Orthus releases “100,000 Hours” Data Leakage Survey Results

Submitted by: Orthus Ltd
Wednesday, 28 November 2007

LONDON, UNITED KINGDOM, - November 28 2007 - Orthus Limited today published the results from monitoring over 100,000 hours of user activity captured through the delivery of their unique Data Leakage Audit Service.

Surveys completed in the last 12 months have looked in detail into the ways in which internal users access, process, store and transmit sensitive information including personal information, financial information, product roadmap and future product detail, contracts, pricing information and HR records.

The findings from the survey showed that every organisation without exception had suffered multiple instances of data leakage – many of them serious and potentially very damaging. The results clearly show that the threat from within is both real and continues to be overlooked. Trusted users are the most likely to be the source of information leaks.

The analysis of 100,000 hours of user activity pinpoints exactly who, where, when and how critical information assets are removed from the infrastructure and demonstrated that the real problem – and the solution – is all about the user.

Key results from the survey showed:

* Corporate data leakage was most likely to occur through mobile devices with 68% of all events identified linked to mobile rather than fixed desktop systems.
* Information Technology and Customer Services Departments had the highest incidence of data leakage.
* Most incidents of data leakage occur during the extended working day (7-7 Monday to Friday).
* The applications most favoured by users to remove sensitive data were identified as web mail, instant messaging (IM) and social networking web sites.
* The top 4 data leakage vectors were identified as mobile devices, web mail, removable media and corporate email.
* All data leakage incidents identified could have been prevented. Existing corporate security policies were not implemented, monitored or enforced.

Richard Hollis, Managing Director of Orthus said “Companies continue to try and protect information by protecting the architecture deploying devices to protect devices. They neglect the protection of data”.

Richard went on to say “Until organisations accept that the majority of losses are associated with authorised users and implement the necessary controls where they are effective – between the user and the information itself – these losses will continue”.

The analysis of user interaction with critical information is accomplished through the deployment of software agents on endpoints, servers and terminal servers. The software visually records suspicious or inappropriate actions. Is information sent or copied to an unauthorised device (such as a PDA, MP3 player, USB flash drive or mobile phone)? Is it uploaded or transferred through an unauthorised

application (IM or social networking sites)?

The software enables the identification of information loss through virtually every vector available to the user.

Each audit is customised to include keywords and phrases specific to the target organisation, as well as a list of files folders and shares containing particularly sensitive information.

About Orthus Limited: Orthus is a leading provider of innovative and independent information security services and solutions. Since its foundation in 2001 Orthus has grown to become one of the leading UK-based providers of security services assisting enterprises in protecting their digital information assets globally.

For more information, or for a copy of the full survey results, please contact Orthus, 31 Southampton Row, London WC1B 5HJ. Tel: +44 (0)203 170 8955 or email info@orthus.com