PRÉSIDENCE DE LA RÉPUBLIQUE DU SÉNÉGAL

DCSSI

RECOMMANDATIONS DE SÉCURITÉ POUR LA PROTECTION DES SITES WEB

I. LOGICIELS ET PLUGINS À JOUR

- Consulter le site web pour les mises à jour ou ajouter un plug-in de notification de mise à jour
- Autoriser les mises à jour automatiques

II. AJOUTER HTTPS & CERTIFICAT SSL

III. MOT DE PASSE

- Créer un mot de passe unique pour chaque nouvelle demande de connexion
- Choisir des mots de passe compliqués et aléatoires
- Eviter d'utiliser des informations personnelles dans le mot de passe
- Ne pas utiliser votre date d'anniversaire ou le nom de votre animal de compagnie
- S'assurer que tous les agents changent fréquemment leur mot de passe

IV. UTILISER UN HEBERGEUR SÉCURISÉ

V. ENREGISTRER L'ACCÈS DES UTILISATEURS ET LES PRIVILÈGES ADMINISTRATIFS

VI. MODIFIER LES PARAMÈTRES PAR DÉFAUT DE VOTRE CMS

- Personnaliser les utilisateurs et leurs paramètres d'autorisation
- Ne pas conserver les paramètres par défaut tels quels

VII. SAUVEGARDER LE SITE WEB

- Conserver les informations du site Web hors site;
- Ne pas stocker les sauvegardes sur le même serveur que le site web; Ils sont aussi vulnérables aux attaques;
- Choisir de conserver la sauvegarde du site Web sur un ordinateur personnel ou un disque dur;
- Trouver un endroit hors site pour stocker les données et les protéger contre les pannes matérielles, les piratages et les virus
- Sauvegarder la sauvegarde pour garantir la redondance.

VIII. CONNAITRE LES FICHIERS DE CONFIGURATION DU SERVEUR WEB

- Se renseigner sur le type de fichiers utilisés avec chaque serveur
- Utilisez un scanner de site Web pour vérifier le site Web et rechercher les logiciels malveillants connus, les virus, l'état de la liste noire, les erreurs de site Web, etc.

IX. UTILISER UN PARE-FEU D'APPLICATION WEB

X. RENFORCER LA SÉCURITÉ DU RESEAU

- Faire en sorte que les connexions à l'ordinateur expirent après une courte période d'inactivité (5mn)
- S'assurer que le système informe les utilisateurs tous les (3) trois mois des changements de mots de passe
- S'assurer que tous les appareils connectés au réseau sont analysés à la recherche de logiciels malveillants chaque fois qu'ils sont connectés