CENTRE FOR
CYBERSECURITY
BELGIUM

NATIONAL CSIRT CHARTER

2026

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: Januari 2026
Version: 2.0 Nederlands
Author: Het Centrum voor Cybersecurity België (CCB)

Het Centrum voor Cybersecurity België (CCB) is de nationale cyberbeveiligingsautoriteit en het nationaal CSIRT in België. Het CCB superviseert, coördineert en waakt over de toepassing van de Belgische cyberveiligheidsstrategie. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, NIS2 entiteiten en de bevolking zich gepast beschermen. Het Centrum voor Cybersecurity België (CCB) is opgericht door het Koninklijk Besluit van 10 oktober 2014.

Inhoudstafel

Inleiding

Het Centrum voor Cybersecurity België (CCB) is de nationale cyberveiligheidsautoriteit in België. Het CCB fungeert als het nationale Computer Security Incident Response Team (CSIRT). De werking van het nationale CSIRT als overheidsdienst is vastgelegd in een wettelijk kader, aangevuld met beslissingen van de Ministerraad en interne documenten. Dit charter bundelt de essentiële elementen uit deze verschillende bronnen in één overzichtelijk document.

Hoewel het niet raadzaam is om een charter vaak aan te passen, is het geen statisch document. Het charter kan worden gewijzigd afhankelijk van de juridische of budgettaire context, of eenvoudigweg na intern onderzoek naar de relevantie ervan. In principe wordt het document om elk jaar geherevalueerd.

1. Algemene informatie

Het Centrum voor Cybersecurity België (CCB) is opgericht door het Koninklijk Besluit van 10 oktober 2014.

Het CCB is aangewezen als nationale cyberbeveiligingsautoriteit in het kader van de uitvoering[1] van de NIS2-wet[2]. In deze rol superviseert, coördineert en waakt het CCB met name over de toepassing van de Belgische cyberveiligheidsstrategie, evenals de naleving van de NIS2-wet door de betrokken entiteiten. Door optimale informatie-uitwisseling kunnen bedrijven, de overheid, NIS2 entiteiten[3] en de bevolking zich gepast beschermen.

De belangrijkste opdrachten van het CCB als nationale cyberbeveiligingsautoriteit[4] zijn:

- opvolgen en coördineren van en toezien op de uitvoering van het Belgisch beleid ter zake;
- vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid beheren;
- de coördinatie verzekeren tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector;
- formuleren van voorstellen tot aanpassing van het regelgevend kader op het vlak van cyberveiligheid;
- in samenwerking met het Coördinatie- en Crisiscentrum van de regering, het crisisbeheer bij cyberincidenten verzekeren;
- opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen;
- coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak;
- coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen;
- informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen.

Onder de NIS2-wet fungeert het CCB ook als het nationale CSIRT[5]. Het Cyber Emergency Response Team (CERT) en het Cyber Threat Research & Intelligence Sharing (CyTRIS) team zijn de twee operationele diensten die samen, binnen het CCB, het nationale CSIRT vormen.

De taak van het CERT bestaat erin cyberaanvallen binnen België te analyseren, in te dammen, te beperken en te stoppen. Het CERT levert technische expertise en bijstand aan andere overheidsdiensten. Sommige diensten worden proactief geleverd, maar het grootste deel van het werk van het CERT is vergelijkbaar met dat van een “cyberbrandweer”.

CyTRIS is verantwoordelijk voor het eerste contact met organisaties die een incident melden bij het CCB. Deze dienst van het CCB controleert dagelijks verschillende bronnen, verzamelt en ordent informatie die nuttig kan zijn om potentiële slachtoffers te waarschuwen en voert diepgaande CTI-analyses en strategische rapportages uit. CyTRIS stuurt ook “spear warnings” (individuele berichten) naar organisaties waarbij een bepaalde kwetsbaarheid is ontdekt op de IT-infrastructuur, malware is aangetroffen of gestolen inloggegevens zijn gevonden. Daarnaast organiseert CyTRIS regelmatig online en fysieke evenementen om belanghebbenden te informeren over actieve cyberdreigingen en hoe zij zich daartegen kunnen beschermen.

De belangrijkste opdrachten van het CCB als nationale CSIRT[6] zijn:

- het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau;
- het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en

[1] Koninklijk besluit van 9 Juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, art. 3.
[2] Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2-wet). De NIS2-wet is de omzetting in België van de richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 (de "NIS2-richtlijn").
[3] Essentiële en belangrijke entiteiten die onder het toepassingsgebied van de NIS2-wet vallen.
[4] NIS2-wet, art. 17.
[5] NIS2-wet, art. 15-16.
[6] NIS2-wet, art. 19.

andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk;
- het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten;
- het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;
- het deelnemen aan het CSIRT-netwerk,
- het optreden als coördinator ten behoeve van het proces van gecoördineerde bekendmaking van kwetsbaarheden;
- het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie;
- het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen
- het opsporen, observeren en analyseren van computerbeveiligingsproblemen;
- het samenwerken en in voorkomend geval uitwisselen van relevante informatie.

Met “cybersecurity” worden alle maatregelen bedoeld die de vertrouwelijkheid, de beschikbaarheid en de integriteit van de informatie- en communicatietechnologieën (ICT) waarborgen: technische maatregelen, maar ook bewustmakingsacties voor de gebruikers.

Bij cybersecurity gaat het echter niet om het gebruik van ICT louter als middel voor activisme, terrorisme, spionage, ondermijning of in het algemeen criminele activiteiten. Deze daden vallen onder de bevoegdheid van andere diensten dan het nationale CSIRT (politie, staatsveiligheid etc.). Ook de identificatie van de daders van misdrijven valt niet onder de bevoegdheid van het nationale CSIRT.

Elk risico, inbreuk op de vertrouwelijkheid, de integriteit en de beschikbaarheid van ICT-systemen, om welke reden dan ook, is echter wel een cyberveiligheidsprobleem.

2. Doelpubliek

Het doelpubliek is het geheel van partijen die gebruik kunnen maken van de diensten van het nationale CSIRT. Sommige diensten zijn slechts voor een deel van het doelpubliek beschikbaar.

Deel uitmaken van het doelpubliek van het nationale CSIRT legt, tenzij een expliciete juridische bepaling, geen enkele verplichting op aan de desbetreffende bedrijven of organisaties jegens het nationale CSIRT, maar geeft aan dat het nationale CSIRT zijn diensten beschikbaar stelt voor deze bedrijven of organisaties.

Wie kan beroep doen op het nationale CSIRT?

- Essentiële entiteiten onder de NIS2-wet.
- Administratieve overheden: de ICT-infrastructuur van de Belgische openbare besturen.
- Andere belangrijke entiteiten zoals gedefinieerd in de NIS2-wet kunnen ook om bijstand vragen, maar deze zal worden verleend op een 'best effort'-basis en in meer beperkte mate.
- Het grote publiek heeft slechts toegang tot een beperkt deel van de diensten van het nationale CSIRT.
- Private rechtspersonen die niet onder NIS2 vallen, kunnen gebruik maken van een beperkt deel van de diensten van het nationale CSIRT.
- Computers, netwerken of communicatiesystemen die zijn geclassificeerd in de zin van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst behoren tot de bevoegdheid van de Nationale Veiligheidsoverheid (NVO) en vallen dus buiten het toepassingsgebied van het CCB en het nationale CSIRT.

3. Bevoegdheid

Het nationale CSIRT beschikt over een coördinerende en adviserende rol. Artikel 21 van de NIS2-wet bepaalt dat het nationale CSIRT alle passende maatregelen neemt om zijn missie te verwezenlijken en aan zijn verplichtingen te voldoen. Deze maatregelen moeten evenredig zijn met die doelstellingen, en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

In deze context, onverminderd het Wetboek van strafvordering[7] mag het nationale CSIRT alle beschikbare gegevens bezitten, onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

Het nationale CSIRT vervult zijn opdrachten altijd met de nodige behoedzaamheid die verwacht mag worden van een overheid, waarbij er steeds bij voorrang voor wordt gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

[7] Art. 28quinquies, § 1, en 57, § 1.

4. Diensten

De diensten die door een nationaal CSIRT kunnen worden aangeboden zijn uiteenlopend en hangen zowel af van het doelpubliek en het gezag van het CSIRT over deze doelgroep, als van zijn institutionele positie. Nationale CSIRT-diensten worden over het algemeen ingedeeld in drie categorieën: proactieve diensten, reactieve diensten en diensten voor het beheer van de veiligheidskwaliteit. In dit hoofdstuk wordt deze indeling overgenomen en wordt het dienstenaanbod van het nationale CSIRT beschreven.

4.1. PROACTIEVE DIENSTEN

Proactieve diensten zijn gericht op het verbeteren van de beveiligingsinfrastructuur en -processen van het doelpubliek voordat een incident plaatsvindt of wordt ontdekt.

MONITORING EN ANALYSE VAN CYBERDREIGINGEN, KWETSBAARHEDEN EN INCIDENTEN

De opdracht van het nationale CSIRT is het opsporen, monitoren en analyseren van online cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau. Dagelijks monitort een team binnen het nationale CSIRT het dreigingslandschap om relevante cyberdreigingen en kwetsbaarheden tijdig te signaleren. Aanvullend levert het nationale CSIRT strategische, operationele en tactische CTI-rapporten om specifieke dreigingen nader te kunnen analyseren.

INFORMATIE DELING

Het nationale CSIRT verstrekt vroegtijdige waarschuwingen, meldingen en over gesignaleerde kwetsbaarheden en cyberdreigingen via zijn website, sociale media, het Early Warning System (EWS)[8] en indien nodig via direct contact (‘Spear Warning’[9]) om relevante belanghebbenden te waarschuwen voor de risico’s die door nieuwe kwetsbaarheden of dreigingsvectoren veroorzaakt worden. Daarnaast organiseert het regelmatig online en fysieke evenementen om doelgroepen te informeren over actieve cyberdreigingen en hoe zij zich daartegen kunnen beschermen.

MONITORING CYBERDOMEIN

Het nationale CSIRT monitort continue de technologische trends, ontwikkelingen en oplossingen op het gebied van cybersecurity en bij uitbreiding, informatiebeveiliging in de breedste zin van het woord. Dit toezicht biedt input voor anderen en maakt het mogelijk om op de hoogte te blijven van de laatste ontwikkelingen op dit gebied.

OPSPORING, OBSERVATIE EN ANALYSE VAN BEVEILIGINGSPROBLEMEN

De opdracht van het nationale CSIRT is het opsporen, observeren en analyseren van online beveiligingsproblemen. Het vormt dan ook het centrale aanspreekpunt voor de melding van beveiligingsincidenten en informatie over cyberdreigingen.[10]

BEVEILIGINGS-ASSESSMENTS / PENETRATIETESTEN/ ATTACK SURFACE MANAGEMENT

Op verzoek kan het nationale CSIRT, afhankelijk van de beschikbaarheid van middelen, een evaluatie of een penetratietest uitvoeren van de infrastructuur (of een deel daarvan) van zijn doelgroep om kwetsbaarheden met mogelijk significante gevolgen op te sporen. Daarnaast kan het proactief risico’s vanuit het perspectief van een aanvaller beoordelen door internetgerichte kwetsbaarheden op te sporen en zo het aantal mogelijke toegangspunten bij doelgroepen tot het netwerk te beperken. Het is mogelijk dat het nationale CSIRT met (externe) derden moet samenwerken om deze dienst te verlenen.

[8] Zie https://ccb.belgium.be/nl/cytris/early-warning-system.
[9] Zie https://ccb.belgium.be/nl/cytris/faq-on-spear-warnings.
[10] Zie https://ccb.belgium.be/nl/cert/een-incident-melden.

VERSPREIDING VAN INFORMATIE OVER CYBERVEILIGHEID

Het nationale CSIRT publiceert in voorkomend geval richtsnoeren of links naar dergelijke documenten, die van belang kunnen zijn voor het doelpubliek[11].

OPSPOREN VAN EN INFORMEREN OVER KWETSBARE OF ONVEILIGE SYSTEMEN

Indien het geen negatieve gevolgen heeft voor de werking van de diensten van de entiteiten, kan het nationale CSIRT proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren.

4.2. REACTIEVE DIENSTEN

De reactieve diensten zijn erop gericht een antwoord te bieden op verzoeken om bijstand, signaleringen, en in het algemeen elke dreiging of aanval gericht op de systemen van het doelpubliek van het nationale CSIRT.

BEHANDELING VAN INCIDENTEN

- Eerste contact en registratie in geval van (NIS2) incidenten

Verwerking van (incident-)meldingen via telefoon en e-mail, en eventueel eerste contactname.

- Analyse van incidenten

Op verzoek van het doelpubliek maakt het nationale CSIRT een postmortem-analyse van een cybersecurityincident. Het doel van deze analyse is om de omvang van het incident en de aangerichte schade vast te stellen, de hoofdoorzaak ervan te achterhalen en eventueel aanbevelingen te doen.

- On-site-incidentbeheer

Op verzoek van bepaalde leden van zijn doelpubliek zal het nationale CSIRT specialisten sturen om de lokale teams bij te staan bij het beheren van een specifiek incident.

- Ondersteuning bij incidentbeheer

Het nationale CSIRT biedt zijn doelgroep ondersteuning bij het afhandelen van veiligheidsincidenten. Deze ondersteuning kan bestaan uit advies per e-mail of telefoon, hulp bij de analyse van forensische gegevens etc.

- Coördinatie van incidenten

Het nationale CSIRT coördineert, in samenwerking met de betrokken actoren, het antwoord op incidenten. Bij ernstige incidenten kan het nationale cybernoodplan worden geactiveerd.

KWETSBAARHEIDSBEHEER - RESPONSCOÖRDINATIE

Wanneer een kwetsbaarheid wordt vastgesteld in een bepaald softwareproduct, kan het nationale CSIRT op aanvraag de mitigatie- en communicatie-inspanningen coördineren tussen de verschillende betrokken partijen (onderzoeker, softwareleverancier, gebruikers etc.).[12] Het kan zijn, dat het nationale CSIRT moet samenwerken met derden om deze dienst te leveren.

[11] Zie https://ccb.belgium.be/advisories
[12] Zie https://ccb.belgium.be/nl/regelgeving/cvdp

ARTEFACTANALYSE

Een artefact is wat overblijft na een (poging tot) binnendringing in een ICT-systeem. Bestanden, logs, informatiesystemen zijn (niet-limitatieve) voorbeelden van artefacten. Het nationale CSIRT kan artefacten analyseren die worden gemeld. Het is mogelijk dat het nationale CSIRT met derden moet samenwerken om deze dienst te verlenen.

4.3. DIENSTEN OP HET GEBIED VAN VEILIGHEIDSKWALITEITSBEHEER

Deze diensten maken gebruik van de bevindingen en de lessen die zijn getrokken uit de praktijk van de verschillende reactieve diensten.

BEWUSTMAKING

Het nationale CSIRT neemt deel aan de sensibiliseringscampagnes van het CCB. Daarnaast organiseert het regelmatig online en fysieke evenementen om doelgroepen te informeren over actieve cyberdreigingen en hoe zij zich daartegen kunnen beschermen.

OPLEIDING

Het nationale CSIRT heeft de mogelijkheid om opleidingen te ontwikkelen in de domeinen die tot zijn bevoegdheden behoren, en om opleidingssessies te organiseren. Het kan zijn, dat het nationale CSIRT zal samenwerken met derden om deze dienst te leveren.

4.4. DIENSTEN DIE HET NATIONALE CSIRT NIET LEVERT

Proactieve diensten:

- Algemene risicoanalyses en modellering
- Bedrijfscontinuïteitsplanning (BCP/DRP) en beveiligingsadvies
- Evaluatie of certificering van beveiligingsproducten

Reactieve diensten:

- Kwetsbaarheidsbeheer - kwetsbaarheden patchen (correcties)
- Operationele veiligheid
- Wederopbouw in het geval van een cyberaanval

5. Serviceniveau

Het nationale CSIRT kan tijdens de kantooruren (09.30 tot 16.30 uur) per e-mail of telefonisch[13] worden gecontacteerd van maandag tot vrijdag, buiten officiële sluitingsdagen.

De ontvangst van mails die naar het nationale CSIRT worden gestuurd, wordt binnen enkele minuten automatisch bevestigd. Dit automatische systeem geeft een uniek nummer aan elke melding. Het is niet gezegd dat het CSIRT systematisch zal kunnen antwoorden op de mail; dit hangt af van de ernst van het incident en van de hoedanigheid van de correspondent.

In samenwerking met het Nationaal Crisiscentrum (NCCN) van het Ministerie van Binnenlandse Zaken is het nationale CSIRT de klok rond telefonisch bereikbaar voor de afhandeling van ernstige incidenten voor essentiële NIS2 entiteiten.

[13] Voor contactgegevens zie paragraaf 6.

6. Samenvatting van het beleid van het nationale CSIRT

6.1. SOORTEN INCIDENTEN EN ONDERSTEUNINGSNIVEAU

Het nationale CSIRT behandelt elk incident dat verband houdt met een netwerk- of informatiesysteem dat zich op het Belgische grondgebied bevindt, of elk internetdomein dat eindigt op ".be". Het niveau van de ondersteuning hangt af van de ernst van het incident en de hoedanigheid van de correspondent.

De prioriteit aan het doelpubliek wordt als volgt gegeven:

1. Essentiële entiteiten onder de NIS2-wet.

2. Administratieve overheden: de ICT-infrastructuur van de Belgische openbare besturen.

3. Belangrijke entiteiten zoals gedefinieerd in de NIS2-wet kunnen ook om bijstand vragen, maar deze zal worden verleend op een 'best effort'-basis en in meer beperkte mate.

4. Het grote publiek heeft slechts toegang tot een beperkt deel van de diensten van het nationale CSIRT. Private rechtspersonen die niet onder NIS2 vallen, kunnen gebruik maken van een beperkt deel van de diensten van het nationale CSIRT.

Computers, netwerken of communicatiesystemen die zijn geclassificeerd in de zin van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst behoren tot de bevoegdheid van de Nationale Veiligheidsoverheid (NVO) en vallen dus buiten het toepassingsgebied van het CCB en het nationale CSIRT.

6.2. SAMENWERKING, INTERACTIE EN INFORMATIEVERSPREIDING

Het nationale CSIRT behandelt de informatie die het ontvangt volgens de geldende Belgische wetgeving. Het nationale CSIRT schenkt dan ook veel aandacht aan het beschermen van de persoonsgegevens en gevoelige informatie die het ontvangt.

Zoals aangegeven in het nationale cybernoodplan[14], coördineert het nationale CSIRT de activiteiten van de verschillende stakeholders in het geval van een nationaal cybersecurityincident. In het geval van een nationale cybersecuritycrisis werkt het nationale CSIRT samen met het Nationaal Crisiscentrum (NCCN) om de activiteiten van de verschillende stakeholders te coördineren.[15]

Als het noodzakelijk is om persoonlijke gegevens te communiceren om een incident te behandelen, zal het nationale CSIRT erop letten om alleen het vereiste minimum aan informatie te versturen.

Gegevens die via e-mail worden overgemaakt in versleutelde vorm, zullen enkel in deze vorm worden opgeslagen en alleen worden ontsleuteld in geval dit noodzakelijk is voor het oplossen van een incident. Indien een overdracht van deze gegevens noodzakelijk is, zal deze ook versleuteld gebeuren.

Het nationale CSIRT hanteert en respecteert het Traffic Light Protocol 2.0 zoals beschreven door FIRST.[16]

Het nationale CSIRT zal zijn ervaring zoveel mogelijk delen met zijn peers en zijn doelpubliek, op voorwaarde dat dit niet in strijd is met de bovenstaande bepalingen. Er zal bijzondere aandacht worden besteed aan de volgende groepen: EGC6, TF-CSIRT7, FIRST8, en het EU CSIRTs Network.

Alleen specifiek door het CCB aangewezen personen zullen contact hebben met de pers.

---

[14] Het nationale plan voor cyberbeveiligingsincidenten en cybercrisisrespons (kortweg nationale cybernoodplan) Dit plan is een nationaal plan in de zin van artikel 9, § 2, van de wet van 15 mei 2007 betreffende de civiele veiligheid. Dit plan is opgesteld door het CCB samen met het NCCN. Het nationale cybernoodplan is geen publiek document. Zie ook art. 29 van de NIS2-wet.
[15] NIS2-wet, art. 18.
[16] https://www.first.org/tlp/.

6.3 COMMUNICATIE EN AUTHENTICATIE

Het nationale CSIRT kan per e-mail worden gecontacteerd via: info@ccb.belgium.be. Uitsluitend in geval van dringende hulp bij incidenten, is het nationale CSIRT ook telefonisch bereikbaar via +32 (0)2 501 05 60. Het nationale CSIRT is bereikbaar tijdens de kantooruren (09.30 tot 16.30 uur) van maandag tot vrijdag, buiten officiële sluitingsdagen.

Voor de afhandeling van ernstige incidenten voor essentiële NIS2 entiteiten is het nationale CSIRT de klok rond telefonisch bereikbaar in samenwerking met het Nationaal Crisiscentrum (NCCN) van het Ministerie van Binnenlandse Zaken.

Voor veilige en discrete communicatie kan er gebruik gemaakt worden van PGP-encryptie. Actuele informatie over de beschikbare emailadressen met de bijbehorende PGP-sleutels staan vermeld op: https://ccb.belgium.be/nl/cert/een-versleuteld-bericht-versturen.

Het nationale CSIRT beschikt over personeelsleden die gemachtigd zijn om geclassificeerde informatie te behandelen in de zin van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst.