La sécurité de votre site web

Pour développer vos parts de marché, vous avez décidé de créer un site vitrine ou de e-commerce. L'ergonomie des pages web et la gestion des stocks sont indispensables pour satisfaire vos clients. Mais leur fonctionnement optimal pourrait être menacé si vous avez négligé la sécurité informatique.

Quelle que soit la solution retenue (site vitrine ou de e-commerce), il est primordial de renforcer la protection de votre site contre diverses menaces numériques. Or, beaucoup de sites web professionnels présentent d'importantes vulnérabilités. En auditant le niveau de sécurité de ses clients français entre juin 2016 et juin 2017, Wavestone, un cabinet spécialisé dans la transformation digitale des entreprises, a constaté que la moitié des sites était affectée par « au moins une faille grave ». Une faille « grave » permet d'accéder à l'ensemble du contenu du site et/ou de compromettre les serveurs. Profiter d'une faiblesse de sécurité sur un site c'est comme si un cambrioleur passait par une fenêtre laissée ouverte.

Quels sont les risques ?

- **Première menace : la prise de contrôle de votre site**
  En accédant aux coulisses de votre boutique en ligne ou de votre site vitrine, une personne malhonnête peut devenir administrateur à votre place. Elle peut alors tout faire : télécharger votre fichier clients et leurs identifiants, récupérer des informations sur vos pratiques commerciales, supprimer des plug-in (ou extensions en français) permettant de gérer les paniers, la facturation, les mailings…
- **Deuxième menace : l'atteinte à votre réputation**
  Mal sécurisé, votre site peut présenter une faille qui pourrait permettre à une personne malveillante de « défigurer » votre page d'accueil en remplaçant les photos de vos produits par des images osées ou des messages illicites (racistes, injurieux…). Visible par tout le monde, cet acte porte directement atteinte à votre notoriété et à votre crédibilité vis-à-vis de vos clients, mais aussi de vos partenaires et actionnaires.
- **Troisième menace : l'indisponibilité de votre site**
  Pas assez bien protégé, votre site peut être victime d'une **attaque DoS** (Denial of Service attack ou attaque par déni de service). Après avoir pris le contrôle de milliers d'ordinateurs à l'insu de leur propriétaire, un pirate peut les configurer de façon à ce qu'ils se connectent en même temps à votre site. Croulant sous les requêtes simultanées, ce dernier devient en quelques secondes inaccessible pour tous les internautes. C'est comme un compteur électrique qui « disjoncte » à cause d'une trop forte demande.
- **Quatrième menace : l'usurpation d'identité numérique**
  Cet acte malveillant est appelé **« Cybersquat »**. Il consiste à déposer un nom de domaine en usurpant le nom de votre PME ou de vos marques en modifiant quelques lettres. Par exemple elyseee.fr. Les noms de domaine ne coûtant pas très chers, pensez à réserver (et à renouveler chaque année) des variantes en .fr et .com.

La sécurité du site web : les mesures élémentaires à mettre en place

- **Installer toutes les mises à jour**
  Comme pour un ordinateur, vous devez **mettre à jour toutes les extensions installées sur votre site et la version de son CMS.** Un « Content Management System » est une solution « packagée » permettant de créer un site et d'y ajouter des pages web et des rubriques. Les CMS les plus connus sont Drupal, Wordpress et Magento. Ces mises à jour limitent ainsi les vulnérabilités.
- **Limiter les accès**
  Assurez-vous que les rubriques et les fichiers de votre site ne sont accessibles qu'aux seules **personnes habilitées.** Veillez aussi à ce qu'elles ne donnent pas leurs identifiants et mots de passe à n'importe qui.

- **Bloquer les tentatives malveillantes**
  Un **« captcha »** est un terme étrange, mais sa fonction est pratique. Lorsqu'une personne veut se connecter à votre site (en tant qu'utilisateur ou client), elle doit taper son identifiant et mot de passe, mais également **répondre à la petite question qui apparaît.** C'est un captcha, acronyme de « Completely Automated Public Turing test to Tell Computers and Humans Apart » ou « Test public de Turing complètement automatique ayant pour but de différencier les humains des ordinateurs »). Cette question peut par exemple demander de cliquer sur tous les carrés représentant un bus dans une image quadrillée. Cette technique permet de bloquer les logiciels-robots incapables de répondre à ce type de requête. C'est une parade efficace contre les tentatives répétées qui pourraient empêcher l'accès à votre site comme une attaque DoS (vérifiez d'ailleurs que votre hébergeur propose bien cette protection).

Ce qu'il ne faut pas faire

- **Utiliser des mots de passe « faibles »**
  L'étude de Wavestone montre que dans **45 % des cas les mécanismes d'authentification ne sont pas suffisamment robustes.** Les mots de passe n'étaient pas assez complexes (avec minimum 8 caractères et comprenant majuscules, minuscules et caractères spéciaux) et les tentatives d'accès à répétition n'étaient pas bloquées.

- **Ne jamais sauvegarder son site**
  Même si votre site est hébergé chez un prestataire informatique ou un fournisseur dans le Cloud, **faites chaque semaine une sauvegarde locale.** Cette précaution permet d'avoir toujours une copie exacte de son site et de l'intégralité de son contenu.

ANNEXE

Lexique : le HTTPS

Le **HTTP** (Hyper Text Transfert Protocol) est un protocole permettant de se connecter à un site web. Le HTTPS (le petit cadenas affiché dans le navigateur web) joue le rôle d'un fourgon blindé : il assure la sécurité du transport des billets

Rapporté à Internet, le **HTTPS protège l'intégrité ainsi que la confidentialité des flux** entre le PC du client et votre site. Ces flux sont sécurisés via le protocole Transport Layer Security (TLS), qui intègre trois niveaux clés :

- **le chiffrement** des échanges (les flux sont codés) ;
- **l'intégrité** des données (elles ne peuvent être ni modifiées, ni corrompues durant leur transfert) ;
- **l'authentification** (les internautes communiquent avec le bon site Web).

Pour inciter les entreprises à migrer leur site vers le HTTPS, Google a décidé de référencer en priorité ces sites. Si vous souhaitez être vu par de nombreuses personnes, voici donc un argument supplémentaire.

Vous souhaitez vous prémunir contre toute cyberattaque ? consultez l'offre Generali Protection Numérique
https://www.generali.fr/professionnel/assurance-cyber-risques/

Generali IARD, Société anonyme au capital de 94 630 300 euros. Entreprise régie par le Code des assurances - 552 062 663 RCS Paris. N° d'identifiant unique ADEME FR232327_01NBYI.
Siège social : 89 rue Taitbout - 75009 Paris.
Société appartenant au Groupe Generali immatriculé sur le registre italien des groupes d'assurances sous le numéro 026.

SG2685MARK-25 - Décembre 2025 - Studio graphique