Ten Deadly Sins in Virtualization Security

Virtualization brings manifold benefits to organizations such as better hardware utilization, cost savings and flexibility in business operations. However, this new technology with all of its added benefits still has inherent risks. Also, since virtualization is deployed across computer-based systems, securing the environment is a key priority. This paper looks at the ten deadly sins of virtualization security.

1. Introduction

Virtualization refers to a framework, which allows multiple operating systems to share the resources of a single underlying server, while at the same time keeping that operating system isolated from the server. In other words, virtualization involves the sharing of a common resource by multiple users. A virtualization layer is placed over a single physical server. This layer hosts multiple virtual machines, and each virtual machine runs an operating system[1] and one or more applications.

The computer and information technology revolution have resulted in increased dependencies on multiple workstations, servers, hardware devices, communication and network devices. This phenomenon has resulted in increased expenditures on IT infrastructure, and has also created new issues such as the need for adequate space requirements, cooling mechanisms, and of course, adequate power. This is where Virtualization comes in. Virtualization technology has introduced never before seen benefits that have greatly reduced hardware costs, server consolidation, improved server utilization and lower maintenance costs.

2. Virtualization Security

Virtualization is a new technology whose security concerns are in an evolving phase. A lack of awareness about security threats in a virtualized environment is a major concern. Inaccurate threat perception and improper change management are some of the factors that lead to errors and create opportunities for hackers.

2.1 Ten deadly sins of virtualization security

i. Improper capacity planning

The main advantage of virtualization is that its technology enables the running of multiple virtual machines on a single, physical server. However, a problem that can occur is that organizations, in an effort to capitalize on the benefits offered by virtualization, may overestimate the physical server's ability to manage multiple virtual machines. This can result in the organization continuing to add

[1] Operating systems running on a virtual machine are referred as guest operating systems.

on more virtual machines to the same physical server, which results in a virtual sprawl. This practice can lead to a situation where the physical machines are overworked resulting in reduced productivity.

Furthermore, virtual machine sprawl can make it inconvenient to implement regular security updates, patch management and can also lead to configuration challenges. While it is easy to create virtual machines and move them between different physical server hosts, a large number of virtual machines can make it difficult for IT personnel to keep a track, or record all virtual resources and their locations. In this confusion, some of the virtual resources may remain unpatched which is of course, a vulnerability that can be exploited by hackers. For example, it would be difficult to curtail the spread of virus infection from an untracked machine to other machines on the network. (The threat of unauthorized access to sensitive corporate data is always a looming threat.)

In contrast, some organizations may underestimate the capacity of a physical server and operate only a few virtual machines. This underestimation can lead to under utilization of the physical server. In the long run, both practices can lead to increased costs. Identifying the optimum physical server and virtual machine ratio is a better practice in the management of virtualized resources.

ii. Lack of proper planning

Lack of planned migration to virtualization may:

a. Lead to mismanagement of resources

b. Lead to cost escalations

c. Result in failure to incorporate all security considerations involved in virtualization environment.

A virtualized environment is different from the physical environment in that the technology involves server consolidation and creation of numerous virtual machines with their own set of operating systems and applications. Virtual machines can not only be moved from one location to another, but they can also be stored in different storage devices. Computers in a physical environment are limited to the use of one operating system and application(s) on a physical machine, while virtualization enables multiple virtual machines with their own set of operating systems and applications to use the resources of one physical machine. The virtualization layer “virtualizes” the hardware for each virtual machine which means that one physical machine can run many applications depending on how the virtual machines are installed. For example, if an underlying machine supports 10 virtual machines, the ratio of software to hardware would be 10:1. (10 different applications make use of the same hardware.)

Security mechanisms used in virtualization must be able to secure the entire spectrum of the virtual environment; virtualization layer, virtual machines, operating system, applications, and related databases. It is important to make a complete assessment of resource aggregation and segregation involved in virtualization for employees who are new to the virtualization environment. It is

also crucial to involve information security experts in the planning and design phase of virtualization to ensure secure virtualized environment.

iii. Not securing the Virtualization Layer

The Virtualization layer acts as a host to the virtual machines and keeps these layers unaffected by any changes in the physical server. Securing the Virtualization Layer is therefore crucial to ensure the smooth flow of operations in the virtualized environment. Errors and vulnerabilities could compromise the virtualization layer because hackers will exploit these vulnerabilities by launching attacks via compromised virtual machines. Vulnerabilities may lead to unauthorized access, unauthorized use of data; execution of malicious code and disruption of services.

Some of the measures include:

- **a.** Strong configuration of the virtualization layer
- **b.** Embedded and thin virtualization layer
- **c.** Use of latest available virtualization layer software with improved security
- **d.** regular patch management,
- **e.** use of latest anti-rootkits
- **f.** removal of unused applications

iv. Media Access Control (MAC) address spoofing

All virtual machines have a virtual network adapter. A virtual network adapter is a program used to connect virtual machines with a network. Each virtual network adapter has an initial MAC address to filter access requests. However, the operating system of a virtual machine can alter the MAC address, which enables the operating system to launch malicious attacks on other devices within the "range" of the virtual network adapter.

MAC address spoofing countermeasures include changing the default settings on the virtual switch[2]. The default settings in a virtual switch are set to accept any request for change in MAC address. By default, they are also not set to compare MAC addresses. These two settings can be set to reject or to disallow changes in the MAC address and facilitate comparison with initial MAC address.

v. Lack of trust zone[3] separation

Virtualization allows for financial and energy savings, and also facilitates reduction of physical IT infrastructure. These benefits make it attractive for organizations to virtualize business critical systems and functions. In a physical

[2] Virtual switch is a software program that enables communication between various virtual machines.

[3] Trust in IT parlance refers to the reliance and dependence on various IT systems.

network, separation of these functions from those of different trust zones is crucial to reduce security risk in virtual environment. Lack of separated trust zones may result in unauthorized access to sensitive information.

Some of the methods for trust zone separation include:

a. Physical separation

b. Virtual separation, and

c. Fully collapsing all servers into virtual infrastructure.

All three of these methods have their relative advantages and disadvantages. Physical separation offers simple configuration, but offers low consolidation. Virtual separation facilitates better resource utilization, but involves complex configuration. Fully collapsed trust zones enhance virtualization, but involve more complex configuration.

vi. Lack of adequate access controls

In a virtualized environment, the association between a physical host and virtual machines is dynamic. There is no one-to-one relationship. Many virtual machines can run on a virtualization platform backed by a physical server, and the server can run diverse virtual machines through the virtualization platform. This functionality poses a challenge to access control and privilege management within the virtualized environment. Lack of adequate access control can result in improper assignment of duties. Therefore the role of the system and network administrator undergoes significant change when managing a virtual environment.

Role-based access control mechanisms may facilitate better management of privileges. Access to the Virtualization Layer may be restricted to authorized system administrators to avoid unauthorized access. There are many “virtualization” software manufactures and roles and privileges may be customized based on the complexity of the virtualization software.

vii. Misconfiguration

One of the important aspects of virtual network security is to ensure that restricted data is isolated and not accessible to other machines in the network. Proper configuration is crucial for smooth flow of operations. Inappropriate configuration may result in risk of inadvertent access to unauthorized data by users. Organizations need to have properly defined configuration policies and procedures in place. Appropriate configuration will ensure proper relationships between virtualization host, virtual machines, operating systems and applications. Virtual machines and the host must be isolated from each other through firewalls. An appropriate configuration should require devices to detect changes in configuration. Configuration should be adaptable to software updates. Regular patch management of the guest operating systems and host is crucial to guard against any vulnerability.

viii. Lack of adherence to licensing requirements

Software used by organization before migrating into virtualization was designed to meet the requirements of the physical environments and may not perform properly in a virtual environment. Therefore it is important to test the feasibility of using the same software in virtualized environment. It is also important to ensure compatibility of operating systems and software used by host server and virtual machines.

Proper analysis of software licensing requirements with respect to operating systems and applications on virtual machines may avoid disruption of activities. Software with an expired license is vulnerable to security threats. Hackers may use this vulnerability to launch an attack on other applications and guest machines. Every application may have different licensing requirements. Adherence to proper licensing requirements can help facilitate proper configuration, faster processing by the virtual machines and continuity in business operations.

ix. In appropriate Log management

Inappropriate log management refers to use of techniques which are not suitable for the virtual environment. Traditional log management techniques when applied in virtual environment, may fail to record logs during movement of one virtual machine to another server and system or network downtime.

Log management systems in virtual environment must be able to log all virtual systems, applications, devices and virtual network. It is crucial to ensure that log files are not modified or tampered with so log files must be kept in a secure location. If there is shift in the location of the virtual machines, it is crucial to ensure that associated log files are shifted as well. Log management should facilitate correlation between different events to reveal a complete trail of activity by a user. It is crucial to have appropriate log management as log files contain evidence. This evidence could be useful in a forensic investigation and can een be utilized in disputes and litigation.

x. Lack of monitoring of virtual machine communication

Physical network security devices may not discern communication between different virtual machines, therefore inadequate monitoring can make the virtual environment vulnerable to threats such as man-in-the-middle attacks, intrusion, unauthorized access and unauthorized use of a virtual machine or information.

A virtual switch facilitates communication between different virtual machines operating on the same platform. A virtual switch requires clearly defined roles to ensure that only designated users monitor inter-virtual machine communication. It can be considered a “best practice” to have separate networks between Inter-virtual machine communication and an external network. Also, only those virtual machines, which are operational, should be connected to network. Measures

should be taken to detect and disable any unauthorized communication between host and guest operating systems. Virtual firewalls and detection systems should be installed to ensure visibility of virtual network traffic.

3. Conclusion

As information technology evolves, virtualization security is going to continue to increase in importance. Attacks in virtual space have just arrived. The real threat lies from vulnerabilities that have yet to be discovered. Following a planned approach toward virtualization can minimize security threats. Organizations can maximize the benefits of virtualization technology by devising a well-planned strategy for migration to a virtualized environment.