# Security and virtualization

The virtualization world is taking many steps forward, organizations have seen many compelling reasons for virtualization: coefficients like unified servers, electricity bills, hardware faster and easy to use, ... made the calculation

***Ricky M. Magalhaes***

**The virtualization world is taking many steps forward, organizations have seen many compelling reasons for virtualization: coefficients like unified servers, electricity bills, hardware faster and easy to use, . has made virtual computing more attractive than ever.**

In some virtualization organizations have become a big part of infrastructure. Once again technology is ahead of the best security practices.

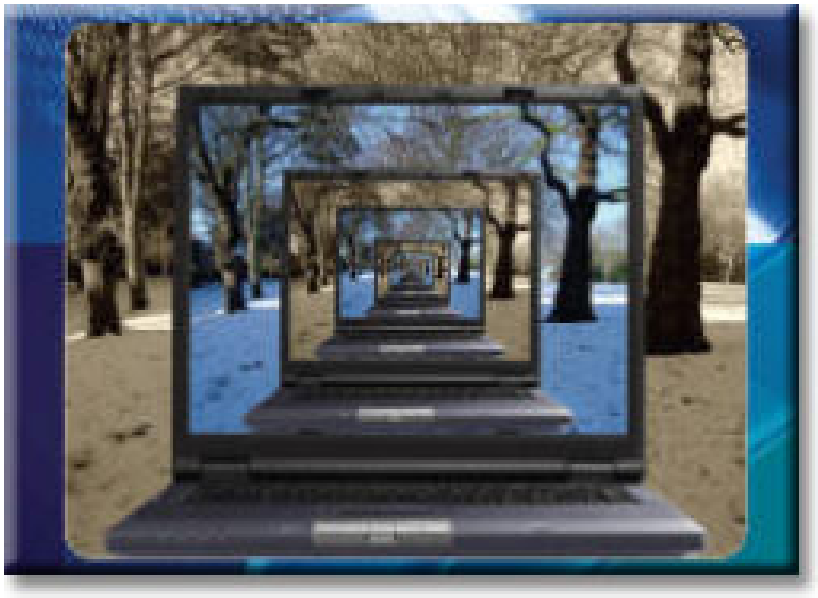
Virtualization environments will gradually become more popular as business solutions are continuous and disaster recovery, typically in the financial sector. This is perfectly appropriate because some of these solutions are in a 'direct sell' environment and are often overlooked during security and upgrade protection.

**Pitfalls when working with virtual environments**

1. If the host is compromised, it may affect the client that the server has configured on the primary host.
2. If the virtual network is compromised, the client is compromised.
3. Client sharing and host sharing need to be protected because shares can be exploited in both cases. The potential risk may result in files being copied to the shared folder filling up the disk.
4. If the host has a problem, all virtual machines will stop working.
5. Virtual machines often merge into level two machines when they have the same characteristics and perform the same way for physical machines. In the next few years there will be some differences between virtual machines and physical machines.
6. Minimal privilege is a technique that seems to be forgotten when it comes to virtualization. This technique reduces the attack surface and should be used in both virtual and physical environments.

**These can be done to better protect the virtual server environment**

1. Upgrade operating systems and applications; This should be done on all virtual machines and on hosts. Master applications need to be kept to a minimum, just need to install things that are really needed.
2. Firewall between virtual computers together, this will isolate the virtual machine and ensure that only authorized procedures can be performed.

3. 

   Separating servers from each other and with the host: Isolation should be considered in each way if possible.

4. Installing and upgrading antivirus software on virtual computers and hosts, virtual computers can also be infected with viruses and worms like physical machines.
5. Using IPSEC or strong encryption between hosts and virtual computers: traffic between virtual machines and hosts can be adjusted. The best action is that communication between machines needs to be encrypted.
6. Without browsing the Internet from host machines, spyware and malware can still be infected on host machines. You need to remember that host machines that manage virtual machines and problems appear on Virtual Machine Host can also lead to serious problems and service losses.
7. Protecting Administrator and admin accounts on the host machine: accessing high-level accounts by unauthorized users can lead to significant security holes. Research has shown that the Administrator (root) account on the host machine is much less secure than the virtual machine or the computer accounts and passwords in the physical network.
8. Fix the host operating system and stop or disable unnecessary services. Keep the operating system compact to ensure that the attack surface area is minimized.
9. Turn off unused virtual machines if you don't really need it.
10. Tighten virtual machines into an enterprise security policy even if they are virtual machines.
11. Protecting host machines to ensure that virtual machines are offline so that unauthorized users cannot interfere with the files of these virtual machines.
12. The solution to isolate processes like the Hyper Visor implementation type is also good, these systems are further isolated, the environment will be better protected.
13. Make sure that the host drivers are upgraded: this will ensure that the hardware runs at the optimum speed but more importantly, the latest software upgrade will ensure that the old driver software errors are compromised. Bad exploits are patched promptly.
14. Disable hardware port technology for each virtual machine if not used: technologies such as USB should be disabled for each virtual machine if the VM environment does not use port technology.
15. Check event logs and security events on both host and virtual machines. Testing is often overlooked in virtual machine environments, the reason may be related to host-based testing performed by virtual software. These records need to be stored in a record store so that they are safe and audited later.

16. In the future, opting to store flash technology for hyper visor software, magnetic media will not only have a certain shelf life but will also include security holes.
17. Limit and reduce the sharing of hardware resources. Security and resource sharing should not go concurrently. Data loophole is one of the few problems but DoS can appear when resources are shared and locked by switching to virtual machines. Because virtual machines share CPUs, RAM, hard drives, and other resources, we need to manage this resource carefully to ensure availability of services.
18. Ensure the network interface card is dedicated to each virtual machine. This can alleviate resource sharing issues, ensuring that traffic is intended and that organization from a virtual machine has some isolation.
19. Investing in hardware is suitable for the purpose and that is the knowledge of virtual machines. Hardware not built to support virtual machines is not good.
20. Partition creates disk boundaries that can be used to isolate and secure each virtual machine on its dedicated partition. If a virtual machine goes beyond the usual limits, dedicated partitions limit the impact on other virtual machines.
21. Ensure that virtual machines do not connect to each other if they do not need to connect. Network isolation is an important issue introduced above. With these virtual machines communication should use a private network card on a different network address range, which is a safer way of pushing the traffic between virtual machines on the exposed network.
22. Manage remote access to virtual machines and especially to host machines.
23. Remember that host machines represent a single point of failure, technologies such as replication and continuity will help reduce risks.
24. Avoid sharing IP addresses.

We need to assume that virtualization technology is not as simple as previously thought and security for it is a really necessary job; In addition, this technology shows many new challenges that need to be addressed.