Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC CSIRT-dienstverlening

Deze communicatieplaat geeft een overzicht van onze CSIRT-dienstverlening onder de NIS2-richtlijn, de Cyberbeveiligingswet (Cbw) en de Network Code on Cybersecurity (NCCS), en de wijze waarop de dienstverlening plaatsvindt.
Het toont daarmee geen totaalbeeld van onze producten en diensten. Ook is de dienstverlening zoals hier weergegeven de komende periode nog volop in ontwikkeling.

Adviseren

Kennisuitwisseling

- Samenwerkings-verbanden
- Kennis-, advies- en onderzoeksproducten

Analyse

- Nationaal situationeel beeld (realtime en periodiek)
- Dreigingsanalyse
- Risicoanalyse
- Beveiligingsadvies

Waarschuwen

Detectie

- Nationaal Detectie Netwerk (NDN)
- Cyber Threat Intelligence feed

Notificatie

- Doelwit en Slachtoffer notificatie
- Kwetsbaarhedenfeed (met waar mogelijk duiding)
- Nationaal Veiligheidsadvies Cyber (NVAC)

Helpen

Coördinatie

- Centraal registratiepunt
- Centraal meldpunt voor kwetsbaarheden en incidenten
- Internationaal Single Point of Contact
- Crisismanagement
- Coordinated Vulnerability Disclosure

Bijstand bij incidenten

- Incidentcoördinatie
- Incidentdata-acquisitie
- Forensische analyse
- Malware analyse
- Handelingsperspectief

Hoe maak je gebruik van de dienstverlening?

Wij bieden onze dienstverlening via drie routes aan en hanteren een Digital First aanpak.

1. Zelf aan de slag

- Website
- Portaal
- API
- Community
- Social media
- Doelgroepbericht

2. Bijeenkomsten

- Face-to-Face
- Bijeenkomst/vergadering
- Event

3. Een-op-een contact

- E-mail/webform
- Telefoon
- Chat

Ga voor meer informatie naar www.ncsc.nl

Adviseren

Kennisuitwisseling

Samenwerkingsverbanden
Door informatieuitwisseling in publiek-private samenwerkingsverbanden versterkt het NCSC haar informatiepositie, ondersteunt het organisaties sneller en gerichter, en gebruikt het de ervaringen om producten en diensten verder te ontwikkelen.

Kennis-, advies- en onderzoeksproducten
Het NCSC biedt openbare kennis-, advies- en onderzoeksproducten waarmee organisaties via concrete stappenplannen risico's in kaart kunnen brengen en de eigen digitale weerbaarheid kunnen versterken. Ook helpen de producten bij het stellen van prioriteiten vanuit technologische trends.

Analyse

Nationaal situationeel beeld (near-realtime en periodiek)
Het NCSC analyseert voortdurend het cyberlandschap op het gebied van dreigingen, kwetsbaarheden en incidenten. Op basis van die analyse worden trends getoond via situationele en sectorale dreigingsbeelden, zodat entiteiten op de hoogte zijn van de cyberrisico's.

Dreigingsanalyse
Het NCSC analyseert trends in het Cyberlandschap op dreigingen die nu spelen en in de toekomst kunnen gaan spelen voor een specifieke sector, Nederland, Europa en de rest van de wereld. Dit draagt bijvoorbeeld bij aan SITREPs, CTI-reports en andere informatie- en adviesproducten.

Risicoanalyse
Het NCSC helpt entiteiten om risicogeïnformeerde besluiten te nemen voor het verhogen van de cyberweerbaarheid binnen het huidige dreigingslandschap.

Beveiligingsadvies
NCSC-beveiligingsadviezen, of advisories, beschrijven actuele kwetsbaarheden en dreigingen, hun risico's en concrete acties, afgestemd op het Kennis- en Adviesportfolio.

Waarschuwen

Detectie

Nationaal Detectie Netwerk (NDN)
Via het NDN ontvangen organisaties dreigingsinformatie, tooling en kennis om detectie binnen hun netwerken, op end-points en in cloudomgevingen zo goed mogelijk in te richten. Door directe terugdeling van dreigingsindicatoren en/of sightings dragen organisaties zelf bij aan de nationale cyberweerbaarheid.

Cyber Threat Intelligence Feed
Via de Cyber Threat Intelligence Feed ontvangen organisaties Indicators of Compromise die helpen bij de detectie binnen hun eigen network. Terugkoppeling van waarnemingen dragen bij aan het nationale cyberbeeld en vroegtijdige waarschuwing van andere partijen.

Notificatie

Doelwit en Slachtoffer notificatie
Op basis van meldingen en dreigings-indicatoren waarschuwt het NCSC organisaties direct als zij doelwit of slachtoffer zijn van een cyberaanval.

Kwetsbaarhedenfeed
Een realtime feed toont actuele kwetsbaarheden met waar mogelijk en relevant hun risico's en passend beveiligingsadvies.

Nationaal Veiligheidsadvies Cyber (NVAC)
Bij ernstige cyberdreigingen geeft het NCSC, namens de NCTV, een Nationaal Veiligheidsadvies Cyber (NVAC) uit. Daarnaast biedt het NCSC de mogelijkheid aan vitale organisaties om hun keuze voor een pas-toe of leg-uit besluit vast te leggen.

Helpen

Coördinatie

Centraal registratiepunt
Het NCSC faciliteert een centraal registratiepunt voor entiteiten die vallen onder de NIS2-richtlijn en Netcode. Het ondersteunt NIS2-organisaties bij het voldoen aan hun wettelijke registratieverplichting.

Centraal meldpunt voor kwetsbaarheden en incidenten
Organisaties die vallen onder de NIS2, Netcode, DORA en CRA kunnen significante cyberincidenten melden op het centrale meldpunt. Deze worden, indien nodig, gedeeld met de aangewezen sectorale CSIRT en toezichthouder. Ook kunnen organisaties hier terecht voor het maken van vrijwillige meldingen. Het melden van kwetsbaarheden gaat via het reguliere CVD-proces (Coordinated Vulnerability Disclosure).

Internationaal Single Point of Contact
Het NCSC fungeert als Single Point of Contact (SPOC) voor nationale en internationale samenwerking op cybergebied. Het verbindt partners, CSIRTs en netwerken, coördineert informatie-uitwisseling en zorgt voor afstemming van wetgeving, taxonomie en terminologie.

Crisismanagement
Na afkondiging van een nationale, Europese of internationale cybercrisis door de NCTV treedt het NCSC op als crisiscentrum en coördineert het de respons, informatie-uitwisseling en ondersteuning van alle betrokken partijen in Nederland.

Coordinated Vulnerability Disclosure
Het NCSC coördineert het proces bij kwetsbaarheden die meerdere entiteiten en sectoren raken. Meldingen kunnen desgewenst anoniem worden gemaakt.

Bijstand bij incidenten

Incidentcoördinatie
Het NCSC beoordeelt incidenten via triage en biedt op basis daarvan passende ondersteuning. De focus ligt op de identificatiefase van het incident, waarbij ondersteuning adviserend, coordinerend of technisch van aard kan zijn.

Incident data-acquisitie
Het NCSC faciliteert entiteiten bij het verzamelen en analyseren van incidentdata om oorzaken te achterhalen en gerichte handelingsperspectieven te bieden.

Forensische analyse
Het NCSC ondersteunt entiteiten bij het uitvoeren van forensische analyses op incidentdata, waarbij digitale sporen worden onderzocht om de oorzaak te reconstrueren. Dit levert helder inzicht over de situatie en stelt het NCSC in staat om een passend handelingsperspectief aan te bieden.

Malware Analyse
In de malware-analysetool kunnen organisaties malware samples uploaden voor statische analyse. Indien nodig kan, naast de geautomatiseerde analyse, ook maatwerkmalwareanalyse worden uitgevoerd.

Handelingsperspectief
Het NCSC adviseert getroffen partijen tijdens alle incidentfasen over passende vervolgstappen en mitigerende maatregelen. Dit stelt hen in staat om zelfstandig of samen met een Incident Response partij passende mitigerende maatregelen te treffen.