eBook

Best Practices for Vulnerability & Patch

As cybercrime explodes so does the need for best practices to help protect your company from hackers

CALIAN®

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

The Reality of Cyber Attacks

The threat is real—these statistics illustrate the severity and reality of cyber attacks.

- Every 39 seconds there is an attack (Security Magazine, 2017)
- Hackers create 300,000 new pieces of malware daily (Source: McAfee)
- 66% of businesses attacked by hackers aren't confident they can recover (Source: Fortune)
- 43% of cyberattacks target small business and 60% of small companies go out of business within six months of a cyberattack (Small Business Trends, 2019)

These statistics aren't surprising in light of edgescan's *2019 Vulnerability Statistics Report*: the most common infrastructure vulnerabilities in 2018 included systems with exposed Common Vulnerabilities and Exposures (CVE) not being patched regularly (p. 6); and according to 2018 threat intel, DoneRDP (Remote Desktop) vulnerabilities were also relatively common and a popular target for attackers (p. 2). Cross-Site Scripting, both reflected and stored, was the most common vulnerability in 2018 at 14.69% (p. 9).

Further findings from edgescan's report show that 33.33% of all high and critical risk vulnerabilities discovered in 2018 were in relation to unsupported Windows Server 2003 systems (no patching, support, end-of-life systems) (p. 10).

These are only a few of the many vulnerabilities highlighted in edgescan's report—which underscores and highlights the urgent need for establishing vulnerability and patch management best practices, as well as guidelines for meeting compliance regulations. This is essential when you consider that 73% of black hat hackers (those with criminal intent) said traditional firewall and antivirus security are irrelevant or obsolete (Hosting Tribunal, n.d.).

Compliance through SIEM

Think about the escalating threats from faceless cybercriminals and the countless vulnerabilities created by people, process and technology—and all the while your business must remain in compliance. In other words, it is imperative to ensure that your IT department has a comprehensive, risk-based approach to managing security with supporting policies, regular scanning for validation, and continuing control enhancements that will identify weaknesses. Side by side with an effective vulnerability management structure, you should be able to fight off malicious attacks and keep those thieves in the night, aka hackers, from continually threatening your business.

An integral part of protecting your business is to implement Security Incident and Event Management (SIEM) and log management. These do not completely protect your business, but they are an important part of your cybersecurity arsenal that will help you to identify and manage threats by monitoring security events and alerts. Crucially important considering the prevalence of compliance mandates that are putting stress on the

At the least, to ensure compliance you should:

- Implement an internal process for handling threats listing vendors, key personnel, responsibilities, and deadlines
- Define the scope of coverage
- Log all applicable events to meet those regulations that require a detailed report of each event
- Highlight events that appear to be threats and describe actions taken and the results
- Document timing, details, and location of event logs

Defeat Threats via Vulnerability Management

Gartner says it best: “A vulnerability is only as bad as the threat exploiting it and the impact on the organization. Security and risk management leaders should rate vulnerabilities on the basis of risk in order to improve vulnerability management program effectiveness” (2019).

Thus, implement a vulnerability management program on the basis of the risk—the threat that is exploiting the vulnerability. To accomplish this, execute vulnerability management best practices.

1. Understand your intricate and pliable attack surface

This is fairly obvious. You must have in-depth knowledge of your attack surface and of what vulnerabilities might exist. Traditionally, the network infrastructure has always been scanned, but today that is not enough: the attack area is complex, borderless, and connected to everyone and everything. It’s practically an open doorway inviting hackers to enter and explore.

The attack surface includes containers, mobile devices, IoT devices, cloud instances, web applications, and point-of-sale (POS) terminals. Endpoints—more than 200 billion connected devices by 2020—are a massive, growing attack surface and, as a result, cybercriminals will exploit their vulnerabilities (Intel, n.d.). Additionally, there are also traditional enterprise assets that are dynamic and interconnected. A cyberattack is just a matter of when.

Therefore, rate vulnerabilities on the basis of risk, look at what the risk is, list your risks in order of priority, and see how to reduce them in the most cost-effective way possible—all while ensuring you meet compliance regulations. The repercussions of non-compliance can be devastating to the business: statutory or legal penalties, damage to the company's reputation, loss of customers’ trust, and so on.

When prioritizing your risks take note of Gartner’s statement: “Vulnerability rating schemes that don’t take into account what threat actors are leveraging in the wild can cause organizations to address less risky issues first” (SecurityIntelligence, 2018).

2. Tap into Threat Intelligence

In its *Implement a Risk-Based Approach to Vulnerability Management* report, Gartner focused on a risk-based approach for a vulnerability management process and used threat intelligence for prioritizing remediation (2019).

Tapping into intelligence such as this helps to fine-tune processes and to kick-start preemptive actions such as patching by using threat landscape trends to guide prioritization and decision making.

3. Manage Open Source Vulnerabilities

WhiteSource’s *Open Source Vulnerability Management Report* surveyed over 650 developers and found that open source vulnerabilities rose by over 60% in 2017 as compared to 2016 (Goldstein, n.d.).

It is difficult to know if the open source components used in your applications are up-to-date with all critical patches applied. To keep your open source software components risk free, you must continually track your open source components and their dependencies, while keeping abreast of open source community intelligence and updates through automated open source management tools.

4. Adopt a DevSecOps Approach

Adopt a DevSecOps approach, one that incorporates tools for tracking, detection, remediation, and patching. By integrating security practices within the DevOps process, you bring IT and security together, enabling your development and security teams to make decisions based on real-time data. Through automating vulnerability detection, remediation, and patching, your teams can then take the data, filter out what is most relevant to them, and prioritize their tasks—all based on real-time data.

Patching Best Practices

Patch management should be a program, not a project as patching has become increasingly important: as cybercrime grows so does the necessity of patching quickly. Many breaches have occurred because patches weren't applied right after release, giving cybercriminals unbelievable opportunities: when a patch is released, the vulnerability is disclosed.

The picture here is clear—patch as soon as you can because it's a race between the company and the cybercriminal as to who does what first. Think of it this way: not patching leaves your customers' sensitive data exposed and your company at risk.

Here are three examples showing what happens without a stringent patching program. In a Ponemon Institute study, 57% of respondents reported their companies had one or more data breaches that could have occurred because a patch was available for a known vulnerability, but not applied (2018, p. 5). Equifax had a two-month-old unpatched Apache Struts vulnerability (Goodin, 2017). And SingHealth had data for 1.5 million patients exposed because of an outdated version of Outlook (Yu, 2018).

One way to keep your systems and applications running smoothly and safely is to automate as much as you can. Manual processes cannot help you guard the gates. With cloud-based automated patch management software you can schedule regular scans and ensure patches are applied under specific conditions or automatically.

These patching best practices will help to ensure the smooth running of your systems and applications:

- ✓ Automate patch management
- ✓ Compile a comprehensive network inventory
- ✓ Identify an exploit then review its vulnerability and exposure
- ✓ Segment managed systems and users based on risk and priority
- ✓ Keep up-to-date on vendor patch releases and vulnerability disclosures
- ✓ Evaluate patches in a test environment, simulate the operational environment, and test for software compatibility
- ✓ Distribute patches after testing
- ✓ Monitor the patched production system for any issues unidentified during testing
- ✓ Audit patches for performance issues and compatibility
- ✓ Apply application patches as quickly as possible
- ✓ Generate detailed patch audit reports

CALIAN®

Reality and the Future

Trying to keep pace with the endless onslaught of security vulnerabilities is an unending task for IT and security teams. The National Vulnerability Database (NVD) shows that historically the industry will see around 5,000 to 7,000 CVEs released each year. These numbers, however, spiked in 2017 to 14,649, continuing to climb to 16,515 in 2018. There are no signs of it slowing down (NVD n.d. as cited in Mukkamala, 2019).

The reality is that malicious attacks will continue to increase in lockstep with the number of vulnerabilities and exposures that are released. This is not to say that all vulnerabilities will be exploited. But, based on these numbers, it is now more important than ever before to build your cybersecurity arsenal with every tool available.

Add vulnerability and patch management programs and best practices to your cybersecurity arsenal. Future proof your security—make sure that what works today, works tomorrow.

CALIAN®

Contact us for a free consultation or to receive a free cloud security audit to assess the effectiveness of your current cybersecurity initiatives.

☎

1.877.225.4264

www.calian.com

CALIAN ®

References

Security Magazine (2017, March 21). *Keep Calm and… Here is a List of Alarming Cybersecurity Statistics*. Retrieved from https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

Small Business Trends (2019, August 22). *Cyber Security Statistics: Numbers Small Businesses Need to Know*. Retrieved from https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

edgescan (2019). *2019 Vulnerability Statistic Report*. Retrieved from https://www.edgescan.com/wp-content/uploads/2019/02/edgescan-Vulnerability-Stats-Report-2019.pdf

Hosting Tribunal (n.d.) *40 Stunning Hacking Statistics that concern us all in 2019*. Retrieved from https://hostingtribunal.com/blog/hacking-statistics/

Gartner (2019, May 6). Gartner Report: *Vulnerability Management via a Risk-Based Approach*. Retrieved from https://www.bankinfosecurity.com/whitepapers/implement-risk-based-approach-to-vulnerability-management-gartner-w-4810

Intel (n.d.). A Guide to the Internet of Things. *How billions of online objects are making the Web wiser*. Retrieved from https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

SecurityIntelligence (2018, September 13). *New Gartner Report Recommends a Vulnerability Management Process Based on Weaponization and Asset Value*. Retrieved from https://securityintelligence.com/new-gartner-report-recommends-a-vulnerability-management-process-based-on-weaponization-and-asset-value/

Goldstein, Ava (n.d.). *Learn From the Best: Vulnerability Management Best Practices from the Best in the Business*. Retrieved from https://resources.whitesourcesoftware.com/blog-whitesource/vulnerability-management-best-practices

Ponemon Institute (2018, June). *Separating the Truths from the Myths in Cybersecurity*. Retrieved from https://www.ponemon.org/local/upload/file/BMC%20Consolidated%20Report%20Final.pdf

Goodin, Dan (2017, September 13). *Failure to patch two-month-old bug led to massive Equifax breach. Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers*. Retrieved from https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

Yu, Eileen (2018, September 21). *SingHealth data breach reveals several 'inadequate' security measures*. Retrieved from https://www.zdnet.com/article/singhealth-data-breach-reveals-several-inadequate-security-measures/

Mukkamala, Srinivas (2019, June 12). *Predicting Vulnerability Weaponization*. Retrieved from https://www.darkreading.com/threat-intelligence/predicting-vulnerability-weaponization/a/d-id/1334919