RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

VIRTUALISATION

La virtualisation est une technologie socle sur laquelle reposent de nombreux SI. **Les infrastructures de virtualisation** (c.-à-d. l'ensemble des logiciels et matériels nécessaires à la fourniture du service de virtualisation) **sont une cible de choix pour les attaquants** afin d'avoir accès plus rapidement et de manière généralisée aux données et applications qu'elles hébergent. Certaines bonnes pratiques permettent de réduire les risques ou les conséquences d'une compromission d'un SI virtualisé.

→ **Former régulièrement les administrateurs** sur les technologies utilisées dans les infrastructures de virtualisation.

→ **Considérer les infrastructures de virtualisation comme critiques pour le SI.** Elles doivent bénéficier des mesures de protection adéquates et être administrées depuis un SI d'administration à l'état de l'art.

→ **Regrouper les nœuds de calcul et le stockage associé par niveau homogène de sensibilité et d'exposition** des applications et/ou des données hébergées.

→ **Mettre en place de la segmentation réseau physique** entre les *zones de confiance** de sensibilité ou d'exposition différentes et **mettre en place de la micro-segmentation réseau** au sein de ces zones.

→ **Maintenir à jour les infrastructures de virtualisation.** Les mises à jour de sécurité doivent impérativement être appliquées en priorité, d'autant plus en cas d'exposition à Internet.

→ **Dédier une interface réseau à l'administration sur les hyperviseurs.** Cette interface doit être connectée à un réseau d'administration à l'état de l'art. Elle ne doit surtout pas être accessible depuis un réseau de production ou Internet.

→ **Prendre en compte l'ensemble du matériel en lien avec l'infrastructure de virtualisation** dans la stratégie d'administration : cartes de management (ex. : HP iLO, Dell iDRAC), baies de stockage, équipements réseau, équipements de sécurité, etc.

→ **Dédier des comptes d'administration** sur l'infrastructure de virtualisation et appliquer le principe de moindre privilège pour les administrateurs.

→ **Rendre les comptes d'administration de l'infrastructure de virtualisation indépendants** des annuaires (ex. : Active Directory) utilisés en production ou sur le SI bureautique. Les chemins de contrôle de ces annuaires doivent être vérifiés régulièrement, de manière à ce qu'ils ne permettent pas d'élévation de privilège depuis les annuaires de production vers l'infrastructure de virtualisation et inversement.

→ **Sauvegarder les éléments nécessaires à la reconstruction des infrastructures de virtualisation** (ex. : configurations, binaires d'installation) de manière indépendante de la sauvegarde des machines virtuelles hébergées.

→ **Vérifier régulièrement les configurations** de l'infrastructure de virtualisation, en particulier sur les points cités dans ce document.

→ **Journaliser, centraliser et superviser les évènements de sécurité** liés à l'infrastructure de virtualisation (ex. : accès, changement de configurations).

(*) cf. https://cyber.gouv.fr/guide-admin-si

V1.0 (02/24)

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