CERT.be

CENTRE FOR CYBER SECURITY BELGIUM

Charter CERT.be

Beschrijving van de diensten

TLP: [WHITE]

The Federal Cyber Emergency Team

Inhoudsopgave

Documentinformatie	
Titel van het beleid	Charter van CERT.be
Goedkeuringsdatum	
Goedkeuringsautoriteit	Eerste minister
Versie	1.2 NL
Vervangt	
Datum volgende herziening	01/01/2019
Aanverwante aanpassingen	
Aanverwant beleid	
Aanverwante procedures	
Eigenaar van het beleid	Directeur CERT.be

1 INLEIDING

Het charter van een CERT is een document in een gecodeerd formaat en is de publieke versie van de documenten die aan de basis liggen van CERT.be. Als overheidsdienst wordt het bestaan van CERT.be geregeld door een geheel van officiële documenten - Koninklijke Besluiten, beslissingen van de Ministerraad etc. - en interne documenten. Dit charter bevat de noodzakelijke elementen van deze niet-uniforme documenten en bundelt ze in één document dat bestemd is voor de CERT.be-peers en voor iedereen die eventueel gebruik wil maken van zijn diensten.

Hoewel het niet aangeraden is om een charter als dit vaak te wijzigen, is het toch geen onaanpasbaar document. Dit charter kan worden gewijzigd naargelang de wetgevende of budgettaire context, of gewoon regelmatig na intern onderzoek naar de relevantie ervan. Het dient minstens om de twee jaar te worden herzien.

2 OPDRACHT

Artikel 17 van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België (CCB)[1] verduidelijkt dat het CCB het beheer overneemt van de dienst Computer Emergency Response Team (CERT), die opgericht werd binnen de voormalige Federale Overheidsdienst Informatie- en Communicatietechnologie (FEDICT).

Deze bepaling verduidelijkt dat de opdrachten van deze dienst bestaan uit: "[...] het opsporen, het observeren en het analyseren van online veiligheidsproblemen alsook het permanent informeren daarover van de gebruikers."

Met toepassing van deze bepaling wordt de voormalige CERT-dienst van FEDICT geïntegreerd binnen het CCB en neemt het CCB dus al diens hierboven beschreven opdrachten over.

Als administratieve dienst van het CCB neemt het CERT deel aan de uitoefening van de andere wettelijke opdrachten van het CCB.

De term "cybersecurity" verwijst niet alleen naar alle maatregelen die het mogelijk maken de vertrouwelijkheid, de beschikbaarheid en de integriteit van de Informatie- en Communicatietechnologieën (ICT) te verzekeren: technische veiligheidsmaatregelen, maar ook naar maatregelen voor de bewustmaking van de gebruikers.

Cybersecurity gaat niet over het gebruik van ICT als loutere tools voor activisme-, terrorisme-, spionage-, ondermijnings- of criminele doeleinden. Deze feiten vallen onder de verantwoordelijkheid van andere diensten dan CERT.be (politie, Staatsveiligheid etc.). Ook de identificatie van daders van misdrijven valt niet onder de bevoegdheid van CERT.be. Elke inbreuk op de vertrouwelijkheid, de integriteit en de beschikbaarheid van ICT-systemen, ongeacht het doel ervan, vormt daarentegen ook een cybersecurityprobleem.

[1] Koninklijk besluit van *10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, B.S., 21 november 2014, p. 91395.*

3 DOELPUBLIEK

AKA CONSTITUENCY

Het doelpubliek - constituency in het Engels - zijn alle partijen die een beroep kunnen doen op de diensten van CERT.be. Bepaalde diensten zijn enkel toegankelijk voor een deel van het doelpubliek.

Het louter deel uitmaken van het doelpubliek van CERT.be houdt geen enkele verplichting in voor de bedrijven of organisaties van dit doelpubliek tegenover CERT.be, maar geeft wel de wil van CERT.be aan om zich ten dienste te stellen van deze bedrijven of organisaties.

3.1 Aanbieders van essentiële diensten en kritieke infrastructuren

De belangrijkste doelgroep van CERT.be bestaat uit de exploitanten van kritieke infrastructuren en de aanbieders van essentiële diensten. De exploitanten van kritieke infrastructuren zijn die bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren[2].

De aanbieders van essentiële diensten zijn de bedrijven en overheidsdiensten die deel uitmaken van de sectoren bedoeld in de NIS-richtlijn [3] en geïdentificeerd als dusdanig door de bevoegde sectorale overheden:

1. Energie
    a. Elektriciteit
    b. Aardolie
    c. Gas
2. Vervoer
    a. Luchttransport
    b. Spoorvervoer

[2] Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, B.S., 15 juli 2011, p. 42320.
[3] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie. Publicatieblad van de Europese Unie,*19 juli 2016*.

c. Vervoer over water

d. Vervoer over de weg

3. Banken
4. Infrastructuur voor de financiële markt
5. Gezondheidszorg
6. Levering en distributie van drinkwater
7. Digitale infrastructuur

3.2 Aanbieders van essentiële openbare diensten

De overheidsdiensten die essentieel zijn voor de Belgische bevolking en die niet gedekt worden door de NIS-richtlijn, worden niet gedefinieerd door wetteksten maar door interne criteria binnen het CCB.

3.3 Administratieve overheden

De ICT-infrastructuur van de Belgische overheidsdiensten is essentieel voor de goede werking van het land, en daardoor maakt ze deel uit van het doelpubliek van CERT.be.

3.4 Privaatrechtelijke rechtspersonen

De privaatrechtelijke rechtspersonen die geen essentiële diensten verlenen, kunnen een beroep doen op een beperkt aantal diensten van CERT.be.

3.5 Het grote publiek

Het grote publiek heeft geen toegang tot alle diensten van CERT.be (zie afdeling 6.5).

3.6 Geclassificeerde systemen

De computers en communicatiesystemen en -netwerken die geclassificeerd zijn in de zin van de wet van 11 december 1998 [4] betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen vallen onder de bevoegdheid van de Nationale Veiligheidsoverheid (NVO) en bijgevolg buiten het toepassingsgebied van het CCB en van CERT.be.

[4] Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, B.S., 7 mei 1999, p. 15752.

4 AFFILIATIE

CERT.be is een administratieve dienst van het Centrum voor Cybersecurity Belgium (CCB), onder het gezag van de Eerste Minister.

5 BEVOEGDHEID

De bevoegdheid is de capaciteit van CERT.be 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.

CERT.be beschikt enkel over die bevoegdheid die hem zou toegewezen worden door de omzetting van de NIS-richtlijn in Belgisch recht[5].

[5] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie. Publicatieblad van de Europese Unie,*19 juli 2016*.

6 DIENSTEN

De diensten die een CERT verleent, kunnen gevarieerd zijn en hangen zowel af van zijn doelpubliek als van zijn gezag over dit doelpubliek, alsook van zijn institutionele positie. De diensten van een CERT kunnen over het algemeen worden ingedeeld in drie categorieën[6]: reactieve diensten, proactieve diensten en diensten met betrekking tot het beheer van de veiligheidskwaliteit. Het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) gebruikt deze categorieën ook voor zijn lijst van diensten die een CERT kan aanbieden[7]. Deze lijst is uitgebreid en elk CERT moet de diensten selecteren die het wil aanbieden in functie van zijn opdracht en middelen.

In dit onderdeel wordt deze indeling besproken, alsook de selectie van de door CERT.be aangeboden diensten.

6.1 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 CERT.

6.1.1 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.

6.1.2 Incidentenbeheer

6.1.2.1 Incidentenanalyse

Op vraag van een lid van het doelpubliek maakt CERT.be de analyse na een veiligheidsincident. Het doel van deze analyse is de omvang van het incident en van de veroorzaakte schade te identificeren, de oorzaak van het incident te bepalen en eventueel aanbevelingen te doen.

6.1.2.2 Incidentenbeheer ter plaatse

[6] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle et M. Zajicek, "Handbook for Computer Security Incident Response Teams (CSIRTs)," Carnegie Mellon University, Pittsburgh, PA, 2003.
[7] ENISA, "CSIRT Services," 27 04 2016, www.enisa.europa.eu/topics/csirt-cert-services [Toegang op 11 07 2017].

Op vraag van bepaalde categorieën van het doelpubliek stuurt CERT.be specialisten om de lokale teams te helpen een veiligheidsincident te beheren.

6.1.2.3 Steun aan het incidentenbeheer

CERT.be biedt zijn doelpubliek bijstand aan bij het beheer van veiligheidsincidenten. Deze bijstand neemt de vorm aan van adviezen via mail of per telefoon, hulp bij de analyse van gegevens etc.

6.1.2.4 Coördinatie van het incidentenbeheer

CERT.be coördineert samen met de betrokken actoren het antwoord op incidenten. In geval van een ernstig incident kan het cybernoodplan worden geactiveerd.

6.1.3 Kwetsbaarheidsbeheer - Coördinatie van het antwoord

Wanneer een kwetsbaarheid wordt ontdekt in software kan CERT.be op aanvraag de mitigatie- en communicatie-inspanningen tussen de verschillende betrokken partijen (onderzoeker, softwarefabrikant, gebruikers etc.) coördineren. Het is mogelijk dat CERT.be moet samenwerken met derden om deze dienst te verlenen.

6.1.4 Artefactanalyse

Een artefact is wat overblijft na een (poging tot) binnendringing in een ICT-systeem. Bestanden, logs, informatiesystemen zijn (niet-limitatieve) voorbeelden van artefacten.

CERT.be heeft de mogelijkheid om artefacten te analyseren die worden voorgelegd door bepaalde categorieën van zijn doelpubliek. CERT.be behoudt zich tevens het recht voor om een beroep te doen op derden om deze dienst aan te bieden.

6.2 Proactieve diensten

De proactieve diensten hebben als doel de infrastructuur en de beveiligingsprocessen van het doelpubliek te verbeteren voordat een incident plaatsvindt of wordt opgespoord.

6.2.1 Aankondigingen

CERT.be doet aankondigingen via zijn website en indien nodig via privékanalen om zijn doelpubliek te waarschuwen voor risico's als gevolg van kwetsbaarheden of het bestaan van nieuwe aanvalsvectoren.

6.2.2 Technologisch toezicht

CERT.be houdt permanent technologisch toezicht in de domeinen van de informaticabeveiliging en de informatiebeveiliging in ruime zin. Dit toezicht biedt de verschillende andere diensten input en maakt het voor CERT.be mogelijk om op de hoogte te blijven van de laatste evoluties hieromtrent.

6.2.3 Opsporing, waarneming en analyse van veiligheidsproblemen

De taak van CERT.be is de online veiligheidsproblemen op te sporen, waar te nemen en te analyseren [1]. Het is dus het centrale contactpunt voor de melding van veiligheids- en informatica-incidenten betreffende de cyberdreiging.

6.2.4 Veiligheidsaudits / Penetratietests

Op aanvraag kan CERT.be, naargelang de beschikbaarheid van zijn middelen, een audit of een penetratietest uitvoeren van de infrastructuur (of een deel ervan) van zijn doelpubliek. Het is mogelijk dat CERT.be een beroep doet op derden om deze dienst te verlenen.

6.2.5 Publicatie van informatie inzake cybersecurity

CERT.be publiceert bij gelegenheid documenten met richtsnoeren of links naar dergelijke documenten die van belang zouden kunnen zijn voor het doelpubliek.

6.3 Beheer van de veiligheidskwaliteit

Deze diensten hebben tot doel gebruik te maken van de lessen die konden worden getrokken uit de praktijk van de verschillende reactieve diensten.

6.3.1 Bewustmaking

CERT.be neemt deel aan de bewustmakingsinspanningen van het CCB.

6.3.2 Opleiding

CERT.be heeft de mogelijkheid om opleidingen te ontwikkelen in de domeinen die tot zijn bevoegdheden behoren, en om opleidingssessies te organiseren.

6.4 Diensten die CERT.be niet verleent

De hieronder vermelde diensten maken deel uit van de lijst van diensten overgenomen door ENISA[8], maar worden niet verleend door CERT.be:

- Reactieve diensten:
    - Kwetsbaarheidsanalyse
    - Kwetsbaarheidsbeheer - kwetsbaarheidscorrectie
- Proactieve diensten:
    - Configuratie en onderhoud van beveiligingstools
    - Ontwikkeling van beveiligingstools
- Beheer van de beveiligingskwaliteit
    - Risicoanalyse
    - Continuïteit van de activiteiten (BCP/DRP)

[8] ENISA, "CSIRT Services," 27 04 2016, www.enisa.europa.eu/topics/csirt-cert-services [Geraadpleegd op 11 07 2017].

- Veiligheidsadvies
- Evaluatie of certificering van producten

6.5 Dienstenaanbod naargelang het doelpubliek

6.5.1 Reactieve diensten

	Aanbieders van essentiële diensten en exploitanten van kritieke infrastructuren	Aanbieders van essentiële openbare diensten	Administratieve overheden	Privaatrechtelijke rechtspersonen	Grote publiek
Meldingen en waarschuwingen	Ja[i]	Ja[i]	Ja[i]	Ja[i]	Ja
Incidentenanalyse	Ja[ii]	Ja[ii]	Ja[i]	-	-
Incidentenbeheer op site	Ja[ii]	Ja[ii]	-	-	-
Support incidentenbeheer	Ja[ii]	Ja[ii]	Ja[i]	Ja[i]	-
Coördinatie incidentenbeheer	Ja[ii]	Ja[ii]	Ja[i]	Ja[i]	-

Coördinatie kwetsbaarheidsbeheer[iii]	Ja[i]	Ja[i]	Ja[i]	Ja[i]	-
Artefactanalyseiii	Ja[ii]	Ja[ii]	-	-	-

6.5.2 Proactieve diensten

	Aanbieders van essentiële diensten en exploitanten van kritieke infrastructuren	Aanbieders van essentiële openbare diensten	Administratieve overheden	Privaatrechtelijke rechtspersonen	Grote publiek
Aankondigingen	Ja[i]	Ja[i]	Ja[i]	Ja[i]	Ja
Technologisch toezicht	Ja[i]	Ja[i]	Ja[i]	Ja[i]	Ja
Opsporing, waarneming en analyse van veiligheidsproblemen	Ja[i]	Ja[i]	Ja[i]	Ja[i]	Ja
Veiligheidsaudits/Penetratietesteniii	Ja[i]	Ja[i]	Ja[i]	-	-
Publicatie van informatie	Ja[i]	Ja[i]	Ja[i]	Ja[i]	Ja

6.5.3 Beheer van de veiligheidskwaliteit

	Aanbieders van essentiële diensten en exploitanten van kritieke infrastructuren	Aanbieders van essentiële openbare diensten	Administratieve overheden	Privaatrechtelijke rechtspersonen	Grote publiek
Bewustmaking	Ja[i]	Ja[i]	Ja[i]	Ja[i]	Ja
Opleidingen	Ja[i]	Ja[i]	Ja[i]	-	-

[i] Tijdens de kantooruren
[ii] De klok rond in samenwerking met het Crisiscentrum
[iii] Eventueel met de deelname van derden

7 DIENSTNIVEAU

CERT.be is alle werkdagen bereikbaar van 9 tot 17 uur via e-mail (cert@cert.be). De ontvangst van de naar cert@cert.be verstuurde e-mails wordt binnen enkele minuten bevestigd door een automatisch systeem. Dit systeem kent een dossiernummer toe bij elk signalement. Het is niet gezegd dat een aanbieder zal antwoorden op de mail; dit hangt af van de ernst van het incident en van de hoedanigheid van de correspondent.

In samenwerking met het Crisiscentrum van de FOD Binnenlandse Zaken is CERT.be de klok rond telefonisch bereikbaar voor de behandeling van veiligheidsincidenten bij de aanbieders van essentiële diensten en exploitanten van kritieke infrastructuren.

8 SAMENVATTING VAN HET BELEID

8.1 Soorten incidenten en supportniveau

CERT.be behandelt elk incident m.b.t. een informatie- of netwerksysteem dat gesitueerd is op Belgisch grondgebied, of elk internetdomein dat eindigt op ".be". Het supportniveau hangt af van de ernst van het incident en van de hoedanigheid van de correspondent.

Er zal als volgt prioriteit worden gegeven aan het doelpubliek:

1. aanbieders van essentiële diensten en exploitanten van kritieke infrastructuren; overheidsdiensten die essentiële diensten verlenen;
2. administratieve overheden;
3. privaatrechtelijke rechtspersonen;
4. het grote publiek.

8.2 Samenwerking, interactie en verspreiding van informatie

CERT.be verwerkt de informatie die hem is toevertrouwd volgens de geldende Belgische wetgeving. CERT.be besteedt dus aandacht aan de bescherming van de persoonsgegevens en van de gevoelige informatie die hem worden meegedeeld.

Zoals verduidelijkt in het Cybernoodplan coördineert CERT.be de activiteiten van de verschillende betrokkenen in geval van een nationaal cybersecurity-incident. In het geval van een nationaal cybersecurity-crisis, CERT.be werkt met de Algemene Directie Crisiscentrum samen om de activiteiten van de verschillende betrokken te coördineren.

Wanneer voor het oplossen van een incident dergelijke gegevens moeten worden verspreid, zal CERT.be erop toezien dat enkel het absolute minimum wordt overgemaakt.

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.

CERT.be gebruikt en respecteert het Traffic Light Protocol als beschreven door FIRST (versie 1.0)[9].

CERT.be zal zijn ervaring zoveel mogelijk delen met peers en met zijn doelpubliek, voor zover dit niet indruist tegen de hierboven vermelde voorzieningen. Er zal bijzondere aandacht worden besteed aan de volgende groepen: EGC[10], TF-CSIRT[11], FIRST[12], en het EU CSIRTs Network.

Enkel de daartoe door het CCB gemachtigde personen zullen contact hebben met de pers.

8.3 Communicatie en authenticatie

CERT.be is bereikbaar via e-mail op cert@cert.be. Er is een PGP-sleutel gekoppeld aan het adres

```
pub   4096R/52982D62 2016-12-31 [expires: 2019-12-31]
      Key fingerprint = 59FC 9F8A 4EE8 8BCF 6558  597E 2AFB E221 5298 2D62
uid       [  full  ] CERT.be <cert@cert.be>
```

CERT.be beschikt over personeel dat gemachtigd is voor de verwerking van de informatie die geclassificeerd is in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen[13].

[9] 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/.
[10] European Governmental CERTs
[11] Task Force – Cooperation of Computer Security Incident Response Teams
[12] Forum of Incident Response Teams
[13] Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, B.S., 7 mei 1999, p. 15752.