

AUDIT DE SÉCURITÉ DES SAUVEGARDES

DONNÉES
SÉCURITÉ
CONFORMITÉ

Maintenir votre infrastructure de sauvegarde sécurisée

- **Nombre de jours** : à partir de 2
- **Périmètre** : Veeam

La sécurisation des données de sauvegarde est aujourd'hui un sujet majeur pour les entreprises, avec des menaces qui ne cessent d'évoluer. Les chiffres parlent d'eux-mêmes :

96%

des attaques par ransomware cible les repository de sauvegarde*

43%

des données affectées ne sont pas restaurable*

27%

des organisations qui ont payé la rançon n'ont pas pu récupérer leurs données même après avoir payé*

85%

des organisations ont subi au moins une attaque de ransomware au cours des 12 derniers mois*

*Source: Veeam Ransomware Trends report 2024

...Pourquoi un audit est essentiel :

- Il permet **d'assurer l'amélioration continue des règles de cybersécurité de vos systèmes d'informations**. Les risques de sinistre en cas de défaillance matérielle, d'erreur humaine, de catastrophe naturelle ou de cyberattaque sont continuellement présents. Les attaquants ciblent les sauvegardes avant de venir chiffrer les données à l'aide de ransomware et utilisent des méthodes de plus en plus sophistiquées, comme l'utilisation de l'intelligence artificielle, pour arriver à leurs fins.
- C'est pourquoi il est **nécessaire de s'assurer de respecter l'ensemble des bonnes pratiques de sauvegarde** pour être capable de **restaurer ces données** en toute circonstance. La réglementation est un enjeu transverse qui impacte fortement la DSI. On parle de **conformité** RGPD, NIS2, etc. Le but est de répondre à ces exigences en étant agile et d'apporter les garanties nécessaires en termes de compliance et de sécurité.
- En adoptant une approche proactive et en mettant en place des mesures de sécurité robustes, les entreprises peuvent non seulement protéger leurs données critiques, mais aussi assurer la continuité de leurs opérations face aux menaces croissantes.

NOTRE OFFRE

monacodigital

En tant que prestataire informatique, Monaco Digital vous accompagne pour vérifier l'application de plus de 70 mesures de sécurité lié à votre environnement de sauvegarde sur les thématiques suivantes :

- Plan de sauvegarde et réplication
- Sécurité physique
- Configuration des composants
- Comptes et permissions
- Chiffrement
- Documentation.

Savez-vous répondre sans hésiter aux questions suivantes afin de garantir la résilience de votre système d'information :

	Oui	Non	Je ne sais pas
• Notre stratégie de sauvegarde est-elle alignée avec les objectifs de continuité d'activité (RPO/RTO) ?	☐	☐	☐
• Notre architecture de sauvegarde respecte-t-elle la règle 3-2-1 (3 copies, 2 supports différents, 1 hors site) ?	☐	☐	☐
• Notre infrastructure est-elle résiliente face aux menaces actuelles (ransomware, attaques ciblées) ?	☐	☐	☐
• Les tests de restauration font-ils partie de notre calendrier d'exploitation régulier ?	☐	☐	☐
• Avons-nous mis en place une authentification multifacteur pour l'accès aux systèmes de sauvegarde ?	☐	☐	☐
• Nos sauvegardes sont-elles chiffrées, tant au repos qu'en transit ?	☐	☐	☐
• Notre stratégie respecte-t-elle les exigences réglementaires de notre secteur ?	☐	☐	☐
• Avons-nous défini des scénarios de reprise après sinistre pour différents types d'incidents ?	☐	☐	☐



Si un certain nombre de questions restent en suspens, alors peut-être qu'une analyse plus fine est nécessaire !

En proposant des **audits complets d'infrastructures**, nos équipes peuvent vous aider à **identifier** les différentes "failles" potentielles de vos écosystèmes de sauvegardes et à les **corriger** avant qu'elles ne se transforment en vulnérabilités coûteuses pour votre organisation.

PROCESS



CONTACTEZ-NOUS

Pour toute demande d'intervention ou de renseignements supplémentaires, n'hésitez pas à nous contacter.



contact@monacodigital.mc
ou contacter votre commercial