Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Ondersteuning bij cyberincidenten

Voor NIS2-organisaties

In de wereld van cyber, waar veranderingen zich in razendsnel tempo opvolgen, krijgen organisaties in onverminderde mate te maken met dreigingen en incidenten. De verantwoordelijkheid van organisaties om hun eigen digitale weerbaarheid op orde te hebben wordt onderstreept door de komst van de Europese NIS2-richtlijn. Cyberincidenten zijn echter nooit helemaal te voorkomen. Op het moment dat zich een incident voordoet kan het Nationaal Cyber Security Centrum (NCSC) bijstand leveren. Wanneer, hoe en in welke mate wij dit doen, lees je in deze publicatie.

Bereid jouw organisatie voor

Een organisatie is te allen tijde zelf verantwoordelijk voor haar eigen cyberweerbaarheid. Het NCSC adviseert om hiervoor minimaal de 5 basisprincipes op orde te hebben. Een onderdeel van deze principes is dat je weet hoe jouw organisatie reageert op incidenten. Door een goede voorbereiding, verminder je de impact van het incident.

In het geval van een cyberincident

Een cyberincident kan niet alleen zorgen voor het onderbreken van de bedrijfsprocessen, maar ook resulteren in aanzienlijke maatschappelijke en economische gevolgen. Om die laatste gevolgen te beperken, worden meerdere sectoren in de NIS2-richtlijn aangemerkt als 'belangrijk' of 'essentieel'. Als jouw organisatie onder deze richtlijn valt, moet je de gevolgen van een incident zo snel mogelijk beheersen. Het NCSC kan, als jouw sectoraal CSIRT, ondersteuning bieden om het incident te identificeren. Vervolgens kan jouw organisatie, eventueel in samenwerking met een Incident Response Partij, mitigerende maatregelen treffen om het incident te verhelpen.

Stap voor stap ondersteuning

1 Beoordeling van het incident

De eerste stap is om het incident zelf (intern) te beoordelen op basis van de eigen risicoanalyse en incidentprocedures. De informatie daaruit is nodig bij een incidentmelding en een eventueel hulpverzoek, indien extra ondersteuning nodig is om grip te krijgen op het incident.

2 Maak een incidentmelding

De Cyberbeveiligingswet schrijft voor dat organisaties *significante incidenten* moeten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Er geldt een gefaseerde meldplicht. De eerste melding is een vroegtijdige waarschuwing die zo snel mogelijk, maar in ieder geval binnen 24 uur na waarneming van het incident plaatsvindt[1]. Een melding maak je via mijn.ncsc.nl of via www.ncsc.nl. Ook bij niet-significante meldingen wordt je nadrukkelijk uitgenodigd een melding te maken zodat het NCSC andere organisaties in een sector, regio of land kan voorbereiden.

3 Doe een hulpverzoek (indien nodig)

Heb je dringend hulp nodig? Het NCSC is voor cyberincidenten 24/7 bereikbaar via de contactmogelijkheden op mijn.ncsc.nl. Minder urgente hulpverzoeken doe je via het meldproces in stap 2.

4 NCSC beoordeelt het incident

Een incident komt via een melding of via andere kanalen bij het NCSC binnen. Deze informatie beoordelen wij vervolgens door middel van triage. Dit is nodig om te bepalen of, en met welke urgentie en intensiteit we ondersteuning bieden. Wij gebruiken hiervoor een afwegingskader waarbij we toetsen op diverse aspecten, zoals de aard en de mogelijke impact van het incident.

5 NCSC biedt ondersteuning en opvolging naar overige organisaties

Vervolgens gaan we na welke ondersteuningsvorm passend is. Hierbij focussen wij ons in de basis op de identificatiefase van het incident. De ondersteuning kan adviserend, coördinerend of technisch van aard zijn. Zo kunnen we bijvoorbeeld data-acquisitie begeleiden, een systeemanalyse of malware-analyse uitvoeren. Op basis van de bevindingen adviseren we over de vervolgstappen. Waarna jouw organisatie, eventueel in samenwerking met een Incident Response Partij, mitigerende maatregelen treft om het incident te verhelpen. In goed overleg delen wij identificatie-resultaten en handelingsperspectieven met andere organisaties. Zo houden we samen Nederland digitaal weerbaar.

1 Voor organisaties die ook onder de Digital Operational Resilience Act (DORA) of Netwerkcode cyber security voor grensoverschrijdend elektriciteitsstromen (Netcode) vallen, kunnen andere termijnen gelden.