IBM X-Force 2011 Trend and Risk Report

CIO Security Priorities

The second half of 2011 continued to demonstrate common reports of weekly wide-scale network security breaches, leaving a wake of leaked customer data, inaccessible web services, and billions of dollars of damages.

IBM X-Force Research and Development

By mid-year, in the midst of frequent reports of data leaks, denial of service attacks, and social Hacktivism, IBM X-Force® declared 2011—"Year of the security breach". By the end of the year, the frequency and scope of these incidents has persisted, and continues to bring awareness to the basic tenets of operating a business and protecting its assets in an increasingly connected world.

Attackers Adapt Techniques in 2011

IBM X-Force saw a rise in new attack trends and an array of significant, widely reported external network and security breaches with documented increases in three key:

- **Attacks targeting shell command injection vulnerabilities more than double**—For years, SQL injection attacks against web applications have been a popular vector for attackers of all types. SQL injection vulnerabilities allow an attacker to manipulate the database behind a website. As progress has been made to close those vulnerabilities—the number of SQL injection vulnerabilities in publicly maintained web applications dropped by 46 percent in 2011—some attackers have now started to target shell command injection vulnerabilities instead. These vulnerabilities allow the attacker to execute commands directly on a web server. Shell command injection attacks rose by two to three times over the course of 2011. Web application developers should pay close attention to this increasingly popular attack vector.
- **Spike in automated password guessing**—Poor passwords and password policies have played a role in a number of high-profile breaches during 2011. There is also a lot of automated attack activity on the Internet in which attacks scan the net for systems with weak login passwords. IBM observed a large spike in this sort of password guessing activity directed at secure shell servers (SSH) in the later half of 2011.

Old methods of attack, such as traditional phishing and spam, are being replaced with new methods of deploying malware.

- **Increase in phishing attacks that impersonate social networking sites and mail parcel services**—The volume of email attributed to phishing was relatively small over the course of 2010 and the first half of 2011, but phishing came back with a vengeance in the second half, reaching volumes that haven't been seen since 2008. Many of these emails impersonate popular social networking sites and mail parcel services, and entice victims to click on links to web pages that may try to infect their PCs with malware. Some of this activity can also be attributed to advertising click fraud, where spammers use misleading emails to drive traffic to retail websites.

Progress in Internet Security

On a positive note, although 2011 saw a rise in new attack trends and an array of significant, widely reported external network and security breaches, the report also revealed improvements in the overall security of Internet-related software. We witnessed declines in spam, the availability of exploit code, and security vulnerabilities that remained unpatched, We also saw significant improvements in the quality of software produced by organizations that use tools like IBM AppScan® to analyze, find, and fix vulnerabilities in their code. IBM found cross site scripting (XSS) vulnerabilities are half as likely to exist in customers' software as they were four years ago.

Emerging Technologies

We continue to explore how companies are keeping up with the complexities of mobile devices and cloud. The mass adoption of mobile devices brings the discussion of "bring your own device" (BYOD) programs to the forefront, and how to mitigate the risks associated with these policies. Cloud adoption faces similar discussions. The question is not whether the cloud is more or less secure, but on what specific controls, and business processes, do we need to be focused to reduce risk and ensure security in a cloud environment.

The sheer number of high profile and highly public incidents throughout 2011 should be a catalyst for executives and business leaders to re-evaluate the effectiveness of existing structures, policy and technology in the enterprise.

IBM believes the way to help clients get ahead of security threats is to connect our analytics and intelligence capabilities across an organization for better prediction and detection. With awareness comes action and change.

IT security is now a board room discussion affecting business results, brand image, supply chain, legal exposure, and audit risk.

About IBM X-Force R&D and IBM security collaboration

IBM Security provides a broad spectrum of security competency.

- IBM X-Force research and development teams discover, analyze, monitor and record a broad range of computer security threats and vulnerabilities. Other IBM groups use that rich data to develop protection techniques for our customers.
- IBM Managed Security Services (MSS) monitors exploits related to endpoints, servers (including web servers), and general network infrastructure. They track exploits delivered over the web as well as other vectors such as email and instant messaging
- Professional Security Services (PSS) delivers enterprise-wide security assessment, design, and deployment services to help build effective information security solutions.
- Our Content security team scours and categorizes web pages through crawling, independent discoveries, and feeds provided by MSS.
- IBM AppScan OnDemand Premium Service collates real-world vulnerability data—which combines automated scanning with manual testing and verification—from security assessments conducted over the past several years.
- IBM Security Services supports the cloud in two ways: Security Services for the Cloud provides security expertise to help clients begin their journey to the cloud, and Security from a cloud-based model that helps customers reduce costs and complexity, improve security posture and meet compliance requirements.
- IBM Identity and access management solutions help organizations centralize and automate the management of identity profiles and access privileges for authorized users.
- IBM data and information security solutions deliver capabilities for data protection and access management that can be integrated to help address information lifecycle security across the enterprise.
- IBM InfoSphere® Guardium® provides a scalable enterprise solution for database security and compliance.
- The QRadar Security Intelligence Platform from Q1 Labs, an IBM Company, offers an integrated solution for SIEM, log management, configuration management and anomaly detection.

For more information

Click here to access the complete "IBM X-Force 2011 Trend and Risk Report" published by IBM Security Systems.

To learn more about offerings from IBM Security, please visit: **ibm.com**/security

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

Produced in the United States of America
March 2012

This document is intended to serve as an executive summary of the full "IBM X-Force 2011 Trend and Risk Report " published by IBM Security Systems. The complete report can be accessed here: http:/www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03012USEN&attachment=WGL03012USEN.PDF

Please Recycle

WGE03017-USEN-00