INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY STUDIES
SPECIAL ISSUE ON ADVANCEMENT IN FIELD OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

To study Security Mechanism in Desktop Virtualization

Mr. Amale B. B.
Assistant Prof.
Dept. of Computer Science, PVP College Pravaranagar
E-mail ID: baban_amale@yahoo.com

Abstract

The idea is that the Linux host operating system will have high security. This comes not from elaborate protections, but simply from doing as little as possible in the host OS. You need to apply the basic precautions of firewall, automatic updates and anti-virus. Beyond this, all desktop attacks rely on some kind of user-initiated action. A desktop that is only used to access a small number of highly trusted sites is at relatively low risk. The VM for day-to-day use still needs to be well secured. Because of all the browsing, downloading and such, it is at high risk. You absolutely need to take the basic precautions, and it is worth taking further precautions.

Keywords:
Desktop Virtualization, Security, access control mechanism, threat infection

Introduction

Desktop virtualization is a computing model that combines the flexibility of a robust desktop experience with the ability to centrally manage virtual client machines. In essence, it's a marriage between the convenience of a user-focused environment and the control of a thin-client model. This offers network administrators greater options in managing, deploying, and securing applications and data network-wide while allowing end users a familiar computing experience and convenience with remote access capabilities. Security refers to all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it.

Following different modes are considered for security and access control mechanism

Update Security Policies

It may seem obvious, but often IT organizations don't realize that they should revise and document security policies to deal with their new virtualization capabilities. For example, with desktop virtualization in place, organizations are changing their security stance on employee-owned computing platforms such as laptops and tablets (e.g. Apple iPads, Droid devices). Naturally, employees will need to obtain approval for any changes to the existing security policy from the designated Chief Information Security Officer or the committee responsible for overseeing those policies.[5][6][8]

Virtual Desktop Hardening

Like physical PCs, virtual desktop operating systems, settings and applications should be hardened using industry standard hardening guidelines. In addition, desktop virtualization has the advantage of making it easier to implement and standardize hardened configurations by using centrally created and maintained template/master images that are linked to the virtual desktops. When a new patch or policy change is issued, desktop virtualization can be used to automatically update all virtual desktops with a simple and consistent configuration change.

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

Virtual Desktop Access Control

Each organization should have a single definitive repository such as Active Directory or LDAP that is used to authorize users and provide access control for enterprise resources. Like physical desktops, virtual desktops should require the user to authenticate and be authorized to use specific workspaces. When a virtual desktop contains information such as regulated personally identifiable information (PII) – credit card information, social security numbers or healthcare information – the virtual desktop should verify that the user is authorized to access that data in that virtual desktop. The desktop virtualization management system should also be able to tie security policies to groups of users, a specific user, or the virtual desktop instance itself. For example, a doctor might need authorization to access a virtual desktop with patient information from his personal computer. However, a computer used for billing that contains a database of patient social security numbers should never be accessed outside the hospital network.[2]

Remote Access Security

When providing remote access to an enterprise network, it's recommended that you verify that the user is running a VPN client from a trusted device. If the VPN client is installed on the host PC and the virtual desktop is sharing the network connection, malware on the host PC could propagate a worm through the enterprise network or intercept network traffic originating in the virtual desktop. To ensure the VPN client is installed on a trusted endpoint, use the pre-authentication host security scanning (aka Network Access Control) functionality of the VPN gateway. In addition, it is recommended that organizations use some type of strong authentication and/or client-side certificates, which can be securely stored and encrypted in conjunction with the virtual desktop.

Isolation Control

For virtual desktops that run on host PCs with separate local operating systems (e.g. client–side virtualization), it is important to ensure that the virtual desktop environment – including applications, data and settings – is isolated from the host PC to prevent malware on the host from infecting the virtual desktop. Isolation also protects private data by preventing data loss through copying, scanning, printing, etc.[7]

Host Security Scanning

Many organizations have implemented Network Access Control (NAC) functionality that scans the PC to verify that it is secure (equipped with up-to-date anti-virus, personal firewall, host intrusion prevention) prior to allowing it to access the corporate network. Similarly, virtual desktops should scan host PCs prior to allowing users to start the virtual desktop session to ensure that the host system is secure. This is an important risk mitigation step to protect from desktop capture and keystroke logger software that may be running on the host PC.

Host Operating System Check

In addition to host security scanning, organizations can use various tools with desktop virtualization to scan the operating system of the host PC to ensure that the critical security patches have been installed prior to allowing the virtual desktop to start. This is just as important to risk mitigation of data loss as host security scanning because out-of-date, unlatched operating systems are one of the top reasons malware spreads.[7]

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

Network Security & Segmentation

When virtual desktops run on host PCs, network traffic typically uses separate virtual network adapters to enable both the virtual desktop and the host PC to send and receive data using the same network interface. With the virtual adapter installed, VPN applications, Windows protocols and services, and other network applications can send and receive network traffic. It is important to ensure that network protocols, services, and applications are isolated from those of the host PC to maintain the integrity of the data that is transmitted and protect the data against malware/spyware. Virtual network adapters typically operate in two modes: bridged or NAT. It's important to consider which networking mode will work best in your environment and provide network security in conjunction with your endpoint security. Personal firewalls, which are widely deployed as part of the Microsoft Windows operating system and endpoint security suites, can provide additional protection from malware for both the host PC and the virtual desktop. To ensure that a personal firewall is present on the host PC, organizations should use host security scanning to verify that a firewall is present prior to allowing the virtual desktop to start. In addition, a personal firewall should be installed inside the virtual desktop to filter network traffic for the virtual network adapter.[1][3][6]

Data Protection & Encryption

When organizations use virtual desktops on a laptop or removable drive with client-side virtualization, they should encrypt the virtual desktop data to ensure that confidential information is not exposed if the device is lost or stolen. If you are in the financial services, retail, government, healthcare or another regulated industry, you may be required to encrypt your workspaces just as you would be required to encrypt the file system or hard drive of a physical PC. Confidential data should also be encrypted in transit when sent over public networks using SSL or IPSec VPN encryption. The keys used for encryption should be stored securely, preferably in a Smart Card/Token or on a Trusted Platform Module (TPM). The encryption technology should use standards-based encryption such as AES and provide secure key management and recovery capabilities.

Staying on top of the increasingly complex regulatory compliance requirements can be challenging for even the most diligent organization. The implementation of desktop virtualization is an opportunity to take control of IT compliance by leveraging the built-in security and management functionality of desktop virtualization platforms to implement controls that help achieve compliance with applicable regulations—a win-win scenario for any organization.[3][4][5][6]

SECURITY BENEFITS DUE TO VIRTUALIZATION

The following are some of the benefits to security [2]

- Centralized storage.
- A virtual environment provides flexibility in that it allows the sharing of systems without necessarily having to share critical information across the systems
- Hardware reductions that occur due to virtualization improve physical security
- Desktop virtualization can be deployed to better control the user environment.

Conclusion

There are a number of security issues that should be considered when planning, deploying, and maintaining virtualization technologies. With the proper configuration management program – defining

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

policies and configuration guidelines, creating procedures to implement the policies and maintain them. In many organizations, network monitoring and intrusion detection solutions have been established to gain visibility and security alerting on critical network segments.

Virtualization is a very important part of the system administration and development. The security aspects needed to be considered very carefully. As with any technology, this consideration needs to occur prior to full rollout to production. By guessing virtualization against both the needs of the business the confidentiality, integrity, and accessibility triangle of security, virtual machines can be used.

References

1. *Davide Adami, Stefano Giordano, Multidomain layer 1 Infrastructure Virtualization as a Feature Internet Services-enabling Paradigm, Journal of Internet engineering 4(1) (December 2010).*
2. *Desktop Virtualization & evolving strategies for IT services Delivery- Jaime Halscott*
3. *Operating System – William Stallings*
4. *Book on Virtual Private networks – Cherley sconn & paul wolf*
5. *Security 2.0 CSO online, April 2005*
6. *Goodrich and Tamassi , Introduction to Computer security (2010, Addison-Wesley*
7. *Boyle and Panko, Corporate Computer Security, 3/e (2013, Prentice Hall)*
8. *Stallings and Brown, Computer Security: Principles and Practice, 2/e (2011, Prentice Hall).*