Un nettoyage fiable commence par une lecture précise de ce qui a changé. L'objectif est de arbitrer entre les options de reprise et organiser la surveillance qui suit, en suivant un choix entre nettoyage et restauration. Le diagnostic ne repose pas sur un seul signal : il rapproche les comptes, les fichiers, les données, les composants et les journaux disponibles. Chaque décision précise ce qui est certain, ce qui reste à contrôler et ce qui conditionne la remise en ligne. La méthode reste valable que l'intervention soit réalisée en interne ou confiée à un prestataire.

Quelle est la date probable de l'incident ? dans une logique de reprise contrôlée

Pour cette zone, il faut relier l'origine probable de l'alerte et le moment où le comportement anormal a été remarqué à la différence entre un dysfonctionnement banal et un indice de compromission. La démarche fondée sur un choix entre nettoyage et restauration demande aussi de contrôler les pages touchées, les fonctions perturbées et les comptes susceptibles d'avoir été utilisés et de ne pas sous-estimer les changements récents apportés au site, à l'hébergement ou aux extensions. Les observations sont séparées des hypothèses, ce qui facilite la décision entre isolation, remplacement, restauration ou surveillance. Après chaque groupe de changements, l'équipe vérifie les fonctions essentielles et conserve les traces nécessaires pour expliquer le résultat obtenu.

La copie disponible est-elle saine ? dans une logique de reprise contrôlée

L'analyse peut commencer par la présence séparée des fichiers, de la base de données et des réglages d'hébergement, puis remonter vers la possibilité qu'une copie ancienne contienne déjà le code indésirable. Dans le cadre de un choix entre nettoyage et restauration, cette progression sert à comprendre le rôle de la date réelle, l'intégrité et le contenu de chaque sauvegarde exploitable et l'effet possible de la capacité à tester une restauration sans écraser l'état courant. Les corrections sont appliquées sur un périmètre défini, avec un point de retour et une personne chargée de valider. Si le comportement change sans que la cause soit identifiée, le site reste sous contrôle renforcé plutôt que d'être déclaré sain trop tôt.

Quelles données récentes seraient perdues ?

Pour cette zone, il faut relier les comptes, les options, les contenus et les réglages qui peuvent contenir une injection à les utilisateurs inconnus et les changements de rôle non expliqués. La démarche fondée sur un choix entre nettoyage et restauration demande aussi de contrôler les scripts ajoutés dans des zones prévues pour du texte ou des paramètres et de ne pas sous-estimer les entrées qui recréent un comportement malveillant après un nettoyage de fichiers. Les observations sont séparées des hypothèses, ce qui facilite la décision entre isolation, remplacement, restauration ou surveillance. Après chaque groupe de changements, l'équipe vérifie les fonctions essentielles et conserve les traces nécessaires pour expliquer le résultat obtenu.

Quels tests départagent les options ? avec une méthode vérifiable

Pour cette zone, il faut relier le fonctionnement du site public, de l'administration, des formulaires et des parcours essentiels à la comparaison des journaux avant et après correction. La démarche fondée sur un choix entre nettoyage et restauration demande aussi de contrôler l'absence de redirections, de scripts inconnus et de comptes non autorisés et de ne pas sous-estimer la vérification depuis plusieurs profils de navigation sans se fier à un seul test. Les observations sont séparées des hypothèses, ce qui facilite la décision entre isolation, remplacement, restauration ou surveillance. Après chaque groupe de changements, l'équipe vérifie les fonctions essentielles et conserve les traces nécessaires pour expliquer le résultat obtenu. Pour approfondir ce contrôle, la ressource [[ANCRE]] peut servir de guide, à condition d'adapter chaque étape au contexte observé.

Qui valide la décision finale ?

Avant d'agir, le responsable décrit les actions attendues de l'hébergeur, du prestataire ou du responsable interne et recherche les personnes qui doivent connaître l'incident sans diffuser d'informations inutiles. Cette lecture, guidée par un choix entre nettoyage et restauration, aide à déterminer si les faits confirmés séparés des hypothèses encore en cours de vérification appartient au même incident. Il faut également tenir compte de les messages destinés aux utilisateurs lorsque le service est limité, car un élément apparemment isolé peut dépendre d'un accès, d'une tâche ou d'un composant commun. Les résultats sont notés au fur et à mesure, puis comparés après correction pour éviter une validation basée uniquement sur l'apparence du site.

Dans ce faq décisionnelle, la clôture doit rester cohérente avec un choix entre nettoyage et restauration. Elle intervient lorsque les accès, les zones techniques et les fonctions publiques ont été revus selon des critères annoncés. Pour arbitrer entre les options de reprise et organiser la surveillance qui suit, les points non vérifiés sont conservés dans le suivi avec une *site WordPress infecté* prochaine action. Cette discipline transforme la site WordPress infecté que faire remise en ligne en décision contrôlée plutôt qu'en simple retour à l'apparence normale.