

Publication	It-analysis.com
Date	6 th May 2009
Circulation	Unclassified



UK companies are still in the dark when securing their networks, says Redstone Managed Solutions

Companies are doing it right on paper but, in reality, there are holes in the process.

Infosecurity 2009, London, UK: Only a fifth of UK organisations are prioritising vulnerability assessments as their key security focus for 2009, while admitting that their biggest security threat is from internal sources, reveals a survey by Redstone Managed Solutions.

Although 76% of organisations include their IT security policy in staff inductions, half of them only review it once a year. A quarter of organisations review it twice a year, and the remaining quarter only sporadically.

Martin Blackhurst, product manager, Redstone Managed Solutions, explains: "Without ongoing review, companies expose themselves to vulnerability for attacks on their IT networks. Audit work is unavoidable to ensure that security policies and practices are effective, and should cover data location through to what should be encrypted and how.

"Companies are still learning or, more likely, are still are not aware of all of the routes via which they become vulnerable and information can slip out. One way of counteracting this is to use technology to prevent emailing, printing, and copy and pasting information."

The most common form of attack (63%) on IT networks in the past 12 months came from infection through e-mail and malicious code from websites visited by staff. Hackers infect the web content of sites visited by companies in the course of business, such as banks and suppliers. When a member of staff visits such a site, they could be at risk of infected code planted in graphics being transferred to their company's network.

Redstone Managed Solutions believes that few companies take active steps to protect themselves from this type of infection. Many e-mails contain graphics such as logos and links to the sender's website. Businesses should arm themselves with web and email protection at the perimeter, or use hosted / managed services to ensure the threat is removed long before it hits the corporate network. Continued vulnerability assessment should also be employed to provide a clear view of their threat landscape, allowing management of risk by patching, or mitigating the risk by using Intrusion Prevention Systems, Intrusion Detection Systems or Host-based Intrusion Prevention System technologies.

Blackhurst advises, "Taking a tiered approach to protection can give an additional layer of back-up in the event of one supplier's solution becoming out of date or unable to guard against a new threat."

The survey also found that only 25% of organisations regard business continuity as the dominant theme shaping their approach to information security this year, despite the added importance of keeping operations running smoothly through the current economic climate.

"The evolution from the physical to the digital world has transformed the security landscape, with attacks becoming more frequent and sophisticated," said Blackhurst, adding, "It is alarming that good intentions can be rolled out in a piecemeal fashion and ultimately lead to poor protection and wasted effort."

