Enhanced vulnerability management process

kpmg.com
Organizations are finding it increasingly difficult to build robust vulnerability management programs due to the overwhelming number of assets, vulnerabilities, and system configurations in their environment. Valuable man-hours are being spent on tool upkeep and chasing down system owners rather than mitigating vulnerabilities or configuration issues. Enhancing the vulnerability management process not only automates these arduous tasks, but also helps to prioritize remediation efforts, creating a more effective and comprehensive vulnerability management program. The result of this method of thinking allows your security team to focus their efforts on the issues with the highest business risk and create meaningful metrics to demonstrate a reduction of risk in the environment.

What is vulnerability management?

Vulnerability management programs provide a framework in which to identify risks on key systems, gradually reduce them to business-tolerable levels, and report on progress. At a minimum, a successful vulnerability management program consists of:

1. Identification and inventory of network connected assets
2. Scanning for vulnerability and configuration issues on discovered assets
3. Prioritization and risk ranking of identified issues
4. Assignment and tracking of remediation efforts
5. Closure of the issue and the exception reporting process
6. Reporting and metrics to track remediation status, trends, and value to the business

An enhanced vulnerability management process (EVMP) is designed to automate these program aspects as much as possible so that your team is able to do more with less while accurately prioritizing efforts on issues with true business impact.

Project challenges

While many organizations have the scanning tools in place to identify these risks, very few manage to integrate them into an automated, self-sustaining, and scalable process. Many difficult questions and challenges face security teams in almost all of the areas outlined above. These include:

Asset Management: How does an organization know that it is scanning EVERYTHING in the environment? More specifically, are the network ranges being scanned by the tool accurate and comprehensive when compared against the current corporate network topology?

- Business Impact Risk Management: With the large number of findings produced as a result of the scanning efforts, are we prioritizing the findings in such a way that the most business critical findings are remediated first?

- Ownership and Accountability: As remediation tasks are identified, who are the individuals that should be tasked with actionable items?

- Reporting and Metrics: How can an organization track remediation status and progress over time?

Although all are important questions, the most pressing challenge facing organizations today is securing the manpower to adequately oversee all the aspects of this complex process.

The future state of vulnerability management

The EVMP leverages three distinct technologies that serve to automate the complex task of vulnerability management at any organization, regardless of size or industry. These three technologies include:

- Vulnerability Scanning Software
- Security Posture Management Software (SPM)
- IT – Governance, Risk Management, and Compliance (GRC) Software

Asset inventory is the primary problem that requires addressing. The SPM software is capable of collecting feeds from all networking devices in the environment in order to build a real-time, up-to-date, accurate map of your network environment. SPM will communicate any changes in the network with the other two systems so that only validated networks are scanned and reported upon.

At the completion of the vulnerability and configuration scanning process, results are automatically sent to the IT GRC system and SPM software. The IT GRC platform imports the scan data and creates a detailed record of vulnerabilities for each known live host along with a preliminary risk ranking based on the scanning engine’s built-in rating system.
Now for the neat part…

The scan results are also sent to the SPM system and actually get RE-RANKED based on what SPM knows about your network. Any number of factors can reclassify a risk rating such as:

• Accessibility from the Internet
• Sensitivity of network segment (i.e., DMZ, PCI, SOX, HIPAA, etc.)
• Existing connections to third parties
• Asset classification risk (i.e., database server, Web server, domain controller, etc.)

To illustrate; if 100 servers were noted as missing a critical patch, the SPM system will identify only the more vulnerable servers based on what it knows about your network and the asset classification value of the device. These could include hosts in the DMZ exposed to the Internet or systems in your sensitive R&D environment. These new risk ratings are then sent back to the IT GRC system where the existing risk rankings can be adjusted and updated to include the modified business risk rankings.

The IT GRC platform can automatically create tickets for your high-risk issues based on business risk and assign them to the appropriate individuals responsible for remediation efforts. Within the IT GRC system remediation time lines can be based on individual vulnerability risk ratings, business impact risk rating, or any other conceivable metric. In addition, notifications can be automatically sent for any past-due tickets, escalations, exceptions, or notification of updated reports and dashboards. Automation and scalability is the keystone to building and implementing successful vulnerability management programs in existing and future-state environments. This means making your security software work for you, not the other way around.

Success stories

Recently, KPMG LLP was approached by a FORTUNE 200 Financial Services client to help them design and implement a Global Vulnerability and Compliance Management program that would allow them to meet the strict fiduciary and legal requirements of becoming a bank holding company. The high-level objectives of this program were to:

• Design and implement a sustainable organizational model for an enterprise security vulnerability and compliance management program used to identify, prioritize, and remediate host, application, and compliance-related issues through use of a variety of automated tools.
• Integrate vulnerability data into SPM tools to accurately re-rank vulnerability ratings based on asset classification and business impact risk.
• Develop and implement an enterprise GRC platform and processes to automate and enable the security vulnerability management program.
• Build the organizational security baselines for all IT devices in the client’s environment with a focus on meeting regulatory requirements for access control, configuration control, logging, and hardening.
• Creation of comprehensive program guides that detail all aspects of the scanning, remediation, and reporting processes and integrates them in the existing organizational framework for sustaining the program and additional roll-outs.
• Retirement of redundant scanning tools and processes throughout the organization.

At the completion of this project, the client had a comprehensive, self-sustaining, scalable solution for all aspects of their vulnerability and compliance management processes. Instead of spending valuable time trying to identify where remediation efforts should be focused, they were able to utilize automated notification and reporting work flows that were based on true business impact risk metrics.

The KPMG approach

At KPMG, we customize our approach to suit our clients’ needs. Critical success factors for these engagements include:

• The depth of experience we bring with our information security services
• Our ability to team with management, implementation professionals, and internal audit personnel
• Our familiarity with integrating leading security technologies to achieve project success
• Our consistent, modular, and easy-to-use methodology
• Our knowledge of the security industry, business risk, and how to make security work for you

Benefit recap

• Accurate, real-time view of your network
• Automation of scanning; menials tasks associated with asset identification to ticketing appear seamless to the end user
• Personalization of vulnerability risk rankings based on your network and business risk
• Automation of remediation work flows and remediation progress tracking
• Reporting and metrics to measure both tactical remediation as well as long-term trends
• Scalable and sustainable approach
For further details on Identity Access Management or other Information Protection services, please contact:

**Greg Bell**  
Global Leader, Information Protection and Business Resilience  
T: 404-222-7197  
E: rgregbell@kpmg.com

**Jay Schulman**  
Managing Director  
T: 312-665-2413  
E: jschulman@kpmg.com

**Deron Grzetich**  
Senior Manager  
T: 312-665-1113  
E: dgrzetich@kpmg.com

**Aaron Hipp**  
Manager  
T: 614-241-4634  
E: ahipp@kpmg.com

Or visit our Web site at www.us.kpmg.com under Advisory Services