Key Trends Redefining Vulnerability Management Programs and Operations

Author:

Vinod Vasudevan,
CTO, Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

After years spent in a comfortable routine, vulnerability management is now being forced to improve its performance. The current programs are increasingly ill-adapted to new modes of attack and an accelerating pace of business. Although organizations periodically run configuration audit and network scanning tools, considerable time and effort are spent on discussing the results, coordinating responses, and tracking closures. Consequently, the end mitigation is slow and partial. At any given time, there may be a large gap between the number of vulnerabilities reported and their actual closures of vulnerabilities. As a result, both protection and productivity suffers.

> "Established vulnerability management is ill-adapted to new modes of attack and an accelerating pace of business. Forward-looking CISOs already know that their VM programs need to be repositioned."

Forward-looking Chief Information Security Officers (CISOs) are changing their VM programs to shift the focus from running scans to reducing the impact of vulnerabilities on the organization. Paladion gathered insights from CISOs about the future of VM programs in their enterprises in different industry segments, identifying key trends likely to now apply to organizations everywhere.

Centralizing Vulnerability Assessment

Many organizations still use a siloed approach to vulnerability assessment. For instance, application security assessment is run as a separate program from network scanning. Secure configuration reviews are conducted as yet another activity. As a result, there is no single view of vulnerability for an asset across all the IT resources involved for that asset. An attacker on the other hand sees all the vulnerabilities of an asset and can exploit any holes in or between resources to begin attacks.

Newer vulnerability management programs centralize all vulnerability assessments, enabling viewing and correlation of all vulnerabilities across the entire IT stack. So, you get to know the overall exposure to an asset and are able to drive remediation based on the asset risk rather than individual vulnerability risk.

Treating All Assets Equal for Vulnerability Testing

So far, the frequency of vulnerability testing has often been governed by the value of the assets to be tested. Higher value assets are tested more often. This technique to optimize cost and effort may have been suitable for the past. Today, however, the risks are different. Perpetrators of targeted attacks now use vulnerabilities anywhere in an IT environment and daisy-chain them to advance towards their end-goals inside the network. A vulnerability in a low value asset can be as critical as a vulnerability in a high value asset if it can be used for propagation. Testing that is staggered in time simply according to the different categories of assets is no longer suitable.

> "Perpetrators of targeted attacks now use vulnerabilities anywhere in an IT environment and daisy-chain them to advance towards their end-goals inside the network."

Instead, scans and tests must be done according to the real vulnerability profile of the organization. Defining this profile, updating it as required, and vulnerability information is paramount. All assets are equal, so the scans and tests should be performed based on the vulnerability profile for a business process or organization.

Running Vulnerability Management as Continuous Operations

Digital transformation is resulting in fast paced changes to IT network and systems. Agile software development releases codes and applications much faster. Attacks in cyberspace are constantly evolving. However, vulnerability testing schedules are sporadic. Threat management through a Security Operations Center has become a continuous operation while vulnerability management lags behind considerably.

Vulnerability management data is only as good as the last version available. Today, most vulnerability assessment tools place no limit on the number of times they are run against an asset. Therefore, tools at network, config, application, or code levels should be run as continuously as conditions permit to allow the organization to stay informed of current threats and security gaps. This may be daily or at least weekly for all assets across all IT stacks. The only exception may be deep, manual testing where effort and complexity may mean a different periodicity.

Prioritize, prioritize, prioritize

Continuous vulnerability checks for all assets across all layers will generate voluminous amounts of data. Even with the lower frequency testing used till now, vulnerability data is quite large and hence remediation lags behind. In most organization, average remediation times have often been well over 60 days.

The solution is a better method for prioritizing the vulnerabilities. So far, organizations have often only applied generic severity ratings in their prioritization of vulnerabilities. They have not systematically gathered threat and exploit data to understand which threats truly materialized. Today, more threat intelligence exists on the vulnerabilities that are in fact exploited. By applying this threat intelligence, organizations can focus on those vulnerabilities that are actually exploited by attackers.

The second factor in prioritizing vulnerabilities is to consider the contextual information. These are around asset details and valuation, network propagation, mean time to remediation, past trends in vulnerabilities, and compensatory controls. Using a security analytics platform such contextual data can be gathered and applied for vulnerability prioritization continuously for every test result.

The third aspect in prioritization, when considering continuous testing is to automate the process to de-duplicate vulnerabilities and assets and to remove false positives across multiple tests. In this way, only new vulnerabilities and changed assets 'bubble up'.

"A prioritization engine can pick out the 2% of vulnerabilities that truly require remediation."

Beyond Detecting Vulnerabilities – Detecting Compromises Too

Recent cyberattacks, more powerful technology, and better organized cybercriminals have led many CISOs to the same conclusion. A security breach is no longer a matter of if, but when. It makes sense for a vulnerability management program to use the same assumption. Not only should vulnerabilities be spotted before attacks, but any signs of such attacks in progress should be detected too. For instance, attacks may exploit vulnerabilities and leave traces in the form of modified configurations.

Today, organizations are running tools to detect indicators of compromise in an asset in parallel with detecting vulnerabilities and weak configurations. In addition, the vulnerability assessment output is getting analyzed for potential compromise scenarios, leveraging data from past breaches in the industry or models of attack trees of linked vulnerabilities.

Automate Mitigation with Security Orchestration

Just as vulnerability assessment must be orchestrated to cover all assets, mitigation can be orchestrated in order to optimize effectiveness and rapidity. Many vulnerabilities can be prevented from being exploited by using the right rules in blocking devices. Examples include an IDPS (intrusion detection and prevention system) or a WAF (web application firewall.) These devices can act as virtual patches for your assets and can be deployed immediately. This is much faster than the days or weeks it usually takes to remediate vulnerabilities. Similarly, automated system administration tools can be used for remediating actions such as configuration changes, deletion of accounts, and patching.

"Virtual patches in the form of an IDPS and WAF can be deployed immediately for your assets."

Digital VM Platforms for Assessment, Reporting, Response, and Tracking

Vulnerability management programs have suffered for too long from cumbersome processes. Tasks executed via paper-based and manual processes have included planning and scheduling of tests, exchanging information for initiating tests, dissemination of test results, negotiations of prioritization, distribution of responsibilities for remediation, and information exchange for carrying out mitigation.

At the same time, businesses are moving towards making their entire user experience more digital. They give employees and customers faster access to information, easier interaction, and simpler processes. These improvements are also being applied to vulnerability management in forward organizations. The entire process can be made seamless and automated through digital platforms serving testers, security analysts, asset owners, administrators and senior management. The right digital VM platform can cover vulnerabilities and threats in code, systems, networks, and business logic; providing threat profiles for applications to help developers build better, safer software, delivered on time, every time.

"The right digital VM platform covers vulnerabilities in code, systems, networks, and business logic."

A digital platform also makes it easier to create and disseminate reports using key metrics like mean time to remediate, most vulnerable assets, and frequently occurring vulnerabilities, to track meaningful progress.

Compliance with requirements and standards such as PCI, SANS, OWASP, and OSSTM can be automatically checked and any issues flagged for resolution.

Conclusion

Vulnerability management is changing today to become more efficient in mitigating vulnerabilities and reducing the attack surface through continuous testing for security gaps. This is achieved through threat and context focused prioritization, automation of mitigation, and digitalization of all processes. New vulnerability management platforms can help organizations implement and achieve such a vulnerability management program swiftly.

Paladion's vulnerability management solution offers expert security resources and advanced cyber technology for vulnerability management programs. Paladion's proprietary VM platform performs customized, frequent, in-depth testing of critical IT assets. It also insures baseline assessments for all other assets. Through effective identification and mitigation of threats, customers benefit from an improved defense-in-depth security posture.

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net