CENTRE FOR
CYBERSECURITY
BELGIUM

EERSTE HULP BIJ EEN CYBERINCIDENT

VOORBEREIDING EN AANPAK VAN INCIDENTEN

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Datum: Mei 2026
Versie: 1.0 Nederlands
Auteur: Centrum voor Cybersecurity België (CCB)

Het Centrum voor Cybersecurity België (CCB) is de nationale autoriteit voor cybersecurity in België. Het CCB werd opgericht bij Koninklijk Besluit van 10 oktober 2014. Op basis van zijn wettelijke opdracht informeert en adviseert het CCB organisaties over het versterken van de voorbereiding van cyberbeveiligingsncidenten en incidentresponse.

Inhoudstafel

Inleiding

Dit document vat de essentiële capaciteiten en acties samen waarover organisaties moeten beschikken voor een doeltreffende incidentbehandeling en coördinatie met het CCB.

Dit document vult het CyberFundamentals Framework en de Safeonweb@work-richtlijnen aan door te focussen op operationele basisvereisten bij de aanpak van een cyberincident.https://cyfun.eu/

1. Voor een incident: minimale capaciteiten

Organisaties moeten minstens over de volgende technische basiscapaciteiten beschikken om een cyberincident snel te detecteren, in te dammen en ervan te herstellen:

Vroegtijdige waarschuwing en snelle respons

- Iemand (intern of extern) moet 24/7 toezicht houden op verdachte activiteiten en onmiddellijk kunnen ingrijpen (Security Operations Centre).

Bescherming van laptops en computers

- Alle toestellen moeten beveiligingssoftware hebben die schadelijke activiteiten automatisch kan detecteren en blokkeren (Endpoint Detection and Response).

Zicht op wat er in uw netwerk gebeurt

- Belangrijke systemen moeten de logs naar een centrale omgeving sturen zodat problemen snel kunnen worden opgemerkt (Security Information and Event Management).

Dit moet minstens omvatten:

  - gebruikersaccounts en aanmeldsystemen
  - firewalls en toegang op afstand
  - toestelbeveiliging
  - e-mailbeveiliging
  - kritieke servers en toepassingen

Deze informatie moet minstens 90 dagen worden bewaard (langer wordt aanbevolen voor kritieke systemen).

Sterke aanmeldbeveiliging

- Multi-Factor Authentication (MFA) moet voor iedereen ingeschakeld zijn, in het bijzonder voor admins en medewerkers die op afstand werken.

Beperken van lateral movement door aanvallers (netwerksegmentatie)

- Het netwerk moet zo zijn ontworpen dat een aanvaller die één systeem binnendringt, zich niet gemakkelijk naar andere systemen kan verplaatsen.

Betrouwbare back-ups

- Organisaties hebben een back-upstrategie nodig die het volgende omvat:

  - minstens één kopie die niet kan worden gewijzigd of verwijderd (immutable back-ups)
  - regelmatige tests om te verifiëren dat gegevensherstel werkt

Alternatief communicatiekanaal

- Zorg voor een communicatiekanaal buiten de normale bedrijfs-e-mail of chat om te communiceren, voor het geval systemen onbeschikbaar of gecompromitteerd zijn.

Duidelijk overzicht van uw omgeving

- Houd een actuele lijst bij van:
  - alle toestellen en systemen
  - hoe het netwerk is opgebouwd (netwerkschema)
  - belangrijke IP-adressen

Noodtoegang (break-glass accounts)

- Voorzie speciale noodaccounts en procedures voor situaties waarin het normale aanmeldsysteem niet beschikbaar is.

Offline noodinformatie

- Kritieke informatie moet ook op papier beschikbaar zijn, zoals:
  - stapsgewijze gidsen (playbooks)
  - sleutelcontacten
  - escalatiepaden
  - hotlines voor leverancierssupport
  - wat te doen bij ransomware, datalekken, frauduleuze e-mails of DDoS-aanvallen

Incidentopvolging

- Gebruik een eenvoudig hulpmiddel of systeem om te registreren:
  - wat er is gebeurd
  - genomen acties en beslissingen
  - getroffen systemen
  - gevonden bewijsmateriaal en indicatoren

Dit zijn de **minimale technische basisvereisten** om een cyberaanval vroegtijdig te detecteren, de schade te beperken en doeltreffend te herstellen.

1.1. ORGANISATORISCH

Technische maatregelen alleen volstaan niet. Goed bestuur en duidelijke voorbereiding zijn minstens even belangrijk en sluiten volledig aan bij de verwachtingen onder NIS2.

Organisaties moeten minstens over het volgende beschikken:

Een duidelijk incidentplan

- Een eenvoudig Incident Response Plan dat uitlegt wie wat doet en hoe problemen worden geëscaleerd.

Plannen om de bedrijfsactiviteiten voort te zetten

- Een Business Continuity Plan dat uitlegt hoe essentiële activiteiten tijdens een crisis kunnen doorgaan.
- Een Disaster Recovery Plan dat prioriteiten vastlegt en bepaalt hoe snel systemen moeten worden hersteld.

Een aanpak voor crisiscommunicatie

- Een duidelijk plan om communicatie tijdens een crisis te beheren, zowel intern als extern.

Een 24/7-contactlijst

- Een actuele lijst van sleutelcontacten, waaronder:
  - technische teams
  - directie
  - juridische adviseurs
  - communicatie
  - externe partners

Een eenvoudige aanpak voor risicobeheer

- Een vastgelegde manier om risico's te identificeren, te evalueren en te beheren. Ook een licht framework volstaat.

Regelmatige oefeningen

- Tabletopoefeningen voor zowel technische teams als leidinggevenden, zodat iedereen weet wat te doen bij een incident.

Zie CyFun® en Safeonweb@work.

2. Tijdens een incident: de eerste 24 uur

De eerste 24 uur tijdens een incident zijn cruciaal.

De prioriteiten zijn:

- stop de verspreiding,
- bewaar bewijsmateriaal, en
- coördineer vroegtijdig met de juiste personen.

Hieronder staat een toegankelijke en eenvoudig te volgen versie van wat er moet gebeuren.

2.1. ONMIDDELLIJK (T+0)

Zodra u een incident vermoedt:

1. Activeer uw Incident Response Plan

Iedereen moet zijn rol kennen en weten wat de volgende stappen zijn.

2. Schakel over naar een alternatief communicatiekanaal

Gebruik een communicatiemiddel buiten de normale bedrijfssystemen (bv. Signal, Threema, SMS) voor het geval e-mail of chat gecompromitteerd is.

3. Bewaar bewijsmateriaal

Houd logs en systeeminformatie intact. Dit helpt om te begrijpen wat er is gebeurd en ondersteunt herstel en onderzoek.

4. Wis, herinstalleer of herstart systemen NIET

Doe dit alleen als het absoluut noodzakelijk is en nadat bewijsmateriaal is veiliggesteld. Deze acties kunnen cruciale informatie vernietigen.

5. Documenteer alles

   Noteer:
   - wat u hebt gedaan
   - wanneer u het hebt gedaan
   - wat u hebt vastgesteld

Dit ondersteunt coördinatie, onderzoek en rapportering.

2.2. BINNEN DE EERSTE 24 UUR

Breng het CCB vroegtijdig op de hoogte

Als u een significant incident vermoedt, informeer het CCB, ook wanneer u nog niet over alle details beschikt.

Vroegtijdige melding maakt het mogelijk om:

- sneller ondersteuning te bieden
- een beter situationeel beeld te krijgen
- sectoroverschrijdend gecoördineerd te reageren

Deel de basisinformatie waarover u beschikt:

Bezorg wat op dat moment beschikbaar is:

- Of het incident kwaadwillig lijkt
- Gekende of geraamde impact
- Getroffen systemen of diensten
- Reeds genomen acties

Waar melden:

- Bel bij hoogdringendheid - het meldformulier kan nadien worden ingevuld
    - Noodcontact CCB: +32 2 501 05 60
- Online melding: https://notif.safeonweb.be/ https://notif.safeonweb.be/
- Dien een klacht in bij de politie
- Informeer uw cyberverzekeraar (indien van toepassing)

Waarom dit belangrijk is:
Vroegtijdige melding en goede documentatie helpen het incident sneller in te dammen en zorgen ervoor dat ondersteuning snel kan worden gemobiliseerd.

3. Tijdens een incident: binnen 72 uur

Binnen de eerste 72 uur moeten organisaties een vollediger beeld hebben van wat er is gebeurd.

Belangrijkste acties:

Dien een formele melding in (indien van toepassing):

- Als het incident aan de NIS2-drempels voldoet, verstuur dan de officiële melding.

Deel geactualiseerde informatie:

Bezorg wat in deze fase bekend is, waaronder:

- de omvang van het incident
- de impact op systemen of diensten
- eventuele gevonden indicators of compromise (IOCs)
- maatregelen die al zijn genomen om het incident in te dammen
- bedrijfsimpact en operationele gevolgen

Als persoonsgegevens getroffen zijn:

- Meld dit aan de Gegevensbeschermingsautoriteit (GBA) zoals vereist onder de GDPR.

Houd het CCB op de hoogte:

- Blijf updates delen met het CCB zodra nieuwe informatie beschikbaar komt.

Waarom dit belangrijk is: duidelijke rapportering en transparantie vroeg in het proces vergemakkelijken de coördinatie en verminderen bredere risico's.

4. Tijdens een incident: binnen 1 maand

Binnen één maand na de eerste melding (of nadat het incident is opgelost) moet een eindbeoordeling worden voorbereid.

Stel een eindrapport op:

Dit moet het volgende bevatten:

- een root-causeanalyse (hoe het incident is begonnen)
- een tijdlijn van wat er is gebeurd
- de volledige impactbeoordeling
- alle containment- en eradication-acties
- genomen herstelstappen
- langetermijnverbeteringen
- duidelijke lessons learned

Lopende incidenten:

Als het incident na één maand nog actief is:

- bezorg een voortgangsupdate
- dien het eindrapport in binnen één maand nadat het incident is afgesloten

Waarom dit belangrijk is:
Een post-incident review helpt de weerbaarheid te versterken en herhaling te voorkomen.

5. Lessons learned en continue verbetering

Voer regelmatig oefeningen uit:

- Organiseer minstens één keer per jaar tabletopoefeningen, en na belangrijke wijzigingen.
- Voer gerichte technische tests uit, zoals:
  - back-uphersteltests
  - oefeningen rond netwerksegmentatie / isolatie
  - oefeningen rond identiteitsherstel

Gebruik een gestructureerd after-actionproces:

- voer een formele after-action review uit
- volg remediëringsstappen op tot ze volledig zijn afgerond

Dit ondersteunt evidence-based verbetering en voortdurende paraatheid.

6. Operationele afstemming met het CCB

Om tijdens een crisis doeltreffend met het CCB samen te werken, moeten organisaties zorgen voor:

Een duidelijke 24/7-contactstructuur

- één permanent bereikbaar contactpunt
- Een duidelijk escalatiepad: incident manager, CIO, CISO, communicatie, DPO

Duidelijke drempels om het CCB te informeren

- Informeer het CCB wanneer een significant incident wordt vermoed, ook als de informatie nog onvolledig is.

Correcte omgang met bewijsmateriaal

- bewaar logs en artefacten
- vermijd wissen, herinstalleren of herstarten vóór triage
- documenteer acties en tijdstippen

Informatiepakket klaar om te delen

Zorg dat deze elementen klaar zijn voor een gecoördineerde respons:

- getroffen diensten
- scope
- IOCs
- tijdlijn
- mitigatieacties
- bedrijfsimpact

Afgesproken veilige communicatiekanalen

- Zoom voor coördinatievergaderingen
- Signal/Threema/telefoon voor crisiscommunicatie
- versleutelde uitwisseling voor gevoelige documenten

7. Hoe het CCB past in de playbooks van een organisatie

Triage en kwalificatie

- Contacteer het CCB wanneer een significant incident wordt vermoed of wanneer richtlijnen of nieuwe IOCs nodig zijn.

Forensisch inzicht

- Het CCB helpt forensische data te analyseren, de toegangen te analyseren en de root cause te identificeren.

Containment & eradication

- Deel IOCs en TTPs
- Ontvang mitigatierichtlijnen
- Neem deel aan een gecoördineerde respons als het incident deel uitmaakt van een bredere campagne

Melding

- Gebruik https://notif.safeonweb.be/ https://notif.safeonweb.be/
- Vul de verplichte velden in
- Houd het CCB op de hoogte naarmate de situatie evolueert

Post-incident

- Bezorg het eindrapport
- Pas aanbevelingen voor verbetering toe

Dit sluit volledig aan bij de aanpak van samenwerking, voorbereiding en sectorbrede weerbaarheid.

Bijlage 1: nuttige links

CyberFundamentals Framework: https://cyfun.eu

NIS2-meldingsgids: https://ccb.belgium.be/sites/default/files/2025-08/NIS2_Notification_guide_v1.3-EN.pdf https://ccb.belgium.be/sites/default/files/2025-08/NIS2_Notification_guide_v1.3-EN.pdf

CCB eerste aanspreekpunt: https://ccb.belgium.be/nl/cert/eerste-hulp-bij-een-cyberaanval

Meldingsformulier voor een incident: https://notif.safeonweb.be/

Crisiscommunicatie bij een cyberaanval: https://atwork.safeonweb.be/nl/news/crisiscommunicatie-bij-een-cyberaanval

Safeonweb at work: https://atwork.safeonweb.be/

Disclaimer

Dit document en de bijlagen ervan werden opgesteld door het Centrum voor Cybersecurity België (CCB), een federale administratie opgericht bij Koninklijk Besluit van 10 oktober 2014 en onder het gezag van de Eerste Minister.

Dit document bevat technische informatie die hoofdzakelijk in het Engels is opgesteld. Deze technische informatie is immers rechtstreeks afkomstig uit rapporten die door verschillende internationale partners aan het CCB werden bezorgd (Europees netwerk van CSIRTs, internationale organisaties, buitenlandse ondernemingen, enz.) en die in het Engels zijn opgesteld. Bovendien wordt deze informatie over de beveiliging van netwerk- en informatiesystemen wegens hoogdringendheid bezorgd aan de betrokken organisaties en aan IT-diensten die de Engelse computerterminologie gebruiken.

Een vertaling van deze technische informatie naar het Nederlands, Frans of Duits kan niettemin bij het CCB worden aangevraagd.

Het CCB aanvaardt geen aansprakelijkheid voor de inhoud van dit document.

De verstrekte informatie:

• is uitsluitend van algemene aard en beoogt niet alle specifieke situaties in aanmerking te nemen;

• is niet noodzakelijk exhaustief, precies of op alle punten up-to-date;

Verantwoordelijke uitgever:

Centrum voor Cybersecurity België
De heer De Bruycker, Algemeen Directeur
Wetstraat 1
1000 Brussel

Wettelijk depot: D/2026/14828/009