06/04/2023

Livrable Veeam

Bonnes pratiques concernant les sauvegardes

Lucas EVIEUX
BTS SIO SISR A1

I. Règle du 3-2-1

Nous allons ici aborder les opérations liées à l'infrastructure de sauvegarde, afin de maintenir une solution constamment à jour pour se prémunir contre les dernières vulnérabilités, et gérer de manière sécurisée les comptes administratifs de l'infrastructure.

L'ANSSI préconise la règle "3-2-1" pour les sauvegardes, impliquant la création de trois copies, sur deux supports distincts, dont une hors ligne.

Une mise à jour récente de cette règle suggère "3-2-1-1-0", intégrant une copie en dehors du site principal (dans le Cloud, par exemple), et des sauvegardes fonctionnelles sans erreur.

Même si cette évolution n'est pas spécifiée dans le guide, l'ANSSI souligne l'importance de contrôler et de tester régulièrement les sauvegardes, incluant la rédaction et la mise en œuvre fréquente d'une procédure de restauration du système d'information.

II. Opérateur de sauvegarde

Les sauvegardes doivent inclure les données des utilisateurs, les médias d'installation, la configuration des applications métiers, et même la sauvegarde de l'infrastructure de sauvegarde elle-même. Chaque instance de sauvegarde doit être associée à des comptes dédiés et facilement identifiables, de même que les comptes d'administrateurs dédiés à la sauvegarde, qui devraient être nominatifs et spécifiques à chaque opérateur. Une approche basée sur les rôles (RBAC) peut être adoptée, avec des rôles distincts pour la gestion quotidienne des sauvegardes et l'administration avancée, par exemple la création de nouvelles stratégies.

III. Bouton d'arrêt d'urgence

En anticipant d'éventuels incidents de sécurité, il est recommandé de mettre en place un "bouton d'arrêt d'urgence" permettant de déconnecter rapidement l'infrastructure de sauvegarde afin d'éviter toute altération en cas d'attaque. L'ANSSI souligne que l'isolation immédiate de l'infrastructure de sauvegarde du reste du système d'information est une mesure prioritaire en cas d'incident de sécurité.

IV. Sauvegarde des machines virtuelles

Les entreprises (sauf celles faisant du cloud) intègrent largement les infrastructures de virtualisation. Dans ce contexte, la sauvegarde des machines virtuelles revêt une importance cruciale, et deux options s'offrent à cet effet :

- Effectuer une sauvegarde directe de la machine virtuelle, englobant ses fichiers, notamment les disques virtuels (VHDX, VMDK, etc.).
- Sauvegarder les données et la configuration de la machine virtuelle en installant un agent sur le système d'exploitation invité.

Une approche hybride peut également être adoptée, combinant les deux méthodes, avec des sauvegardes réalisées à des fréquences différentes.

L'ANSSI propose également un tableau des avantages et inconvénients de ces méthodes :

	Sauvegarde fichiers disque de la machine virtuelle	Installation agent au sein de la machine virtuelle
Avantages	■ L'opérateur de sauvegarde n'a pas accès au contenu de la machine virtuelle si celle-ci est chiffrée. ■ Possible optimisation du volume de sauvegarde si l'installation des machines virtuelles est automatisée avec distinction entre les disques « vivants » (données, journaux) et les disques « figés » (systèmes d'exploitation, applications).	■ Granularité possible pour la sauvegarde et restauration de fichiers. ■ Homogénéité de l'exploitation dans le cas où l'on sauvegarde également des serveurs physiques.
Inconvénients	■ La restauration peut poser problème pour le redémarrage de certaines applications (bases de données, Active Directory) ou être inadaptée pour certaines demandes de restauration (serveur de fichiers). ■ Problèmes de performances avec les sauvegardes en mode déduplication par blocs si la machine virtuelle est chiffrée.	■ Augmentation de la surface d'attaque sur les serveurs sauvegardés (agent local avec privilèges élevés). ■ L'opérateur de sauvegarde peut accéder aux données en clair des serveurs sauvegardés.