

Sécuriser son site web d'entreprise

HTTPS, mises à jour, comptes admin, sauvegardes : garder la vitrine de l'entreprise hors d'atteinte.

9 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/securiser-site-web

Un site piraté, c'est une vitrine défigurée, des clients redirigés vers des arnaques, un référencement Google pénalisé et parfois des données clients dérobées. La plupart des piratages de sites exploitent des négligences simples à corriger.

1. Le socle

- HTTPS partout, avec redirection automatique et certificat renouvelé (Let's Encrypt est gratuit)
- CMS, thèmes et extensions à jour — la cause n° 1 des piratages WordPress
- Supprimer les extensions et thèmes inutilisés (désactivé ne veut pas dire inoffensif)
- Sauvegardes automatiques du site et de sa base de données, stockées hors de l'hébergement

2. Les comptes

- Pas de compte « admin » : un identifiant non devinable et un mot de passe fort
- Double authentification sur l'administration du site et sur l'hébergement
- Un compte par intervenant, supprimé quand la mission s'achève
- Le compte du registrar (nom de domaine) est critique : MFA obligatoire — qui contrôle le domaine contrôle emails et site

3. Durcissement et surveillance

- Limiter les tentatives de connexion et masquer la page d'admin si possible
- Pare-feu applicatif (WAF) via l'hébergeur ou un service dédié
- En-têtes de sécurité (CSP, HSTS...) configurés sur le serveur
- Surveillance de disponibilité et alerte en cas de modification anormale

4. Reconnaître un site compromis — et réagir

- Signes visibles : contenu modifié, redirections vers des sites douteux, avertissement « site dangereux » dans Google ou le navigateur
- Signes discrets : pages inconnues dans les résultats Google (spam pharmaceutique, contrefaçons), envois d'emails depuis le serveur, comptes administrateurs inconnus, fichiers récents non expliqués
- Réaction : mettre le site en maintenance, changer tous les mots de passe (admin, hébergement, base de données, FTP), restaurer une sauvegarde saine ANTÉRIEURE à la compromission, puis corriger la faille (extension vulnérable le plus souvent) avant de rouvrir
- Demander la réexamination à Google (Search Console) pour lever l'avertissement — sinon il reste des semaines

ATTENTION

Restaurer la sauvegarde d'hier ne suffit pas si la compromission date du mois dernier : vous restaurez la porte dérobée avec. Il faut identifier la date et le vecteur d'entrée — c'est là qu'un professionnel fait gagner des jours — puis restaurer en amont et colmater. D'où l'importance de sauvegardes avec un historique profond (30 jours et plus).

L'essentiel à retenir

- 01 Forcer le HTTPS avec un certificat valide et auto-renouvelé
- 02 Mettre à jour CMS et extensions chaque mois
- 03 Activer la MFA sur l'admin du site, l'hébergement et le registrar
- 04 Automatiser des sauvegardes stockées hors de l'hébergement, historique 30 jours
- 05 Supprimer extensions inutilisées et comptes obsolètes
- 06 Surveiller le site : disponibilité, résultats Google, Search Console

Questions fréquentes

Notre site est un simple site vitrine sans données clients. Que risque-t-on vraiment ?

Trois choses : votre image (défiguration, redirections douteuses vues par vos prospects), votre référencement (Google blackliste les sites compromis — des mois à s'en remettre), et votre infrastructure (le serveur piraté sert de relais pour attaquer d'autres cibles ou héberger du phishing, ce qui engage votre responsabilité). Le site « sans valeur » a donc bien une valeur — pour l'attaquant.

WordPress est-il dangereux ?

WordPress lui-même est bien maintenu ; le danger vient de son écosystème : des dizaines de milliers d'extensions de qualité inégale. Un WordPress à jour avec peu d'extensions, toutes maintenues et à jour, plus MFA et sauvegardes, est un site raisonnable. Un WordPress avec 40 extensions dont la moitié abandonnées est une compromission en attente — quel que soit le CMS d'ailleurs.

Qui est responsable de la sécurité : nous, l'agence web ou l'hébergeur ?

L'hébergeur sécurise le serveur (selon l'offre) ; l'agence livre un site sain ; mais la maintenance dans la durée — mises à jour, sauvegardes, surveillance — doit être explicitement attribuée par contrat, sinon personne ne la fait. Le contrat de maintenance annuel (quelques dizaines d'euros par mois) est le plus souvent la réponse pragmatique.

Le certificat HTTPS suffit-il à dire qu'un site est « sécurisé » ?

Non — le cadenas garantit seulement le chiffrement de la connexion, pas l'honnêteté ni la sécurité du site : les sites de phishing ont presque tous un cadenas aujourd'hui. Le HTTPS est indispensable mais c'est le plancher, pas le plafond : la sécurité du site se joue dans les mises à jour, les comptes et les sauvegardes.

Pour aller plus loin

Cybermalveillance.gouv.fr — piratage de site Internet — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/piratage-site-internet-defiguration

Google Search Console — état de sécurité de votre site — search.google.com/search-console

Un projet cloud ou d'infrastructure ?

Choix, migration, sécurisation, supervision : Cyberionis conçoit des infrastructures sobres et qui durent.
contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr