ITPro Today™

EXECUTIVE SUMMARY

Vulnerability Management: It's So Much More Than Patching

Nick Cavalancia, Contributor, *IT Pro Today*
Dan Richings, Vice President, Solutions & Support, Adaptiva

MARCH 26, 2019

KEY TAKEAWAYS

- Vulnerability management is a mindset: a continuous process with a detailed focus.
- Organizations need processes to detect, prioritize, resolve, and review threats.
- Employees need to be a part of the business's vulnerability management plan.
- IT teams need to focus on threat actions, points of entry, and frequency in 2019.
- Adaptiva Evolve VM provides automated next-generation vulnerability management.

in partnership with

adaptiva

Vulnerability Management: It's So Much More Than Patching

OVERVIEW

Security strategy revolves around addressing threats and vulnerabilities, which includes ensuring all systems and applications in the production environment are up to date with the proper patches, updates, and system configurations applied. With so many different systems, technologies, and devices in a single organization, knowing about and remediating every risk is a daunting task. This challenge is exacerbated by the daily onslaught of newly discovered vulnerabilities.

Vulnerability management processes can help businesses identify and fix high vulnerabilities, but the sheer number of known and yet-to-be-found software issues makes this a daunting, impossible task. Automated solutions, like Adaptiva Evolve VM, allow organizations to quickly identify and resolve issues, decreasing the risk of attack.

CONTEXT

Nick Cavalancia discussed vulnerability management and the standards and processes IT teams can use to develop a vulnerability management mindset within an organization. Dan Richings discussed the benefits of Adaptiva Evolve VM's automated solution.

KEY TAKEAWAYS

Vulnerability management is a mindset: a continuous process with a detailed focus.

Vulnerability management goes beyond just patching operating systems and applications; it's an enterprise-wide organizational mindset. Because numerous vulnerabilities are released every day, organizations need to have a continuous, detail-focused process to be successful in thwarting threats to their systems.

Several standards already exist that help organizations define vulnerabilities and develop protocols to manage them.

> We've got to make sure the organization is as secure as humanly possible all of the time. It's more of a culture, a mindset. It's a way of how we're going to operate.
>
> *Nick Cavalancia*

Vulnerability Management Standards, Configurations, and Information	
Scanning & assessing vulnerabilities	Security content automation protocol (SCAP) is an open standards-based protocol developed by the National Institute of Standards and Technology (NIST). It includes: – Management, measurement, and compliance definitions (OVAL) – Common vulnerabilities and exposures (CVE) – Common configuration enumeration (CCE) defining common configurations – Common platform enumeration (CPE) defining common platforms – Vulnerability scoring (CVSS)
Configuration baseline	Defines the baseline that should be in place and associated benchmarks. – US Government Configuration Baseline (USGCB) is limited in scope and typically focuses on older systems, but can help define baselines for older Windows systems – Center for Internet Security (CIS) offers downloadable, detailed benchmarks for numerous systems and applications – Defense Information Systems Agency (DISA) offers security technical implementation guides (STIG) for specific implementations
Vulnerability definitions	Several databases are available that identify and define CVEs along with what needs to be done for remediation. – Mitre's CVE database is the original vulnerabilities database – National Vulnerability Database pulls from other vulnerability databases to create a comprehensive database with impact and severity information – Microsoft Security Updates focuses on Microsoft-specific CVEs

Vulnerability Management: It's So Much More Than Patching

Vulnerability Management Standards, Configurations, and Information	
Vulnerability compliance	Most compliance standards offer a high level requirement to establish and maintain levels of security. The Payment Card Industry (PCI) standard is more specific and a good starting point for thinking about compliance needs. Section 11 states: – All actively and passively detected systems have been scanned in the last 90 days – No systems have exploitable vulnerabilities – No systems have critical vulnerabilities – No systems have high vulnerabilities

Organizations need processes to detect, prioritize, resolve, and review threats.

Organizations need to develop and follow a vulnerability management process that meets their needs. This includes detecting threats, prioritizing them, deploying resolutions, and reviewing and reporting on outcomes.

- **Detect** vulnerabilities using a network-based scan, at least weekly, to look externally. Use agent-based authenticated scans to view vulnerabilities from within the operating system.
- **Prioritize** issues and vulnerabilities so the riskiest are remediated first.
- **Deploy** patches, updates, and configuration changes to the affected operating systems and applications.
- **Review** the results, comparing scans after the remediation to the previous scan to understand what problems remain.

Employees need to be a part of the business's vulnerability management plan.

Employees across the organization need to understand the importance of vulnerability management and how they can help ensure the business is secure from cyberattacks. Frequent and continuous security awareness training (SAT) helps create a security culture by providing a heightened sense of awareness as well as an understanding of what is important and why.

Employee Security Training Topics

- Authentication topics, such as secure and secret passwords that are not shared with others
- Social engineering risks through phishing and other common methods
- How to handle sensitive data
- Unintentional data exposure risks, such as when a laptop is stolen
- Identifying and reporting on incidents when they occur so they can be responded to immediately

As part of the training, the security policy and an expectation of employee cooperation with assessment and remediation tasks also need to be communicated to employees.

IT teams need to focus on threat actions, points of entry, and frequency in 2019.

The SANS Institute provides a regularly updated list of the 25 most dangerous software errors. In March 2019 this list included insecure computer interactions, system resource problems, and missing defenses. While that list can help identify the latest hot vulnerabilities, the real focus for IT teams in 2019 is on more general concepts of threat actions and point of entry, as well as frequency.

Vulnerabilities to Focus on in 2019	
Threat actions and points of entry	What are the bad actors doing and how do they spread their exploits? What points of entry are most vulnerable to an attack? – Email attachments and links, and how to secure the operating system against these threats – Web links, and how to prevent the browser from automatically downloading viral scripts and other items – Microsoft Office and other third-party applications containing malicious items and scripts
Frequency	How often are vulnerabilities exploited and are scans frequent enough for resolution? – Zero day exploits – More frequent scans and remediation

Vulnerability Management: It's So Much More Than Patching

Adaptiva Evolve VM provides automated next-generation vulnerability management.

Most organizations cannot keep up with the volume of vulnerabilities, even when using assessment tools. This results in a general philosophy of partial remediation, which can leave them open to attack.

Adaptiva Evolve VM provides an automated, next-generation vulnerability management solution that follows the full cycle of vulnerability management: detection, prioritization, remediation, and review.

> Attackers don't necessarily focus on vulnerability severity when they're planning an attack. They also have first mover advantage and they don't hesitate to exploit low criticality vulnerabilities.
>
> *Dan Richings*

Evolve VM resolves vulnerabilities and compliance issues in minutes, rather than the months it can take to detect and remediate security issues. The next generation:

- **Is resolution focused** rather than assessment focused, designed for finding and fixing problems as quickly as possible.
- **Is network protective** rather than network intensive; the solution uses peer-to-peer powered assessment and remediation to negate network degradation.
- **Triggers remediation automatically** rather than waiting on service desk tickets to move through process timelines.
- **Uses self-managed automation** instead of manual administration.

The solution includes an interactive dashboard, endpoint compliance and vulnerability checks, and real-time remediation actions. It also includes a visual workflow designer and engine, allowing IT teams to create custom compliance and security checks, easily integrating with other third-party products.

ADDITIONAL INFORMATION

For more information on Adaptiva Evolve VM or to set up a demo, visit http://www.adaptiva.com.

Vulnerability Management: It's So Much More Than Patching

BIOGRAPHIES

Nick Cavalancia

Contributor, *IT Pro Today*

Nick Cavalancia has over 25 years of enterprise IT experience, is an accomplished consultant, speaker, trainer, writer, and columnist, and has achieved industry certifications including MCSE, MCT, Master CNE and Master CNI. Nick has owned an MSP focused on the SMB, an enterprise IT consulting company, and today runs Techvangelism, where he serves the IT community as technical evangelist, working with some of the most recognized tech companies today. Nick has authored, co-authored and contributed to nearly two dozen books on Microsoft technologies, and regularly speaks, writes and blogs on a variety of topics.

Dan Richings

Vice President, Solutions & Support, Adaptiva

Dan Richings, VP of Solutions & Support, based in the UK, drives Adaptiva's outstanding engineering and exceptional customer experience throughout EMEA. Dan has an extensive technical skill set, and has been working with SCCM since it was still "SMS." He has been performing operating system deployment since 2001. His diverse background includes technical and leadership roles in the retail automotive, multinational engineering, and international project development and construction industries. Dan holds a computer science degree, BSc (Hons) Computing, from Swansea University. In his free time, Dan enjoys racquetball, airsoft, and karting.