Get the basics right, secure the servers

Servers lie at the heart of every organisation's ICT infrastructure. Servers run the business critical applications: the core databases, the web sites, and the line of business applications. Servers run the services that support system management, user authentication and authorisation, central security and log management applications.

Servers are therefore the foundation on which every ICT infrastructure is built.

Correctly configured servers save you money by helping prevent security and operations incidents, a far cheaper option than recovering after an incident has occurred. And when incidents do occur, it is vital to have the correct information available to facilitate full forensic investigation.

Configuring servers in compliance with appropriate guidelines, regulations, frameworks and policies is the key to protecting your ICT Infrastructure, and all the information it contains. Correctly configured and continuously monitored servers help to create an effective and efficient ICT operation.

Increasingly, the ability in ICT to achieve and demonstrate compliance to regulations, legislation, IT frameworks and best practice guides is essential. For many organisations in both the public and private sectors, ICT is subject to rigorous internal and external audit. Other organisations are subject to self certifying industry regulations such as the PCI DSS. Demonstrable Governance of ICT operations is important in many sectors that are subject to external regulation and control.

Business operation today often demands the interconnection of diverse business units and geographic locations, both within the organisation and across organisational boundaries. This widespread interconnectedness increases the need for secure ICT infrastructures.

Typical challenges faced by those responsible for managing servers include:

- Verification that appropriate controls have been set, are configured correctly and are being monitored.
- Confirmation that servers are configured in line with internal and external security policy, and operational requirements.
- Confirmation that servers are up to date, with applications and system patches to a 'known state'.
- Collection of audit trails for audit inspection and forensic investigation.

For most organisations, managing the ICT infrastructure can be a major challenge without the right tools, no matter how competent their ICT staff. For some organisations the solution is to outsource their entire ICT operation or parts of the operation. A more effective alternative is to use automated tools such as those provided by Assuria.

Get the basics right, secure the servers

Assuria solutions are designed to address many of the challenges when managing the core IT servers. Relatively simple tasks such as correctly configuring a server to implement security controls are a key first step in creating a secure and efficient environment. Unfortunately, this is a step that is often overlooked but, with Assuria Auditor to help, secure server configurations can be easily achieved.

Assuria Auditor deep scans servers, performing thousands of checks on each system. Once scanned, the results can be analysed and reports generated to provide vulnerability assessment, configuration assurance, policy compliance and other vital system information. Change detection features allow easy monitoring and reporting of potentially harmful or unauthorised system changes. Assuria Auditor is available for Windows, Unix, Linux and VMware ESX systems.

Assuria Auditor provides preventative security, operating unobtrusively from the inside, as opposed to the techniques of external network scanning or penetration testing. Such credentialised configuration examination is essential for protection of important information assets, to ensure compliance to security policy and standards and to enable investigation of changes.

Assuria Log Manager ensures the integrity and continuity of audit log data by collecting the audit logs from enterprise wide systems into a central point, in a secure and forensically sound way. The collected logs can be used for analysis and management reporting. With Assuria Log Manager the original logs are always available for forensic investigation or even evidential use.

Assuria Log Manager provides the audit conformation that server security controls are indeed working. For the auditors, Assuria Log Manager provides full audit trails from operating systems, databases, network devices, websites and applications.

Assuria Auditor and Assuria Log Manager are easy to use enterprise class tools that help to create a secure foundation on which to build the secure ICT infrastructure.

To find out more about Assuria products please contact Assuria or visit http://www.assuria.com.

Assuria Limited
Science & Technology Centre,
The University of Reading,
Earley Gate,
Reading,
RG6 6BZ
United Kingdom.