RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

ADOPTER LES BONNES PRATIQUES

LA SÉCURISATION DES SITES INTERNET

Vitrine promotionnelle des organisations (entreprises, collectivités, associations…), voire élément clé de leur activité, les sites Internet ou « sites Web » sont des éléments très exposés de leur système d'information. Ils peuvent être la cible de nombreuses attaques comme les défigurations, les dénis de service, ou même le vol des données personnelles ou bancaires des internautes s'étant créé un compte sur le site… Ces attaques peuvent entraîner de graves préjudices pour l'organisation qui en est victime : atteinte à l'image et à la réputation, pertes directes de revenus, etc. Que l'hébergement du site et son administration soient internalisés ou externalisés, il est essentiel de les sécuriser au mieux pour réduire les risques de piratage. **Voici 10 bonnes pratiques à adopter ou faire appliquer par son prestataire pour assurer la sécurité de votre site Internet.**

1 SÉCURISEZ LE SERVEUR HÉBERGEANT VOTRE SITE

Protégez votre serveur en adoptant une stratégie de « défense en profondeur » qui vise à mettre en œuvre plusieurs mesures de protection indépendantes au niveau de l'architecture matérielle et logicielle du serveur et de son infrastructure d'hébergement. Par exemple, mettez en place et installez des solutions de sécurité (antivirus, pare-feu, serveur mandataire inverse, solution anti-DDoS…) pour pouvoir faire face aux principales menaces. Si votre hébergement est externalisé, assurez-vous des moyens mis en œuvre par votre prestataire pour protéger votre site.

2 CONFIGUREZ ET SÉCURISEZ VOTRE SERVEUR POUR VOTRE JUSTE BESOIN

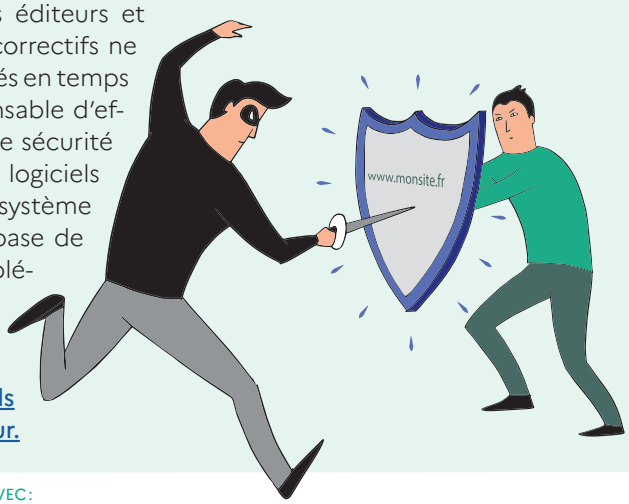
Configurez et sécurisez votre serveur en fonction des seuls services indispensables à votre activité, en partant du principe que tout ce qui n'a pas besoin d'être autorisé doit être interdit pour éviter les points d'accès superflus et potentiellement dangereux. Sécurisez sa configuration en instaurant des règles comme le filtrage d'adresses IP ou de requêtes autorisées d'administration, l'interdiction de certains formats de fichiers à risque si vous n'en avez pas l'utilité… Réduisez au maximum les informations délivrées par les services ainsi que dans le code source de votre site Internet et bloquez la navigation dans vos dossiers afin d'empêcher l'affichage du contenu des répertoires de votre site. Enfin, désactivez et/ou limitez les services et fonctionnalités non utilisés pour réduire les risques inutiles de piratage.

3 METTEZ À JOUR SANS TARDER LES ÉQUIPEMENTS ET LES LOGICIELS DE VOTRE SITE

La grande majorité des attaques de sites Internet est rendue possible par l'exploitation de failles de sécurité par les cybercriminels pour en prendre le contrôle. Ces failles sont régulièrement corrigées par les éditeurs et constructeurs, mais ces correctifs ne sont pas toujours appliqués en temps utile. Il est donc indispensable d'effectuer les mises à jour de sécurité des équipements et des logiciels (système d'exploitation, système de gestion de contenu, base de données, modules complémentaires, extensions…) de votre site Internet dès qu'elles sont disponibles. Tous nos conseils pour gérer vos mises à jour.

4 UTILISEZ DES MOTS DE PASSE ROBUSTES ET DIFFÉRENTS POUR CHAQUE SERVICE

Pour réduire les risques de piratage et sécuriser au mieux vos comptes privilégiés, notamment les comptes d'administrateurs de votre site Internet, utilisez des mots de passe suffisamment longs, complexes et différents pour chaque service. Imposez également l'utilisation d'un mot de passe solide aux utilisateurs disposant de droits sur le site Internet et veillez à leur renouvellement régulier ou à la moindre suspicion de divulgation. Si possible, activez la double authentification. Tous nos conseils pour gérer vos mots de passe.



EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

5 RÉALISEZ DES SAUVEGARDES RÉGULIÈRES DE VOTRE SITE

En cas de panne, de piratage ou de destruction de vos équipements, vous pouvez perdre les données enregistrées sur ces supports. Aussi, effectuez des sauvegardes régulières de votre site web, de sa configuration et de ses bases de données, et testez sa restauration pour vous assurer de son bon fonctionnement. En cas de besoin, vous pourrez ainsi restaurer votre site Internet à une date antérieure à l'incident. Veillez à déconnecter votre support de sauvegarde après utilisation pour qu'il ne soit pas exposé à une attaque. Tous nos conseils pour gérer vos sauvegardes.

6 SÉCURISEZ LES COMMUNICATIONS DE VOTRE SITE INTERNET

Utilisez le protocole HTTPS qui assure le chiffrement d'informations entre l'ordinateur de l'internaute et votre site Internet. Afin d'éviter que des cybercriminels n'interceptent les données qui transitent, comme les données de connexion, les témoins de connexion (cookies), les informations bancaires, etc.

7 LIMITEZ LES UTILISATEURS PRIVILÉGIÉS

Pour réduire les risques liés à un piratage de compte, il convient d'appliquer le principe de « moindre privilège » en limitant le nombre d'utilisateurs ayant accès aux outils et fonctionnalités d'administration du site Internet ainsi que leurs privilèges et droits d'accès. Définissez des rôles d'utilisateurs et leurs périmètres pour que chaque utilisateur dispose uniquement des droits d'accès nécessaires à l'accomplissement de ses tâches. Privilégiez des comptes utilisateurs individuels à des comptes génériques ou fonctionnels, en particulier pour les utilisateurs privilégiés (administrateurs), sous peine d'augmenter les risques de compromission en cas de divulgation de leurs mots de passe.

8 PROTÉGEZ VOTRE NOM DE DOMAINE

Il est important de protéger le nom de domaine de son site (ex: monnomdedomaine.fr) pour éviter qu'il ne soit utilisé frauduleusement. Enregistrez votre nom de domaine auprès de l'INPI en complément de sa réservation auprès d'un bureau d'enregistrement. Mettez en place et adoptez une politique de gestion de votre nom de domaine pour le sécuriser. Par ailleurs, utilisez des solutions comme le verrou de registre (.FR Lock pour un domaine en .fr) et DNSSEC pour réduire les risques de piratage. Enfin, il faut savoir qu'un nom de domaine s'enregistre pour une période déterminée (1 à 10 ans). Veillez donc à renouveler à temps cet enregistrement au risque de voir votre nom de domaine libéré et réutilisé par un tiers malveillant.

9 SOYEZ VIGILANT SI VOUS UTILISEZ DES EXTENSIONS

Les systèmes de gestion de contenu (ou CMS en anglais), comme WordPress ou Joomla!, proposent de leur ajouter des extensions pour compléter leurs fonctionnalités. Ces extensions peuvent constituer une brèche dans la sécurité de votre site Internet si elles sont obsolètes, non mises à jour ou insuffisamment sécurisées. Aussi, avant utilisation d'une extension, vérifiez sa notoriété ainsi que sa date de dernière mise à jour qui, si elle remonte à plusieurs années, indique que l'extension n'est plus maintenue par son développeur. En outre, ne téléchargez vos extensions qu'auprès du site officiel de l'éditeur de votre CMS.

FAITES AUDITER RÉGULIÈREMENT LA SÉCURITÉ DE VOTRE SITE

Afin d'être assuré que les mesures de sécurité sont bien appliquées et qu'aucune faille de sécurité connue ne pourrait mettre en danger votre site Internet, faites-en réaliser un audit de sécurité régulièrement par des prestataires spécialisés.

10 SURVEILLEZ L'ACTIVITÉ DE VOTRE SITE INTERNET AU QUOTIDIEN

Surveillez régulièrement l'activité de votre site Internet, notamment celle de votre système de gestion de contenu (mise à jour d'articles, connexion au portail d'administration du site Internet, dépôt de fichiers...) pour y détecter une activité inhabituelle ou illicite et pouvoir ainsi prendre à temps les mesures nécessaires pour en limiter les effets.

POUR ALLER PLUS LOIN

- **Par l'ANSSI :** Recommandations pour la sécurisation des sites web
- **Par l'AFNIC :** Guide pratique du titulaire d'un nom de domaine .FR

DOCUMENT RÉALISÉ AVEC NOTRE MEMBRE : afnic

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 10