IBM X-Force 2010 Mid-Year Trend and Risk Report

CIO Security Priorities: Key security issues to address

For more information on the **Availability of Vulnerability Fixes and Patches**, see page 19 of the 2010 X-Force Mid-Year Trend and Risk Report.

Did you know that the number of reported vulnerabilities reached record levels during the first half of 2010, up 36 percent? Did you also know that over half (55 percent) of all vulnerabilities disclosed had no patch available as a fix? What does your company do to protect your assets from compromise when there's no patch available?

IBM Security Network Intrusion Prevention System (IPS)[1] products and services provide IBM Virtual Patch® technology protection for your assets—all available for management either locally, or by IBM Managed Protection Services, your trusted managed security services advisor.

For more information, see **Web Application Vulnerabilities** on page 70 of the 2010 X-Force Mid-Year Trend and Risk Report.

Over half of all vulnerabilities disclosed in the first half of 2010 affected web software applications used to create corporate and other types of websites worldwide. Do you have controls in place to specifically provide protection for web-facing applications? Are you confident your home-grown web applications are secure throughout the software development life cycle?

IBM provides end-to-end web application security with the IBM Web Application Security bundle:

- *Secure code development, source code testing and vulnerability management with IBM Rational® AppScan® and Rational AppScan Source Edition*
- *Real-time protection of web applications with IBM Web Application Security inside IBM Security Network IPS products*
- *Security and performance for web services with IBM WebSphere® DataPower® appliances*
- *Management of user access to web applications with Tivoli® Access Manager*
- *Application assessment services with IBM Professional Security Services*
- *IBM Managed Protection Services specifically designed to provide protection for Web 2.0 and web applications*

For more information, see **Web Application Vulnerabilities** on page 70 of the 2010 X-Force Mid-Year Trend and Risk Report.

Attacks based on vulnerabilities in websites continue to skyrocket. Do you know how much of your website is built from off-the-shelf software versus developed in-house? When was the last time you assessed your web applications?

IBM provides assessment through Rational AppScan products, host and network protection through the IBM Security Intrusion Prevention Solutions and IBM Secure Web Gateway Service, all backed by IBM Managed Protection Services specifically designed to provide protection for Web 2.0 and web applications.

For more information, see **Document Format Vulnerabilities** on page 79 of the 2010 X-Force Mid-Year Trend and Risk Report.

Attackers continue to find new ways to trick users by hiding malware in documents that your employees think are harmless, like Microsoft® Office® applications and Adobe® PDF files. Vulnerability disclosures and attacks through websites, or sent via email, continue to grow during the first half of 2010 where four Adobe vulnerabilities made the top five exploitation list. How many MSOffice or PDF files are sent or downloaded daily in your organization? What controls do you have in place to patch these programs against known vulnerabilities and prevent zero-day exploitation?

With IBM Security Solutions and Services, IBM offers protection against known and unknown vulnerabilities using vulnerability-centric and heuristic technology based on the shell code typically leveraged in these types of attacks.

For more information, see **Malicious Websites** on page 88 of the 2010 X-Force Mid-Year Trend and Risk Report.

Attackers use search engine optimization techniques to get their malicious websites listed at the top of search engine results. Attackers also use this technique to trick end users into downloading rogue anti-virus. What do you have in place to protect your end users from infecting your enterprise by simply browsing the web?

IBM detects and protects against malicious websites from multiple entry points. In addition to IBM Web Application Security, our IBM Security Network IPS technology is embedded in our protection agents (and globally monitored by Managed Security Services) and provides blocking and reporting on both old and new malicious URLs. This compliments more traditional protection technologies such as web crawling and threat research. In addition to blocking web exploits using our IPS technology, we can also block malicious websites with the IBM Secure Web Gateway Service and Managed Security Service for Web Security

For more information, see **Spam Volume** on page 92 of the 2010 X-Force Mid-Year Trend and Risk Report.

URL spam (email with links to the spam content) is still the predominant type of spam. Many of these spam messages are hosted on trusted websites, making it harder for end users to ignore and more difficult for spam filters to detect. If you use anti-spam products, how does your vendor's technology detect these messages as spam when the spam content isn't even in the email itself?

IBM is in the enviable position of being able to monitor spam and phishing, and the content on the Internet at the same time. With more than 10 billion analyzed web pages and files, along with 40 million documented spam and phishing attacks, keeping up with URL spam is simple for the IBM Secure Web Gateway Service, IBM Lotus® Protector/Network Mail, and IBM Secure Mail Services

The X-Force Threat Analysis Service is available as a customized daily service that informs your IT staff of the latest threats, protection available and overall trends in the industry to keep your organization proactively prepared for the evolving threat landscape.

How does your team maintain the knowledge needed to keep up with the changing threat landscape, such as the trends discussed here and in the 2010 X-Force Mid-Year Trend and Risk Report?

IBM Security Solutions and Services provide the security intelligence and protection you need, by analyzing threats across the entire spectrum. Consider the following data backing our products and services:

- *10 billion analyzed web pages and images*
- *150 million intrusion attempts daily*
- *40 million spam and phishing attacks analyzed and categorized*
- *51 thousand documented vulnerabilities*
- *Millions of unique malware samples*

For more information

For more information on the 2010 X-Force Trend and Risk Report, please visit: **ibm.com**/security/x-force or contact your local IBM representative or IBM business partner.

© Copyright IBM Corporation 2010

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
October 2010
All Rights Reserved

IBM, the IBM logo, ibm.com and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

The use of third-party data, studies and/or quoted material does not represent an endorsement by IBM of the publishing organization, nor does it necessarily represent the viewpoint of IBM.

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.

All information contained in this document is current as of the initial date of publication only and is subject to change without notice. IBM shall have no responsibility to update such information. The information contained in this document does not affect or change IBM product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of IBM or third parties.

Please Recycle

All information contained in this document was obtained in specific environments, and is presented as an illustration. The results obtained in other operating environments may vary.

The information contained in this document is provided on an "as is" basis without any warranty, either expressed or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or noninfringement.

In no event will IBM be liable for damages arising directly or indirectly from any use of the information contained in this document. Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. Use of those websites is at your own risk. IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA. U.S. Patent No. 7,093,239

[1] IBM Security Network Intrusion Prevention System was formerly called IBM Proventia® Network Intrusion Prevention System.

[2] IBM Multi-Function Security was formerly called IBM Proventia Network Multi-Function Security.

WGE03005-USEN-00