SAINT®

Next-Generation Vulnerability Management

How vulnerability management can protect business operations, mitigate risks, simplify compliance and improve IT management

Contents

Brought to you compliments of

SAINT®

Why CIOs Should Care About Vulnerability Management

Not long ago, vulnerability management was an "additional duty" delegated solely to security specialists. Now, vulnerability management is a key concern for CIOs and top IT managers.

In the past, most organizations conducted one or two vulnerability scans annually and an occasional penetration test. Today, vulnerability management best practices include continuous monitoring, compliance reporting and advanced analytics.

What has changed, and why should IT managers care about vulnerability management?

Many of the largest and most public data breaches involve software vulnerabilities. Advanced persistent threats (APTs) and targeted phishing attacks are taking advantage of vulnerabilities in desktop applications, plug-ins and servers. Organizations must identify and remove these vulnerabilities if they want to prevent data breaches, ensure continuous business operations and keep their name out of the newspapers.

Government regulations and industry standards like PCI DSS, HIPAA and FISMA require specific vulnerability management tools and activities. Other standards are less explicit, but include language that compliance officers and auditors interpret as recommending vulnerability scans, penetration testing, continuous monitoring and other vulnerability management practices.

New vulnerability management tools dramatically improve the productivity of security and IT operations staffs. Features like dashboards, advanced analytics, customizable policies and integration with security information and event management (SIEM) products eliminate time-consuming manual tasks and provide information that allows IT managers and staff members to set priorities, react faster to threats and track metrics related to the organization's security posture.

In short, while vulnerability management activities are still performed by security personnel, CIOs and IT managers have many reasons to make sure they are supported by the right tools.

In this paper, we will look at how vulnerability management tools and best practices help protect business operations, simplify compliance and improve IT management and productivity.

As part of our discussion, we will reference examples from SAINT 8, a next-generation solution from SAINT Corporation, to illustrate how modern vulnerability management tools can address today's threats in a proactive, systematic and highly automated fashion.

Preventing Data Breaches and Protecting Business Operations

"Vulnerabilities" include defects in software products that attackers can utilize to penetrate networks, access confidential data and interfere with operations. The U.S. National Vulnerability Database includes more than 55,000 such software flaws in its Common Vulnerabilities and Exposures (CVE) list.[1]

A broader definition of vulnerabilities also encompasses misconfigured hardware and software, software services that are common attack points and shortcomings that can be attacked by brute-force methods, such as weak passwords.[2]

What is eminently clear is that many of the most damaging and widely publicized data breaches involved vulnerabilities that were used by attackers to gain a beachhead within a corporate network. Three examples are highlighted on the next page.

[1] "CVE List Surpasses 55,000 CVE Identifiers," CVE, March 21, 2013

[2] CVE terms this latter category "Exposures."

Return to top

SAINT®

The RSA Data Breach

In 2011, an EMC employee clicked on a link in a phishing email and downloaded an attached Excel file. When the spreadsheet was opened, an embedded flash object exploited an Adobe Flash vulnerability (CVE-2011–0609) to plant a remote access Trojan on the employee's system. The attacker used the Trojan to acquire high-level credentials ("privilege escalation"), find information about authentication technology developed by RSA, EMC's information security division, and send the information to an outside server. The breach cost RSA $66 million to replace customers' security tokens, monitor customer security and harden its infrastructure, and the resulting publicity dealt a major blow to the company's reputation.

Sources: "Anatomy of an Attack," RSA;
"How We Found the File That Was Used to Hack RSA," F-Secure

The Utah Department of Health Debacle

In 2012, the Utah Department of Health put a server with a weak password online. Hackers exploited the vulnerability to download the names, addresses, Social Security numbers and medical billing codes of an estimated 780,000 people before the breach was discovered. The attack resulted in a criminal investigation by the FBI and, ultimately, the resignation of the CIO of Utah's Department of Technology Services.

Sources: "Utah CIO Steve Fletcher Resigns, State Promises Security Reforms," *Government Technology*

The Java Alarm

In 2013, researchers uncovered several vulnerabilities in widely used Java 6 and Java 7 plug-ins that allow attackers to download remote access Trojans and other malware to potentially millions of PCs. The risk was so severe that U.S. security agencies and many information security firms suggested disabling Java in Web browsers.

Sources: "Zero Day Java Vulnerability Allows McRat Trojan Infections," *InformationWeek*;
US-CERT Alert (TA13-064A): Oracle Java Contains Multiple Vulnerabilities

Return to top

The implications are clear: To prevent data breaches and protect business operations, organizations must be able to detect vulnerabilities across the entire enterprise.

A vulnerability management product can address these threats if it provides:

Breadth. It should include the ability to identify vulnerabilities across all types of software packages and hardware devices; browsers and plug-ins; client, server and Web applications; and security and networking devices.

Integrated scanning and penetration testing. Vulnerability scanning typically identifies hundreds or thousands of vulnerabilities. Penetration testing determines which vulnerabilities can most readily be exploited and, therefore, need to be remediated first. Penetration testing also provides information on methods attackers could use to exploit the vulnerabilities.

Tools to assess vulnerability to phishing and social engineering. APTs and other sophisticated attacks usually exploit human errors. Organizations need to be able to assess how well their employees can recognize and deflect social engineering lures such as phishing emails and USB flash drives infected by malware.

Data collection and analytics. Organizations need to compile vulnerability information from across the enterprise and use analytic tools to separate critical risks from potential risks as well as monitor vulnerability patterns over time.

Simplifying Compliance and Configuration Auditing

Vulnerability management tools and activities are specifically mandated in many government regulations and industry standards, including PCI DSS, HIPAA and FISMA.

Payment Card Industry Data Security Standard (PCI DSS)

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

6.6 For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis...by either...reviewing public-facing Web applications via manual or automated application vulnerability security assessment tools or…installing a Web-application firewall in front of public-facing Web applications.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification.

Source: PCI DSS Version 2.0

Return to top

SAINT®

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

164.308 (a)(1)(ii)(A) A covered entity must...conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

164.308 (a)(1)(ii)(B) A covered entity must...implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Organizations must identify and document reasonably anticipated threats to e-PHI...Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.

Sources: HIPAA section 164.308; HIPAA Security Standards: Guidance on Risk Analysis

Federal Information Security Management Act (FISMA)

RA-5 VULNERABILITY SCANNING. The organization:

a. Scans for vulnerabilities in the information system and hosted applications...and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques…for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact.

CA-7 CONTINUOUS MONITORING. The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes…

c. Ongoing security control assessments…;

e. Correlation and analysis of security-related information generated by assessments and monitoring.

Source: NIST Special Publication 800-53

Many other government regulations and industry standards mandate the use of reasonable precautions against "foreseeable risks," which are often expected to include vulnerability management practices.

The cost of neglect can be severe, including fines of hundreds of thousands of dollars for noncompliance and multimillion-dollar penalties for serious breaches.[3]

A vulnerability management product can help IT managers simplify compliance if it:

- Performs all of the scanning, penetration testing, assessment and measurement functions required by regulations and standards.
- Provides reports formatted to meet the requirements of standards audits.
- Is certified for use with the standard (where appropriate certifications exist).

Improving IT Productivity and Management

For IT security and operations staffs, tasks such as identifying and remediating vulnerabilities, responding quickly to threats and performing security forensics after suspicious events are consuming more and more time.

A vulnerability management product can improve IT staff productivity if it provides:

- **Efficient data collection**, so security and operations personnel can gather vulnerability information from all systems across the entire business.
- **Customizable policies**, so vulnerability scanning and penetration testing can be focused on the systems, threats and regulatory requirements specific to the organization.
- **Integration with SIEM, patch management, compliance reporting and service management systems**, so vulnerability information can be used to perform forensics, improve patching, speed up audits and assist technical support representatives.

A few vulnerability management solutions are also designed to support CIOs and IT managers by offering:

- **Dashboards and trend reports**, so managers can assess the current security posture of the organization and use metrics to document improvement over time.
- **Advanced analytics**, so managers and security staff can pinpoint problem areas and focus on eliminating the most critical vulnerabilities.

[1] For examples, see: PCI Noncompliant Consequences, FocusOnPCI.com; "Retailer Challenges VISA $13.2M PCI Fine in Court," Threatpost, March 12, 2013; "HHS Toughens HIPAA Violation Penalties," *Credit Union Times*, April 10, 2013; "Alaska DHSS settles HIPAA security case for $1,700,000," U.S. Department of Health and Human Services

Return to top

Applying Next-Generation Vulnerability Management

How, exactly, can a vulnerability management product prevent the kinds of data breaches highlighted earlier, simplify compliance and audits, and improve IT productivity?

The following are some examples based on SAINT 8, a next-generation vulnerability management solution that provides not only vulnerability scanning and penetration testing, but also continuous monitoring, extensive compliance reporting and advanced analytics.

Preventing Data Breaches and Protecting Business Operations

The RSA data breach, the Utah Department of Health incident, and the Java 6 and 7 alerts involved problems that are unfortunately all too common:

- Vulnerabilities in desktop applications and plug-ins (CVE-2011-0609 related to Adobe Flash for RSA, and CVE-2013-1493 and CVE-2013-0809 for Java 6 and 7), possibly on hundreds or thousands of systems.
- Users willing to click on a link in an unknown email or visit an infected website (one employee at RSA, and potentially millions of computer users with Java 6 and 7).
- Weak passwords (Utah Department of Health).
- Servers and databases with weak or misconfigured security settings (possibly involved in the privilege escalation and data exfiltration phases of the RSA breach and in breaches related to Java 6 and 7).

SAINT 8 addresses these problems by:

- Testing thousands of systems to identify vulnerabilities in operating systems, browsers, plug-ins, databases, network devices, and desktop, server and Web applications. This is particularly important for vulnerabilities where exploits are publicly available and popular among attackers — for example, the well-known remote command execution vulnerability in the Microsoft Windows Server Service (MS08-067) and the vulnerabilities in Oracle Java SE 7, for which users are taking weeks or months to install patches.
- Providing tools to help organizations assess users' vulnerability to phishing and social engineering attacks. An example is a phishing tool that replicates a real website, entices users to enter passwords and then collects the passwords.
- Probing endpoints to detect weak passwords, as well as servers to pinpoint weak or misconfigured security settings — for example, identifying SSL-enabled websites that still accept the SSLv2 protocol, which has known weaknesses.
- Collecting data from across the enterprise, so IT management can obtain a comprehensive picture of vulnerabilities and focus resources on high-priority issues.

Simplifying Compliance and Configuration Auditing

As shown earlier in the three excerpts from standards, typical compliance requirements include:

- Identifying vulnerabilities and assessing their potential impact (PCI DSS, HIPAA, FISMA).
- Reviewing Web applications for vulnerabilities (PCI DSS).
- Running network vulnerability scans (PCI DSS, FISMA).
- Performing penetration tests (PCI DSS).
- Implementing continuous monitoring (FISMA).

Many regulatory authorities and standards require or recommend vulnerability assessments as part of a comprehensive risk management strategy (PCI, FISMA, HIPAA, Sarbanes-Oxley, NERC CIP).

And as mentioned earlier, many other regulations, standards and auditors view these and other vulnerability management measures as necessary to "reduce risks and vulnerabilities to a reasonable and appropriate level."

SAINT 8 addresses these requirements very effectively by:

- Providing predefined scanning policies and report templates for PCI DSS, FISMA, HIPAA, SOX, NERC CIP and other standards.
- Integrating vulnerability scanning, configuration assessment and penetration testing into a single vulnerability assessment suite.
- Offering scanning approved for a variety of compliance processes by the PCI Security Standards Council, NIST, FISMA and FedRAMP.[4]

Improving IT Productivity and Management

SAINT 8 improves the efficiency of IT security and operations staff through additional services that:

- Collect vulnerability data from all types of systems and applications, to help enterprises assess risk levels across the organization.
- Provide prepackaged vulnerability scanning policies to save staff time.
- Provide the ability to create custom scan policies and vulnerability checks to support local requirements.

[1] SAINT is an Approved Scanning Vendor certified by the PCI Security Standards Council to provide scanning and attestation services; SAINT's scanning and configuration auditing capabilities have been validated by NIST as an approved SCAP solution, as an FDCC Scanner, Authenticated Configuration Scanner, Authenticated Vulnerability and Patch Scanner, and Unauthenticated Vulnerability Scanner; SAINT 8 has been approved for use in support of risk management and compliance under FISMA and FedRAMP for its vulnerability scanning and CyberScope reporting capabilities.

Return to top

- Integrate with SIEM, patch management, compliance reporting, service management and other enterprise systems so vulnerability information can be used effectively for forensics, software patching, audits and user technical support.
- Use dashboards and advanced analytics to help managers easily identify risks and quickly prioritize remediation activity.

This type of functionality should always be included in assessments of vulnerability management tools.

Better Security and Better Management

Vulnerability management is now an important topic for CIOs and IT managers as well as security experts. It is critical for risk assessment and risk mitigation, and for blocking many of the most serious targeted attacks and data breaches.

Next-generation vulnerability management products also provide key reports for compliance, showing that organizations are taking prudent steps to avoid foreseeable risks. They also help IT security and operations groups set priorities, avoid unnecessary work and respond faster to security issues.

Next-generation vulnerability management products give IT managers tools to oversee resources more efficiently and apply continuous improvement methods to security programs.