08 juin 2023 -08:00

Le Centre pour la cybersécurité en Belgique met en garde : Prenez dès maintenant la mesure la plus importante contre les cyberattaques. Installez l'authentification en deux étapes (2FA) sur toutes les connexions externes

Empêchez les pirates informatiques d'entrer !

Le Centre pour la Cybersécurité Belgique (CCB) conseille à toutes les entreprises et organisations de notre pays d'activer au plus vite l'authentification à deux facteurs. Cette mesure est généralement simple et peu onéreuse à mettre en œuvre. Un petit effort de la part de l'organisation et des collaborateurs qui peut faire une grande différence pour votre cybersécurité.

Chaque jour dans notre pays, au moins une entreprise est victime d'une attaque de type ransomware ou de chantage à la suite d'un vol d'informations sensibles. Au cours du premier trimestre 2023, 27 organisations nous ont déjà signalé des attaques de ransomware. Régulièrement, des hôpitaux et d'autres établissements de soins de santé sont victimes d'attaques qui ont des conséquences majeures sur les soins aux patients. Six mois après la cyberattaque dont a été victime la ville d'Anvers, les dégâts n'ont toujours pas été entièrement réparés.

> "L'impact d'une cyberattaque est souvent considérable. L'entreprise victime ne peut plus assurer son fonctionnement quotidien, elle perd des informations cruciales, subit une atteinte importante à sa réputation et voit ses coûts augmenter rapidement."
>
> Miguel De Bruycker
> Directeur général, Centre pour la Cybersécurité Belgique

Nous ne sommes pas sans défense contre les ransomwares : installez l'authentification en deux facteurs dès aujourd'hui

Aucun secteur n'est épargné, mais les attaques par ransomware peuvent souvent être évitées. Notre enquête sur ces incidents montre que les cybercriminels utilisent souvent des identifiants de connexion volés pour lancer leur attaque. Ces identifiants de connexion sont bien souvent subtilisés au moyen de

messages de phishing ou de virus informatiques dérobant les mots de passe dans le navigateur.

Une grande partie de ces cyberattaques peut être évitée en ayant recours à l'authentification à deux facteurs (2FA) ou multifacteur (« multifactor authentication », MFA) pour toutes les connexions à distance de l'entreprise. Cette technique repose sur l'utilisation d'au minimum un deuxième facteur au moment des connexions à distance des collaborateurs au réseau de l'entreprise ou à leur boîte mail professionnelle: par exemple, un mot de passe et un code généré sur smartphone. Pour l'accès à distance, veillez ainsi à toujours utiliser une combinaison d'au moins deux éléments parmi une donnée que vous connaissez (un mot de passe, par exemple), qui vous caractérise (la reconnaissance faciale, par exemple) ou que vous possédez (un smartphone/numéro de téléphone, par exemple).

Primordiale et pas compliquée

L'authentification à deux facteurs ou MFA doit être une première étape sur la voie d'un environnement plus sûr, suivie par d'autres mesures comme les mises à jour de sécurité rapides et les back-ups hors ligne réguliers. Mais attelez-vous dès aujourd'hui à la première étape.

Comment implémenter MFA?

Ensemble, luttons contre la cybercriminalité!

Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Michele Rignanese
Porte-parole(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

Katrien Eggers
Porte-parole(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be