WALL STREET TECHNOLOGY ASSOCIATION™
TICKER
WWW.WSTA.ORG/PUBLICATIONS

Information Security Considerations

for Server Virtualized Information Infrastructure

By John P. Pironti

Server virtualization is quickly becoming the next killer solution in information infrastructure, which means that it is also becoming the next great target. The benefits that can be realized from introducing server virtualization solutions within information infrastructure are obvious, but the information security threats and vulnerabilities that are introduced by using these solutions may not be as obvious. Unfortunately in the race to virtualize their server environments, many organizations do not involve information security representatives during the architecture and design phase and only involve them after implementation, if at all. Many organizations feel that the traditional information security controls that are already in place in current server solutions are sufficient to secure these new virtualized environments, but in reality there are numerous new considerations that must be addressed. While nothing replaces a threat and vulnerability analysis of an organization's information infrastructure in order to determine appropriate vulnerability management requirements and capabilities, there are some concepts that are essential to server virtualization security.

> It is important to recognize that the most effective information security techniques are not new concepts or technologies, but the adaptation of current control frameworks, processes and capabilities to accommodate the introduction of server virtualization.

Patching

One of the key information security capabilities within an organization is its ability to patch systems after testing the patch to verify it is beneficial to the organization. Server virtualization represents a unique challenge in this area in that current patch management solutions focus on systems and environments that are running at the time of patch deployment. If a virtual server is not running or if it there is no patch management agent installed as part of its creation, it is possible that it will not be patched. The organization will be unaware of the virtual server that has not been patched until it is compromised or it performs a focused analysis on system patch status. It is important to have an accurate inventory of all virtual servers within an organization's information infrastructure and the applications installed on them. This will allow the organization to perform inventories to ensure the timely patching of all virtual servers.

Identification of Virtual Servers

The ease in which new virtual servers can be created and removed is a key benefit of server virtualization. Unfortunately, the adversary community is also aware of this fact. They often will try to create rogue virtual servers within an environment to use as an attack source that can circumvent many of the traditional application and network security controls that may be in place. For instance, if an attacker is able to create a virtual server on a system that is authorized to access sensitive databases and information stores, it is likely to be capable of bypassing network and host based intrusion detection controls because it is

controls because it is considered a trusted host within the environment. It is vital to have a defined process for managing the creation and removal of virtual servers within an organization's information infrastructure as well as management of the access control properties associated with these servers in order to account for business-appropriate virtual environments. With an accurate accounting, basic scanning tools can distinguish business-appropriate virtual servers from those that are not approved to be running within the organization's information infrastructure.

Virtual Appliances

Virtual appliances are software virtual servers which software vendors have configured and tuned to allow for the most efficient and effective capabilities of their solutions. Unfortunately, what a vendor defines as an ideal configuration for their solution may not be compliant to configuration requirements and information security policies of an organization. For instance, a vendor may decide that certain controls such as integrity checks, firewall configurations, authentication mechanisms, and others may cause inefficiency for their solution and will remove them in their virtual appliance solution. It is vital to ensure that all virtual server capabilities, including virtual appliances that are introduced into an organization's information infrastructure, comply with the configuration guidelines and standards that have been defined and implemented by the organization, not the vendor.

Segmentation

The vendor community which creates and supports server virtualization software has attempted to create an aura of security capabilities associated with their solutions. The most obvious of these is the assertion that the hypervisor, or layer between the virtualized environment and base operating system, is impenetrable and secure. However, there are already early indications from security researchers that this may not be the case. The hypervisor represents a new attack vector and technology and as such, has only recently become interesting to adversaries who are now finding new and interesting ways to exploit it. It is important to continue physical separation as well as logical for environments with differing functions and sensitive information assets. For instance, it is critical to remember to continue to segment development, staging, and production environments into different network, storage, and system environments. Virtualization has made it easy and attractive from an operations perspective to combine some or all of these capabilities, but from an information security and operational readiness perspective, this is not recommended.

Final Thoughts

The introduction and utilization of virtual servers is a current reality in many organizations and inevitability in most others. The information security controls that are required to protect these capabilities are not new, but rather they are tried and tested techniques that have been in place since the introduction of the logical partition (LPAR) in the mainframe world. It is important to recognize that the most effective information security techniques are not new concepts or technologies, but the adaptation of current control frameworks, policies, processes and capabilities to accommodate the introduction of server virtualization.

John P. Pironti, CISA, CISM, CISSP, ISSAP, ISSMP is the Chief Information Risk Strategist at Getronics, 978-625-6540; email: john.pironti@getronics.com; web: www.getronics.com.