Virtualisation

This may seem a strange topic for the Security Watch article. Many vendors are pitching server virtualisation technologies such as EMC's VMWare and Microsoft's Virtual PC/Server as the answer to server room sprawl.

The basic principle behind virtualisation is that you can install software on a server that will permit the installation of other operating systems on the same server. They can all co-exist and run at the same time and the virtualisation software allows each guest operating system think that it is the only one on the physical server. The virtualisation software can automatically allocate resources such as memory, processor time and disk space as the guest operating system requests it.

Server room managers have realised that many of their servers installed for specific application delivery are spending the majority of their time idling. This is extremely inefficient on a number of levels. Real estate for computer rooms is expensive, especially in city centre locations. The physical footprint of these sprawling servers can be greatly reduced through the use of virtualisation. In an era where the "power of one" is the motto of any eco-sensitive person, the thought of servers running at idle most of the time and still consuming vast amounts of electricity and generating significant amounts of heat is disheartening.

Where virtualisation becomes attractive from a security perspective is the power it offers teams that are responsible for the operational availability of the services being offered. It is a very simple process to take a snapshot of a running virtual machine and save it as a backup. This set of files that make up a virtual machine can now be transferred to another server that has the virtualisation software installed and the server can be started up. With some vendors, there are free "players" available for this task. This copy of the primary server can now have security and other patches applied in an offline manner and tested. There are no concerns over hardware compatibility etc as the virtualisation software handles all of that. Once basic system testing has been performed on the copy of the application server, another snapshot can be taken of the primary as a rollback point and the patches applied as necessary. Any issues discovered as a result of the patching can be overcome by rolling back to the snapshot.

This sounds very straightforward, and it is. For too long, the security teams in most organisations have been recommending that new operating system patches, application server patches or general software patches are installed as soon as possible after release. However, those personnel with operational responsibility for the availability of application servers would fiercely resist this. This was due to the workload it entails for creating exact replica servers for testing and the problems with rollback in the event of a problem. This often meant that no patching took place and the risk profile of the organisation grew.

In this era of ever increasing threats and exploits for published vulnerabilities, running a data centre, or any server operation, without an operational and active patching policy is bordering on the negligent. If there is a breach of security as a result of not patching, it must surely be viewed in the same light as getting in to a car and being injured in a car crash as a result of not wearing your seatbelt. The crash in this instance is caused by a fault the manufacturer had warned you about and had offered free replacement of the faulty component but you never took them up on their offer to replace the faulty item.

Virtualisation technology offers huge advantages to the server room/data centre managers, and for one of the first times, offers the security team in any organisation an assist in the play for aggressive patch deployment.

From a security perspective, there are differences between the two main environments outlined above. While these are the two main products in the Intel server environment, there are others but with lower market presence. One of the biggest design differences between the two is that of the host operating system. With Microsoft Virtual Server, the general purpose Windows Server operating system acts as the host. That means it too must be patched at the frequency that the guest Windows operating systems must be patched. With the VMWare ESX Server, the host operating system is actually a proprietary kernel based on the SIM OS from Stanford University. This thin operating system means that the ESX Server rarely has to be patched or updated when compared to the Microsoft Windows Server operating systems.

Another attraction from a security and operational perspective is the benefit gained in the Disaster Recovery or Business Continuity Planning area. It is very easy to create virtual server hosting environment in another location and move the virtual machines between them and not have to worry about hardware compatibility issues etc.

While server virtualisation offers many benefits to us for server patching and DR/BCP roles, it will only be effective where an organisation has implemented strong policies and procedures around the operation of the environment. However, it is still a major step forward!

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com