RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

VIRTUALIZATION

As technologies on which many information systems rely, virtualization infrastructures (i.e., all of the software and hardware required to provide the virtualization service) are a prime target for attackers seeking quick, widespread access to the data and applications hosted therein. However, a number of best practices can help to reduce the risks and consequences of a virtualized IS's compromise.

→ **Provide administrators with regular training** on the technologies used in virtualization infrastructures.

→ **Consider virtualization infrastructures as critical for the IS.** They must therefore be adequately protected and managed from a state-of-the-art administration IS.

→ **Group compute nodes and associated storage based on homogeneous levels of sensitivity and exposure** of hosted applications and/or data.

→ **Implement physical network segmentation** between trust zones* of different sensitivity or exposure, and **set up network micro-segmentation** within these zones.

→ **Keep virtualization infrastructures up to date.** Security updates must be applied as a matter of priority, even more so when exposed on the Internet.

→ **Dedicate a network interface to hypervisor administration**. This interface must be connected to a state-of-the-art administration network. It must not be accessible from a production network or the Internet.

→ **Include all hardware linked to the virtualization infrastructure** within the administration strategy: management controllers (e.g. HP iLO, Dell iDRAC), disk arrays, network equipment, security equipment, etc.

→ **Dedicate administration accounts** on the virtualization infrastructure and apply the principle of least privilege for administrators.

→ **Make administration accounts for the virtualization infrastructure independent** of the directories (e.g. Active Directory) used in production or on the office IS. The control paths of these directories must be checked regularly, to ensure that they do not allow privileges to be elevated from production directories to the virtualization infrastructure, and vice versa.

→ **Backup the elements required to rebuild virtualization infrastructures** (e.g. configurations, installation binaries) independently of the backup of hosted virtual machines.

→ **Verify virtualization infrastructure configurations on a regular basis**, particularly with regards to the points mentioned in this guide.

→ **Log, centralize and monitor security events** related to the virtualization infrastructure (e.g. access, configuration changes).

(*) See Recommendations to secure administration of IT systems | ANSSI (cyber.gouv.fr)

V1.0 (02/24)

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