? Dan moet je, als bestuurder, ervoor zorgen dat jouw organisatie zicht heeft op haar cyberrisico's en passende en evenredige maatregelen (**zorgplicht**) treft om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie besloten in uw netwerken en informatiesystemen te beschermen. De Cbw schrijft daarbij een aantal maatregelen voor die jouw organisatie moet implementeren. Daarnaast moet jouw organisatie geregistreerd staan in het landelijk entiteitenregister (**registratieplicht**). Dit register is beschikbaar via het NCSC. Verder moet je significante incidenten melden bij de toezichthouder en het CSIRT (**meldplicht**). Onder significante incidenten vallen incidenten die een ernstige operationele verstoring van de diensten of aanzienlijke financiële verliezen voor de organisatie (kunnen) evenals incidenten waardoor derden aanzienlijke materiële of immateriële schade (kunnen) lijden.

* Wetsvoorstel ligt in de Tweede Kamer.

Jouw rol als bestuurder: Sturen op digitale weerbaarheid

Als bestuurder moet je toezien op de naleving van alle verplichtingen onder de Cbw. Zo dien je ervoor te zorgen dat jouw organisatie geregistreerd staat en effectief kan communiceren met toezichthoudende instanties en CSIRT's (Cyber Security Incident Response Teams - computercrisisteams) bij significante incidenten. Ook dien je op de hoogte te zijn van de cyberrisico's die jouw organisatie loopt, de beheersmaatregelen die deze risico's mitigeren goed te keuren en toe te zien op de uitvoering ervan.
Door cyberrisico's tijdig en continu te monitoren is jouw organisatie in staat om passende en evenredige maatregelen te treffen.
Cyberrisicomanagement voor IT en OT is niet anders dan het beheersen van andere bedrijfsrisico's, hoewel de gevolgen van een cyberaanval vaak ernstiger kunnen zijn vanwege de directe impact op fysieke processen. Als bestuurder heb je de verantwoordelijkheid om ervoor te zorgen dat cyberbeveiliging een kernonderdeel is van de risicobeheerstrategie van jouw organisatie.
Zorg ervoor dat:

1. Je een **effectief cyberrisicomanagementproces** faciliteert. Richt een duidelijk **proces** in met een duidelijke set **verantwoordelijkheden**. Als eindverantwoordelijke voor de organisatie ben je de eigenaar van dit proces en zal je hierbij nauw betrokken moeten zijn. De Cbw benadrukt dat het beheersen van **cyberrisico's** een continu proces is dat blijvende aandacht vereist, net zoals andere operationele of financiële risico's.
2. Jij en de relevante medewerkers uit jouw organisatie, een **goed begrip** hebben van jouw OT-systemen, de bedreigingen ten aanzien van jouw OT-systemen en hoe deze te beheersen. **Voldoende kennis** om risico's in te schatten en om mitigerende maatregelen goed te keuren en te implementeren is ook een eis vanuit de Cbw. De verplichte **opleiding** kan jou hierbij helpen.
3. Jij de eindverantwoordelijkheid neemt voor het informatiebeveiligingsbeleid en dit beleid goedkeurt. Dit beleid moet een heldere uiteenzetting zijn van de beheersmaatregelen die jouw organisatie toepast om cyberrisico's passend, evenredig en afdoende te mitigeren. Naast beleid omtrent risicobeheersing stelt de Cbw een aantal **elementen verplicht** als onderdeel van jouw informatiebeveiligingsbeleid, waaronder preventieve maatregelen, incidentrespons, opleiding van het management en supply-chain beveiliging. Ook ben je als bestuurder verantwoordelijk voor het **controleren van de effectiviteit** van jouw informatiebeveiligingsbeleid.

Het bestuur aan het stuur: Cyber als integraal onderdeel van risicomanagement voor OT

Als bestuur wordt van je verwacht dat je voldoende competenties en kennis hebt om te sturen op digitale weerbaarheid. Uiteraard kun je hierbij leunen op verschillende professionals binnen en buiten jouw organisatie. Denk bijvoorbeeld aan jouw CISO (Chief Information Security Officer), die gespecialiseerd is in het cyberrisicobeheersingsproces) of professionals die technische beveiligingsmaatregelen kunnen implementeren. Het is wel aan jou om grip te houden op de digitale weerbaarheid van jouw organisatie. Zoek je handvatten om jouw rol praktisch in te vullen? Begin door de volgende vragen aan de relevante medewerkers te stellen:

- Hebben we een volledig overzicht van onze OT-omgeving?
  - Zijn al onze OT- en IT-systemen en hun onderlinge afhankelijkheden in kaart gebracht?
  - Welke systemen zijn cruciaal voor de bedrijfscontinuïteit?
- Hebben we een robuust risicomanagementplan dat specifiek is gericht op OT?
  - Heeft de organisatie een juist en volledig beeld van de mogelijke dreigingen waar onze organisatie mee te maken kan krijgen?
  - Hebben we de noodzakelijke risico analyses uitgevoerd op onze netwerken en informatiesystemen en worden deze risicoanalyses periodiek herzien?
  - Hebben we de uit de risico analyses resulterende maatregelen geïmplementeerd?
  - Worden onze cyberrisico's regelmatig geëvalueerd en geprioriteerd?
  - Hebben we een strategie voor risicobeperking?
  - Zijn er regelmatige kwetsbaarheidsscans en penetratietests uitgevoerd op onze OT-systemen?
  - Worden deze resultaten geïmplementeerd in ons risicobeheerplan?
- Zijn we in staat om snel te reageren op een incident in onze OT-systemen?
  - Hebben we incidentresponsprocedures die specifiek gericht zijn op het beschermen van OT? Voldoet dit aan de tijdslijnen die in Cbw gesteld worden?
  - Kunnen we de productie voldoende snel herstellen in geval van een cyberaanval?
- Hoe goed is de samenwerking tussen onze OT- en IT-afdelingen?
  - Wordt er effectief gecommuniceerd en samengewerkt tussen de OT- en IT-teams?
- Is ons personeel voldoende getraind op het gebied van cyberveiligheid?
  - Hoe gaan we om met onze leveranciers en externe partijen?
  - Hebben we duidelijke beveiligingsrichtlijnen voor derden die toegang hebben tot onze OT-systemen?
  - Worden zij gecontroleerd op naleving van beveiligingsmaatregelen inclusief rapportage?

Meer weten?

Wil je meer weten over de Cbw en wat dit betekent voor jouw organisatie? Op deze pagina vind je hier meer informatie over: https://www.nctv.nl/onderwerpen/cyberbeveiligingswet/wat-betekent-de-cyberbeveiligingswet-voor-organisaties

Wil je actief aan de slag met het sturen op risicomanagement? Op deze pagina vind je meer informatie over het risicomanagementproces en hoe je effectief kunt sturen op effectieve informatiebeveiliging: https://www.ncsc.nl/wat-kun-je-zelf-doen/risicomanagement

Er zijn verschillende handvatten die jouw organisatie kan gebruiken voor het realiseren van passende weerbaarheid op jouw OT-systemen. Kijk hier voor de Routekaart risicomanagement | Wat kun je zelf doen? | Nationaal Cyber Security Centrum