

Security Auditing in a Virtual Environment

Security auditing considerations within a Virtual Environment

Increasing and widespread use of the virtual platform can be seen as a direct response by enterprises to global cost saving initiatives and the embracing of newer, cleaner and faster technologies. The investment is still available even in the current economic climate.

The traditional data centre was the first to embrace the use of virtualisation and with larger businesses changing or planning to change to virtual instances the trickledown effect on smaller scale concerns is inevitable. Virtualisation is seen as the way forward for most organisations.

Within these virtual environments the benefits are immediately plain to see with the impact on capacity management due to the consolidation of the old physical model. Although decreasing in physical presence the overall technical model remains the same. The usual IT management platforms and back office systems are there, only now they reside within fewer physical entities.

The current growth rate for virtualisation technology is increasing as fast as deployments allow and forecasts show that it will not abate in the coming years. The growth rate has its own drawbacks as the required skills will, in the short term at least, be hard to find as professional communities grapple to get up to speed. The combination of growth rate, the demand for greater scale and complexity and the lack of skills will inevitably create associated risk.

It is when the question of security is raised that causes most debate. In addition to rapid uptake, limited understanding of the technology or lack of clearly defined ownership responsibility and the swiftness with which a virtual environment can tear up and tear down, most virtual environments will be less secure than the physical environments they replaced. The impact on the traditional IT operation is worth watching.

It would be a keen point for discussion to suggest that the arrival of widespread virtualisation usage is comparable in security terms to the impact of the introduction of networking as a common business initiative a few decades ago. It certainly does work and has multiple benefits but what and where are the risks?

From a corporate governance and internal auditing perspective things haven't changed too much and the traditional in-house IT auditing tools may change or adapt but the real question is what do you need to look for?

The following are some commonly discussed top security concerns with virtualisation (sources; www.cio.com and www.isaca.org)

1. Risk Assessment & managing oversight and responsibility

Understand the peculiar and particular risks associated with virtualisation and its impacts upon the enterprise. The main concerns are how IT resources are separated and aggregated in a virtual environment, and how the virtual environment security is managed.

Risk assessment is the first step in that process and the risk analysis should reflect an understanding of the risks inherent when considering a virtual environment and the potential for impact upon the existing environment and its associated security controls. Business continuity is a prime example.

Unlike physical servers, which are the direct responsibility of the data-centre operations or IT managers in whose physical domain they sit, responsibility for virtual servers is often left up in the air.

Clearly defined roles and responsibilities for virtual instances within the asset register should help resolve some of the ownership issues. As mentioned before the physical environment has changed but the applications and operating systems remain.

2. Patching and maintenance

The most tangible risk that can come out of a lack of responsibility is the failure to keep up with the constant, labour-intensive process of patching, maintaining and securing each virtual instance in a company. Unlike the physical servers on which they sit, which are usually managed and configured by assigned owners who also install the latest patches, virtual machines tend to be launched from images that may have been created, configured and patched weeks or months before.

Most companies maintain a small number of standard baseline images from which to launch or relaunch new virtual machines for a variety purposes. They may also keep many server images stored on an array of storage media after being laboriously configured to support specific applications or business requirements. How that media is handled and their associated security controls is also something else that would require some scrutiny.

Both Microsoft and VMware supply patch-management schedules with their base infrastructure products. Both require disk images stored in libraries to be launched periodically so they can be patched.

In addition to verifying the validity of the patch management process this begs obvious questions about procedures for keeping up to date images and are they securely hardened in keeping with a specific best practice or even regulatory compliance and how that process is managed?

3. Visibility, compliance and effective Access Controls

Virtual servers are designed to be, if not invisible, then at least very low profile, at least within the data centre. All the storage or bandwidth or floor space or electricity they need comes from the physical server on which they sit. To data-centre managers not specifically tasked with monitoring all the minute interactions of the VMs inside each host, a set of virtual servers becomes an invisible network within which there are few controls.

Check for best practices or controls for traffic from one server to other servers, and from server to external devices. Also, evaluate the sufficiency of controls such as a (virtual) firewall and (virtualised) intrusion detection system, where applicable. A developing best practice is to exclude the use of virtualisation in the DMZ (the layer between the Internet and the entity's LAN).

The fact that several partitions normally are physically located on a single server increases the risk of malicious activities. In a "regular" host/server of the past, if an attack occurred, it would normally be restricted to the data on that machine. In virtualisation, an attack could penetrate several different databases located on various VMs on the host machine. Thus, the risk of malicious attack in virtualisation is greater due to scope.

The same is true about administrative access to the host machine. Because administrative (admin) rights could affect all partitions, the management console needs to have tight access controls, locked down to specific users and specific partitions or machines. Once access is gained, the person with admin rights could gain access to any of the databases or applications in any of the several partitions. A typical mistake in virtualisation management is to allow too much access to users, for example, a developer given admin rights to a virtual partition.

Segregation in networks and virtualisation instances would need to be controlled and those controls must be rigorously and regularly tested. In addition the access control policies need to be robust and strictly adhered to.

4. VM sprawl and Change Management

Another consequence of the lack of oversight of virtual machines is sprawl—the uncontrolled proliferation of virtual machines launched, and often forgotten, by IT managers, developers or business-unit managers who want extra servers for some specific purpose, and lose track of them later.

This may be particularly tricky to spot given the lack of a singular and uniquely identifying physical entity.

The already mentioned ease of tear up and tear down for virtualisation is a real cause of concern when it comes to the change management. How is virtualisation managed within the identified change control process?

The understanding of the virtual environment and subsequent evaluation and testing of controls will likely focus on the network map. Determine where in the virtualisation world the following types of systems are located, if they exist:

Systems development

Systems testing (staging or sandbox environment)

Production systems (the larger the company, the more of these will exist)

Regional or remote business unit servers (if applicable)

Evaluate the completeness and accuracy of virtualisation documentation. For instance, evaluate/test change controls. In the virtualisation world, make sure the documents for change control being validated are from the right partition and on the right server. It is also necessary to know with certainty how to determine completeness and accuracy of the change documentation.

The bottom line is that a mechanism must exist to be able to evaluate the process of creating, deploying, managing and making changes to virtual machines.

5. Managing Virtual Appliances

A primary concern is that of the management console. Best practice calls for management tools to run on a separate network. Such a configuration has the potential to prevent VMs from prying into the console communications with which it is trying to control the VM.

A similar best practice is the hypervisor, the software tool that houses the VM servers. There is an embedded type of hypervisor that comes with the physical VM and is not part of a general purpose operating system. VMware's embedded hypervisor is only 32 MB (skinny by comparison; and the smaller the code, the safer it is from breaches). This, combined with the fact that it is not part of an operating system, increases the security of the hypervisor

One of the very best things about virtual infrastructures is the ability to buy or test a product from a third-party vendor and have it up and running in minutes, rather than having to clear space on a test server, install the software, get it to talk to the operating system and the network and then, hours later, see whether it does what it's supposed to.

There is an operating system and application in every package, each one with its own configuration and patch status and you have no idea what's in there or who's going to maintain it or what the long-term risk is going to be. It has a full application and operating system all configured and ready to run. In five minutes you can try out that new anti-spam server. But what operating system is in the package and is it patched, and if not, who is going to give you the patch?

Conclusion

Much of what currently exists for corporate governance, compliance and auditing can work in virtualisation. What is important is to apply what already works effectively in the traditional physical environment. Use specific analysis and give careful consideration to the peculiarities of the virtual environment not forgetting collection of evidence and assurance regarding controls over those unique aspects of virtualisation. Become aware of best practices in virtualisation using the many easily accessible and readily available sources of information. Without introducing too much unnecessary complexity and using basic and existing techniques, adapting and applying them to the special circumstances of the virtualisation world, the same quality of security will replicate that of the physical environment.