CENTRE FOR CYBERSECURITY BELGIUM

Avis n° 1/2024 du 24 janvier 2024

Directive du CCB pour les systèmes informatiques des administrations et institutions publiques

---

Le Centre pour la Cybersécurité Belgique (CCB) invite les administrations et les institutions publiques à activer dès que possible l'authentification en deux étapes (2FA) sur toutes les connexions externes à leurs réseaux et systèmes. C'est la responsabilité de chaque service public de garantir la prestation de services et d'assurer la sécurité optimale des données des citoyens. 2FA est un outil simple et facilement réalisable qui fait toute la différence pour la cybersécurité des administrations publiques.

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 2023, 120 organisations privées et publiques ont effectué une notification au CCB. Les villes, les municipalités et les autres services publics ne sont pas épargnés, comme nous l'enseignent les cyberattaques de l'année dernière. Pourtant, ces attaques peuvent souvent être évitées.

Selon l'article 3, 6°, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, le CCB a notamment pour mission d'élaborer, de diffuser et de veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics.

Par conséquent, le CCB demande aux administrations et aux institutions publiques de mettre en œuvre les lignes directrices suivantes dans le domaine de la cybersécurité :

- **Installer aussi vite que possible l'authentification en deux étapes**

Il ressort des incidents que nous avons observés que les cybercriminels utilisent souvent des identifiants de connexion volés pour lancer leur attaque. La meilleure façon d'armer votre organisation contre cela est d'utiliser l'authentification en deux étapes (2FA) pour toutes les connexions provenant de l'extérieur de l'entreprise ou de l'organisation.
Plus d'informations sur l'implémentation de 2FA : https://atwork.safeonweb.be/fr/MFA

- **Rendre votre organisation conforme au *framework* Cyber Fundamentals du CCB**

Le CCB dispose d'un cadre, appelé "Cyber Fundamentals", qui guide les organisations vers une cyber-résilience appropriée. Nous invitons toutes les administrations et institutions publiques à adopter le niveau approprié des Cyber Fundamentals en tant que norme de sécurité pour l'organisation. Le CCB fournit également un outil simple permettant de déterminer facilement le niveau approprié.
Plus d'informations sur le *framework* Cyber Fundamentals : https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework

Centre pour la Cybersécurité Belgique
Sous l'autorité du Premier Ministre
Rue de la Loi 18 - 1000 Brussels
www.ccb.belgium.be

.be

- **Les administrations et les institutions publiques ne doivent pas se laisser extorquer**

Le CCB conseille de s'attaquer collectivement aux paiements de ransomware afin de saper le modèle économique des ransomwares et de perturber ces activités criminelles. Nous ne tolérerons pas les actes d'extorsion de ces cybercriminels.
C'est pourquoi nous déconseillons vivement à quiconque de payer le prix d'un rançongiciel. Le paiement d'une rançon aux auteurs d'un rançongiciel :

- Ne garantit pas la fin d'un incident ni le retrait des logiciels malveillants ;
- Encourage les criminels à poursuivre et à étendre leurs activités ;
- Fournit aux criminels des ressources supplémentaires ;
- Ne garantit pas que vous récupérerez vos données ni qu'elles ne seront pas rendues publiques.

Miguel De Bruycker
Directeur Général CCB

Centre pour la Cybersécurité Belgique
Sous l'autorité du Premier Ministre
Rue de la Loi 18 - 1000 Brussels
www.ccb.belgium.be