Back-up protocols often ignore security devices

Submitted by: Maillot Jaune Communications
Tuesday, 3 April 2012

Reading, Berkshire – Osirium (www.osirium.com) a leader in Privileged User & Infrastructure Management has today warned organisations to carefully review back up policies that extend beyond file servers and user access devices.

Uncovered during research conducted by QuoCirca, for Osirium, the lack of back-up processes associated with security devices became quickly apparent. The study found that in around 50% of organisations, such devices do not get backed up weekly, and fewer than 30% ran back-ups daily. It was also found that device problems would often take hours to get them functioning again, particularly if the system administrator needed to rebuild the device using out of date settings or, in the worst case, from scratch.

“The risk value of backing up these devices should not be under-estimated,” said David Guyatt, CEO at Osirium. “Firewalls often have complex rules programmed into them whilst content filtering devices contain policies about what users can and cannot do with content, so the operational risk from losing these security services without any reliable backup and restore process escalates considerably.

Most organisations use a wide range of security devices from an equally wide range of network and security vendors, so the issue in question perhaps becomes more about managing the many different back-up protocols associated with each vendor device because they’re often seen as complex, costly and resource intensive. Organisations often don’t allocate sufficient budget to manage this adequately, which was further reflected in the research statistic that 42% of organisations have 30 day gaps between backing-up security devices”.

Whilst organisations do try to backup critical devices and servers at regular intervals these are often conducted under excessive workloads. Back-up goals get compromised so critical servers become a priority whilst back-ups on the less obvious, but just as important infrastructure devices, are often delayed, Guyatt continued, “Rather than having a specific backup up process in place for each device Osirium offers a single interface, multi-vendor solution that automates these back-ups across a wide range of products to bring control back within the organisation.”

Specifically, Osirium allows organisations to schedule, or select, individual device configuration back-ups and automatically scale the task across multi-vendor infrastructures as well as running back-ups before and after configuration changes, to provide ’roll-back’ services. Furthermore, Osirium can also delegate backup initiatives to other parties, such as help desks, which allows them to execute back-ups without needing full system administrator access.

About the Research
The research was completed by Quocirca and 100 interviews were collected. At the time of answering the questions, those surveyed were not aware that the research was being conducted on behalf of Osirium. Respondents were qualified in as follows:
- Must be involved in IT management with one of the following job functions: IT manager, IT security manager, IT infrastructure manager

- Must answer yes to: “are you involved with, or knowledgeable in how your organisation views and manages issues relating to privileged users (that is how the granting of the extra privileges that IT administrators require to do their jobs is controlled), the automation of IT admin tasks and how these issues relate to your organisation’s ability to meet the regulatory requirements that govern it?”

About Osirium
Osirium drives down operational risk and eases the pain of managing and maintaining multi-vendor IT infrastructures by providing a central, secure access point and a “built-in” best practice foundation which tracks all SysAdmin changes in the infrastructure and allows you to easily meet and maintain compliance.

Osirium dramatically improves productivity and reduces human error by automating routine and repetitive SysAdmin tasks and delegating them to less costly help desk staff, to provide faster problem resolutions with fewer errors.
Osirium is establishing itself as a new and unique IT infrastructure security solution and is already helping some of the world’s biggest brands and public sector bodies.

For more information please see: www.osirium.com

Media contact:
Clare Shephard
maillot jaune communications
tel: 07736 793332
eml: clare.shephard@maillot-jaune.co.uk

Osirium contact:
Andre Armstrong
tel: 0118 324 2444
eml: andre.armstrong@osirium.com