Sécurité, Wordpress

Cyberattaque sur un site WordPress Que faire dans les premières heures ?

Un site WordPress piraté exige des décisions rapides mais méthodiques : isoler, préserver les preuves, sécuriser les accès, identifier la porte d'entrée, restaurer proprement et surveiller la réinfection. Repères pratiques pour dirigeants de PME.

Publié le 27 mai 2026

Ce document reproduit le contenu publié à l'adresse indiquée en pied de page, dans sa version disponible à la date de sa génération. Il est fourni à titre exclusivement informatif et ne constitue ni un conseil juridique, réglementaire, fiscal ou professionnel, ni une garantie d'exhaustivité, d'exactitude ou d'actualité. Les textes officiels et la situation propre du lecteur doivent être vérifiés avant toute décision. Dans les limites permises par la loi applicable, Nasteo n'assume aucune responsabilité au titre des décisions prises ou des conséquences résultant de l'utilisation de ce document.

Ce qu'il faut retenir de ce dossier

Une cyberattaque sur un site WordPress peut prendre plusieurs formes : redirections malveillantes, spam SEO, compte administrateur inconnu, fichiers PHP suspects, pages injectées, formulaire détourné, malware, backdoor ou blocage complet du site. La première erreur consiste à supprimer trop vite les traces ou à restaurer sans comprendre la cause.

Dans les premières heures, les priorités sont simples : limiter l'exposition, préserver les preuves, sécuriser les accès, identifier la porte d'entrée, puis seulement restaurer et surveiller. WordPress rappelle que la sécurité vise la réduction du risque, pas son élimination complète, et insiste sur les sauvegardes, la limitation des accès, les mises à jour, les journaux et la surveillance.

Pour une PME, l'enjeu n'est pas seulement technique. Il faut aussi décider qui intervient, qui communique, qui contacte l'hébergeur, qui vérifie les données personnelles, qui suit Google Search Console et qui documente l'incident pour éviter une réinfection.

Ne pas confondre urgence et précipitation

Lorsqu'un site WordPress semble piraté, la réaction naturelle est de vouloir tout remettre en ligne immédiatement. C'est compréhensible : le site peut être un outil commercial, un support de contact, une boutique ou un portail client. Mais une restauration trop rapide peut effacer des preuves, réintroduire la faille ou remettre en ligne une sauvegarde déjà compromise.

Le bon réflexe est de gérer l'incident comme une séquence : contenir, observer, sécuriser, diagnostiquer, restaurer, vérifier, surveiller. Cette méthode évite de traiter seulement le symptôme visible, par exemple une page injectée, alors que la vraie porte d'entrée peut être une extension vulnérable, un compte administrateur compromis, un accès FTP ancien ou un mot de passe réutilisé.

Attention aux nettoyages superficiels

Limiter l'exposition sans détruire les traces

La première décision consiste à limiter les dégâts. Selon la situation, il peut être préférable de mettre le site en maintenance, de bloquer temporairement certains accès, de désactiver l'exécution PHP dans certains dossiers ou de demander à l'hébergeur d'isoler l'espace compromis. L'objectif est de protéger les visiteurs et les données, tout en conservant suffisamment d'éléments pour comprendre l'incident.

?Si le site sert du malware

Couper ou restreindre rapidement l'accès public. Un site qui infecte ou redirige les visiteurs doit être isolé avant toute action de confort.

?Si le site est e-commerce

Bloquer temporairement les paiements et préserver les commandes. Vérifier les connecteurs de paiement, les comptes administrateurs et les emails transactionnels.

?Si les formulaires sont détournés

Désactiver provisoirement les formulaires concernés, contrôler les notifications, les destinataires et les données stockées.

?Si un compte admin apparaît

Ne pas se contenter de le supprimer. Il faut comprendre comment il a été créé et vérifier les autres accès : FTP, hébergement, base de données, emails.

Visuel de contenu à créer : image-cyberattaque-site-wordpress-premieres-heures-timeline.webp

Préserver ce qui permettra de comprendre l'incident

Avant de nettoyer, il faut conserver les éléments utiles : journaux serveur, liste des fichiers modifiés récemment, comptes utilisateurs, extensions installées, date des dernières mises à jour, captures d'écran, messages d'alerte, emails suspects, logs SMTP, avertissements Google ou alertes de l'hébergeur.

Cette étape peut sembler secondaire dans l'urgence, mais elle évite de perdre la cause racine. Sans journaux et sans copie de l'état compromis, le nettoyage devient un pari : le site peut être remis en ligne, puis se faire réinfecter quelques heures ou quelques jours plus tard.

Éléments à conserver

- Copie des fichiers compromis avant suppression.
- Export de la base de données au moment de l'incident.
- Journaux web, PHP, FTP/SFTP, accès hébergement et erreurs serveur.
- Liste des comptes administrateurs WordPress et hébergement.
- Liste des extensions et thèmes avec leurs versions.
- Captures d'écran des alertes navigateur, Google ou antivirus.

17Cyber est le guichet officiel d'assistance en ligne pour les victimes de cybermalveillance. Il permet de qualifier la menace, d'obtenir des premières mesures et, lorsque nécessaire, d'être orienté vers les bons interlocuteurs ou vers les forces de l'ordre.

Changer les mots de passe ne suffit pas

La sécurisation des accès doit être large. Un attaquant peut être entré par WordPress, mais aussi par FTP, l'hébergement, la messagerie, un poste utilisateur compromis, une extension vulnérable ou un ancien compte prestataire. WordPress recommande notamment de limiter les accès, d'utiliser des mots de passe forts, d'activer la double authentification et de supprimer les extensions non utilisées.

Accès à contrôler	Risque	Action immédiate
Administrateurs WordPress	Contrôle total du site	Réinitialiser les mots de passe, supprimer les comptes inconnus, activer la double authentification.

FTP / SFTP / SSH	Modification directe des fichiers	Révoquer les accès anciens, créer des comptes nominatifs, vérifier les connexions récentes.
Hébergement / Plesk / cPanel	Accès fichiers, base, emails, sauvegardes	Changer le mot de passe, activer MFA si disponible, vérifier les comptes secondaires.
Base de données	Injection, création de comptes, modification de contenu	Changer l'utilisateur ou le mot de passe SQL si nécessaire, vérifier wp_users et wp_options.
Messagerie	Réinitialisation de mots de passe, détournement d'emails	Changer les accès, vérifier les règles de transfert et les connexions suspectes.

Point de vigilance

Il faut éviter les comptes partagés. Chaque prestataire ou collaborateur doit avoir son propre accès, avec un rôle adapté. C'est indispensable pour comprendre qui a fait quoi et pour révoquer proprement un accès.

Identifier la porte d'entrée avant de restaurer

Restaurer une sauvegarde sans comprendre la faille peut remettre en ligne un site vulnérable. Le diagnostic doit rechercher la porte d'entrée probable : extension obsolète, thème abandonné, compte administrateur compromis, fichier PHP déposé dans wp-content/uploads, code malveillant injecté dans un fichier légitime, permissions trop ouvertes, mot de passe faible, poste utilisateur infecté ou accès hébergeur non maîtrisé.

1. 1Comparer les fichiers avec une version saineRechercher les fichiers PHP récents, les modifications inattendues dans le thème, les extensions, le cœur WordPress, le dossier wp-content/uploads et les fichiers de configuration. Une porte dérobée peut être un nouveau fichier, mais aussi une ligne de code ajoutée dans un fichier légitime.
2. 2Contrôler la base de donnéesVérifier les comptes administrateurs, les options WordPress, les scripts injectés dans le contenu, les redirections et les tâches planifiées.
3. 3Auditer extensions et thèmesIdentifier les composants non maintenus, vulnérables, premium non mis à jour, doublonnés ou inutilisés.
4. 4Relire les journauxRepérer les requêtes suspectes, connexions administrateur, uploads inhabituels, erreurs PHP et accès depuis des IP inconnues.

Mesure de durcissement utile

Lorsque la configuration serveur le permet, il est recommandé d'empêcher l'exécution de fichiers PHP dans le dossier wp-content/uploads. Cette mesure limite l'exploitation d'un fichier malveillant déposé dans le répertoire des médias. Elle doit être appliquée avec prudence par le prestataire technique, selon que le serveur utilise Apache, Nginx ou une configuration managée.

Analogie :

Restaurer proprement, puis durcir

La restauration doit partir d'une sauvegarde antérieure à la compromission, mais cette sauvegarde doit être vérifiée. Il faut ensuite appliquer les mises à jour, supprimer les composants inutiles, corriger les permissions, désactiver l'édition de fichiers depuis le tableau de bord et renforcer les accès.

WordPress indique que les hébergeurs fiables doivent fournir des versions stables et récentes des logiciels serveur, ainsi que des méthodes fiables de sauvegarde et de récupération. Le durcissement WordPress recommande aussi de tenir le cœur, les thèmes et les extensions à jour, de supprimer les plugins inutilisés, de protéger wp-config.php, de limiter les droits et de surveiller les journaux.

?Nettoyer

Supprimer fichiers malveillants, comptes inconnus, plugins inutilisés, thèmes abandonnés et redirections suspectes.

?Durcir

MFA, mots de passe forts, droits limités, désactivation de l'édition de fichiers, permissions adaptées, WAF si nécessaire.

?Surveiller

Contrôle des logs, scans de malware, surveillance Google Search Console, alertes hébergeur et vérification des formulaires.

Désactiver l'édition de fichiers

Pour limiter les modifications de code depuis l'administration WordPress, le prestataire peut ajouter dans wp-config.php : define('DISALLOW_FILE_EDIT', true);. Cette mesure ne remplace pas la sécurisation des comptes administrateurs, mais elle réduit les possibilités d'action d'un attaquant qui aurait obtenu un accès au tableau de bord.

Ne pas oublier Google, les navigateurs et les visiteurs

Une compromission WordPress peut déclencher des alertes navigateur, des messages de sécurité, une détection de spam SEO ou une baisse de confiance dans les résultats Google. Une fois le site nettoyé, il faut contrôler Google Search Console, vérifier les pages indexées, chercher les URLs inconnues, consulter les rapports de sécurité et demander un réexamen si une alerte a été émise.

La partie visible du problème n'est pas toujours la plus grave. Le spam SEO peut créer des centaines de pages cachées, des liens vers des sites frauduleux ou des redirections conditionnelles visibles uniquement pour certains visiteurs ou robots. C'est pourquoi le contrôle doit porter à la fois sur le site, la base, les journaux et l'index Google.

Contrôles après nettoyage

- Google Search Console : rapport de sécurité, couverture, pages indexées, actions manuelles.
- Recherche Google : requêtes de type site:exemple.fr pour détecter des pages inconnues.
- Navigateurs : absence d'alerte de sécurité ou de redirection.

- Formulaires : réception normale des demandes et absence de destinataires suspects.
- Logs : absence de nouvelles tentatives d'écriture ou de création de compte.

Vérifier rapidement les obligations RGPD

Une cyberattaque sur un site WordPress peut impliquer des données personnelles : comptes clients, formulaires de contact, commandes WooCommerce, journaux, adresses e-mail ou messages transmis par les visiteurs. Le sujet doit donc être traité dès les premières heures, en parallèle du diagnostic technique.

La CNIL rappelle que toutes les violations ne doivent pas nécessairement être notifiées. En revanche, lorsqu'une violation de données personnelles entraîne un risque pour les droits et libertés des personnes concernées, le responsable du traitement doit documenter l'incident et notifier la CNIL au plus tôt, dans un délai maximal de 72 heures. Si le risque est élevé, les personnes concernées doivent aussi être informées dans les meilleurs délais.

À vérifier sans attendre

- Quelles données personnelles étaient stockées ou accessibles depuis le site ?
- Des comptes clients, commandes, formulaires ou exports ont-ils pu être consultés ou copiés ?
- Le niveau de risque pour les personnes concernées justifie-t-il une notification à la CNIL ?
- Qui pilote le sujet RGPD : dirigeant, DPO, responsable conformité, conseil externe ?
- L'incident est-il documenté dans un registre interne, même si aucune notification n'est finalement nécessaire ?

Point de prudence

Les décisions qui aggravent souvent l'incident

- ?Restaurer trop viteUne sauvegarde peut être déjà infectée ou remettre en ligne la vulnérabilité initiale.
- ?Effacer les tracesSupprimer les logs, fichiers ou comptes suspects empêche de comprendre le mode d'entrée.
- ?Changer seulement le mot de passe WordPressL'accès peut venir de l'hébergement, du FTP, de la base, de la messagerie ou d'un ancien prestataire.
- ?Garder les extensions inutiliséesUn plugin désactivé mais présent reste un fichier exploitable sur le serveur.
- ?Ne pas surveiller après remise en ligneLes réinfections surviennent lorsque la porte d'entrée n'a pas été supprimée.

Checklist dirigeant : premières heures après compromission

Visuel de contenu à créer : image-cyberattaque-site-wordpress-premieres-heures-checklist.webp

Action | Objectif
Mettre le site en sécurité | Protéger les visiteurs et limiter la diffusion du malware ou des redirections.
Créer une copie de l'état compromis | Conserver les preuves et permettre l'analyse de la porte d'entrée.
Contacter l'hébergeur | Obtenir logs, isolation temporaire, sauvegardes et assistance technique.
Réinitialiser les accès critiques | WordPress, FTP/SFTP, hébergement, base de données, messagerie, registrar.
Identifier la faille probable | Extension, thème, compte, fichier, permission, accès prestataire ou poste compromis.
Restaurer depuis une version saine | Remettre en ligne sans réintroduire la compromission.
Mettre à jour et durcir | Fermer la porte d'entrée et réduire la surface d'attaque.
Surveiller pendant plusieurs jours | Détecter une réinfection, des pages spam ou de nouvelles tentatives.

Ce que les lecteurs demandent souvent

Faut-il couper immédiatement le site ?

Une restauration de sauvegarde suffit-elle ?

Doit-on déposer plainte ?

Que faire si des données personnelles sont concernées ?

Comment éviter une réinfection ?

Conclusion

Une cyberattaque WordPress se traite rarement en un seul clic. Le vrai objectif n'est pas seulement de faire disparaître le symptôme visible, mais de comprendre comment l'attaquant est entré, ce qu'il a modifié et comment éviter qu'il revienne.

Pour une PME, les premières heures doivent suivre une méthode claire : contenir, préserver, sécuriser, diagnostiquer, restaurer, vérifier et surveiller. Cette discipline réduit le risque de réinfection et permet de reprendre l'activité avec davantage de maîtrise.

Un diagnostic court peut suffire à déterminer les priorités : urgence visiteur, données exposées, sauvegarde saine, faille probable, qualité de l'hébergement, sécurité des accès et surveillance post-incident.

Sources

• WordPress.org, Hardening WordPress : principes de durcissement, mises à jour, sauvegardes, accès, fichiers, plugins, journaux et surveillance.

• WordPress.org, Editing wp-config.php : constante DISALLOW_FILE_EDIT pour désactiver l'éditeur de fichiers de thèmes et d'extensions.

• 17Cyber, Mon assistance en ligne : guichet officiel d'assistance en ligne pour les victimes de cybermalveillance.

• CNIL, Violations de données personnelles : les règles à suivre : documentation interne, notification à la CNIL dans un délai maximal de 72 heures lorsque la violation présente un risque, information des personnes en cas de risque élevé.

• Google Search Central, Security issues : suivi des problèmes de sécurité, spam et demandes de réexamen après nettoyage.

• ANSSI, 10 règles d'or en matière de sécurité numérique : sauvegardes, mises à jour, mots de passe, double authentification et vigilance.

• WordPress.org, Updating WordPress : bonnes pratiques de mise à jour et sauvegardes préalables.