Safeonweb
@Work

UNE INITIATIVE DE

CENTRE FOR CYBER SECURITY BELGIUM

CYBERFONDAMENTAUX

SMALL

Version 2023-03-01

Centre pour la Cybersécurité Belgique
18 Rue de la Loi
1000 Bruxelles
Belgique

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

Table des matières

Introduction 3
1 PROTÉGER TOUTES LES CONNEXIONS AVEC L'AUTHENTIFICATION MULTIFACTORIELLE .. 4
2 INSTALLER IMMÉDIATEMENT TOUTES LES MISES À JOUR DE SÉCURITÉ 4
3 INSTALLER UN ANTIVIRUS 5
4 SÉCURISER VOTRE RÉSEAU 5
5 SAUVEGARDER VOS DONNÉES 6
6 DROITS D'ADMINISTRATION 6
7 RECOMMANDATIONS FINALES 7

Introduction

Le **cadre des cyberfondamentaux du CCB** est un ensemble de mesures concrètes visant à :
-protéger les données,
-réduire considérablement le risque des cyber-attaques les plus courantes,
-augmenter 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 "**Petit**", trois niveaux d'assurance sont prévus : **Basique, Important et Essentiel**.

Le **niveau de départ** "**Petit**" permet à une organisation de procéder à une première évaluation, en excluant les aspects liés au développement interne des applications.

Le niveau initial Small est destiné aux micro-organisations (à l'exception des environnements à haut risque) ou aux organisations ayant des connaissances techniques limitées.

Le cadre est un document évolutif qui continuera d'être mis à jour et amélioré en fonction des réactions des parties prenantes, de l'évolution des risques liés à des menaces de cybersécurité spécifiques, de la disponibilité de solutions techniques et de l'évolution des connaissances.

1 PROTÉGER TOUTES LES CONNEXIONS GRÂCE À L'AUTHENTIFICATION MULTIFACTORIELLE

Utilisez l'authentification multifactorielle dans la mesure du possible. Toujours utiliser l'authentification multifactorielle pour l'accès à distance

Orientations

La plupart des outils d'authentification multifactorielle combinent votre mot de passe avec des éléments que vous possédez (smartphone, badge, carte d'identité) ou que vous êtes (empreinte digitale). L'utilisation d'éléments multiples pour l'authentification réduit le risque de piratage.

- Encouragez tout le monde à utiliser une phrase de passe, un ensemble d'au moins trois mots communs aléatoires combinés en une phrase qui offre une très bonne combinaison de mémorisation et de sécurité. Si vous optez pour un mot de passe classique :
  - Il doit être long, comporter des minuscules et des majuscules, éventuellement des chiffres et des caractères spéciaux.
  - Évitez les termes évidents tels que "mot de passe", les séquences de lettres ou de chiffres comme "abc", les nombres comme "123".
  - Évitez d'utiliser des informations personnelles qui peuvent être trouvées en ligne.
- Que vous utilisiez des phrases de passe ou des mots de passe
  - Ne les réutilisez pas ailleurs.
  - Ne les partagez pas avec vos collègues.
  - Activer l'authentification multifactorielle. Il existe un grand nombre d'outils d'authentification multifactorielle. Il est préférable de choisir un outil d'authentification multifactorielle qui offre une variété d'options d'authentification.

    L'AMF est de la plus haute importance pour les systèmes orientés vers l'internet, comme par exemple l'accès à distance. L'accès à distance peut être réalisé par le biais, par exemple, d'un VPN (réseau privé virtuel) ou d'un RDP (protocole de bureau à distance).
  - Modifiez votre mot de passe dès que vous soupçonnez qu'il a été compromis.

2 INSTALLER IMMÉDIATEMENT TOUTES LES MISES À JOUR DE SÉCURITÉ

Mettez en œuvre les mises à jour/patchs de sécurité pour tous vos logiciels dès qu'ils sont disponibles.

Orientations

- Alors que les développeurs se battent avec les cybercriminels pour rendre leurs logiciels plus sûrs et moins vulnérables aux dernières attaques, l'application de correctifs le plus tôt possible est la clé d'une plus grande cybersécurité.
- Envisagez les mesures suivantes :
  - Limitez-vous à l'installation des applications (systèmes d'exploitation, microprogrammes ou plugins) dont vous avez besoin pour faire fonctionner votre organisation.
  - N'installez que les versions des logiciels que vous souhaitez utiliser et qui sont prises en charge par le fournisseur.
  - Automatisez autant que possible le processus de mise à jour en définissant les mises à jour automatiques comme paramètre par défaut sur les systèmes d'exploitation de vos terminaux.
  - Il existe des produits qui peuvent analyser votre système et vous avertir lorsqu'une mise à jour est disponible pour une application que vous avez installée. Si vous utilisez l'un de ces produits, assurez-vous qu'il vérifie les mises à jour pour chaque application que vous utilisez. Si vous n'utilisez pas ces produits, désignez un jour par mois pour vérifier la disponibilité de nouveaux correctifs et les installer.

3 INSTALLER UN ANTIVIRUS

Mettez en œuvre une solution antivirus sur tous les types d'appareils et maintenez-la à jour afin de garantir son efficacité continue.

Orientations

Même avec les meilleures précautions, vous pouvez être confronté à l'intrusion d'un virus ou d'un logiciel malveillant. Un logiciel anti-malware est une deuxième barrière qui vous protège de l'impact des cyber-incidents.

- Le logiciel anti-malware choisi doit protéger contre tous les types de logiciels malveillants tels que les virus, les logiciels espions, les logiciels publicitaires et les rootkits.
- Il est recommandé de configurer le logiciel anti-programmes malveillants pour qu'il vérifie automatiquement les mises à jour au moins une fois par jour (ou lorsqu'elles sont disponibles en "temps réel"), puis d'exécuter rapidement une analyse complète. Lorsque plusieurs appareils sont utilisés (ordinateurs personnels, ordinateurs portables, tablettes...), il convient d'installer et de mettre à jour le logiciel anti-malware sur tous ces appareils.
- À titre préventif, les règles suivantes doivent être appliquées :
  - Ne partagez pas de clés USB ou de disques durs externes entre vos ordinateurs ou appareils personnels et professionnels.
  - Ne connectez aucun matériel inconnu / non fiable à votre système ou réseau et n'insérez aucune clé USB externe inconnue. Ces dispositifs peuvent contenir des logiciels malveillants. Désactivez la fonction AutoRun pour les lecteurs portables (USB, optiques...) sur vos ordinateurs professionnels afin d'éviter que de tels programmes malveillants ne s'installent sur vos systèmes.
  - N'installez pas de logiciels piratés car ils peuvent contenir des logiciels malveillants.

4 SÉCURISEZ VOTRE RÉSEAU

Protégez votre réseau en installant un pare-feu.

Protéger les données sur le réseau auquel on accède par WiFi en utilisant des normes de cryptage sans fil.

Accordez une attention particulière à la sécurité de l'accès à distance .

Orientations

- Ne communiquez à personne vos mots de passe WIFI.
- Si nécessaire, séparez le réseau WIFI de vos invités/visiteurs de votre réseau professionnel.
- Des pare-feu doivent être installés et configurés entre votre réseau interne et l'internet. Il peut s'agir d'un point d'accès/routeur (sans fil) ou d'un routeur fourni par le fournisseur d'accès à Internet (FAI). Les pare-feu doivent être activés et mis à jour. Vous pouvez consulter le catalogue de services de votre FAI sur les services de sécurité du réseau fournis.
  - Veillez à ce que le mot de passe administratif de votre pare-feu soit modifié lors de l'installation et régulièrement par la suite. Pensez également à modifier le mot de passe de l'administrateur
  - Le cryptage rend vos informations stockées électroniquement illisibles pour toute personne ne disposant pas du mot de passe ou de la clé correcte. Réglez votre routeur pour qu'il utilise au moins WiFi Protected Access (WPA-2 ou WPA-3 si possible), avec l'Advanced Encryption Standard (AES) pour le cryptage.

5 SAUVEGARDEZ VOS DONNÉES

Effectuez régulièrement des sauvegardes automatisées de vos informations.
Mettez une copie de sauvegarde HORS LIGNE (non connectée au réseau) toutes les semaines ou toutes les deux semaines.
Après les changements majeurs, sauvegardez vos systèmes afin de pouvoir les restaurer plus facilement.

Orientations
Pensez à l'importance que vous accordez aux données critiques de votre organisation. Créer et tester des copies de sauvegarde vous permettra de restaurer vos données et vos systèmes TIC (Technologies de l'Information et de Communication) en cas d'incident majeur de cybersécurité (par exemple, une attaque par ransomware).
Quelques lignes directrices de base à prendre en compte :

- Identifiez les données que vous devez sauvegarder. Il s'agit des données/informations essentielles sans lesquelles votre organisation ne pourrait pas fonctionner.
- Déterminez la fréquence des sauvegardes en fonction de la quantité de données (mises à jour ou créées) qui seront perdues ou qui devront être réintroduites après une panne.
- Séparez les supports de sauvegarde de vos autres systèmes de stockage. Une sauvegarde hors ligne est très importante pour limiter la possibilité que votre sauvegarde soit également cryptée ou effacée en cas de piratage.
- Tester la restauration des données à intervalles réguliers. Il s'agit également d'un contrôle de base qui permet de vérifier si la procédure de sauvegarde fonctionne correctement.

6 DROITS D'ADMINISTRATION

Veillez à ce que personne ne dispose de privilèges d'administrateur pour les tâches quotidiennes.

Orientations
Un administrateur dispose d'un grand nombre d'accès à votre système. Il est très important de protéger ces comptes, car ils ont une grande valeur pour les cybercriminels. Prenez en compte les principes suivants pour protéger ces comptes :

- Séparez les comptes d'administrateur des comptes d'utilisateur. Pour le travail quotidien, un compte d'utilisateur sans privilèges d'administrateur suffit.
- Exiger l'authentification multifactorielle pour tous les accès via les comptes d'administrateurs.

7 RECOMMANDATIONS FINALES

Protégez physiquement vos ordinateurs et appareils mobiles contre le vol ou l'utilisation incorrecte.

Restreindre l'accès aux locaux, aux sauvegardes, aux serveurs et aux composants du réseau aux seules personnes autorisées.

Savoir comment et qui contacter en cas de cyber-incident.

Orientations

- Sécurité physique et restriction d'accès :
  - La sécurité physique est la protection du personnel, du matériel, des logiciels, des réseaux et des données contre les actions et les événements physiques qui pourraient causer des pertes ou des dommages graves à votre organisation.
  - Il existe des systèmes de gestion des appareils mobiles à un prix abordable qui peuvent être une option si vous utilisez beaucoup d'appareils mobiles. L'activation d'applications telles que "Find My Phone" sur vos téléphones portables peut constituer une première étape.
  - Gérer strictement les clés d'accès aux locaux et les codes d'alarme.
- En cas d'incident :
  - Conservez une copie hors ligne (disque dur hors ligne ou ordinateur portable, copie papier, ...) de tout document dont vous pourriez avoir besoin lors d'un incident ou d'une crise de cybersécurité en répondant aux questions suivantes :
    - Qui dois-je contacter en cas de cyberincident ?
    - De quelles informations ai-je besoin pour les contacter ?
    - Quelles informations demanderont-ils ?
  - Consultez également nos recommandations dans le guide CCB Cyber Security Incident Management, qui propose une approche pragmatique de la gestion des incidents de cybersécurité et peut servir d'inspiration pour votre propre plan d'intervention en cas d'incident ou votre cahier des charges.

Avis de non-responsabilité

Le présent document et ses annexes ont été élaborés par le Centre pour la cybersécurité en 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 français. Ces informations concernent la sécurité des réseaux et des systèmes d'information s'adresse aux services informatiques et peuvent utiliser des termes anglais du langage informatique. Une traduction en anglais, néerlandais et allemand de ces informations techniques sont également rendu accessible par le CCB.

Le CCB **n'**accepte **aucune 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.

Rédacteur responsable

Centre pour la Cybersécurité de Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 18
1000 Bruxelles

Dépôt légal

D/2023/14828/001