CENTRE FOR CYBERSECURITY BELGIUM

PREMIERS SECOURS EN CAS DE CYBERINCIDENT

PRÉPARATION ESSENTIELLE ET RÉPONSE AUX INCIDENTS

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date : Mai 2026
Version : 1.0 français
Auteur : Centre pour la Cybersécurité Belgique (CCB)

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale en matière de cybersécurité en Belgique. Le CCB a été créé par l'Arrêté royal du 10 octobre 2014. Sur la base de sa mission légale, le CCB informe et conseille les organisations afin d'améliorer leur préparation et leur réponse aux incidents.

Table des matières

Introduction

Ce document résume les capacités et actions essentielles que les organisations devraient mettre en place afin d'assurer une gestion efficace des incidents et une coordination avec le CCB.

Le document complète également le CyberFundamentals Framework et les recommandations Safeonweb@work en mettant l'accent sur les éléments opérationnels essentiels. https://atwork.safeonweb.be/

1. Avant un incident : capacités minimales de préparation

Les organisations devraient disposer au minimum des capacités techniques de base suivantes afin de détecter rapidement un cyberincident, de le contenir et de reprendre ses activités :

Alerte précoce et réponse rapide

- Une personne ou une équipe (interne ou externe) doit assurer une surveillance 24/7 des activités suspectes et être en mesure d'agir immédiatement (Security Operations Centre).

Protection des ordinateurs portables et postes de travail

- Tous les appareils devraient disposer d'un logiciel de sécurité capable de détecter et de bloquer automatiquement les activités malveillantes (Endpoint Detection and Response).

Visibilité sur ce qui se passe dans votre réseau

- Les systèmes importants devraient transmettre leurs journaux d'activité vers un emplacement central afin que les problèmes puissent être détectés rapidement (Security Information and Event Management).

Cela devrait comprendre au minimum :

  - les comptes utilisateurs et les systèmes d'authentification
  - les pare-feux et les accès à distance
  - la protection des appareils
  - la sécurité de la messagerie électronique
  - les serveurs et applications critiques

Ces informations devraient être conservées pendant au moins 90 jours (une durée plus longue est recommandée pour les systèmes critiques).

Protection renforcée des connexions

- L'authentification multifacteur (MFA) doit être activée pour tous, en particulier pour les administrateurs et les travailleurs à distance.

Limiter les déplacements d'un attaquant (segmentation du réseau)

- Le réseau devrait être conçu de manière à empêcher un attaquant qui compromet un système de se déplacer facilement vers d'autres systèmes.

Sauvegardes fiables

- Les organisations ont besoin d'une stratégie de sauvegarde comprenant :

  - au moins une copie qui ne peut pas être modifiée ni supprimée (immutable)
  - des tests réguliers afin de vérifier que la restauration des données fonctionne

Canal de communication alternatif

- Un moyen de communication doit être prévu en dehors de la messagerie ou du chat habituels de l'entreprise, au cas où ces systèmes seraient indisponibles ou compromis.

Vue claire de votre environnement

- Tenez à jour une liste de :
  - tous les appareils et systèmes
  - la structure du réseau
  - les adresses IP importantes

Accès d'urgence (comptes break-glass)

- Maintenez des comptes d'urgence spécifiques et des procédures pour les situations dans lesquelles le système d'authentification habituel est indisponible.

Informations d'urgence hors ligne

- Les informations critiques devraient également être disponibles sur papier, notamment :
  - des guides étape par étape (playbooks)
  - les contacts clés
  - les voies d'escalade
  - les lignes d'assistance des fournisseurs
  - les actions à mener en cas de ransomware, de violation de données, d'e-mails frauduleux ou d'attaques DDoS

Suivi des incidents

- Utilisez un outil ou système simple pour consigner :
  - ce qui s'est passé
  - les actions et décisions prises
  - les systèmes affectés
  - les preuves et indicateurs trouvés

Il s'agit des éléments **techniques minimaux nécessaires** pour détecter rapidement une cyberattaque, limiter les dommages et assurer une reprise efficace.

1.1. ORGANISATIONNEL

Les mesures techniques seules ne suffisent pas. Une bonne gouvernance et une préparation claire sont tout aussi importantes et pleinement conformes aux attentes de NIS2.

Les organisations devraient disposer au minimum des éléments suivants :

Un plan d'incident clair

- Un plan de réponse aux incidents simple qui explique qui fait quoi et comment les problèmes sont escaladés.

Des plans pour maintenir l'activité

- Un plan de continuité d'activité expliquant comment les activités essentielles peuvent se poursuivre pendant une crise.
- Un plan de reprise après sinistre qui fixe les priorités et définit les délais de restauration des systèmes.

Une approche de communication de crise

- Un plan clair pour gérer la communication pendant une crise, tant en interne qu'en externe.

Une liste de contacts 24/7

- Une liste à jour des contacts clés, notamment :
  - les équipes techniques
  - la direction
  - les conseillers juridiques
  - la communication
  - les partenaires externes

Une approche simple de gestion des risques

- Une méthode définie pour identifier, évaluer et gérer les risques. Même un cadre léger est suffisant.

Des exercices réguliers

- Des exercices tabletop pour les équipes techniques comme pour les dirigeants, afin que chacun sache quoi faire lorsqu'un incident survient.

Pour le modèle complet de gouvernance de base, consultez les ressources CyFun® et Safeonweb@work.

2. Pendant un incident : les premières 24 heures

Les premières 24 heures d'un incident sont critiques.

Les priorités sont les suivantes :

- arrêter la propagation,
- préserver les preuves, et
- coordonner rapidement avec les bonnes personnes.

Vous trouverez ci-dessous une version accessible et facile à suivre des actions à entreprendre.

2.1. IMMÉDIATEMENT (T+0)

Dès que vous suspectez un incident :

1. Activez votre plan de réponse aux incidents

Chacun doit connaître son rôle et les prochaines étapes à suivre.

2. Passez à un canal de communication alternatif

Utilisez un moyen de communication extérieur aux systèmes habituels de l'entreprise (par exemple Signal, Threema, SMS) au cas où l'e-mail ou le chat seraient compromis.

3. Préservez les preuves

Conservez les journaux et les informations système intacts. Cela aide à comprendre ce qui s'est passé et soutient la reprise ainsi que l'enquête.

4. NE PAS effacer, réinstaller ou redémarrer les systèmes

Ne le faites que si c'est absolument nécessaire et uniquement après avoir sécurisé les preuves. Ces actions peuvent détruire des informations cruciales.

5. Documentez tout

   Notez :
   - ce que vous avez fait
   - quand vous l'avez fait
   - ce que vous avez observé

Cela soutient la coordination, l'enquête et le reporting.

2.2. DANS LES PREMIÈRES 24 HEURES

Prévenez rapidement le CCB

Si vous suspectez un incident significatif, informez le CCB même si vous ne disposez pas encore de tous les détails.

Une notification précoce permet :

- un soutien plus rapide
- une meilleure compréhension de la situation
- une réponse coordonnée entre secteurs

Partagez les informations de base dont vous disposez :

Fournissez les informations disponibles à ce moment-là :

- si l'incident semble malveillant
- l'impact connu ou estimé
- les systèmes ou services affectés
- les actions déjà entreprises

Où notifier :

- Appelez en cas d'urgence - le formulaire de notification peut être complété ensuite
  - Contact d'urgence CCB : +32 2 501 05 60
- Notification en ligne : https://notif.safeonweb.be/ https://notif.safeonweb.be/
- Déposez une plainte auprès de la police
- Informez votre assureur cyber (le cas échéant)

Pourquoi c'est important : Une notification précoce et une bonne documentation aident à contenir l'incident plus rapidement et permettent de mobiliser le support nécessaire sans délai.

3. Pendant un incident : dans les 72 heures

Dans les 72 premières heures, les organisations devraient disposer d'une vision plus complète de ce qui s'est passé.

Actions clés :

Soumettez une notification formelle (le cas échéant) :

- Si l'incident atteint les seuils NIS2, envoyez la notification officielle.

Partagez les informations mises à jour :

Fournissez tout ce qui est connu à ce stade, notamment :

- le périmètre de l'incident
- l'impact sur les systèmes ou services
- les éventuels indicateurs de compromission (IOCs) identifiés
- les mesures déjà prises pour contenir l'incident
- l'impact métier et les effets opérationnels

Si des données à caractère personnel sont affectées :

- Notifiez l'Autorité de protection des données (APD) conformément au RGPD.

Tenez le CCB informé :

- Continuez à partager les mises à jour avec le Centre pour la Cybersécurité Belgique (CCB) à mesure que de nouvelles informations deviennent disponibles.

Pourquoi c'est important : une communication claire et transparente dès le début du processus facilite la coordination et réduit les risques plus larges.

4. Pendant un incident : dans le mois

Dans le mois suivant la notification initiale (ou après la résolution de l'incident), une évaluation finale devrait être préparée.

Préparez un rapport final :

Celui-ci devrait inclure :

- une analyse de la cause profonde (comment l'incident a commencé)
- une chronologie des événements
- l'évaluation complète de l'impact
- toutes les actions de confinement et d'éradication
- les étapes de reprise mises en œuvre
- les améliorations à long-terme
- les enseignements clairs

Incidents en cours :

Si l'incident est toujours actif après un mois :

- fournissez une mise à jour de l'état d'avancement
- soumettez le rapport final dans le mois suivant la clôture de l'incident

Pourquoi c'est important :
La revue post-incident contribue à renforcer la résilience et à prévenir la récurrence.

5. Retour d'expérience et amélioration continue

Organisez des exercices réguliers :

- Organisez des exercices sur table au moins une fois par an, ainsi qu'après des changements majeurs.
- Réalisez des tests techniques ciblés, tels que :
  - des tests de restauration de sauvegardes
  - des exercices de segmentation / isolation du réseau
  - des exercices de restauration des identités

Utilisez un processus structuré d'analyse a posteriori:

- Menez une revue formelle a posteriori
- Suivez les mesures de remédiation jusqu'à leur achèvement complet

Cette approche soutient une amélioration fondée sur les preuves et une préparation continue.

6. Cohérence opérationnelle avec le CCB

Pour collaborer efficacement avec le CCB pendant une crise, les organisations devraient assurer :

Une structure de contact claire 24/7

- Un point de contact joignable en permanence
- Une voie d'escalade claire : incident manager, CIO, CISO, communication, DPO

Des seuils clairs pour notifier le CCB

- Notifiez le CCB lorsqu'un incident significatif est suspecté, même si les informations sont encore incomplètes.

Une gestion correcte des preuves

- Préservez les journaux (logs) et les artefacts
- Évitez d'effacer, de réinstaller ou de redémarrer avant la phase de triage
- Documentez les actions et les horodatages

Un dossier d'informations prêt à être partagé

Préparez ces éléments pour une réponse coordonnée :

- services affectés
- périmètre
- IOCs
- chronologie
- actions de mitigation
- impact métier

Des canaux de communication sécurisés convenus

- Zoom pour les réunions de coordination
- Signal/Threema/téléphone pour la communication de crise
- Échange chiffré pour les documents sensibles

7. Comment le CCB s'intègre dans les playbooks d'une organisation

Triage et qualification

- Contactez le CCB lorsqu'un incident significatif est suspecté ou lorsque des orientations ou de nouveaux IOCs sont nécessaires.

Analyse forensique

- Le CCB aide à analyser les preuves, à comprendre le point d'entrée et à identifier la cause racine.

Confinement et éradication

- Partagez les IOCs et les TTPs
- Recevez des recommandations de mitigation
- Participez à une réponse coordonnée si l'incident fait partie d'une campagne plus large

Notification

- Utilisez https://notif.safeonweb.be/
- Renseignez les champs obligatoires
- Tenez le CCB informé à mesure que la situation évolue

Post-incident

- Transmettez le rapport final
- Appliquez les recommandations d'amélioration

Cette approche est pleinement alignée sur les principes **de collaboration, de préparation et de résilience sectorielle.**

Annexe 1 : liens utiles

CyberFundamentals Framework : https://cyfun.eu

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

Premier point de contact CCB : https://ccb.belgium.be/cert/first-port-call-event-cyberattack

Formulaire de notification d'un incident : https://notif.safeonweb.be/

La communication de crise en cas de cyberattaque: https://atwork.safeonweb.be/fr/news/la-communication-de-crise-en-cas-de-cyberattaque

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

Clause de non-responsabilité

Ce document et ses annexes ont été préparés par le Centre pour la Cybersécurité Belgique (CCB), une administration fédérale créée par l'Arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre.

Ce document contient des informations techniques rédigées principalement en anglais. En effet, ces informations techniques sont extraites directement de rapports transmis au CCB par divers partenaires internationaux (réseau européen des CSIRTs, organisations internationales, entreprises étrangères, etc.), qui sont rédigés en anglais. En outre, ces informations relatives à la sécurité des réseaux et des systèmes d'information sont adressées, en raison de l'urgence, aux organisations concernées ainsi qu'aux services IT qui utilisent les termes anglais du langage informatique.

Une traduction de ces informations techniques en néerlandais, en français ou en allemand peut néanmoins être demandée au CCB.

Le CCB décline toute responsabilité quant au contenu de ce document.

Les informations fournies :

• sont exclusivement de nature générale et ne visent pas à prendre en considération toutes les situations particulières ;

• ne sont pas nécessairement exhaustives, précises ou à jour sur tous les points ;

Éditeur responsable :

Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 1
1000 Bruxelles

Dépôt légal : D/2026/14828/008