COMMENT SÉCURISER LE SITE WEB DE VOTRE ENTREPRISE

Le site web est la vitrine de votre entreprise. Comment développer un site web attrayant, facile à utiliser et sûr ? Voici un aperçu de tout ce que vous devez prendre en compte.

Une question pour commencer

Afin d'évaluer pourquoi la sécurité du site web est importante et les domaines à privilégier, répondez à la question suivante :

À quelles fins utilisez-vous votre site web ?

Présentation de l'entreprise :

Dans ce cas, un site web sécurisé vous aide principalement à améliorer la crédibilité de la marque. Il crée la première impression des utilisateurs envers la marque. Il peut avoir un effet positif sur la manière dont les clients perçoivent votre activité. Un site web de qualité et protégé empêche également les cybercriminels d'afficher du contenu inapproprié ou malveillant, par exemple sur votre page d'accueil.

Vente de produits et de services :

Les observations tirées du point précédent s'appliquent également au e-commerce. Toutefois dans ce cas, les transactions financières doivent être prises en compte dans l'infrastructure de sécurité du site web. Les solutions de cybersécurité vous aident à assurer la disponibilité de votre boutique en ligne, et protéger les informations des cartes bancaires de vos clients.

> ***Les fuites de données ainsi que les sites web compromis ou dysfonctionnels peuvent nuire à la crédibilité de la marque. La formule est simple : une marque de mauvaise réputation = mauvais résultats commerciaux. Des pirates ont parfois uniquement pour objectif d'empêcher l'accès à un site web, mais dans la plupart des cas, ils tentent de voler les données des clients et éventuellement de les vendre.***
>
> **— Martin Cambal,**
> Global Web Development Manager chez ESET

Checklist de sécurité du site web

Vous pouvez entreprendre plusieurs actions pour veiller au bon fonctionnement de votre site web.

Restez informé·e et favorisez la sensibilisation :

- Configurez des rappels vous invitant à consulter régulièrement le site de l'OWASP qui surveille les menaces en ligne récentes.
- Recherchez votre propre page sur Google pour déterminer comment elle est présentée parmi les résultats de recherche. Les brèches et les vulnérabilités potentielles sont généralement signalées par l'avertissement « Ce site a peut-être été piraté ».
- Rappelez-vous que le nombre de visites que vous voyez, par exemple dans Google Analytics, n'est pas représentatif du trafic sur votre site web.
- Découvrez les guides gratuits de durcissement d'un site web et les checklists de sécurité proposés par Google et d'autres grandes entreprises de technologie. Ils peuvent vous aider à mettre en œuvre un serveur web sécurisé.
- Mettez l'accent sur la formation et l'éducation des collaborateurs aux risques cyber et identifiez les vulnérabilités liées au facteur humain.

Faites confiance à des partenaires authentifiés, mais soyez conscient·e de leurs limites :

- Lorsque vous utilisez un hébergeur, recherchez un prestataire conforme à la norme ISO 27001, qui garantit que vos données seront en sécurité chez lui.
- Utilisez les services de Let's Encrypt, une autorité de certification à but non lucratif, pour vous doter gratuitement d'un certificat SSL valide.
- Tenez compte du fait que le code des plateformes comme WordPress est open source, et que n'importe qui peut le consulter et éventuellement exploiter ses imperfections.
- Si vous utilisez une telle plateforme, veillez à ce que la partie administration ne soit accessible qu'à partir d'adresses IP spécifiques ou d'un VPN.
- Cachez les éléments du système de gestion de contenu (CMS) et modifiez le code source pour que les attaquants ne puissent déterminer le CMS que vous utilisez.
- Mettez en place une couche de protection supplémentaire pour vous connecter à votre CMS, comme l'authentification multifacteur.

Vérifiez l'état de votre site web :

- Gardez une trace du trafic du site web et du réseau à l'aide d'un journal, qui devrait toujours couvrir au moins les 30 derniers jours.
- Surveillez correctement les journaux du serveur et des accès. Une analyse approfondie est généralement plus efficace que la simple recherche d'erreurs dans les applications web que vous avez développées.
- Le logiciel de surveillance devrait contrôler en permanence la disponibilité du site web, au moins chaque minute.
- Si vous gérez un site web à fort trafic, limitez le nombre de pages qui peuvent être consultées à partir d'une même adresse IP.
- Effectuez des mises à jour régulièrement, de préférence une fois par mois. Ne repoussez jamais celles-ci, elles sont indispensables à la cyberhygiène de l'entreprise.
- Vérifiez les en-têtes de sécurité pour savoir si votre page répond aux normes de sécurité de base et avancées.

N'oubliez pas les règles d'hygiène des noms de domaine et de la messagerie :

- Mettez en œuvre un système de validation d'emails (SPF, Sender Policy Framework) pour empêcher les campagnes d'hameçonnage et de spam de se propager sous le nom de votre entreprise.
- Configurez un ensemble d'adresses IP de confiance autorisées à utiliser votre nom de domaine.
- Gérez de manière responsable les enregistrements de votre système de nom de domaine (DNS) ainsi que l'accès à ceux-ci.
- Utilisez un prestataire de services de messagerie externe pour s'occuper des serveurs de messagerie.
- N'envoyez pas d'emails en volume.
- Surveillez l'utilisation de votre nom de domaine.
- Créez des sous-domaines dédiés à différentes fins, par exemple pour les conversations transactionnelles.
- Activez le reporting DMARC pour contrôler l'efficacité de la configuration SPF.

En matière de cybersécurité, mieux vaut prévenir que guérir :

- Sauvegardez les journaux, de préférence sur un stockage central.
- Sauvegardez votre site web et élaborez un plan d'objectif de temps de récupération (RTO) et d'objectif de point de récupération (RPO), ainsi qu'un plan de reprise sur incident.
- Appuyez-vous sur le principe du moindre privilège, et limitez le nombre de règles d'accès.
- N'oubliez pas : dès lors qu'un pirate parvient à s'introduire sur votre site web, vous ne pouvez plus faire confiance à la sécurité de ce dernier. Après avoir résolu la cyberattaque, réinstallez l'ensemble du site web à partir d'une sauvegarde.
- Appuyez-vous sur les principes de sécurité des infrastructures. Implémentez plusieurs systèmes indépendants plutôt qu'un seul système monolithique.

Après avoir vérifié tous ces points, vous aurez fait de votre mieux pour protéger le site web de votre entreprise. Vous recherchez plus d'informations sur chacune de ces étapes ? Découvrez la série d'articles du site web DSG comprenant encore plus de conseils pratiques émis par des professionnels :

- Protéger plutôt que rebrander : ou pourquoi la sécurité de votre site est primordiale
- Le site web de votre entreprise est-il une cible facile pour les pirates ?
- 6 conseils pour sécuriser facilement le site web de votre entreprise
- Comment améliorer la sécurité de votre site web
- Vous utilisez des services d'hébergement web simplifiés ? Découvrez comment assurer la sécurité de votre site web et de votre messagerie professionnelle

À propos d'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique pour protéger le patrimoine numérique des entreprises, les infrastructures critiques et les consommateurs du monde entier contre des cybermenaces. Nous protégeons les terminaux fixes et mobiles, les outils collaboratifs, et assurons la détection et le traitement des incidents. Établis dans le monde entier, nos centres de R&D récoltent et analysent les cybermenaces pour protéger nos clients et notre monde numérique. Pour plus d'informations, consultez le site www.eset.com/fr/ ou suivez-nous sur LinkedIn, Facebook et Twitter.