Securing Virtualised Environments

Focus on the Fundamentals

Making tangible commercial gains through the use of technology can be a highly effective business strategy. Virtualisation of ICT infrastructure has been one of the more recent strategies to achieve solid gains from your technology spend. Organisations of all sizes are either evaluating it or using it. Virtualisation of IT server infrastructure is now commonplace. Ask an ICT Services Provider; you can be guaranteed they are using virtualisation to some extent to deliver services to their clients.

The business benefits supporting virtualisation are numerous; they include:

- Less Environmental Impact (Green IT) – The replacement of many physical systems (the traditional model) into fewer platforms running multiple virtualised systems minimises energy consumption and your carbon footprint. The impact on the environment is further reduced due to the relatively fewer computing systems that would require disposal, and or recycling, at the end of their usable life;
- Lowering your cost of ownership – Doing more with less; consolidating IT systems into a virtualised environment can help reduce the financial overheads associated with acquiring platforms (i.e. servers and data storage) and services (i.e. application service delivery). Cost gains can also be realised by the relatively lower cost of deployment, maintenance and management;
- Providing business continuity and disaster recovery – High levels of IT service delivery & business continuity is arguably far easier to achieve using virtualised systems.
- Simplified Service Delivery - Software-as-a-Service providers are using virtualised environments to deliver applications to multiple clients over the Internet. The service model employs a build-one, serve-many capability meaning you can acquire on-demand applications as your organisation requires. This is the basis of the cloud computing phenomenon; it can significantly reduce your procurement timeline.

What's the catch?

Put simply, the security of information assets is often overlooked during the planning and deployment stages of a virtualisation program. According to a report prepared by research company Gartner they believe in five years that virtualised systems likely will be more secure than their physical counterparts, but until then, it will be rough sledding for organisations transitioning to the new technology.

Furthermore Gartner research indicates that, at YE09, only 18% of enterprise data centre workloads that could be virtualised had been virtualised, with the number growing to more than 50% by YE12. As more and more workloads are virtualised, as workloads of different trust levels are combined and as virtualised workloads become more mobile, the security issues associated with virtualisation become more critical to address.

The question we should be asking ourselves at the conceptual stages of a virtualisation project is how I can deliver IT services, efficiently, cost effectively, and securely. Security within your virtualisation project can be achieved if you focus on the security fundamentals of confidentiality, integrity, and availability.

A game plan based on security fundamentals

Confidentiality – A significant benefit of virtualised environments is that they consolidate services onto fewer systems than their physical counterparts. If this is not achieved in a secure manner and one virtual system is vulnerable to attack it may result in all virtualised systems on that platform also falling victim to malicious activity. This potential scenario needs to be thought through at the planning stages. Consider how to enforce segregation between various systems and between entities.

It is not recommended to have a virtualised platform bridging two distinct zones of trust. For example, internet facing systems such as email gateways or remote access entry points (lower trust) should not be virtualised on the same system where internal systems are resident such as payroll or HR (higher trust).

Similarly, if you have systems hosted at a service provider in a multi-tenant environment (multiple distinct entities on a single platform) your service provider must have the capability to keep the entities isolated which is not a trivial task in shared infrastructure.

Policies and procedures need to be developed to not only govern what virtualised systems should cohabit on a given platform but they should also consider who should have the administrative access rights to the wealth of information maintained within the consolidated virtual environment. Do you have sound governance to address this matter? Can your internal IT team or third party service provider demonstrate how polices and procedures segregate systems and protect the confidently of your information assets? If your answer to the above question(s) is no then it is highly recommended that you consult with your information security advisor to prepare a set of standards designed to protect the confidentiality of your information assets.

Integrity – Virtualised systems are no different from their physical counterparts in respect to ongoing security maintenance. Your enterprise wide patch management framework should also extend to your virtualised environment including the new technology that has been introduced - the virtualisation layer. Virtualised systems that are not patched systematically are far more likely to fall victim to a security breach which could potentially lead to loss of data bringing into question the integrity of the entire virtualised

environment. The issue here is not a technology issue per se; the issue is caused by a lack of planning and implementing appropriate patch management practices. It is essential that your internal IT team or service provider demonstrate how their patch management practice will service your virtualisation environment.

The notion of integrity also relates to the personnel that have administrative access rights to alter security controls and data on virtualised systems. By collapsing physical systems into virtualised environments many of the traditional administrative roles and responsibilities have become blurred. Virtualisation projects, if managed incorrectly, can introduce significant security blind spots; the administrative checks and balances may have dissolved due to the lack of defined demarcation points. Make sure that you have appropriate role based access controls (RBAC) to protect the integrity of systems and data in your virtualised environment.

Defining and implementing a suitable RBAC framework needs to be complemented with appropriate audit procedures. If the virtualised systems are implemented by your internal IT team you will need to invest in tools that log all activity across all layers. Of course the procedures to undertake audits need to be defined, including assigning personnel to perform the task. Clearly the same personnel maintaining the systems should not also audit the systems; segregation of duties needs to be established. If you are using an ICT service provider they need to be able to demonstrate their own RBAC framework and audit procedures. It is recommended that service providers use third party auditors to assess their procedures and environment.

Availability – One of the great selling points for virtualised systems, regardless if they are delivered by your internal IT organisation or a service provider, is the redundancy capabilities inherent in the technology. That said, appropriate process and procedures are needed to ensure the availability of virtualised systems and services.

Your patch management practices also have a role to play here; a breach of security caused by a lack of system maintenance could cause disruption to service availability and loss of data. The patch management program needs to extend to dormant systems to aid in the availability of service(s).

It is critical that practices and procedures are defined to cater for planned and unplanned system downtime; the potential implications for ignoring this can be devastating.

Summary

Remember virtualisation is simply the platform enabler. It is not inherently insecure but it is often deployed and managed in an insecure manner due to lack of planning, skills, procedures, and tools. Establish your virtualisation plan well ahead of deployment and make sure the project includes stakeholders from your information security team who are fully conversant in the principles of information security.

If you intend to outsource to an ICT service provider it is only reasonable that they can demonstrate that their infrastructure and delivery platforms have well defined information security measures and controls. It is essential that you have the ability to audit their service based on the agreed security principles and a frequency that meets your business needs. Build this into your service agreement before you sign the contract.

Sense of Security is a leading independent provider of IT security and risk management consulting services, with expertise in assessment and assurance, as well as strategy and architecture, through to deployment and ongoing management. Sense of Security's consultants are information security experts with a thorough knowledge and understanding of the technical, commercial, and regulatory requirements of information and communications technology (ICT) security. For more information on Sense of Security services visit www.senseofsecurity.com.au