Reactie Holland Solar:

Cyberbeveiligingsbesluit en Ministeriele Regeling zorgplicht

Holland Solar is de brancheverenigingvoor alle bedrijven die actief zijn in de Nederlandse zonne-energiesector. Holland Solar vertegenwoordigt 270 leden uit de hele sector, waaronder fabrikanten van systeemcomponenten, groothandels, projectontwikkelaars, operation & maintenance bedrijven en installateurs.

In dit document doet Holland Solar een aantal aanbevelingen voor het Cyberbeveiligingsbesluit en de Ministeriele Regeling voor de zorgplicht. Een aantal belangrijke aspecten van de implementatie van de Cyberbeveiligingswet zal nog nader worden uitgewerkt bij Ministeriele Regeling. Hieronder wordt daarom ook aandacht gevraagd voor die punten die nog zullen worden uitgewerkt en die voor de zonne-energiesector belangrijk zijn.

Algemeen

1. Holland Solar verwelkomt de conceptversie van het Cyberbeveiligingsbesluit (Cbb) en de Ministeriele Regeling (MR) voor de zorgplicht, en de mogelijkheid hier via een publieksconsultatie input voor te kunnen regelen. We ondersteunen de doelen van de Cyberbeveiligingswet om de digitale veiligheid van Nederland te verhogen, en onderstrepen de belangrijke en groeiende rol van zonne-energie in de vitale energiesector.
2. We benadrukken graag dat de nadruk in de AMvB meer op praktische toepassing moet liggen dan op de schriftelijke vastlegging van bijvoorbeeld risico's en maatregelen.
3. In zowel het CBB als in de Nota van Toelichting wordt op meerdere plekken de term 'periodiek' gebruikt (zie bijvoorbeeld artikel 9). We bevelen aan om in de Nota van Toelichting toe te lichten hoe 'periodiek' moet worden begrepen, namelijk dat de entiteit dit zelf kan bepalen op basis van de eigen risicoanalyse.
4. Voor de uitvoerbaarheid voor bedrijven die in meerdere Europese landen actief zijn, is het belangrijk dat de implementatie van NIS2 zoveel mogelijk Europees geharmoniseerd wordt. Er lijken echter vrij significante verschillen te ontstaan in de manier waarop lidstaten NIS2 nationaal uitwerken. Sommige lidstaten vereisen bijvoorbeeld expliciet het toepassen van specifieke normen, waar Nederland voor een meer open benadering kiest. Holland Solar verwelkomt de benadering die Nederland

kiest, en verzoekt het Ministerie het belang van harmonisatie op Europees niveau zo veel mogelijk te bevorderen.

5. Van kleine bedrijven die zelf direct onder de nieuwe wet vallen, of die er indirect mee te maken krijgen via hun opdrachtgevers, wordt een vrij hoog maturiteitsniveau gevraagd. Om goed te kunnen voldoen aan deze verwachtingen en verantwoordelijkheden, is ondersteuning vanuit de overheid die specifiek gericht is op de behoeften van kleine bedrijven van groot belang. De sector hecht daarom ook groot belang aan voldoende capaciteit voor het NCSC als nationale CSIRT. Het is bovendien belangrijk dat de rol van het DTC als dienstverlenende en ondersteunende entiteit goed wordt doorgezet na het opgaan van het DTC in het NCSC. Daarnaast raden we aan bij de overheidsondersteuning voor met name MKB bedrijven zoveel mogelijk aan te sluiten bij bestaande programma's, zoals de website van het DTC en niet te kiezen voor het creëren van nieuwe platformen, om verdere informatie-versnippering te voorkomen.
6. Voor alle bedrijven brengt de wet aanzienlijke regeldruk en kosten met zich mee, en enige onzekerheid omdat bepaalde onderdelen van de Cbw nog niet volledig uitgewerkt zijn. Bovendien komen er meerdere nieuwe wetten en regels aan op het gebied van cyberveiligheid van bedrijven en producten. te verbeteren. Bedrijven moeten voldoende tijd krijgen om de wetgeving goed te implementeren.
7. De samenhang van het pakket Cbw en Cbb met de Wet weerbaarheid kritieke entiteiten (Wwke) en het Besluit weerbaarheid kritieke entiteiten (Bwke) is van groot belang. Bedrijven doen hun risicoanalyse volgens een all-hazards approach. Om de regeldruk niet onnodig te verhogen is het van groot belang dat de samenhang tussen beide trajecten wordt bewaakt. Dit betekent specifiek dat we graag één kanaal voor meldingen onder zowel de Cbw als de Wwke zouden zien, en één toezichthouder voor beide wetten die een integrale audit kan doen.
8. Artikel 66 van de Cbw regelt dat de Wet open overheid niet van toepassing is op informatie die door partijen met het CSIRT wordt gedeeld, om vertrouwelijkheid van deze informatie te waarborgen. In haar advies over de Cbw vraagt de Raad van State dit nader te motiveren. Deze vertrouwelijkheid is zeer belangrijk om informatie delen tussen partijen het CSIRT mogelijk te maken, we dringen er daarom op aan deze clausules in de Cbw te behouden en zoals gevraagd door de Raad van State goed te onderbouwen.

Hoofdstuk 2: Aanwijzing CSIRT

1. Het NCSC wordt aangewezen als nationale CSIRT. Vanuit deze rol beschikt het over uitgebreide informatie over actuele dreigingen. Er is behoefte aan meer duidelijkheid

over welke informatie op welke manier en op welke momenten door het NCSC met bedrijven zal worden gedeeld.

Hoofdstuk 3: Toepassingsbereik

2. Één van de omvangscriteria onder de Cbw is het aantal medewerkers van een bedrijf. De definitie hiervan verwijst naar Europese afspraken over de classificatie van grote, middelgrote en kleine bedrijven. Hieruit wordt duidelijk dat het aantal medewerkers wordt berekend in termen van FTE. Bij de uitvoering van de wet zou het voor bedrijven verduidelijking geven als in de Nota van Toelichting of één van de onderliggende regelingen wordt vermeld dat het aantal medewerkers wordt berekend in FTE.
3. De uitwerking van de gevolgen voor bedrijven met complexe bedrijfsmodellen is op dit moment nog een punt van zorg. Onder andere hoe de totale omzet, balans en het aantal medewerkers van bedrijven met complexe bedrijfsstructuren berekend moeten worden, kan bepalen of een bedrijf wel of niet direct onder de nieuwe wetgeving valt. Bovendien brengt het registreren van alle entiteiten binnen complexe bedrijfsstructuren een buitenproportionele regeldruk met zich mee.
4. De Minister heeft onder de Cyberbeveiligingswet de mogelijkheid bedrijven aan te wijzen als belangrijke of essentiele entiteit, ook als het bedrijf niet aan de omvangscriteria voldoet. Het is voor bedrijven belangrijk dat zo snel mogelijk wordt gecommuniceerd op basis van welke criteria dit zal gebeuren.
5. Bedrijven die uitsluitend productie beheren maar geen eigenaar zijn van installaties, vallen buiten de scope van de wet. In de zonne-energiesector komt het echter voor dat partijen grote vermogens beheren (>100MW) in opdracht van meerdere eigenaren die zelf niet voldoende opgesteld vermogen bezitten om binnen de scope van de wet te vallen. Dit kan gelden voor zowel grootzakelijke systemen als bij aggregators van consumentensystemen. De verwachting is dat dit in de toekomst vaker zal gaan voorkomen. We bevelen daarom aan te onderzoeken of het beheren van grote vermogens één van de criteria zou kunnen zijn om bedrijven op aan te wijzen als belangrijke of essentiële entiteit. Daarbij moet ook aandacht zijn voor welke partij welke juridische verantwoordelijkheid heeft: een beheerder kan tenslotte niet verantwoordelijk worden gehouden voor zaken aan een systeem waarover die geen invloed heeft. Hierover gaan we graag verder in gesprek.

Hoofdstuk 4: Zorgplicht

6. We benadrukken graag dat de nadruk in de AMvB en de MR meer op praktische toepassing moet liggen dan op de schriftelijke vastlegging van bijvoorbeeld risico's en

maatregelen. In meerdere artikelen van de Ministeriële Regeling wordt bijvoorbeeld voorgeschreven dat bepaalde activiteiten in procedures moeten worden vastgelegd. De essentie is dat de activiteiten worden gedocumenteerd en aantoonbaar worden toegepast. Het soort document (proces, instructie, procedure, etc.) waarin dit wordt vastgelegd is niet relevant.

Hoofdstuk 5: Training

7. Artikel 22 van de Cbb lijkt te vereisen dat de trainer extern is aan het bedrijf. We bevelen aan te verduidelijken of dit inderdaad het geval is, of dat een trainer ook een interne expert kan zijn. De CISO van de meeste bedrijven zal voldoen aan alle eisen die in Artikel 22.2 worden gesteld. De rol heeft bovendien kennis en expertise over het veiligheidsbeleid en bedrijfsvoering van het eigen bedrijf. Het inhuren van externe trainers brengt bovendien significante extra kosten met zich mee. We bevelen daarom aan bedrijven de ruimte te laten de training aan het bestuur door een gekwalificeerde eigen CISO te laten verzorgen
8. Er moet een duidelijke certificering komen voor de opleidingsplicht voor bestuursleden zodat bedrijven kunnen beoordelen of een opleiding voldoet. De nieuwe opleidingsverplichting zal de druk op aanbieders van opleidingen sterk vergroten. Er moet daarom voldoende tijd worden gelaten voor bedrijven om aan deze verplichting te voldoen.

Hoofdstuk 6: Meldingen van significante incidenten

9. Er zal bij Ministeriele Regeling worden uitgewerkt welke criteria zullen gelden om te bepalen of er sprake is van een “significant incident”. Holland Solar ondersteunt dat dit in sectorale regelingen wordt uitgewerkt. Helderheid over de definitie van wat een significant incident is, is belangrijk voor bedrijven om de wet goed te kunnen uitvoeren. Voor de energiesector zou uitval van vermogen boven een ondergrens hier in ieder geval onderdeel van moeten zijn. We gaan hier graag verder over in gesprek.
10. Het is daarnaast belangrijk dat deze criteria zo snel mogelijk duidelijk worden, omdat bedrijven tijd nodig hebben om dit in hun bedrijfsvoering uit te werken. Als dit niet lukt, leidt dat tot juridische en operationele risico’s voor bedrijven.

Hoofdstuk 7: Registratieplicht

11. Voor de uitvoerbaarheid is het belangrijk dat bedrijven op groepsniveau met één e-herkenning de registratie van al hun onderliggende entiteiten kunnen regelen. Op dit moment is het nog het geval dat voor iedere entiteit apart e-herkenning moet worden aangevraagd. Dit leidt tot extra uitvoeringskosten voor bedrijven.