CENTRE FOR CYBERSECURITY BELGIUM

Directive n° 1/2025
13 mars 2025

Directive du CCB pour les systèmes d'information de toutes les organisations privées ou publiques établies (ou actives) en Belgique

En vertu de l'article 17, 7° de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après, la « loi NIS2 »), l'Autorité nationale de cybersécurité (le Centre pour la Cybersécurité Belgique, ci-après « le CCB ») est notamment chargée d'élaborer, de diffuser et de veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de systèmes d'information.

Chaque jour dans notre pays, une organisation ou une entreprise est victime d'une attaque par rançongiciel ou d'une extorsion après le vol d'informations sensibles. En 2024, le CCB a reçu 352 notifications d'incidents provenant d'organisations privées et publiques. Des petites PME aux grandes organisations, personne n'est épargné, comme nous l'enseignent les cyberattaques de l'année dernière. Pourtant, ces attaques peuvent souvent être évitées.

Par conséquent, le CCB demande aux organisations privées et publiques établies (ou actives) en Belgique de mettre en œuvre les lignes directrices suivantes dans le domaine de la cybersécurité :

1. Utilisez des moyens d'authentification multifacteur (MFA)

Le CCB invite l'ensemble des organisations privées et publiques établies (ou actives) en Belgique à activer dès que possible au moins une méthode d'authentification multifacteur (MFA) sur toutes les connexions externes des réseaux et systèmes qu'elles utilisent. L'authentification multifacteur est un outil simple et facile à mettre en œuvre, qui fait toute la différence pour la cybersécurité d'une organisation.

Il ressort des incidents que nous avons observés que les cybercriminels utilisent souvent des identifiants de connexion volés pour lancer leurs attaques. Un des meilleurs moyens de protéger votre organisation contre cela est d'utiliser l'authentification multifacteur pour toutes les connexions provenant de l'extérieur de l'entreprise ou de l'organisation.

Plus d'informations sur l'implémentation de l'authentification multifacteur sont disponible sur notre site internet : https://atwork.safeonweb.be/fr/MFA.

2. Sécurisez votre organisation à l'aide du CyberFundamentals (CyFun®) Framework du CCB

Le CCB invite l'ensemble des organisations privées et publiques établies (ou actives) en Belgique à utiliser le CyberFundamentals (CyFun®) Framework pour sécuriser leurs réseaux et systèmes d'information.

CyFun® compile une série de mesures concrètes visant à :

- protéger les données ;
- réduire considérablement le risque des cyberattaques les plus courantes ;
- accroître la cyber-résilience d'une organisation.

Pour répondre à la gravité de la menace à laquelle une organisation est exposée, outre le niveau de départ « Small », trois niveaux d'assurance sont prévus : Basic, Important et Essential. Le référentiel a été validé à l'aide des profils d'attaque du CERT (obtenus à la suite d'attaques réussies). La conclusion est la suivante :

- les mesures du niveau d'assurance Basic permettent de couvrir 82 % des attaques ;
- les mesures du niveau d'assurance Important permettent de couvrir 94 % des attaques ;
- les mesures du niveau d'assurance Essential permettent de couvrir 100 % des attaques.

En outre, CyFun® :

- **repose sur des normes reconnues** : CyFun® sélectionne des contrôles pertinents basés sur des normes internationalement reconnues telles que NIST CSF, ISO/IEC 27001, CIS Controls et IEC 62443. Il inclut également les exigences découlant de la loi NIS2 ;
- **correspond aux mesures nécessaires et proportionnées aux risques** pour prévenir les principales attaques identifiées par le CCB ;
- **peut être utilisé sans assistance externe** : chaque contrôle est accompagné de conseils pour faciliter sa mise en œuvre. L'outil d'auto-évaluation de CyFun® permet d'évaluer correctement la mise en œuvre des mesures ;
- **permet d'obtenir une vérification ou une certification par un organisme externe** : vous pouvez valider votre mise en œuvre en demandant une évaluation par un organisme d'évaluation de la conformité accrédité et agréé. Cette attestation fournit la preuve de votre mise en œuvre à vos clients et à vos autorités (par exemple, pour se conformer à NIS2).

Dans le contexte de la loi NIS2, le CyFun® est un outil permettant de démontrer, de manière pratique, la mise en œuvre des exigences légales : non seulement pour les entités essentielles soumises à une évaluation périodique de la conformité mais aussi pour les entités importantes. Disponible gratuitement, il offre des outils concrets pour la mise en œuvre des mesures minimales de gestion des risques, pour le choix du niveau adéquat du référentiel, pour l'auto-évaluation et pour la correspondance avec d'autres normes reconnues.

En outre, une mise en œuvre du CyFun® validée ou certifiée par un organisme d'évaluation de la conformité (CAB) accrédité et agréé confère aux entités concernées une **présomption de conformité** dans le cadre de la supervision prévue par la loi NIS2. Le CCB recommande ainsi vivement à toutes les entités soumises à la loi NIS2 à utiliser le CyFun®.

Plus d'informations sur le référentiel CyFun® sont disponibles sur notre site internet : https://cyfun.be.

Miguel De Bruycker

Directeur général du CCB