Vulnerability Management: Your Questions,...

NOVEMBER 2020 Synack

Over the past few years, we've had news of massive data breaches within the most respected companies. In 2020, Twitter reported a breach of its platform, with captured Twitter handles being ransomed for $1000 to $2000 apiece. Fake tweets were sent out in retaliation for non-compliance. This same year, Marriott Hotels suffered a data breach, resulting in 5.2 million customers impacted.

Suffering an IT incident like this can be devastating for management and terrifying for customers. As such, it's important to know how to protect yourself and your business. With that in mind, we're dedicating today's blog to the topic of security and vulnerability management, and what it means for your business.

What is Vulnerability Management?

According to Gartner, “an effective vulnerability management program requires consistent processes, business context, risk prioritization, timely remediation, mitigation, actionable metrics, and all of this without business disruption and zero forbearance for business consequences.” Vulnerability management is an established IT practice and must not be confused with the more focused techniques of vulnerability assessment.

Vulnerability management tends to be very reactive. Proactive vulnerability management is a better approach. It involves much more than simply patching vulnerabilities as they appear. It is a proactive discipline that surveys the entire IT infrastructure of your organization and seeks to patch gaps in the infrastructure before they appear. This is much more than simply patching known vulnerabilities. Vulnerability management involves IT security awareness and dealing with gaps across the entire organization.

What is Considered a Vulnerability?

Any means by which a bad faith actor can gain control of a service endpoint, application, server, or information can be considered a vulnerability. These can include the following:

Programming or software bugs

Incorrectly configured software installations

Mobile devices and virtual servers

Web apps, containers, IoT devices

Cloud infrastructure

As technology progresses and the pace of software development and code releases accelerates, vulnerability points increase.

What is the Difference Between Vulnerability Management and Vulnerability Assessment?

Vulnerability management is an ongoing process of securing an organization's IT infrastructure versus attack, while the purpose of vulnerability assessment projects are short-term efforts that identify your organization's immediate vulnerabilities. VA vulnerability assessment efforts and penetration tests are just one part of keeping your IT assets safe. With teams pushing code at a practically continuous cadence, CISOs can no longer only rely on point-in-time, check-the-box security testing. The increasingly dynamic and complex attack surfaces of today's digital environment require a more agile model than traditional penetration testing and more control and quality insights than other crowdsourced solutions. Because attack surfaces are constantly evolving, access to cybersecurity expertise and adversarial insights are critical to identify and resolve exploitable vulnerabilities.

IT vulnerability assessments will usually include a series of tests to determine how vulnerable your organization and its assets are. An important point to remember is that *vulnerability assessments are part of vulnerability management, not a replacement.* Vulnerability management, conversely, is a long-term cyclical practice that is essential for any company.

According to the SANS Institute, a long-term vulnerability management strategy contains six different components:

Asset Inventory

This is a full inventory of all IT resources and assets – data centers, servers, software resources, and a survey of all corporate networks, including third-party solutions.. In fact, an organization's security score can drop by 5-15% when expanding the scope of testing to include 3rd party assets.

Information Management

These are human security related issues. Beyond the usual password discipline and such, this concerns how much knowledge of assets is released to the public, consideration of the personnel who have control of assets, and estimating how attackers might exploit weak points using social engineering.

Risk Assessment

Risk assessment is understanding how the practice of the organization's day to day business can expose it to risk, especially on an interdepartmental level.

Vulnerability Assessment

A Vulnerability Assessment is a key ingredient of a vulnerability management program This is the aforementioned outside audit that identifies avenues of attack. This is also often called *vulnerability analysis.* This involves extensive system vulnerability scanning for broad attack surface coverage and other tests for additional security insight.

Reporting and Remediation

This is where the results of risk and vulnerability assessments are submitted with recommendations to remediate the outstanding issues in the short term along with suggestions for long term security strategy.

Response Planning

This is planning for how to respond in the face of catastrophic security events, such as a data breach or a large-scale ransomware attack.

What is the Vulnerability Management Process?

While the step above is part of the security vulnerability assessment, the vulnerability management process is a continual strategy that is adjusted for the marketplace and various other factors. This process should be included in management's normal process of business strategy.

The cycle looks like this:

Discover

This stage takes inventory of all IT and business assets involved in operations.

Prioritize

The assets now need to be segmented into groups and prioritized based on importance to business function.

Assess

Next is assessing a base level of risk with each asset and what your organization can tolerate. This process is ongoing as you remediate issues and establish a baseline of risk tolerance for your various assets.

Verify and Report

Additional scans and tests are conducted using vulnerability assessment tools after remediation takes place. Staff creates reporting presentations for both the C Suite as well as internal use. Using Synack's platform, customers are provided with The Synack Attacker Resistance Score (ARS) rating that

provides a realistic assessment of assets' actual hardness against attack based on penetration test performance data. It's empirical, not theoretical, and all the more powerful as a result.

Vulnerability Management Solutions

Several providers have platforms that enable company IT staff to perform scans and otherwise check daily and weekly for vulnerabilities. IT Staff should use a vulnerability management system, ideally one with a real-time view of top exploitable vulnerabilities and expert remediation guidance, in conjunction with an outside firm to perform quarterly and yearly audits, while advising on a long-term strategy to keep the organization's assets secure.

Synack's continuous crowdsourced security platform was built to augment security teams so they can find and fix vulnerabilities more effectively and efficiently than alternative methods – all in a single, integrated platform.

Vulnerability Management & Best Security Practice: Synack Has Your Answers

At Synack, we deal with vulnerability management every day. Instead of leaving your organization's assets to chance, today is a good time to have a conversation with us about how we can help you implement a vulnerability management strategy that will protect your business and your customers. Contact us to learn more about our security testing products and solutions.

Related Articles



Seatbelts, Airbags and your Cybersecurity

Charlie Waterhouse
29 OCTOBER

Cloud Exploits: The Risk From Subdomain Takeovers and How to Prevent Them From Happening

Andy Condliffe
9 OCTOBER

Cloud Security on the Rise

Synack
8 OCTOBER

Got questions?

Contact Us

DC 38°90'72" N
77°03'69" W