Energie- en waterbedrijven doelwit voor cybercriminelen

Water en energie spelen een cruciale rol in ons dagelijks leven: als basisbehoefte, maar ook in ons huis of op het werk kunnen wij niet meer zonder. De technologische vooruitgang die onze water- en energievoorziening slimmer maakt, zorgt er tegelijk voor dat deze diensten kwetsbaarder zijn geworden voor cyberaanvallen. Veel van deze diensten zijn namelijk afhankelijk van informatietechnologie en internet.

De Wet beveiliging netwerk- en informatiesystemen (Wbni) stelt het treffen van adequate beveiligingsmaatregelen verplicht. Ook is er een meldplicht in het geval van een cyberincident. Op basis van deze wetgeving worden de energie- en watersector aangewezen als aanbieder van essentiële diensten en moeten ze aan een aantal aanvullende wettelijke eisen voldoen.

Maatregelen nemen tegen cyberaanvallen is verplicht

Zo zijn aanbieders van essentiële diensten verplicht om zorg te dragen voor adequate technische en organisatorische maatregelen, zodat de continuïteit van de aangeboden dienst kan worden gewaarborgd. Ook is er een meldplicht in geval van een cyberincident. Om compliant te blijven, is het dus essentieel om de technische en organisatorische maatregelen periodiek te evalueren.

Wij helpen water- en energiebedrijven via de volgende modules voldoen aan de wettelijke verplichtingen, zoals neergelegd in de Wbni.

>>

Wij helpen u graag succesvol te ondernemen

Neem contact op met:

Naomi Blomsteel
Senior Client Manager
+ 31 (0) 6 212 554 31
naomi.blomsteel@aon.nl

Saida Nhass CIPP/E
Practice Lead Compliance Consulting
+31 (0)6 20423691
saida.nhass@aon.nl

Cristina Stamate
Cyber Risk Consultant
+31 (0)6 50411705
cristina.stamate@aon.nl

aon.nl/energie

AON
Empower Results®

Cyberweerbaarheids-modules

MODULE 1: Cyber Impact Analyse

Onze Cyber Impact Analyse geeft u snel inzicht in uw belangrijkste cyberrisico's en de (financiële) impact wanneer deze zich openbaren. Dit doen wij op basis van interviews met sleutelfiguren, het beoordelen van relevante informatie en de toepassing van onze opgebouwde kennis en ervaring. Dit resulteert in een rapport met uitgewerkte scenario's en aanbevelingen voor een hogere cybervolwassenheid die aansluit bij de risicobereidheid van een organisatie. Tevens bepalen wij welke schades wel en niet verzekerbaar zijn, zodat de klant samen met Aon heel gericht de gewenste cyberdekking kan bepalen.

MODULE 2: Bedrijfscontinuïteitsmanagement

Een belangrijke verplichting van de Wbni is het garanderen van de bedrijfscontinuïteit en de beschikbaarheid van de essentiële diensten. Wij maken inzichtelijk in hoeverre de kritische activiteiten afhankelijk zijn van informatietechnologie. Ook bieden wij oplossingsrichtingen om gestructureerd en planmatig de impact van een cyberincident te reduceren en het herstel te bespoedigen binnen vooraf gedefinieerde hersteltijden en niveaus. Onze bewezen aanpak is gebaseerd op de geldende standaarden op dit gebied (NEN ISO 22301). Wij hebben zitting in de NEN BCM-commissie en zijn geaccrediteerd als ervaren en bewezen begeleider door certificerende instanties.

MODULE 3: Trainen en oefenen

Een van de belangrijkste voorbereidingen op crisissituaties is een crisisoefening. Een crisisoefening helpt bedrijven om snel te reageren als zich een echte crisissituatie voordoet. Wij gebruiken in oefeningen realistische en herkenbare scenario's die organisaties écht kunnen treffen. De uitkomsten van een oefening zijn daardoor direct bruikbaar, bijvoorbeeld voor het aanscherpen van plannen en werkwijzen.

MODULE 4: Ondersteuning bij incident

Als zich een cyberincident voordoet, dient dit adequaat afgehandeld te worden, met minimale impact. Aon biedt gespecialiseerde ondersteuning in de afhandeling van cyberincidenten waardoor de gevolgen zo veel mogelijk worden beperkt. Wij bieden niet alleen ondersteuning op IT-vlak, maar geven ook uitgebreide support bij de verplichte melding en de communicatie aan stakeholders. Hierdoor voldoet een bedrijf niet alleen aan wettelijke verplichtingen, maar vermindert het ook andere risico's zoals reputatieschade.

MODULE 5: Compliancescan

Wilt u zeker weten of uw organisatie aan de gestelde wettelijke eisen voldoet en zo boetes voorkomt? Laat dan een compliancescan uitvoeren. Door een dergelijke scan uit te voeren, krijgt u snel zicht in de mate van compliance en kunt u tijdig verbeterpunten doorvoeren waardoor afbreukrisico's worden beperkt. Deze scan wordt uitgevoerd via een gepersonaliseerde online vragenlijst. De resultaten worden in een rapportage en op prioriteit gestelde actiepuntenlijst inzichtelijk gemaakt. Op deze manier heeft u snel en efficiënt inzicht in de grootste (compliance) risico's.

MODULE 6: Cyberverzekering

Zodra de cyberrisico's binnen een bedrijf in kaart zijn gebracht, kan een organisatie ervoor kiezen zich te beschermen tegen de gevolgen van een cyberincident. Een cyberverzekering biedt 24/7 hulp aan in geval van een cyberincident. Hierdoor kan uw organisatie binnen afzienbare tijd de normale bedrijfsvoering hervatten. Daarnaast dekt de cyberverzekering (in)directe financiële schade, dus ook die aan anderen en zelfs een door de toezichthouder opgelegde boete. Onze adviseurs begrijpen de risico's en kennen de beste dekkingen in de zich nog ontwikkelende markt. Wij hanteren geen standaardaanpak, maar werken met u samen om een cyberverzekering te leveren die voor uw bedrijfsvoering relevant is.

19.0024.01 Cybersecurity wet essentiele diensten V3