20.2. Virtualisation

Objective

20.2.1. To identify virtualisation specific risks and apply mitigations to minimise risk and secure the virtual environment.

Context

20.2.2. Virtualisation is the software simulation of the components of an information system and may include the simulation of hardware, operating systems, applications, infrastructure and storage. Underlying the simulation is hardware and control or simulation software, often described as a virtual machine (VM).

20.2.3. A Hypervisor is a fundamental component of a virtual environment and provides a supervisory function and framework that enables multiple operating systems, often described as “Guest Operating Systems”, to run on a single physical device.

20.2.4. A fundamental construct in the management of risk in virtual environments is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular trust Zone. As assets are added to a Trust Zone, they inherit the security policies set for that Trust Zone.

20.2.5. Trust Zones will also apply the Principal of Least Privilege, which requires that each element in the network is permitted to access only those other network elements that are required for the node to perform its business function.

20.2.6. Virtualisation is radically changing how agencies and other organisations select, deploy implement and manage ICT. While offering significant benefits in efficiency, resource consolidation and utilisation of CIT assets, virtualisation can add risks to the operation of a system and the security of the data processed and managed by that system.

20.2.7. Virtualisation adds layers of technology and can combine many, traditionally discrete and physically separate components, into a single physical system. This consolidation invariably creates greater impact if faults occur or the system is compromised. Virtual systems are designed to be dynamic and to facilitate the movement and sharing of data. This characteristic is also a prominent attack vector and can make the enforcement and maintenance of security boundaries much more complex.

20.2.8. Virtualisation is susceptible to the same threats and vulnerabilities as traditional ICT assets but traditional security offers limited visibility of virtualised environments where the assets configurations and security postures are constantly changing. Incidents in virtualised environments can rapidly escalate across multiple services, applications and data sets, causing significant damage and making recovery complex.

Virtualisation risks

20.2.9. Virtualisation risks can be considered in four categories:

- Risks directly related to virtualisation technologies;
- Systems architecture; implementation and management;
- The usage and business models; and
- Generic technology risks.

Mitigations

20.2.10. The controls described elsewhere in this manual deal with generic technology risks. Important steps in risk mitigation for virtual environments include:

- Identify and accurately characterise all deployed virtualisation and security measures beyond built-in hypervisor controls on VMs.
- Comparing security controls against known threats and industry standards to determine gaps and select appropriate controls.
- Identify and implement anti-malware tools, intrusion prevention and detection, active vulnerability scanning and systems security management and reporting tools.

References

20.2.11.

Further references can be found at:

Reference	Title	Publisher	Source
NIST Special Publication 800-125, January 2011	**Guide to Security for Full Virtualisation Technologies**	NIST	SP 800-125, Guide to Security for Full Virtualization Technologies | CSRC (nist.gov)
	The Security Technical Implementation Guides,	Defense Information Systems Agency,	Security Technical Implementation Guides (STIGs) – DoD Cyber Exchange
	Virtualization Security Checklist	ISACA	Virtualization Security Checklist - PDF Free Download (docplayer.net)
	Guidelines for System Hardening	ACSC	Guidelines for System Hardening | Cyber.gov.au
	Virtual Machine Security Guidelines	The Center for Internet Security	CIS Benchmarks (cisecurity.org)
	Software-Defined Networking (SDN) Definition	Open Networking Foundation	Software-Defined Networking (SDN) Definition - Open Networking Foundation
	Network segmentation and segregation	ASD	Implementing Network Segmentation and Segregation | Cyber.gov.au

Rationale & Controls

Functional segregation between servers

20.2.12.R.01. **Rationale**

Agencies may implement segregation through the use of techniques to restrict a process to a limited portion of the file system, but this is often less effective. Virtualisation technology MUST be carefully architected to avoid cascade failures.

20.2.12.R.02. **Rationale**

The key element in separating security domains of differing classifications is physical separation. Current virtualisation technology cannot guarantee separation.

20.2.12.R.03. **Rationale**

The use of virtualisation technology within a security domain is a recognised means of efficiently architecting a system.

20.2.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4877]

Virtualisation technology MUST NOT be used for functional segregation between servers of different classifications.

20.2.12.C.02. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must Not** [CID:4878]

Virtualisation technology MUST NOT be used for functional segregation between servers in different security domains at the same classification.

20.2.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4879]

Agencies SHOULD ensure that functional segregation between servers is achieved by:

- physically, using single dedicated machines for each function; or
- using virtualisation technology to create separate virtual machines for each function within the same security domain.

20.2.12.C.04. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4880]

Virtualisation technology SHOULD NOT be used for functional segregation between servers in different security domains at the same classification.

Risk Management

20.2.13.R.01. **Rationale**

Where virtualisation technologies are to be used, risk identification, assessment and management are important in order to identify virtualisation specific risks, threats and treatments.

20.2.13.C.01.

Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must [CID:4883]

Agencies MUST undertake a virtualisation specific risk assessment in order to identify risks, related risk treatments and controls.

20.2.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4884]

Agencies SHOULD undertake a virtualisation specific risk assessment in order to identify risks and related risk treatments.

Systems Architecture

20.2.14.R.01. **Rationale**

It is important to include virtualisation specific concepts, constraints, mitigations and controls in the design of systems architectures that propose using virtualisation technologies, in order to gain maximum advantage from the use of these technologies and to ensure security of systems and data is maintained.

20.2.14.R.02. **Rationale**

Virtual environments enable a small number of technical specialists to cover a wide range of activities such as network, security, storage and application management. Such activities are usually undertaken as discrete activities by a number of individuals in a physical environment. To remain secure and correctly and safely share resources, VMs must be designed following the principles of separation and segregation through the establishment of trust zones.

20.2.14.R.03. **Rationale**

Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and managed by a separate application described as a controller. SDNs are intended to provide flexibility by enabling network engineers and administrators to respond to rapidly changing business requirements. Separation and segregation principles also apply to SDNs.

20.2.14.R.04. **Rationale**

In addition to segregation of key elements, VM security can be strengthened through functional segregation. For example, the creation of separate security zones for desktops and servers with the objective of minimising intersection points.

20.2.14.R.05. **Rationale**

Poor control over VM deployments can lead to breaches where unauthorised communication and data exchange can take place between VMs. This can create opportunity for attackers to gain access to multiple VMs and the host system.

20.2.14.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:4891]

Agencies MUST architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones or security domains.

20.2.14.C.02. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must Not** [CID:4892]

Agencies MUST NOT permit the sharing of files or other operating system components between host and guest operating systems.

20.2.14.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4893]

Agencies SHOULD architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones.

20.2.14.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4894]

Agencies SHOULD design virtualised systems and environments to enable functional segregation within a security domain.

20.2.14.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4895]

Agencies SHOULD harden the host operating systems following an agency or other approved hardening guide.

20.2.14.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4896]

Agencies SHOULD separate production from test or development virtual environments.

20.2.14.C.07. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4897]

Agencies SHOULD NOT permit the sharing of files or other operating system components between host and guest operating systems.

Systems Management

20.2.15.R.01. **Rationale**

VMs are easy to deploy, often without formal policies or controls to manage the creation, management and decommissioning of VMs. This is sometimes described as "VM sprawl", which is the unplanned proliferation of VMs. Attackers can take advantage of poorly managed and monitored resources. More deployments also mean more failure points, so VM sprawl can create operational difficulties even if no malicious activity is involved.

20.2.15.R.02. **Rationale**

A related difficulty occurs with **unsecured VM migration** when a VM is migrated to a new host, and security policies and configuration are not updated. VMs may also be migrated to other physical servers with little or no indication to users that a migration has occurred. Unsecured migration can introduce vulnerabilities through poor configuration and incomplete security and operational monitoring.

20.2.15.R.03. **Rationale**

Denial of service attacks can be designed specifically to exploit virtual environments. These attacks range from traffic flooding to the exploit of the virtual environment host's own resources.

20.2.15.R.04. **Rationale**

The ability to monitor VM backbone network traffic is vital to maintain security and operations. Conventional methods for monitoring network traffic are generally not effective because the traffic is largely contained and controlled within the virtual environment. Careful selection and implementation of hypervisors will ensure effective monitoring tools are enabled, tested and monitored.

20.2.15.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:4903]

Agencies MUST ensure a VM migration policy and related SOPs are implemented.

20.2.15.C.02. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:4904]

Agencies MUST implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.

20.2.15.C.03. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:4905]

Agencies MUST implement controls to safely decommission VMs when no longer required, including elimination of images, snapshots, storage, backup, archives and any other residual data.

20.2.15.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4906]

Agencies SHOULD ensure a VM migration policy and related SOPs are implemented.

20.2.15.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4907]

Agencies SHOULD implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.

20.2.15.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4908]

Agencies SHOULD implement controls to safely decommission VMs when no longer required.

20.2.15.C.07. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4909]

Agencies SHOULD implement security and operational management and monitoring tools which include the following minimum capabilities:

- Identify VMs when initiated;
- Validate integrity of files prior to installation;
- Scan new VMs for vulnerabilities and misconfigurations;
- Load only minimum operating system components and services;
- Set resource usage limits;
- Establish connections to peripherals only as required;
- Ensure host and guest time synchronisation;
- Detect snapshot rollbacks and scans after restores;
- Track asset migration; and
- Monitor the security posture of migrated assets.

Authentication and Access

20.2.16.R.01. **Rationale**

VM sprawl can compromise authentication and access procedures, identity management, and system logging. This can be complicated with the use of customer-facing interfaces, such as websites.

20.2.16.R.02. **Rationale**

Host and guest interactions and their system vulnerabilities can magnify virtual system vulnerabilities. The co-hosting and multi-tenancy nature of virtual systems and the existence of multiple data sets can make a serious attack on a virtual environment particularly damaging.

20.2.16.R.03. **Rationale**

A guest OS can avoid or ignore its VM encapsulation to interact directly with the hypervisor either as a direct attack or through poor design, configuration and control. This can give the attacker access to all VMs in the virtual environment and potentially, the host machine. Described as a "VM escape", it is considered to be one of the most serious threats to virtual systems.

20.2.16.R.04. **Rationale**

Hyperjacking is a form of attack that takes direct control of the hypervisor in order to gain access to the hosted VMs and data. This attack typically requires direct access to the hypervisor. While technically challenging, hyperjacking is considered a real-world threat.

20.2.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4915]

Agencies MUST maintain strong physical security and physical access controls.

20.2.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4916]

Agencies MUST maintain strong authentication and access controls.

20.2.16.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4917]

Agencies SHOULD maintain strong data validation checks.