



The Next Generation of Managed Security Services

Contents

- 2 Introduction
- 2 An ounce of prevention
- 4 Selecting a Managed Security Services Partner
- 5 IBM ISS spells relief
- 7 At your service
- 7 Knowledge is power
- 8 Keeping safe and sound at a lower cost-of-ownership
- 9 Utility Provider Places Trust in IBM Internet Security Systems

Introduction

You have just polished off your morning latte when you get the call: a virus has brought your network to its knees. Your company is at a standstill. Customers and partners are getting bounced off your Web site, employees are taking extended coffee breaks, and reporters and angry shareholders are flooding the phone lines.

Contrary to popular belief, there is such a thing as bad publicity. No executive wants his or her business featured on the evening news because it succumbed to the latest Internet worm or Trojan horse. To protect critical systems, enterprises deploy a myriad of firewalls and gateway appliances, but these technologies are only effective at blocking access to certain systems. They cannot proactively monitor incoming network traffic or anticipate the source of the next attack.

An ounce of prevention

The need to act instead of react is the reason why the market for managed security service providers (MSSPs) is growing at such a rapid pace. Worldwide spending on managed security services is expected to eclipse \$4.8 billion by 2009* , according to analyst firm IDC. This surge in the popularity of MSSPs is largely based on the fact that companies simply cannot keep up with the escalating demands of information security. Enterprises today are locked in a continuing battle with online enemies that are smart and destructive, and can strike at any moment.

Given the wide variety of threats that businesses face—from viruses to denial of service attacks to unauthorized Web site access, it comes as no surprise that companies managing their own information security often fall short of the in-house resources needed to protect online systems 24x7x365. Sophisticated security requires highly-skilled personnel who are often expensive to recruit, hire and retain: a challenging problem for firms with limited IT budgets.



The price of un-preparedness is even higher. According to a recent Computer Security Institute/FBI Computer Crime and Security Survey of 313 companies, virus contamination and unauthorized access to information accounted for the most dollars lost—\$26.3 billion in 2006* . Even those organizations that can afford ample in-house security expertise may not be getting the return on investment (ROI) that they anticipate as costly resources spend their shifts watching management consoles instead of strategically planning ways to improve security posture.

MSSPs change this paradigm significantly. By trusting security operations to an MSSP and taking advantage of their expert tools, skills and processes, enterprises can improve system uptime and performance while avoiding large investments in technology and resources.

Not only do MSSPs help protect companies that do not have the manpower or budget to build and operate security infrastructure on a 24x7x365 basis, they can also increase productivity. Allowing an MSSP to handle day-to-day security monitoring and management gives organizations an opportunity to re-allocate in-house IT resources to more strategic initiatives. MSSPs also facilitate business continuity by providing advanced intelligence to thwart attacks before they cause damage and disrupt business operations. This layer of proactive protection lends a competitive edge by keeping businesses functional even when a sophisticated new virus or worm is spreading rapidly across the Internet.

Faced with increasingly sophisticated Internet attacks as well as mounting budget and regulatory pressures, more enterprises are using managed security service providers for business continuity, lower total cost of ownership (TCO), compliance with regulatory requirements and competitive advantages.



Selecting a Managed Security Services Partner

When selecting an MSSP, the most important consideration is whether that MSSP is committed to delivering exceptional protection. The most reliable method of determining an MSSP's level of dedication is to review the provider's accountability if it violates the terms of its service level agreement (SLA). For this reason, enterprises should consider IBM Managed Protection Services (MPS) from IBM Internet Security Systems (ISS).

Traditional vendor SLAs usually offer clients only one day of free service if a violation occurs, which is not much compensation given the amount of financial damage hacker attacks can cause. IBM Managed Protection Services offer a higher standard of protection through performance-based SLAs that guarantee response times and countermeasures for security events. For example, when IBM ISS publishes software updates for the latest threats circulating the Internet, it promises to apply that intelligence to customer systems within 24 hours. If IBM ISS does not meet this goal or any other goal listed in its SLA, customers receive a free month of Managed Protection Services, not just one day.

Further, IBM ISS offers the MSSP industry's only money-back protection payment*, providing companies with a cash payment of US \$50,000 for any security breach resulting from a successful attack listed on the company's X-Force® Certified Attack List. The IBM Internet Security Systems X-Force research and development team is world-renowned for its proactive research on security flaws in software and the techniques hackers use to attack networks. The X-Force Certified Attack List includes the most critical security threats and is updated regularly. IBM ISS is the only MSSP to offer clients this high level of accountability. As a result, IBM ISS clients can remain confident in their enterprise protection, even in the face of Internet threats.



“A provider may meet all of the requirements of its SLAs, but if it does not prevent a threat, the customer does not receive any value,” says Rick Miller, director of Managed Security Services at IBM Internet Security Systems. “Our guaranteed offerings and performance-based SLAs demonstrate our confidence and commitment in preserving clients’ investment in their online systems.”

IBM ISS spells relief

MSSPs differ greatly not only in the levels of accountability that they offer, but in many other respects as well. Many providers monitor the security of a few network devices, but do not supply the kind of guaranteed, comprehensive protection that businesses require to defend their online assets. IBM Managed Protection Services are designed to deliver the infrastructure, knowledge resources and on-demand expertise that organizations need to secure their systems from Internet attacks all at a fraction of the cost of in-house security resources.

IBM Managed Protection Services are designed to provide networks, servers and desktops with 24x7x365 comprehensive protection and expert management, monitoring and escalation. Network services span firewall, intrusion prevention, anti-virus, anti-spam, content security and VPN capabilities found in the IBM protection platform. IBM ISS provides MPS for servers across a variety of platforms and operating systems using IBM RealSecure® and Proventia® server products. IBM ISS provides MPS for desktops using IBM RealSecure and Proventia Desktop Endpoint Security products, which incorporate award-winning desktop firewall, intrusion prevention, anti-virus compliance, virus prevention system (VPS) and buffer overflow exploit prevention technologies.



IBM Managed Protection Services are a part of the protection on demand approach to security. Protection on demand capabilities are designed to deliver protection to organizations of all sizes, helping them to proactively respond to Internet threats while integrating security with key business processes. IBM's innovative managed security services approach blends market leading services, technologies and security intelligence into a single solution that can be utilized when, where and how clients need it. The result is a cost-effective solution that helps organizations optimize resources, improve flexibility and responsiveness, and address regulatory requirements.

The IBM ISS global network of Security Operations Centers (SOCs) monitors client servers, firewalls, intrusion prevention systems and other network elements 24x7x365 to identify and address unauthorized behavior before it disrupts business operations. In addition, IBM ISS provides knowledge assets such as the X-Force Certified Attack List, a continuously updated inventory of Internet threats compiled by the company's elite research and development organization. Armed with this early warning intelligence, enterprises can stay one step ahead of hackers and promote business continuity by addressing problems before they spread.

"Today, the time frame between the discovery of a vulnerability and hacker exploitation of that weakness is continuing to shrink," says Miller. "For this reason, it is extremely important for companies to team up with a security partner that warns them of threats in advance of an attack so they can use that knowledge to proactively protect information resources."

Unlike other MSSPs, IBM ISS solutions are designed to protect vulnerabilities the weak spots commonly targeted by Internet attacks. With this form of preemptive protection, clients can choose to patch vulnerable systems during a sensible schedule rather than an emergency.



IBM ISS clients can avoid deployment hassles while receiving a customized solution designed to meet performance and security needs.

At your service

Bundled services are another important feature of IBM Managed Protection Services. IBM Emergency Response Services help clients develop incident response procedures, including planning, forensic analysis, preservation of evidence and data recovery. These expert services help clients respond quickly and effectively to security breaches to keep critical systems up and running, and minimize damage to their business.

IBM Deployment Services are another valuable component of Managed Protection Services. Implementing new technologies can be a long, people-intensive process and can disrupt IT operations. By providing skilled security personnel who help clients install, configure and integrate new security technologies within existing IT environments, IBM Deployment Services help deployments go smoothly.

“Making an initial investment in new security technology is one thing, but more often than not, the larger cost is deploying and managing that technology,” says Miller. “Deployment Services help clients use IBM ISS technology effectively, without breaking the bank.”

Knowledge is power

In addition to helping companies cost-effectively fortify their systems, IBM Managed Protection Services can assist executives in justifying investments in IT security. CIOs typically have a difficult time quantifying just how the Internet threatens information resources. Managed Protection Services help by providing a Web-based management portal that enables executives to see the ongoing status of their security operations, including attempts to gain unauthorized access, how those attempts were stopped and recommendations on how to prevent similar attacks. Equipped with this information, CIOs can show decision makers the real threats facing the business and emphasize the need for 24x7x365 managed security.



The management portal also helps companies observe that their online systems are in compliance with new government regulations. For example, the Sarbanes-Oxley Act requires executives to periodically disclose the status of internal controls on corporate financial systems. To help meet such demands, the portal integrates service-level data from devices across client networks and displays this information in easy-to-read, business focused reports. Indeed, enterprises can no longer keep security issues a secret, and a portal helps executives gather the systems information they need quickly and efficiently.

“A provider may meet all of the requirements of its SLAs, but if it does not prevent a threat, the customer does not receive any value.”

Rick Miller
Managed Security Services,
IBM Internet Security Systems

Keeping safe and sound at a lower cost-of-ownership

For a fixed monthly fee, managed security services help enterprises protect critical online systems on a 24x7x365 basis while reducing total cost of ownership (TCO). Because they already possess the right tools, people and processes, MSSPs also allow companies to boost IT productivity and return on investment (ROI) by freeing up internal resources to focus on longer-term initiatives. In addition, they help executives achieve and maintain compliance with regulatory requirements.

When evaluating MSSPs, organizations looking to outsource information security should consider providers that will guarantee information security and be fully accountable if they do not meet expectations. Armed with such a high standard of protection, companies can stay up and running-while hackers take down competitors, thus improving their standing in the marketplace and reassuring customers, partners and shareholders that they made the right choice.



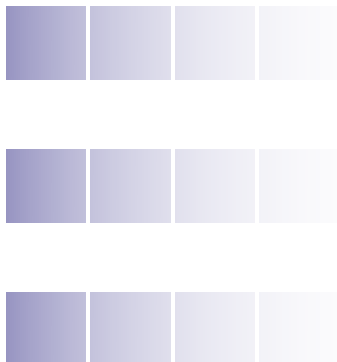
Utility Provider Places Trust in IBM Internet Security Systems

For one rural U.S.-based utility company, keeping up with the evolving threat of Internet worms and other sophisticated attacks was becoming overwhelming. The company had been using anti-virus software and an intrusion detection system, but it did not have enough people to proactively monitor critical IT security systems.

“Our business is a 24/7 operation, and we did not have the staff to manage and maintain our information security to the extent we felt was necessary,” says Mark Dayton, the company’s network supervisor. “The last thing we wanted to do was repair systems that should have never been broken in the first place.”

However, Dayton had trouble demonstrating to the rest of the company why IT security was so essential and deserving of more attention. “When you live in a small town where people do not lock their cars and some do not even lock their homes, the idea that someone in another part of the world would try to hack into our systems is hard to sell,” says Dayton. “We needed a way to categorize and quantify these threats to persuade decision makers that our company faced a real danger.”

Fortunately, the experts at IBM Internet Security Systems were able to help Dayton come up with the data to justify his concerns. Dayton was impressed by the competence of IBM ISS staff as well as the provider’s updated intelligence on current threats spreading across the Internet. “IBM Internet Security Systems helped us find out what was going on, where it was going on and what internal measures we could take to lessen the likelihood of an attack damaging our business,” says Dayton. “The team gave us real data we could use to substantiate what we had been saying all along.”



With new security intelligence in hand, the utility company chose to outsource its day-to-day security operations to IBM ISS. By off-loading security to a trusted expert, Dayton has been able to keep the company's original infrastructure intact, yet free up IT staff to focus on higher level security projects. As a result, the company can now make faster decisions, shortening the time-to-market for critical IT initiatives. For enterprises that still need convincing that Internet attacks pose a viable threat to their business, Dayton has some advice.

"Companies need to realize that, no matter how big or small they are, they are still vulnerable to people attempting to raid their systems," says Dayton. "Enterprises can no longer afford to cross their fingers and hope that an attack does not happen. IBM ISS lets companies know what to expect and what internal measures they can take to lessen the likelihood of an attack damaging their business."

About IBM Internet Security Systems, Inc.

IBM Internet Security Systems (ISS) is the trusted expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and helps reduce regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the X-Force research and development team—a world authority in vulnerability and threat research.

To learn more about preemptive protection and IBM Managed Protection Services, please visit ibm.com/services/us/iss or contact an IBM ISS location near you.





Notes:

- * IDC Executive Brief: IBM to Acquire ISS to Bolster Sale of Managed Security Services (#203464)
- * 2006 CSI/FBI Computer Crime and Security Survey

© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.
07-07

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

RealSecure, Proventia and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.