

Publication	telehrphbusinessclub.co.uk
Date	1 st May 2009
Circulation	12,500,000

The Telegraph BUSINESSCLUB

Securing new frontiers

The web has undeniably become an integral part of life, for individuals and for businesses. The vast majority of an organisation's transactions are web-based at some point. Infection by malicious code passed on through websites has become one of the newest and most rapidly growing security threats to web browsing, taking advantage of businesses whose sites are not secure.

Criminals hack into websites, such as bank or supplier websites, visited legitimately and trustingly by companies every day. Once in the site, hackers infect the web content and plant malware in ways such as adding extra boxes or populated graphics. When a user subsequently visits the site, they could be vulnerable to infected code being transferred from a trusted website that has been turned into a harmful portal.

The growth of Web 2.0 platforms makes the potential to pass on malware even easier by people becoming desensitized to running active code within browsers, such as the ability within social networking sites to throw virtual gifts at friends. Users are therefore less likely to spot any odd 'site behaviour'.

Research has found that 44pc of SMEs have become victims of cyber crime, losing revenues estimated at £750m each year. Six out of ten businesses have admitted they could not continue if their IT systems fail.

Therefore, why do so few businesses actively protect their own browsers from malware? While businesses are right to have virus protection on desktops and e-mail systems, most e-mail content comes from the web in the form of embedded graphics such as logos and signatures and URL links back to the originator's website.

Once introduced to an IT system from the web, an attack of infected code could spread through a company's infrastructure, potentially crippling the company and infecting its customers and partners. This can lead to bad PR, poor financial performance, loss of time and business continuity and possible legal action over liability. Current economic circumstances make it all the more important that businesses avoid anything that could disrupt their operations, reputation or customer service.

It is vital that companies conduct continual vulnerability assessments to ensure they are aware of their threat landscape across all systems and services. Businesses armed with this information are much better placed to act on managing risk either by patching, or mitigating the risk by providing protection in terms of IPS (Intrusion Prevention System)/IDS (Intrusion Detection System) or HIPS (Host-based Intrusion Prevention System) technologies.





Security breaches hand hackers and cybercriminals the opportunity to launch many flavours of malware into a company's infrastructure. The last thing any business wants is to be used as a platform for spreading spam and viruses without their knowledge.

A tiered level of protection should also be implemented. It may not necessarily be good practice to have malware detection and protection from the same provider throughout the whole company. This provides a level of back-up in the case of one solution either not being up to date, or not having protection against a certain threat. After all, not every vendor can be first in delivering protection against new threats.

Companies need advice and guidance with regard to their IT security infrastructure and should approach it with a firm focus on risk management rather than just throwing product at an unknown and hoping some of it will stick. An uncoordinated approach will generally lead to poor protection and wasted time in managing an ineffective solution.

By Martin Blackhurst

Product Manager, Redstone Managed Solutions.

