Les questions aident à choisir entre agir seul, restaurer, reconstruire ou déléguer. L'angle retenu, « décider selon le niveau de confiance », commence par une observation prudente de l'installation et de son contexte. Un symptôme visible peut provenir d'un compte détourné, d'un composant vulnérable, d'un fichier modifié ou d'une donnée injectée. La réponse doit donc préserver un retour arrière, limiter les changements concurrents et définir ce qui sera considéré comme une reprise acceptable.

Comprendre la portée de la compromission

Une compromission ne se résume pas à un fichier suspect : elle peut toucher les accès, les extensions, les données et les tâches planifiées. L'objectif initial consiste à comprendre l'étendue du problème avant de supprimer des éléments qui pourraient servir au diagnostic. Cette étape prend tout son sens lorsqu'elle reste liée au périmètre réel du site et aux actions déjà menées. Pour approfondir cette étape, la méthode détaillée dans [[ANCRE]] peut servir de repère avant de poursuivre. Une intervention ordonnée réduit le risque d'oublier une porte d'accès encore active. Le responsable doit distinguer l'urgence de remise en ligne du besoin de fiabiliser durablement l'installation. Cette lecture globale aide à choisir entre une correction ciblée, une restauration contrôlée ou l'appui d'un prestataire.

- Écrire le périmètre observé afin de ne pas réduire l'incident à un seul symptôme, puis comparer l'état obtenu à une référence fiable.
- Réévaluer l'ordre des actions dès qu'un nouvel indice modifie le risque, sans confondre rapidité et validation.
- Éviter une remise en ligne avant la rotation des accès et les tests, avec une trace des modifications réalisées.
- Mobiliser l'hébergeur ou un spécialiste seulement avec un mandat précis, avec un responsable et un critère de fin.
- Écrire le périmètre observé afin de ne pas réduire l'incident à un seul symptôme, en séparant le fait observé de l'hypothèse.

Traiter d'abord ce qui peut aggraver l'incident

Les identités sensibles et les portes d'entrée durables doivent être traitées avant les optimisations secondaires. L'ordre d'action commence par stabiliser la situation et Cliquez pour la source conserver les traces nécessaires avant toute correction irréversible. L'ordre logique tient compte des liens entre l'hébergement, WordPress, les

extensions, la base et les services connectés. Une équipe gagne en fiabilité lorsqu'elle associe cette phase à un responsable, un résultat attendu et une possibilité de retour arrière. Le plan d'action n'est pas figé : chaque découverte peut modifier le niveau d'urgence ou la séquence des contrôles. Une mesure simple, sûre et facilement annulable peut précéder une opération plus lourde qui exige davantage de préparation.

Le choix entre nettoyage, restauration et reconstruction dépend de la confiance accordée à l'état actuel du site. Une restauration est pertinente seulement si la sauvegarde est datée, testable et antérieure à la compromission probable. Le contrôle doit rester proportionné à l'incident tout en couvrant les chemins qui pourraient maintenir la compromission. Le nettoyage manuel suppose des compétences, du temps et la capacité de comparer l'installation à des références fiables. La reconstruction offre parfois une meilleure assurance quand l'historique est flou ou que plusieurs couches sont touchées. La décision finale doit inclure le coût d'une récidive et pas seulement celui de l'intervention immédiate.

Corriger les erreurs qui favorisent la récidive

Supprimer uniquement le fichier signalé laisse souvent intact le compte compromis, le composant vulnérable ou la tâche persistante. Installer plusieurs outils de sécurité en urgence peut compliquer le diagnostic et créer des conflits. Le contrôle doit rester proportionné à l'incident tout en couvrant les chemins qui pourraient maintenir la compromission. Restaurer une sauvegarde sans la tester risque de réintroduire le même code ou d'effacer des données récentes utiles. Changer un seul mot de passe ne suffit pas lorsque plusieurs niveaux d'accès sont concernés. Remettre le site en ligne avant la validation complète transforme souvent un incident contenu en problème récurrent.

Mobiliser hébergeur et prestataire au bon moment

Le propriétaire du site décide du niveau de service attendu et valide les compromis acceptables. L'administrateur technique exécute ou coordonne les sauvegardes, les contrôles et les corrections. Cette étape prend tout son sens lorsqu'elle reste liée au périmètre réel du site et aux actions déjà menées. L'hébergeur peut fournir des journaux, isoler un espace ou restaurer certains éléments selon le service disponible. Un prestataire spécialisé intervient sur les zones qui dépassent les compétences ou le temps disponibles. La clôture doit être validée conjointement sur les aspects techniques et fonctionnels.

La fin de l'intervention ne correspond pas au dernier fichier supprimé. Elle arrive lorsque les accès ont été repris, les composants comparés à des sources fiables, les fonctions essentielles testées et la surveillance renforcée. Dans une logique décider selon le niveau de confiance, chaque correction doit pouvoir être reliée à un indice ou à un risque identifié. Une sauvegarde propre, un relevé des changements et des responsabilités de suivi donnent alors à l'équipe un point de départ plus fiable pour la maintenance.