Sécurisez le site web de votre entreprise

Département de Communication et de Transformation Numérique

Les sites web non sécurisés sont vulnérables aux attaques. Protégez les informations relatives à votre entreprise et à vos clients en suivant les étapes de la liste de contrôle ci-dessous.

DES ÉTAPES POUR TRAVAILLER PAR SOI-MÊME:

- ☐ **Créez un mot de passe de connexion long et solide** pour votre site web, différent de ceux utilisés pour d'autres services. Nous recommandons une phrase de passe de quatre mots ou plus.
- ☐ **Activez l'authentification à deux facteurs (2FA)** 2FA vérifie que vous êtes bien la personne que vous dites être, en vous demandant une deuxième information (souvent un code) ainsi que votre mot de passe. Cela ajoute une couche de sécurité supplémentaire.
- ☐ **Maintenez votre logiciel à jour** Cela inclut votre système de gestion de contenu (SGC), les plugins ou modules externes que vous utilisez, et d'autres éléments tels que votre serveur web.
- ☐ **Sauvegardez régulièrement les données de votre entreprise** Faites-en sorte que les sauvegardes se fassent automatiquement et stockez-les dans un endroit sûr, mais facile d'accès, comme un tiroir ou une armoire verrouillée, de préférence hors site. Grâce aux sauvegardes, vous pouvez restaurer vos données rapidement et facilement en cas de perte, de fuite ou de vol.
- ☐ **Créez un plan d'intervention** pour vous guider en cas de problème. Ce plan doit comprendre les coordonnées de vos responsables informatiques et de communication. Un tel plan vous aidera à minimiser l'impact d'un incident et à vous remettre rapidement sur pied.
- ☐ **Signalez les incidents de cybersécurité à CERT VU** Ils peuvent vous conseiller sur les prochaines étapes. Les informations que vous fournissez seront également utiles pour créer des conseils préventifs pour les autres.

ÉTAPES À FRANCHIR AVEC VOTRE FOURNISSEUR INFORMATIQUE:

- ☐ **Activez le HTTPS sur toutes les pages**, y compris sur votre SGC, où vous apportez des modifications à votre site web.
- ☐ **Configuré pour recevoir des alertes** lorsque quelqu'un apporte des modifications au site web ou au SGC.
- ☐ **Vérifiez régulièrement votre SGC**, pour vous assurer que les 2FA et les alertes sont toujours correctement configurées.
- ☐ **Suivez les meilleures pratiques en matière de cybersécurité** lorsque vous apportez des modifications à votre site web. Assurez-vous que le développeur de votre site web ou le support informatique respecte les techniques de cybersécurité décrites dans l'OWASP.
- ☐ **Vérifiez que vous avez toujours besoin de tous les plugins installés sur votre site web.** Si vous n'en avez plus besoin, supprimez-les - ils font de votre site web une cible plus facile pour les attaquants.
- ☐ **Obtenir la conformité à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).** La norme PCI DSS permet de garantir que les transactions en ligne sont sûres et sécurisées, et que les données des cartes des clients sont protégées contre les attaques. Votre banque exige que votre site de commerce en ligne soit conforme à la norme PCI DSS, alors parlez-leur de ce que cela implique.

Il vous est fortement conseillé de ne pas traiter vous-même les paiements en ligne. Utilisez un fournisseur de passerelle de paiement tiers qui est déjà conforme à la norme PCI DSS.

Pour en savoir plus, consultez:
https://cert.gov.vu/

2020_VU_VUF