RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

LES RÈGLES D'OR DE LA SAUVEGARDE

1/ CONSTRUIRE ET PROTÉGER

→ Définissez une politique de sauvegarde en identifiant les données critiques pour l'activité de votre entreprise et en précisant la fréquence à laquelle il est important de les sauvegarder.

→ Considérez les opérations de sauvegarde et de restauration comme des opérations sensibles d'administration devant bénéficier des protections adéquates : poste d'administration durci, flux dans un réseau d'administration, etc.

→ Rendez indépendante votre infrastructure de sauvegarde vis-à-vis de vos annuaires de production (*Active Directory*, etc.).

→ Assurez-vous du contrôle d'accès à vos sauvegardes pour garantir qu'elles ne seront ni modifiées ni altérées et toujours disponibles, en particulier dans le cadre de l'utilisation d'offres de sauvegarde Cloud.

→ Soyez vigilant sur la sensibilité des données sauvegardées en cas de solution hors-site, dans un cloud public ou chez un prestataire externe. Chiffrez les sauvegardes au préalable par vos propres moyens si nécessaire.

→ Faites évoluer continuellement votre infrastructure de sauvegarde au même rythme que l'évolution de vos SI (virtualisation, cloud, etc.) et en fonction de l'évolution de la menace.
Ne conservez pas une infrastructure obsolète en production.

2/ ANTICIPER ET RÉAGIR

→ Définissez une stratégie de restauration, en lien avec votre PRA et en tenant compte des principaux scénarios d'attaque identifiés sur vos SI (rançongiciels, espionnage, etc.). Réalisez régulièrement des tests de restauration.
Impliquez la direction sur les modes dégradés acceptables en cas de crise Cyber.

→ N'oubliez pas d'inclure les médias d'installation et les configurations de vos applications métier dans vos sauvegardes.

→ Réalisez régulièrement et impérativement des sauvegardes hors-ligne (déconnectées du SI).

→ Prévoyez une procédure d'isolation d'urgence du système de sauvegarde (serveurs, médias, etc.) en cas de suspicion de compromission ou d'attaque en cours.

→ Après un incident, tenez compte du fait que vos sauvegardes peuvent contenir les vecteurs de compromission. Restaurez à partir de sources de confiance (images officielles, binaires d'installation signés), contrôlez la conformité des configurations, faites un scan antivirus des données.

v1.0