CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

Bruxelles, le 07/06/2023

Madame, Monsieur,

Prenez dès maintenant la mesure la plus importante contre les cyberattaques : installer l'authentification à deux facteurs (2FA) pour toutes les connexions externes

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. L'examen de ces incidents révèle que les cybercriminels utilisent souvent des données de connexion volées pour commettre 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.

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.

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat, 18 – Brussels

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

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).

Pour savoir comment mettre en œuvre la MFA, consultez le site Internet du CCB : https://www.cert.be/fr/paper/mieux-proteger-les-comptes-grace-lauthentification-multifacteur

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.

Ensemble, luttons contre la cybercriminalité!

Je vous prie d'agréer, Madame, Monsieur, l'expression de ma considération distingué.

Miguel De Bruycker

Digitally signed by Miguel De Bruycker
Date: 2023.06.08 19:57:36 +02'00'

Miguel DE BRUYCKER
Directeur Général CCB

CENTRE FOR
CYBER SECURITY BELGIUM
Wetstraat, 18 – Brussels

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