Rational. software

Cyber security solutions from IBM: assess and defend against security vulnerabilities.

Highlights

- ***Helps defend against Internet-based threats to the network***
- ***Enables agencies to scan and test for common Web application vulnerabilities***
- ***Helps simplify, protect and accelerate your XML and Web services deployments***
- ***Provides a comprehensive solution that supports cyber security, compliance and evolution***

Building cyber security into the lifecycle

In the first half of 2008, the IBM Internet Security Systems™ (ISS) X-Force® research and development team analyzed and documented 3,534 computer-related vulnerabilities, exposures or configuration settings that could compromise a system's confidentiality, integrity or accessibility. This risk exposure is up 5 percent from the first half of 2007.[1]

Government networks are vulnerable to this increasing threat. In 2007, the U.S. Government Accountability Office (GAO) found that "significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems."[2]

These weaknesses were not the result of a lack of standards, but a lack of compliance. In doing business around the world, IBM has found that only a comprehensive approach will work to protect enterprise or mission-critical systems against cyber attacks.

Detecting, protecting and managing vulnerabilities within the infrastructure

When most people in the U.S. government look at addressing vulnerabilities within their enterprise or mission-critical systems, they start by assessing the vulnerabilities within their operational environment. But in today's Internet-centric world, there are numerous vulnerabilities—found in both an organization's infrastructure and its applications—that individuals, organizations and foreign nations are attempting to exploit in hopes of penetrating or disrupting the critical systems the U.S. government relies on.

A robust IT governance program includes policies, processes and technologies to continuously discover new and existing assets (possible rogue connections, authorized but non-compliant systems and other assets attempting to connect to your network). It should assess and remediate (detect, protect and manage) vulnerabilities and provide continuous host-based and network security. Finally, it should provide centralized command and control including updates, alerts, reporting and role-based access.

The first line of defense is to effectively detect, protect and manage the vulnerabilities that exist within the infrastructure (servers, routers, switches, etc.) of the operational systems. IBM ISS products and services scan for, detect, protect and manage vulnerabilities within your operational infrastructure.

The X-Force team — a leading cyber security research and development organization — conducts continuous research and analyses into virtually all aspects and components of operational systems. The group provides continuous detection of vulnerabilities and can deliver protection against those vulnerabilities while industry vendors create and deploy patches to address them.

Additionally, the IBM Proventia® Network Multi-Function Security (MFS) unified threat management (UMT) device and IBM Proventia Network Enterprise Scanner provide protection at the gateway and network levels to defend against Internet-based threats without jeopardizing network bandwidth or availability.

Addressing application security and vulnerabilities as a second line of defense

In addition to securing your infrastructure, your organization needs to address Web application security and vulnerabilities (cross-site scripting, structured query language [SQL] injection, buffer overflow, etc.) within the operational environment. This is essential for a comprehensive defense-in-depth strategy. The IBM Rational® AppScan® solution automates vulnerability assessments for the broadest set of technologies including Asynchronous JavaScript and XML (AJAX), Adobe® Flash and Web services. It provides customization and extensibility for the open source community, advanced remediation recommendations, a Pyscan framework for penetration testers and over 40 regulatory compliance reports including Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) 800-53A, Director of Central Intelligence Directive (DCID) 6/3, Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and many others.

After securing your applications to protect against unauthorized access to your underlying systems, your organization can deploy IBM Rational Policy Tester™ software to monitor and manage the quality, privacy and accessibility content and compliance of your Web site. Rational Policy Tester can help ensure that your critical, proprietary or operational data does not end up on your Web site and then made available to the outside world. It can be used to assess your Web sites for Operational Security (OPSEC) compliance.

Deploying SOA appliances to keep pace with new technologies

The emergence of service-oriented architecture (SOA) opens up exciting new methods for systems development and integration where functionality can be built around business processes and packaged as services. But a comprehensive cyber security solution needs to protect SOA as a new frontier of both opportunity and vulnerability.

Designed by some of the world's top XML and Web services security experts, IBM WebSphere® DataPower® SOA Appliances software delivers comprehensive and configurable

security and policy enforcement functions, from Web services security to XML access control.

Bringing it all together

None of the solutions outlined above can fully address cyber security by itself, and IBM understands this situation. For years, we have sent our protection and detection technologies out to do battle in the cyber trenches each day. We've learned that it's relatively easy to protect networks, but work must still be accomplished over e-mail; users must still have the ability to share data via the Web; and organizations must still integrate their back-office systems with other organizations' systems.

The need to share information opens the door for exploits of all Web applications and Web service XML traffic. But the tools detailed here work in conjunction to perform security-rich transmission of important government information—including critical intelligence information—safely out to the war fighter, and they can limit the ability of cyber criminals and other adversaries to compromise the flow of resources to the front lines.

Gaining operational awareness

IBM Tivoli® Security Information and Event Manager software provides a centralized security and compliance management solution to give you visibility into the security posture of the enterprise. Tivoli Security Information and Event Manager takes the reporting and events derived from all of the other parts of the cyber solution and provides valuable security insights that you can act on.

Tivoli Security Information and Event Manager facilitates compliance by using centralized dashboard and reporting capabilities. It helps you protect intellectual property and privacy by auditing the behavior of all users—privileged and nonprivileged. And it manages security operations effectively and efficiently with centralized security event correlation, prioritization, investigation and response.

Evolving cyber security to keep pace with applications development

Once the operational systems receive information assurance (IA) certification, many people assume they have achieved full enterprise security. In truth, they have only addressed the current version of the operational system. As systems evolve, the introduction of new features, functionality and technologies—for both hardware and software—introduces new vulnerabilities. With each major change, the whole IA process must be repeated to ensure that the latest version of the operational system is security sound.

To fully achieve enterprise security, you need to make cyber security part of the total lifecycle of the system, starting with development. Integration between security products from IBM and the Rational change and risk management suite supports that total lifecycle coverage.

In development, there are several points in the lifecycle process where IA and security measures must be considered, including:

- *Requirements definition.*
- *System modeling and design.*
- *Code development.*
- *Testing phases.*

As with functional defects or bugs, the earlier in the process you identify vulnerabilities, the easier it is to address them. By using the IBM Rational Unified Process® (IBM RUP®) solution, you can identify and address defects earlier in the development cycle, helping you avoid the high costs and long hours associated with fixing defects once a system is deployed to the operational environment. This means that a newly deployed operational system can be much more security rich at the outset, thus allowing the operational system to achieve IA certification more quickly and at a lower overall cost.

Extending IA and cyber security beyond traditional development

When you extend IA and security measures beyond the traditional development lifecycle phases and incorporate it into the defect tracking and workflow processes of the development lifecycle, you have a traceable and repeatable process for identifying, assessing and addressing security defects in your operational system.

Vulnerability defects identified by security offerings from IBM can be reported as defects directly in the development process. And once the change to the system reaches the testing phase, IBM solutions can help you test the remedy within your environment, helping to ensure that the defect has been addressed. Lastly, security offerings from IBM can help you test the predeployment version of the system before you deliver it to operations. This approach not only enables the optimization of the software development lifecycle (SDLC) but is a requirement of all certification and accreditation standards.

Why IBM?

IBM offers the strategies, capabilities and technologies necessary to address critical cyber challenges. Our comprehensive approach enables the successful management and protection of the cyber system's technology, human capital, compliance, governance and risk management layers.

We invested over US$1.5 billion in security technology in 2008 alone, including the three core solutions that comprise cyber security solutions from IBM:

- *IBM Rational AppScan — a cutting-edge suite of automated Web application security solutions that can scan and test for common Web application vulnerabilities, and includes IBM Rational Policy Tester for OPSEC assurance.*
- *IBM Proventia Network MFS — a solution designed to defend against Internet-based threats to your network.*
- *IBM WebSphere DataPower SOA Appliances — a solution that helps protect the information in transit between service and client for security-rich XML and Web services transactions.*

For more information

To learn more about cyber security solutions from IBM, contact your IBM sales representative or IBM Business Partner, or visit:

ibm.com/federal/security

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

Produced in the United States of America
January 2009

1 IBM, *IBM Internet Security Systems X-Force® 2008 Mid-Year Trend Statistics*, July 2008.

2 U.S. Government Accountability Office, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, Gregory C. Wilshusen, March 12, 2008.

RAS14013-USEN-00