RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

SAUVEGARDE DES SYSTÈMES D'INFORMATION

1/ CONSTRUIRE ET PROTÉGER

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

→ **Considérer 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.

→ **Rendre indépendante l'infrastructure de sauvegarde** vis-à-vis des annuaires de production (ex. : Active Directory).

→ **S'assurer du contrôle d'accès des 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*.

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

→ **Faire évoluer continuellement l'infrastructure de sauvegarde** au même rythme que l'évolution des 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

→ **Définir une stratégie de restauration**, en lien avec le plan de reprise d'activité et en tenant compte des principaux scénarios d'attaque identifiés sur les SI (rançongiciels, espionnage, etc.). **Réaliser régulièrement des tests de restauration.** Impliquer la direction sur les modes dégradés acceptables en cas de crise cyber.

→ **Ne pas oublier d'inclure les médias d'installation et les configurations** des applications métier dans les sauvegardes.

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

→ **Prévoir 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, tenir compte du fait que les sauvegardes peuvent contenir les vecteurs de compromission. **Restaurer à partir de sources de confiance** (images officielles, binaires d'installation signés), contrôler la conformité des configurations, faire un scan antivirus des données.

V1.1 (12/23)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr