CENTRE FOR
CYBER SECURITY
BELGIUM

Nationaal CSIRT-handvest

CHANCELLERY OF
THE PRIME MINISTER

.be

CENTRUM VOOR
CYBERSECURITY BELGIË

01

Inleiding

Over dit document

Het Nationale CSIRT wordt als overheidsdienst geregeld door een wetgevend kader bestaand alsook beslissingen van de Ministerraad en interne documenten. Dit handvest verzamelt de nuttige elementen uit deze verschillende bronnen en bundelt ze in één enkel document.

Hoewel het niet raadzaam is om zo'n handvest vaak aan te passen, is het toch geen statisch document. Het handvest 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 de twee jaar gerevalueerd.

02

Missie

Koninklijk besluit van 10 oktober 2014

Het Centrum voor Cybersecurity België (CCB) werd opgericht bij het koninklijk besluit van 10 oktober 2014. Het CCB valt onder de bevoegdheid van de eerste minister.

Het Centrum voor Cybersecurity België is de nationale autoriteit voor cybersecurity in België. Het CCB nam het Computer Emergency Response Team (CERT) over en integreerde het om activiteiten uit te voeren met betrekking tot het opsporen, observeren en analyseren van online beveiligingsproblemen en om de gebruikers continu te informeren over deze problemen.
De belangrijkste opdrachten van het CCB die in het koninklijk besluit worden beschreven, 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.

NIS-WET

Artikel 3 van het koninklijk besluit van 12 juli 2019 tot uitvoering van de wet van 7 april 2019 betreffende de beveiliging van netwerk- en informatiesystemen (NIS-wet) bepaalt dat het Centrum voor Cybersecurity België wordt aangeduid als nationaal CSIRT in de zin van de NIS-wet.

Artikel 60 van de NIS-wet bepaalt de taken van het nationale CSIRT als volgt:

1. monitoren van incidenten op nationaal en internationaal niveau, met inbegrip van de verwerking van persoonsgegevens met betrekking tot het monitoren van deze incidenten;
2. ten behoeve van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;
3. reageren op incidenten;
4. zorgen voor een dynamische risico- en incidentanalyse en situatiekennis;
5. computerbeveiligingsproblemen opsporen, observeren en analyseren;

6. stimuleren van de vaststelling en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken op het gebied van procedures voor de behandeling van incidenten en risico's, en van systemen voor de classificatie van incidenten, risico's en informatie;
7. zorgen voor op samenwerking gerichte contacten met de particuliere sector en met andere administratieve diensten of publiek overheden;
8. deelnemen aan het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn.

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 cyberveiligheid gaat het niet alleen om het gebruik van ICT 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.

03

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 bepalingen, 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.

Aanbieders van essentiële diensten en kritieke infrastructuren

Een belangrijk deel van de het doelpubliek van het nationale CSIRT bestaat uit exploitanten van kritieke infrastructuren en essentiële diensten. Deexploitanten van kritieke infrastructuren worden geïdentificeerd in de wet van 1 januari 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.
De aanbieders van essentiële diensten zijn de bedrijven en overheidsdiensten die deel uitmaken van de sectoren waarop de NIS-richtlijn betrekking heeft en die als zodanig door de relevante sectorale autoriteiten worden geïdentificeerd:

1. Energie
    a. Elektriciteit
    b. aardolie
    c. Gas
2. Transport
    a. Luchtvervoer
    b. Spoorwegvervoer
    c. Vervoer over water
    d. Vervoer over de weg
3. Banken
4. Infrastructuren voor de financiële markten
5. Gezondheidszorg
6. Drinkwatervoorziening en -distributie
7. Digitale infrastructuren

Overheidsdiensten

Overheidsdiensten die essentieel zijn voor de Belgische bevolking maar die niet onder de NIS-richtlijn vallen, vallen ook onder het doelpubliek waar het CCB diensten aan verleend.

Administratieve overheden

De ICT-infrastructuur van de Belgische overheidsdiensten is essentieel voor de goede werking van het land, en valt daarom onder het doelpubliek van het nationale CSIRT.

Private rechtspersonen

Private rechtspersonen die geen essentiële diensten aanbieden, kunnen gebruikmaken van een beperkt deel van de diensten van het nationale CSIRT.

Grote publiek

Het grote publiek heeft slechts toegang tot een beperkt deel van de diensten van het nationale CSIRT (zie hieronder).

Geclassificeerde informatiesystemen

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

04

Affiliatie

Het Centrum voor Cybersecurity België (CCB) is een administratieve dienst onder het gezag van de eerste minister.

05

Bevoegdheid

De bevoegdheid is de capaciteit van CSIRT om zijn doelpubliek in zijn geheel of gedeeltelijk te verplichten om een of andere veiligheidsmaatregel te nemen om een veiligheidsincident te voorkomen of op te lossen.

Het nationale CSIRT beschikt over een coördinatie en adviserende rol maar heeft wel op basis van artikel 62 van de NIS-wet de verplichting om alle passende maatregelen te nemen om zijn missie te verwezenlijken en zijn verplichtingen na te komen. In deze context heeft het nationale CSIRT het recht om alle nodige gegevens te bewaren, te verwerken en over te maken, zelfs als die gegevens voortkomen uit een ongerechtige toegang tot een informaticasysteem door een derde.

06

Diensten

De diensten die door een 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. CSIRT-diensten worden over het algemeen ingedeeld in drie categorieën: reactieve diensten, proactieve diensten en diensten voor het beheer van de veiligheidskwaliteit. Het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) hanteert deze categorieën ook in zijn lijst van mogelijke CSIRT-diensten. De lijst is zeer uitgebreid en elk CSIRT moet zijn eigen selectie maken in functie van zijn opdracht en middelen.
In dit hoofdstuk wordt deze indeling overgenomen en wordt het dienstenaanbod van het nationale CSIRT beschreven.

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 tegen de systemen van het doelpubliek van het CSIRT.

Meldingen en waarschuwingen

Deze dienst bestaat uit de publicatie van informatie waarbij een aanval, een waarschuwing, een dreiging etc. worden beschreven en in het verschaffen van aanbevelingen in verband met acties op korte termijn die helpen om het probleem op te lossen.

Behandeling van incidenten

Analyse van incidenten

Op verzoek van een lid 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 gegevens etc.

Coördinatie van incidenten

Het nationale CSIRT coördineert, in samenwerking met de betrokken actoren, de antwoord op incidenten. Bij ernstige incidenten kan het Cyber Emergency Plan 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.). Het kan zijn dat het nationale CSIRT moet samenwerken met derden om deze dienst te leveren.

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 door sommige categorieën van zijn doelgroep zijn gemeld. Het is mogelijk dat het nationale CSIRT met derden moet samenwerken om deze dienst te verlenen.

Proactieve diensten

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

Aankondigingen

Het nationale CSIRT doet aankondigingen via zijn website en indien nodig via private kanalen om zijn doelgroep te waarschuwen voor risico's veroorzaakt door nieuwe kwetsbaarheden of dreigingsvectoren.

Technologisch toezicht

Het nationale CSIRT houdt een permanent technologisch toezicht in de domeinen van cybersecurity en informatiebeveiliging in de breedste zin van het woord. Dit toezicht biedt input voor andere 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[1]. Het vormt dan ook het centrale aanspreekpunt voor de melding van beveiligingsincidenten en informatie over cyberdreigingen.

Beveiligings-assessments / penetratietesten

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. Het is mogelijk dat het nationale CSIRT met (externe) derden moet samenwerken om deze dienst te verlenen.

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.

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.

Opleiding

Het nationale CSIRT heeft de mogelijkheid om opleidingen te ontwikkelen in de domeinen die tot zijn bevoegdheden behoren, en om opleidingssessies te organiseren.

[1] Koninklijk besluit van 14 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, *B.S.,* 21 november 2014, p. 91395.

Diensten die het nationale CSIRT niet levert

Reactieve diensten:

- Kwetsbaarheidsbeheer - kwetsbaarheden patchen (correcties)
- Operationele veiligheid

Proactieve diensten:

- Configuratie en onderhoud van beveiligingstools
- Ontwikkeling van beveiligingstools
- Beheer van de beveiligingskwaliteit:
    - Algemene risicoanalyses en modellering
    - Bedrijfscontinuïteitsplanning (BCP/DRP) en
    - Beveiligingsadvies
    - Evaluatie of certificering van beveiligingsproducten

Dienstenaanbod in functie van het doelpubliek

Reactieve diensten

	Aanbieders van essentiële diensten en kritieke infrastructuren	Aanbieders van essentiële openbare diensten	Administratieve overheden	Private rechtspersonen	Grote publiek
Waarschuwingen	Ja[2]	Ja[2]	Ja[2]	Ja[2]	Ja
Analyse van incidenten	Ja[3]	Ja[3]	Ja[2]	-	-
Behandeling van incidenten ter plaatse	Ja[3]	Ja[3]	-	-	-
Ondersteuning bij incidentafhandeling	Ja[3]	Ja[3]	Ja[2]	Ja[2]	-
Coördinatie van de afhandeling van incidenten	Ja[3]	Ja[3]	Ja[2]	Ja[2]	-
Coördinatie van de kwetsbaarheidsbehandeling[4]	Ja[2]	Ja[2]	Ja[2]	Ja[2]	-
Artefactanalyse[4]	Ja[3]	Ja[3]	-	-	-

[2] Tijdens de kantooruren
[3] De klok rond in samenwerking met het Crisiscentrum
[4] Afhankelijk van capaciteit en eventueel met de deelname van derden

Proactieve diensten

	Aanbieders van essentiële diensten en kritieke infrastructuren	Aanbieders van essentiële openbare diensten	Administratieve overheden	Private rechtspersonen	Grote publiek
Aankondigingen	Ja[2]	Ja[2]	Ja[2]	Ja[2]	Ja
Technologishc toezicht	Ja[2]	Ja[2]	Ja[2]	Ja[2]	Ja
Opsporing, observatie en analyse van beveiligingsproblemen	Ja[2]	Ja[2]	Ja[2]	Ja[2]	Ja
Beveiligings assesement / Penetratietests4	Ja[2]	Ja[4]	-	-	-
Verspreiding van informatie	Ja[2]	Ja[2]	Ja[2]	Ja[2]	Ja

Beheer van de veiligheidskwaliteit

	Aanbieders van essentiële diensten en kritieke infrastructuren	Aanbieders van essentiële openbare diensten	Administratieve overheden	Private rechtspersonen	Grote publiek
Bewustmaking	Ja[2]	Ja[2]	Ja[2]	Ja[2]	Ja
Opleidingen	Ja[2]	Ja[2]	Ja[2]	-	-

07

Serviceniveau

Het nationale CSIRT kan tijdens de kantooruren (09.00 tot 17.00 uur) per e-mail (cert@cert.be) worden gecontacteerd. 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 incidenten voor aanbieders van essentiële diensten en kritieke infrastructuren.

08

Samenvatting van het beleid

Soorten incidenten en ondersteuningsniveau

Het nationale CSIRT behandelt elk incident dat verband houdt met een informatie- of netwerksysteem 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. aanbieders van essentiële diensten en kritieke infrastructuren;
   aanbieders van essentiële overheidsdiensten;
2. administratieve overheden;
3. bedrijven;
4. het grote publiek.

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 Cyber Emergency Plan, 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 om de activiteiten van de verschillende stakeholders te coördineren.

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 met de PGP-sleutel van CERT.be, zullen enkel in deze vorm worden opgeslagen en alleen worden ontsleuteld ingeval dit noodzakelijk is voor het oplossen van een incident. Indien een overdracht van deze gegevens noodzakelijk is, zal deze ook versleuteld gebeuren door middel van de PGP-sleutel.

Het nationale CSIRT hanteert en respecteert het Traffic Light Protocol zoals beschreven door FIRST (versie 2.0)[5].

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: EGC[6], TF-CSIRT[7] , FIRST[8] , en het EU CSIRTs Network.

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

Communicatie en authenticatie

Het nationale CSIRT kan per e-mail worden gecontacteerd via cert@cert.be. Dit adres is gekoppeld aan een PGP-sleutel:

```
pub   rsa4096 2023-01-10 [SC] [expires: 2024-02-14]
      0C4B 3994 17CB DF05 A988  20F3 EBD4 C7C3 28CF D3D6
uid           [  full  ] CERT.be 2023 <cert@cert.be>
sub   rsa4096 2023-01-10 [E] [expires: 2024-02-14]
```

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 en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen[9].

[5] Forum of Incident Response and Security Teams (FIRST), “Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance — Version 1.0,” 16 08 2016, www.first.org/tlp/.
[6] Europese gouvernementele CERT's.
[7] Task Force - Samenwerking van Computer Security Incident Response Teams.
[8] Forum of Incident Response Teams.
[9] Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *B.S.,* 7 mei 1999*,* p. 15752.

Nationaal CSIRT-handvest

CENTRUM VOOR
CYBERSECURITY BELGIË
Wetstraat 16 - Brussel

T.: +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be