Helping to protect businesses from security threats delivered via the Web

IBM Express Managed Security Services for Web security

Highlights

- ***Helps protect IT investments and productivity from Web-based threats***
- ***Scans Web traffic for viruses and spyware and helps stop them before they reach your corporate network***
- ***Helps enforce Internet usage policies by blocking access to inappropriate Web sites***
- ***Provides a hosted solution designed to offer better protection at a lower total cost of ownership (TCO)***

Facing increasingly sophisticated threats to your business

Your e-mail may be protected against viruses and spyware, but is your Web access as secure as it can be?

Businesses and individuals that use the Internet are facing a significant shift in the nature of security threats. While e-mail is still the most common way that attackers attempt to deliver viruses and spyware, it is now more secure than in the past. This is likely due to two factors: better tools are available for identifying and neutralising threats; and users are more aware of how to handle e-mails containing suspicious attachments.

In response to this greater e-mail security, virus and spyware developers are increasingly exploiting Web-browsing applications as a delivery method. Aided by the unrestricted Web surfing of many business users and driven by potential financial gain from stealing personal information and intellectual property, the hackers and virus writers are motivated, creative and relentless in their pursuit of new vulnerabilities.

Unlike e-mail threats, which typically target an individual machine and require some action by the user, Web security threats can launch sophisticated, coordinated attacks that require little, if any, user action. Spyware, adware and other malicious software often installs itself without the user's knowledge – leaving no trace, quietly collecting information and disrupting system performance. Once installed, the malicious software can be difficult to detect and remove, often reinstalling over and over again and disabling superflous security measures. Handling such an attack can cause a significant drain on any information technology (IT) department.

Unrestricted Web browsing by employees doesn't help. Smart businesses have Internet usage policies in place to curb unproductive surfing; but they often depend on employees acting in good faith. Yet various industry figures indicate that a significant percentage of all business Web activity is not

business related. And without any technical safeguards in place, even innocuous Web browsing can lead a user to inappropriate content or to Web sites that act as launching pads for installing malicious software.

Facing the challenges that these threats impose is difficult for any business, but especially for small and mid-size businesses that typically have limited resources. Because of the sophistication and constant evolution of the threats, and the numerous attack methods used, maintaining Web security often requires more resource dedication and focus than IT departments can provide.

Meeting Web security threats before they reach your network

The traditional approach to Web security has been to install security software at the desktop, or software and hardware appliances at the network edge. The main problem with these approaches is that they allow threats to reach your network – similar to leaving your front door open and hoping that burglars won't walk in.

Most traditional security solutions also are difficult to set up, monitor and maintain, requiring updates for virus and spyware definitions that can actually take your systems offline – slowing productivity and consuming precious IT support resources. Typically, they provide only limited protection against 'zero hour' outbreaks – new and undetected malicious software that can attack systems before virus definitions are updated. Traditional URL filtering approaches also have their shortcomings, often either overprotecting by blocking access to necessary sites or underprotecting by ignoring suspicious activities from seemingly harmless URLs.

The IBM Managed Security Services for Web security suite is designed to help protect your IT investments and productivity by reducing the threat of spyware and viruses delivered via Web-browsing – and by effectively enforcing corporate Internet usage policies by filtering access to inappropriate or potentially dangerous URLs. Part of the IBM Express Managed Services family, these Web security services were created specifically for mid-size business. And as hosted services, they require no investments in hardware or software and very little management on your part once established. They're priced per user, per month, so you can affordably scale your solution according to your needs.

The suite comprises four service options:

- *Anti-virus*
- *Anti-virus and anti-spyware*
- *URL filtering*
- *Anti-virus, anti-spyware and URL filtering.*

Helping to prevent viruses and spyware from reaching desktops

The anti-virus and anti-spyware services are designed to offer real-time scanning of your inbound and outbound Web traffic. Using virus-scanning engines and spyware, adware and phishing databases that we selected based on their accuracy, our services help provide a greater level of protection than can be offered by single vendor solutions – which are typically cost-prohibitive to build in house. IBM's anti-virus and anti-spyware services are designed to quickly analyse the content of a Web page or a file type request and determine if it is safe to pass on to the end user's browser. Unacceptable requests are quarantined and deleted.

The anti-virus and anti-spyware services do more than help protect your IT infrastructure against known threats; they also help safeguard against unidentified malicious activities. Using an advanced heuristic analysis,

the services are designed to improve their capabilities the more they work. They identify patterns of activity associated with threats, which helps them to prevent the 'zero-hour' attacks that have become increasingly prevalent. And since the services analyse Web threats outside of your network, the risk of those threats infecting your systems is virtually eliminated.

Additionally, because the services monitor outbound traffic as well, they can detect and prevent attempts to launch spyware and virus attacks from within your network – helping to protect your company and brand reputation. These comprehensive services are fully hosted and designed to operate with little involvement by your IT department – but you still retain a measure of control over your service. A Web-based administrative interface allows you to set your own preferences – permitting non-invasive adware, for example – as well as to establish alerts and reporting features.

Allowing safeguarded, controlled Internet access

The IBM Managed Security Services for Web security – URL filtering service assists you in enforcing Internet usage policies and helps ensure relevant regulatory and legislative compliance by monitoring and controlling the content that enters your network. It also helps to prevent accidental visits by business users to inappropriate sites. And it can help defeat phishing and spoofing techniques that may lead users to inadvertently reveal confidential information or install spyware.

The service is highly configurable and allows for various URL category- and content-based policies, giving you greater control while helping to protect your employees and your brand reputation. URL filtering can help you:

- *Enforce policies based on Multipurpose Internet Mail Extensions (MIME) file types to restrict broad content types, such as audio and video*
- *Enforce policies based on actual file types, such as MP3, MP4 and AAC*
- *Control access to more than 60 URL categories and block anonymous proxy services that reroute traffic to inappropriate destinations*
- *Block access to Web-based e-mail, which is usually not work related and can circumvent desktop anti-virus and anti-spyware software*
- *Restrict access to some sites during business hours and allow fewer restrictions after hours*
- *Configure the service with user- and group-level settings, using existing directory information.*

Unlike e-mail, for which a certain amount of delay is tolerable, efficient Web browsing for business purposes requires speed. The anti-virus, anti-spyware and URL filtering services are designed to monitor your Web traffic and redirect threats to IBM's security-rich infrastructure with no noticeable delay to the end user. Think of it as an extra 'hop' in the routing of your network traffic – the delay is measured in mere milliseconds, but the business benefits can be significant.

All the IBM Express Managed Security Services for Web security modules are accessible to administrators via a Web-based interface that is easy to use and enables you to modify services as needs change. And the services are designed to complement the IBM Express Managed Services for e-mail security solution.

Helping to lower the cost of securing your Web access

IBM Express Managed Security Services for Web security offers compelling potential business benefits. By identifying and removing threats before they reach your network, this enhanced level of protection helps you achieve business-critical goals:

- *Ensuring business continuity*
- *Improving employee productivity*
- *Protecting company information.*

Because they are hosted solutions, IBM's anti-virus, anti-spyware and URL filtering services help you to avoid additional investments in hardware and software – while improving the protection of your business, infrastructure and productivity. IBM Express Managed Security Services for Web security modules include IBM Help Desk services, plus access to the IBM Incident Response Team, which is ready to assist you in the unlikely event of a Web security breach.

Why IBM?

You can gain confidence and peace of mind by leveraging a service solution from IBM. Businesses worldwide trust IBM to develop security products and services that help meet tomorrow's security challenges today. With our world-class hosting facilities, security expertise and network of IBM Business Partners, we can help protect your business functions, company reputation and brand.

For more information

To find out more about IBM Express Managed Security Services for Web security, contact your IBM representative (or IBM Business Partner if applicable), or visit:

ibm.com/services

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU

Tel: 0870 010 2503
ibm.com/services/uk

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

Tel: 1890 200 392
ibm.com/services/ie

IBM South Africa Limited
Private Bag X9907
Sandhurst
2146
South Africa

Tel: 0860 700 777
ibm.com/services/za

UK company-wide registration to ISO9001.
Certificate number FM 92089.

The IBM home page can be found at **ibm.com**

ITSDUK6001-00 (02/06) PK (06-IGS-002074)